English

FUJITSU Server BS2000

# SE700 / SE500 / SE300

Administration and Operation

User Guide

Valid for:

M2000 V6.1A
X2000 V6.1A
HNC V6.1A

Edition November 2015

## Comments… Suggestions… Corrections…

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

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

## Certified documentation according to DIN EN ISO 9001:2008

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

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

## Copyright and Trademarks

The Linux-based basic software M2000, X2000, and HNC which is installed on the Management Unit, Server Unit x86, and HNC contains Open Source Software. The licenses for this can be found in the LICENSES directory on the relevant installation DVD.

# Contents

1 Introduction . . . 11

1.1 Documentation for the SE servers . . . 13
1.2 Objective and target groups of this manual . . . 14
1.3 Summary of contents . . . 15
1.4 Changes since the last edition of the manual . . . 16
1.5 Notational conventions . . . 17
1.6 Names and abbreviations . . . 18
1.7 Open Source Software . . . 19

2 Architecture and strategies . . . 21

2.1 Architecture . . . 21
2.2 Software of the SE server . . . 24
2.2.1 Structure of the software . . . 24
2.2.2 Software status, system version and update status . . . 25
2.2.3 Updates to the basic software and add-on packs . . . 26
2.2.3.1 Naming conventions . . . 27
2.2.3.2 Security fix . . . 27
2.2.3.3 Service pack . . . 28
2.2.3.4 Hot fix . . . 28
2.2.3.5 Add-on pack . . . 28
2.2.4 Management applications . . . 30
2.3 Networks . . . 31
2.3.1 Services . . . 33
2.3.1.1 IPv6 autoconfiguration . . . 33
2.3.1.2 Domain Name System (DNS) . . . 34
2.3.1.3 Managing the "senet" domain . . . 34
2.3.1.4 ACL functionality . . . 35

2.3.1.5 NTP server . . . 36
2.3.2 Integration of BS2000 into the SE Manager . . . 36
2.3.3 Integration of BS2000 into the LAN . . . 37
2.3.4 Integration of the XenVM guest systems into the LAN (only SU x86) . . . 39
2.3.5 Overview of the possible LAN connections of the VMs . . . 40
2.3.6 Important information about IP configuration . . . 41

**2.4 Management Unit and SE Manager . . . 42**
2.4.1 Role and user strategy . . . 42
2.4.2 IP-based access to the Management Unit . . . 45
2.4.3 Redundant Management Units . . . 46

**2.5 Virtualization . . . 48**
2.5.1 Implementing VM2000 . . . 48
2.5.2 Virtualization on Server Unit x86 . . . 51
2.5.2.1 CPU pool management . . . 53
2.5.2.2 Main memory management . . . 55
2.5.2.3 BS2000 devices . . . 55
2.5.2.4 XenVM devices . . . 56

**2.6 Customer Support and maintenance . . . 60**
2.6.1 Tasks of Customer Support . . . 60
2.6.2 Tasks of the customer . . . 60
2.6.3 Maintenance and remote service . . . 62
2.6.4 Handling updates . . . 62
2.6.4.1 Providing updates . . . 62
2.6.4.2 Tasks and responsibilities when installing updates . . . 63

**3 Operating the SE Manager . . . 65**

**3.1 Calling the SE Manager . . . 66**
3.1.1 Logging in . . . 67
3.1.2 Logging out . . . 67

**3.2 Session management . . . 68**
3.2.1 Session timeout . . . 68
3.2.2 Automatic update . . . 69

**3.3 SE Manager interface . . . 70**
3.3.1 Window types . . . 70
3.3.2 Main window . . . 71
3.3.3 Terminal window . . . 74
3.3.4 The dialog . . . 76
3.3.5 The wizard . . . 77
3.3.6 Web UIs of Application Units . . . 78

**3.4 Working with the SE Manager . . . . . . . . . . . . . . . . . . . . . . . . . . . 79**
3.4.1 Calling an object or function in the SE Manager . . . . . . . . . . . . . . . . . . . 79
3.4.2 Navigation . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 80
3.4.3 Filtering and sorting a table . . . . . . . . . . . . . . . . . . . . . . . . . . . 82
3.4.4 Executing an action . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 83
3.4.5 Calling the online help . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 85
3.4.6 Error handling . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 87

**4 Dashboard . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 89**

**5 Operating and managing systems on Server Units . . . . . . . . . . . . . . . . 93**

**5.1 Setting BS2000 operation mode . . . . . . . . . . . . . . . . . . . . . . . . . . 95**
5.1.1 Server Unit /390 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 95
5.1.2 Server Unit x86 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 97

**5.2 Opening the BS2000 console and dialog window . . . . . . . . . . . . . . . . . 99**
Messages on the BS2000 console . . . . . . . . . . . . . . . . . . . . . . . . . . 99

**5.3 SVP console on Server Unit /390 . . . . . . . . . . . . . . . . . . . . . . . . . 101**

**5.4 Working in Native BS2000 mode . . . . . . . . . . . . . . . . . . . . . . . . . 102**
5.4.1 Starting (IPL) and shutting down a BS2000 system, executing an IPL dump . . . . . 102
5.4.2 Setting options . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 102
5.4.3 Evaluating KVP logging . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 103

**5.5 Working in VM2000 mode . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 105**
5.5.1 VM administration . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 105
5.5.2 Managing VM resources . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 106
5.5.3 Setting VM options . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 107
5.5.4 Operating a VM . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 108
5.5.4.1 Start and shut down a BS2000 guest system, create a dump / enable and disable (and delete) a BS2000 VM . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 109
5.5.4.2 Managing devices of the VM . . . . . . . . . . . . . . . . . . . . . . . . . . 110

**5.6 Working in XenVM mode (on Server Unit x86) . . . . . . . . . . . . . . . . . . 115**
5.6.1 VM administration . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 115
5.6.2 Managing VM resources . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 118
5.6.3 Tracking VM installation . . . . . . . . . . . . . . . . . . . . . . . . . . . . 119
5.6.4 Setting VM options . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 121
5.6.4.1 Defining the remaining runtime for shutdown . . . . . . . . . . . . . . . . . . 121
5.6.4.2 Setting VM-specific options (auto start and delay) . . . . . . . . . . . . . . . 122

5.6.5 Operating a VM . . . 123
5.6.5.1 Displaying VM information . . . 123
5.6.5.2 Opening the console of the XenVM . . . 123
5.6.5.3 Starting and shutting down the XenVM . . . 124
5.6.5.4 Changing the configuration of the XenVM . . . 125
5.6.5.5 Managing devices of the XenVM . . . 126

**6 Operating and managing systems on Application Units . . . 133**

**6.1 Operating a Native system . . . 133**

**6.2 Operating virtual machines . . . 135**

**6.3 Installing an operating system on an Application Unit . . . 137**

**7 Managing applications . . . 141**

**7.1 SE Management applications . . . 143**
7.1.1 BS2000 Backup Monitor . . . 143
7.1.2 openUTM WebAdmin . . . 144
7.1.3 ROBAR . . . 144

**7.2 Managing user-defined management applications . . . 146**

**7.3 Administering user-defined links . . . 147**

**8 Monitoring performance . . . 149**

**9 Managing devices . . . 151**

**9.1 Managing BS2000 devices . . . 152**
9.1.1 Device addresses . . . 152
9.1.2 Device management on Server Unit /390 . . . 154
9.1.2.1 Predefined BS2000 devices . . . 154
9.1.2.2 Device connection via Management Unit and HNC . . . 155
9.1.2.3 Configuration in IORSF files . . . 156
9.1.3 Device management on Server Unit x86 . . . 157
9.1.3.1 Predefined BS2000 devices . . . 157
9.1.3.2 Connection of peripheral devices . . . 157

9.1.4 Managing disks . . . 159
9.1.4.1 Displaying generated disks on Server Unit /390 . . . 159
9.1.4.2 Managing disks on Server Unit x86 . . . 160
9.1.5 Managing KVP devices . . . 162
9.1.6 Managing LAN devices . . . 166
9.1.7 Managing tape devices . . . 168
9.1.7.1 Emulated tape devices . . . 170
9.1.7.2 Emulated tape devices from the BS2000 viewpoint . . . 172

**9.2 Managing XenVM devices on Server Unit x86 . . . 175**
9.2.1 Managing disk pools . . . 175
9.2.2 Managing virtual disks . . . 178
9.2.3 Managing virtual switches . . . 180
9.2.4 Managing installation sources . . . 182

**10 Managing hardware . . . 183**

**10.1 Managing units of the SE server . . . 184**
10.1.1 Powering a unit on or off, rebooting a unit . . . 184
10.1.2 Managing the Server Unit /390 . . . 187
10.1.2.1 Displaying system information and interfaces of the SU /390 . . . 187
10.1.2.2 Displaying the IP configuration of the SU /390 . . . 187
10.1.3 Managing the Management Unit . . . 189
10.1.3.1 Displaying system information and interfaces of the Management Unit . . . 189
10.1.3.2 Managing the IP configuration . . . 193
10.1.3.3 Managing routing of the Management Unit . . . 195
10.1.3.4 Managing the DNS configuration . . . 196
10.1.3.5 Managing SNMP . . . 197
10.1.3.6 Setting the system time (time synchronization or local) . . . 199
10.1.3.7 Entering CLI commands . . . 201
10.1.3.8 Managing updates of the Management Unit . . . 202
10.1.3.9 Managing configuration data (CSR) of the MU . . . 204
10.1.3.10 Generating diagnostic data . . . 205
10.1.3.11 Managing service access . . . 206
10.1.4 Managing the HNC . . . 209
10.1.4.1 Displaying system information and interfaces of the HNC . . . 209
10.1.4.2 Managing the IP configuration of the HNC . . . 212
10.1.4.3 Managing routing of the HNC . . . 213
10.1.4.4 Displaying the DNS configuration of the HNC . . . 214
10.1.4.5 Configuring Net-Storage on the HNC . . . 214
10.1.4.6 Managing updates . . . 217
10.1.4.7 Managing configuration data (CSR) of the HNC . . . 217
10.1.4.8 Generating diagnostic data . . . 218

10.1.5 Managing Server Unit x86 . . . 219
10.1.5.1 Displaying system information and interfaces of the unit . . . 219
10.1.5.2 Managing the IP configuration of the SU x86 . . . 222
10.1.5.3 Managing routing of the SU x86 . . . 222
10.1.5.4 Managing the DNS configuration of the SU x86 . . . 223
10.1.5.5 Configuring Net-Storage on the SU x86 . . . 223
10.1.5.6 Managing updates of the SU x86 . . . 226
10.1.5.7 Managing configuration data (CSR) of the SU x86 . . . 226
10.1.5.8 Generating diagnostic data . . . 227
10.1.6 Managing Application Units . . . 228
10.1.6.1 Configuring an Application Unit . . . 228
10.1.6.2 Displaying hardware information of the Application Unit . . . 230
10.1.6.3 Managing the IP configuration of the Application Unit . . . 231

**10.2 Managing IP networks . . . 233**
10.2.1 Displaying information on networks and switches . . . 233
10.2.1.1 Overview of IP networks . . . 234
10.2.1.2 Information on the IP network SENET . . . 235
10.2.1.3 Information on switches . . . 236
10.2.1.4 Graphical display of the internal IP network topology . . . 237
10.2.1.5 Overview of the performance and utilization of the Net Unit ports . . . 239
10.2.2 Configuring SENET . . . 240
10.2.3 Managing a Data Network Public . . . 241
10.2.3.1 Configuring the ACL settings of the DANPU network . . . 243
10.2.3.2 Information on the performance and utilization of the DANPU ports . . . 245
10.2.4 Managing a Data Network Private . . . 246
10.2.4.1 Add network . . . 247
10.2.4.2 Activate RADVD / DNS / NTP server . . . 248
10.2.4.3 Managing members of a DANPR network . . . 248
10.2.4.4 Configuring the ACL settings of the DANPR network . . . 248
10.2.4.5 Information on the performance and utilization of the DANPR ports . . . 248
10.2.5 Managing a Management Network Public . . . 249
10.2.5.1 Configuring the ACL settings of the MANPU network . . . 250
10.2.5.2 Information on the performance and utilization of the MANPU ports . . . 250
10.2.6 Management Network Private . . . 251
10.2.6.1 Information on the performance and utilization of the ports of the internal management networks . . . 253
10.2.6.2 Managing members of optional MONPR networks . . . 253
10.2.6.3 Configuring ACL settings of optional MONPR networks . . . 254

**10.3 Managing FC networks . . . 255**
10.3.1 Overview of FC networks . . . 255
10.3.2 Configuring settings . . . 256
10.3.3 Displaying messages . . . 257
10.3.4 Displaying connections . . . 257

**10.4 Managing storage systems . . . 258**
10.4.1 Overview of the storage systems . . . 258
10.4.2 Storage Manager . . . 259

**10.5 HW inventory . . . 260**
10.5.1 Rack view . . . 260
10.5.2 Displaying units . . . 262
10.5.3 Displaying components . . . 263
10.5.4 Administration . . . 264

**10.6 Managing energy settings . . . 265**
10.6.1 Monitoring energy consumption of the units of the SE server . . . 265
10.6.2 Simulating energy saving scenarios for the SE server . . . 266
10.6.3 Scheduled power on/off of units of the SE server . . . 267

**11 Managing authorizations . . . 269**

**11.1 User . . . 269**
11.1.1 Managing accounts . . . 269
11.1.2 Managing passwords . . . 272
11.1.3 Managing individual rights . . . 275
11.1.4 Displaying sessions . . . 276

**11.2 Configuration . . . 278**
11.2.1 IP-based access restriction to the MU . . . 278
11.2.2 Digital certificate . . . 279
11.2.2.1 Confirming/importing a certificate in the web browser . . . 280
11.2.3 Managing certificates . . . 282
11.2.3.1 Using the standard certificate . . . 283
11.2.3.2 Creating and enabling a new self-signed SSL certificate . . . 285
11.2.3.3 Requesting an SLL certificate . . . 285
11.2.3.4 Uploading and activating a customer-specific certificate . . . 286

**Glossary . . . 289**

**Related publications . . . 293**

**Index . . . 295**

# 1 Introduction

With the completely newly developed FUJITSU Server BS2000 SE Series, FUJITSU now offers a server infrastructure which consists of three server lines. Under the umbrella of this SE infrastructure, multiple application scenarios are possible in various combinations for both mainframe applications and applications of the open world. This new platform stands out on account of the unrivaled performance scalability (scale-up and scale-out), and ensures that users can manage their application workloads securely, quickly and efficiently across technological boundaries with maximum availability.
One major aim in developing the SE series was to provide a uniform management strategy which offers customers significant added value through maximum integration, and guarantees extremely cost-effective operation of their IT.
The new SE server line succeeds the tried and tested S and SQ server lines, integrating the advantages of both lines in an optimal manner. The heart of the SE series is formed by the /390-based Server Units, the x86-based Server Units, the Net Unit (NU) and the Management Unit (MU). All components are integrated into a standard 19" rack and are supplied to customers ready to use. With its newly developed processors and appreciably higher system performance, the new generation of the SE series offers enhanced configuration options, maximum availability and, not least of all, significantly reduced power consumption.
Depending on requirements, the SE server contains all the system components needed for operation as an overall application:

- SU /390 for BS2000 guest systems
- Server Unit x86 with BS2000, Linux or Windows guest systems
- Application Units x86 for operating Native or hypervisor systems (e.g. Linux, Windows, VMware, OVM, etc.)
- Shareable tape and disk periphery
- A high-speed, server-internal infrastructure to connect the components with each other and with the customer's IP and FC networks.

The SE server offers the following advantages:

- Cross-system administration with state-of-the-art, browser-based GUI (SE Manager) as a single point of operation
- Joint system monitoring of all components
- Uniform redundancy strategy
- Joint service process
- All options for consolidation through virtualization
- SE components and infrastructure are preconfigured and supplied to customers ready to use

SE servers consequently enable flexible and application-specific implementation which fulfills high SLAs through the use of high-end components and an end-to-end redundancy concept, and nevertheless permits cost-effective operation of the overall system with few resources thanks to its uniformity.

Intel x86-based server systems with their VMware, Linux or Windows system platforms also profit from the concepts for stable system operation tested on the mainframe:

- Selection of high-quality server components
- Redundant hardware components
- Prepared operating concepts which also include high availability
- Comprehensive tests before release
- Comprehensive service concept.

The management interface which is uniform for all SE servers, the SE Manager, permits a view of all the system components involved and, from this higher-level perspective, enables the resources to be optimized through efficient distribution of the application to the systems which are currently utilized least.

SE servers consequently permit particularly stable system operation which includes not only the mainframe platforms which have to date been known to be particularly failsafe, but also other Server Units and the infrastructure and peripherals employed by the SE server. This can be achieved with fewer resources for administration and system operation than for separate operation of different IT systems.

## 1.1 Documentation for the SE servers

A wide range of documentation is available for the SE servers. As the BS2000 OSD/XC software package comprises the BS2000 OSD/BC operating system and additional system-related software products, the documentation for BS2000 OSD/XC consists of the following:

- The manuals on BS2000 OSD/BC, which provide the basic literature on BS2000 OSD/XC.
- The manuals for the system-related software products which belong to the BS2000 OSD/XC software package also apply.

Any additions to the manuals are described in the Readme files for the various product versions. These Readme files are available at *http://manuals.ts.fujitsu.com* under the various products.
Current information, version and hardware dependencies and instructions for installing and using a product version are contained in the associated Release Notice. Release Notices, in particular those relating to BS2000 OSD/XC, M2000, X2000, and HNC, are available at *http://manuals.ts.fujitsu.com*.

The documentation for the SE servers consists of the following parts:

- Operating Manual SE700 / SE500 / SE300 (consisting of a number of modules):
  - Basic Operating Manual SE700 / SE500 / SE300
  - Server Unit /390 (SE700 / SE500)
  - Server Unit x86 (SE700 / SE500 / SE300)
  - Additive Components (SE700 / SE500 / SE300)
- Operation and Administration
- Security Manual
- Quick Guide

## 1.2 Objective and target groups of this manual

This manual is intended for people who operate an SE server:

- As administrator you manage the entire SE server with all its components and the operating systems which run on it. You need a good knowledge of the BS2000, Linux and Windows operating systems and of the network and peripherals.

  As administrator you can also manage the integration of the optional Application Units on which an open operating system (by default Linux) runs in Native mode or in a virtualized manner (e.g. under VMware® vSphere 5).

- For other users, roles are provided with a customized selection of functions (e.g. operator, XenVM administrator, etc.) to permit the assigned tasks to be performed.

## 1.3 Summary of contents

Chapter 2 contains fundamental information which is relevant for all readers (e.g. architecture, fundamental operating functions).

Chapter 3 contains fundamental information on the SE Manager, the central user interface of the SE server.

The subsequent chapters describe the tasks on the SE server and the user interface of the SE Manager. They are based on the tree structure of the SE Manager.

Detailed information on the data displayed, the dialog boxes, and operation of the SE Manager is provided in the online help of the SE Manager.

### README file

For information on any functional changes or extensions to this manual, please refer to the product-specific Readme file.

In addition to the product manuals, Readme files for each product are available to you online at *http://manuals.ts.fujitsu.com*. You will also find the Readme files on the Softbook DVD.

*Information under BS2000*

When a Readme file exists for a product version, you will find the following file on the BS2000 system:

```
SYSRME.<product>.<version>.<lang>
```

This file contains brief information on the Readme file in English or German (<lang>=E/D). You can view this information on screen using the `/SHOW-FILE` command or an editor. The `/SHOW-INSTALLATION-PATH INSTALLATION-UNIT=<product>` command shows the user ID under which the product's files are stored.

*Additional product information*

Current information, version and hardware dependencies and instructions for installing and using a product version are contained in the associated Release Notice. These Release Notices are available online at *http://manuals.ts.fujitsu.com*.

## 1.4 Changes since the last edition of the manual

This manual describes the functionality of the SE Manager with the use of the basic software M2000/X2000/HNC V6.1A.

This status provides the following functional extensions:

- Support of partitionable AUs on PRIMQUEST base (AU87 or DBU87)
- Support of the 10 Gb Net Unit
- Extension of the role concept: new roles *BS2000 administrator* and *AU administrator*
- Extension of the access concept: IP-based access to the Management Unit
- Extensions in the functionality of the SE Manager

## 1.5 Notational conventions

The following notational conventions are used in this manual:

| | |
|---|---|
| ℹ | This symbol indicates important information and tips which you should bear in mind. |
| ⚠ | This symbol and the word CAUTION! precede warning information. In the interests of system and operating security you should always observe this information. |
| ► | The action which you must perform is indicated by this symbol. |
| italics | Texts from the SE Manager (e.g. menu name, tab) |
| monospace | System inputs and outputs |
| **`monospaced`**<br>**`semibold`** | Statements which are entered via the keyboard are displayed in this font. |
| <abc> | Variables which are replaced by values. |
| Key symbols | Keys are displayed as they appear on the keyboard. When uppercase letters need to be entered, the Shift key is specified, e.g. SHIFT - A for A. If two keys need to be pressed at the same time, this is indicated by a hyphen between the key symbols. |

[ ] The titles of related publications in the text are abbreviated. The complete title of each publication which is referred to by a number is listed in the Related Publications chapter after the associated number.

## 1.6 Names and abbreviations

Because the names are used frequently, for the sake of simplicity and clarity the following **abbreviations** are employed:

- **SE server** for the FUJITSU Server BS2000 SE Series (Server Units /390 and x86) with the following models:
  - **SE300** for FUJITSU Server BS2000 SE300 (with SU300, optionally AUs)
  - **SE500** for FUJITSU Server BS2000 SE500 (with SU500, optionally SU300 and AUs)
  - **SE700** for FUJITSU Server BS2000 SE700 (with SU700, optionally SU300 and AUs)

- **SU** for the Server Unit irrespective of the unit type
  A distinction is made between SUs depending on the unit type:
  - **SU /390** for Server Unit /390 (type of Server Unit with one or more /390 processors)
  - **SU x86** for Server Unit x86 (type of Server Unit with one or more x86 processors)

  A distinction is made between the following SUs according to models:
  - **SU300** for the Server Unit of the unit type SU x86 in SE300, optionally in SE500 / SE700
  - **SU500** for the Server Unit of the unit type SU /390 in SE500
  - **SU700** for the Server Unit of the unit type SU /390 in SE700

- **MU** for the Management Unit. The MU permits central, user-friendly and cross-system management on the SE server.
- **AU** for the Application Unit (with x86-based hardware)
- **HNC** (High Speed Network Connect) connects the SU /390 with the LAN and as a net client also permits access to the Net-Storage. HNC designates both Linux-based basic software and the hardware unit itself on which this basic software executes.
- **BS2000 server** as the generic term for all SE servers and the existing S and SQ servers. BS2000 servers are operated with the relevant BS2000 operating system.
- **BS2000** for the BS2000 OSD/BC operating system in compound nouns, e.g. BS2000 system.

## 1.7 Open Source Software

The Linux-based basic software M2000, X2000, and HNC which is installed on the Management Unit, Server Unit x86, and HNC contains Open Source Software. The licenses for this can be found in the LICENSES directory on the relevant installation DVD.

# 2 Architecture and strategies

## 2.1 Architecture

In the maximum configuration, a FUJITSU Server BS2000 of the SE Series (SE server for short) consists of the following components:

- Management Unit (MU) with SE Manager
  The Management Unit can be redundant in design.
  A redundant Management Unit ensures that the components of the SE server can also be operated when an MU fails. In particular this means that the SKP functionality is then still available for operating an SU /390.

- Server Units
  - An SU /390 enables operation of BS2000 (Native BS2000 or VM2000).
  - An SU x86 enables operation of BS2000 (Native BS2000 or VM2000). XenVM operation with Linux or Windows guest systems is also possible as an option.

  Depending on the model family, the following combinations are possible:
  - SE700 with an SU /390 and optionally up to two further SU x86
  - SE500 with an SU /390 and optionally up to two further SU x86
  - SE300 with an SU x86 and optionally up to two further SU x86

- Application Units (AUs)
  Up to 20 AUs can be operated on the SE server. An AU enables operation of applications under Linux, Windows or hypervisor-based systems.

- Net Unit (for SU /390 with HNC)
  The Net Unit offers maximum performance and security for internal communication in an SE server and for a connection to customer networks (IP networks). In the case of SE500 and SE700 the Net Unit is always redundant in design. In the case of SE300 redundancy of the Net Unit is optional.
  The Net Unit is supplied preconfigured, is autonomous with respect to SE server management, and can easily be connected to the customer network.

- Rack console and KVM switch
- Peripherals (storage)
- Optional hardware components:
  Disk storage systems (for SU x86, AU), tape library systems (for SU x86), FC switches

All components of the SE server are integrated into a joint rack. Information on the current hardware configuration of your SE server is displayed by the SE Manager in the *Hardware → HW Inventory* menu (see section “HW inventory” on page 260).

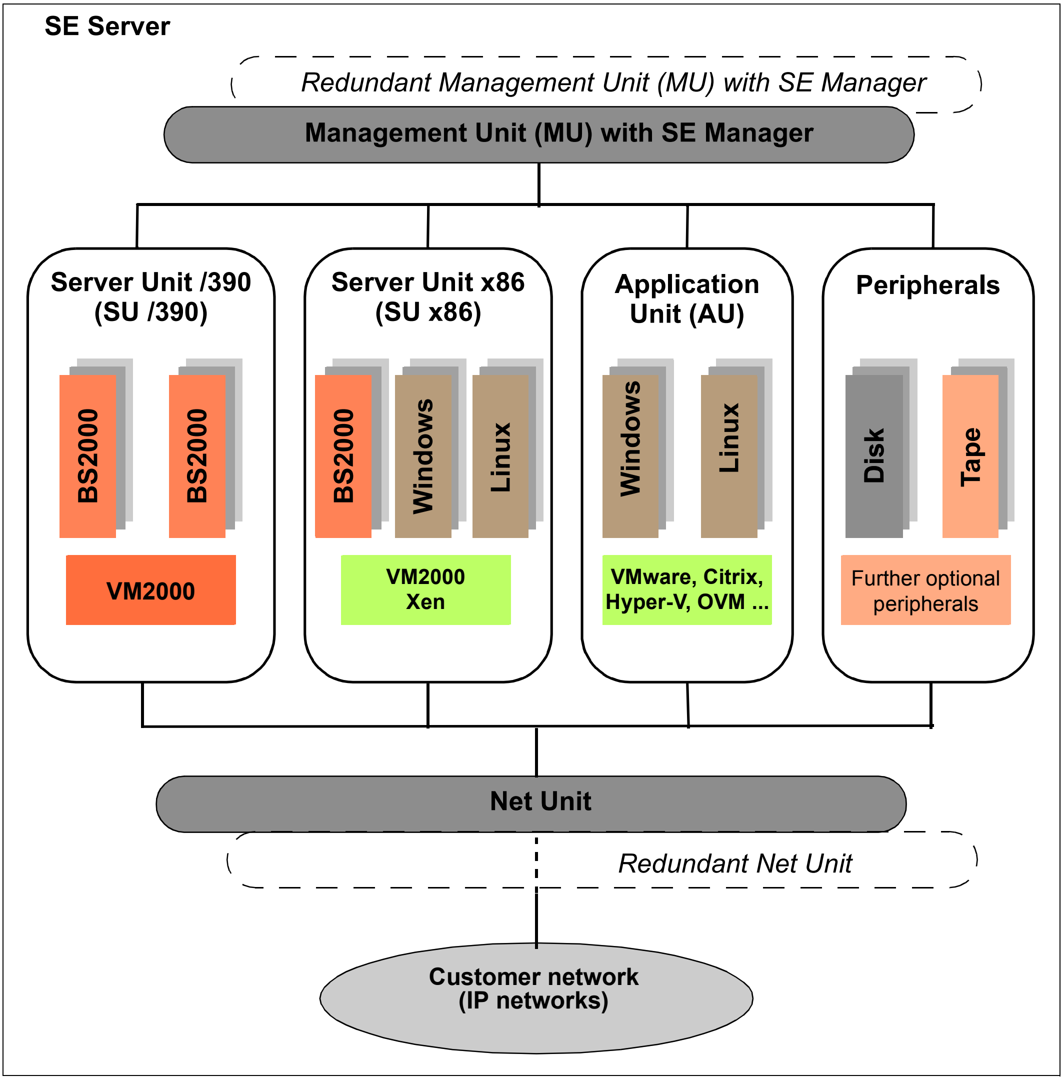

SE Server
Redundant Management Unit (MU) with SE Manager
Management Unit (MU) with SE Manager
Server Unit /390 (SU /390)
BS2000
BS2000
VM2000
Server Unit x86 (SU x86)
BS2000
Windows
Linux
VM2000 Xen
Application Unit (AU)
Windows
Linux
VMware, Citrix, Hyper-V, OVM ...
Peripherals
Disk
Tape
Further optional peripherals
Net Unit
Redundant Net Unit
Customer network (IP networks)

Bild 1: Architecture of SE servers

The SE Manager enables you to operate and manage all components of the SE server centrally from the Management Unit. The SE Manager offers a user-friendly, web-based user interface for this purpose.

# 2.2 Software of the SE server

## 2.2.1 Structure of the software

### M2000

M2000 is the basic software of the Management Unit. It provides, among other things, the following main functions for accessing SE servers:

- SE Manager as Single Point of Administration
- SE Desktop on the local console of the Management Unit
- Integration into Remote Service
- The role and operating strategy
- Functions for SU x86:
  - Operation of the BS2000 systems and of the system on XenVMs
- Functions of the Net Unit
  - Adjusting the configuration
  - Providing services

In the case of SE700 / SE500, M2000 also provides the following SKP functions for operating and managing the SU /390:

- Operation of the BS2000 systems (BS2000 console window, BS2000 dialog box, SVP console window)
- Management of the BS2000 VMs

### X2000

X2000 is the basic software of the SU x86. It provides, among other things, the following functions:

- Execution system for BS2000 systems and XenVMs (including I/O system)
- Management functions for administering the BS2000 VMs and the XenVMs in the SE Manager
- Management functions for administering the BS2000 devices and the XenVM devices in the SE Manager
- Configuration of the Net-Storage for the BS2000 systems of the SU x86

### HNC

HNC is the basic software of the HNC. It provides, among other things, the following functions:

- Network connection for the BS2000 systems of the SU /390
- Configuration of the Net-Storage for the BS2000 systems of the SU /390

### Add-on packs

In addition to the standard software M2000, X2000, and HNC, an SE server offers enhancements by means of add-on packs.

The possible installation of add-on packs on the MU enables costs and maintenance to be avoided on the SE server for additional servers, e.g. for ROBAR for openSM2. See also section “Add-on pack” on page 28.

## 2.2.2 Software status, system version and update status

In addition to the system version, the software status also includes the updates which are installed on the unit. Software updates can only be installed if they are available on the local system.

Under *SW version* in the system information the SE Manager displays on the MU, SU x86, and HNC the version of the basic software M2000, X2000 or HNC, including the update status.
On the SU /390 the SE Manager displays the HCP (Hardware Control Program) software (e.g. in the SU /390 information on page 187), but in this case does not support update management.

The software status consequently has the following components:

| Component | Example | Description |
|---|---|---|
| Version | `6.1A` | |
| Revision | `REV=0100` | Update status |
| Service pack | `6.1A, REV=0100, No.01` | – A service pack has a sequence number (`01` in the example)<br>– Service packs increment the update status. |
| Security fix | `6.1A, No.001` | – Security fixes are assigned to a version and update status.<br>– Security fixes have a sequence number for each version status and each update status (`001` in the example) |

| Component | Example | Description |
|---|---|---|
| Hot fix | `6.1A, REV=0100, A0603507-H03` | – Hot fixes are assigned to a version and update status<br>– In their name hot fixes contain a problem message number (A0603507 in the example) and a sequence number (H03 in the example) |

In contrast to the other update types, add-on packs are autonomous software products which FUJITSU makes available for installation on the Management Units. An add-on pack is either a software product which is installed by default (e.g. StorMan on the Management Unit) or one which is optional.
Add-on packs are managed like updates to the basic software, but the software status displayed consists of the product name and a product-specific version designation.

## 2.2.3 Updates to the basic software and add-on packs

You can transfer the following types of updates to the Management Unit, the SU x86 and the HNC and manage them there:

- Security fix
- Service pack
- Hot fix
- Add-on pack

### 2.2.3.1 Naming conventions

Updates are supplied as files of the following types:

- `iso.gz` for files which can be downloaded from the download server
- `iso` for files which are supplied on CD/DVD

The following naming conventions apply for the files containing the updates:

| | |
|---|---|
| Security fix | e.g. `MV6.1A.SF.001.iso[.gz]`<br>The security fix with the number `001` is assigned to the version and update status `6.1A`. |
| Hot fix | e.g. `MV6.1A0100.A0603507-H03.iso[.gz]`<br>The hot fix with the name `A0603507-H03` is assigned to the version and update status `6.1A REV=0100`. |
| Service pack | e.g. `MV6.1A0100.SP.01.iso[.gz]`<br>The service pack sets the version and update status to `6.1A REV=0100`. The count for the security fixes is reinitialized (set to `000`). |
| Add-on pack | e.g. `MV.STORMAN-6.0.0-12.4.iso`<br>This add-on pack contains StorMan V6.0 |

The first letter in the file name indicates the basic software of the associated unit:

- X for X2000 on the Server Unit
- M for M2000 on the Management Unit
- H for HNC on the HNC

### 2.2.3.2 Security fix

A security fix contains all the security-relevant updates for the Linux-based basic software which have appeared since the last service pack. Security fixes protect the system against, for example, unauthorized intrusion and attacks from the outside. Whether you install current security fixes depends on your security requirements and whether the SE server can be accessed only via the protected administration LAN or also from the outside. The functional use of the SE server is also guaranteed without the current security fixes.

A security fix may also be installed by the customer. Installation takes place in the SE Manager under an administrator account.

#### 2.2.3.3 Service pack

A service pack contains a collection of corrections for the Linux-based operating system. It contains all previous service packs and security fixes, as well as selected hot fixes.

A service pack can only be installed by Customer Support. Installation can only be performed using a CLI command under the Customer Support account.

#### 2.2.3.4 Hot fix

A hot fix contains a patch with which an urgent problem in your system can be rectified as quickly as possible.

A hot fix can only be installed by Customer Support. Installation can only be performed using a CLI command under the Customer Support account.

#### 2.2.3.5 Add-on pack

Add-on packs are software components on a unit which have their own web interfaces that are integrated into the SE Manager. The type and location of the integration into the SE Manager depends on the category to which the add-on pack is to be assigned, e.g. Application, Monitoring, Hardware Management.

Add-on packs have their own version schema and can be replaced independently of the basic software.

An add-on package contains software which FUJITSU provides for use on the units. Currently add-on packs are only provided for the Management Unit. By default a distinction is made between installed and optional add-on packs:

– In the case of an add-on pack which is installed by default, the customer must, if necessary, install newer versions.
– In the case of an optional add-on pack, the customer must also perform installation or uninstallation. Customer Support can also do this when requested.

Add-on packs are also distinguished by whether they are chargeable or included in the price and preinstalled.

The fact that the web interfaces of the add-on packs are integrated into the SE Manager means the following:

– The add-on packs are visible as links in the SE Manager's menu.

– When such a link is clicked, the add-on pack's web interface is opened in the same browser window.

- You log into the add-on pack's web interface implicitly using the account with which you are working in the SE Manager and in the same session. The same setting therefore applies for the session timeout in the event of inactivity. Logging off in the add-on also leads to logging off in the SE Manager and thus to the login window of the SE Manager.
- From the add-on pack's web interface there is a link back to the last valid main window in the SE Manager.

Add-on packs have their own online help systems and, when necessary, are described in separate product manuals. These online helps are integrated into that of the SE Manager, but can also be called separately.

*Overview of the current add-on packs in the SE Manager on the MU:*

| **Add-on<br>(product name)** | **Chargeable** | **Preinstalled ex works** | **Integration into the SE Manager** |
|---|---|---|---|
| OPENSM2<br>(openSM2 Performance Monitor) | Yes | Optional | Category: Monitoring<br>→ *Performance* |
| OPENUTM<br>(openUTM Server Administration) | Yes | No | Category: Application<br>→ *Applications* → *SE management application* |
| ROBAR<br>(ROBAR-SV Server) | Yes | Optional | Category: Application<br>→ *Applications* → *SE management application* |
| STORMAN<br>(Storage Manager) | No | Yes | Category: Hardware Management<br>→ *Hardware* → *Storage* |

Tabelle 1: Add-on packs in the SE Manager on the MU

### 2.2.4 Management applications

Management applications have graphical interfaces which can be reached via the web and operated using the browser.

A distinction is made between SE management applications and user-defined management applications.

- SE Management applications execute on the Management Units and are fully integrated into the SE Manager. They are implemented as a permanent part of the SE Manager or as add-on packs (see “Add-on pack” on page 28).

  The following SE management applications are currently available:

  - BS2000 Backup Monitor  
    The BS2000 Backup Monitor is a permanent part of the SE Manager.
  - openUTM WebAdmin  
    openUTM WebAdmin is implemented as an optional add-on pack.
  - ROBAR (ROBAR-SV Server)  
    ROBAR is implemented as an optional add-on pack.

- User-defined management applications are applications which support integration into the SE infrastructure. When you click a user-defined management application, it is opened in a new browser window.

  See also section “Managing user-defined management applications” on page 146.

  > i In contrast to this, "user-defined links" are only links to arbitrary internet pages or links to web-based applications which execute on systems of the SE server. When it is clicked, a user-defined link is opened in a new browser window.
  >
  > See also section “Administering user-defined links” on page 147.

## 2.3 Networks

The Net Unit supplies the central link of all the SE server's IP network connections. It concentrates the network connections of the various Server Units to the outside into the customer network (public networks) and, internally, establishes the network connections between the various Server Units (private networks).

The hardware of the Net Unit is supplied preconfigured. All the cable connections to the Server Units are implemented professionally in the cabinet in the factory. Connections to the customer networks (data networks, management networks) only need to be established to the reserved connection ports of the Net Unit (uplinks). In terms of the software the Net Unit is fully installed and immediately ready to operate.

Up to two uplinks are possible per public network to provide the connection to the customer's LAN structure. The uplinks are provided without vendor dependencies and can be connected to any switch (managed or unmanaged). The uplinks are operated without a VLAN ID (i.e. untagged), and no switch protocol (e.g. spanning tree) is used.

Only the relevant configuration measures need to be implemented in the operating systems to use the networks. It is not necessary to involve network administrators of the customer network.

Private networks have been configured for the Sever Units to communicate with each other. These separate the network communication within the SEs totally from the customer network. The private networks are protected from each other and can be configured flexibly according to customer requirements. Network security is automatically enhanced because of this protection and the flexibility to configure and operate private networks independently of the customer infrastructure.

The private networks can be operated with high performance, do not influence the customer network, and cannot be influenced by it (e.g. they continue to function even when the customer infrastructure fails).

The Net Unit can be designed with redundancy in the interest of protection against failure. By default, SE700 and SE500 incorporate a redundant Net Unit. Redundancy can be ordered as an option for SE300.

The BS2000 systems communicate with the MU over a private network, see section “Integration of BS2000 into the SE Manager” on page 36.

The following logical networks are supported:

- Data Network Public
  - Data Network Public (DANPU): when required, up to 8 additive networks DANPU<n> (where <n>= 01..08) can be configured for connecting applications to the public customer network.
- Data Network Private
  - Data Network Private (DANPR): when required, up to 99 networks DANPR<n> (where <n>= 01..99) can be configured for internal private customer networks for SE servers.
- Public management networks
  - Management Admin Network Public (MANPU) for administrative access to the MU, BS2000 systems and AUs
  - Management Optional Network Public (MONPU): the additive administration network can be configured when required (e.g. when AIS Connect is not to be operated via MANPU but over a separate network).
- Management Network Private
  - Management Control Network Local (MCNLO) for the local SE server communication
  - Management Control Network Private (MCNPR) for SE server communication
  - Management Optional Network Private (MONPR): when required, up to 8 additive networks MONPR<n> (where <n>= 01..08) can be configured for SE server communication.
  - Management SVP Network Private (MSNPR) enables SVP communication to the SU /390 on SE700/SE500

In addition to the connections of the units to the switches of the Net Unit, direct cabling from the units to the customer network can also be used.

The SE Manager shows a graphical display of the network topology with all the network components and connections in the *Topology* tab of the *Hardware → IP networks* menu. See section “Graphical display of the internal IP network topology” on page 237.

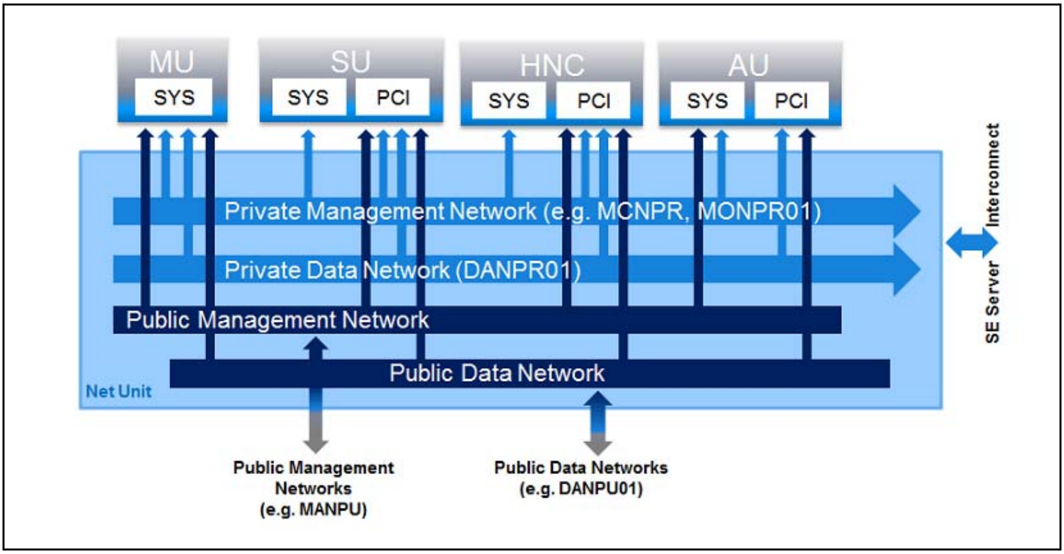

MU
SYS
SU
SYS
PCI
HNC
SYS
PCI
AU
SYS
PCI
Private Management Network (e.g. MCNPR, MONPR01)
Private Data Network (DANPR01)
Public Management Network
Public Data Network
Net Unit
SE Server Interconnect
Public Management Networks (e.g. MANPU)
Public Data Networks (e.g. DANPU01)

Bild 2: Block diagram of the Net Unit

## 2.3.1 Services

### 2.3.1.1 IPv6 autoconfiguration

IPv6 autoconfiguration based on the "radvd" (Router Advertisement Daemon) which runs on the MU is provided for communication in the MCNPR network segment. Optionally IPv6 autoconfiguration is also provided for the private network segments MONPR and DANPR.

The prefix "fd5e:5e5e:<vlan-id>:0::/64" (for MCNPR where vlan-id 600 = fd5e:5e5e:600:0::/64) is preconfigured. When conflicts occur on the customer side, Customer Support can set a different prefix (change the first 32 bits of the prefix).

Connected units (with enabled IPv6 autoconfiguration) are then assigned an IPv6 address based on the MAC address (e.g. fd5e:5e5e:600:0:219:99ff:fee2:79d/64).

IPv6 autoconfiguration is automatically enabled for MCNPR by means of the installation and is required for the management functions for the units. IPv6 autoconfiguration can optionally be activated for private network segments.

Each MU is assigned its own static IPv6 address during configuration in MCNPR (e.g. fd5e:5e5e:600::101/64 = IPv6 prefix + suffix <mu-id>0<se-id>) with which the MU in the network segment can be addressed.

### 2.3.1.2 Domain Name System (DNS)

A DNS server for the "senet" domain which provides name resolution for communication runs on the MU. The DNS server is configured in such a manner that it performs name resolutions for "senet" itself and forwards other name resolutions to external DNS servers which must be configured manually.

The static IPv6 address of the local MU is the first name server in the DNS configuration of the MU. Two further external DNS servers and the external domain search list can be configured.

The IPv6 addresses of the two possible MUs are preconfigured on an SU x86 or HNC. No further configuration is required.

DNS queries are thus directed to the MU via the network segment MCNPR. The MU then either resolves the address itself for the "senet" domain or forwards the request to the customer's external DNS servers.

Name resolutions can also be used for the other network segments MONPR and DANPR. For this purpose the relevant network segments must be configured on the MU in the SE Manager, and IPv6 autoconfiguration must be enabled (see section “Managing the IP configuration” on page 193).

### 2.3.1.3 Managing the "senet" domain

You manage the names and aliases of the "senet" domain in the SE Manager. You can add, modify or delete DNS entries (see section “Configuring SENET” on page 240).

The aliases are assigned according to the following schema:

| Component | MCNPR SE alias<br>(x01..n; y=1..8; z=01..99) | Description |
|---|---|---|
| MU | mu<x>-se<y>.senet | M2000 |
| SU /390 | su0bs2-se<y>.senet<br>su0vm<z>-se<y>.senet | BS2000 (Native/monitor VM)<br>BS2000-VMs |
| SU x86 | su<x>-se<y>.senet<br>su<x>irmc-se<y>.senet<br>su<x>bs2-se<y>.senet<br>su<x>vm<z>-se<y>.senet | X2000<br>SU x86 iRMC<br>BS2000 (Native/monitor VM)<br>BS2000-VMs |
| Managed Switch | nswa<x>-se<y>.senet<br>nswb<x>-se<y>.senet | nswa = 1 Gbit<br>nswb = 10 Gbit |
| HNC | hnc<x>-se<y>.senet<br>hnc<x>irmc-se<y>.senet | HNC<br>HNC iRMC |
| AU x86 PRIMERGY | au<z>-se<y>.senet | System (e.g. VMware) |
| AU x86 PRIMEQUEST | auc<z>-se<y>.senet<br>auc<z>p<nr>.se<y>.senet | Management Board of the PRIMEQUEST<br>Partition of a PRIMEQUEST |
| RAID system | prd<z>-se<y>.senet | e.g. ETERNUS DX (prd=periphery raid) |
| Tape library | ptl<z>-se<y>.senet | e.g. LT40 S2 (ptl=periphery tape library) |
| Other periphery | pot<z>-se<y>.senet | (pot=periphery other) |
| ROBAR | rob<z>-se<y>.senet | ROBAR controller |

Tabelle 2: Name schema of the SE aliases

### 2.3.1.4 ACL functionality

You can lock or release individual TCP/UDP ports (services) for the DANPU<xx>, MANPU, MONPU, DANPR<xx>, and MONPR<xx> networks in an ACL (Access Control List):

- Either the administrator defines an ACL list of the type "permit" in which all released services (ports) are explicitly entered.

  > i After the ACL of the type "permit" has been configured, the list is initially empty. Access to the network is thus locked for all services (ports).

- Or the administrator defines an ACL list of the type "deny" in which all the locked services (ports) are explicitly entered.

One ACL list each can be defined for IPv4 and IPv6.

### 2.3.1.5 NTP server

The MU of the SE server is configured as an NTP server and is used as the central NTP server for the SE server.

The units SUx86 and HNC are configured in such a manner that time synchronization takes place from the local SE server's MU.

The static IPv6 address of the MU can be used for time synchronization of an AU with the local SE server's MU.

## 2.3.2 Integration of BS2000 into the SE Manager

The VM Management for SU /390 in VM2000 operation mode requires communication between the monitor system and the MU. The BS2000 Backup Monitor also requires communication between the BS2000 systems on which the backup requests take place and the MU.

The communication uses the internal network MCNPR (see figure 2 on page 33) and must be configured as follows:

- In the BS2000 systems mentioned a suitable BCAM configuration must be configured by means of the templates provided. See also the BCAM manual [12].
- The REWAS subsystem must be installed and have been started.

## 2.3.3 Integration of BS2000 into the LAN

From the viewpoint of BS2000 devices, the ZASLAN, LOCLAN and BRGLAN are devices which are used for the LAN connection to the external physical network or for internal communication in the Server Unit. They can be created in the SE Manager (see section “Managing LAN devices” on page 166) and must, in the case of VM2000, then be assigned to the BS2000 VM concerned.

### BS2000 ZASLAN

In the case of a ZASLAN connection, BS2000 uses a LAN interface of its own (Ethernet controller) independently of other LAN interfaces. Only via such a connection does BS2000 obtain a direct view of the physical network.

In VM2000 mode a LAN interface can be used jointly by all connected BS2000 guest systems. To permit this, a separate ZASLAN connection is configured for each BS2000 VM. The associated devices are connected to their particular VM (using the ADD-VM-DEVICES command).

The ZASLAN interfaces are displayed or modified in the SE Manager using *Devices → <unit> (SU<model>) → BS2000 devices*in the *LAN* tab.

i All PCI ports can be used for the ZASLAN connections.

The following can be observed on the SU x86: LAN interfaces cannot be used simultaneously for ZASLAN and virtual switches.

### LOCLAN

The local LAN is a network implemented by software in the Linux-based basic system concerned (X2000/M2000/HNC). The local LAN connections are consequently not included in the figure illustrating the LAN structure (see figure 2). The connection of BS2000 to the local LAN is implemented on an SU x86 system with connections implemented by software (MANLO: Management Network LOCLAN), and on an SU /390 by FC connections between SU /390 and MU (MANLO) or HNC.

The following addresses are preconfigured for BS2000 and the basic system (X2000/M2000):

| System | IP address |
|---|---|
| Basic system | 192.168.138.12 |
| BS2000 (Native or monitor system) | 192.168.138.21 |
| BS2000 guest systems on other VMs | 192.168.138.22 etc. |

A second MU is automatically assigned the addresses 192.168.139.x. If address conflicts occur, only Customer Support can configure other address ranges.

### BRGLAN (only SU x86)

A BRGLAN connection connects BS2000 with an internal virtual switch and enables a LAN connection to the other virtual machines (= Xen LINUX/Windows guest systems) which are also connected to the same virtual switch.

A BRGLAN connection is required to implement one of the following connections:

– The Native BS2000 system for the XenVMs on the same virtual switch

– BS2000 VMs for XenVMs on the same virtual switch

i If only BS2000 VMs communicate with each other, LOCLAN connections should be used.

The BRGLAN connection is a protected internal connection in the Server Unit which is implemented in the software and thus does not occupy any slots.

With BRGLAN the packet size can be up to 1500 bytes.

An internal virtual switch is configured using the SE Manager. A separate BRGLAN connection is configured in X2000 for each VM with a BS2000 guest system. The associated devices are assigned to the relevant VM.

i The BRGLAN connection requires that at least one virtual switch exists. Virtual switches can be configured only in conjunction with the operation of XenVMs, i.e. a XenVM license must exist. For details, see “Integration of the XenVM guest systems into the LAN (only SU x86)” on page 39.

BRGLAN connections are virtual network connections and are therefore not displayed in the physical LAN structure (see figure 2).

### 2.3.4 Integration of the XenVM guest systems into the LAN (only SU x86)

The Linux/Windows systems on the XenVMs communicate with each other or with external systems via software instances which are known as virtual switches (or vSwitches for short). Virtual switches are made available as XenVM devices. A XenVM is connected either when the XenVM is created or at a later point in time by assigning a virtual Network Interface Card to the vSwitch.

Depending on the connection type provided, a distinction is made between two types of vSwitch:

- **Internal vSwitch**

  An internal vSwitch enables the XenVMs connected to it to use a communication connection which is protected locally. Internal vSwitches can also be used by the BS2000 Native system and by BS2000 VMs (see "BRGLAN (only SU x86)" on page 38).

- **External vSwitch**

  An external vSwitch uses a LAN interface which permits an external LAN connection. All XenVMs connected to this vSwitch use this connection to communicate with external systems.
  If more than one unused LAN interface is available, an external vSwitch can also use two LAN interfaces. In this case the XenVm connection is configured with redundancy (also referred to as "bonding").

The virtual switches and their current assignment to XenVMs are displayed in the SE Manager by selecting *XenVM devices → Networks* on the *Virtual switches* tab. New virtual switches can be created there and unused switches can be deleted.

i Only PCI ports can be used for the external vSwitches.

LAN interfaces (PCI-Ports) cannot be used more than once (e.g. for multiple virtual switches or for a virtual switch and a ZASLAN).

## 2.3.5 Overview of the possible LAN connections of the VMs

The figures below provide an overview of the possible internal and external LAN connections of the VMs running on the Server Unit (BS2000 on SU /390 or BS2000 and XenVM on SU x86). Physical network integration is shown in figure 2.

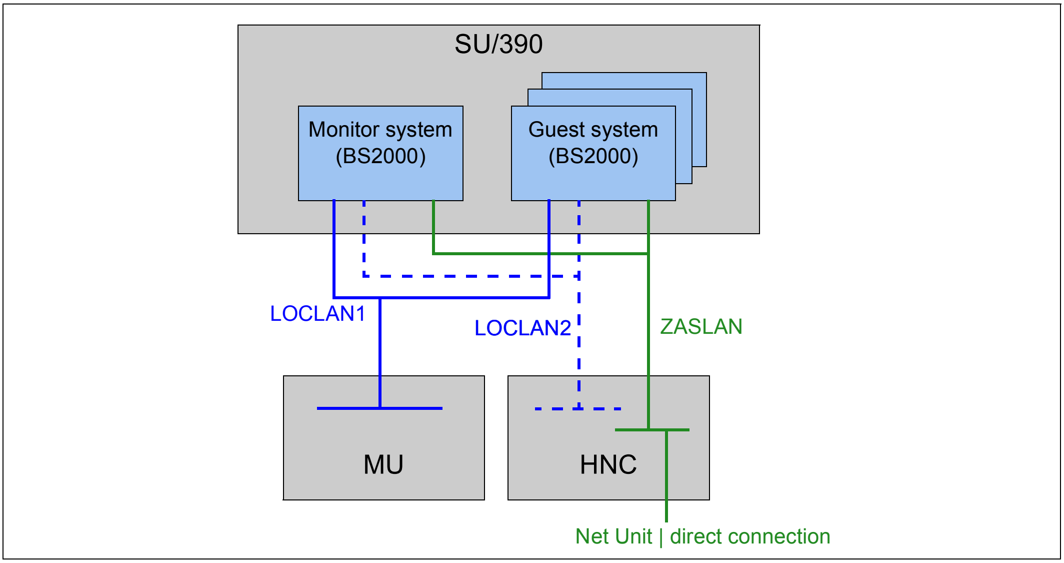


Bild 3: Overview of possible internal and external LAN connections (Server Unit /390)

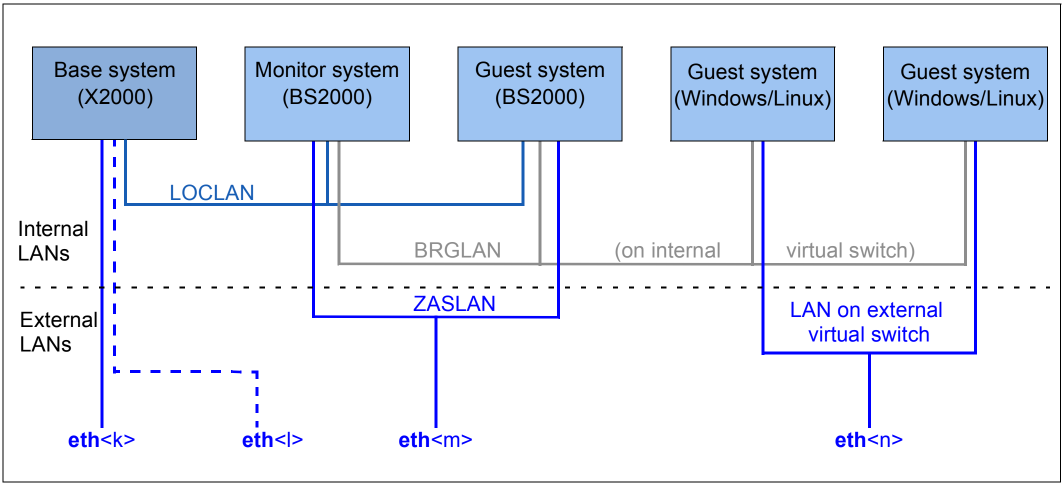


Bild 4: Overview of possible internal and external LAN connections (Server Unit x86)

## 2.3.6 Important information about IP configuration

After your SE server has been installed, the IPv6 protocol is enabled throughout the system.

Use of IPv6 for all networks of the SE server is enabled by default. You can perform the following configuration measures separately on a network-specific basis:

- When the IPv6 protocol is enabled throughout the system, you can enable or disable the use of IPv6 for specific networks.
  IPv6 is permanently set for the internal network (MCNPR).
- Enable/disable Autoconf (Stateless Address Autoconfiguration)
  This setting is evaluated only when IPv6 is enabled:
  Autoconf is a user-friendly automatic procedure which enables the system to specify its own LAN addresses on the basis of information which is provided both locally and remotely. Autoconf requires a router which is responsible in the network that, when requested by the system, assigns the so-called IPv6 prefixes (one prefix per available network).
  The system supplements these prefixes for each LAN interface to make them unambiguous addresses, the supplement being based by default on the MAC address of the LAN interface concerned.
  A LAN interface configured in this way is automatically linked to all available networks.
  In contrast to Autoconf, in the case of DHCP IPv6 address assignment (stateful) is performed by an instance in the network which also manages the current state of the address assignment.
- Enable/disable DHCPv6
  DHCPv6 requires a DHCP server in the network which distributes IPv6 addresses.
- Enable/disable DHCPv4
  DHCPv4 requires a DHCP server in the network which distributes IPv4 addresses.

In all cases of dynamic address distribution, the addresses assigned are provided with Validity times by the Autoconf router or the DHCP server.

Any number of IPv6 addresses (and also IPv4 addresses) can be allocated explicitly.

When IPv6 is used, IPv6 routes can also be configured.

# 2.4 Management Unit and SE Manager

The Management Unit together with the SE Manager enables central monitoring, administration and operation of all units of the SE server and the systems running on it. Additional cross-unit functions are also available, e.g. for displaying the components of the SE server, together with the operating status or performance monitoring.

## 2.4.1 Role and user strategy

Depending on how the system is viewed, different tasks must be performed to administer and operate the SE server which are categorized in multiple task areas. The task areas correspond to the roles described below.

- Administrator
- BS2000 administrator
- XenVM administrator
- AU administrator
- Operator
- Service

The roles are tied to an account. In other words the user takes over a role when he/she logs in on the SE Manager with an account which is assigned to this role. A user who takes over a task area (i.e. a role) must be authorized to execute all the functions which are required to perform these tasks.

When the system is delivered, there are predefined accounts for the *Administrator* and *Service* roles, see “Predefined accounts” on page 44.

All roles from the *Service* role can be assigned to further accounts, see “Further accounts with role assignment” on page 45.

The task areas of the various roles are described in detail below. For further information, see the online help.

### Administrator

This task area comprises management of all units on the SE server and management and operation of the systems which run on Server Units and Application Units of the SE server.

- BS2000 systems:
  For BS2000 on a Server Unit, the task area comprises operation of the BS2000 system or, under VM2000, operation and partial management of the BS2000 guest systems..
- XenVM systems:
  For a Server Unit x86 with a XenVM license the task area also comprises management of the virtual machines (XenVMs) and their devices for Linux and Windows guest systems.
- Application Units:
  For the optional Application Units the task area comprises the configuration and management of the Application Units and the systems running on these.

The administrator can also open a Linux shell on the Management Unit and can use this to call CLI commands. The `cli_info` command lists the M2000-specific commands which are available. You can obtain a detailed description of the commands in the online help.

All administrator accounts are of equal value.

### BS2000 administrator

Comprises (largely) the subset of the **Administrator** task area which refers to BS2000 systems.

All BS2000 administrator accounts are equal ranking.

General access to the Linux shell is not possible. A BS2000 administrator can, however, access the BS2000 console, the BS2000 dialog and the SVP console outside the SE Manager by means of ssh client PuTTY. To do this, he/she can execute the *bs2Console*, *bs2Dialog* and *svpConsole* commands as remote commands by means of PuTTY.

### XenVM administrator

Comprises (largely) the subset of the **Administrator** task area which refers to XenVM systems.

All XenVM administrator accounts are equal ranking.

### AU administrator

Comprises (largely) the subset of the **Administrator** task area which refers to Application Units.

All AU administrator accounts are equal ranking.

### Operator

This task area is a subset of the administrator tasks and largely consists of operating the BS2000 systems for ongoing operation or, under VM2000, operation and partial management of the BS2000 guest systems.

All operator accounts are initially equivalent. The administrator can equip them with individual authorizations for accessing BS2000 or the individual BS2000 VMs.

General access to the Linux shell is not possible. A BS2000 administrator can, however, access the BS2000 console, the BS2000 dialog and the SVP console outside the SE Manager by means of ssh client PuTTY. To do this, he/she can - depending on the individual rights - execute the *bs2Console*, *bs2Dialog* and *svpConsole* commands as remote commands by means of PuTTY.

### Service

This role includes all tasks of Customer Support, such as maintenance and configuration of the SE server and registration of Application Units.

### Predefined accounts

As supplied, the following local accounts are predefined on the SE server for the existing roles:

- admin (administrator role)
- service (Customer Support role)

The predefined account *admin* is protected by an initial password. The administrator can configure further accounts. Further details are provided in the section “Managing accounts” on page 269 and in the Security Manual [6].

The predefined account *service* is available solely to Customer Support. A service account cannot be administered in the SE Manager.

### Further accounts with role assignment

The administrator can configure further accounts for an administrator, BS2000 administrator, operator, XenVM administrator or AU administrator. He/She assigns the *Administrator, BS2000 administrator, operator, XenVM administrator* or *AU administrator* role during configuration. The use of person-related accounts is therefore also possible.

### Accesses to BS2000

All administrator and BS2000 administrator accounts have access authorization to the BS2000 console and BS2000 dialog of all BS2000 systems.
An administrator can assign these authorizations individually to an operator account, in VM2000 mode specifically for particular guest systems.

For information on accesses to BS2000, see section “Managing individual rights” on page 275.

### Accesses to the operating system on XenVMs and Application Units

The customer is responsible for configuring accounts in the operating systems on XenVMs and Application Units, possibly linked to a strategy for particular roles or authorizations. This depends on the options of the operating system concerned.

## 2.4.2 IP-based access to the Management Unit

By default, access to the MU is unrestricted and permitted for all IP addresses and networks. However, the administrator can configure access to the MU (applies for the SE Manager and CLI) in such a manner that it is possible only for explicitly entered IP addresses or for IP addresses from an explicitly entered IP network.

The current configuration of the access to the MU is displayed in the *IP networks* tab of the SE Manager (see *Authorizations → Configuration*, section “IP-based access restriction to the MU” on page 278).

### 2.4.3 Redundant Management Units

Central operation and administration of the SE server is guaranteed without interruption after an MU has failed if the SE server has a second MU.

On SE500 and SE700 two MUs mean that the SKP functionality is also provided with redundancy.

*Redundancy of the SKP functionality*

As a result, when one MU fails the SU /390 can still be operated via the SVP.

With respect to the SKP functionality, one MU is always "active" and the other is "passive". Only the active MU can access the SVP of the SU /390. SVP accesses of the passive MU take place by means of automatic redirection via the active MU.

On the *BS2000 operation mode* tab of the SU /390 you see the current status of the MUs with respect to the SKP functionality. There you can also switch over the passive MU, i.e. the two MUs change status (see *Systems → <unit> (SU</390>)*, “Switching Management Unit” on page 96).

The SE Manager shows the current status of the SVP network and of the MU connections in the *IP configuration* of the SU /390 (see *Hardware → Server (SE<model>) → <unit> (SU</390>) → Management*, “Managing the IP configuration” on page 193).

*Operating redundant MUs*

When two MUs are available, in other words MU redundancy exists, you can log into the SE Manager on either of the two MUs. Operation and administration of the SE server is possible without restriction on either of the two MUs.

In the title bar the SE Manager displays the redundant MUs and permits a "change" to the SE Manager of the other MU via a link. This necessitates logging in again as an independent new session begins on the SE Manager of the other MU.

The MU on whose SE Manager the user is currently logged in is the local MU in this session, and the other MU is the redundant MU.

The following must be borne in mind in the SE Manager with respect to the redundant MU:

- Downloading from the redundant MU is not permitted. Uploading to the redundant MU is not supported, either.
- The management applications of the various MUs are independent installations and only accessible in the SE Manager of the local MU.
- AUs are registered separately on both MUs and are monitored explicitly on each MU.

- The following applies for the IP network:
  - Manual SENET DNS entries must be entered on both MUs.
  - Configurations for private networks (e.g. activation of the RADVD/DNS/NTP server) must be implemented on both MUs.
- The following applies for the FC network: As displays are based on local configurations and settings of the MUs, they can differ.
- The following applies for the authorizations:
  - Accounts must be configured identically on both MUs.
  - For operator accounts with individual authorizations, the server-related authorization and system-related authorization for SU /390 must be configured in the same manner.
- Only local sessions are displayed on each MU.

# 2.5 Virtualization

## 2.5.1 Implementing VM2000

Depending on the architecture of the Server Unit there are two fundamentally different technical implementations of VM2000.

### Implementation principle for SU /390

On SU /390 VM2000 controls the hardware of the Server Unit.

The VM2000 monitor manages all VMs and provides its functions via the VM2000 interface.

The VM2000 hypervisor controls execution of all guest systems on the VMs. Differentiated scheduling mechanisms ensure optimum execution of the guest systems.

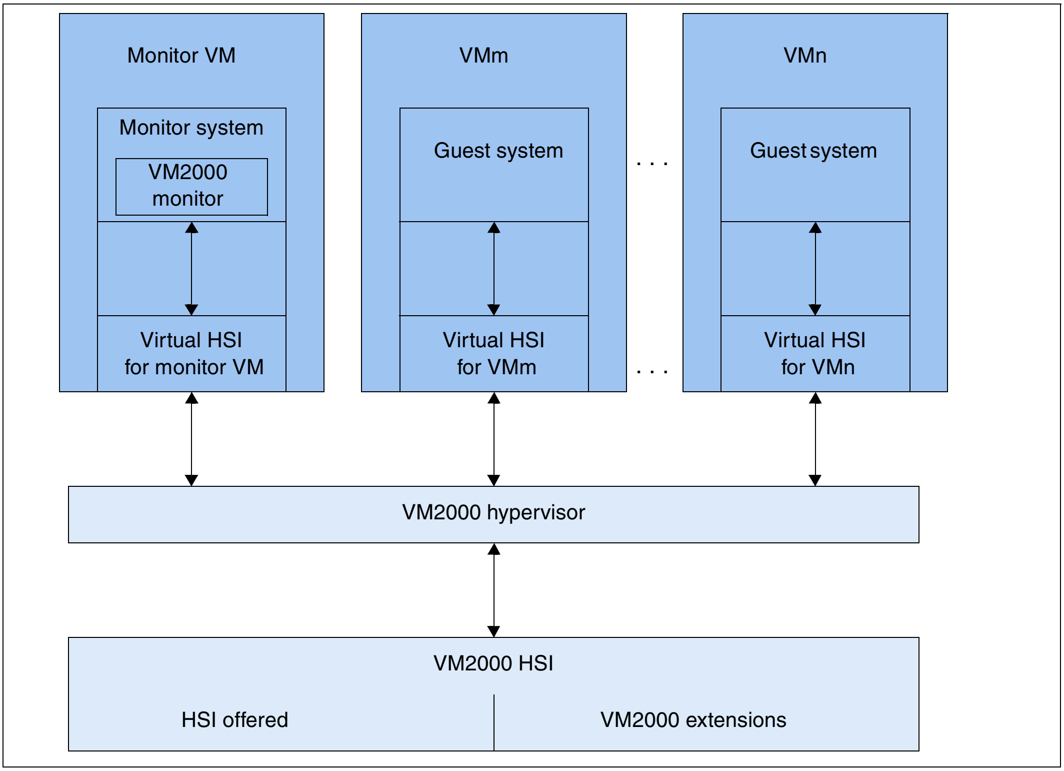


Bild 5: Structure of VM2000 on SU /390

Further information is provided in the "VM2000" manual [11].

### Implementation principle for SU x86

On SU x86 the X2000 basic system controls the hardware of the Server Unit.

The VM2000 monitor manages the VMs with the guest system BS2000 (**BS2000-VM**) and provides its functions via the VM2000 user interface.

The Xen hypervisor virtualizes the global resources CPU and main memory, controls the execution of all VMs (scheduling), and ensures load balancing for CPU usage.

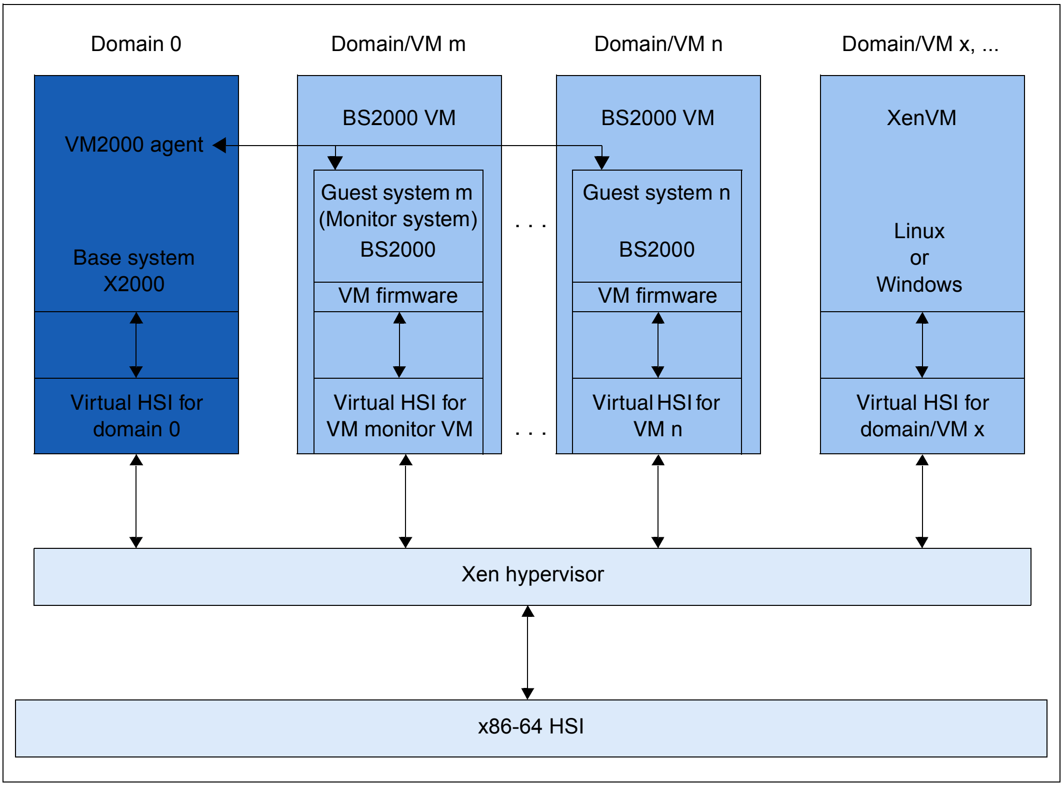


Bild 6: VM2000 on SU x86

Further information is provided in the "VM2000" manual [11].

### Roles

Actions for the BS2000 VMs can be initiated from different roles:

- Fundamental functions for VM management (including configuring BS2000 VMs), operating the BS2000 VMs, and device management are available to the administrator in the SE Manager.
- The full VM2000 functional scope is available to the VM2000 and VM administrators via the interface of VM2000. The VM2000 commands operate and manage all BS2000 VMs. A detailed description of the VM2000 functional scope is contained in the "VM2000" manual [11].

## 2.5.2 Virtualization on Server Unit x86

Virtualization permits parallel execution of BS2000, Linux, and Windows systems with their applications on a Server Unit x86. The basic software X2000 together with Xen and if necessary VM2000 permits other systems to execute.

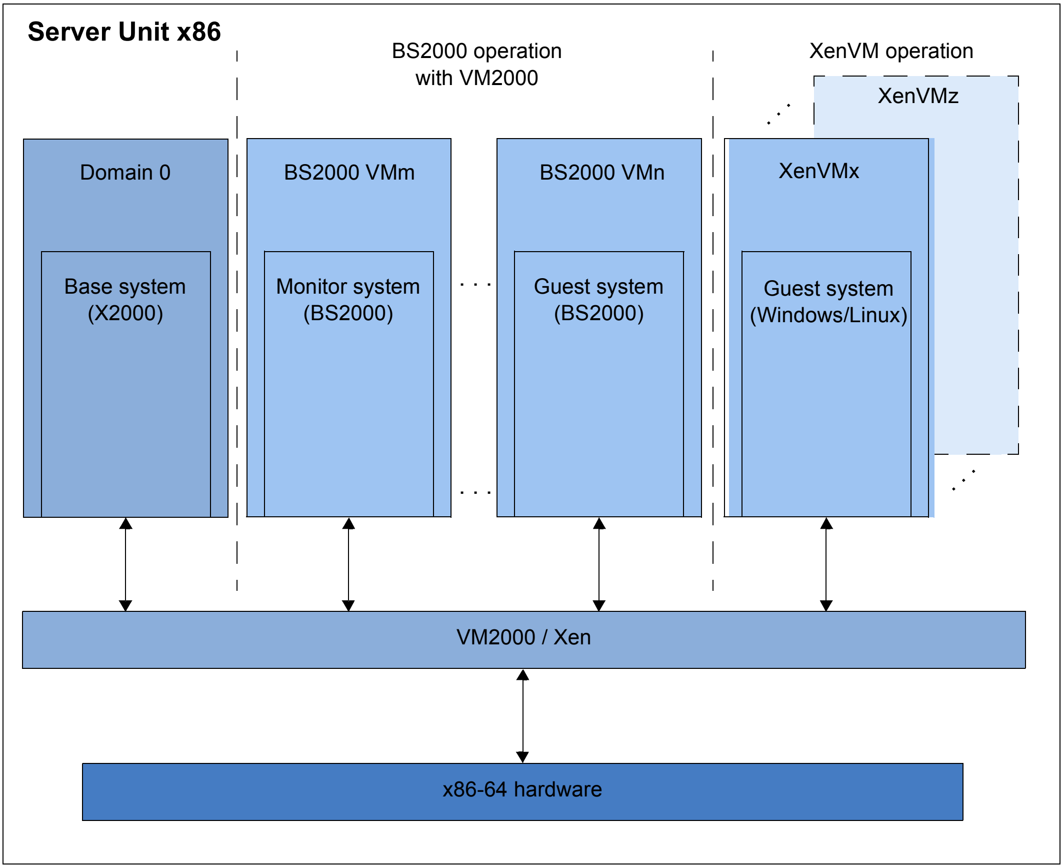


Bild 7: SE server architecture with VM2000 (Server Unit x86)

### BS2000 operation

BS2000 operation is possible in either Native or VM2000 mode:

- In Native mode, precisely one Native BS2000 system is available.
- In VM2000 mode, a BS2000 system, the monitor system, is started under VM2000. Further BS2000 VMs can be created with VM2000.

### XenVM operation

XenVM operation is possible as an option. When a XenVM license is installed on the Server Unit x86, the SE Manager offers functions for configuring, managing and operating virtual machines, which are known as XenVMs. The following Linux and Windows systems are explicitly supported as guest operating systems on these XenVMs:

- Red Hat Enterprise Linux
- SUSE Linux Enterprise Server
- Windows Server

The use of other guest operating systems is always possible. For information on this subject, please contact Customer Support.

Depending on the guest operating system used, a distinction is made between the following virtualization types:

- **Full virtualization** (synonym: hardware virtualization) for Windows Servers and “another operating system", not explicitly supported guest operating systems
  The guest system can run on real hardware without modification on the XenVM. Xen emulates some selected components which the guest system supports.
- **Paravirtualization** for the Linux systems which are explicitly supported
  The XenVM is only similar to the real hardware. Modifying the kernel enables the guest system to run on the XenVM.

### 2.5.2.1 CPU pool management

The real CPUs of the Server Unit x86 are distributed to groups of CPUs, which are known as CPU pools. Each real CPU can be assigned to at most one CPU pool.

One main objective of this distribution to different CPU pools is to seal off the carrier system from the other systems and to separate the Native BS2000 system (or the BS2000 guest systems) from the XenVM guest systems. For the operation of BS2000 this ensures a stable performance in accordance with the SE server model.

A virtual machine (VM) is assigned permanently to a CPU pool in accordance with the VM type (BS2000-VM or XenVM) when it is generated. It can use only the CPUs from this CPU pool, even if CPUs in parallel CPU pools are unused. The scheduling of CPU performance always relates only to the CPUs of a particular CPU pool. The weightings between individual VMs (via limitation and weight) in a CPU pool can thus not influence the weightings among the VMs in another CPU pool.

The distribution of the real CPUs to CPU pools is implemented automatically on the basis of the installed hardware and the installed licenses when the Server Unit x86 is started up and cannot be changed by the user. The CPU pools can be extended by integrating further hardware or by installing further licenses.

The BS2000 CPUs, i.e. those CPUs which are used by the BS2000 systems in accordance with the server model, can be split into further CPU pools using VM2000 means.

The hardware and licenses are installed by Customer Support, and this requires a maintenance window.

In normal operation the CPU pools are configured and managed as follows:

- **Pool 0**
  This pool is reserved exclusively for the X2000 basic system. It contains a quarter of the existing real CPUs, but at least 2 CPUs.

- **BS2000 pools**
  The standard pool is used exclusively by the Native BS2000 system or by the BS2000 VMs. Provided no further BS2000 CPU pools are configured, this pool contains all the BS2000 CPUs.
  When further CPU pools are configured with VM2000 means, the BS2000 CPUs can be displayed in other BS2000 CPU pools. The standard pool is retained in this case, but may possibly no longer contain CPUs. BS2000 VMs are assigned to one of these CPU pools when they are created. In ongoing operation, VM2000 means can be used to switch them dynamically between these pools.

- **Linux/Windows pool**
  This pool exists only if a XenVM license is installed and when sufficient CPUs are available. It is used exclusively by XenVMs.

- Depending on the hardware and licenses which are installed, further unused real CPUs can exist in the Server Unit outside the pools, the so-called **free CPUs**.

The CPU pools are also visible under VM2000, but the naming of static pools is retained in VM2000 for compatibility reasons. The table below shows the names of the CPU pools in the X2000 basic system and the names in VM2000.

| **CPU pool** | **User** | **Name in X2000** | **Name in VM2000** |
|---|---|---|---|
| Pool 0 | X2000 | Pool 0 | *POOL0 |
| Standard BS2000 pool | BS2000 | bs2_pool<br>co_bs2-pool [1] | *STDPOOL |
| Pool configured in VM2000 | BS2000 | <name 1..8><br>co_<name 1..8> [1] | <name 1..8> |
| Linux/Windows pool | XenVM | lw_pool | *FOREIGN |
| Free CPUs (not a pool) | | | |

Tabelle 3: Overview of the CPU pools (X2000 and VM2000 views)

[1] For CPUs which are not attached. These are as a rule the CoD CPUs (which are called extra CPUs in VM2000)

In normal operation enough CPUs are available for every pool. A lack of CPUs can occur in the following exceptional situations:

- Reduced operation: a hardware failure means that fewer CPUs are operational at system startup.

- Abnormal operation: a change of license means that more CPUs are required.

In the case of reduced or abnormal operation the basic system automatically reacts with the following step-by-step measures to rectify the lack of CPUs:

1. The (free) CPUs not used so far are used
2. Step-by-step reduction of the Linux/Windows pool to 2 CPUs
3. The BS2000 CoD CPUs are omitted
4. Alternating omission of one CPU and of the BS2000 pool down to 2 CPUs
5. Pool 0 is reduced to 1 CPU
6. The last but one CPU of the Linux/Windows pool and of the BS2000 pool is omitted
7. Cancelation of the Linux/Windows pool

In the VM overview (BS2000) the SE Manager displays the CPU pools to which the particular BS2000 VMs are assigned. An additional table shows all the BS2000 CPU pools (also the empty pools).

For information on BS2000 and BS2000 VMs, see also section “Working in Native BS2000 mode” on page 102 and section “Working in VM2000 mode” on page 105, and for information on XenVMs, see also section “Working in XenVM mode (on Server Unit x86)” on page 115.

### 2.5.2.2 Main memory management

Around 30%, but at most 16 GB, of the existing main memory is reserved for the X2000 basic system and the firmware of the BS2000 systems.

BS2000 can use the remaining 70% on the Native system or on the BS2000 VMs. In optional XenVM operation the XenVM systems also use this main memory share.

The main memory cannot be reserved in advance for a particular type of virtual machine (BS2000 VMs or XenVMs). It is only ever assigned to the guest system concerned when a virtual machine is started if the amount of free main memory requested is available.

### 2.5.2.3 BS2000 devices

The real devices of the periphery are not directly visible to BS2000 (Native BS2000 and BS2000 VMs). Only the devices emulated in the X2000 basic system are visible. See also section “Managing BS2000 devices” on page 152.

### 2.5.2.4 XenVM devices

When a XenVM is created, not only the main memory and CPUs are configured, but also virtual devices. From the viewpoint of the guest system (Linux/Windows), these devices look like real devices. To enable the guest system to recognize and use the devices configured on the XenVM, the corresponding device drivers must be installed in the guest system.

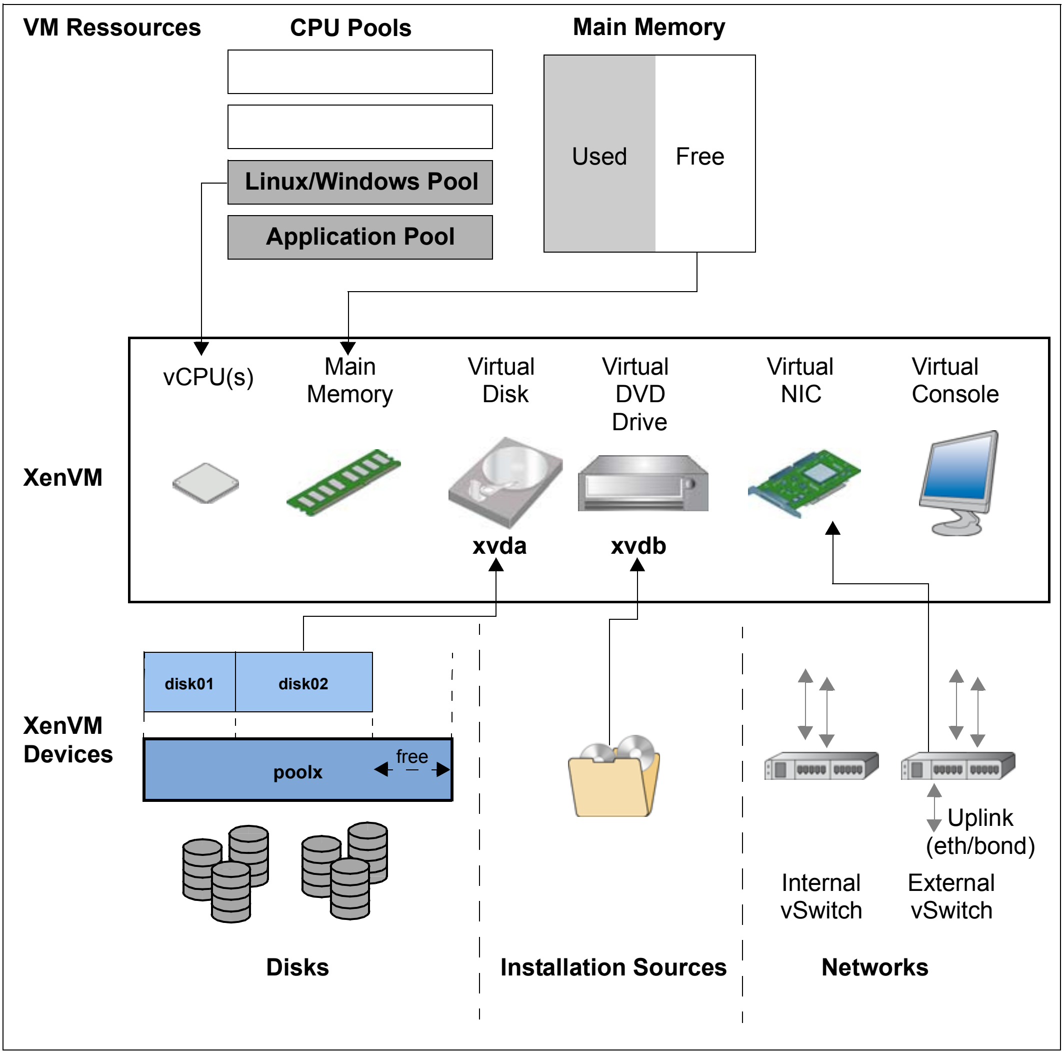


Bild 8: Configuring XenVM devices on the XenVM

The following block-oriented virtual devices can be made available to a XenVM:

- Virtual disk
  The XenVM requires at least one disk in order to install and start the guest system. When the XenVM is configured, a virtual disk is created and the guest system is installed on it. Alternatively a disk which has already been installed and which has become free can be used.

- Virtual DVD drive
  The XenVM requires at least one virtual DVD drive in order to install the guest system onto the disk from an installation source. An installation source is either an image file of an operating system (or of other software) or an (additional) installation configuration file which is available locally. The configuration of a virtual DVD drive enables read access to an installation source.

The maximum number of block-oriented devices which can be configured on a XenVM depends on the virtualization type:

– 100 in the case of paravirtualization
– 4 (or 16 when the VMDP[1] drivers are used) in the case of full virtualization

The following devices are also required:

- Virtual console
  The console is required in particular for installation. It permits entries to be made which are requested during installation. After the operating system has been started, it also enables the system to be accessed. To permit access to the console, a graphics card is configured for the keyboard assignment when the XenVM is created.

- Virtual Network Interface Card (NIC)
  Virtual Network Interface Cards can optionally be configured to enable the XenVM to communicate with other XenVMs or another network. In this case the Network Interface Card is connected to a virtual switch (vSwitch).

[1] SUSE Linux Enterprise Virtual Machine Driver Pack: The basic software X2000 supports the use of these paravirtualized drivers. See http://www.suse.com/products/vmdriverpack for information on using and procuring the drivers.

To permit a virtual disk, a DVD drive or a virtual Network Interface Card to be configured on a XenVM, the following resources must be available in the XenVM device management:

- Disk pools
- Installation sources
- Virtual switches

### Disk pools and virtual disks

The physical disks of the connected disk storage peripherals can be assigned to so-called disk pools and form a linear storage space. SAS-RAID systems (e.g. ETERNUS JX40) and external FC disks are supported.

A virtual disk is a section of a disk pool. The virtual disk is seen as a uniform and contiguous disk by the XenVM which uses it (in figure 7, for example, as device xvda; the corresponding device in a fully virtualized system would be hda), see also the figure below with the abstraction levels.

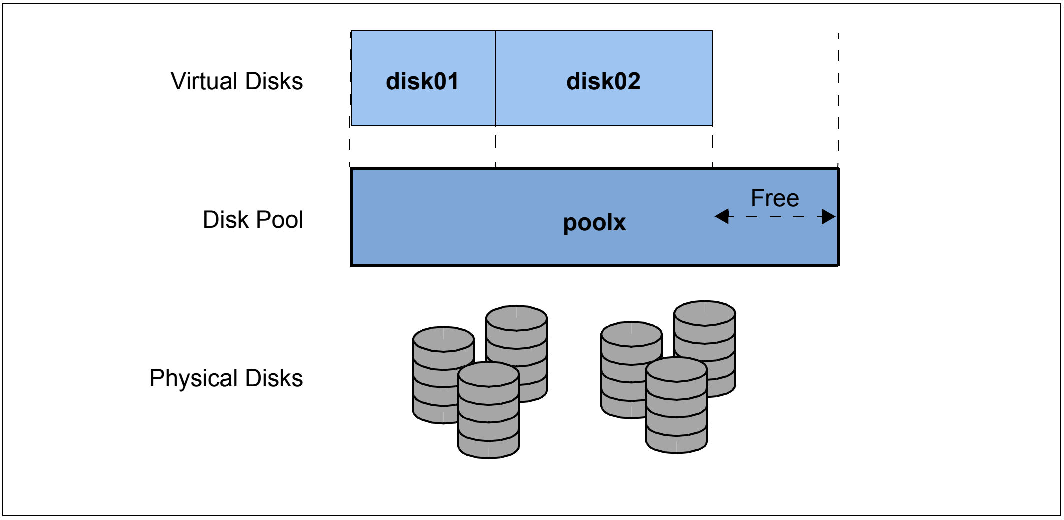


Bild 9: Virtual disks - abstraction level of disk usage

External FC disks can be connected to more than one host, which permits switching, i.e. alternating use of these disks.

For information on tasks in the XenVM device management see section “Managing XenVM devices on Server Unit x86” on page 175.

### Installation sources

ISO images of CDs/DVDs and installation configuration files which can be used to automate installation are referred to as installation sources. The ISO images provided as installation sources are employed primarily for system installation, but can, for instance, also be used to install applications or to provide data for the guest systems.

The installation sources are managed in a local library with 80 GB of storage space.

A XenVM can be assigned installation sources; the Linux/Windows systems see these as (virtual) drives. This assignment takes place either when the XenVM is created or at a later point in time, i.e. during ongoing operation.

For information on tasks in the XenVM device management see section “Managing installation sources” on page 182.

### Virtual switches

The Linux/Windows systems on the XenVMs communicate with each other or with external systems via software instances which are known as virtual switches (or vSwitches for short).

### Tape drives

Tape drives cannot be operated on XenVMs. Data backup of the Linux/Windows systems can be implemented via the IP network, e.g. by means of a Networker backup using an external backup server.

## 2.6 Customer Support and maintenance

### 2.6.1 Tasks of Customer Support

Customer Support has the following tasks:

- Diagnostics and debugging
- Software/hardware maintenance work
  - Installation of service packs
  - Installation of hot fixes
  - Installation of security fixes
  - Software/firmware upgrades
  - Model upgrades
- Hardware upgrades
- The contractually agreed annual maintenance
  - Updating the software/firmware
  - Changing batteries
  - Customer-specific measures
  - Configuration data backup at the end of the maintenance work

### 2.6.2 Tasks of the customer

In some cases Customer Support sometimes needs your assistance on site to perform maintenance activities. As a customer, you have the following tasks in the maintenance strategy:

- Permitting access to the SE server
  - Opening remote service access if required (requirement for the service and maintenance strategy)
  - Permitting access to the rack (e.g. to the local console)

- Assisting Customer Support when there are software/firmware updates for the units; in agreement with Customer Support, the following tasks may need to be performed:
  - Transferring the updates from CD/DVD to disk
  - Uploading service packs
  - Uploading hot fixes
  - Uploading and installing security fixes
  - Uploading, installing and uninstalling add-on packs
  - Deleting update files which are not installed
- Generating and supplying diagnostic documentation
- Scheduled provision of an annual maintenance window of approx. 5 hours
- If necessary, also unscheduled provision of a maintenance window

The following also applies when Application Units are operated:

- As customer you are responsible for operating the software on the Application Units. This includes tasks such as software installation, configuration, updates and importing patches. You obtain updates and patches yourself as part of their license agreement.
- If required, you install a new operating system or modify the SE server's LAN configuration and ensure the connection to status monitoring and remote service.
- When maintenance is performed, you grant Customer Support at least temporary access to the Application Unit's iRMC and root access to the operating system level of the Application Unit. The procedure and the type of access are agreed on individually between you and Customer Support.

When communicating with Customer Support, always specify your SE server unambiguously by means of the serial numbers of the system components. Determine the serial numbers as follows:

► In the tree structure select *Hardware → HW inventory* and open the *Units* tab.

Alternatively you can also inquire this information as follows:

► In the tree structure select *Hardware → Server → <unit name> → Information*.

The *System* tab shows system information for the selected unit.

#### Maintenance windows of the SE server

The SE server is designed to operate without interruption. To guarantee interrupt-free operation over lengthy periods, Customer Support performs certain maintenance work roughly once a year. This maintenance work (e.g. the installation of corrections) is performed within planned maintenance windows agreed on with the customer (e.g. in periods when there is a minimum load on the server).

## 2.6.3 Maintenance and remote service

The SE server is normally connected to remote service. The connection to the Support Center is established via the Management Unit using an internet connection (AIS Connect).

Customer Support configures the remote service in accordance with customer wishes when system installation is performed or when the SE server is placed in service.

## 2.6.4 Handling updates

### 2.6.4.1 Providing updates

Current security fixes are provided for downloading on the FUJITSU support pages. You download the updates required to your administration PC.

Alternatively, you can also receive updates such as service packs or hot fixes by email, on CD/DVD or by means of remote service.

When security requirements are more stringent, current security fixes must be installed regularly, see the Security Manual [6].

### 2.6.4.2 Tasks and responsibilities when installing updates

The table below shows the tasks of the administrator and of Customer Support and also the sequence when installing and managing updates.

| **Update type** | **Administrator** | **Service** |
|---|---|---|
| Security fix | All tasks are performed by the administrator:<br>– Clarify requirements<br>– Provide maintenance window (if necessary)<br>– Procure security fix<br>– Transfer security fix to system<br>– Install security fix and, if necessary, activate it explicitly with reboot | Inform and support the customer when required |
| Service pack | – Provide maintenance window | – Clarify requirements<br>– Procure service pack<br>– Transfer service pack to system<br>– Install service pack (via Teleservice or on site) |
| Hot fix | – Provide maintenance window (if necessary) | – Clarify requirements<br>– Procure hot fix<br>– Transfer hot fix to system (via remote service or on site)<br>– Install hot fix (via remote service or on site) |
| Add-on pack | – Clarify requirements[1]<br>– Procure software<br>– Transfer software to system<br>– Install/uninstall software | – Clarify requirements[1] |

[1] with respect to optional add-on packs or new versions of the add-on packs installed by default

# 3 Operating the SE Manager

This chapter describes how you operate an SE server using the SE Manager.

**Requirement:**

To enable you to access the SE Manager GUI and operate the SE server, one of the following web browsers must be installed on your computer.

The web browsers currently supported are:

- Firefox 17 (ESR) +
- Internet Explorer 10 & 11 (with or without compatibility mode)

Restrictions can apply when other browsers are used (e.g. for uploads, downloads, XenVM consoles, hardware inventory)

ℹ You can obtain information on restrictions when using older versions from your Customer Support contact.

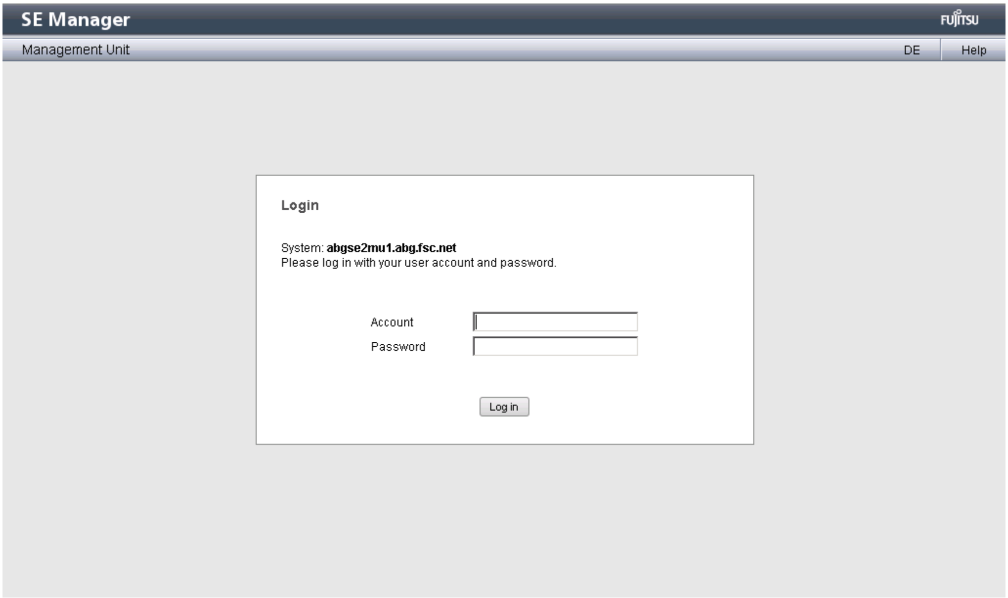
## 3.1 Calling the SE Manager

► Enter the address of the SE server in the address bar of the browser.

If the browser now displays a warning about the security certificate, click *Continue to this website*.

► Press the ↵ key.

The connection is set up. The login window is opened. The login window provides access to the web application. It has a different format from the other windows:



Login

System: **abgse2mu1.abg.fsc.net**
Please log in with your user account and password.

Account
Password

The login window is also displayed to permit you to log in again if you have logged out or the session was terminated owing to inactivity (see the section “Session management” on page 68).

### 3.1.1 Logging in

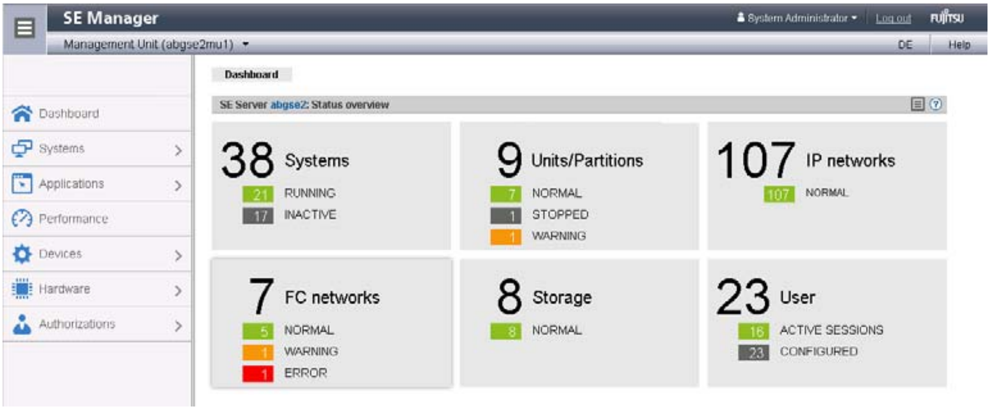
Access to the SE Manager is protected. You must log in with your account and the associated password.
Exception: The SE Manager help is unprotected.

- ► Enter your account in the login window.
- ► Enter your password.

> i When the SE server is supplied, the password *admin* is set for standard account *admin*. Change the password immediately after you have logged in for the first time (see section “Managing passwords” on page 272).

- ► Click *Log in*.

The *Dashboard* tab opens as the welcome page. It provides a quick overview of the systems, units, IP networks, FC networks, storage, and users of the SE server. The information displayed is described in the SE Manager help.



### 3.1.2 Logging out

- ► In the header area of the SE Manager main window click *Log out* to terminate the session. See section “Main window” on page 71.

The login window opens.

## 3.2 Session management

When you log in on the SE Manager, a session with a unique session ID is set up. The server regards all requests with the same session ID as connected and are assigned to your account.

This means in particular that a session which has not yet timed out is regarded as still valid when, in the browser, you close the tab via which you are logged in on the SE Manager (without logging out explicitly). When you connect to the SE Manager again before the session timeout has expired, you are redirected again to the dialog box opened most recently without having to log in once more.

### 3.2.1 Session timeout

You click *Log out* in the header area of the main window to terminate the current session explicitly. If you do not log out explicitly, the session terminates if there is no activity for 20 minutes, i.e. if the SE Manager registers no action in this time.

Each user can change this setting for himself/herself in the range from 5 through 60 minutes or exclude it:

- ► Click in the login information in the header area. A list containing the menu item *Individual settings* opens.
- ► Click *Individual settings*. The *Change update cycle and session timeout* dialog box opens in which you can enable/disable the session timeout and set the timeout in the range from 5 to 60 minutes.

The individual setting is stored in the SE Manager on a user-specific basis.

If you click in the main window after the session has terminated, the login window opens and you must log in again.

When you start an action in a dialog box after a session has timed out, the following message appears:

*The action could not be executed. Your session has expired. Please log in again.*

The login window appears after the dialog closes. See section “The dialog” on page 76.

### 3.2.2 Automatic update

Automatic update ensures that the data displayed in the main window is up to date. All the data displayed is updated in each cycle, in particular:

- the object lists and their statuses in the working area
- the object lists and their statuses in the tree structure

For information on "working area" and "tree structure", see section “Main window” on page 71.

While an automatic update is running, the update icon (rotating wheel) on the right-hand edge of the tabs shows this.

By default an update cycle of 30 seconds is available for each user. Each user can change this setting for himself/herself in the range from 10 through 120 seconds or exclude the automatic update. The setting is specified in the *Change update cycle and session timeout* dialog box (see section “Session timeout” on page 68). The individual setting is stored on an account-specific basis.

#### Suspend automatic update

As soon as you change the displayed data (filter, sort, click on a selection field, scroll), the automatic update is suspended.

The suspended update is indicated by the fixed icon on the top right-hand edge of the tabs. When you click this icon, the page is refreshed and automatic update is resumed. All changes which you have made on this page are then lost (e.g. filter set, selection fields selected).

# 3.3 SE Manager interface

The sections below describe the interface of the SE Manager and introduce terms which are used in the manual.

## 3.3.1 Window types

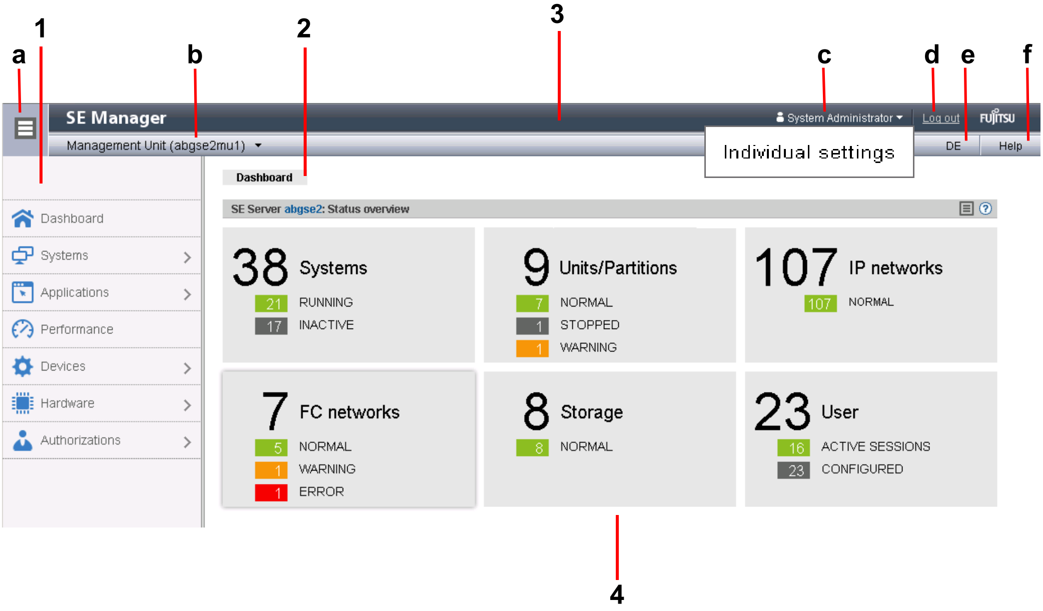
Various window types are used in the SE Manager:

- **Login window**: a window in which you log in using your account and password.
  See section “Logging in” on page 67.
- **Main window**: a window which is always visible between logging in and logging out on the SE Manager; it contains the navigation elements and the workarea in which information is output and actions are initiated.
  See section “Main window” on page 71.
- **Terminal window**: a window which is opened from the SE Manager and enables access to the BS2000 console, BS2000 dialog, SVP console or the shell of the MU. A terminal window can only be opened when there is an active session and subsequently remains open irrespective of the SE Manager's session.
  See section “The dialog” on page 76.
- **Dialog box**: a window which opens when an action starts and closes again after the action has been completed. It is also used to output error messages concerning the action being performed.
  See section “The dialog” on page 76.
- **Wizard**: a utility which guides you step by step through a sequence of windows (dialogs) to perform a task.
  See section “The wizard” on page 77.
- **Help window**: a window which opens in a separate tab or window of the browser when the online help is called.
  See section “Calling the online help” on page 85.

## 3.3.2 Main window

The main window of the SE Manager opens as soon as you have logged in on the SE Manager. The next two figures provide an example to name the areas in the main window and the principle controls.

**SE Manager: areas in the main window**



**1**: Tree structure

Main menus for selecting objects which are displayed in the working area

**2**: Tabs

Tabs for selecting objects which are displayed in the working area.

The *update* icon (rotating wheel) is displayed on the right-hand edge while the data is being updated automatically.

**3**: Header area

Contains general information and settings for the SE Manager:

**a** Click the icon to hide or display the tree structure again.

b *Management Unit (<unit name>) [location]* provides information about the Management Unit via which you are currently operating the SE Manager.

*<unit name>* is the name of the Management Unit.

If a location is configured with SYSLOCATION, *<location>* displays the entry.

If the field ends with the arrow icon, redundant Management Units are available. Click the field to obtain a list with links to the available Management Units.

c Displays the login information: user account or, if defined, the person-related name of the user account.
Click the login information and *Individual settings* in the following pop-up. In the subsequent dialog box you can set the cycle of the automatic update and the session timeout for your user account.
A tool tip for login information displays the values currently set.

d Click *Logout* to end the session.

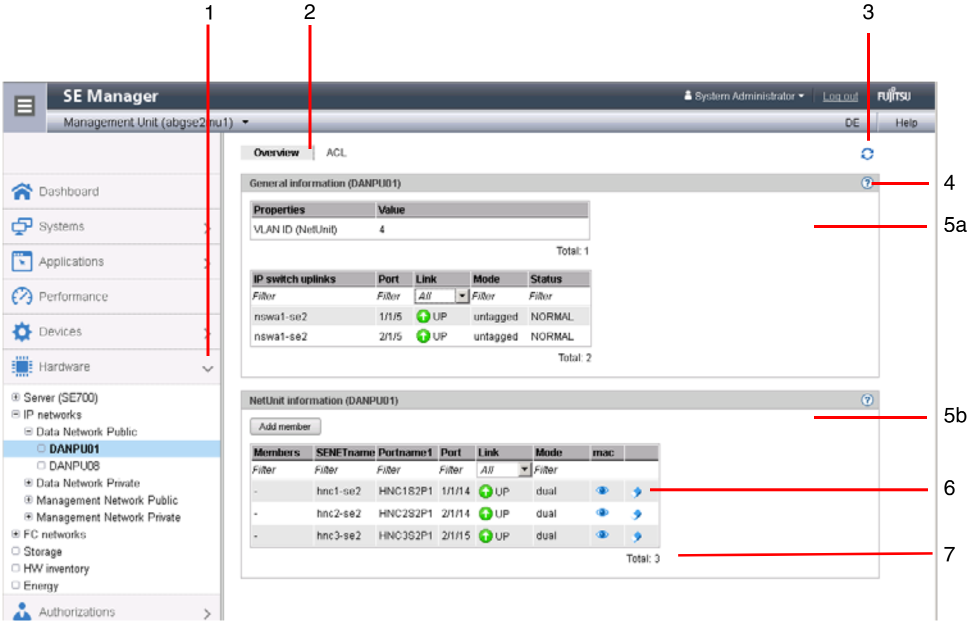
e Clicking the language option displayed (*DE* or *EN*) switches the web interface to the language selected.

f Click *Help* to open the SE Manager help in a new tab.

**4**: Working area

Displays data and enables dialog boxes and wizards to be opened to execute actions.

### SE Manager: elements of the main window



General information (DANPU01)

| Properties | Value |
|---|---|
| VLAN ID (NetUnit) | 4 |

Total: 1

| IP switch uplinks | Port | Link | Mode | Status |
|---|---|---|---|---|
| *Filter* | *Filter* | *All* | *Filter* | *Filter* |
| nswa1-se2 | 1/1/5 | UP | untagged | NORMAL |
| nswa1-se2 | 2/1/5 | UP | untagged | NORMAL |

Total: 2

NetUnit information (DANPU01)

| Members | SENETname | Portname1 | Port | Link | Mode | mac | |
|---|---|---|---|---|---|---|---|
| *Filter* | *Filter* | *Filter* | *Filter* | *All* | *Filter* | | |
| - | hnc1-se2 | HNC1S2P1 | 1/1/14 | UP | dual | | |
| - | hnc2-se2 | HNC2S2P1 | 2/1/14 | UP | dual | | |
| - | hnc3-se2 | HNC3S2P1 | 2/1/15 | UP | dual | | |

Total: 3

**1** Active main menu of the tree structure

**2** Active tab

3 *Update* icon to manually update the displayed information. This icon is displayed when the automatic update is suspended (see page 69). If the automatic update is active, the rotating wheel is briefly displayed as an update icon in the rhythm of the update.

**4** *Help* icon for calling the SE Manager help on a context-sensitive basis (see page 85)

**5 a, b** The information is subdivided into groups (in the example above, 5a and 5b). Each group contains one or more tables with properties of the objects displayed.

**6** Icons for triggering actions

**7** Number of entries in the table *Total: <n>* or *Total <objects>: <n>*

### 3.3.3 Terminal window

BS2000 console window, BS2000 dialog box, SVP console window, and shell terminal (CLI) are opened in a separate terminal window after they are called in the SE Manager. Subsequently the terminal window remains open irrespective of the SE Manager's session.

The terminal window and its embedding in the SE Manager have the following properties, among others:

- No further login is required when the terminal window is called.
- The size of the window can be changed flexibly.
- A virtual keyboard (matching the functionality):
  The virtual keyboard enables all required characters and function keys to be entered irrespective of the real keyboard's layout.
- Copy & paste functions:
  - Copy/paste with the context menu in the terminal window
  - Cross-window copy/paste (terminal window ↔ Windows) under Windows

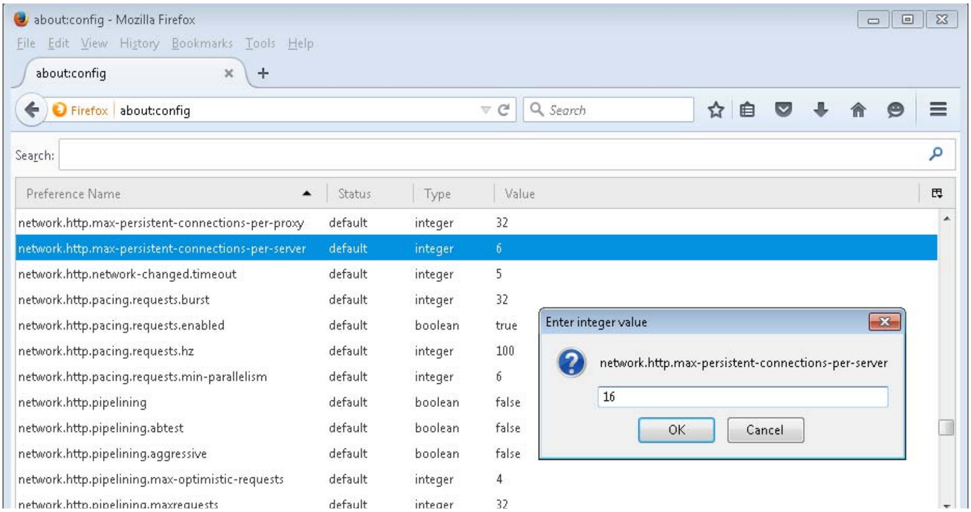
    →Windows:
    Copying with *COPY* (context menu) or *CTRL+C* in the terminal window.
    Pasting with *Paste* (context menu) or *CTRL+V* in Windows.

    →Terminal window:
    Copying with *Copy* (context menu) or *CTRL+C* in Windows.
    Pasting with *PASTE* (context menu) in the terminal window or via the menu bar of Firefox (**no** *CTRL+V* is possible in the terminal window!)
- In the event of a loss of connection, the *Connect* button appears in the middle of the terminal window. When you click this button, the terminal window session is continued and you can once again make entries. A prerequisite for this is that the SE Manager session in which the terminal window was opened is still active.

i If you want more than one terminal window to remain open in parallel (e.g. with BS2000 console windows), this must also be supported on the client side by the number of possible connections to a server. You must configure your browser appropriately for this purpose.

*Configuration for Firefox:*

By default Firefox supports six connections to a server. A higher number can be configured as shown in the figure below.


about:config - Mozilla Firefox
File Edit View History Bookmarks Tools Help
about:config
Firefox about:config
Search
Search:

| Preference Name | Status | Type | Value |
|---|---|---|---|
| network.http.max-persistent-connections-per-proxy | default | integer | 32 |
| network.http.max-persistent-connections-per-server | default | integer | 6 |
| network.http.network-changed.timeout | default | integer | 5 |
| network.http.pacing.requests.burst | default | integer | 32 |
| network.http.pacing.requests.enabled | default | boolean | true |
| network.http.pacing.requests.hz | default | integer | 100 |
| network.http.pacing.requests.min-parallelism | default | integer | 6 |
| network.http.pipelining | default | boolean | false |
| network.http.pipelining.abtest | default | boolean | false |
| network.http.pipelining.aggressive | default | boolean | false |
| network.http.pipelining.max-optimistic-requests | default | integer | 4 |
| network.http.pipelining.maxrequests | default | integer | 32 |

Enter integer value

network.http.max-persistent-connections-per-server

16

OK Cancel

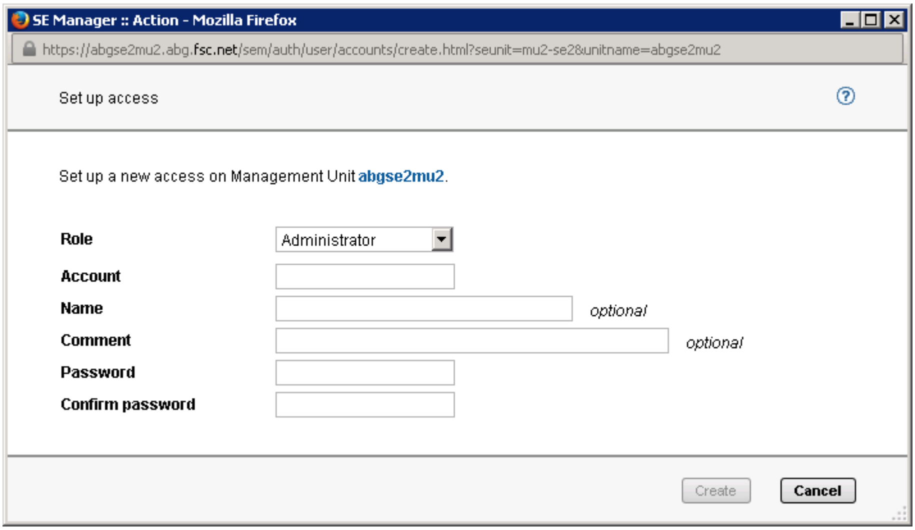
*Configuration for Internet Explorer:*

By default Internet Explorer also supports six connections to a server. How you increase this number when required is explained at:

http://support.microsoft.com/kb/282402/de

## 3.3.4 The dialog

A dialog opens as soon as you start an action:



SE Manager :: Action - Mozilla Firefox
https://abgse2mu2.abg.fsc.net/sem/auth/user/accounts/create.html?seunit=mu2-se2&unitname=abgse2mu2

Set up access

Set up a new access on Management Unit **abgse2mu2**.

| | | |
|---|---|---|
| **Role** | Administrator ▾ | |
| **Account** | | |
| **Name** | | *optional* |
| **Comment** | | *optional* |
| **Password** | | |
| **Confirm password** | | |

A dialog comprises:

- Title bar with the following information:
  *SE Manager :: Action*
- Header area
  Information on the action
  *Help* icon (optional) for calling the help on a context-sensitive basis
- Parameter area (optional): fields for entering or selecting parameter values. The syntax check takes place immediately a value is entered in a field. When entries are incorrect, an i icon is displayed next to the field. When you drag the mouse over the i icon, possible values or the maximum character length and permissible characters are displayed.
- Area with the labeled buttons, e.g. *Create* and *Cancel*.

A dialog box opens for each action in which you can either

- control the action using options
- confirm the action (dialog box with empty parameter area)

Alternatively you can also cancel the action.

You start an action action using an icon or button. Following confirmation the action is executed and the dialog box remains open. Each action displays feedback in the associated dialog box. You can then terminate the dialog box with *Close* and thus refresh the working area of the main window. If you close the dialog box in another way, the working area is not refreshed.

ℹ No types of lock are provided when actions are executed. This means that, for example, multiple dialog boxes can create, select or delete the same object in parallel. When devices are configured, the same unit IDs or MNs can, for example, be selected simultaneously. All actions are executed for this object, but only the first action is successful and the other actions fail and lead to an error message.

When an action has failed, in addition to the error messages the original message of the command called can also be displayed. Irrespective of the language setting in the SE Manager, such original messages are always displayed in English.

You can press function key *F5* to update the SE Manager manually. Not every action modifies the table contents.

ℹ Do not close the dialog using the close function in the browser window because the working area is then not updated immediately. The browser functionality should never be used in dialogs.

The section “Executing an action” on page 83 describes what you must take into account when executing an action.

### 3.3.5 The wizard

A wizard is a utility which takes you through a task step by step.

As a rule a wizard consists of several steps (dialogs) which you must complete. The number of steps in a wizard depends on

- the number of parameters which are required for the action
- the grouping of the parameters

You control execution of the wizard using the buttons at the bottom right in each step.

| | |
|---|---|
| *Next* | Opens the next step in the wizard. |
| *Back* | Opens the previous step in the wizard. |
| *Cancel* | Cancels the wizard without saving your changes. |
| *<action>* | Closes the task and executed the wizard with your settings. *<action>* on the button means the action to be executed, e.g. *Add* or *Create*. |

Feedback from the system is displayed in the wizard's last dialog box.

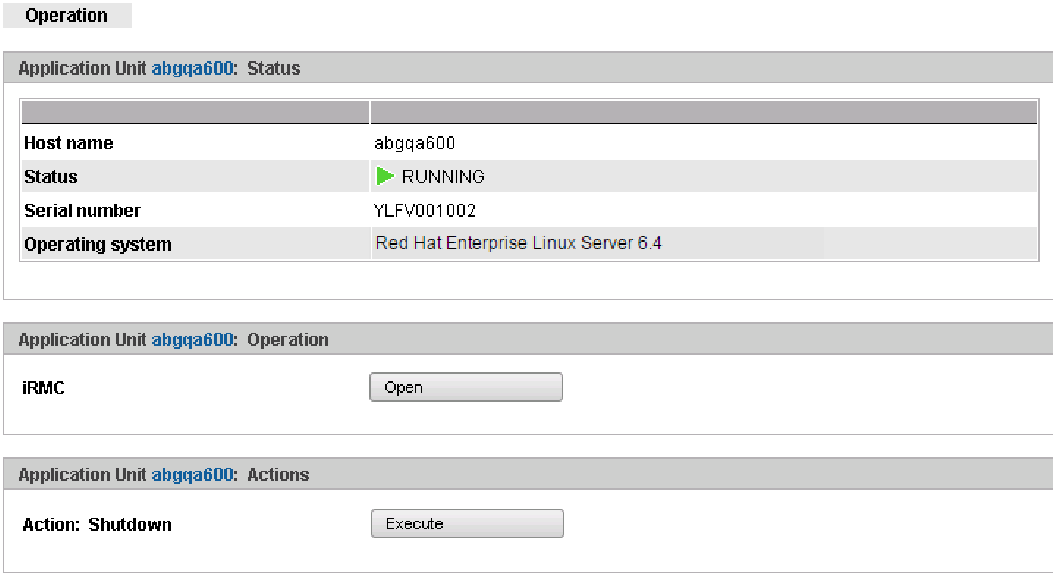
### 3.3.6 Web UIs of Application Units

On Application Units web applications such as a VMware ESXi Server or an Oracle VM Manager can run which are operated using a browser window of their own.

*Example:*

A VMware ESXi Server runs on the AU.

*Systems* → *<unit name>(AU<model>)* → *Virtual machines* → <*vm name*> provides you with the *Operation* tab.



Operation

Application Unit abgqa600: Status

| | |
|---|---|
| Host name | abgqa600 |
| Status | ▶ RUNNING |
| Serial number | YLFV001002 |
| Operating system | Red Hat Enterprise Linux Server 6.4 |

Application Unit abgqa600: Operation

iRMC

Application Unit abgqa600: Actions

Action: Shutdown

The *open* action opens a separate browser window to execute the required actions. This window also remains open irrespective of the session.

# 3.4 Working with the SE Manager

## 3.4.1 Calling an object or function in the SE Manager

Proceed as follows to call a function area in the SE Manager:

► Select an object or function in the primary navigation by clicking it.

A tab opens in the working area which enables you to manage or operate the object or function Some functions are distributed over more than one tab, and these are displayed at the top of the working area.

In the working area the content which belongs to the function area of the first tab is displayed in one or more tables. Buttons or icons may also be available to execute actions.

► If required, select another tab by clicking it.
Alternatively you can also switch directly between the associated tabs in the tree structure using an object's or function's tool tip.

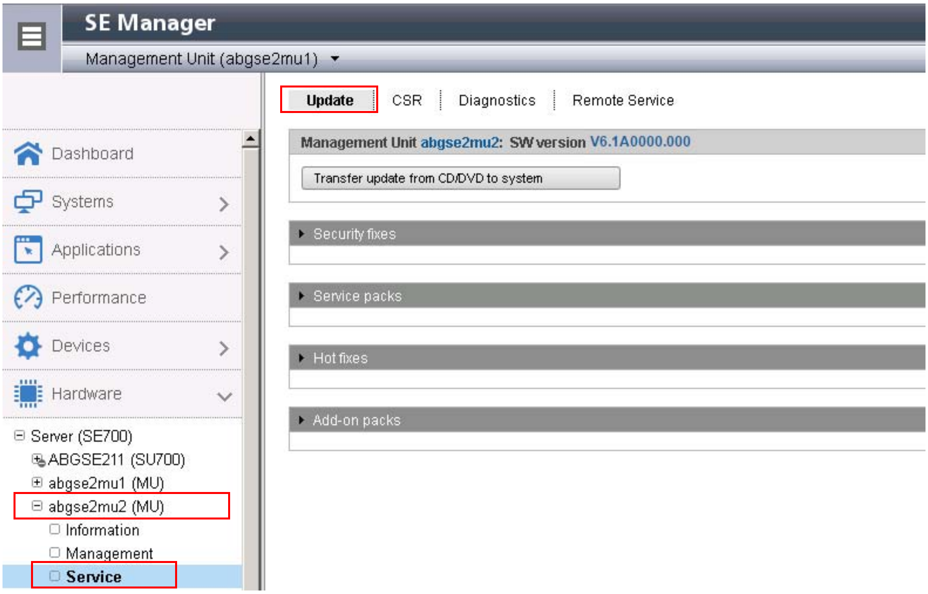
The content of the working area changes if you select another tab.

The selected menu item and the selected tab are highlighted by being displayed in bold black print against a blue or gray background.

*Example*

*Hardware* → *Server* → *<unit name>(MU)* → *Service*, *Update* tab

*Hardware → Server → <unit name>(MU) → Service* corresponds to a selection in the tree structure, *Update* of a selection in the secondary navigation, also called tabs.



Management Unit abgse2mu2: SW version V6.1A0000.000

Transfer update from CD/DVD to system

The objects and functions which are displayed in the tree structure depend on the server component and the configuration.

## 3.4.2 Navigation

The navigation in the SE Manager is distributed over the main menus *Dashboard*, *Systems*, *Application*, *Performance*, *Devices*, *Hardware*, and *Authorizations.* With the exception of *Dashboard* and *Performance*, all the main menus can be expanded.

When you click a main menu, the tree structure beneath it expands. Below this you see objects and functions as links. Navigation using the main menus is also referred to as the primary navigation.

When you click a link, a tab opens in the working area which enables you to manage or operate the object or function Some functions are distributed over more than one tab, and these are displayed at the top of the working area. These tabs are also referred to as secondary navigation.

A main menu expands in the following cases:

- When you click the main menu again.
- When you click a link in another main menu.

### Links to add-on software

After add-on packs have been installed, the SE Manager can also contain links to the GUI of the software concerned. When you click such a link, the GUI is displayed in the SE Manager. You use the *SE Manager* entry in the GUI's main menu to exit the GUI and return to the SE Manager.

The *Performance* main menu is a link to openSM2. It is only available when the add-on pack is installed.

The link to the Storage Manager (StorMan) is available under the *Hardware* main menu. It is displayed in the tree structure with *Storage*.

If other add-on software is installed, you will find the corresponding links in the *Applications* main menu.(e.g. ROBAR, openUTM)

### Authorizations

The scope and thus the visibility of the functions depends on the role which is assigned to your account.

New links are created in the tree structure for the following functions:

- *Systems* main menu:
  - when creating a BS2000 VM
  - when creating a XenVM
  - after a virtual machine has been created on an AU
- *IP networks* main menu:

  when creating a new network

In the tree structure an operator with configured individual rights sees only the BS2000 VMs which are permitted for him/her. A BS2000, AU, or XenVM administrator sees only the functions for managing "his/her" systems (BS2000 systems, Application Units or XenVMs).

## 3.4.3 Filtering and sorting a table

### Filtering a table

In tables you can restrict the view of the data displayed using free text or filter lists in table columns. Filters thus make it easier to handle extensive tables. Import filters are available which filter the data to build up a table.

A filter is retained only until the next time the main window is set up, in other words until an action is executed or the page has been explicitly refreshed. The entries are then displayed again.

Detailed information on filtering tables together with the various filter options is provided in the SE Manager help.

The various filters can also be combined. They are described in the SE Manager help at the places where they can be used.

i Automatic update is suspended by filtering (see section “Automatic update” on page 69).

### Sorting a table

A table is sorted according to the values of a selected column.

► Drag the mouse cursor over the column headings in the table.
When the mouse cursor turns into a symbolic hand, you can sort the table according to the values of this column.

► Click the column heading.

The table is sorted.

If you click on the same column heading again, the sort order changes from ascending to descending or vice versa.

A sort is retained only until the next time the main window is set up, in other words until an action is executed or the page has been explicitly refreshed. The entries are then displayed again. Sorting according to a different column cancels the previous sort order.

i Automatic update is suspended by a sort (see section “Automatic update” on page 69)

### 3.4.4 Executing an action

This section describes how an action is typically executed.

You start an action in the SE Manager's working area. Two options are available after you have selected a tab:

- ► Click a button.
- ► Click an icon in a table (e.g. *Change*, *Delete*).
  Icons always belong to a particular record (of a table row) and are therefore contained in this table row. Each icon stands for a particular task which you can execute. Detailed information on the SE Manager's icons is provided in the SE Manager help.

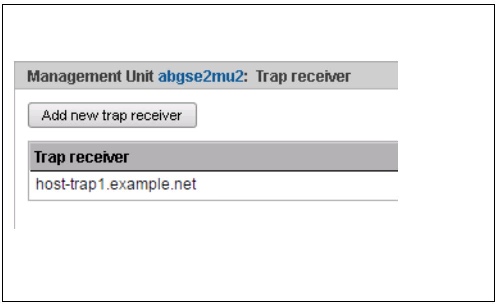
After you have started the action, a dialog opens.
See the section “Main window” on page 71 for the layout.

Proceed as follows in interactive mode:

- ► If required, control the action with options.
- ► Confirm the action.

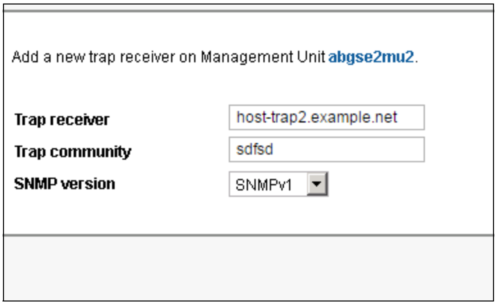
Following confirmation the action is executed and the dialog box remains open. Each action displays feedback in the associated dialog box. You can then terminate the dialog box with *Close* and thus refresh the working area of the main window. If you close the dialog box in another way, the working area is not refreshed.

#### Example of how an action is executes


Management Unit abgse2mu2: Trap receiver

| Trap receiver |
|---|
| host-trap1.example.net |

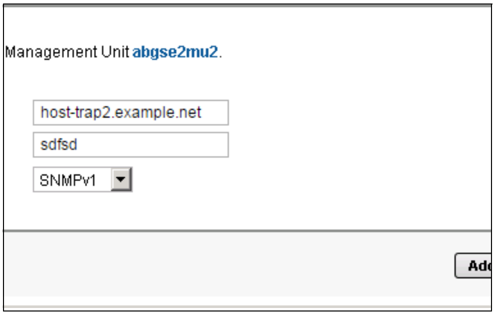
- ► Proceed as follows to log in on the SE Manager:
- ► Select *Hardware* → *Server* → *<unit name> (MU)* → *Management*, *SNMP* tab.
- ► *Trap receiver* group: click *Add new trap receiver*.
  A dialog with a parameter area opens.



Add a new trap receiver on Management Unit abgse2mu2.

| | |
|---|---|
| **Trap receiver** | host-trap2.example.net |
| **Trap community** | sdfsd |
| **SNMP version** | SNMPv1 |

- ► Enter an IP address.
- ► Enter a trap community.
- ► Select the SNMP version.



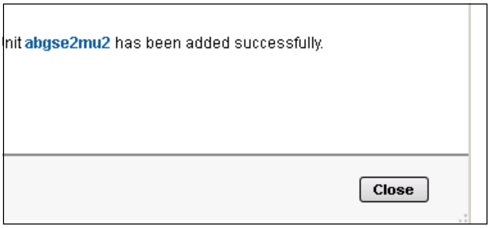
Management Unit abgse2mu2.

host-trap2.example.net

sdfsd

SNMPv1

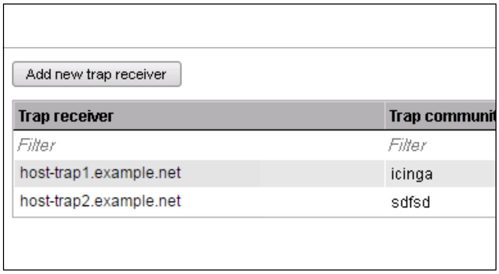
- ► Click *Add*.



nit abgse2mu2 has been added successfully.

After a wait time, the message that the trap receiver has been successfully added appears.

- ► Click *Close*.



| Trap receiver | Trap communit |
|---|---|
| Filter | Filter |
| host-trap1.example.net | icinga |
| host-trap2.example.net | sdfsd |

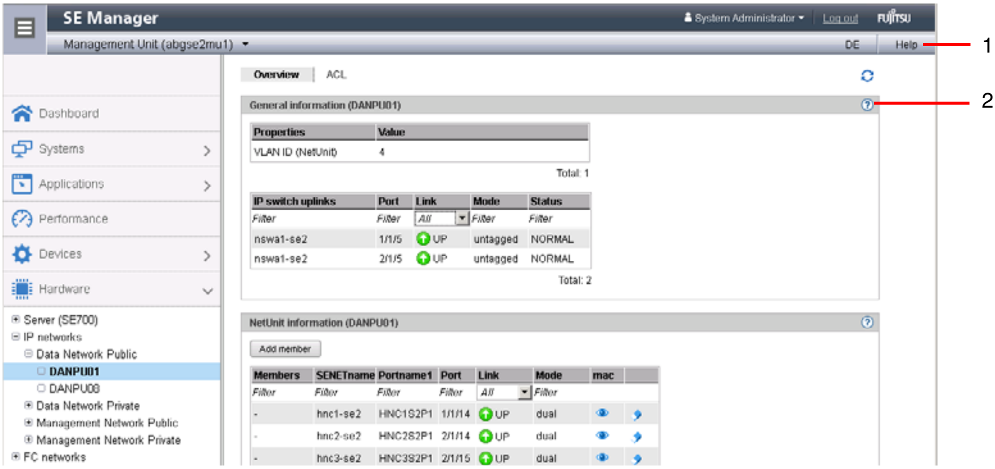
The table displays the added trap receiver.

### 3.4.5 Calling the online help

The SE Manager incorporates an integrated, context-sensitive online help, the SE Manager help.

The SE Manager help contains information on all groups of the SE Manager.

There are two ways to call the SE Manager help:



| Properties | Value |
|---|---|
| VLAN ID (NetUnit) | 4 |

Total: 1

| IP switch uplinks | Port | Link | Mode | Status |
|---|---|---|---|---|
| *Filter* | *Filter* | *All* | *Filter* | *Filter* |
| nswa1-se2 | 1/1/5 | UP | untagged | NORMAL |
| nswa1-se2 | 2/1/5 | UP | untagged | NORMAL |

Total: 2

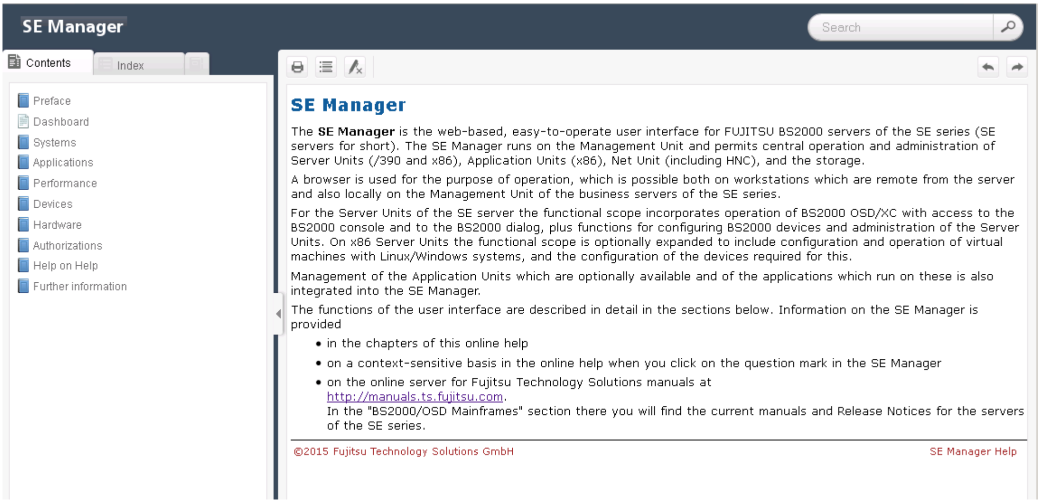
| Members | SENETname | Portname1 | Port | Link | Mode | mac | |
|---|---|---|---|---|---|---|---|
| *Filter* | *Filter* | *Filter* | *Filter* | *All* | *Filter* | | |
| - | hnc1-se2 | HNC1S2P1 | 1/1/14 | UP | dual | | |
| - | hnc2-se2 | HNC2S2P1 | 2/1/14 | UP | dual | | |
| - | hnc3-se2 | HNC3S2P1 | 2/1/15 | UP | dual | | |

Bild 10: Calling the SE Manager help

**1** Using*Help* in the SE Manager header area:
The homepage of the SE Manager help is called in a new tab of the browser window.

**2** Using the *Help* icon (question mark) in the selected group:
Information on the functionality of the group is displayed on a new tab in the browser window.

The figure below shows the homepage of the SE Manager help:



**SE Manager**

The **SE Manager** is the web-based, easy-to-operate user interface for FUJITSU BS2000 servers of the SE series (SE servers for short). The SE Manager runs on the Management Unit and permits central operation and administration of Server Units (/390 and x86), Application Units (x86), Net Unit (including HNC), and the storage.

A browser is used for the purpose of operation, which is possible both on workstations which are remote from the server and also locally on the Management Unit of the business servers of the SE series.

For the Server Units of the SE server the functional scope incorporates operation of BS2000 OSD/XC with access to the BS2000 console and to the BS2000 dialog, plus functions for configuring BS2000 devices and administration of the Server Units. On x86 Server Units the functional scope is optionally expanded to include configuration and operation of virtual machines with Linux/Windows systems, and the configuration of the devices required for this.

Management of the Application Units which are optionally available and of the applications which run on these is also integrated into the SE Manager.

The functions of the user interface are described in detail in the sections below. Information on the SE Manager is provided

- in the chapters of this online help
- on a context-sensitive basis in the online help when you click on the question mark in the SE Manager
- on the online server for Fujitsu Technology Solutions manuals at http://manuals.ts.fujitsu.com.
  In the "BS2000/OSD Mainframes" section there you will find the current manuals and Release Notices for the servers of the SE series.

©2015 Fujitsu Technology Solutions GmbH SE Manager Help

Bild 11: Homepage of the SE Manager help

The area on the left contains the table of contents, which is structured in a similar way to the primary and secondary navigation of the SE Manager.

The content selected is displayed on the right. The area on the left can be expanded and collapsed to accommodate size of the content area.

Instead of the content, you can also have the following displayed in the area on the left:

- Index with an entry field for searches
- Glossary with a entry field for searches

To select the tab required, click in the top of the area on the left.

You can print out the contents displayed (*Print topic* icon).

The contents of the SE Manager help are also supplied as PDF files. You will find the PDF files under *Further documentation* in the SE Manager help.

### Searching the help

You can navigate and search in the entire SE Manager help irrespective of how it was called. The search field for searches is on the right above the work area.

- ► Enter the term you wish to search for.
- ► Click the *Search* icon. In the working area the *Search* page lists all topics in which the term appears. The header, the first lines, and the path name of the topic are displayed.

- ► Click a topic header in the table. The topic is displayed on the right in the work area. All places which contain the search term are also highlighted.

**Saving favorites**

The browser's functions enable you to save two different types of favorite in the help:

- Topics which you want to make a note of
- Page with the result list of a search

### 3.4.6 Error handling

This section provides information on handling errors and problems.

The following problems can occur:

- You cannot establish a connection.
- You cannot start an action.
- Errors occur when an action is started.
- The connection is interrupted.

**Measures**

- ► If you cannot establish a connection, check the address entered, and also the availability and, if necessary, the system status of the SE server’s system components.
- ► If execution of an action fails, the cause is specified in the parameter area of the dialog.
- ► With some actions, e.g. a reboot of the MU, in which you operate the SE Manager, the connection is interrupted. Log in again after such an action.
- ► Search for the relevant topic in the SE Manager help if you require further information (see the section “Calling the online help” on page 85).
- ► If you still cannot solve the problem, contact Customer Support.

# 4 Dashboard

The *Dashboard* menu contains the *Dashboard* tab, which provides a quick overview of the *systems*, *units*, *IP networks*, *FC networks*, *storage*, and *users* of the SE server. The *Dashboard* is displayed after you have logged in on the SE Manager.

i If at least one AU87 or DBU87 is available, *Units/Partitions* is displayed instead of *Units*. With AU87 or DBU87, the chassis of the AU and the partitions are each counted as individual units.

Up to 3 status classes are displayed per object type. If more than 3 status classes are currently assigned, the last line displays the status class with the highest priority level. The totals display also contains the less urgent problematical statuses which cannot be displayed separately.

The tab offers the following functionality for this purpose:

- Displaying the status overview in the tile view
- Displaying the status overview in the list view
- Displaying the overview page associated with a component
- Filtering the overview page according to an object type
- Displaying the overview for a component / object type filtered according to status

Detailed information on the *Dashboard* tab is provided in the SE Manager help.

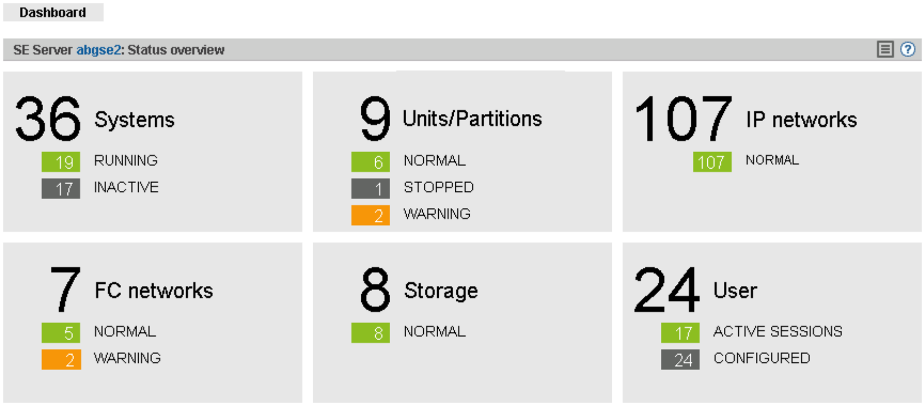
### Displaying the status overview in the tile view

► In the tree structure select *Dashboard*.

The *Dashboard* tab with the *Status overview* group opens. This enables you to see at a glance whether any problem exists.

► If the tile view is not displayed, click the *Tiles* icon in the group header.

The tile view opens.



SE Server abgse2: Status overview

36 Systems
19 RUNNING
17 INACTIVE

9 Units/Partitions
6 NORMAL
1 STOPPED
2 WARNING

107 IP networks
107 NORMAL

7 FC networks
5 NORMAL
2 WARNING

8 Storage
8 NORMAL

24 User
17 ACTIVE SESSIONS
24 CONFIGURED

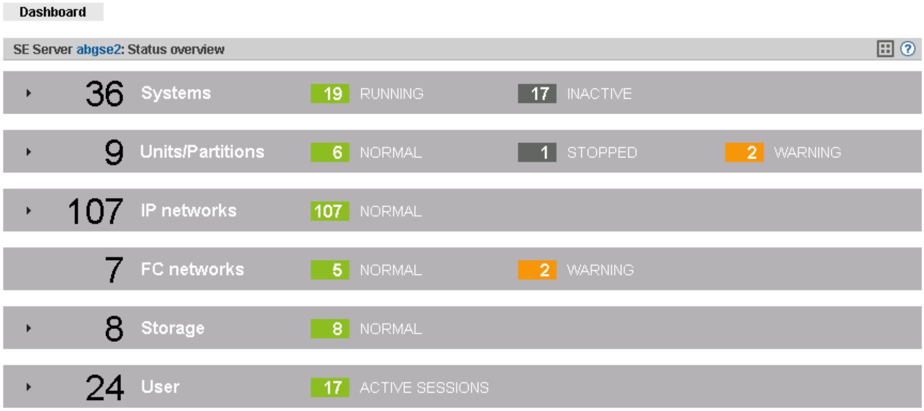
### Displaying the status overview in the list view

- In the tree structure select *Dashboard*.

  The *Dashboard* tab with the *Status overview* group opens. This enables you to see at a glance whether any problem exists.

- If the list view is not displayed, click the *List* icon in the group header.

  The list view opens.



SE Server abgse2: Status overview

36 Systems 19 RUNNING 17 INACTIVE

9 Units/Partitions 6 NORMAL 1 STOPPED 2 WARNING

107 IP networks 107 NORMAL

7 FC networks 5 NORMAL 2 WARNING

8 Storage 8 NORMAL

24 User 17 ACTIVE SESSIONS

- Click the arrow at the start of a component row.

  The list for the selected component expands. In the expanded status the information is subdivided further, and displayed in a line for each object type.

### Displaying the overview page associated with a component

- ► In the tree structure select *Dashboard*.
- ► When the *Dashboard* tab in the tile view opens, click the tile for the required component, e.g. *Systems*.
- ► When the *Dashboard* tab opens in the list view, click the component name in the list header of the required component, e.g. *Systems*.

The corresponding overview page opens, in this case the *Systems* main menu with the *Overview* tab.

### Filtering the overview page according to an object type

- ► In the tree structure select *Dashboard*.
- ► If the list view is not displayed, click the *List* icon in the group header.
- ► Click the arrow at the start of a component row to which the required object belongs, e.g. *Units*.

  The list for the selected component expands.
- ► In the expanded list, click the required object type, e.g. *Management Unit*.

The associated overview page opens with the corresponding filter, in this example the *Hardware* main menu with the *Units* tab. Only Management Units are displayed.

### Displaying the overview for a component / object type filtered according to status

Up to 3 status classes are displayed. If more than 3 status classes are currently assigned, the last line displays the status class with the highest priority level. The totals display also contains the less urgent problematical statuses which cannot be displayed separately.

You cannot filter the overview for the *Units* or *Units/Partitions* component and for the associated object types according to *Status*.

- ► In the tree structure select *Dashboard*.
- ► If the list view is not displayed, click the *List* icon in the group header.

- ► Select one of the following procedures:
  - ► In order to display the overview for a component filtered according to status, in the list header click the status of the required component according to which you wish to filter the overview, e.g. for the component *Systems* the status *INACTIVE*.

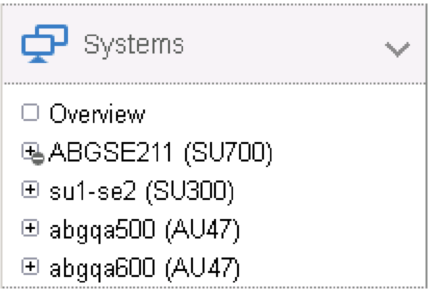
    The associated overview page opens with the corresponding filter, in this example the *Systems* main menu with the *Overview* tab. Only the systems with the status *INACTIVE* are displayed.
  - ► In order to display the overview for an object type filtered according to status, in the line with the required object type click the status according to which you wish to filter the overview, e.g. for the object type *VM2000* the status *INACTIVE.*

    The associated overview page opens with the corresponding filter, in this example the *Systems* main menu with the *Overview* tab. Only the VM2000 systems with the status *INACTIVE* are displayed.

# 5 Operating and managing systems on Server Units

The systems referred to here are the Native and virtual operating systems which run on the various units of the SE server.

You operate and manage the systems using the *Systems* menu in the tree structure. See the following example for an SE700:



In the tree structure displayed, the units are shown on which the so-called "productive systems" with their applications run, i.e. Server Units with BS2000 systems and Application Units with Unix, Linux or Windows systems. In each case the name is followed by the type of Server Unit in parentheses:

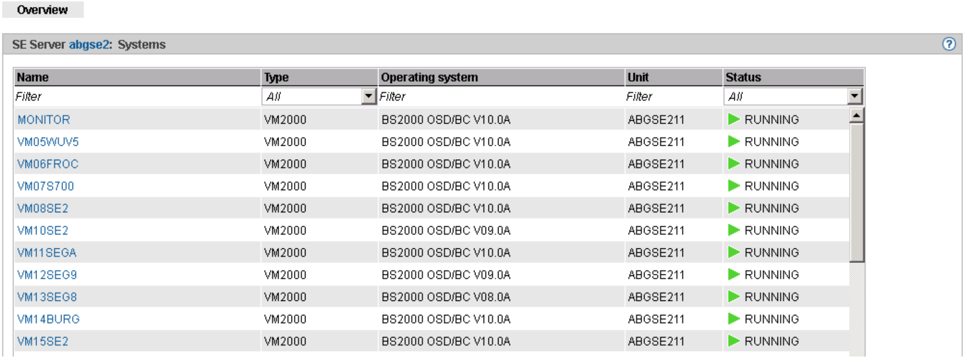
- In the example, SU700 refers to a Server Unit of the type /390.
- In the example, SU300 refers to a Server Unit of the type x86.
- In the example, AUnn refers to Application Units based on an x86-based server.

i The operation and administration of the systems on AUs are described in the chapter “Operating and managing systems on Application Units” on page 133.

## Overview of all systems of the SE server

► Select *Systems* → *Overview*, *Overview* tab.

The *Overview* tab displays information on all systems present on the SE server. See the following example for an SE300:



SE Server abgse2: Systems

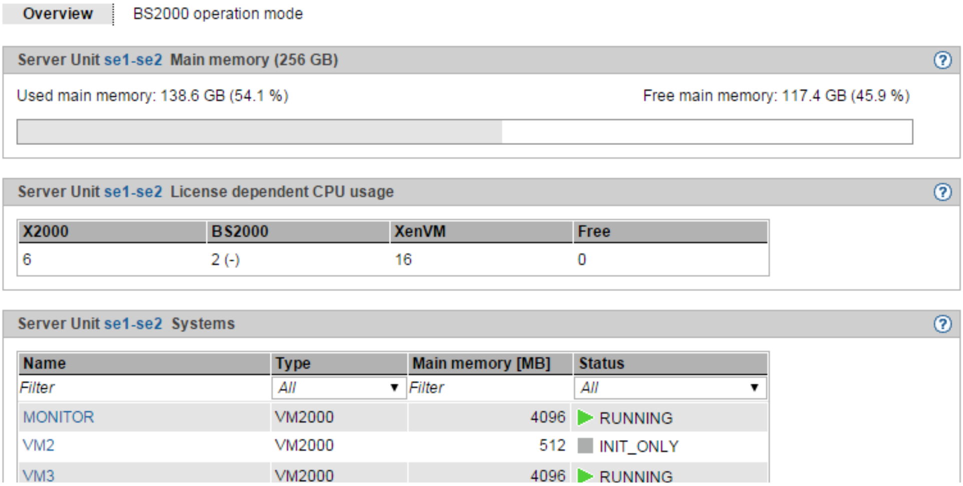
| Name | Type | Operating system | Unit | Status |
|---|---|---|---|---|
| Filter | All | Filter | Filter | All |
| MONITOR | VM2000 | BS2000 OSD/BC V10.0A | ABGSE211 | ▶ RUNNING |
| VM05WUV5 | VM2000 | BS2000 OSD/BC V10.0A | ABGSE211 | ▶ RUNNING |
| VM06FROC | VM2000 | BS2000 OSD/BC V10.0A | ABGSE211 | ▶ RUNNING |
| VM07S700 | VM2000 | BS2000 OSD/BC V10.0A | ABGSE211 | ▶ RUNNING |
| VM08SE2 | VM2000 | BS2000 OSD/BC V10.0A | ABGSE211 | ▶ RUNNING |
| VM10SE2 | VM2000 | BS2000 OSD/BC V09.0A | ABGSE211 | ▶ RUNNING |
| VM11SEGA | VM2000 | BS2000 OSD/BC V10.0A | ABGSE211 | ▶ RUNNING |
| VM12SEG9 | VM2000 | BS2000 OSD/BC V09.0A | ABGSE211 | ▶ RUNNING |
| VM13SEG8 | VM2000 | BS2000 OSD/BC V08.0A | ABGSE211 | ▶ RUNNING |
| VM14BURG | VM2000 | BS2000 OSD/BC V10.0A | ABGSE211 | ▶ RUNNING |
| VM15SE2 | VM2000 | BS2000 OSD/BC V10.0A | ABGSE211 | ▶ RUNNING |

► When you click on a system in the *Name* column, the *Operation* tab of the selected system opens.

## Overview of the systems of a System Unit

► Select *Systems* → *<unit>(SU<model>)*, *Overview* tab.

The *Overview* tab displays information the systems present on the SU. See the following example for an SU300:



Server Unit se1-se2 Main memory (256 GB)

Used main memory: 138.6 GB (54.1 %)

Free main memory: 117.4 GB (45.9 %)

Server Unit se1-se2 License dependent CPU usage

| X2000 | BS2000 | XenVM | Free |
|---|---|---|---|
| 6 | 2 (-) | 16 | 0 |

Server Unit se1-se2 Systems

| Name | Type | Main memory [MB] | Status |
|---|---|---|---|
| Filter | All | Filter | All |
| MONITOR | VM2000 | 4096 | ▶ RUNNING |
| VM2 | VM2000 | 512 | ■ INIT_ONLY |
| VM3 | VM2000 | 4096 | ▶ RUNNING |

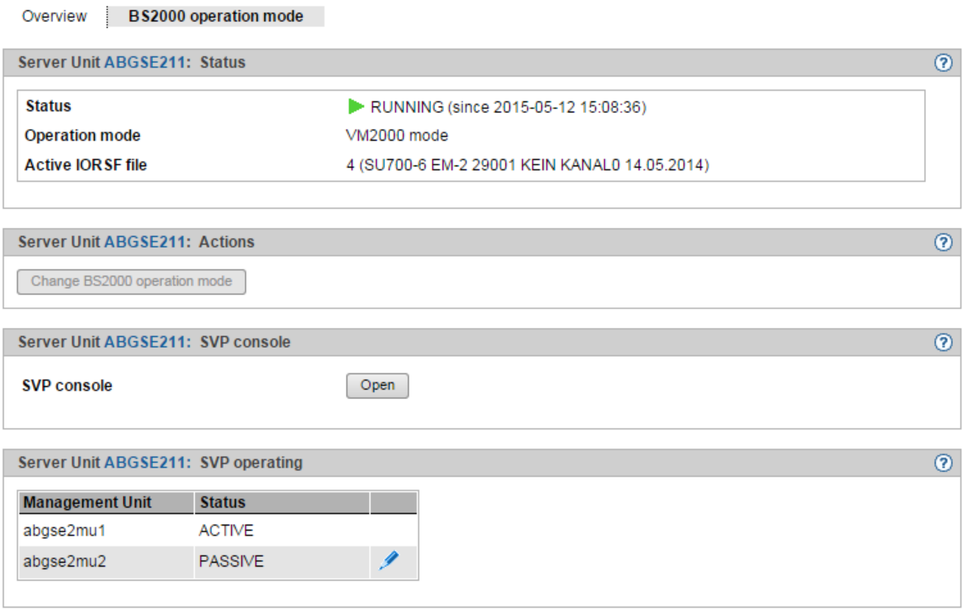
► When you click on a system in the *Name* column, the *Operation* tab of the selected system opens.

## 5.1 Setting BS2000 operation mode

You set BS2000 operation mode on a unit-specific basis.

### 5.1.1 Server Unit /390

► Select *Systems → <unit>(SU</390>), BS2000 operation mode* tab.



Server Unit ABGSE211: Status

|  |  |
|---|---|
| Status | ▶ RUNNING (since 2015-05-12 15:08:36) |
| Operation mode | VM2000 mode |
| Active IORSF file | 4 (SU700-6 EM-2 29001 KEIN KANAL0 14.05.2014) |

Server Unit ABGSE211: Actions

Server Unit ABGSE211: SVP console

SVP console

Server Unit ABGSE211: SVP operating

| Management Unit | Status |  |
|---|---|---|
| abgse2mu1 | ACTIVE |  |
| abgse2mu2 | PASSIVE | 🖉 |

The *BS2000 operation mode* in the *Status* group display the operation mode set (Native BS2000 mode or VM2000 mode) and permits this setting to be changed in the *Actions* group:

*Change BS2000 operation mode*

You can change the operation mode only when no BS2000 system is active.

► In the *Actions* group click *Change BS2000 operation mode*. In the subsequent *Set BS2000 operation mode and initiate BS2000 IPL* dialog box, change the operation mode and enter the IPL parameters.

*Switching Management Unit*

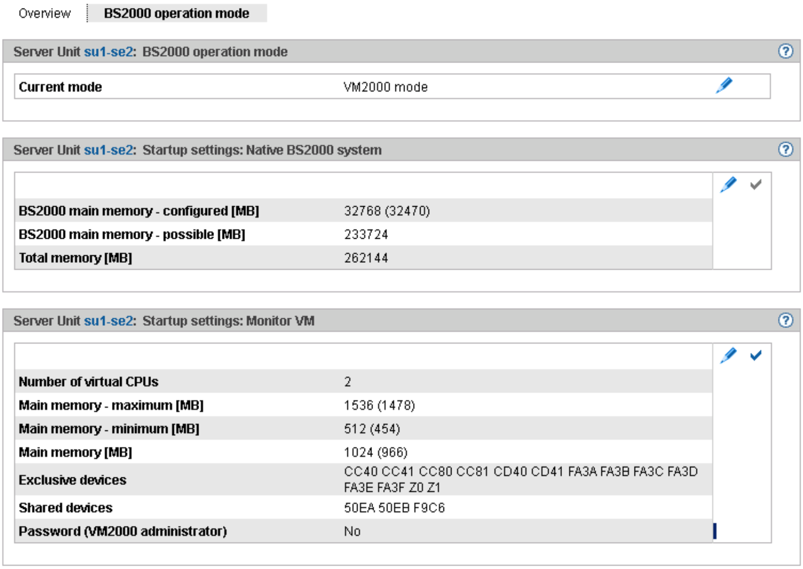
When redundant Management Units exist, they are displayed in the *SVP operating* table: An MU is always *ACTIVE* with respect to SVP operating, and the others are *PASSIVE*.

- ► By the passive MU, click the *Change* icon to switch to the other MU.

See also “Redundant Management Units” on page 46.

## 5.1.2 Server Unit x86

- ► Select *Systems → <unit>(SU<x86>), BS2000 operation mode* tab.



Server Unit su1-se2: BS2000 operation mode

| | |
|---|---|
| Current mode | VM2000 mode |

Server Unit su1-se2: Startup settings: Native BS2000 system

| | |
|---|---|
| BS2000 main memory - configured [MB] | 32768 (32470) |
| BS2000 main memory - possible [MB] | 233724 |
| Total memory [MB] | 262144 |

Server Unit su1-se2: Startup settings: Monitor VM

| | |
|---|---|
| Number of virtual CPUs | 2 |
| Main memory - maximum [MB] | 1536 (1478) |
| Main memory - minimum [MB] | 512 (454) |
| Main memory [MB] | 1024 (966) |
| Exclusive devices | CC40 CC41 CC80 CC81 CD40 CD41 FA3A FA3B FA3C FA3D FA3E FA3F Z0 Z1 |
| Shared devices | 50EA 50EB F9C6 |
| Password (VM2000 administrator) | No |

The *BS2000 operation mode* tab in the *BS2000 operation mode* group displays the operation mode set (Native BS2000 mode or VM2000 mode) and permits this setting to be changed:

*Changing the operation mode*

You can change the operation mode only when BS2000 is not active or is running in Native mode.

- ► Click the *Change* icon and confirm the switch to the other operation mode.

i When you switch mode, the Automatic IPL option is implicitly set to No. This setting can be changed again after the operation mode has been changed successfully (*Options* or *VM options* tab).

The groups below show the current startup settings for the operation mode concerned.

- ► To change the main memory size for the Native BS2000 system, click the Change icon in the *Startup settings for Native BS2000 system* group.

► To change the number of virtual CPUs, the main memory settings, the device lists or the access password for the monitor VM, click the Change icon in the *Startup settings for monitor VM* group.

Changes will take effect only after the setting has been enabled by enabling the icon in the group concerned or after you have switched the operation mode.

## 5.2 Opening the BS2000 console and dialog window

The BS2000 console and dialog window is opened using the *Operation* tab.

- Open the *Operation* tab. Depending on the mode in which BS2000 is running (Native/VM2000) and on the SU type on which it resides (SU /390 or SU x86), you reach the tab as follows:
  - Native BS2000: Select *Systems → <unit>(SU<model>) → BS2000* , *Operation* tab.
  - VM2000 on SU /390: Select *Systems → <unit>(SU</390>) → Virtual machines → <bs2000-vm>*, *Operation* tab.
  - VM2000 on SU x86: Select *Systems → <unit>(SU<x86>) → Virtual machines → BS2000 → <bs2000-vm>*, *Operation* tab.
- In the *Console and dialog* group, click *Open* by the required function (*BS2000 console* or *BS2000 dialog*).

  The BS2000 console window or BS2000 dialog window opens.

### Messages on the BS2000 console

The base system M2000 or X2000 issues messages on the BS2000 console. On an SU /390 these messages are issued by the M2000 of the MU, and on an SU x86 by the X2000 of the SU. With the exception of the messages for write operations to CDROM/DVD, these messages are not issued via the BS2000 system component MIP (Message Improvement Processing) and are therefore not stored in a BS2000 message file.

Specifically, M2000/X2000 issues messages of the following message classes on the BS2000 console:

| Message class | Meaning |
|---|---|
| KVP | Messages of the console distribution program (KVP) |
| SVR | Messages of the SVP emulation (to SU x86 only) |
| IOD | Messages of the I/O handler for bus devices (to SU x86 only) |
| HAL | Messages of the Hardware Abstraction Layer (to SU x86 only) |
| SNX | Messages for write operations to CDROM/DVD CDROM/DVD (SNXCDxx) or messages relating to a fault in a peripheral component which cannot be reported via an I/O to BS2000. |

In BS2000 OSD/BC V10.0 and higher, you can inquire response and any meaning texts for messages of M2000/X2000 using the HTML application "System messages" (online at *http://manuals.ts.fujitsu.com* or on the "BS2000 SoftBooks" DVD).

i In BS2000 you can only inquire the message text, meaning and response text for a message code with the HELP-MSG-INFORMATION command only if the message is stored in a BS2000 message file.

## 5.3 SVP console on Server Unit /390

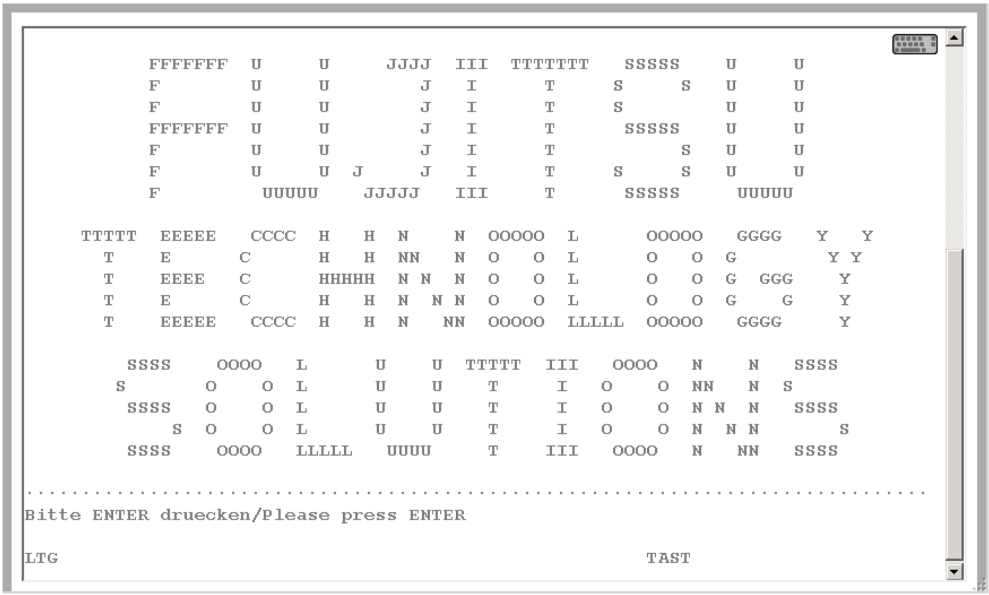
A Server Unit /390 is operated via the SVP (service processor). Some important SVP functions, for instance for IPL or IORSF, are also available directly on the SE Manager.

Alternatively, SVP functions can be called under menu control on an SVP console via SVP frames. The SVP console is accessed via the SE Manager:

► Select *Systems → <unit>(SU</390>), BS2000 operation mode* tab.

► In the *SVP console* group click *Open*.

The SVP console window opens.



```
           FFFFFFF  U     U     JJJJ  III  TTTTTTT   SSSSS    U     U
           F        U     U        J   I      T     S     S   U     U
           F        U     U        J   I      T     S         U     U
           FFFFFFF  U     U        J   I      T      SSSSS    U     U
           F        U     U        J   I      T           S   U     U
           F        U     U  J     J   I      T     S     S   U     U
           F         UUUUU    JJJJJ   III     T      SSSSS    UUUUU

     TTTTT  EEEEE   CCCC  H   H  N    N  OOOOO  L      OOOOO   GGGG   Y   Y
       T    E      C      H   H  NN   N  O   O  L      O   O  G        Y Y
       T    EEEE   C      HHHHH  N N  N  O   O  L      O   O  G  GGG    Y
       T    E      C      H   H  N  N N  O   O  L      O   O  G    G    Y
       T    EEEEE   CCCC  H   H  N   NN  OOOOO  LLLLL  OOOOO   GGGG     Y

         SSSS    OOOO   L      U    U  TTTTT  III   OOOO   N    N   SSSS
        S       O    O  L      U    U    T     I   O    O  NN   N  S
         SSSS   O    O  L      U    U    T     I   O    O  N N  N   SSSS
             S  O    O  L      U    U    T     I   O    O  N  N N       S
         SSSS    OOOO   LLLLL   UUUU     T    III   OOOO   N   NN   SSSS

................................................................................
Bitte ENTER druecken/Please press ENTER

LTG                                                    TAST
```

You can operate the SVP console in the familiar manner. A detailed description of how to operate the SVP is provided in the "Server Unit /390" Operating Manual [2].

## 5.4 Working in Native BS2000 mode

You can perform the following actions in Native BS2000 mode:

- Starting (IPL) and shutting down a BS2000 system, executing an IPL dump
- Setting options
- Evaluating KVP logging

### 5.4.1 Starting (IPL) and shutting down a BS2000 system, executing an IPL dump

You perform these actions with the *Operation* tab of the BS2000 system:

► Select *Systems* → *<unit>(SU<model>)* → *BS2000, Operation* tab.

In the *Actions* group you can select one of the following actions:

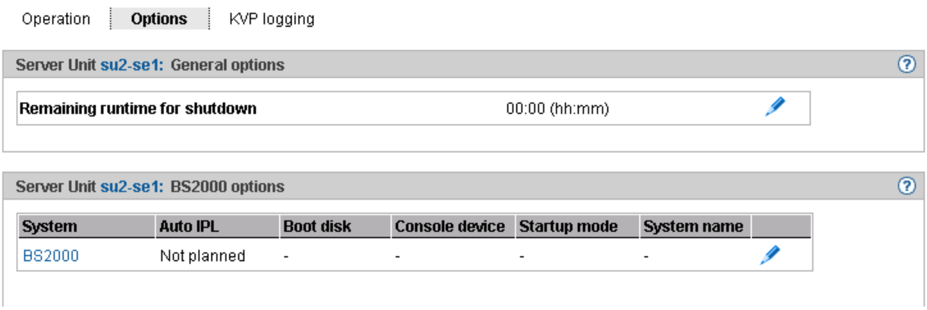
- BS2000 shutdown (only for SU x86)
- BS2000 IPL
- BS2000 dump IPL

### 5.4.2 Setting options

You manage the options using the *Options* tab of the BS2000 system. You can set startup and auto IPL.

On an SU x86 you can also change the remaining runtime for the shutdown.

► Select *Systems* → *<unit>(SU<model>)* → *BS2000, Options* tab.



Server Unit su2-se1: General options

| | |
|---|---|
| **Remaining runtime for shutdown** | 00:00 (hh:mm) |

Server Unit su2-se1: BS2000 options

| System | Auto IPL | Boot disk | Console device | Startup mode | System name |
|---|---|---|---|---|---|
| BS2000 | Not planned | - | - | - | - |

The *Options* tab displays the *General options* (only for SU x86) and *BS2000 options* groups and offers the following functionality:

*Defining the remaining runtime for the shutdown (only for Server Unit x86)*

The remaining runtime is the time which is available to BS2000 to terminate itself when the Server Unit is shut down. The remaining runtime is only of any significance when the SU is shut down or restarted. BS2000 receives a shutdown request which is handled in accordance with the setting in the system parameter SHUTPROC (see the “System Administration” manual [9]). The configured remaining runtime is then available for the BS2000 shutdown. You define the remaining runtime for BS2000 in Native mode or in VM2000 mode for the monitor system. In VM2000 mode the remaining runtime defined then applies for all BS2000 guest systems (see section “Setting VM options” on page 107).

If you enter the value 00:00, there is no defined remaining runtime, i.e. when the SU is powered off or restarted, the system always waits for BS2000 to shut down.

► In the *General options* group click *Change* and set the required remaining runtime.

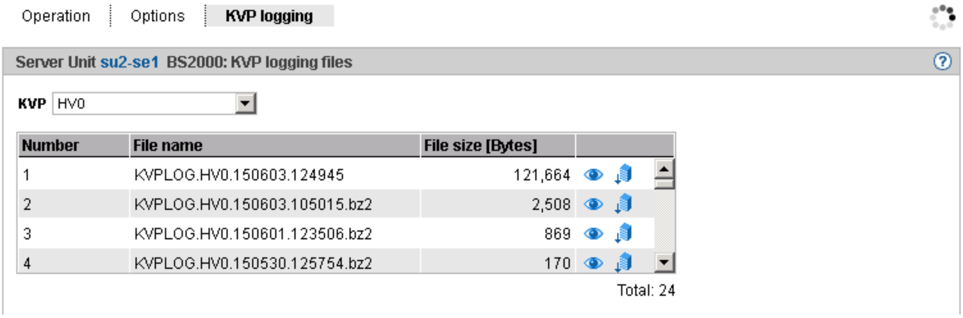
*Setting BS2000 options (startup and auto IPL)*

► In the *BS2000 options* group click *Change* and set the required values.

### 5.4.3 Evaluating KVP logging

You manage KVP logging using the *KVP logging* tab of the BS2000 system. You can select and display logging entries specifically using a subsequent dialog.

► Select *Systems* → *<unit>(SU<model>)* → *BS2000*, *KVP logging* tab.



Server Unit su2-se1 BS2000: KVP logging files

KVP HV0

| Number | File name | File size [Bytes] | |
|---|---|---|---|
| 1 | KVPLOG.HV0.150603.124945 | 121,664 | |
| 2 | KVPLOG.HV0.150603.105015.bz2 | 2,508 | |
| 3 | KVPLOG.HV0.150601.123506.bz2 | 869 | |
| 4 | KVPLOG.HV0.150530.125754.bz2 | 170 | |

Total: 24

The *KVP logging* tab displays the list of KVP logging files and offers the following options:

*Displaying KVP logging file selectively*

- ► In the *KVP logging* group select the required KVP from the *KVP* list.

  The KVP logging files which exist for this KVP are listed. The *Display* icon opens the *Display KVP logging file selectively* dialog box in which you can define the view of the content of the KVPLOG file to be displayed.

  The logging records are displayed in a separate window.

*Downloading the KVP logging file*

- ► In the *KVP logging* group select the required KVP from the *KVP* list. Click the *Download* icon by the required KVP logging file. Enter the path and file names in the system-specific Explorer window and save the file.

# 5.5 Working in VM2000 mode

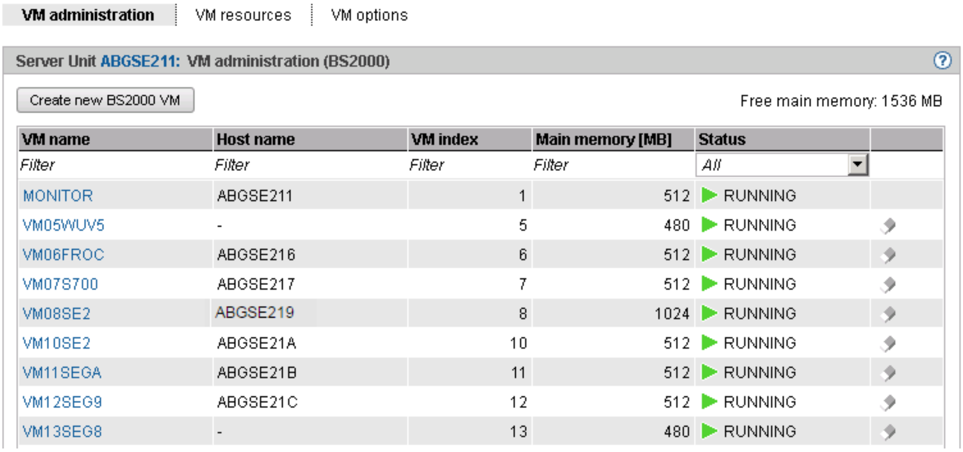
You manage the BS2000 VMs of a Server Unit using the menu item *Virtual machines* (SU /390) or *Virtual machines* → *BS2000* (SU x86).

For an SU /390, the VM2000 management by SE Manager is only possible when the REWAS is active, see also section “Integration of BS2000 into the SE Manager” on page 36.

## 5.5.1 VM administration

You manage the BS2000 VMs using the *VM administration* tab. You can create and delete BS2000 VMs.

► In the tree structure select
*Systems* → *<unit>(SU</390>)* → *Virtual machines, VM administration* tab
or
*Systems* → *<unit>(SU<x86>)* → *Virtual machines* → *BS2000, VM administration* tab.



Server Unit ABGSE211: VM administration (BS2000)

Free main memory: 1536 MB

| VM name | Host name | VM index | Main memory [MB] | Status | |
|---|---|---|---|---|---|
| Filter | Filter | Filter | Filter | All | |
| MONITOR | ABGSE211 | 1 | 512 | ▶ RUNNING | |
| VM05WUV5 | - | 5 | 480 | ▶ RUNNING | |
| VM06FROC | ABGSE216 | 6 | 512 | ▶ RUNNING | |
| VM07S700 | ABGSE217 | 7 | 512 | ▶ RUNNING | |
| VM08SE2 | ABGSE219 | 8 | 1024 | ▶ RUNNING | |
| VM10SE2 | ABGSE21A | 10 | 512 | ▶ RUNNING | |
| VM11SEGA | ABGSE21B | 11 | 512 | ▶ RUNNING | |
| VM12SEG9 | ABGSE21C | 12 | 512 | ▶ RUNNING | |
| VM13SEG8 | - | 13 | 480 | ▶ RUNNING | |

The *VM administration* tab displays the list of all the unit's BS2000 VMs.

The following functions are available:

*Creating a BS2000 VM*

► On the *VM administration* tab click *Create new BS2000 VM*.

In the *Create new BS2000 VM* wizard you can specify the required properties of the BS2000 VM step by step.

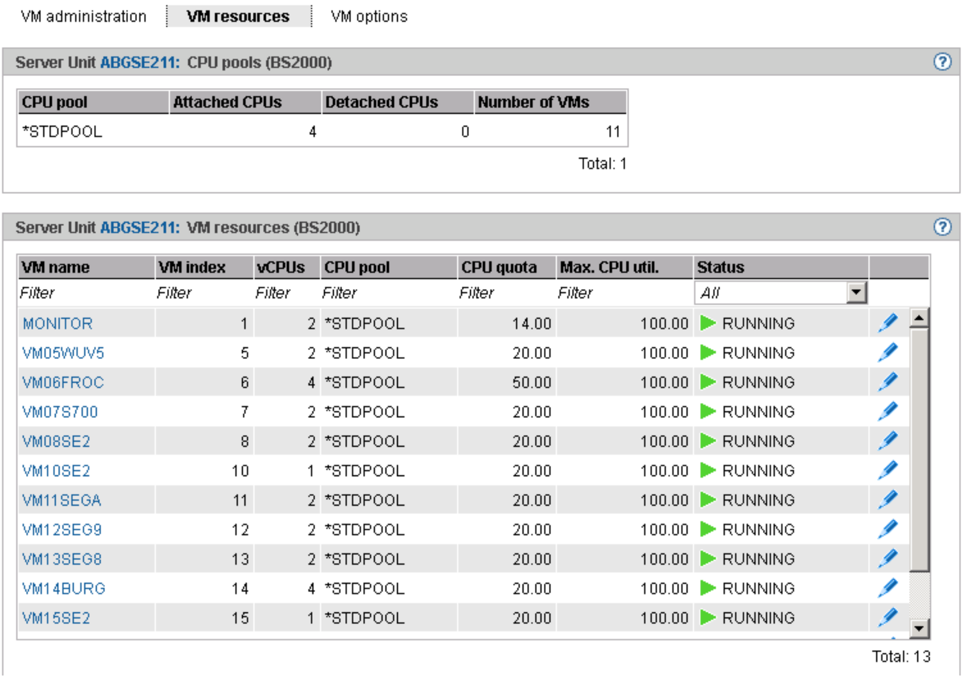
*Deleting a BS2000 VM*

- ► By the required VM click the *Delete* icon and confirm the action.

## 5.5.2 Managing VM resources

You manage the VM resources of the BS2000 VMs using the *VM resources* tab. You can change the resources of a BS2000 VM.

- ► In the tree structure select
  *Systems → <unit>(SU</390>) → Virtual machines, VM resources* tab
  or
  *Systems → <unit>(SU<x86>) → Virtual machines → BS2000, VM resources* tab.



Server Unit ABGSE211: CPU pools (BS2000)

| CPU pool | Attached CPUs | Detached CPUs | Number of VMs |
|---|---|---|---|
| *STDPOOL | 4 | 0 | 11 |

Total: 1

Server Unit ABGSE211: VM resources (BS2000)

| VM name | VM index | vCPUs | CPU pool | CPU quota | Max. CPU util. | Status |
|---|---|---|---|---|---|---|
| Filter | Filter | Filter | Filter | Filter | Filter | All |
| MONITOR | 1 | 2 | *STDPOOL | 14.00 | 100.00 | ▶ RUNNING |
| VM05WUV5 | 5 | 2 | *STDPOOL | 20.00 | 100.00 | ▶ RUNNING |
| VM06FROC | 6 | 4 | *STDPOOL | 50.00 | 100.00 | ▶ RUNNING |
| VM07S700 | 7 | 2 | *STDPOOL | 20.00 | 100.00 | ▶ RUNNING |
| VM08SE2 | 8 | 2 | *STDPOOL | 20.00 | 100.00 | ▶ RUNNING |
| VM10SE2 | 10 | 1 | *STDPOOL | 20.00 | 100.00 | ▶ RUNNING |
| VM11SEGA | 11 | 2 | *STDPOOL | 20.00 | 100.00 | ▶ RUNNING |
| VM12SEG9 | 12 | 2 | *STDPOOL | 20.00 | 100.00 | ▶ RUNNING |
| VM13SEG8 | 13 | 2 | *STDPOOL | 20.00 | 100.00 | ▶ RUNNING |
| VM14BURG | 14 | 4 | *STDPOOL | 20.00 | 100.00 | ▶ RUNNING |
| VM15SE2 | 15 | 1 | *STDPOOL | 20.00 | 100.00 | ▶ RUNNING |

Total: 13

The *VM resources* tab provides information on the use of the CPU pools and displays the list of BS2000 VMs with the VM resources. The following function is available:

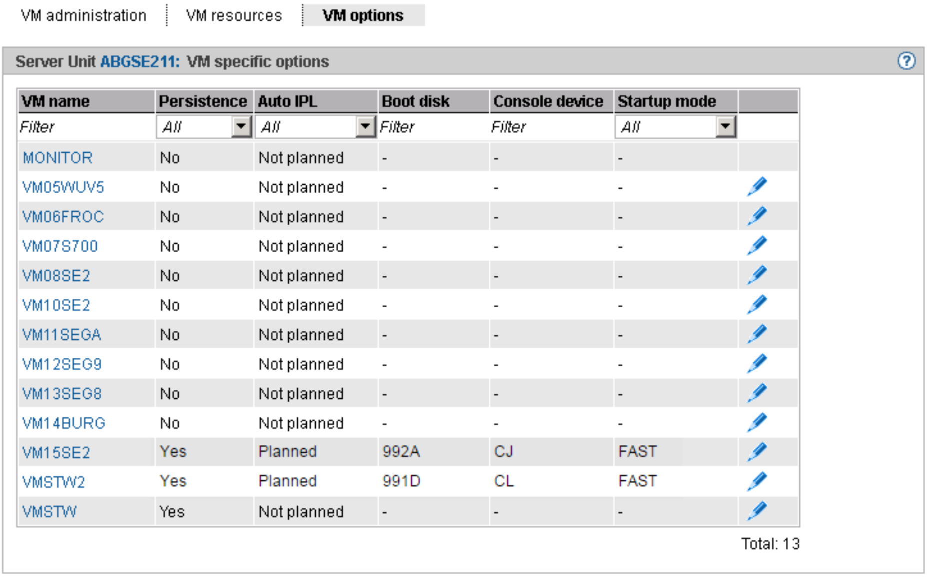
*Changing resources of a BS2000 VM*

- ► By the required BS2000 VM click the *Change* icon and make the requisite changes in the *Change resources* dialog box.

### 5.5.3 Setting VM options

You manage the VM resources of the various BS2000 VMs using the *VM options* tab. You can change VM-specific options, and you can also change the settings for persistence and automatic IPL for the monitor VM and persistent BS2000 VMs.
On an SU x86 you can also set the remaining runtime for the shutdown.

► In the tree structure select
*Systems → <unit>(SU</390>) → Virtual machines, VM options* tab
or
*Systems → <unit>(SU<x86>) → Virtual machines → BS2000, VM options* tab.



Server Unit ABGSE211: VM specific options

| VM name | Persistence | Auto IPL | Boot disk | Console device | Startup mode | |
|---|---|---|---|---|---|---|
| Filter | All | All | Filter | Filter | All | |
| MONITOR | No | Not planned | - | - | - | |
| VM05WUV5 | No | Not planned | - | - | - | ✎ |
| VM06FROC | No | Not planned | - | - | - | ✎ |
| VM07S700 | No | Not planned | - | - | - | ✎ |
| VM08SE2 | No | Not planned | - | - | - | ✎ |
| VM10SE2 | No | Not planned | - | - | - | ✎ |
| VM11SEGA | No | Not planned | - | - | - | ✎ |
| VM12SEG9 | No | Not planned | - | - | - | ✎ |
| VM13SEG8 | No | Not planned | - | - | - | ✎ |
| VM14BURG | No | Not planned | - | - | - | ✎ |
| VM15SE2 | Yes | Planned | 992A | CJ | FAST | ✎ |
| VMSTW2 | Yes | Planned | 991D | CL | FAST | ✎ |
| VMSTW | Yes | Not planned | - | - | - | ✎ |

Total: 13

The *VM options* tab displays the settings of the VMs in the *VM-specific options* group. For an SU x86 (see figure) the *General options* group with the remaining runtime for the shutdown is displayed beforehand.

The following functions are available:

*Setting VM-specific options (persistence, startup, and auto IPL)*

► In the *VM-specific options* group click the *Change* icon by the required VM and make the requisite changes in the *Change VM-specific options* dialog box.

*Defining the remaining runtime for the shutdown (only for Server Unit x86)*

The remaining runtime is the time which is available to BS2000 to terminate itself when the Server Unit is shut down. The remaining runtime is only of any significance when the SU is shut down or restarted. BS2000 receives a shutdown request which is handled in accordance with the setting in the system parameter SHUTPROC (see the “System Administration” manual [9]). In VM2000 mode first the guest systems receive the termination signal. When all guest systems have shut down or half the remaining runtime has elapsed, the monitor system receives the termination signal. If guest systems have not yet shut down, they are now subjected to hard termination by the monitor system. If the monitor system has shut down or at the latest at the end of the remaining runtime, X2000 is terminated. For the setting for the remaining runtime for Native mode, see section “Setting options” on page 102.

If you enter the value 00:00, there is no defined remaining runtime, i.e. when the SU is powered off or restarted, the system always waits for the monitor system to shut down.

► In the *General options* group click *Change* and set the required remaining runtime in the *Change remaining runtime for shutdown* dialog box.

## 5.5.4 Operating a VM

As soon as a BS2000 VM has been created, the tree structure is extended by a VM-specific menu *<bs2000-vm>:*

*Systems → <unit>(SU</390>) → Virtual machines → <bs2000-vm>*

or

*<unit >(SU<x86>) → Virtual machines → BS2000 → <bs2000-vm>*

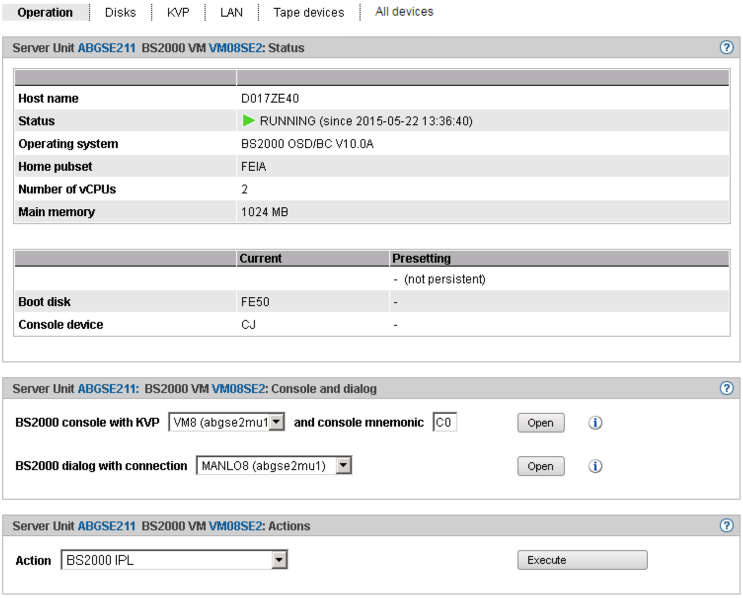
In the menu the functions are assigned to tabs according to topics.

You can:

- Start and shut down a BS2000 guest system, create a dump / enable and disable (and delete) a BS2000 VM
- Managing devices of the VM

### 5.5.4.1 Start and shut down a BS2000 guest system, create a dump / enable and disable (and delete) a BS2000 VM

► Select:
*Systems → <unit>(SU</390>) → Virtual machines → <bs2000-vm>*, *Operation* tab
or
*Systems → <unit>(SU<x86>) → Virtual machines → BS2000 → <bs2000-vm>*, *Operation* tab.



Server Unit ABGSE211 BS2000 VM VM08SE2: Status

| | |
|---|---|
| Host name | D017ZE40 |
| Status | ▶ RUNNING (since 2015-05-22 13:36:40) |
| Operating system | BS2000 OSD/BC V10.0A |
| Home pubset | FEIA |
| Number of vCPUs | 2 |
| Main memory | 1024 MB |

| | Current | Presetting |
|---|---|---|
| | | - (not persistent) |
| Boot disk | FE50 | - |
| Console device | CJ | - |

Server Unit ABGSE211: BS2000 VM VM08SE2: Console and dialog

BS2000 console with KVP VM8 (abgse2mu1 and console mnemonic C0

BS2000 dialog with connection MANLO8 (abgse2mu1)

Server Unit ABGSE211 BS2000 VM VM08SE2: Actions

Action BS2000 IPL

The *Operation* tab displays the status of the VM, offers access to the BS2000 console and dialog box, and enables the following actions:

- BS2000 IPL
- BS2000 dump IPL
- BS2000 shutdown (on the monitor VM)
- BS2000 VM activation (persistent VMs only)
- BS2000 VM deactivation (persistent VMs only)
- BS2000 VM activation and deletion (only non-persistent VMs except the monitor VM)

The description of the BS2000 console window and dialog is provided in section “Opening the BS2000 console and dialog window” on page 99.

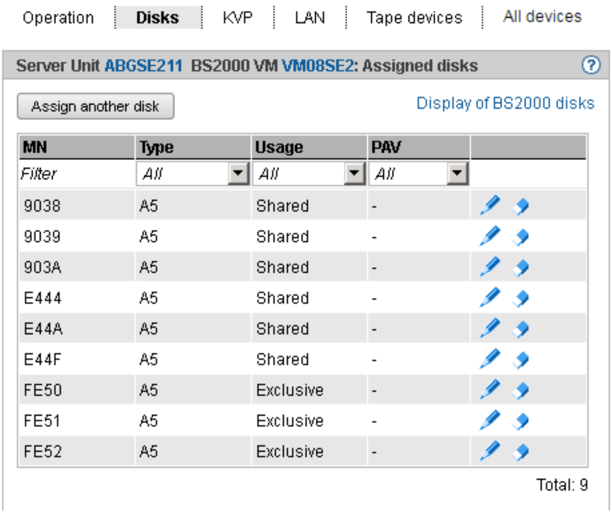
### 5.5.4.2 Managing devices of the VM

- ▶ Select:
  *Systems → <unit>(SU</390>) → Virtual machines → <bs2000-vm>*, *Disks*, *KVP*, *LAN*, *Tape devices* or *All devices* tab
  or
  *Systems → <unit>(SU<x86>) → Virtual machines → BS2000 → <bs2000-vm>*, *Disks*, *KVP*, *LAN*, *Tape devices* or *All devices* tab.

#### Disks tab

This tab enables you to assign disks to or remove disks from a BS2000 VM or to change its usage.

The *Disks* tab displays all disks which are assigned to the BS2000 VM.



Server Unit ABGSE211 BS2000 VM VM08SE2: Assigned disks

| MN | Type | Usage | PAV | |
|---|---|---|---|---|
| Filter | All | All | All | |
| 9038 | A5 | Shared | - | ✎ ⬥ |
| 9039 | A5 | Shared | - | ✎ ⬥ |
| 903A | A5 | Shared | - | ✎ ⬥ |
| E444 | A5 | Shared | - | ✎ ⬥ |
| E44A | A5 | Shared | - | ✎ ⬥ |
| E44F | A5 | Shared | - | ✎ ⬥ |
| FE50 | A5 | Exclusive | - | ✎ ⬥ |
| FE51 | A5 | Exclusive | - | ✎ ⬥ |
| FE52 | A5 | Exclusive | - | ✎ ⬥ |

Total: 9

i The *PAV* column is displayed only for SU /390.

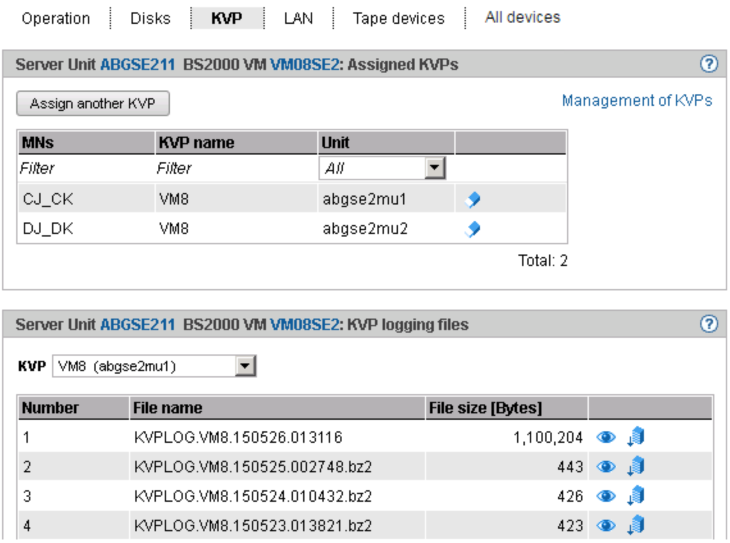
- ▶ Click *Assign another disk* to assign another disk individually to the VM.
- ▶ Click the *Change* icon by a disk to change the usage of this disk (Shared/Exclusive).
- ▶ Click the *Withdraw* icon by a disk to withdraw this disk from the VM.

For further information on displaying BS2000 disks, see section “Displaying generated disks on Server Unit /390” on page 159 and section “Managing disks on Server Unit x86” on page 160.

### KVP tab

This tab enables you to assign further KVPs to the BS2000 VM or to display KVP logging files.

The *KVP* tab lists all assigned KVPs and all KVP logging files.



Server Unit ABGSE211 BS2000 VM VM08SE2: Assigned KVPs

| MNs | KVP name | Unit | |
|---|---|---|---|
| Filter | Filter | All | |
| CJ_CK | VM8 | abgse2mu1 | |
| DJ_DK | VM8 | abgse2mu2 | |

Total: 2

Server Unit ABGSE211 BS2000 VM VM08SE2: KVP logging files

KVP VM8 (abgse2mu1)

| Number | File name | File size [Bytes] | |
|---|---|---|---|
| 1 | KVPLOG.VM8.150526.013116 | 1,100,204 | |
| 2 | KVPLOG.VM8.150525.002748.bz2 | 443 | |
| 3 | KVPLOG.VM8.150524.010432.bz2 | 426 | |
| 4 | KVPLOG.VM8.150523.013821.bz2 | 423 | |

*Assigning a KVP*

- In the *Assigned KVPs* group click *Assign another KVP* and select a KVP in the subsequent dialog box.

*Withdrawing a KVP*

- In the *AssignedKVPs* group click the *Withdraw* icon by a KVP and confirm the action.

*Displaying KVP logging file selectively*

- In the *KVP logging files* group select the required KVP from the *KVP* list.

  The KVP logging files which exist for this KVP are listed. The *Display* icon opens the *Display KVP logging file selectively* dialog box in which you can define the view of the content of the KVPLOG file to be displayed.

  The logging records are displayed in a separate window.

*Downloading the KVP logging file*

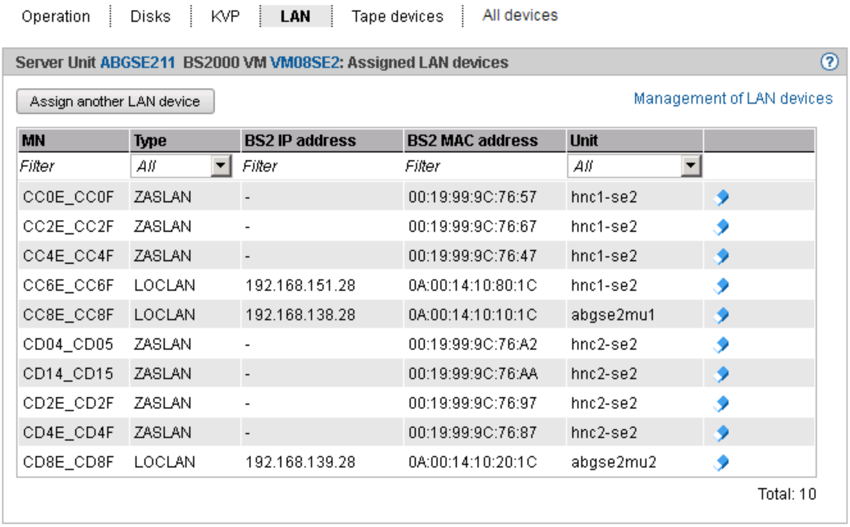
- In the *KVP logging files* group select the required KVP from the *KVP* list. Click the *Download* icon by the required KVP logging file, enter the path name and file name in the system-specific Explorer window, and save the file.

Further details on KVPs are contained in the section “Managing KVP devices” on page 162.

### LAN tab

This tab enables you to assign further LAN devices (as a device pair) to the BS2000 VM or to remove LAN devices from it.

The *LAN* tab lists all LAN device which are assigned to the BS2000 VM.



Server Unit ABGSE211 BS2000 VM VM08SE2: Assigned LAN devices

| MN | Type | BS2 IP address | BS2 MAC address | Unit | |
|---|---|---|---|---|---|
| Filter | All | Filter | Filter | All | |
| CC0E_CC0F | ZASLAN | - | 00:19:99:9C:76:57 | hnc1-se2 | |
| CC2E_CC2F | ZASLAN | - | 00:19:99:9C:76:67 | hnc1-se2 | |
| CC4E_CC4F | ZASLAN | - | 00:19:99:9C:76:47 | hnc1-se2 | |
| CC6E_CC6F | LOCLAN | 192.168.151.28 | 0A:00:14:10:80:1C | hnc1-se2 | |
| CC8E_CC8F | LOCLAN | 192.168.138.28 | 0A:00:14:10:10:1C | abgse2mu1 | |
| CD04_CD05 | ZASLAN | - | 00:19:99:9C:76:A2 | hnc2-se2 | |
| CD14_CD15 | ZASLAN | - | 00:19:99:9C:76:AA | hnc2-se2 | |
| CD2E_CD2F | ZASLAN | - | 00:19:99:9C:76:97 | hnc2-se2 | |
| CD4E_CD4F | ZASLAN | - | 00:19:99:9C:76:87 | hnc2-se2 | |
| CD8E_CD8F | LOCLAN | 192.168.139.28 | 0A:00:14:10:20:1C | abgse2mu2 | |

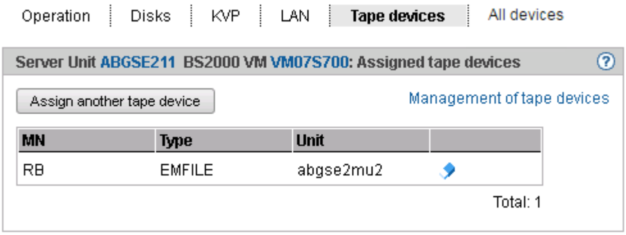
Total: 10

- Click *Assign another LAN device* to assign another LAN device pair to the VM.
- Click the *Remove* icon by a LAN device to remove the LAN device from the VM.
- Click *Management of LAN devices* to branch to the hardware device management, see section “Managing LAN devices” on page 166.

### Tape devices tab

This tab enables you to assign further tape devices individually to the BS2000 VM or to remove tape devices from it.

The *Tape device* tab lists all tape device which are assigned to the BS2000 VM.



Server Unit ABGSE211 BS2000 VM VM07S700: Assigned tape devices

| MN | Type | Unit | |
|---|---|---|---|
| RB | EMFILE | abgse2mu2 | |

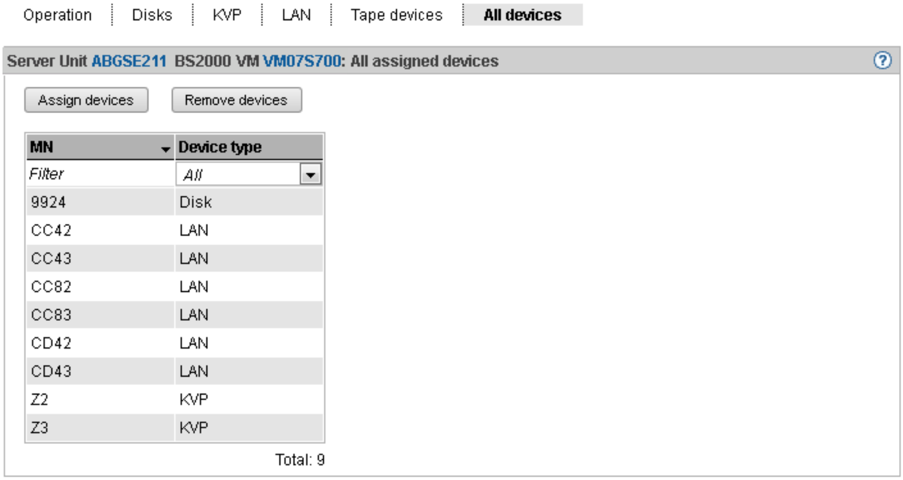
Total: 1

- ► Click *Assign another tape device* to assign another tape device individually to the BS2000 VM.
- ► Click the *Remove* icon by a tape device to remove the tape device from the BS2000 VM.
- ► Click *Management of tape devices* to branch to the hardware device management, see section “Managing tape devices” on page 168.

### *All devices* tab

This tab enables you to assign or remove further BS2000 devices to or from the BS2000 VM on a cross-type basis. In other words the assignment or removal applies for sets of devices which are defined via MN lists, MN areas or MNs with wildcards.

The *All devices* tab lists all BS2000 device which are currently assigned to the BS2000 VM.



Server Unit ABGSE211 BS2000 VM VM07S700: All assigned devices

| MN | Device type |
|---|---|
| *Filter* | *All* |
| 9924 | Disk |
| CC42 | LAN |
| CC43 | LAN |
| CC82 | LAN |
| CC83 | LAN |
| CD42 | LAN |
| CD43 | LAN |
| Z2 | KVP |
| Z3 | KVP |

Total: 9

The device mnemonic and the device type are displayed for each assigned BS2000 device.

- ► Click *Assign devices* to start the *Assign BS2000 devices* wizard. The wizard enables you to assign multiple BS2000 devices to the BS2000 VM on a cross-type basis.
- ► Click *Remove devices* to open the *Remove BS2000 devices* dialog box. There you can remove devices from the VM on a cross-type basis.

Wildcards and range specifications are possible when you specify the devices.

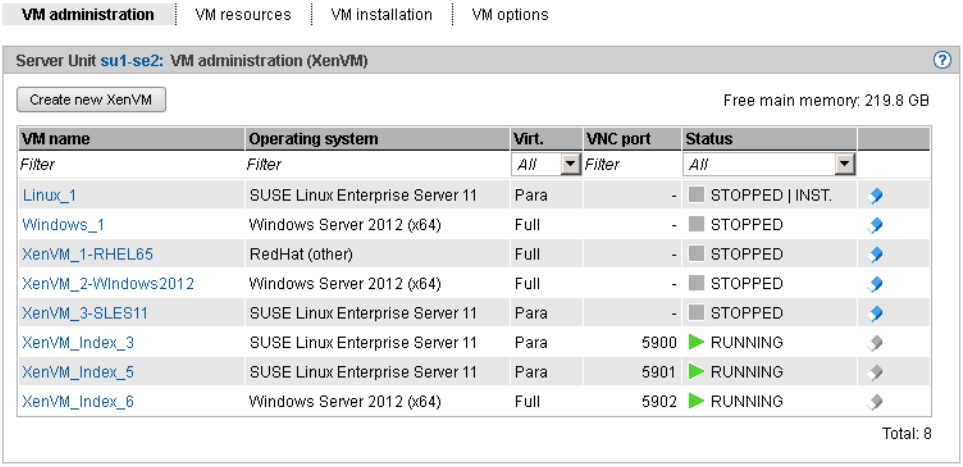
## 5.6 Working in XenVM mode (on Server Unit x86)

You manage the XenVMs of a Server Unit x86 using the menu item *Virtual machines* → *XenVM*.

### 5.6.1 VM administration

The *VM administration* tab displays an overview of the existing XenVMs and enables you to create or delete XenVMs.

► Select *Systems* → *<unit> (SU<x86>)* → *Virtual machines* → *XenVM*, *VM administration* tab.



**VM administration** | VM resources | VM installation | VM options

**Server Unit su1-se2: VM administration (XenVM)**

Create new XenVM

Free main memory: 219.8 GB

| VM name | Operating system | Virt. | VNC port | Status | |
|---|---|---|---|---|---|
| *Filter* | *Filter* | *All* | *Filter* | *All* | |
| Linux_1 | SUSE Linux Enterprise Server 11 | Para | - | ■ STOPPED \| INST. | |
| Windows_1 | Windows Server 2012 (x64) | Full | - | ■ STOPPED | |
| XenVM_1-RHEL65 | RedHat (other) | Full | - | ■ STOPPED | |
| XenVM_2-WIndows2012 | Windows Server 2012 (x64) | Full | - | ■ STOPPED | |
| XenVM_3-SLES11 | SUSE Linux Enterprise Server 11 | Para | - | ■ STOPPED | |
| XenVM_Index_3 | SUSE Linux Enterprise Server 11 | Para | 5900 | ▶ RUNNING | |
| XenVM_Index_5 | SUSE Linux Enterprise Server 11 | Para | 5901 | ▶ RUNNING | |
| XenVM_Index_6 | Windows Server 2012 (x64) | Full | 5902 | ▶ RUNNING | |

Total: 8

The *VM administration* tab provides information on the XenVMs which have already been configured.

#### Create new XenVM

When a XenVM is created, not only the main memory and CPUs are configured, but also virtual devices. From the viewpoint of the guest system (Linux/Windows), these devices look like real devices. To enable the guest system to recognize and use the devices configured on the XenVM, the corresponding device drivers must be installed in the guest system.

*Requirements*

- This action is not possible if the maximum number of 64 VMs (BS2000 and XenVM) has been reached.

- Before you begin to create a XenVM, the required resources should be available. The system requirements depend on the operating system which is to be installed. You must in particular ensure that a virtual disk of a sufficient size exists or can be created so that the guest system can be installed without any problem. The Data Center Edition of Windows 2008 Server requires, for example, at least 18 GB of disk storage. Before creation begins, missing resources must be configured to offer sufficient capacity, e.g. create or extend disk pool (see section "Managing virtual disks" on page 178), upload ISO image of the required operating system to the local library as an installation source (see section "Managing installation sources" on page 182).

► Click *Create new XenVM*.

In the *Create new XenVM* wizard you can specify the required properties of the XenVM step by step.

The wizard initiates the process of VM creation in the background and, depending on the installation type, also installation and startup of the XenVM.

*Monitoring configuration of the XenVM and error handling*

When a XenVM is configured, all the resources specified in the wizard must be available at this time.

If the configured XenVM is started immediately, configuration of a XenVM is a process which can take somewhat longer depending on the resources specified (in particular main memory).

As a complete check to ensure that all the configuration data is correct and consistent only takes place in the course of this process, an error (e.g. incorrect installation source) results in the process aborting relatively quickly (aborted status on the *VM installation* tab), and no XenVM is configured. In this case the error message and error cause can be displayed directly in the dialog window.

However, it can occur that the configuration process starts normally (e.g. reaches the INSTALL status in the case of installation), but the configured XenVM is subsequently discarded (e.g. because of a memory bottleneck). In this case you will find no XenVM in the dialog window despite the supposed positive acknowledgment. If the XenVM is displayed in the navigation, you will also find the current status in the XenVM-specific *Operation* tab.

If the installation or configuration process has not reached one of the statuses ABORTED, INSTALL or FINISHED after a certain time, the monitoring function of the process is aborted with a corresponding message. You will find the current status in the logging file of the installation or configuration process (see the *VM installation* tab). If the XenVM is displayed in the navigation, you will also find the current status on the XenVM-specific *Operation* tab.

*XenVM console*

If the XenVM has been started, you can open the XenVM console. When installation takes place, you can then, for example, track the messages while the operating system is installed and answer queries, see section “Opening the console of the XenVM” on page 123.

### Deleting XenVM

This action is only available in the VM status *STOPPED*.

▶ Click on the *Delete* icon by the XenVM to be deleted, specify whether the virtual disks are also to be deleted, and confirm the action.

Depending on requirements, first the virtual disks of the XenVM are deleted. Then the XenVM is deleted.

## 5.6.2 Managing VM resources

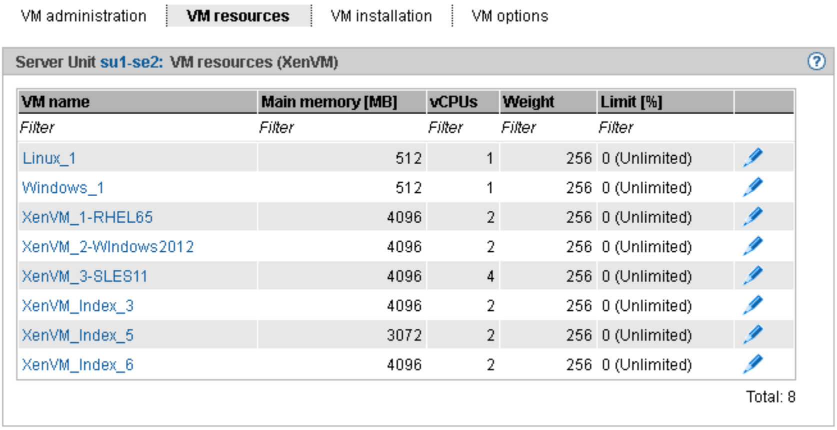
The *VM resources* tab provides an overview of the current distribution of the resources virtual CPUs and main memory. You can also change the weight and limit for a XenVM.

Detailed information on the *VM resources* tab is provided in the SE Manager help.

### Changing the weight and limit for the XenVM

► In the tree structure select *Systems → <unit> (SU<x86>) → Virtual machines → XenVM*, *VM resources* tab.

The *VM resources* tab displays the current resource distribution.



Server Unit su1-se2: VM resources (XenVM)

| VM name | Main memory [MB] | vCPUs | Weight | Limit [%] | |
|---|---|---|---|---|---|
| Filter | Filter | Filter | Filter | Filter | |
| Linux_1 | 512 | 1 | 256 | 0 (Unlimited) | ✎ |
| Windows_1 | 512 | 1 | 256 | 0 (Unlimited) | ✎ |
| XenVM_1-RHEL65 | 4096 | 2 | 256 | 0 (Unlimited) | ✎ |
| XenVM_2-WIndows2012 | 4096 | 2 | 256 | 0 (Unlimited) | ✎ |
| XenVM_3-SLES11 | 4096 | 4 | 256 | 0 (Unlimited) | ✎ |
| XenVM_Index_3 | 4096 | 2 | 256 | 0 (Unlimited) | ✎ |
| XenVM_Index_5 | 3072 | 2 | 256 | 0 (Unlimited) | ✎ |
| XenVM_Index_6 | 4096 | 2 | 256 | 0 (Unlimited) | ✎ |

Total: 8

► In the table row of the XenVM for which you wish to change the VM resources *Weight* and/or *Limit [%]* click the*Change* icon.

The *Change resources* dialog box opens.

► Change the values for *Weight* and/or *Limit [%]*.

Detailed information on these parameters is provided in the SE Manager help.

► Click *Modify* to confirm the changes.

## 5.6.3 Tracking VM installation

The operating system of the XenVM is installed from the defined installation source before the initial startup. On the *VM installation* tab you can query the status of the installation process required to do this at any time. The installation log can also be viewed at any time. This enables any errors which have occurred to be analyzed.

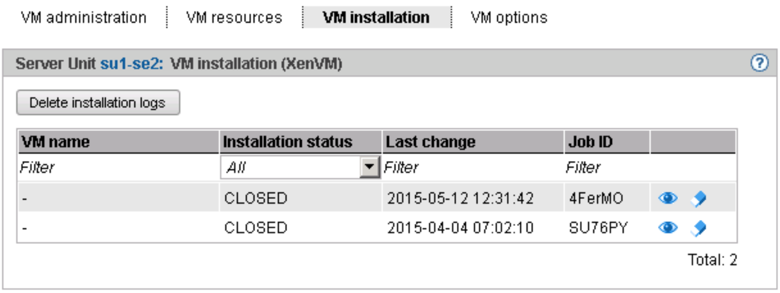
If the installation process has not yet been completed for a XenVM, this is also displayed as a supplement to the VM status in the overview of the XenVMs and in the operating menu of the XenVM

If the installation process has not yet been completed for a XenVM, this is also displayed as a supplement to the VM status in the overview of the XenVMs and on the *Operation* tab of the XenVM

Detailed information on the *VM installation* tab is provided in the SE Manager help.

► In the tree structure select *Systems* → *<unit name>(SU<x86>)* → *Virtual machines* → *XenVM*, *VM installation* tab.

The *VM installation* tab displays the XenVMs and the installation history.



VM administration | VM resources | **VM installation** | VM options

**Server Unit su1-se2: VM installation (XenVM)**

Delete installation logs

| VM name | Installation status | Last change | Job ID | |
|---|---|---|---|---|
| *Filter* | *All* | *Filter* | *Filter* | |
| - | CLOSED | 2015-05-12 12:31:42 | 4FerMO | |
| - | CLOSED | 2015-04-04 07:02:10 | SU76PY | |

Total: 2

The information displayed is described in the SE Manager help.

► Select one of the following actions for VM installation:

Detailed information on these actions is provided in the SE Manager help.

► Aborting the installation process

This action is not available for installation processes which have already been terminated (*Installation status FINISHED*, *CANCELED*, *FAILED* or *CLOSED*).

► Click the *Abort* icon to abort the installation process.

A new installation process can be started for the XenVM with *Start XenVM* (see section “Starting and shutting down the XenVM” on page 124).

- ► Displaying the installation log
  - ► Click the *Display installation log* icon to display the content of the logging file in a dialog box.
- ► Delete installation log

  This action is only possible for installation processes which have already been completed (*installation status FINISHED*, *CANCELED, FAILED* or *CLOSED*).

  - ► Click the *Delete installation log* icon to delete the log for a single installation process.
- ► Deleting more than one installation log

  This action is only possible for installation processes which have already been completed (*installation status FINISHED*, *CANCELED, FAILED* or *CLOSED*).

  - ► Click *Delete installation logs* to delete the logs of more than one installation process. The *Delete installation logs* dialog box opens.
  - ► Select installation logs to be deleted and confirm the deletion.

## 5.6.4 Setting VM options

The *VM options* tab provides the following functions:

- Display or change remaining runtime for shutdown (globally for XenVMs)
- Displays and changes the XenVMs' auto start settings

Detailed information on the *VM options* tab is provided in the SE Manager help.

### 5.6.4.1 Defining the remaining runtime for shutdown

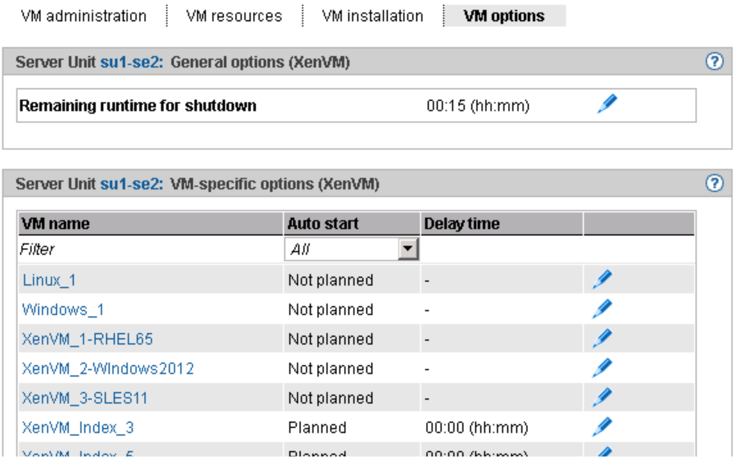
The remaining runtime is the time available to the systems on the XenVMs to shut themselves down when the Server Unit shuts down. The remaining runtime is only of any significance when the Server Unit is shut down or restarted.

You define the remaining runtime globally for all XenVMs. When the Server Unit is shut down or restarted, all XenVMs receive the termination signal to shut themselves down within the remaining runtime. After the remaining runtime has elapsed, XenVMs which are still running are forced to shut down.

The value 00:00 means that no remaining runtime is defined, i.e. in the event of a shutdown or restart the system always waits for the XenVMs to shut down. However, you are recommended to define a remaining runtime. Otherwise a guest system which encounters an error when it shuts down can prevent the Server Unit from being powered off or restarted since no hard termination takes place with a remaining runtime of 0 (the system waits until all XenVMs have terminated).

► Select *Systems* → *<unit> (SU<x86>)* → *Virtual machines* → *XenVM*, *VM options* tab.

The *VM options* tab opens. The *General options* group displays the remaining runtime for shutdown.



Server Unit su1-se2: General options (XenVM)

| | | |
|---|---|---|
| Remaining runtime for shutdown | 00:15 (hh:mm) | |

Server Unit su1-se2: VM-specific options (XenVM)

| VM name | Auto start | Delay time | |
|---|---|---|---|
| *Filter* | *All* | | |
| Linux_1 | Not planned | - | |
| Windows_1 | Not planned | - | |
| XenVM_1-RHEL65 | Not planned | - | |
| XenVM_2-Windows2012 | Not planned | - | |
| XenVM_3-SLES11 | Not planned | - | |
| XenVM_Index_3 | Planned | 00:00 (hh:mm) | |
| XenVM_Index_5 | Planned | 00:00 (hh:mm) | |

- ► In the *General options* group click the *Change* icon by the *Remaining runtime for shutdown* parameter and select the required hour and minute values.

### 5.6.4.2 Setting VM-specific options (auto start and delay)

Automatic startup (or automatic system initialization) means that the operating system of the specified XenVM is started automatically after the Server Unit has been powered on or after a restart. Whether auto start is to be possible and a possible time delay are configured separately for each XenVM

The XenVMs are started asynchronously. XenVMs with the same start time being started in any order.

- ► In the tree structure select *Systems → <unit name>(SU<x86>) → Virtual machines → XenVM*, *VM options* tab.

  The *VM-specific options* group displays a list of the created XenVMs with their names and the current auto start settings.

- ► Click the *Change* icon by the required XenVM and define the requisite auto start setting.

## 5.6.5 Operating a VM

As soon as a XenVM has been configured, the tree structure below *Systems → <unit> (SU<x86>) → Virtual machines → XenVM* is expanded by a XenVM-specific menu *<XenVM name>*. In the menu the functions are assigned to tabs according to topics.

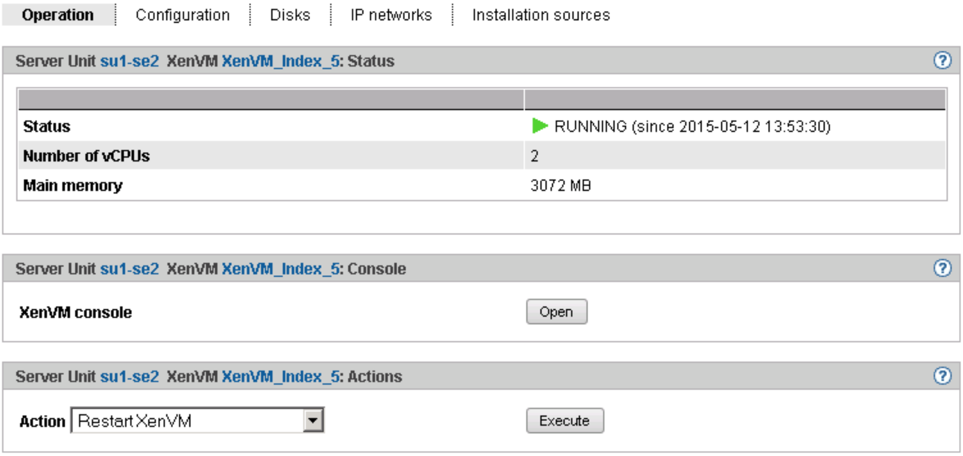
### 5.6.5.1 Displaying VM information

The *Operation* tab provides you with information on the current status of the XenVM and enables you to open the XenVM console window and various actions to operate the XenVM.

Detailed information on the *Operation* tab is provided in the SE Manager help.

► Select *Systems → <unit> (SU<x86>) → Virtual machines → XenVM → <XenVM name>*, *Operation* tab.

The *Operation* tab displays the *State*, *Console*, and *Actions* groups.



Server Unit su1-se2 XenVM XenVM_Index_5: Status

| | |
|---|---|
| Status | RUNNING (since 2015-05-12 13:53:30) |
| Number of vCPUs | 2 |
| Main memory | 3072 MB |

Server Unit su1-se2 XenVM XenVM_Index_5: Console

XenVM console Open

Server Unit su1-se2 XenVM XenVM_Index_5: Actions

Action Restart XenVM Execute

### 5.6.5.2 Opening the console of the XenVM

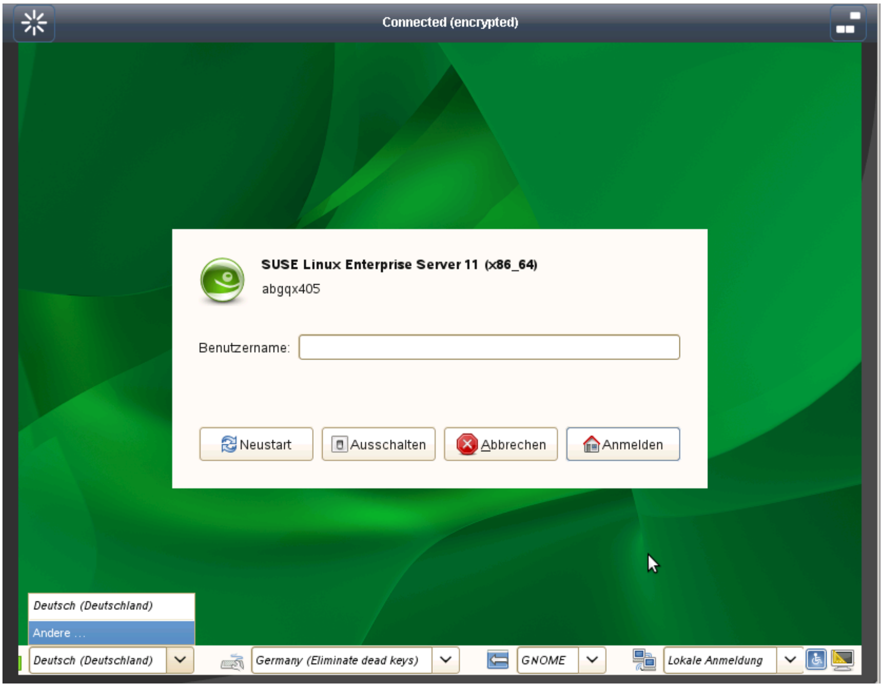
The console window can be opened at any time, i.e. irrespective of the status of the XenVM. You consequently have the option of opening the console before the XenVM is started, to observe the messages during system startup, and to diagnose any errors which may occur.

Proceed as follows to open the XenVM console using the SE Manager:

► Select *Systems → <unit> (SU<x86>) → Virtual machines → XenVM → <XenVM name>*, *Operation* tab.

- ► Click *Open* in the *Console* group.

  A dialog opens in which a VNC console is loaded as an applet. If possible, the connection to the XenVM will be established automatically.



Connected (encrypted)

SUSE Linux Enterprise Server 11 (x86_64)
abgqx405

Benutzername:

### 5.6.5.3 Starting and shutting down the XenVM

- ► Select *Systems* → *<unit> (SU<x86>)* → *Virtual machines* → *XenVM* → *<XenVM name>*, *Operation* tab.

  Depending on the current VM status, a list of actions is available to you in the *Actions* group which lead to a change in the VM status.

  – *Start XenVM*

  – *Restart XenVM*

  – *Shut down XenVM*

  – *Pause XenVM*

  – *Unpause XenVM*

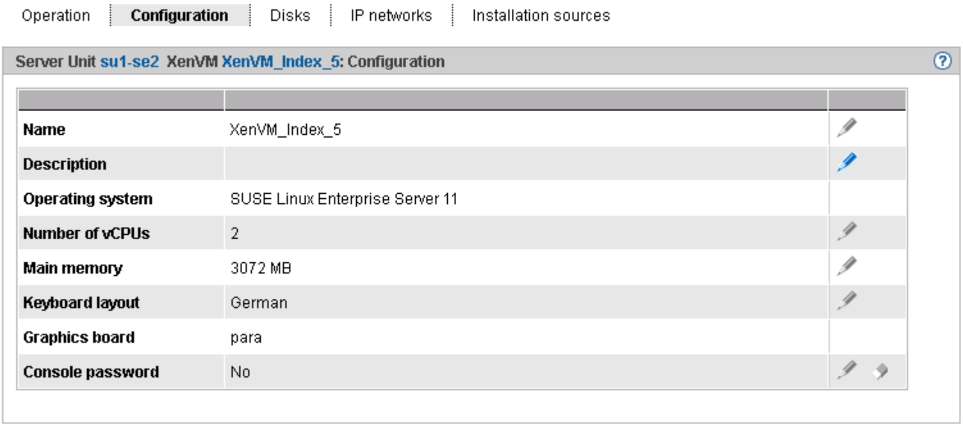
  – *Power off XenVM*

### 5.6.5.4 Changing the configuration of the XenVM

You define the configuration settings of the XenVM when you create the XenVM, see section “VM administration” on page 115. With the exception of the operating system and the graphics card, you can also alter the configuration settings later.

► In the tree structure select *Systems* → *<unit> (SU<x86>)* → *Virtual machines* → *XenVM* → *<XenVM name>*, *Configuration* tab

The *Configuration* tab displays the settings which are currently configured for the XenVM:



Server Unit su1-se2 XenVM XenVM_Index_5: Configuration

| | | |
|---|---|---|
| **Name** | XenVM_Index_5 | ✎ |
| **Description** | | ✎ |
| **Operating system** | SUSE Linux Enterprise Server 11 | |
| **Number of vCPUs** | 2 | ✎ |
| **Main memory** | 3072 MB | ✎ |
| **Keyboard layout** | German | ✎ |
| **Graphics board** | para | |
| **Console password** | No | ✎ |

The information displayed is described in the SE Manager help.

► In the list click on the *Change* icon by the setting which you wish to change.

A dialog box for changing the configuration setting opens.

### 5.6.5.5 Managing devices of the XenVM

When they are created, XenVMs are already assigned a minimum basic configuration of XenVM devices:

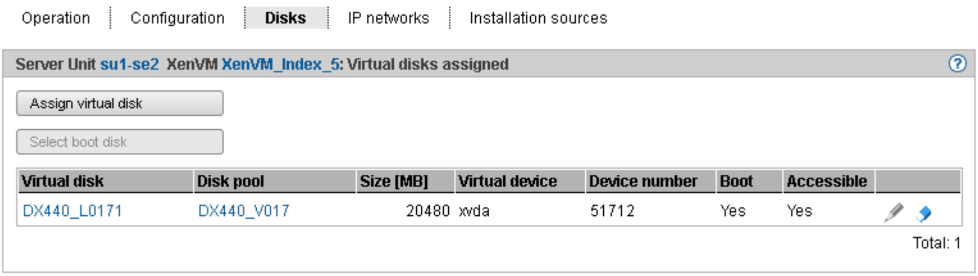
- One virtual disk
- One virtual DVD device if the installation is a standard installation (the guest system is installed from an installation source on disk)
- Optional: one virtual Network Interface Card

You can adjust the assignment of XenVM devices to current requirements.

#### Disks tab

You assign disk storage space to a XenVM by means of a virtual disk. You configure the virtual disk in a disk pool in which free storage space still exists. A disk pool makes available its storage space, which is provided on physical disks (see section “Managing XenVM devices on Server Unit x86” on page 175). You configure the first virtual disk of the XenVM when you create the XenVM, see section “VM administration” on page 115.

► Select *Systems* → *<unit> (SU<x86>)* → *Virtual machines* → *XenVM* → *<XenVM name>*, *Disks* tab.



Server Unit su1-se2 XenVM XenVM_Index_5: Virtual disks assigned

| Virtual disk | Disk pool | Size [MB] | Virtual device | Device number | Boot | Accessible | |
|---|---|---|---|---|---|---|---|
| DX440_L0171 | DX440_V017 | 20480 | xvda | 51712 | Yes | Yes | |

Total: 1

The *Disks* tab displays the virtual disks which are currently assigned to the XenVM. You can assign a virtual disk, select the boot disk, change the capacity of an assigned disk or remove a disk:

*Assigning another virtual disk*

- Click *Assign virtual disk* (above the table). In the *Assign virtual disk* dialog box you specify the device name and determine whether the disk is to be created or whether an existing disk is to be used.

The assigned newly created or reused disk is immediately available on the XenVM with the specified device name. A disk which already exists will, if necessary, also be used by other XenVMs.

*Select boot disk*

By default the configured virtual disk becomes the boot disk when the XenVM is created. If changes to the configuration mean that no boot disk is defined any more or if further disks are available in addition to the boot disk, you can redefine the boot disk.
This action is only possible when the XenVM is in the *STOPPED* or *STOPPED/INSTALLATION* status:

- Click *Select boot disk* (above the table). Select one of the virtual disks as the boot disk in the *Select boot disk* dialog box.

The selected disk immediately becomes the boot disk. The next time the XenVM is started, an attempt is made to load the operating system from this disk.

*Increasing the capacity of a virtual disk*

You can increase the size of a virtual disk as long as the associated disk pool has sufficient storage space.
This action is only possible when the XenVM is in the *STOPPED* or *STOPPED/INSTALLATION* status:

- Click the *Change* icon by the disk to be extended and specify the size of the additional storage space (in MB).

If the specified value does not exceed the maximum value, the virtual disk is increased in size by this value. The entry being rounded up to a value which is divisible by 4.
Too low a maximum value indicates that the disk pool does not have enough free storage space. In this case first expand the disk pool.

*Removing virtual disks*

You can remove a virtual disk from the configuration of the XenVM. The disk remains available as a free virtual disk and can be used again on a different XenVM.
This action is independent of the status of the XenVM, i.e. also possible in the *RUNNING* status.

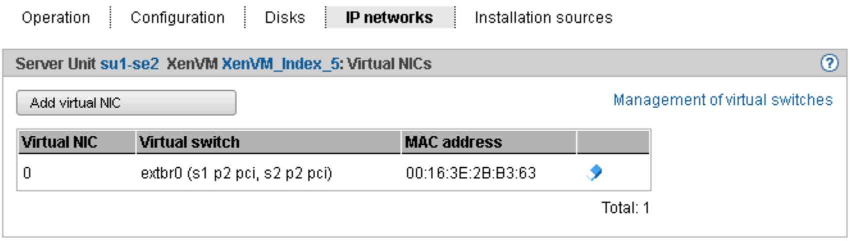
► Click the *Remove* icon by the disk to be removed and confirm the action.

The virtual disk is immediately removed from the configuration of the XenVM. The disk is displayed with the XenVM devices as a free virtual disk.
When you have removed the boot disk, you must define another disk as the boot disk before you next start the XenVM.

### IP networks tab

When you create the XenVM, you can optionally configure a virtual Network Interface Card to permit network access for the XenVM (see section “VM administration” on page 115). The virtual Network Interface Card establishes the XenVM’s network connection via a virtual switch. You make virtual switches available as XenVM devices (see section “Managing XenVM devices on Server Unit x86” on page 175).

- ► Select *Systems* → *<unit> (SU<x86>)* → *Virtual machines* → *XenVM* → *<XenVM name>*, *IP networks* tab.



Server Unit su1-se2 XenVM XenVM_Index_5: Virtual NICs

| Virtual NIC | Virtual switch | MAC address | |
|---|---|---|---|
| 0 | extbr0 (s1 p2 pci, s2 p2 pci) | 00:16:3E:2B:B3:63 | |

Total: 1

The *IP networks* tab displays the configured virtual NICs of the XenVM. You can add or remove a virtual NIC:

*Add virtual NIC*

- ► Click *Add virtual NIC* and enter the required settings in the *Add virtual NIC* dialog box.

  The virtual Network Interface Card is configured immediately.

*Removing a virtual NIC*

You can remove a virtual Network Interface Card which is no longer required from the configuration. In a fully virtualized guest system removal during ongoing operation may be rejected in accordance with the installed VMDP drivers and a message to this effect issued.

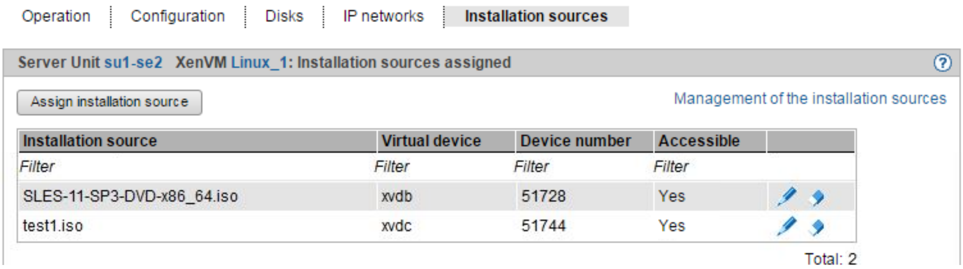
- ► Click the *Delete* icon by the virtual Network Interface Card to be deleted and confirm the action.

The virtual Network Interface Card is removed from the configuration. The MAC address which was used is once more freely available.

### Installation sources tab

When the XenVM is created, you specify an installation source from which the XenVM's operating system is to be installed (see section "VM administration" on page 115). Possible installation sources are available in the local library on the Server Unit (see section "Managing XenVM devices on Server Unit x86" on page 175). You must assign an installation source which is to be used for installing the XenVM to the XenVM as a virtual DVD device.

► Select *Systems → <unit> (SU<x86>) → Virtual machines → XenVM → <XenVM name>, Installation sources* tab.


Operation
Configuration
Disks
IP networks
Installation sources
Assign installation source
Management of the installation sources

Server Unit su1-se2 XenVM Linux_1: Installation sources assigned

| Installation source | Virtual device | Device number | Accessible | |
|---|---|---|---|---|
| *Filter* | *Filter* | *Filter* | *Filter* | |
| SLES-11-SP3-DVD-x86_64.iso | xvdb | 51728 | Yes | |
| test1.iso | xvdc | 51744 | Yes | |

Total: 2

The *Installation sources* tab displays the installation sources of the XenVM. During an installation process, the installation configuration file is also displayed if required. You can add, replace or remove an installation source retroactively:

*Assign installation source*

The XenVM always boots from the installation source with the lowest virtual device number (e.g. from hda or xvda). How the other installation sources are handled is decided by the guest system.

► Click *Assign installation source* (above the table) and enter the required settings in the *Assign installation source* dialog box.

The new installation source is immediately added to the installation sources of the XenVM.

*Switching the installation source*

The installation source can also be changed during ongoing operation. You can only assign no installation source if you are using a fully virtualized guest system (Windows or *Other operating System*).

The virtual drive is retained (possible also as an empty drive). Access from the active guest system is immediately possible (e.g. for calling the setup to install an application).

► Click the *Switch* icon by the installation source you wish to swap and select another installation source from the list.

The new installation source is immediately added to the installation sources of the XenVM.

*Removing an installation source*

You can remove the assignment to the XenVM for an installation source which is no longer to be used. This action is independent of the status of the XenVM, i.e. also possible in the *RUNNING* status.

► Click the *Remove* icon by the installation source you wish to remove and confirm the action.

The assignment of the installation source to the virtual device of the XenVM is immediately canceled. The virtual device can be used for new assignments. The installation source remains available in the local library.

# 6 Operating and managing systems on Application Units

As a rule an operating system of another vendor (Windows, Linux or Unix systems) runs on an Application Unit. The scope of the setting and display options thus depends on the operating system concerned. An Application Unit can be operated with a Native operating system or a hypervisor system. A hypervisor system permits the operation of VMs. These are displayed in the SE Manager and can be operated with it.

The following hypervisor systems can be configured: HyperV Windows Server, VMware vSphere, Oracle VM Server, Citrix XenServer.

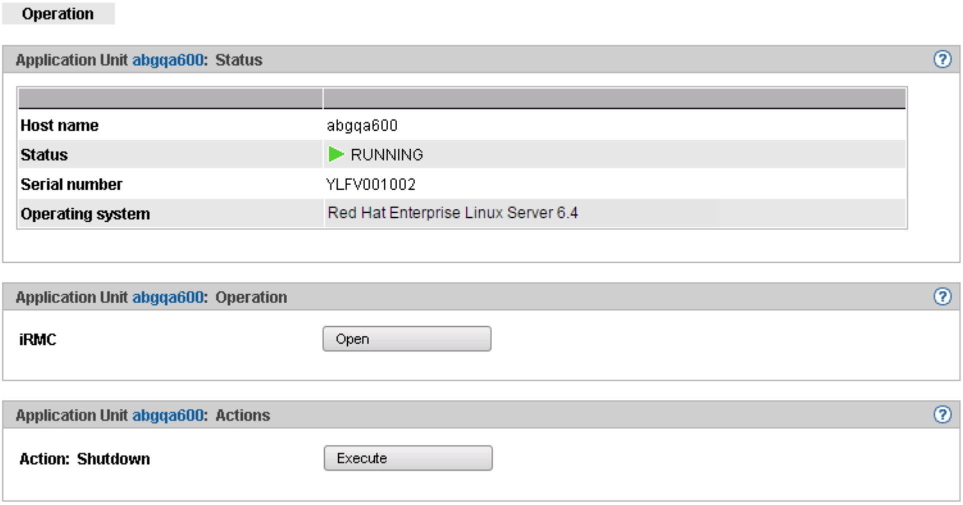
Application Units are displayed in the tree structure as *<unit name>(AUxx)*.

## 6.1 Operating a Native system

You operate a Native system via the Operation tab.

► In the tree structure select *Systems → <unit name>(AU<model>)*, *Operation* tab.

The *Operation* tab opens (example for a Linux Red Hat System).



Operation

Application Unit abgqa600: Status

| | |
|---|---|
| Host name | abgqa600 |
| Status | ▶ RUNNING |
| Serial number | YLFV001002 |
| Operating system | Red Hat Enterprise Linux Server 6.4 |

Application Unit abgqa600: Operation

Application Unit abgqa600: Actions

## Operation

► In the *Operation* tab click *Open* in the *Operation* group.

– In this way you open the web interface of the iRMC's AU for an AU47 and AU25.

– In this way you open the web interface of the Management Board for an AU87/DBU87.

## Booting or shutting down the system

The possible actions depend on the particular status of the system: If the system is running, the *Operation* tab in the *Actions* group displays the text Shutdown. If the system is not running, the text Boot is displayed.

► In the *Actions* group click *Execute* to shut down or boot the system.

## 6.2 Operating virtual machines

When an AU is operated with a hypervisor system, VMs can be configured (via this hypervisor system). You operate the VMs of an AU using the menu item *Virtual machines*.

As soon a VM has been configured, the tree structure below *Systems → <unit name>(AUxx) → Virtual machines* is expanded by a VM-specific menu *<VM name>*.

> In the case of AU87 or DBU87, systems run on the individual partitions of the AU. As soon a VM has been configured, the tree structure below *Systems → <unit name>(AU87/DBU87) → <unit-name>(<partition>) →Virtual machines* is expanded by a VM-specific menu *<VM name>*. You can operate the VM in this window.

### Information on VMs

The *VM overview* tab provides information on the virtual machines which run on the AU under a hypervisor (HyperV Windows Server, VMware vSphere, Oracle VM Server, Citrix XenServer).

► Select *Systems → <unit name>(AU<model>) → Virtual machines, VM overview* tab.

On AU87 or DBU87 you select *Systems → <unit-name>(AU87/DBU87) → <unit-name>(<partition>) → Virtual machines*, *VM overview* tab.

The *VM overview* tab displays the configured VMs.

### Operating a VM

In the VM-specific menu you receive detailed information on the VM. Depending on the situation, you can also execute an action directly for the VM (e.g. starting a VM).

– In the tree structure select *Systems → <unit name>(AUxx) → Virtual machines → <VM name>.*

  Depending on the situation, *Systems → <unit-name>(AU87/DBU87) → <unit-name>(<partition>) → Virtual machines → <VM-name>*, *VM overview* tab.

  The *Operation* tab opens and in the *Status* group displays the properties and current status of the VM.

  In addition to the hypervisor types Oracle VM Manager and VMware vSphere, the *Operation* group is also displayed provided the associated hypervisor is active and can be reached by the Management Unit, i.e.

  – The Oracle VM Manager must be integrated as a user-defined application, see section “Managing user-defined management applications” on page 146.

  – A VM with vCenter Server must be running for VMware vSphere on the Application Unit.

- Click *Open* in the *Operation* group VMware vSphere Web Client or Oracle VM Manager.

  The VM Manager opens in a new window. After logging in successfully, you obtain access there to manage the VMware hosts/systems or the Oracle VM hosts/systems.

Some actions for the VM can also be called directly in the SE Manager:

- In the *Actions* group click an action which is to be executed directly for the VM. Depending on the situation, the actions *Start VM*, *Restart VM*, *Shutdown VM*, *Pause VM*, *Unpause VM* and *Stop VM* are available for selection.
  These actions are also available for VMs of the hypervisor Citrix XenServer and Microsoft HyperV.

## 6.3 Installing an operating system on an Application Unit

As administrator you manage the applications and the operating system on AUs.

When requested by the customer, an AU is configured on the vendor side and provided with an operating system. In this case it is supplied preinstalled and the steps described below are not required. It is also possible for the customer to reinstall the operating system in this case.

### Configuring the SAS/SATA Controller Card

The AU has a SAS/SATA RAID Controller with “MegaRAID functionality”. You can configure the SAS/SATA RAID Controller either before installation with the LSI WebBIOS or during installation with the ServerView Installation Manager. For basic RAID configurations the ServerView Installation Manager can be used in the context of operating system installation.

> The controller provides a separate utility for configuring the MegaRAID. Detailed information on this subject is provided in the “LSI MegaRAID SAS Software” manual [17].
>
> Further information on modular RAID Controllers is provided in the “LSI Controllers Modular RAID Controller” Installation Guide [18].
>
> Descriptions of operating systems which are not contained in the controller manual are provided in the corresponding Readme files on the driver CDs.

### Configuring the integrated Remote Management Controller (iRMC)

The iRMC-LAN interface is already preconfigured for your administration LAN by the vendor. This enables you to utilize all functions of the iRMC such as Advanced Video Redirection (AVR) and Remote Storage for operating system installation.

If you want to use a configuration other than the preconfigured network configuration, adjust the iRMC’s configuration accordingly.

You configure important server parameters such as the ASR&R settings (Automatic Server Reconfiguration and Restart) and watchdog settings in the web interface of the Application Unit’s iRMC.

Further information is provided in the “iRMC S2 - integrated Remote Management Controller” manual [12].

### Configuration and operating system installation with the ServerView Installation Manager

The ServerView Installation Manager which is contained on the enclosed ServerView Suite DVD1 enables you to perform operating system installation and also to configure hardware-specific parameters of the AU. This includes configuring settings with the ServerView Configuration Manager and configuring the RAID Controller with the ServerView RAID Manager.

You can read how you operate the ServerView Installation Manager and further information in the associated manual [15].

### Configuration and operating system installation without the ServerView Installation Manager

In the case of manual installation without the ServerView Installation Manager you can configure all aspects of server, RAID and operating system installation in accordance with your requirements.

*Configuring a RAID Controller*

The SAS/SATA RAID Controller is configured with “MegaRAID functionality” using the controller’s WebBIOS tool (see “Configuring the SAS/SATA Controller Card” on page 137).

*Installing the operating system:*

- ► Insert the CD/DVD/BD of the operating system which is to be installed.
- ► Restart the AU.
- ► Follow the instructions on the screen and those in the manual for the operating system.

### Installing ServerView agents and the ServerView RAID Manager

AUs are permanently monitored as part of the maintenance concept for SE servers; hardware problems are reported to the Support Center.

ServerView agents and the ServerView RAID Manager must be installed in the Application Unit’s operating system to permit hardware monitoring.

- ► Install the ServerView agents and the ServerView RAID Manager. Use one of the following options for this purpose:
  - – You can download the software from the internet by specifying the Application Unit’s serial number: *http://support.ts.fujitsu.com*, section *Driver & Downloads*. You will find the two software packages under *Server Management Software*.

- You can install the software from ServerStart DVD1, which is supplied with the Application Unit.
- You can install the software when the operating system is installed if you install the operating system with the ServerView Installation Manager.

The associated installation instructions are provided in the Installation Guides for the ServerView Operation Manager [16] and [17].

### Configuring the network for the internal LAN and the administration LAN

AUs have two defined networks for the connection to the MU and for administration:

- The internal SE server network (connection to the MU for status monitoring and for Customer Support purposes)
- The administration network

Configure these networks when you install the operating system.

*Identifying the eth interfaces of the AU*

When you configure the LAN address in the management network on the AU, first determine which eth interface is provided for the management network.

You can determine the assignment of the eth interfaces to the port by comparing the MAC addresses. Use the following resources for this purpose:

- The ID card which is located at the front of the AU. On this you will find the MAC addresses for LAN A (which corresponds to Port 1) and LAN B (which corresponds to Port 2).
- An operating-system-specific command/tool (e.g. *ifconfig.* under Linux) which displays the MAC address of the corresponding port for every eth interface.

Configure the internal LAN on Port 1 and the administration LAN on Port 2.

Further information on LAN port assignment is provided in the “Additive Components” Operating Manual [4].

*Configuring LAN interfaces*

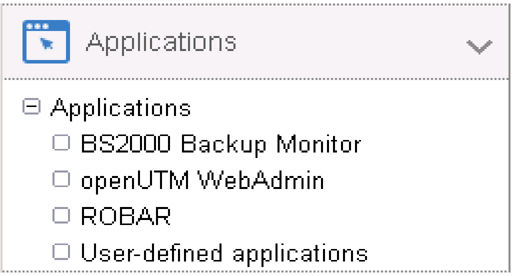
You configure the interfaces identified for the management network using Linux resources with the appropriate IP addresses, subnetwork masks, and gateways.

You configure the IP address in the management network in accordance with your administration network, as defined with Customer Support in the installation checklist.

i There is also an option of connecting an AU to the internal data networks (DANPRnn) or external data networks (DANPUnn). Ask your Customer Support staff for details.

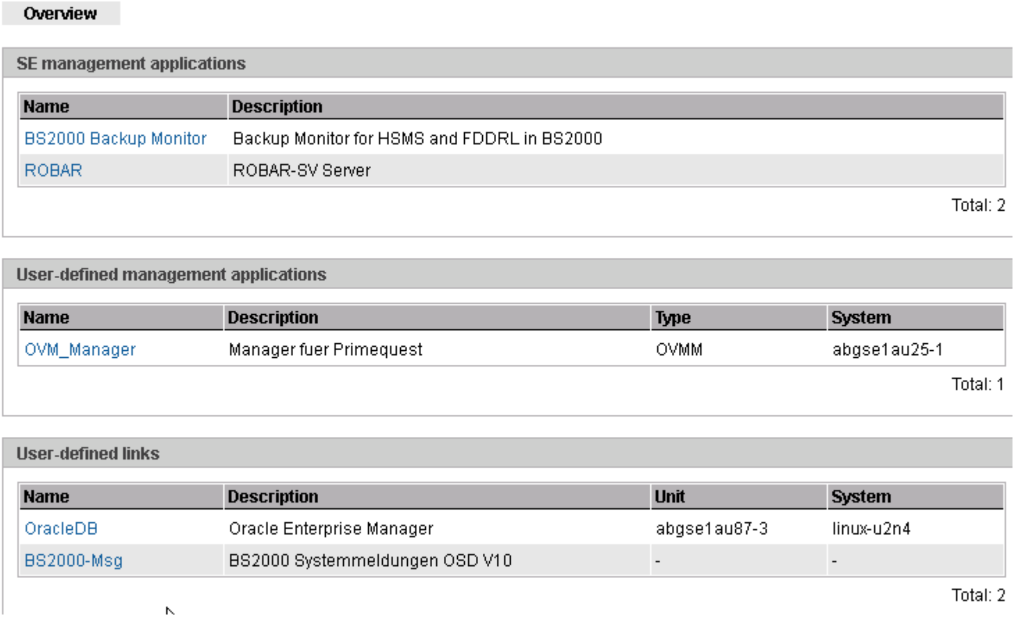
# 7 Managing applications

You manage applications using the *Applications* menu in the tree structure:



### Overview of all applications of the SE server

► Select *Applications* → *Overview* in the tree structure. The *Overview* tab opens.



SE management applications

| Name | Description |
|---|---|
| BS2000 Backup Monitor | Backup Monitor for HSMS and FDDRL in BS2000 |
| ROBAR | ROBAR-SV Server |

Total: 2

User-defined management applications

| Name | Description | Type | System |
|---|---|---|---|
| OVM_Manager | Manager fuer Primequest | OVMM | abgse1au25-1 |

Total: 1

User-defined links

| Name | Description | Unit | System |
|---|---|---|---|
| OracleDB | Oracle Enterprise Manager | abgse1au87-3 | linux-u2n4 |
| BS2000-Msg | BS2000 Systemmeldungen OSD V10 | - | - |

Total: 2

The application list consists of three groups:

- SE management applications are fully integrated into the SE Manager.
- User-defined management applications are opened in a new window or tab in the browser
- User-defined links are opened in a new window or tab in the browser

# 7.1 SE Management applications

SE Management applications execute on the Management Units and are fully integrated into the SE Manager. For details, see section “Management applications”.

The following SE Management application is currently integrated:

- BS2000 Backup Monitor

The following SE Management applications can be integrated:

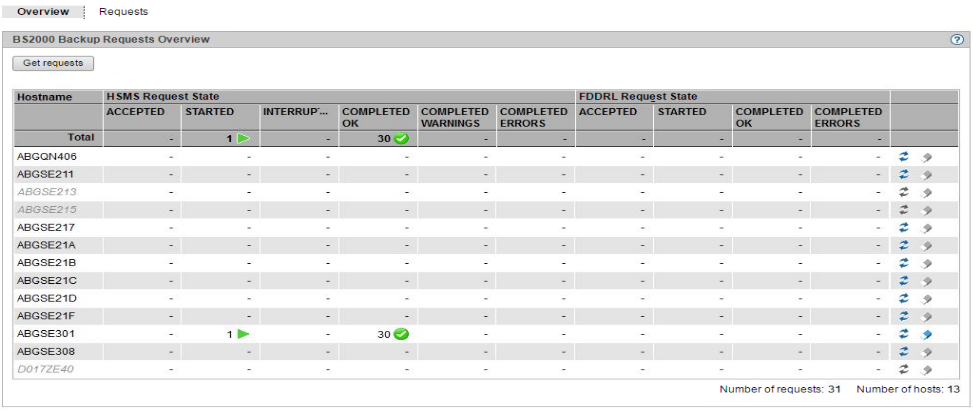
- openUTM WebAdmin
- ROBAR

openUTM WebAdmin and ROBAR are chargeable products, each with its own online help.

## 7.1.1 BS2000 Backup Monitor

The BS2000 Backup Monitor monitors backup requests which have been submitted in the BS2000 systems of the SE server using the software products HSMS and FDDRL. Whether or which information of a BS2000 system is transferred to the BS2000 Backup Monitor is controlled by an HSMS or FDDRL parameter.

► Select *Applications → BS2000 Backup Monitor → Overview, Overview* tab.



| Hostname | HSMS Request State | | | | | | FDDRL Request State | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | ACCEPTED | STARTED | INTERRUP'... | COMPLETED OK | COMPLETED WARNINGS | COMPLETED ERRORS | ACCEPTED | STARTED | COMPLETED OK | COMPLETED ERRORS | |
| Total | - | 1 ▶ | - | 30 ✓ | - | - | - | - | - | - | |
| ABGQN406 | - | - | - | - | - | - | - | - | - | - | |
| ABGSE211 | - | - | - | - | - | - | - | - | - | - | |
| *ABGSE213* | - | - | - | - | - | - | - | - | - | - | |
| *ABGSE215* | - | - | - | - | - | - | - | - | - | - | |
| ABGSE217 | - | - | - | - | - | - | - | - | - | - | |
| ABGSE21A | - | - | - | - | - | - | - | - | - | - | |
| ABGSE21B | - | - | - | - | - | - | - | - | - | - | |
| ABGSE21C | - | - | - | - | - | - | - | - | - | - | |
| ABGSE21D | - | - | - | - | - | - | - | - | - | - | |
| ABGSE21F | - | - | - | - | - | - | - | - | - | - | |
| ABGSE301 | - | 1 ▶ | - | 30 ✓ | - | - | - | - | - | - | |
| ABGSE308 | - | - | - | - | - | - | - | - | - | - | |
| *D017ZE40* | - | - | - | - | - | - | - | - | - | - | |

Number of requests: 31 Number of hosts: 13

In the *Overview* tab you can call and delete requests.

► The *Requests* tab provides you with detailed information on the various requests and, when necessary, enables you to display the report file.

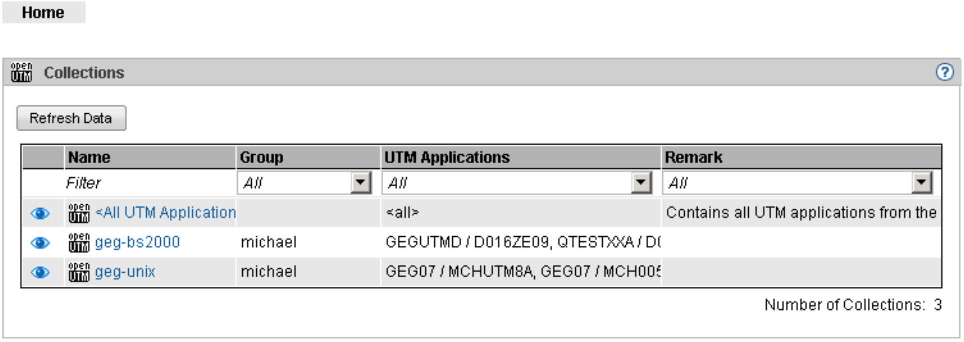
The display of the backup requests for each SE Manager is only possible when the REWAS is active, see section “Integration of BS2000 into the SE Manager” on page 36.

### 7.1.2 openUTM WebAdmin

openUTM WebAdmin enables you to manage openUTM applications on the SE server. openUTM WebAdmin has its own online help.

► Select *Applications → openUTM WebAdmin.*

The *Overview* tab displays the homepage *Home* of openUTM WebAdmin.



| | Name | Group | UTM Applications | Remark |
|---|---|---|---|---|
| | *Filter* | *All* | *All* | *All* |
| 👁 | <All UTM Application | | <all> | Contains all UTM applications from the |
| 👁 | geg-bs2000 | michael | GEGUTMD / D016ZE09, QTESTXXA / D( | |
| 👁 | geg-unix | michael | GEG07 / MCHUTM8A, GEG07 / MCH00 | |

Number of Collections: 3

The menus of openUTM WebAdmin are displayed in the tree structure.

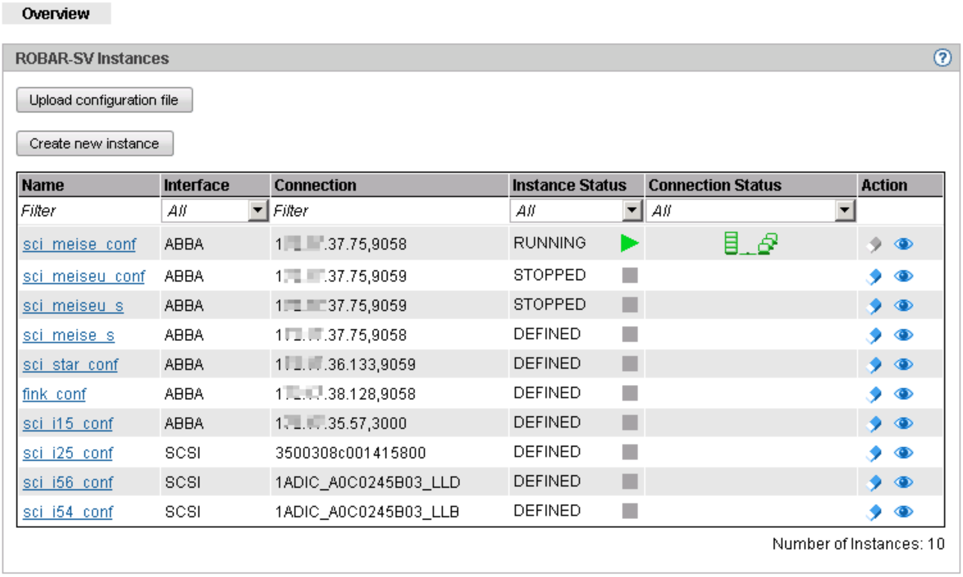
► *SE Manager* in the tree structure returns you to the SE Manager.

### 7.1.3 ROBAR

You use the ROBAR-SV Manager to manage ROBAR-SV instances on the SE server. The ROBAR-SV Manager has its own online help.

► Select *Applications → ROBAR.*

The *Overview* tab displays all ROBAR-SV instances.



Overview

ROBAR-SV Instances

Upload configuration file

Create new instance

| Name | Interface | Connection | Instance Status | Connection Status | Action |
|---|---|---|---|---|---|
| Filter | All | Filter | All | All | |
| sci_meise_conf | ABBA | 1[redacted].37.75,9058 | RUNNING ▶ | | |
| sci_meiseu_conf | ABBA | 1[redacted].37.75,9059 | STOPPED ■ | | |
| sci_meiseu_s | ABBA | 1[redacted]37.75,9059 | STOPPED ■ | | |
| sci_meise_s | ABBA | 1[redacted].37.75,9058 | DEFINED ■ | | |
| sci_star_conf | ABBA | 1[redacted].36.133,9059 | DEFINED ■ | | |
| fink_conf | ABBA | 1[redacted].38.128,9058 | DEFINED ■ | | |
| sci_i15_conf | ABBA | 1[redacted].35.57,3000 | DEFINED ■ | | |
| sci_i25_conf | SCSI | 3500308c001415800 | DEFINED ■ | | |
| sci_i56_conf | SCSI | 1ADIC_A0C0245B03_LLD | DEFINED ■ | | |
| sci_i54_conf | SCSI | 1ADIC_A0C0245B03_LLB | DEFINED ■ | | |

Number of Instances: 10

In this tab you can upload a configuration file, select and edit the configuration file of an instance, generate a new ROBAR-SV instance or delete ROBAR-SV instances.

The menus of the ROBAR-SV instances and of the ROBAR-SV management are displayed in the tree structure.

► *SE Manager* in the tree structure returns you to the SE Manager.

## 7.2 Managing user-defined management applications

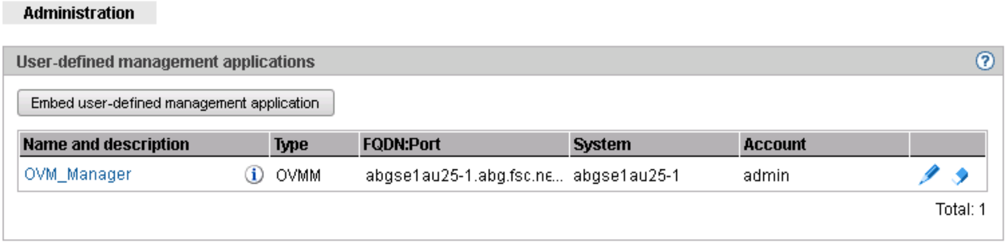
When required, you can integrate a user-defined management application into the SE Manager. User-defined management applications extend the infrastructure of the SE Manager.

The URL (link) and access data are required for the integration. The link enables you to switch directly from the SE Manager to an application. Each application opens in a separate tab or window in the browser.

The access data is used as an interface between the SE Manager and the management application. In the case of the Oracle VM Managers, this permits the integration of the Application Unit's VMs into the SE Manager.

- ► Select *Applications → User-defined management applications, Administration* tab.

  The *Administration* tab in the *User-defined management applications* group displays the list of the user-defined management applications which are integrated into the SE Manager.



Administration

User-defined management applications

Embed user-defined management application

| Name and description | Type | FQDN:Port | System | Account | |
|---|---|---|---|---|---|
| OVM_Manager ⓘ | OVMM | abgse1au25-1.abg.fsc.ne... | abgse1au25-1 | admin | |

Total: 1

- ► The *Change* and *Remove* icons enable you to change application properties (e.g. a URL) or remove the link to an application from the SE Manager.
- ► Clicking the name of an application in this table causes it to open. Thus, for example, the Oracle VM Manager is opened to administer the VMs of an Application Unit.
- ► *Link user-defined management applications* enables you to integrate further applications into the SE Manager.

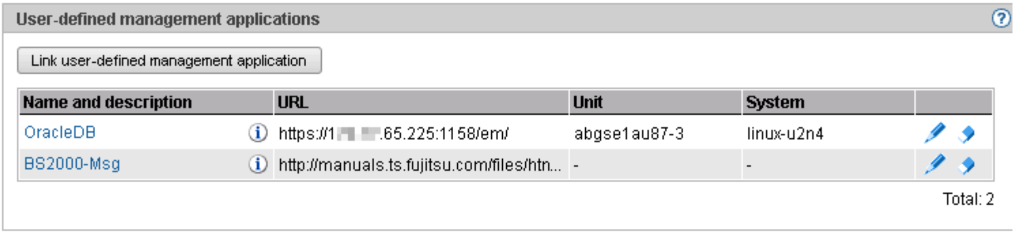
*Note on the Oracle VM Manager*

If you wish to operate an Oracle VM Manager via its web interface, you must integrate Oracle VM Manager as a user-defined application. Here you must ensure that you supply the values for FQDN port and system (AU on which the management application is running) correctly, because these values can no longer be modified after they have been integrated.

## 7.3 Administering user-defined links

► Select *Applications* → *User-defined management applications, Administration* tab.

In the *User-defined links* group the *Administration* tab displays the list of the user-defined links which are embedded in in the SE Manager.



User-defined management applications

| Name and description | | URL | Unit | System | |
|---|---|---|---|---|---|
| OracleDB | ⓘ | https://1[redacted] [redacted].65.225:1158/em/ | abgse1au87-3 | linux-u2n4 | ✎ |
| BS2000-Msg | ⓘ | http://manuals.ts.fujitsu.com/files/htn... | - | - | ✎ |

Total: 2

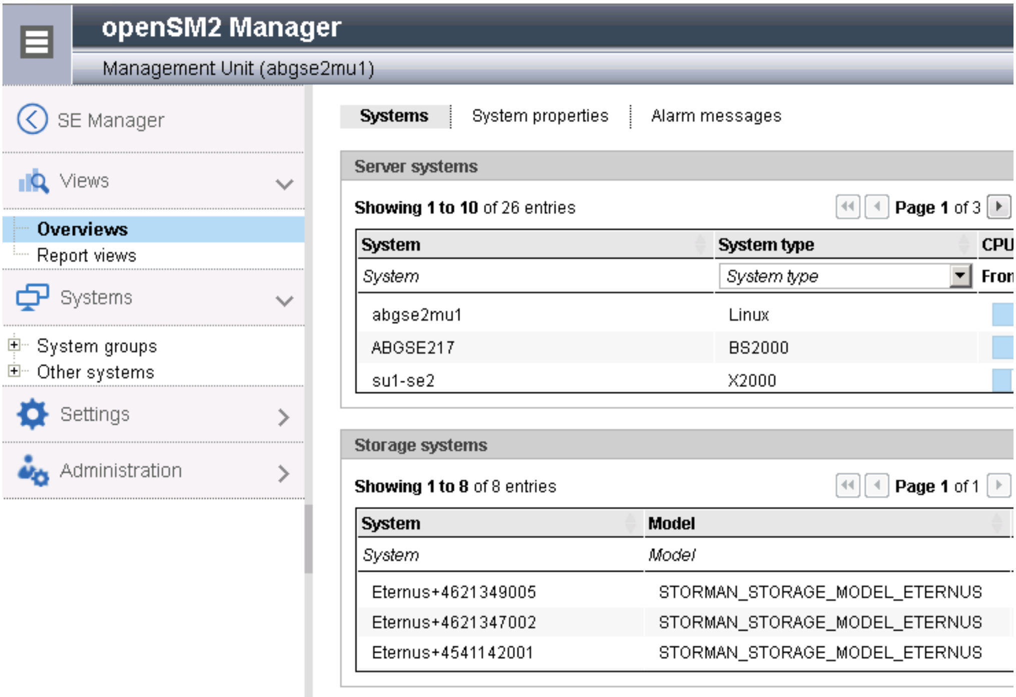
► The *Change* and *Remove* icons enable you to change application properties (e.g. a URL) or remove the link to an application from the SE Manager.

► *Embed user-defined link* enables you to integrate further external links into the SE Manager.

# 8 Monitoring performance

The openSM2 Performance Monitor can be integrated into the SE Manager. This enables the performance of the Server Units and the systems running on them to be monitored centrally using the SE Manager. openSM2 is optional and chargeable.

► In the tree structure click *Performance*. The openSM2 Manager's homepage opens.. The layout is the same as the layout of the SE Manager.



Server systems

Showing 1 to 10 of 26 entries    Page 1 of 3

| System | System type | CPU |
|---|---|---|
| System | System type | Fron |
| abgse2mu1 | Linux | ▨ |
| ABGSE217 | BS2000 | ▨ |
| su1-se2 | X2000 | ▨ |

Storage systems

Showing 1 to 8 of 8 entries    Page 1 of 1

| System | Model |
|---|---|
| System | Model |
| Eternus+4621349005 | STORMAN_STORAGE_MODEL_ETERNUS |
| Eternus+4621347002 | STORMAN_STORAGE_MODEL_ETERNUS |
| Eternus+4541142001 | STORMAN_STORAGE_MODEL_ETERNUS |

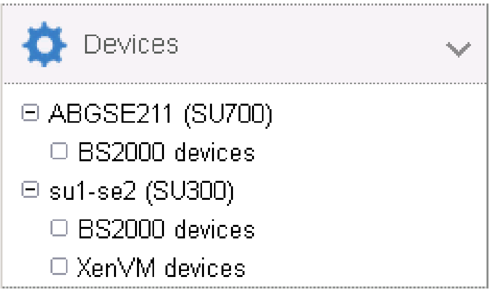
► You use the tree structure and tabs of openSM2 to call the functions of openSM2.

► *SE Manager* in the tree structure returns you to the SE Manager.

Further details on openSM2 are contained in the openSM2 User Guide [13].

# 9 Managing devices

You manage the devices of the SE server using the *Devices* menu in the tree structure. The example below shows an SE700:



The devices are managed on an SU-specific basis:

- BS2000 devices
- XenVM devices (exist only on an SU x86 with an XenVM license, in the example SU300)

# 9.1 Managing BS2000 devices

For an SU x86 you manage BS2000 devices via the SU itself (menu item BS2000 devices). Detailed information is provided in the sections on disks, LAN devices, KVP, and tape devices.

A few special aspects apply for an SU /390, see Device management on Server Unit /390.

## 9.1.1 Device addresses

### Mnemonic and unit ID

In BS2000 devices are identified and addressed by means of their mnemonic name. The mnemonic name is known as mnemonic for short and abbreviated to MN (in BS2000 sometimes also abbreviated with MNEM).

*Example*

On the BS2000 console an emulated tape drive with the mnemonic AF is addressed in the /SHOW-DEVICE-STATUS and /ATTACH-DEVICE commands:

```
/SHOW-DEVICE-STATUS AF
%  MNEM DEV-TYPE CONF-STATE POOL VSN   DEV-A    PHASE    ACTION
%  AF   BM1662FS DETACHED    SW         FREE            NO ACTION
/ATTACH-DEVICE AF
% MSG-000.165608  %  NKR0042 'DEVICE     =AF': ATTACH ACCEPTED
%XAAE-000.165608  %  NKR0116 ASSIGN FOR 'DEVICE=AF' IN PROCESS
% MSG-000.165608  %  NKR0110 'DEVICE     =AF' ATTACHED AND ASSIGNED
! UCO-000.165608  %  NBR0740 COMMAND COMPLETED 'ATTACH-DEVICE'; (RESULT:
SC2=000, SC1=000, MC=CMD0001); DATE: 2015-01-09
/SHOW-DEVICE-STATUS AF
+XAAD MNEM DEV-TYPE CONF-STATE POOL VSN   DEV-A    PHASE    ACTION
+XAAD AF   BM1662FS ATTACHED    SW         FREE            NO ACTION
```

Tape drive AF is initially in the (CONF-STATE) DETACHED status; it is then successfully attached using the /ATTACH-DEVICE command. The second command, /SHOW-DEVICE-STATUS, shows the new status.

With the exception of disks and real tape devices, the devices visible to BS2000 on an SU /390 are emulated devices and not directly the real devices. On an SU x86 this applies for all devices. The following designation is more precise then "emulated devices": BS2000 emulations of the real devices.

The device address must be specified when an emulated device is configured in BS2000. The names in BS2000 for the channel path identifier and unit address are Host Connector and Unit ID, with Unit ID corresponding to the host LUN.

| Device address | | |
|---|---|---|
| **BS2000** | **X2000 / SU /390** | **Periphery** |
| Channel path identifier | Host Connector | - |
| Logical unit number | Unit ID in X2000 or<br>LUN on SU /390 | Host LUN or LUN<br>(LUN = Logical Unit Number) |

For information on device addresses in BS2000, please also refer to the “System Installation” manual [8].

When a device is generated for BS2000, the following details are required in addition to the type-specific data:

- Unit ID on SU x86 or LUN on SU /390
  Possible values:
  - Unit ID: hexadecimal, two digits in the range 00 through FF
  - LUN: 0000 through FFFF

  All values are functionally equivalent.
- Mnemonic
  Possible values:
  - alphanumeric, two characters (character set: digits and letters)
  - hexadecimal, four characters (character set: numbers from 1000 through FFFF)

  The mnemonics can be selected in such a way that every customer-specific naming schema is supported. On an MU no check is made to see whether the specification matches the mnemonic configured in BS2000. To prevent misunderstandings, they should be identical.

Every combination of the possible values is permitted.

## 9.1.2 Device management on Server Unit /390

On the SU /390, all the devices which are used must be generated in the IORSF. One or more IORSF files are stored in the SVP. One IORSF file is used for the IPL. This is the "current" IORSF file.

KVP devices, LAN devices, and emulated tape devices of the SU /390 are emulated on the MU. ZASLAN devices of the SU /390 are emulated on the HNC. However, the relevant devices must always also be generated in the current IORSF.

Apart from the devices which are emulated on the MU or HNC, further devices, namely disks and real tape devices, exist in BS2000.

For devices which are emulated on the MU, the Host Connector is always 00. For devices which are emulated on the HNS, the Host Connector is 00 or 01.

Channel 00 is a FICON channel. FC-SCSI channels have a CHPID ≥ 02.

There are no device licenses. LUNs 0000 through FFFF can be used without restriction for configuring devices irrespective of the type.

Information on the generated BS2000 devices of the SU /390 is displayed when the data of the current IORSF file is available.

### 9.1.2.1 Predefined BS2000 devices

The following BS2000 devices are predefined for the SU /390:

| Type | MN | HC | LUN | Details |
|---|---|---|---|---|
| KVP | C2_C3 | 00 | C3_C4 | Name: HV0 |
| LOCLAN | CC80_CC81 | 00 | 80_81 | Name: MANLO1<br>IP address: 192.168.138.21<br>Address space: 192.168.138.xx |
| CDROM | T0 | 00 | 60 | Real CD-ROM drive |
| EMFILE | T1 | 00 | 61 | emfile0061 |
| *In the case of MU redundancy on MU2:* | | | | |
| KVP | C4_C5 | 00 | C3_C4 | Name: HV0 |
| LOCLAN | CD80_CD81 | 00 | 80_81 | Name: MANLO1<br>IP address: 192.168.139.21<br>Address space: 192.168.139.xx |
| CDROM | TA | 00 | 60 | Real CD-ROM drive |
| EMFILE | TB | 00 | 61 | emfile0061 |

Tabelle 4: Predefined BS2000 devices on SU /390 (MU)

On the HNC the following BS2000 devices are predefined for the SU /390:

| Type | MN | HC | LUN | Details |
|---|---|---|---|---|
| LOCLAN | - | - | - | -<br>Address space: 192.168.151.xx |
| ZASLAN | CC40_CC41 | 00 | 40_41 | Name: MCNPR<br>Slot: s2 p0 pci |
| *In the case of HNC redundancy on HNC2:* | | | | |
| LOCLAN | - | - | - | -<br>Address space: 192.168.152.xx |
| ZASLAN | CD40_CD41 | 00 | 40_41 | Name: MCNPR<br>Slot: s2 p0 pci |

Tabelle 5: Predefined BS2000 devices on SU /390 (HNC)

### 9.1.2.2 Device connection via Management Unit and HNC

When a device is added, in the first step the MU or HNC on which the device is emulated must be specified:

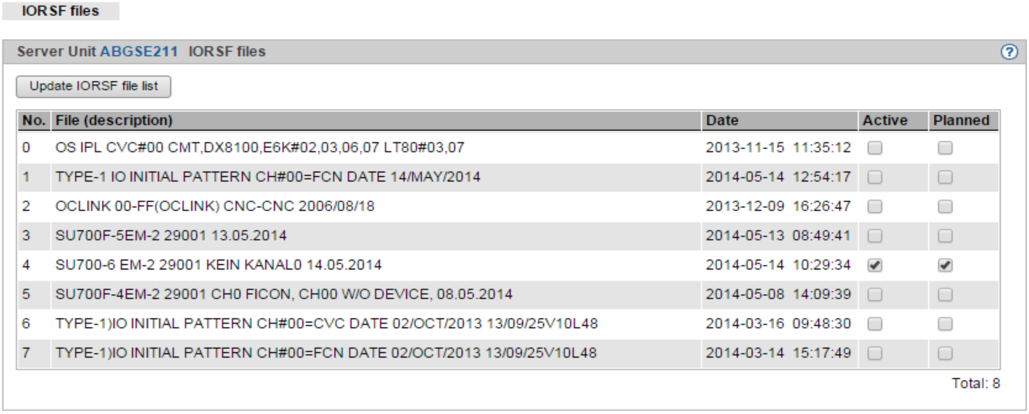
- You can manage (add, change, remove) LAN devices (ZASLAN and LOCLAN) of an SU /390 via the HNC, see, for example, “Add new LAN device” on page 167.
- You can manage KVPs, LAN devices (LOCLAN), and emulated tape devices via the MU.

Details are provided in the sections below:

- “Adding a new KVP” on page 164
- “Removing a KVP” on page 165
- “Add new LAN device” on page 167
- “Adding a LAN device” on page 167
- “Add new tape devices” on page 169
- “Remove tape device” on page 169

### 9.1.2.3 Configuration in IORSF files

► Select *Devices → <unit>(SU</390>), IORSF files* tab.



| No. | File (description) | Date | Active | Planned |
|---|---|---|---|---|
| 0 | OS IPL CVC#00 CMT,DX8100,E6K#02,03,06,07 LT80#03,07 | 2013-11-15 11:35:12 | ☐ | ☐ |
| 1 | TYPE-1 IO INITIAL PATTERN CH#00=FCN DATE 14/MAY/2014 | 2014-05-14 12:54:17 | ☐ | ☐ |
| 2 | OCLINK 00-FF(OCLINK) CNC-CNC 2006/08/18 | 2013-12-09 16:26:47 | ☐ | ☐ |
| 3 | SU700F-5EM-2 29001 13.05.2014 | 2014-05-13 08:49:41 | ☐ | ☐ |
| 4 | SU700-6 EM-2 29001 KEIN KANAL0 14.05.2014 | 2014-05-14 10:29:34 | ☑ | ☑ |
| 5 | SU700F-4EM-2 29001 CH0 FICON, CH00 W/O DEVICE, 08.05.2014 | 2014-05-08 14:09:39 | ☐ | ☐ |
| 6 | TYPE-1)IO INITIAL PATTERN CH#00=CVC DATE 02/OCT/2013 13/09/25V10L48 | 2014-03-16 09:48:30 | ☐ | ☐ |
| 7 | TYPE-1)IO INITIAL PATTERN CH#00=FCN DATE 02/OCT/2013 13/09/25V10L48 | 2014-03-14 15:17:49 | ☐ | ☐ |

Total: 8

The *IORSF files* tab provides information about the IORSF files which are available on the MU.

► Click *Update IORSF file list* to display the IORSF files which are currently available on the SVP.

The previous file list is deleted and the current data is transferred from the SVP. In this case the active IORSF file is implicitly transferred and edited, and the device lists in the BS2000 devices menu are refreshed.

## 9.1.3 Device management on Server Unit x86

On an SU x86 all the BS2000 devices (disks, KVP, LAN devices, tape devices) are emulated in X2000.

The devices are managed on the SU x86 concerned.

When devices are added, device licenses may need to be taken into account.

### 9.1.3.1 Predefined BS2000 devices

The following BS2000 devices are predefined on SU x86:

| Type | MN | HC | Unit ID | Details |
|---|---|---|---|---|
| Disk | D0 | 00 | 08 | Internal disk; generated as standby pubset |
| KVP | Z0_Z1 | 00 | 04_05 | Name: HV0 |
| LOCLAN | CC80_CC81 | 0C | 80_81 | Name: MANLO1<br>Address: 192.168.138.21<br>Address space: 192.168.138.xx |
| ZASLAN | CC40_CC41 | 0C | 40_41 | Name: MCNPR<br>Slot: s1 p0 pci |
| CDROM | CD | 00 | CD | Real CD-ROM drive |
| EMFILE | EF | 00 | EF | emfile00ef |

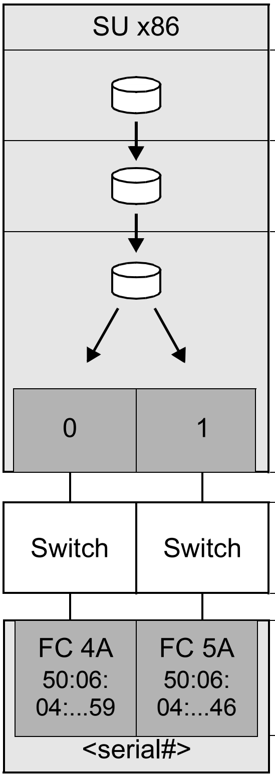
Tabelle 6: Predefined BS2000 devices on SU x86

### 9.1.3.2 Connection of peripheral devices

When BS2000 devices which reside on peripheral devices (disks, tapes) are configured, as a rule not only the X2000 level plays a role, but also other levels.

The various levels are explained on the basis of an example of a connected (via FibreChannel) disk storage system:

- The BS2000 disks are mapped on Linux disks.
- The Linux disks are operated via one or more FibreChannel HBAs (Host Bus Adapters).
- The SU x86 is connected to the disk storage system either directly or via a FibreChannel switch.



| Instance | Level | Task / explanation | Configuration example |
|---|---|---|---|
| BS2000 | | MN | 2000 |
| X2000 | 4 | Assignment of BS2000 device to Linux device | MN 2000 : /xemp<serial#><lun> |
| Multipath | 3 | path administration , mapping to physical device and assignment to WWPN of the storage system | /xemp<serial#><lun> →<br>0: wwn 50:06:04:...59<br>and<br>1: wwn 50:06:04:...46 |
| Switch | 2 | Zoning<br>Visability of ports | |
| FC adapter | 1 | Assignment from LUN to logical device # | 4A : lun 000 → logical volume 010<br>5A : lun 000 → logical volume 010 |

Bild 12: Device configuration on an SU x86 taking a disk storage system as an example

FibreChannel-connected BS2000 disks on an SU x86 must be configured at Storage(1), Switch(2) and X2000(4) levels. No special configuration is necessary at Multipath(3) level. However, it is necessary for Multipath to know the connected devices. For this purpose Customer Support can scan the devices, if required. When an operational interruption is acceptable, you can as an alternative reboot the Server Unit.

- Storage level
  The settings in the storage system should be made by a qualified technician.
- FibreChannel switch
  The zone is set in the FibreChannel switch.
- X2000
  Use the SE Manager to configure the disks of the storage system as BS2000 disks of the SU x86. Customer Support must partition disks of the type D3475-8F up front. If disks of the type D3475-8F are taken over from an SX server, they retain the Solaris label (for reasons of compatibility).

## 9.1.4 Managing disks

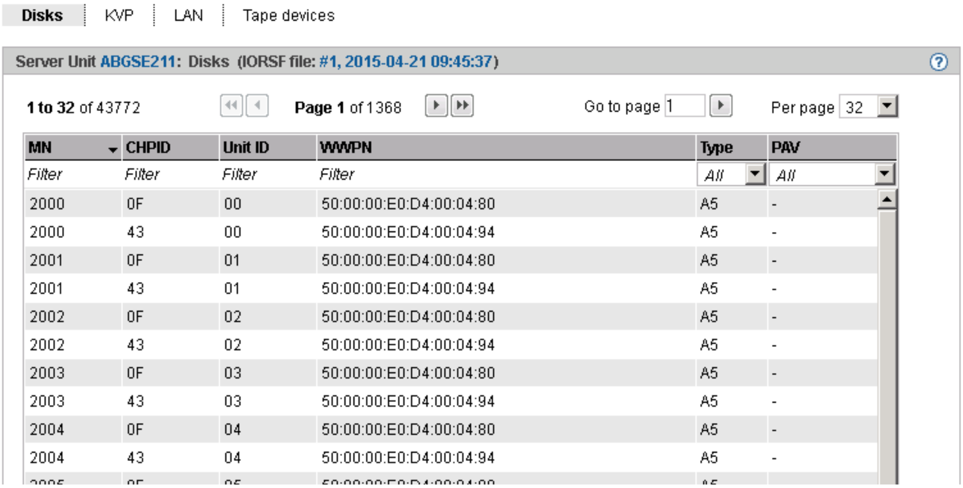
Disks of the type 8F (D3475-8F) or A5 (D3435) are connected to an SE server. The disks are connected either internally (within the SE server) or externally (in other storage systems or cabinets).

For the Server Units, the *Disks* tab offers the following functionality for managing disks. Functions above and beyond the displaying of disks are only available for the Server Unit x86.

### 9.1.4.1 Displaying generated disks on Server Unit /390

The devices are displayed only if the active IORSF file has the status "File transferred".

► Select *Devices* → *<unit> (SU</390>)* → *BS2000 devices*, *Disks* tab.



Server Unit ABGSE211: Disks (IORSF file: #1, 2015-04-21 09:45:37)

**1 to 32** of 43772 **Page 1** of 1368 Go to page 1 Per page 32

| MN | CHPID | Unit ID | WWPN | Type | PAV |
|---|---|---|---|---|---|
| *Filter* | *Filter* | *Filter* | *Filter* | *All* | *All* |
| 2000 | 0F | 00 | 50:00:00:E0:D4:00:04:80 | A5 | - |
| 2000 | 43 | 00 | 50:00:00:E0:D4:00:04:94 | A5 | - |
| 2001 | 0F | 01 | 50:00:00:E0:D4:00:04:80 | A5 | - |
| 2001 | 43 | 01 | 50:00:00:E0:D4:00:04:94 | A5 | - |
| 2002 | 0F | 02 | 50:00:00:E0:D4:00:04:80 | A5 | - |
| 2002 | 43 | 02 | 50:00:00:E0:D4:00:04:94 | A5 | - |
| 2003 | 0F | 03 | 50:00:00:E0:D4:00:04:80 | A5 | - |
| 2003 | 43 | 03 | 50:00:00:E0:D4:00:04:94 | A5 | - |
| 2004 | 0F | 04 | 50:00:00:E0:D4:00:04:80 | A5 | - |
| 2004 | 43 | 04 | 50:00:00:E0:D4:00:04:94 | A5 | - |
| 2005 | 0F | 05 | 50:00:00:E0:D4:00:04:80 | A5 | |

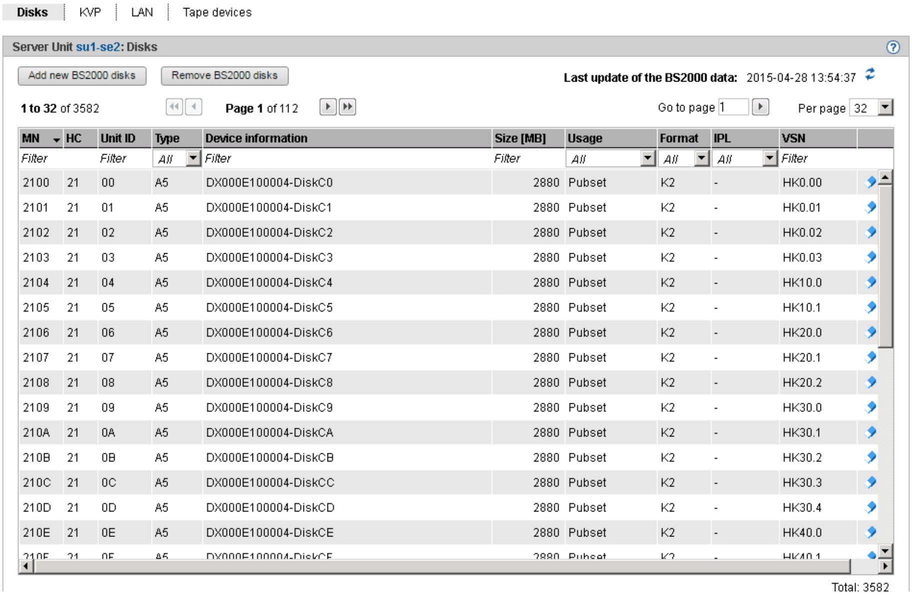
The *Disks* tab provides information about the BS2000 disks which are configured in the active IORSF file. Depending on the scope of the settings, the table can be spread over several pages. You can scroll in the table and change the settings. You can reduce the content of extensive tables by selecting filter criteria.

In VM2000 mode the table contains an additional column: if a device assignment exists, the last column *Assigned* (after*VSN*) displays the VM.

### 9.1.4.2 Managing disks on Server Unit x86

#### Displaying disks

► Select *Devices → <unit> (SU<x86>) → BS2000 devices*, *Disks* tab.



Server Unit su1-se2: Disks

Last update of the BS2000 data: 2015-04-28 13:54:37

1 to 32 of 3582 Page 1 of 112 Go to page 1 Per page 32

| MN | HC | Unit ID | Type | Device information | Size [MB] | Usage | Format | IPL | VSN |
|---|---|---|---|---|---|---|---|---|---|
| Filter | | Filter | All | Filter | Filter | All | All | All | Filter |
| 2100 | 21 | 00 | A5 | DX000E100004-DiskC0 | 2880 | Pubset | K2 | - | HK0.00 |
| 2101 | 21 | 01 | A5 | DX000E100004-DiskC1 | 2880 | Pubset | K2 | - | HK0.01 |
| 2102 | 21 | 02 | A5 | DX000E100004-DiskC2 | 2880 | Pubset | K2 | - | HK0.02 |
| 2103 | 21 | 03 | A5 | DX000E100004-DiskC3 | 2880 | Pubset | K2 | - | HK0.03 |
| 2104 | 21 | 04 | A5 | DX000E100004-DiskC4 | 2880 | Pubset | K2 | - | HK10.0 |
| 2105 | 21 | 05 | A5 | DX000E100004-DiskC5 | 2880 | Pubset | K2 | - | HK10.1 |
| 2106 | 21 | 06 | A5 | DX000E100004-DiskC6 | 2880 | Pubset | K2 | - | HK20.0 |
| 2107 | 21 | 07 | A5 | DX000E100004-DiskC7 | 2880 | Pubset | K2 | - | HK20.1 |
| 2108 | 21 | 08 | A5 | DX000E100004-DiskC8 | 2880 | Pubset | K2 | - | HK20.2 |
| 2109 | 21 | 09 | A5 | DX000E100004-DiskC9 | 2880 | Pubset | K2 | - | HK30.0 |
| 210A | 21 | 0A | A5 | DX000E100004-DiskCA | 2880 | Pubset | K2 | - | HK30.1 |
| 210B | 21 | 0B | A5 | DX000E100004-DiskCB | 2880 | Pubset | K2 | - | HK30.2 |
| 210C | 21 | 0C | A5 | DX000E100004-DiskCC | 2880 | Pubset | K2 | - | HK30.3 |
| 210D | 21 | 0D | A5 | DX000E100004-DiskCD | 2880 | Pubset | K2 | - | HK30.4 |
| 210E | 21 | 0E | A5 | DX000E100004-DiskCE | 2880 | Pubset | K2 | - | HK40.0 |
| 210F | 21 | 0F | A5 | DX000E100004-DiskCF | 2880 | Pubset | K2 | - | HK40.1 |

Total: 3582

The *Disks* tab displays the configured BS2000 disks. Depending on the scope of the settings, the table can be spread over several pages. You can scroll in the table and change the settings. You can reduce the content of extensive tables by selecting filter criteria.

i In VM2000 mode the table contains an additional column: if a device assignment exists, the last column *Assigned* (after*VSN*) displays the VM.

The following options are available to you:

*Add new BS2000 disks*

► Click *Add new BS2000 disks*.

In the *Add new BS2000 disks* wizard you can specify the required properties and the desired number of BS2000 disks step by step.

*Remove BS200 disks*

► Click *Remove BS2000 disks*.

In the *Remove BS2000 disks* wizard you can specify an interval of MNs for the BS2000 disks to be removed. The same prerequisites apply as for Remove disk.

*BS2000 data:updating*

► Click the *Update BS2000 data* icon and confirm the action.

*Remove disk*

i The following requirements must already be satisfied:

- The disk must be out of service as a BS2000 device in order to prevent data loss (/EXPORT-PUBSET and /DETACH-DEVICE commands).
- In VM2000 mode the disk may not be assigned to a VM.

► By the required disk, click the *Remove* icon and confirm the action.

### 9.1.5 Managing KVP devices

A KVP (console distribution program) with the name *HV0* is preconfigured on the MU and SU x86 (see table 4 on page 154 and table 6 on page 157). You can delete the existing KVP and then define a new one with different values.

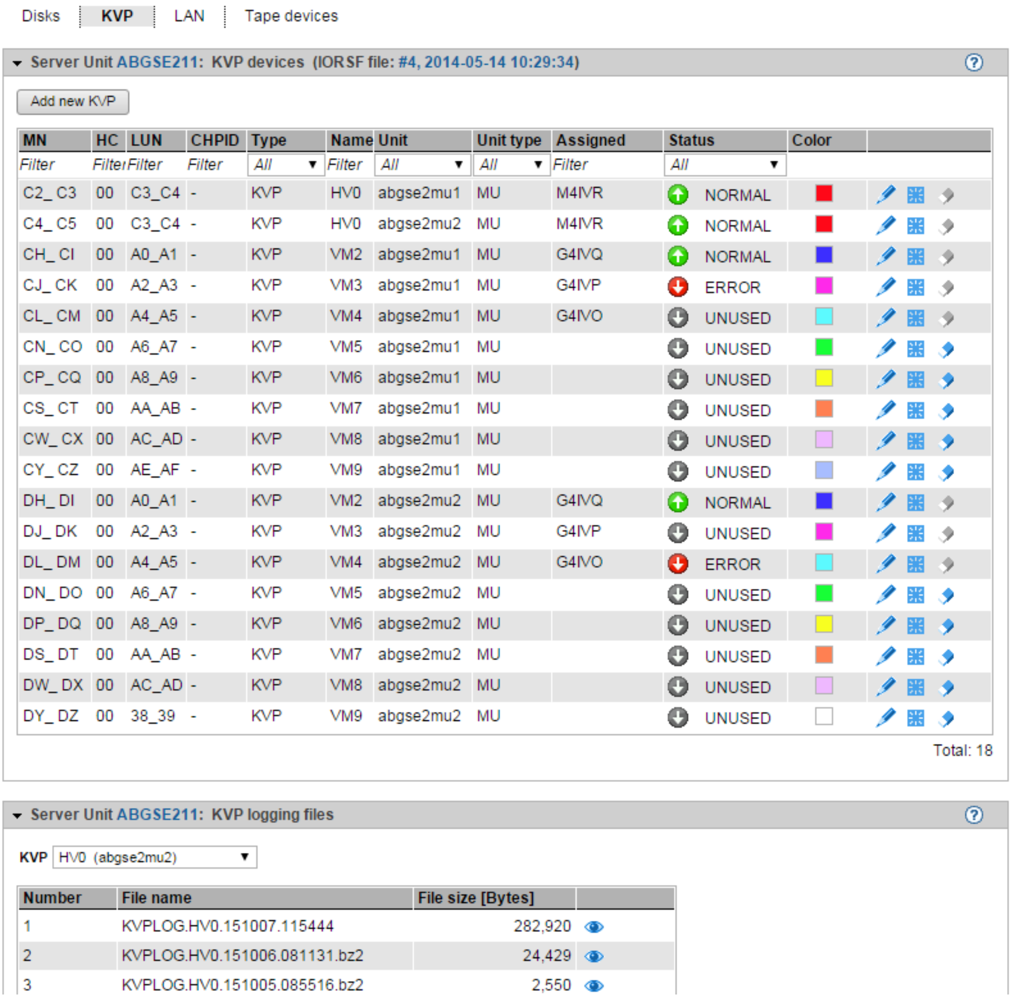
BS2000 sees a KVP as two (emulated) KVP devices (or a device pair) which are identified by their mnemonic names.

For VM2000 mode it is necessary to define at least one KVP per VM. By default *HV0* is the monitor system's KVP.

Access to a BS2000 console always takes place via the KVP and the home account. An operator requires an individual right for access. For information on this, see section “Opening the BS2000 console and dialog window” on page 99.

**Recommendation:**
Define precisely one KVP for each VM (in the case of SU /390 for each MU).

► Select *Devices* → *<unit> (SU<model>)* → *BS2000 devices, KVP* tab.



Disks | **KVP** | LAN | Tape devices

▾ Server Unit ABGSE211: KVP devices (IORSF file: #4, 2014-05-14 10:29:34)

Add new KVP

| MN | HC | LUN | CHPID | Type | Name | Unit | Unit type | Assigned | Status | Color | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| *Filter* | *Filter* | *Filter* | *Filter* | *All* ▼ | *Filter* | *All* ▼ | *All* ▼ | *Filter* | *All* ▼ | | |
| C2_C3 | 00 | C3_C4 | - | KVP | HV0 | abgse2mu1 | MU | M4IVR | NORMAL | 🟥 | |
| C4_C5 | 00 | C3_C4 | - | KVP | HV0 | abgse2mu2 | MU | M4IVR | NORMAL | 🟥 | |
| CH_CI | 00 | A0_A1 | - | KVP | VM2 | abgse2mu1 | MU | G4IVQ | NORMAL | 🟦 | |
| CJ_CK | 00 | A2_A3 | - | KVP | VM3 | abgse2mu1 | MU | G4IVP | ERROR | 🟪 | |
| CL_CM | 00 | A4_A5 | - | KVP | VM4 | abgse2mu1 | MU | G4IVO | UNUSED | 🟦 | |
| CN_CO | 00 | A6_A7 | - | KVP | VM5 | abgse2mu1 | MU | | UNUSED | 🟩 | |
| CP_CQ | 00 | A8_A9 | - | KVP | VM6 | abgse2mu1 | MU | | UNUSED | 🟨 | |
| CS_CT | 00 | AA_AB | - | KVP | VM7 | abgse2mu1 | MU | | UNUSED | 🟧 | |
| CW_CX | 00 | AC_AD | - | KVP | VM8 | abgse2mu1 | MU | | UNUSED | 🟪 | |
| CY_CZ | 00 | AE_AF | - | KVP | VM9 | abgse2mu1 | MU | | UNUSED | 🟦 | |
| DH_DI | 00 | A0_A1 | - | KVP | VM2 | abgse2mu2 | MU | G4IVQ | NORMAL | 🟦 | |
| DJ_DK | 00 | A2_A3 | - | KVP | VM3 | abgse2mu2 | MU | G4IVP | UNUSED | 🟪 | |
| DL_DM | 00 | A4_A5 | - | KVP | VM4 | abgse2mu2 | MU | G4IVO | ERROR | 🟦 | |
| DN_DO | 00 | A6_A7 | - | KVP | VM5 | abgse2mu2 | MU | | UNUSED | 🟩 | |
| DP_DQ | 00 | A8_A9 | - | KVP | VM6 | abgse2mu2 | MU | | UNUSED | 🟨 | |
| DS_DT | 00 | AA_AB | - | KVP | VM7 | abgse2mu2 | MU | | UNUSED | 🟧 | |
| DW_DX | 00 | AC_AD | - | KVP | VM8 | abgse2mu2 | MU | | UNUSED | 🟪 | |
| DY_DZ | 00 | 38_39 | - | KVP | VM9 | abgse2mu2 | MU | | UNUSED | ⬜ | |

Total: 18

▾ Server Unit ABGSE211: KVP logging files

KVP HV0 (abgse2mu2) ▼

| Number | File name | File size [Bytes] | |
|---|---|---|---|
| 1 | KVPLOG.HV0.151007.115444 | 282,920 | |
| 2 | KVPLOG.HV0.151006.081131.bz2 | 24,429 | |
| 3 | KVPLOG.HV0.151005.085516.bz2 | 2,550 | |

The *KVP* tab with the groups *KVP devices* (or *KVPs* in the case of SU x86) and *KVP logging* opens. When expanded, the groups display a table containing the current KVPs and the logging files of the selected KVPs (see section “Managing KVP devices” on page 165).

ℹ Information on the generated KVP devices on SU /390
The devices are displayed only if the IORSF file has the status "File transferred".

- Entries of the type IORSF display devices which are generated exclusively in the IORSF.
- Entries of the type KVP display the KVP devices already defined. If the KVP is also generated in the IORSF, a valid channel path identifier is displayed under CHPID. Otherwise only a warning icon is displayed under CHPID, and the device must still be generated (in BS2000 with /ADD-IO-UNIT).

ℹ In VM2000 mode the table contains an additional column: if a device assignment exists, the *Assigned* column displays the VM.

**The *KVP* tab offers the following functionality for managing KVPs:**

*Adding a new KVP*

The KVP is created by this action.

► In the group *KVP devices* (or *KVPs* in the case of SU x86) click *Add new KVP*.

In the *Add KVP* wizard you can specify the required properties of the KVP step by step.

*Changing the color of a KVP*

With this action you define the color for the console window's frame. This enables a number of opened console windows to be distinguished just by their frame color.

► In the group *KVP devices* (or *KVPs* in the case of SU x86) click on the *Change* icon by the required KVP and select a new color code.

*Adding a KVP device*

The restart allows you to rectify a problematical situation which affects the device. Open KVP connections (console windows) are then terminated.

► Click the *Restart* icon by the required KVP.

*Removing a KVP*

ℹ When the KVP is removed, the associated KVP logging files are also deleted. The history of the BS2000 systems is then no longer complete.

► In the *KVP devices* group (or *KVPs* in the case of SU x86) click on the *Remove* icon by the required KVP.

*Displaying KVP logging file selectively*

ℹ As access is possible to all KVPs, files of a KVP whose assignment to a BS2000 guest system has already been deleted can still be displayed. This also permits the BS2000 history of BS2000 guest systems which have already been deleted to be traced if necessary.

Only the KVP assignment is displayed, not the VM assignment, because a different VM assignment may have been valid in a previous session.

You can also view the log files of a KVP which is not assigned to any BS2000 system (e.g. because the latter has already been deleted). This enables you to access all logs of all KVPs of this Unit

► In the *KVP logging* group select the required KVP from the *KVP* list.

The KVP logging files which exist for this KVP are listed. The *Display* icon opens the *Display KVP logging file selectively* dialog box in which you can define the view of the content of the KVPLOG file to be displayed.

The logging records are displayed in a separate window.

*Downloading the KVP logging file*

► In the *KVP logging* group select the required KVP from the *KVP* list. Click the *Download* icon by the required KVP logging file. Enter the path and file names in the system-specific Explorer window and save the file.

## 9.1.6 Managing LAN devices

An SU /390's BS2000 system is integrated into a LAN via ZASLAN and LOCLAN, the MU permitting the connection via LOCLAN and the HNC via ZASLAN and LOCLAN.

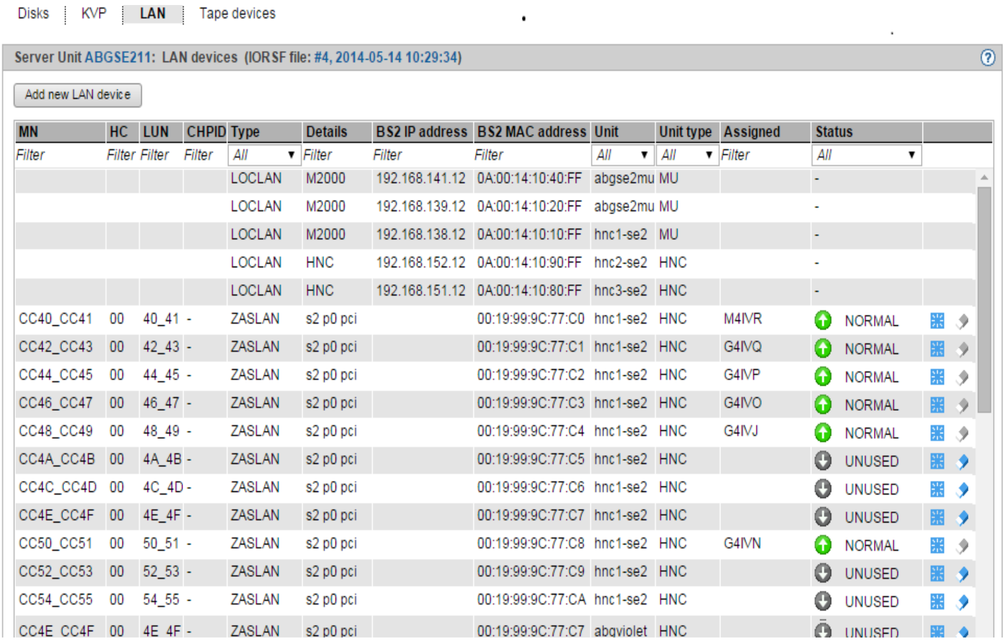
An SU x86's BS2000 system is integrated into a LAN via ZASLAN, LOCLAN, and BRGLAN.

From the BS2000 viewpoint, a LAN device is always a device pair.

For VM2000 mode it is necessary to define at least one LOCLAN device per VM.

> **i** Recommendation:
> In VM2000 mode define precisely one LOCLAN device for each VM (in the case of SU /390 for each MU).

► In the tree structure select *Devices* → *<unit> (SU<model>)* → *BS2000 devices, LAN* tab.



Server Unit ABGSE211: LAN devices (IORSF file: #4, 2014-05-14 10:29:34)

| MN | HC | LUN | CHPID | Type | Details | BS2 IP address | BS2 MAC address | Unit | Unit type | Assigned | Status |
|---|---|---|---|---|---|---|---|---|---|---|---|
| *Filter* | *Filter* | *Filter* | *Filter* | *All* ▾ | *Filter* | *Filter* | *Filter* | *All* ▾ | *All* ▾ | *Filter* | *All* ▾ |
| | | | | LOCLAN | M2000 | 192.168.141.12 | 0A:00:14:10:40:FF | abgse2mu | MU | | - |
| | | | | LOCLAN | M2000 | 192.168.139.12 | 0A:00:14:10:20:FF | abgse2mu | MU | | - |
| | | | | LOCLAN | M2000 | 192.168.138.12 | 0A:00:14:10:10:FF | hnc1-se2 | MU | | - |
| | | | | LOCLAN | HNC | 192.168.152.12 | 0A:00:14:10:90:FF | hnc2-se2 | HNC | | - |
| | | | | LOCLAN | HNC | 192.168.151.12 | 0A:00:14:10:80:FF | hnc3-se2 | HNC | | - |
| CC40_CC41 | 00 | 40_41 | - | ZASLAN | s2 p0 pci | | 00:19:99:9C:77:C0 | hnc1-se2 | HNC | M4IVR | NORMAL |
| CC42_CC43 | 00 | 42_43 | - | ZASLAN | s2 p0 pci | | 00:19:99:9C:77:C1 | hnc1-se2 | HNC | G4IVQ | NORMAL |
| CC44_CC45 | 00 | 44_45 | - | ZASLAN | s2 p0 pci | | 00:19:99:9C:77:C2 | hnc1-se2 | HNC | G4IVP | NORMAL |
| CC46_CC47 | 00 | 46_47 | - | ZASLAN | s2 p0 pci | | 00:19:99:9C:77:C3 | hnc1-se2 | HNC | G4IVO | NORMAL |
| CC48_CC49 | 00 | 48_49 | - | ZASLAN | s2 p0 pci | | 00:19:99:9C:77:C4 | hnc1-se2 | HNC | G4IVJ | NORMAL |
| CC4A_CC4B | 00 | 4A_4B | - | ZASLAN | s2 p0 pci | | 00:19:99:9C:77:C5 | hnc1-se2 | HNC | | UNUSED |
| CC4C_CC4D | 00 | 4C_4D | - | ZASLAN | s2 p0 pci | | 00:19:99:9C:77:C6 | hnc1-se2 | HNC | | UNUSED |
| CC4E_CC4F | 00 | 4E_4F | - | ZASLAN | s2 p0 pci | | 00:19:99:9C:77:C7 | hnc1-se2 | HNC | | UNUSED |
| CC50_CC51 | 00 | 50_51 | - | ZASLAN | s2 p0 pci | | 00:19:99:9C:77:C8 | hnc1-se2 | HNC | G4IVN | NORMAL |
| CC52_CC53 | 00 | 52_53 | - | ZASLAN | s2 p0 pci | | 00:19:99:9C:77:C9 | hnc1-se2 | HNC | | UNUSED |
| CC54_CC55 | 00 | 54_55 | - | ZASLAN | s2 p0 pci | | 00:19:99:9C:77:CA | hnc1-se2 | HNC | | UNUSED |
| CC4E_CC4F | 00 | 4E_4F | - | ZASLAN | s2 p0 pci | | 00:19:99:9C:77:C7 | abgviolet | HNC | | UNUSED |

The *LAN* tab lists the configured LAN devices.

ℹ *Information on the generated LAN devices on SU /390*
The devices are displayed only if the IORSF file has the status "File transferred".

– Entries of the type IORSF display devices which are generated exclusively in the IORSF.
– Entries of the type LOCLAN and ZASLAN display the LAN devices already defined. If the device is also generated in the IORSF, a valid channel path identifier is displayed under CHPID. Otherwise only a warning icon is displayed under CHPID, and the device must still be generated (in BS2000 with /ADD-IO-UNIT).

ℹ In VM2000 mode the table contains an additional column: if a device assignment exists, the *Assigned* column displays the VM.

**The *LAN* tab offers the following functionality for managing the LAN devices:**

*Add new LAN device*

► Click *Add new LAN device*.

In the *Add LAN device* wizard you can specify the required properties of the LAN device step by step.

*Restart LAN device*

The restart allows you to rectify a problematical situation which affects the device.

► By the required device click the *Restart* icon and confirm the action.

*Adding a LAN device*

► Click the *Remove* icon by the required LAN device and confirm the action.

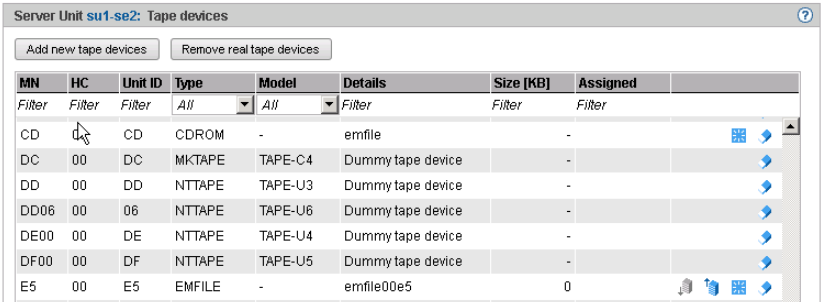
## 9.1.7 Managing tape devices

The *Tape devices* tab offers the following functionality for managing tape devices.

The *Tape devices* tab offers the following functionality for managing tape devices.

► Select *Devices → <unit name> (SU<model>) → BS2000 devices, Tape devices* tab.

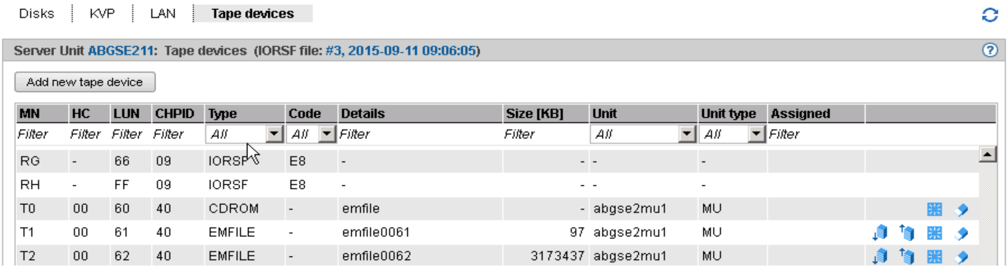
Example for SU x86:



Server Unit su1-se2: Tape devices

| MN | HC | Unit ID | Type | Model | Details | Size [KB] | Assigned |
|---|---|---|---|---|---|---|---|
| Filter | Filter | Filter | All | All | Filter | Filter | Filter |
| CD | 00 | CD | CDROM | - | emfile | - | |
| DC | 00 | DC | MKTAPE | TAPE-C4 | Dummy tape device | - | |
| DD | 00 | DD | NTTAPE | TAPE-U3 | Dummy tape device | - | |
| DD06 | 00 | 06 | NTTAPE | TAPE-U6 | Dummy tape device | - | |
| DE00 | 00 | DE | NTTAPE | TAPE-U4 | Dummy tape device | - | |
| DF00 | 00 | DF | NTTAPE | TAPE-U5 | Dummy tape device | - | |
| E5 | 00 | E5 | EMFILE | - | emfile00e5 | 0 | |

Example for SU /390:



Server Unit ABGSE211: Tape devices (IORSF file: #3, 2015-09-11 09:06:05)

| MN | HC | LUN | CHPID | Type | Code | Details | Size [KB] | Unit | Unit type | Assigned |
|---|---|---|---|---|---|---|---|---|---|---|
| Filter | Filter | Filter | Filter | All | All | Filter | Filter | All | All | Filter |
| RG | - | 66 | 09 | IORSF | E8 | - | - | - | - | |
| RH | - | FF | 09 | IORSF | E8 | - | - | - | - | |
| T0 | 00 | 60 | 40 | CDROM | - | emfile | - | abgse2mu1 | MU | |
| T1 | 00 | 61 | 40 | EMFILE | - | emfile0061 | 97 | abgse2mu1 | MU | |
| T2 | 00 | 62 | 40 | EMFILE | - | emfile0062 | 3173437 | abgse2mu1 | MU | |

The *Tape devices* tab lists the configured tape devices. EMFILEs without a tape assignment are displayed with the type DATA.

ℹ *Information on the generated tape devices on SU /390*

The devices are displayed only if the IORSF file has the status "File transferred".

– Entries of the type IORSF display devices which are generated exclusively in the IORSF.
– Entries of the type EMFILE, CDROM, and DATA display the emulated tape devices already defined. If the device is also generated in the IORSF, a valid channel path identifier is displayed under CHPID. Otherwise only a warning icon is displayed under CHPID, and the device must still be generated (in BS2000 with /ADD-IO-UNIT).

ℹ In VM2000 mode the table contains an additional column: if a device assignment exists, the *Assigned* column displays the VM.

**The *Tape devices* tab offers the following functionality for managing the tape devices:**

*Add new tape devices*

► Click *Add new tape devices*.

In the *Add new tape devices* wizard you can specify the required properties and - in the case of real tape devices of an SU x86 - the required number of tape devices.

*Remove real tape devices (SU x86 only)*

► Click *Remove real tape devices*.

In the *Remove real tape devices* wizard you can specify an interval of MNs for the real tape devices to be removed.

*Restart tape device*

The restart allows you to rectify a problematical situation which affects the device.

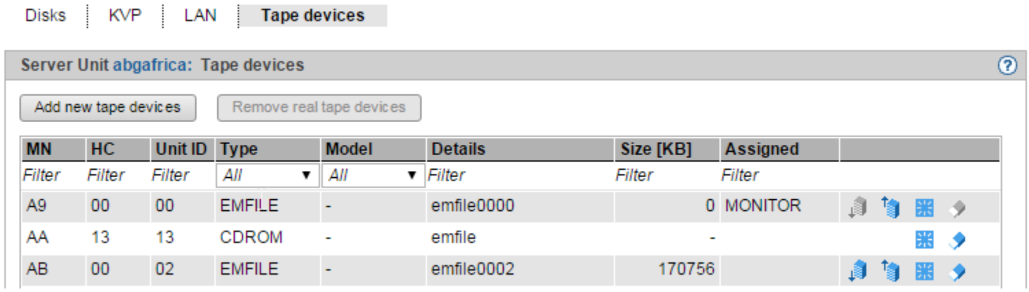
► By the required device click the *Restart* icon and confirm the action.

*Remove tape device*

► Click the *Remove* icon in the row with the required tape device and confirm the action.

### 9.1.7.1 Emulated tape devices

You manage emulated tape devices using the *Tape devices* tab of the SU /390 or SU x86, see the example below for an SU x86:



| MN | HC | Unit ID | Type | Model | Details | Size [KB] | Assigned |
|---|---|---|---|---|---|---|---|
| Filter | Filter | Filter | All ▼ | All ▼ | Filter | Filter | Filter |
| A9 | 00 | 00 | EMFILE | - | emfile0000 | 0 | MONITOR |
| AA | 13 | 13 | CDROM | - | emfile | - | |
| AB | 00 | 02 | EMFILE | - | emfile0002 | 170756 | |

The SE Manager supports the configuration of emulated tape devices. Emulation enables BS2000 tapes to be presented either as files in the Linux file system (EMFILEs) or as files on CD or DVD (CDROM files). This permits data exchange between BS2000 systems by means of compatible EMFILEs or CDROM files. With the help of the EMFILEs/CDROM files, you can, for example, read in BS2000 correction packages from CD or DVD or transfer files containing diagnostic data by means of CD, DVD or LAN. Another possible application is exporting BS2000 data temporarily to the Linux file system.

It is also possible to write CDROM files directly to a CD/DVD medium on the SU x86's integrated DVD burner. For the SU /390 this can be done on the MU's integrated DVD burner.

Data CDs and DVDs written in ISO9660 or UDF format and containing precisely one file with the name *emfile* are supported.

i You can replace EMFILEs/CDROM files with EMFILEs/CDROM files of other servers (SQ servers). The data formats of the EMFILEs/CDROM files on these servers are compatible.

You can upload and download EMFILEs, and remove emulated tape files.

*Download*

When you initiate a download, the tape device in BS2000 should not be attached, i.e. if necessary a DETACH command should be issued first.

► Click the *Download* icon by the required tape device, enter the path and file names in the system-specific Explorer window and save the file.

*Upload*

When you initiate an upload, the tape drive in BS2000 should not be attached, i.e. if necessary a DETACH command should be issued first.

A download enables EMFILEs to be stored in a different place and an upload enables them to be read in again later. This also permits files to be exchanged with other systems. The names of files to be downloaded must comply with the conventions for EMFILE names. Existing files of the same name are overwritten when files are uploaded.

► Click the *Upload* icon by the required tape device, select the file in the dialog box, and click *Upload*.

*Remove*

When you delete data, the tape drive in BS2000 should not be attached, i.e. if necessary a DETACH command should be issued first.

► Click the *Remove* icon by the required tape device and confirm the action.

In the case of an emulated tape device you can select in the dialog box whether you want to remove the device and/or whether you want to delete the EMFILE. If you only remove the device, the data is subsequently displayed with the device type DATA.

### 9.1.7.2 Emulated tape devices from the BS2000 viewpoint

Instead of the EMFILEs and CDROM files, BS2000 sees tape devices of the type BM1662FS which are addressed by means of their mnemonics. In the drives tapes of the type T6250 (T9G) are visible which are addressed using their VSNs and are handled in the same way.

#### EMFILEs

The following BS2000 commands are relevant for tape drives which are emulated by EMFILEs:

ATTACH-DEVICE
Attaches a tape device; mandatory before use.

DETACH-DEVICE
Detaches a tape device. The actions uploading, downloading, deletion of the data, and removal of the emulated device via the SE Manager only make sense in the “detached” status.

INIT utility routine
Initialization of a tape using the INIT utility routine; mandatory if a new EMFILE emulates a tape. For details, see the "Utility Routines" manual [10]. Specify “T9G” as the volume type and define the VSN.

#### CDROM files

The following BS2000 commands are relevant for tape devices which are emulated by CDROM files:

ATTACH-DEVICE
Attaches a tape device; mandatory before use. Even if the CD or DVD drive is empty, the corresponding tape device can be attached in BS2000. When you have inserted a CD/DVD later, enter the CHECK-TAPE command to make the mounted volume known to BS2000.

CHECK-TAPE
Makes a mounted volume (CD/DVD) in the emulated tape drive known to BS2000. The CHECK-TAPE command is needed if the drive was still empty when a previous ATTACH command was issued or the CD/DVD was changed after UNLOAD-TAPE.

DETACH-DEVICE

Detaches a tape device. Access to the CD drive from Linux is forbidden while the device concerned is attached in BS2000. After it has been detached, any CD still contained in the drive can be ejected by pressing the button on the drive.

UNLOAD-TAPE

Burns a CD or DVD, which is then ejected.

INIT utility routine

Initialization of a volume by the INIT utility routine; mandatory when a CD/DVD straight from the factory is inserted. For details, see the “Utility Routines” manual [10]. Specify “T9G” as the volume type and define the VSN. If the CD/DVD is rewritable, any existing data is overwritten.
You use the ERASE operand in the INIT statement to initiate complete deletion of a rewritable CD/DVD.

### Procedure for burning a CD/DVD

Proceed as follows to burn a CD or DVD in the drive of the MU or SU x86:

- ► Initialize the CDROM file using the INIT utility routine and specify a VSN in the process.
- ► Make the CD or DVD known to BS2000: ATTACH-DEVICE or (if that has already been issued) CHECK-TAPE
- ► Write the CDROM file with BS2000 means.
  All data on a rewritable medium is deleted here.
- ► Write the CDROM file with BS2000 means.
  This file is initially buffered on hard disk. The buffered file must contain more than 5 tape blocks, and the data must be terminated with a double tape mark (indicating the logical end of a BS2000 tape).
  The buffered data is retained until it is deleted when initialization takes place again (INIT) or until a data medium is written for this drive again.
- ► Burn another CD/DVD using the UNLOAD-TAPE command.

  After the medium has been burned, it is ejected from the DVD burner (i.e. the drive opens).
- ► Burn another CD/DVD or detach the device (DETACH-DEVICE).

### CD/DVD media supported

The following media are supported for the burning functionality:

- CD-R
- DVD-RW / DVD+RW
- DVDRAM
- DVD-RW / DVD+RW
- DVDRAM

The end-of-tape processing depends on the size of the medium. The maximum net size of the CDROM file is 4200 MB and is correspondingly lower in the case of a smaller medium since the space for the table of contents and lead-in / lead-out is deducted (CD: up to 32 MB / DVD: up to 128 MB).

### Times of different CD/DVD media

The burning times (or initialization times) depend on the medium used and the possible speed for burning/deleting. The table below provides some information for estimating roughly how long the procedure will take (tests with a few different media).

| **Medium** | **Time** | | |
|---|---|---|---|
| | INIT | INIT ... ERASE | UNLOAD-TAPE (burn) |
| DVD-R 8x | 2 sec | - | 11 min (4200 MB) |
| CD-R 52x | 2 sec | - | 7 min (650 MB) |
| CD-RW 4x-10x | 130 sec | 10 min | 10 min (650 MB) |
| DVD+RW 1x-4x | 30 sec | 16 min | 15 min (4200 MB) |
| DVDRAM 3x-20x | 20 sec | 40 min | 37 min (4200 MB) |

## 9.2 Managing XenVM devices on Server Unit x86

The various device-specific functions and tasks are described below:

- Managing disk pools
- Managing virtual disks
- Managing virtual switches
- Managing installation sources

With these functions you make XenVM devices available for use by XenVMs. You can make changes for individual devices, delete them, and also add new individual devices.

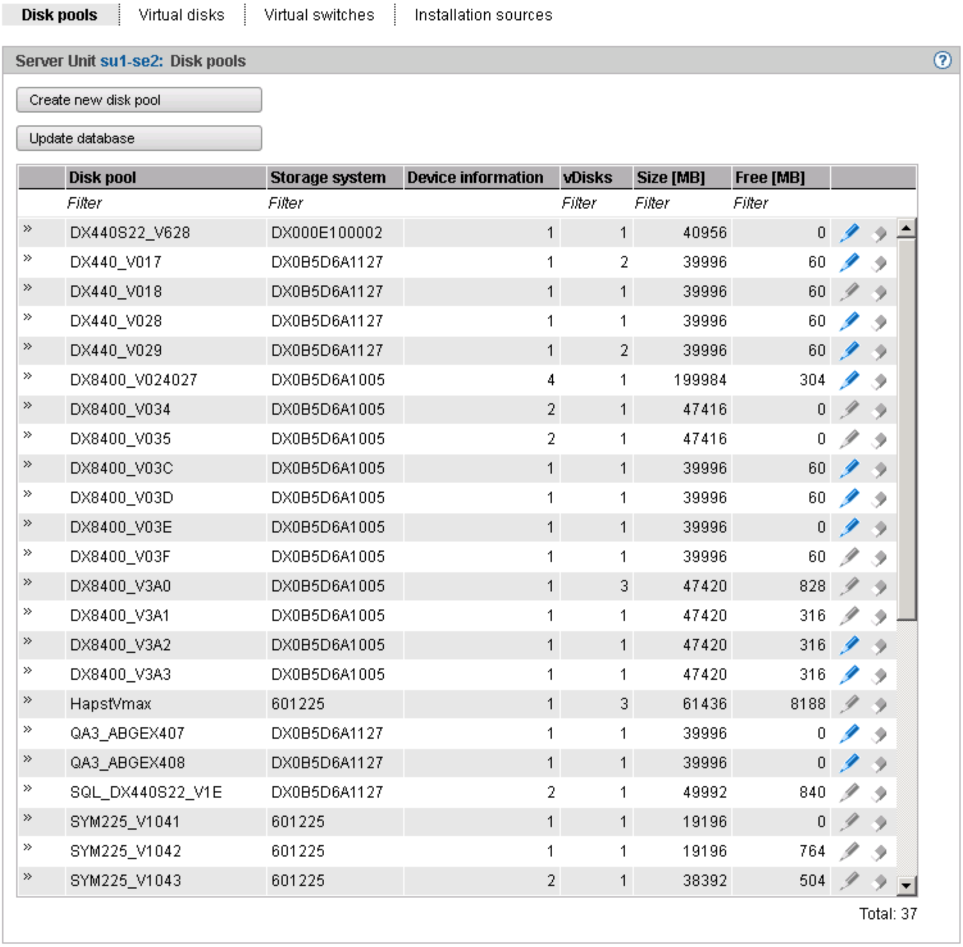
XenVM devices are initially assigned to a XenVM when the XenVM is created. Further devices can be assigned or removed using the XenVM-specific menu.

### 9.2.1 Managing disk pools

Disk pools with free storage space are required to create or expand the capacity of virtual disks. For details, see section “Managing virtual disks”.

The *Disk pools* tab provides the following functions:

► Select *Devices* → *<unit> (SU<x86>)* → *XenVM devices* → *XenVM*, *Disk pools* tab.



**Disk pools** | Virtual disks | Virtual switches | Installation sources

Server Unit su1-se2: Disk pools

Create new disk pool

Update database

| | Disk pool | Storage system | Device information | vDisks | Size [MB] | Free [MB] |
|---|---|---|---|---|---|---|
| | *Filter* | *Filter* | | *Filter* | *Filter* | *Filter* |
| » | DX440S22_V628 | DX000E100002 | 1 | 1 | 40956 | 0 |
| » | DX440_V017 | DX0B5D6A1127 | 1 | 2 | 39996 | 60 |
| » | DX440_V018 | DX0B5D6A1127 | 1 | 1 | 39996 | 60 |
| » | DX440_V028 | DX0B5D6A1127 | 1 | 1 | 39996 | 60 |
| » | DX440_V029 | DX0B5D6A1127 | 1 | 2 | 39996 | 60 |
| » | DX8400_V024027 | DX0B5D6A1005 | 4 | 1 | 199984 | 304 |
| » | DX8400_V034 | DX0B5D6A1005 | 2 | 1 | 47416 | 0 |
| » | DX8400_V035 | DX0B5D6A1005 | 2 | 1 | 47416 | 0 |
| » | DX8400_V03C | DX0B5D6A1005 | 1 | 1 | 39996 | 60 |
| » | DX8400_V03D | DX0B5D6A1005 | 1 | 1 | 39996 | 60 |
| » | DX8400_V03E | DX0B5D6A1005 | 1 | 1 | 39996 | 0 |
| » | DX8400_V03F | DX0B5D6A1005 | 1 | 1 | 39996 | 60 |
| » | DX8400_V3A0 | DX0B5D6A1005 | 1 | 3 | 47420 | 828 |
| » | DX8400_V3A1 | DX0B5D6A1005 | 1 | 1 | 47420 | 316 |
| » | DX8400_V3A2 | DX0B5D6A1005 | 1 | 1 | 47420 | 316 |
| » | DX8400_V3A3 | DX0B5D6A1005 | 1 | 1 | 47420 | 316 |
| » | HapstVmax | 601225 | 1 | 3 | 61436 | 8188 |
| » | QA3_ABGEX407 | DX0B5D6A1127 | 1 | 1 | 39996 | 0 |
| » | QA3_ABGEX408 | DX0B5D6A1127 | 1 | 1 | 39996 | 0 |
| » | SQL_DX440S22_V1E | DX0B5D6A1127 | 2 | 1 | 49992 | 840 |
| » | SYM225_V1041 | 601225 | 1 | 1 | 19196 | 0 |
| » | SYM225_V1042 | 601225 | 1 | 1 | 19196 | 764 |
| » | SYM225_V1043 | 601225 | 2 | 1 | 38392 | 504 |

Total: 37

The *Disk pools* tab displays the existing disk pools together with their properties.

**The *Disk pools* tab offers the following functionality for managing disk pools:**

*Creating a disk pool*

XenVMs use disk pools to create virtual disks.

ℹ If a free physical disk (a free node) is selected when a disk pool is created or extended, despite the database having been updated it can occur that the disk is not yet free and the action will fail with a reference to a remote application. This can happen, for example, when the storage system is also used by another Linux system and the disks there are managed using means of the basic software Logical Volume Manager.

► Click *Create new disk pool* (above the table of disk pools).

In the *Create disk pool* wizard you can specify the required properties of the disk pool step by step.

*Updating the database for virtual disks*

When various servers access a disk storage system, it can make sense to update the administrative copy of the database for the virtual disks on the Server Unit of the SE server.

► Click *Update database* (above the table of disk pools) and confirm the action.

The database for the virtual disks will be updated and the current inventory of virtual disks displayed.

*Extending a disk pool*

You can extend a disk pool when it no longer has enough free storage space for further virtual disks. In this case you assign the disk pool another physical disk which provides the storage space required.

► Click the *Change* icon by the required disk pool and extend the pool by the physical disk.

*Deleting a disk pool*

ℹ You can delete a disk pool only if it contains no virtual disk.

► Click the *Delete* icon by the required disk pool and confirm the action.

The disk pool selected is deleted immediately. The physical disks which were assigned to the disk pool are once more freely available.

## 9.2.2 Managing virtual disks

A virtual disk is a section of a disk pool which is seen as a uniform and contiguous disk by the XenVM which uses it. When you create or extend a disk pool, you assign the pool one or more physical volumes of a disk storage system.

When you create or extend a disk pool, you assign the pool one or more physical volumes of a disk storage system.

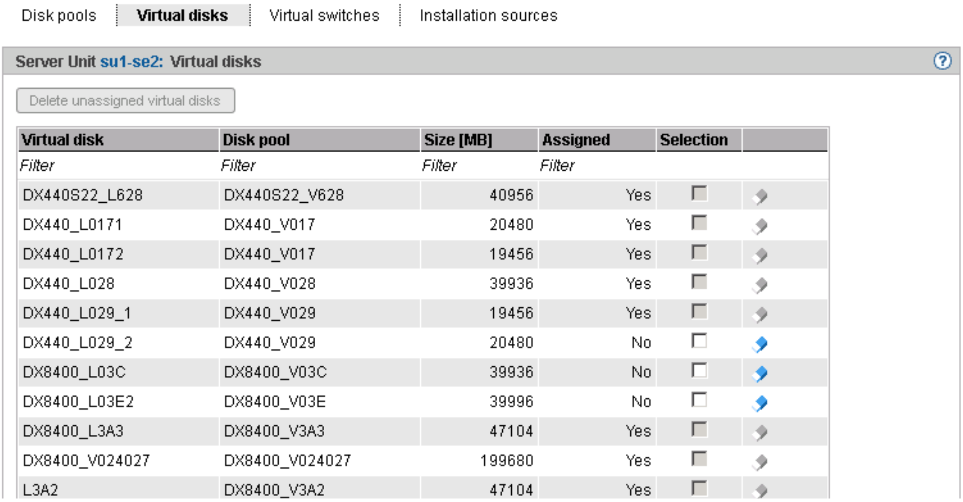
A disk pool corresponds to a volume of the disk storage system.

Virtual disk creation always involves them being assigned immediately to a XenVM (in the XenVM-specific menu, see page 126).
When a XenVM is deleted, the assigned virtual disks can also optionally be deleted. If the disks are not also deleted, they remain available as free virtual disks.

The *Virtual disks* tab provides the following functions:

- Displaying information about all virtual disks
- Deleting unassigned disks

► Select *Devices → <unit> (SU<x86>) → XenVM devices → XenVM, Virtual disks* tab.



Disk pools | **Virtual disks** | Virtual switches | Installation sources

Server Unit su1-se2: Virtual disks

Delete unassigned virtual disks

| Virtual disk | Disk pool | Size [MB] | Assigned | Selection | |
|---|---|---|---|---|---|
| *Filter* | *Filter* | *Filter* | *Filter* | | |
| DX440S22_L628 | DX440S22_V628 | 40956 | Yes | □ | |
| DX440_L0171 | DX440_V017 | 20480 | Yes | □ | |
| DX440_L0172 | DX440_V017 | 19456 | Yes | □ | |
| DX440_L028 | DX440_V028 | 39936 | Yes | □ | |
| DX440_L029_1 | DX440_V029 | 19456 | Yes | □ | |
| DX440_L029_2 | DX440_V029 | 20480 | No | □ | |
| DX8400_L03C | DX8400_V03C | 39936 | No | □ | |
| DX8400_L03E2 | DX8400_V03E | 39996 | No | □ | |
| DX8400_L3A3 | DX8400_V3A3 | 47104 | Yes | □ | |
| DX8400_V024027 | DX8400_V024027 | 199680 | Yes | □ | |
| L3A2 | DX8400_V3A2 | 47104 | Yes | □ | |

The *Virtual disks* tab displays information on all **virtual disks**. If multiple assignments exist, these are displayed under *Assigned*.

The *Virtual disks* tab offers the following functionality for managing virtual disks:

*Deleting unassigned disks*

When unassigned disks are no longer required, you can delete them. This increases the free storage space for creating new virtual disks in the disk pool concerned. You can delete unassigned disks either individually or by selecting more than one disk:

– *Deleting individual disks*

► Click the *Delete* icon by the required unassigned disk and confirm the action.

The selected virtual disk is deleted immediately.

– *Deleting a selection of disks*

► In all rows with unassigned disks which are to be deleted, enable the selection field in the *Selection* column. Click *Delete unassigned virtual disks* (above the table) and confirm the action.

The selected virtual disks are deleted immediately.

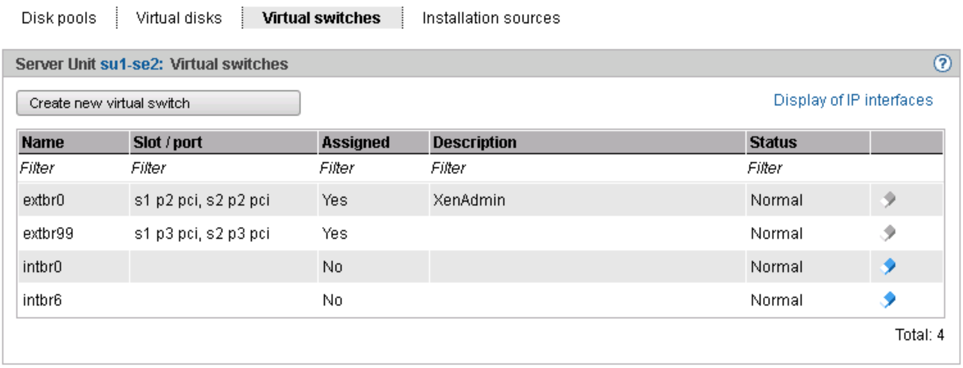
## 9.2.3 Managing virtual switches

For the network connection of a XenVM you configure a virtual Network Interface Card and assign the connection to a virtual switch. The virtual switch presents the connection to a network. Depending on the type of network connection required, different types of virtual switches are needed:

- An **internal** virtual switch permits a local protected communication link for the XenVMs attached to it. These switches can also be used by the BS2000 Native system or by BS2000 VMs for communicating with XenVMs.
- An **external** virtual switch is assigned to a LAN interface which permits an external LAN connection. The XenVMs connected to it share this connection for communicating with external systems.
  If more than one unused LAN interface is available, an external vSwitch can also be assigned to two LAN interfaces. In this case the XenVM connections can be distributed to the two interfaces (also referred to as “bonds”). This redundant configuration is designed to ensure the high availability of the LAN connection.
  External switches use the LAN interface exclusively.

### Displaying configured virtual switches

► Select *Devices → <unit> (SU<x86>) → XenVM devices → XenVM, Virtual switches* tab.



Server Unit su1-se2: Virtual switches

| Name | Slot / port | Assigned | Description | Status | |
|---|---|---|---|---|---|
| *Filter* | *Filter* | *Filter* | *Filter* | *Filter* | |
| extbr0 | s1 p2 pci, s2 p2 pci | Yes | XenAdmin | Normal | ✎ |
| extbr99 | s1 p3 pci, s2 p3 pci | Yes | | Normal | ✎ |
| intbr0 | | No | | Normal | ✎ |
| intbr6 | | No | | Normal | ✎ |

Total: 4

The *Virtual switches* tab displays all the virtual switches.

The tab offers the following functionality for managing the virtual switches:

*Creating a virtual switch*

► Click *Create new virtual switch* (above the table).

In the *Create virtual switch* wizard you can specify the required properties of the virtual switch step by step.

The virtual switch is created and then displayed in the table of virtual switches. You can now use this virtual switch to configure virtual Network Interface Cards.

*Removing a virtual switch*

You can remove a virtual switch from the configuration if it is not used for network connections. This means that no virtual Network Interface Cards may be assigned to the switch.

► Click the *Delete* icon by the required virtual switch and confirm the action.

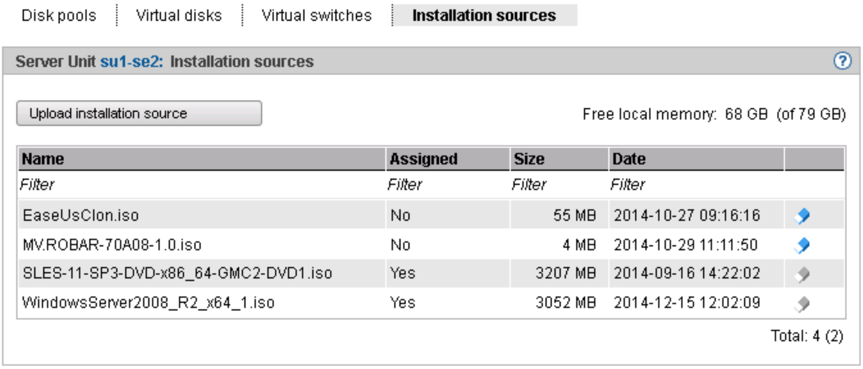
The selected virtual switch is immediately removed from the configuration. In the case of an external virtual switch, the assigned LAN interfaces are once more freely available.

## 9.2.4 Managing installation sources

A medium (CD or DVD) from which the operating system for a XenVM can be installed is available on the Server Unit in file form as an installation source.
Installation sources are either ISO image files (suffix **iso**) or installation configuration files (in the case of SLES e.g. AutoYAST-XML files). The administrator or XenVM administrator manages these files in a local library on the Server Unit.

When a XenVM is installed, a virtual DVD drive must be configured which reads in the data from the installation medium, i.e. from an installation source (see “Assign installation source” on page 130).

- Select *Devices → <unit> (SU<x86>) → XenVM devices → XenVM, Installation sources* tab.


Disk pools
Virtual disks
Virtual switches
Installation sources
Server Unit su1-se2: Installation sources
?
Upload installation source

Free local memory: 68 GB (of 79 GB)

| Name | Assigned | Size | Date | |
|---|---|---|---|---|
| *Filter* | *Filter* | *Filter* | *Filter* | |
| EaseUsClon.iso | No | 55 MB | 2014-10-27 09:16:16 | |
| MV.ROBAR-70A08-1.0.iso | No | 4 MB | 2014-10-29 11:11:50 | |
| SLES-11-SP3-DVD-x86_64-GMC2-DVD1.iso | Yes | 3207 MB | 2014-09-16 14:22:02 | |
| WindowsServer2008_R2_x64_1.iso | Yes | 3052 MB | 2014-12-15 12:02:09 | |

Total: 4 (2)

The *Installation sources* tab displays the installation sources available.

The *Installation sources* tab provides the following functions:

*Delete installation source*

You can delete an installation source only if it is not assigned to a XenVM.

- Click the *Delete* icon by the required installation source and confirm the action.

*Upload installation source*

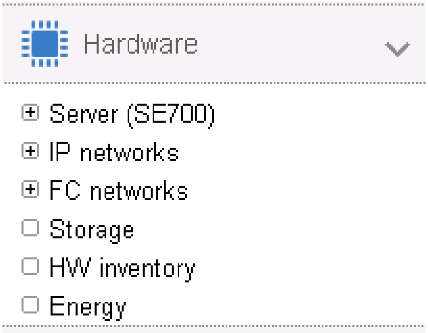
As a XenVM cannot access the Server Unit’s physical DVD drive, direct installation from a CD/DVD is not possible. However, the SE Manager offers the option of uploading an ISO image file from the PC to the local library as an information source.

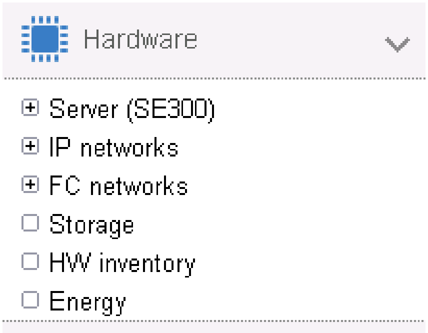
- Click *Upload information source* and select the required ISO image file in the browser dialog box.

After the update, the updated table displays the newly create ISO image file as an installation source in the local library.

# 10 Managing hardware

You manage the hardware of the SE server using the *Hardware* menu in the tree structure, see the examples of an SE700 and an SE300 below:





The menu has the same layout for all SE servers and contains the following items:

- *Server (SE<model>)*: Here you manage all existing units of the SE server, see section "Managing units of the SE server" on page 184.
- *IP networks*: Here you manage all private and public networks of the SE server, see section "Managing IP networks" on page 233.
- *FC networks*: Here you manage the Fibre Channel networks of the SE server, see section "Managing FC networks" on page 255.
- *Storage*: Here you manage the storage components which are integrated into the SE server, see section "Managing storage systems" on page 258.
- *HW inventory*: Here you can have the hardware configuration displayed on the screen in graphic or tabular form, see section "HW inventory" on page 260.
- *Energy*: Here you manage the energy settings of the SE server, e.g. powering the units on or off automatically, see section "Managing energy settings" on page 265.

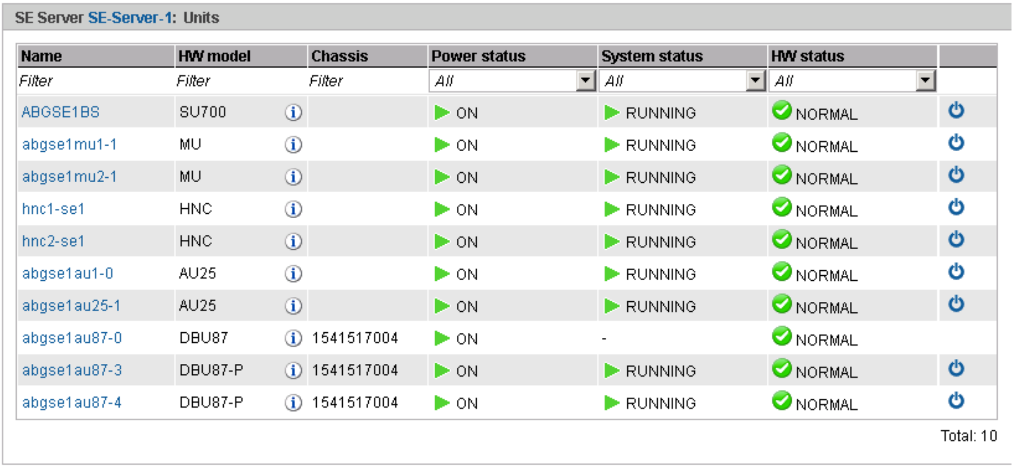
# 10.1 Managing units of the SE server

You manage the units of the SE server using the menu *Hardware → Server (SE<model>)*. When you expand this menu, all the existing units are listed.

## 10.1.1 Powering a unit on or off, rebooting a unit

- ► Select *Hardware* and click *Server (SE<model>)*.

  The *Units* tab displays information on all Management Units, Server Units, HNCs, and Application Units of the SE server.



SE Server SE-Server-1: Units

| Name | HW model | | Chassis | Power status | System status | HW status | |
|---|---|---|---|---|---|---|---|
| Filter | Filter | | Filter | All | All | All | |
| ABGSE1BS | SU700 | ⓘ | | ▶ ON | ▶ RUNNING | ✓ NORMAL | ⏻ |
| abgse1mu1-1 | MU | ⓘ | | ▶ ON | ▶ RUNNING | ✓ NORMAL | ⏻ |
| abgse1mu2-1 | MU | ⓘ | | ▶ ON | ▶ RUNNING | ✓ NORMAL | ⏻ |
| hnc1-se1 | HNC | ⓘ | | ▶ ON | ▶ RUNNING | ✓ NORMAL | ⏻ |
| hnc2-se1 | HNC | ⓘ | | ▶ ON | ▶ RUNNING | ✓ NORMAL | ⏻ |
| abgse1au1-0 | AU25 | ⓘ | | ▶ ON | ▶ RUNNING | ✓ NORMAL | ⏻ |
| abgse1au25-1 | AU25 | ⓘ | | ▶ ON | ▶ RUNNING | ✓ NORMAL | ⏻ |
| abgse1au87-0 | DBU87 | ⓘ | 1541517004 | ▶ ON | - | ✓ NORMAL | |
| abgse1au87-3 | DBU87-P | ⓘ | 1541517004 | ▶ ON | ▶ RUNNING | ✓ NORMAL | ⏻ |
| abgse1au87-4 | DBU87-P | ⓘ | 1541517004 | ▶ ON | ▶ RUNNING | ✓ NORMAL | ⏻ |

Total: 10

i If, as in the example, at least one AU87 or DBU87 is available, *HW model* is followed by an additional *Chassis* column. In the case of AU87 or DBU87, the chassis of the AU and the partitions are each displayed as single units. Actions are only possible for partitions.

Depending on the status, you use the *Units* tab to power a unit on or off or reboot it. Depending on the unit type, the following actions are possible:

| Unit type | Power on | Reboot | Shutdown | Power off immediately |
|---|---|---|---|---|
| MU | X | X | X | X |
| SU /390 | X | | | X |
| SU x86 | X | X | X | X |
| HNC | X | X | X | X |
| AU | X | | X | X |

### Powering on the unit

*Requirement*

The unit is switched off (POWER OFF status).

*Procedure*

► Click the *Power on* icon by the required unit and confirm the action with *Execute* in the subsequent dialog box.

The powered-off unit is powered on. You will receive a message when the operation has been completed.

### Rebooting a unit (MU, SU x86 and HNC only)

*Requirement*

You can reboot a unit only when the unit is accessible, i.e. the *HW status* is not *NOT_ACCESSIBLE*.

i When you reboot the local MU, the connection in the SE Manager is cleared down. You must log in again after the rebooting the MU.

*Procedure*

► Click the *Power off* icon by the required unit.

► In the subsequent dialog box, select *Reboot* and confirm the action with *Execute.*

The unit is rebooted. You will receive a message when the operation has been completed.

### Shutting down the unit or immediately powering it off

*Requirement*

You can power off a unit only when the unit is accessible, i.e. the *HW status* is not *NOT_ACCESSIBLE*.

*Procedure*

► Click the *Power off* icon by the required unit.

► In the dialog box which then appears, select the option *Shut down* or *Power off immediately* and confirm the action with *Execute.*

i Only *Power off immediately* is available for the SU /390.

The unit is shut down or powered off immediately. You will receive a message when the operation has been completed.

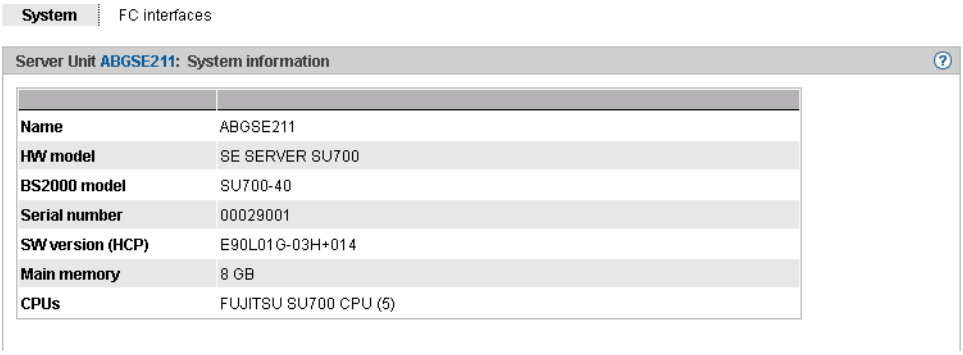
## 10.1.2 Managing the Server Unit /390

### 10.1.2.1 Displaying system information and interfaces of the SU /390

You obtain the system information and interfaces of the SU /390 using the associated *Information* menu.

#### Displaying system information of the SU /390

- ► Select *Hardware* → *Server (SE<model>)* → *<unit> (SU</390>)* → *Information*, *System* tab.

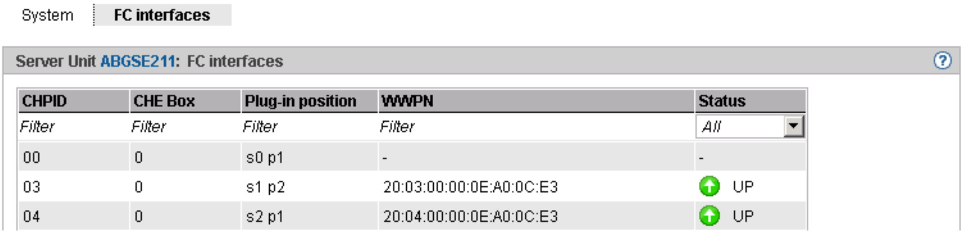


Server Unit ABGSE211: System information

| | |
|---|---|
| **Name** | ABGSE211 |
| **HW model** | SE SERVER SU700 |
| **BS2000 model** | SU700-40 |
| **Serial number** | 00029001 |
| **SW version (HCP)** | E90L01G-03H+014 |
| **Main memory** | 8 GB |
| **CPUs** | FUJITSU SU700 CPU (5) |

#### Displaying FC interfaces of the SU /390

- ► Select *Hardware* → *Server (SE<model>)* → *<unit> (SU</390>)* → *Information*, *FC interfaces* tab.



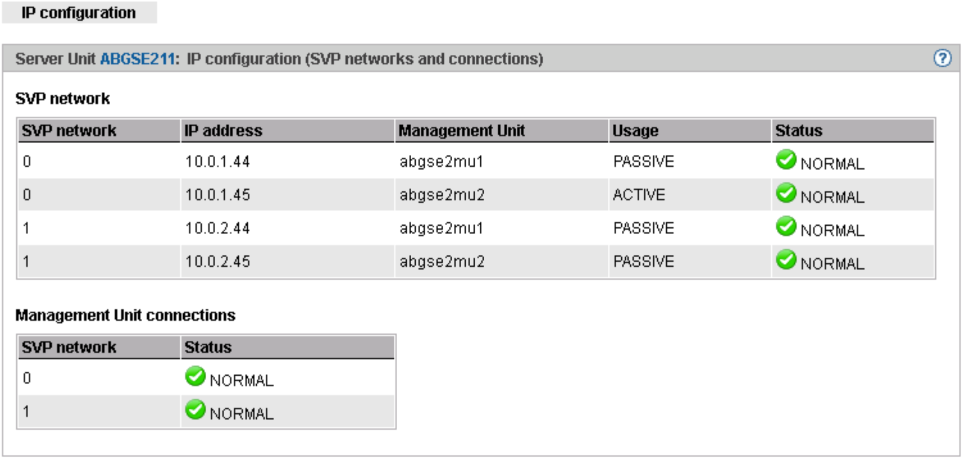
Server Unit ABGSE211: FC interfaces

| CHPID | CHE Box | Plug-in position | WWPN | Status |
|---|---|---|---|---|
| *Filter* | *Filter* | *Filter* | *Filter* | *All* |
| 00 | 0 | s0 p1 | - | - |
| 03 | 0 | s1 p2 | 20:03:00:00:0E:A0:0C:E3 | UP |
| 04 | 0 | s2 p1 | 20:04:00:00:0E:A0:0C:E3 | UP |

### 10.1.2.2 Displaying the IP configuration of the SU /390

The IP configuration of the SU /390 is displayed using the associated *Management* menu. The *IP configuration* tab displays information on SVP networks and connections:

► Select *Hardware* → *Server (SE<model>)* → *<unit> (SU</390>)* → *Management*, *IP configuration* tab.



Server Unit ABGSE211: IP configuration (SVP networks and connections)

SVP network

| SVP network | IP address | Management Unit | Usage | Status |
|---|---|---|---|---|
| 0 | 10.0.1.44 | abgse2mu1 | PASSIVE | ✓ NORMAL |
| 0 | 10.0.1.45 | abgse2mu2 | ACTIVE | ✓ NORMAL |
| 1 | 10.0.2.44 | abgse2mu1 | PASSIVE | ✓ NORMAL |
| 1 | 10.0.2.45 | abgse2mu2 | PASSIVE | ✓ NORMAL |

Management Unit connections

| SVP network | Status |
|---|---|
| 0 | ✓ NORMAL |
| 1 | ✓ NORMAL |

## 10.1.3 Managing the Management Unit

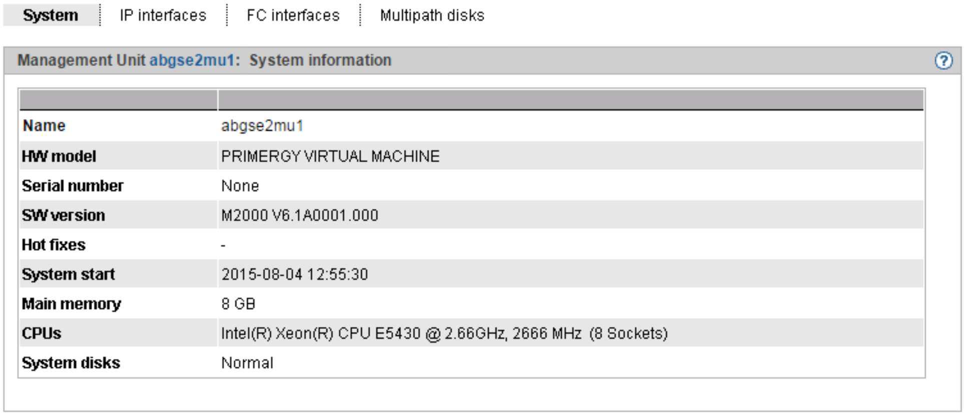
### 10.1.3.1 Displaying system information and interfaces of the Management Unit

You obtain the system information and interfaces of the Management Unit using the associated *Information* menu. Options provided in this menu:

- Displaying system information of the MU
- Displaying FC interfaces of the MU
- Displaying and changing IP interfaces of the MU

### Displaying system information of the MU

► Select *Hardware* → *Server (SE<model>)* → *<unit> (MU)* → *Information*, *System* tab:



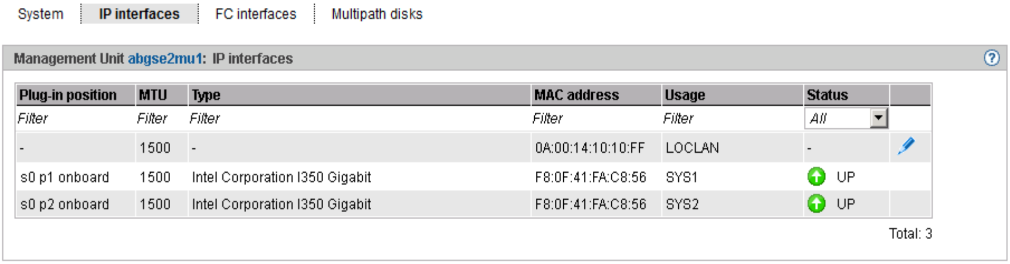
Management Unit abgse2mu1: System information

| | |
|---|---|
| **Name** | abgse2mu1 |
| **HW model** | PRIMERGY VIRTUAL MACHINE |
| **Serial number** | None |
| **SW version** | M2000 V6.1A0001.000 |
| **Hot fixes** | - |
| **System start** | 2015-08-04 12:55:30 |
| **Main memory** | 8 GB |
| **CPUs** | Intel(R) Xeon(R) CPU E5430 @ 2.66GHz, 2666 MHz (8 Sockets) |
| **System disks** | Normal |

In the case of *System disks*, *Normal* means that the mirror disk is decoupled. *In maintenance* means that the mirror is active for the system disks, and the data is being synchronized (in preparation for a software update).

### Displaying and changing IP interfaces of the MU

► Select *Hardware → Server (SE<model>) → <unit> (MU) → Information*, *IP interfaces* tab:



Management Unit abgse2mu1: IP interfaces

| Plug-in position | MTU | Type | MAC address | Usage | Status | |
|---|---|---|---|---|---|---|
| Filter | Filter | Filter | Filter | Filter | All | |
| - | 1500 | - | 0A:00:14:10:10:FF | LOCLAN | - | ✎ |
| s0 p1 onboard | 1500 | Intel Corporation I350 Gigabit | F8:0F:41:FA:C8:56 | SYS1 | ● UP | |
| s0 p2 onboard | 1500 | Intel Corporation I350 Gigabit | F8:0F:41:FA:C8:56 | SYS2 | ● UP | |

Total: 3

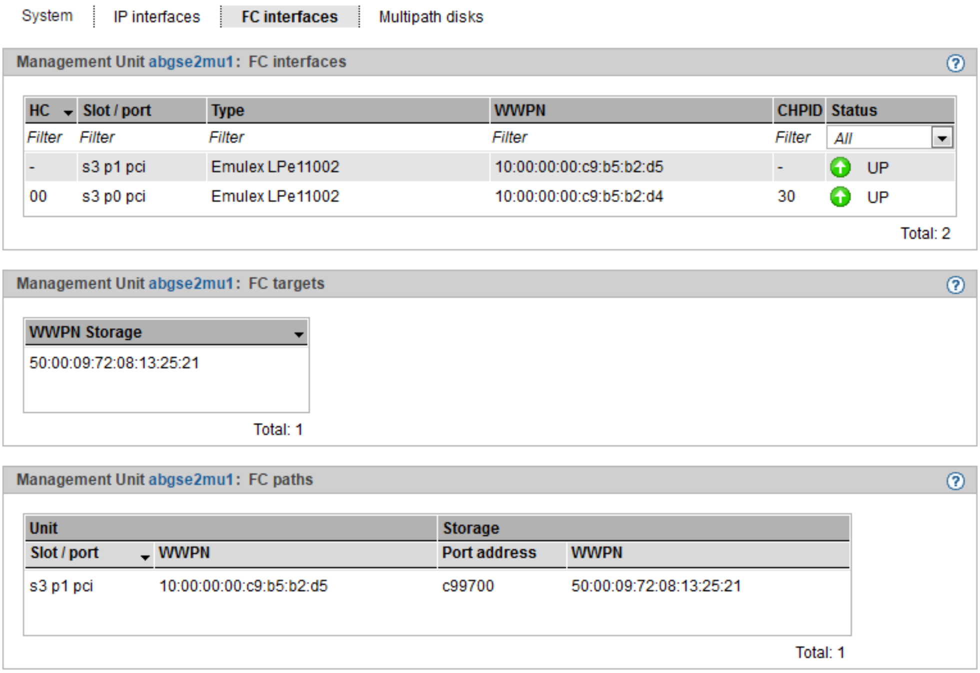
*Changing the packet length in the case of LOCLAN and PCI interfaces*

In the *IP interfaces* tab of the Management Unit you can change the packet length. In the case of a PCI interface, normal operation is required for this purpose, i.e. the *Status UP* is displayed.

► Click the *Change* icon in the row with the required IP interface, and in the subsequent dialog box select the required packet length.

### Displaying FC interfaces of the MU

► Select *Hardware → Server (SE<model>) → <unit> (MU) → Information*, *FC interfaces* tab:



Management Unit abgse2mu1: FC interfaces

| HC | Slot / port | Type | WWPN | CHPID | Status |
|---|---|---|---|---|---|
| Filter | Filter | Filter | Filter | Filter | All |
| - | s3 p1 pci | Emulex LPe11002 | 10:00:00:00:c9:b5:b2:d5 | - | UP |
| 00 | s3 p0 pci | Emulex LPe11002 | 10:00:00:00:c9:b5:b2:d4 | 30 | UP |

Total: 2

Management Unit abgse2mu1: FC targets

| WWPN Storage |
|---|
| 50:00:09:72:08:13:25:21 |

Total: 1

Management Unit abgse2mu1: FC paths

| Unit | | Storage | |
|---|---|---|---|
| Slot / port | WWPN | Port address | WWPN |
| s3 p1 pci | 10:00:00:00:c9:b5:b2:d5 | c99700 | 50:00:09:72:08:13:25:21 |

Total: 1

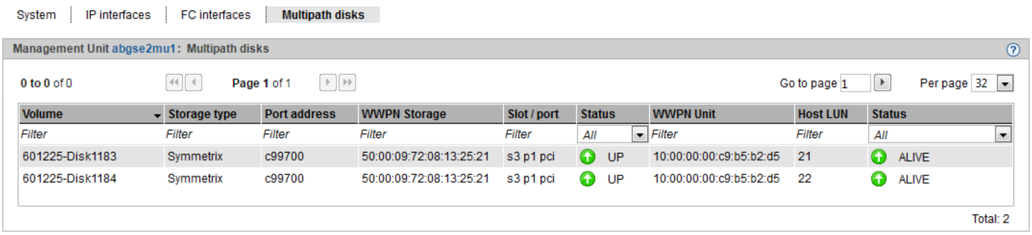
The *FC interfaces* tab displays three groups with information on the FC interfaces:

- *FC interfaces* provides information for each FC interface of the MU on the host controller used, the plug-in position (slot and port), the *Type* (firmware and revision status), the local WWPN (**W**orld **W**ide **P**ort **N**umber) of the FC interface, and the connection channel to the Server Unit /390 (**C**hannel **P**ath **ID -** CHPID). The hardware status of the FC interface is also displayed (*UP*/*DOWN*).
- *FC targets* contains the WWPNs of the FC interfaces on the accessible FC controllers (targets). The WWPN identifies a port unambiguously worldwide.
- *FC paths* contains information on the connections between the units and the accessible FC controllers. Address information on the end points of the various connections is displayed.

### Displaying multipath disks of the MU

For the FC disks the *Multipath disks* tab displays the status of the paths from the unit to the storage system and the end points of the paths, i.e. the interfaces on the storage system and on the unit.

► Select *Hardware* → *Server (SE<model>)* → *<unit> (MU)* → *Information*, *Multipath disks* tab:



| Volume | Storage type | Port address | WWPN Storage | Slot / port | Status | WWPN Unit | Host LUN | Status |
|---|---|---|---|---|---|---|---|---|
| *Filter* | *Filter* | *Filter* | *Filter* | *Filter* | *All* | *Filter* | *Filter* | *All* |
| 601225-Disk1183 | Symmetrix | c99700 | 50:00:09:72:08:13:25:21 | s3 p1 pci | UP | 10:00:00:00:c9:b5:b2:d5 | 21 | ALIVE |
| 601225-Disk1184 | Symmetrix | c99700 | 50:00:09:72:08:13:25:21 | s3 p1 pci | UP | 10:00:00:00:c9:b5:b2:d5 | 22 | ALIVE |

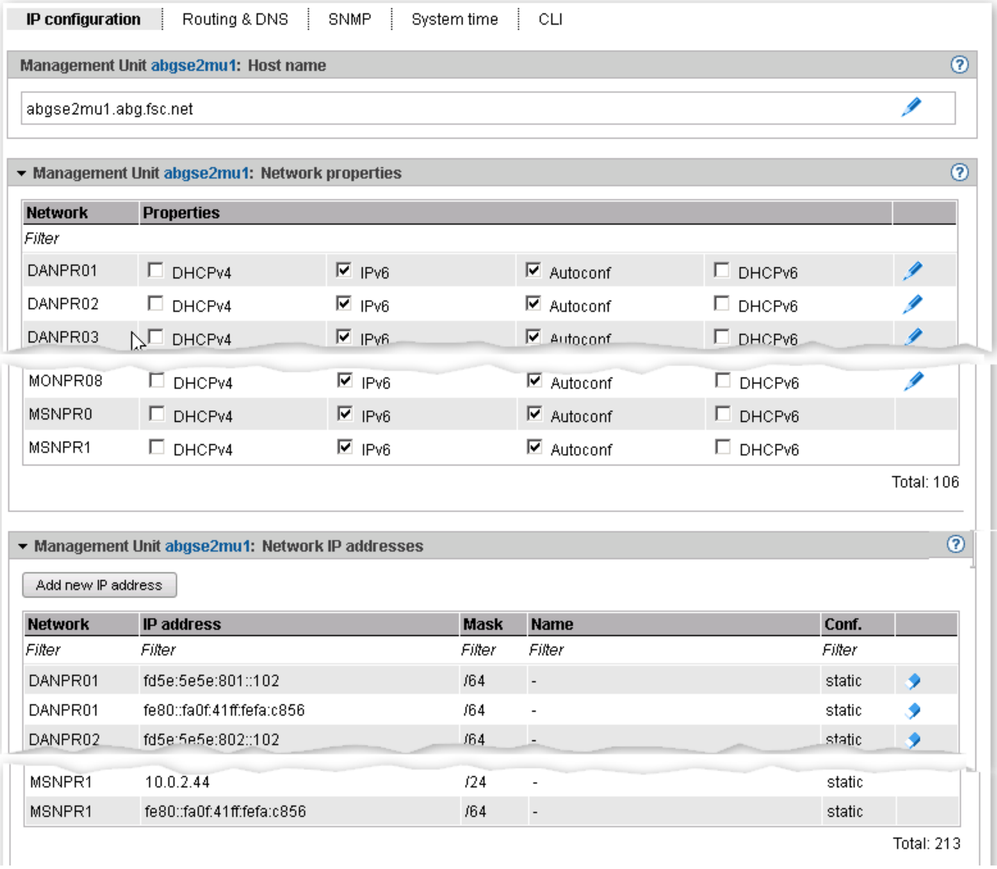
Total: 2

The display takes place page by page, with you being able to define the number of entries per page yourself. Above the table you see which page of the output is currently being displayed. Here you will also find functions which enable to to scroll through the output.

### 10.1.3.2 Managing the IP configuration

You manage the IP configuration of the Management Unit using the associated *Management* menu, *IP configuration* tab.

► Select *Hardware → Server (SE<model>) → <unit> (MU) → Management*, *IP configuration* tab.



Management Unit abgse2mu1: Host name

abgse2mu1.abg.fsc.net

Management Unit abgse2mu1: Network properties

| Network | Properties | | | | |
|---|---|---|---|---|---|
| Filter | | | | | |
| DANPR01 | ☐ DHCPv4 | ☑ IPv6 | ☑ Autoconf | ☐ DHCPv6 | |
| DANPR02 | ☐ DHCPv4 | ☑ IPv6 | ☑ Autoconf | ☐ DHCPv6 | |
| DANPR03 | ☐ DHCPv4 | ☑ IPv6 | ☑ Autoconf | ☐ DHCPv6 | |
| MONPR08 | ☐ DHCPv4 | ☑ IPv6 | ☑ Autoconf | ☐ DHCPv6 | |
| MSNPR0 | ☐ DHCPv4 | ☑ IPv6 | ☑ Autoconf | ☐ DHCPv6 | |
| MSNPR1 | ☐ DHCPv4 | ☑ IPv6 | ☑ Autoconf | ☐ DHCPv6 | |

Total: 106

Management Unit abgse2mu1: Network IP addresses

| Network | IP address | Mask | Name | Conf. | |
|---|---|---|---|---|---|
| Filter | Filter | Filter | Filter | Filter | |
| DANPR01 | fd5e:5e5e:801::102 | /64 | - | static | |
| DANPR01 | fe80::fa0f:41ff:fefa:c856 | /64 | - | static | |
| DANPR02 | fd5e:5e5e:802::102 | /64 | - | static | |
| MSNPR1 | 10.0.2.44 | /24 | - | static | |
| MSNPR1 | fe80::fa0f:41ff:fefa:c856 | /64 | - | static | |

Total: 213

The *IP configuration* tab displays information on the host name, network properties, and addresses of the MU in three groups.

The following options are available to you:

*Changing the host name and domain of the MU*

► In the *Host name* group click the *Change* icon and change the host name and domain in the subsequent dialog box.

*Changing network properties of the MU*

- ► In the *Network properties* group click the *Change* icon by the required network. In the subsequent dialog box you can enable or disable the required properties.

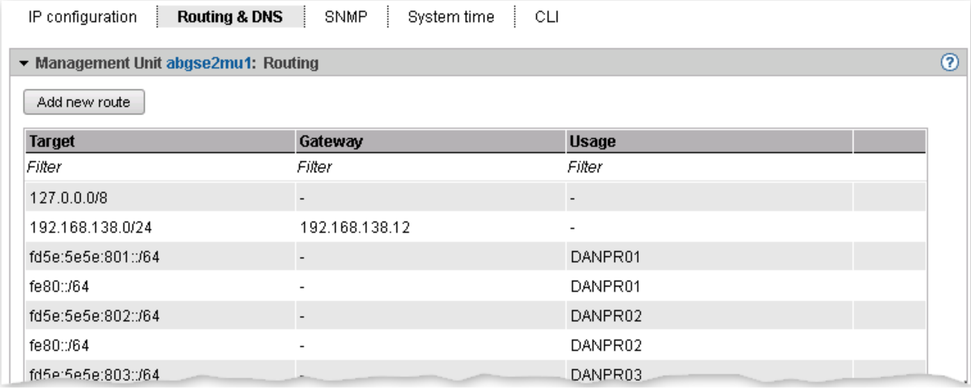
*Add new IP address*

- ► In the *Network IP addresses* group click *Add new IP address*.
  In the *Add IP address* wizard you can specify the required properties of the IP address step by step.

### 10.1.3.3 Managing routing of the Management Unit

You manage routing of the Management Unit using the associated *Management* menu, *Routing & DNS* tab.

► Select *Hardware* → *Server* → *<unit> (MU)* → *Management*, *Routing & DNS* tab.



| Target | Gateway | Usage | |
|---|---|---|---|
| *Filter* | *Filter* | *Filter* | |
| 127.0.0.0/8 | - | - | |
| 192.168.138.0/24 | 192.168.138.12 | - | |
| fd5e:5e5e:801::/64 | - | DANPR01 | |
| fe80::/64 | - | DANPR01 | |
| fd5e:5e5e:802::/64 | - | DANPR02 | |
| fe80::/64 | - | DANPR02 | |
| fd5e:5e5e:803::/64 | - | DANPR03 | |

You use the *Routing & DNS* tab with the *Routing* and *DNS configuration* groups to manage the routing and DNS configuration of the unit. The routing is displayed in the *Routing* group above.

The following options are available to you:

*Adding a new route to the MU (only for MANPU or MONPU networks)*

► In the *Routing* group click *Add new route* (above the table). Make the required entries in the subsequent dialog box and confirm the action.

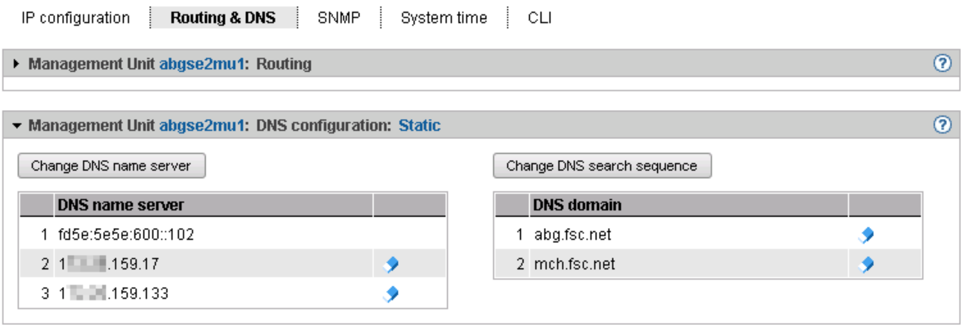
*Deleting a route on MU (only for MANPU or MONPU networks)*

► In the *Routing* group click the *Delete* icon by the required route and confirm the action.

### 10.1.3.4 Managing the DNS configuration

You manage the DNS configuration of the Management Unit using the associated *Management* menu, *Routing & DNS* tab.

▶ Select *Hardware → Server → <unit> (MU) → Management*, *Routing & DNS* tab.



IP configuration | **Routing & DNS** | SNMP | System time | CLI

▸ Management Unit abgse2mu1: Routing

▾ Management Unit abgse2mu1: DNS configuration: Static

Change DNS name server

| | DNS name server | |
|---|---|---|
| 1 | fd5e:5e5e:600::102 | |
| 2 | 1[redacted].159.17 | ✗ |
| 3 | 1[redacted].159.133 | ✗ |

Change DNS search sequence

| | DNS domain | |
|---|---|---|
| 1 | abg.fsc.net | ✗ |
| 2 | mch.fsc.net | ✗ |

The DNS configuration is displayed in the lower *DNS configuration* group.

The following options are available to you:

*Changing the DNS name server configuration of the MU*

Up to two external DNS name servers can be configured.

▶ To enter or change the entry for an external DNS name server, click *Change DNS name server*, and after changing the DNS name server configuration confirm the action.

▶ To remove an external DNS name server, click the *Remove* icon in the row with the required DNS name server and confirm the action.

*Changing the search sequence of the MU or removing a domain*

▶ In the *DNS configuration* group select one of the following procedures:

  ▶ To change the DNS search sequence, click *Change DNS search sequence*, and after changing the DNS search sequence confirm the action.

  ▶ To remove a DNS domain from the DNS configuration, click the *Remove* icon in the row with the required DNS domain and confirm the action.

i The MU is preconfigured as a DNS server for the internal domain "senet" via the internal LAN (IPv6 address fd5e:5e5e:600::102). This entry cannot be removed.

### 10.1.3.5 Managing SNMP

SNMP (Simple Network Management Protocol) is a communication protocol for network, system and application management and enables the units to be monitored over a LAN. An SNMP manager can communicate with the installed SNMP agent via a management station.

You administer central SNMP integration of the SE server using the SE Manager on the Management Unit. The preconfiguration is created in such a manner that you can also use SNMP to monitor the other units of the SE server on the management stations provided a configuration for SNMP integration exists on the Management Unit (read access, trap receiver):

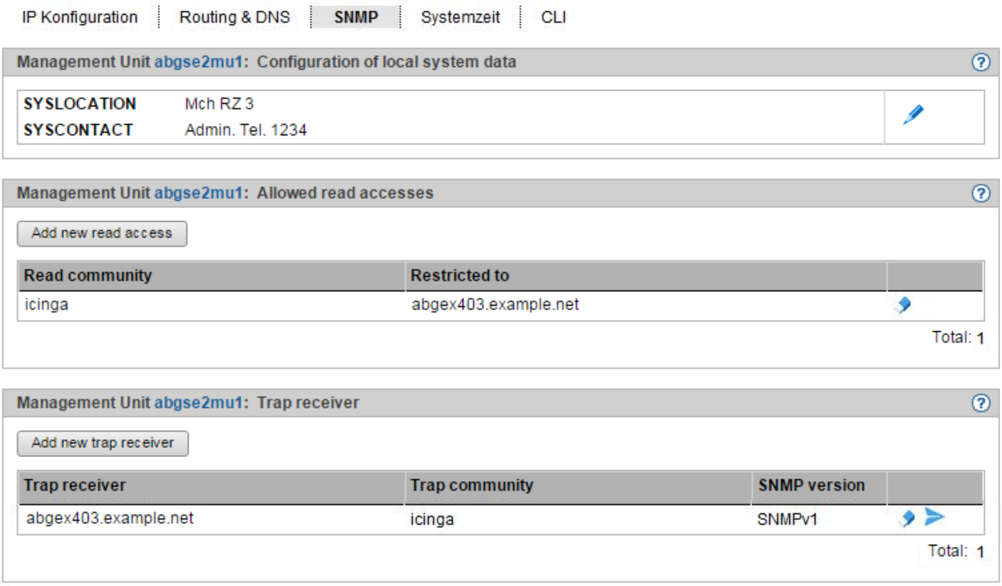
- Queries regarding the Server Unit /390 are possible on the Management Unit (see the private MIBs).
- Management stations cannot address the SNMP agent on the Server Unit x86 or HNC directly, but only via the Management Unit. When the query takes place, the unit name must be prefixed. The SNMP agent supports the MIB-II and private MIBs for queries.
- In defined error situations (e.g. status changes) the SNMP agent on the Server Unit x86 or HNC sends traps via the Management Unit to the external management stations. The sender of the trap is always the Management Unit.
- On Application Units, on the other hand, you must configure SNMP yourself.

The following private MIBs must be imported to the management station in order to permit access in read mode and to enable the traps to be interpreted:

- `/usr/share/snmp/mibs/FUJITSU-SESERVER-MIB.txt`
- `/usr/share/snmp/mibs/FUJITSU-SU390-MIB.txt`

Access to these MIB files on the Management Unit is, for example, possible under any administrator account with scp (secure copy).

► Select *Hardware* → *Server (SE<model>)* → *<unit >(MU)* → *Management*, *SNMP* tab:



Management Unit abgse2mu1: Configuration of local system data

| | |
|---|---|
| SYSLOCATION | Mch RZ 3 |
| SYSCONTACT | Admin. Tel. 1234 |

Management Unit abgse2mu1: Allowed read accesses

| Read community | Restricted to |
|---|---|
| icinga | abgex403.example.net |

Total: 1

Management Unit abgse2mu1: Trap receiver

| Trap receiver | Trap community | SNMP version |
|---|---|---|
| abgex403.example.net | icinga | SNMPv1 |

Total: 1

The *SNMP* tab displays information on the configuration of the local system data, allowed read accesses, and trap receivers.

The following functions are available in the SNMP tab:

*Changing local system data for SNMP*

► In the *Configuration of local system data* group click the *Change* item, and in the subsequent dialog box make changes to the system file.

ℹ The SE Manager displays the SYSLOCATION in the header.

*Adding or removing allowed read accesses*

► In the *Allowed read accesses* group select one of the following procedures:

  ► To add a new read right, click *Add new read access*, and after making the necessary entries confirm the action.

  ► To remove a read access, click the *Remove* icon by the required read access and confirm the action.

*Adding or removing trap receivers*

- In the *Trap receiver* group select one of the following procedures:
  - To add a trap receiver, click *Add new trap receiver* , and after making the necessary entries confirm the action.
  - To remove a trap receiver, click the *Remove* icon in the row with the required trap receiver and confirm the action.

*Sending a test trap*

- In the *Trap receiver* group, click the *Send test trap* icon in the row with the required test receiver and confirm the action.

### 10.1.3.6 Setting the system time (time synchronization or local)

The Management Units are available as NTP servers for all units of the server via the internal LAN. SU x86 and HNC are preconfigured with respect to NTP; AU configuration must be performed as required by the administrator responsible.

To ensure high time accuracy, you can also configure automatic time leveling with a so-called NTP server, e.g. one which supplies a time which is as accurate as a radio clock, using NTP (Network Time Protocol).

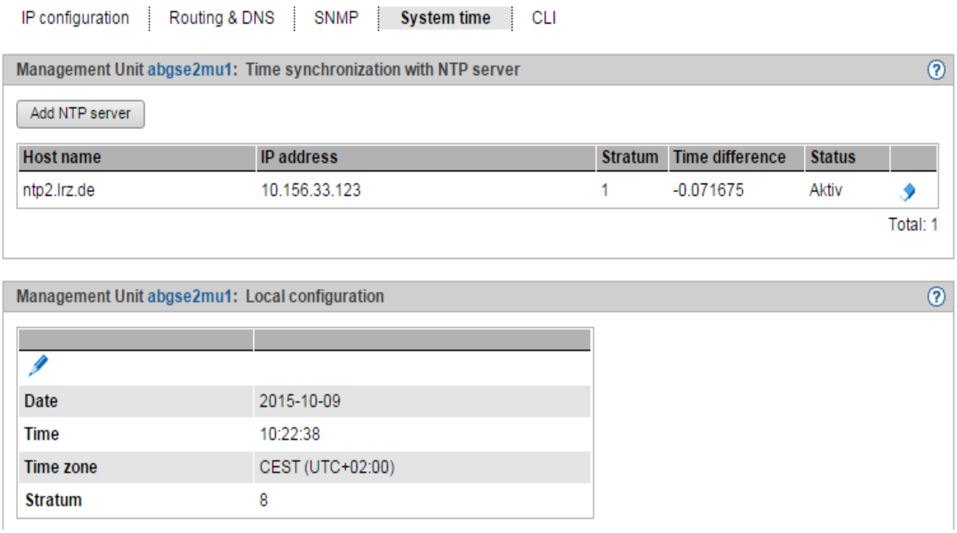
#### Effect on the time setting of the systems on the SE server

The time settings of the other systems are synchronized with the system time of the Management Unit. The Management Unit is the basic timer.

When changes are made to the time management which affect the Server Unit, bear in mind that the time settings in BS2000 systems and of XenVMs that are started later are also affected. Here you should in particular avoid large leaps in time which are caused by setting the time manually.

Details on BS2000 are provided in the "Synchronization of the system time" section of the "BS2000 OSD/BC System Administration" manual [9].

- ► Select *Hardware → Server (SE<model>) → <unit>(MU) → Management, System time* tab:



Management Unit abgse2mu1: Time synchronization with NTP server

| Host name | IP address | Stratum | Time difference | Status | |
|---|---|---|---|---|---|
| ntp2.lrz.de | 10.156.33.123 | 1 | -0.071675 | Aktiv | |

Total: 1

Management Unit abgse2mu1: Local configuration

| | |
|---|---|
| Date | 2015-10-09 |
| Time | 10:22:38 |
| Time zone | CEST (UTC+02:00) |
| Stratum | 8 |

The *System time* tab displays the NTP servers which are entered for automatic time synchronization and the local time of the MU.

*Adding or removing an NTP server*

- ► To add an NTP server, click *Add NTP server* in the *Time synchronization with NTP server* group, and after making the necessary entries confirm the action.
- ► To remove an NTP server from the NTP configuration, click the *Remove* icon by the required NTP server in the *Time synchronization with NTP server* group and confirm the action.

*Changing the local time*

You can only change the local time if no NTP server is active.

> **i** Changes to the time can also have an effect on productive operation. See also section “Effect on the time setting of the systems on the SE server” on page 199".

- ► In the *Local time* group click the *Change* icon, and after making the necessary entries confirm the action.

### 10.1.3.7 Entering CLI commands

The SE Manager offers the administrator access to the CLI (**C**ommand **L**ine **I**nterface) on the Management Unit.

► Select *Hardware → Server (SE<model>) → <unit>(MU) → Management, CLI* tab.

On the *CLI* tab you can open a Linux shell in a terminal window and use the CLI for text-based administration by means of commands.

► Click *Open*.

A terminal window opens, and you are automatically logged in to M2000.
Information on the terminal window is provided on page 74.

### 10.1.3.8 Managing updates of the Management Unit

The administrator uses the *Updates* tab to manage updates for the Management Units.

Updates extend the system or the M2000 basic software of the MU:

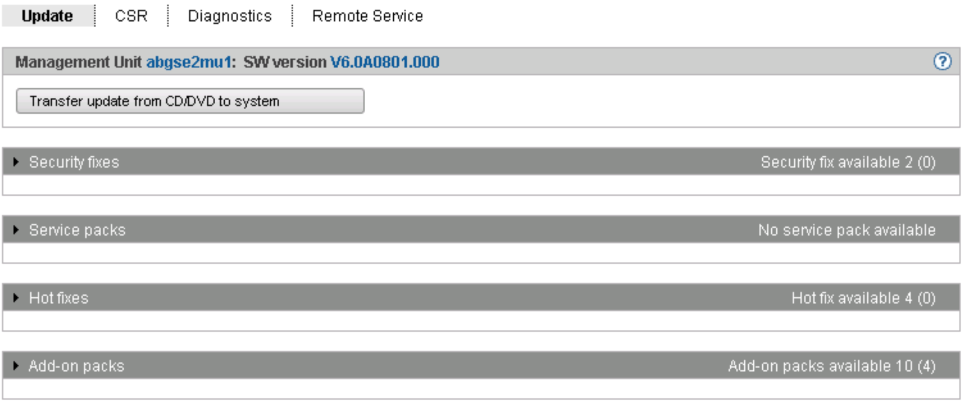
- Security fixes contain selected software packages of the basic software and close security gaps.
- Service packs are used to update and enhance the functionality of the basic software as a whole.
- Hot fixes solve customer-specific problems.
- Add-on packs enhance the basic software and are functional software components which have their own version schema.

Updates or their installation sources can be integrated into the system in various ways, with the customer and Customer Support as a rule sharing the tasks (see section “Tasks of Customer Support” on page 60 and section “Tasks of the customer” on page 60):

- Updates can be supplied by FUJITSU on CD/DVD.
- Updates can be uploaded from PC to the MU. Before this is done, they must, for example, be downloaded from a FUJITSU Download Server to a PC.
- Updates can be prepared in advance and even installed by Customer Support.

The *Updates* tab provides you with information on the current status of the updates:

► Select *Hardware* → *Server (SE<model>)* → *<unit> (MU)* → *Service, Updates* tab.



Update | CSR | Diagnostics | Remote Service

Management Unit abgse2mu1: SW version V6.0A0801.000

Transfer update from CD/DVD to system

▸ Security fixes — Security fix available 2 (0)

▸ Service packs — No service pack available

▸ Hot fixes — Hot fix available 4 (0)

▸ Add-on packs — Add-on packs available 10 (4)

The group header of each update type contains a general overview of the information. To obtain detailed information or to execute actions, expand the group concerned.

The *Updates* tab offers the following functions:

- Transfer update from CD/DVD to system
  All updates contained on the CD/DVD are transferred to the system.
  They are then displayed in the relevant group and can be used further.
- *Security Fixes* group
  The customer can upload and install security fixes.
  He/She can delete security fixes which have not been installed or their installation sources.
- *Service Packs* group
  The customer can upload service packs.
  He/She can delete service packs which have not been installed or their installation sources.
  Only Customer Support can install service packs (see section “Tasks of Customer Support” on page 60 and section “Tasks of the customer” on page 60).
- *Hot Fixes* group
  The customer can upload hot fixes.
  He/She can delete hot fixes which have not been installed or their installation sources.
  Only Customer Support can install hot fixes (see section “Tasks of Customer Support” on page 60 and section “Tasks of the customer” on page 60).
- *Add-on Packs* group
  The customer can upload, install, and uninstall add-on packs or delete add-on packs which have not been installed.
  Installation and uninstallation of add-on packs have an immediate effect on the SE Manager (e.g. adjustment of the tree structure).

### 10.1.3.9 Managing configuration data (CSR) of the MU

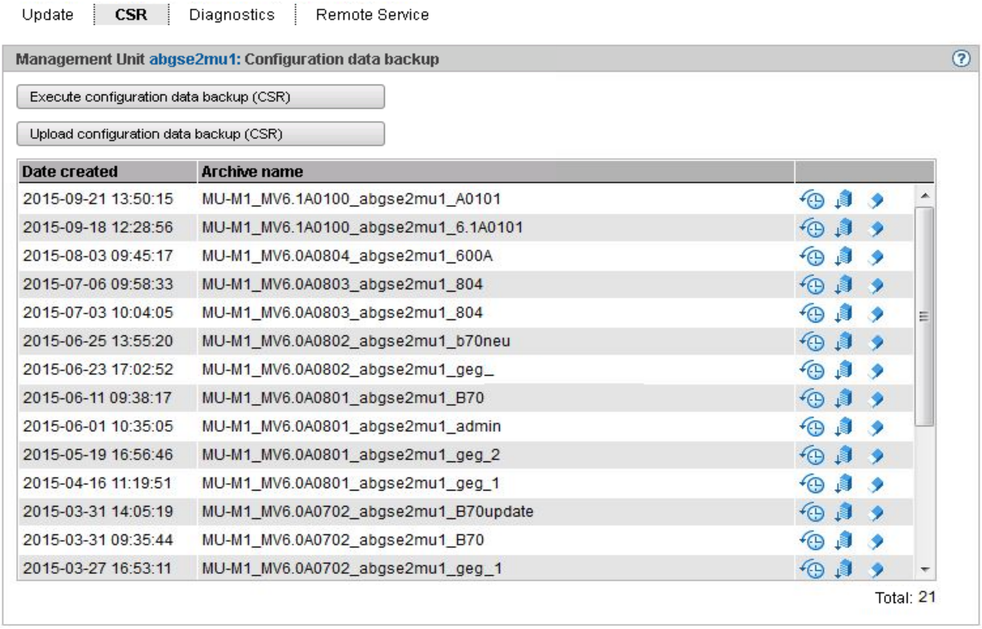
You use a CSR backup (CSR = Configuration Save and Restore) to back up the configuration data of the Management Unit in an archive. The backup archive contains the complete configuration of the basic system, e.g. the BS2000 devices of the SU /390, the accounts, and the NTP configuration. Each backup archive has a creation date and an archive name.

A CSR backup enables the configuration of the unit concerned at the time the backup was made to be restored.

Tip: Perform a CSR backup after each configuration change.

You manage the configuration data of the Management Unit using the associated *Service* menu, *CSR* tab.

► Select *Hardware → Server (SE<model>) → <unit> (MU) → Service*, *CSR* tab.



Update
CSR
Diagnostics
Remote Service

Management Unit abgse2mu1: Configuration data backup

Execute configuration data backup (CSR)
Upload configuration data backup (CSR)

| Date created | Archive name |
|---|---|
| 2015-09-21 13:50:15 | MU-M1_MV6.1A0100_abgse2mu1_A0101 |
| 2015-09-18 12:28:56 | MU-M1_MV6.1A0100_abgse2mu1_6.1A0101 |
| 2015-08-03 09:45:17 | MU-M1_MV6.0A0804_abgse2mu1_600A |
| 2015-07-06 09:58:33 | MU-M1_MV6.0A0803_abgse2mu1_804 |
| 2015-07-03 10:04:05 | MU-M1_MV6.0A0803_abgse2mu1_804 |
| 2015-06-25 13:55:20 | MU-M1_MV6.0A0802_abgse2mu1_b70neu |
| 2015-06-23 17:02:52 | MU-M1_MV6.0A0802_abgse2mu1_geg_ |
| 2015-06-11 09:38:17 | MU-M1_MV6.0A0801_abgse2mu1_B70 |
| 2015-06-01 10:35:05 | MU-M1_MV6.0A0801_abgse2mu1_admin |
| 2015-05-19 16:56:46 | MU-M1_MV6.0A0801_abgse2mu1_geg_2 |
| 2015-04-16 11:19:51 | MU-M1_MV6.0A0801_abgse2mu1_geg_1 |
| 2015-03-31 14:05:19 | MU-M1_MV6.0A0702_abgse2mu1_B70update |
| 2015-03-31 09:35:44 | MU-M1_MV6.0A0702_abgse2mu1_B70 |
| 2015-03-27 16:53:11 | MU-M1_MV6.0A0702_abgse2mu1_geg_1 |

Total: 21

The following options are available to you:

*Executing configuration data backup for the MU*

► Click *Execute configuration data backup (CSR)* and confirm the action after selecting a file archive for configuration data backup.

*Upload configuration data backup to an MU*

- ▶ Click *Upload configuration data backup (CSR)*, select a backup file, and confirm the action.

*Downloading/deleting configuration data backup for the MU*

- ▶ To download the file archive, click the *Download* icon in the row with the required file archive, select whether you wish to open or save the file archive, and confirm the action.

  ℹ Do not change the file names of CSR backups after you have downloaded them, otherwise they will not be accepted when they are uploaded.

*Deleting configuration data backup for the MU*

- ▶ To delete the file archive, click the *Delete* icon in the row with the required file archive and confirm the action.

*Restoring configuration data from a file archive*

- ▶ Click the *Restore* icon in the row with the required file archive and confirm the action. If the Customer Support staff has already prepared restoration, the action is rejected with a message to this effect.

⚠ Restoration leads to the unit being rebooted immediately.

### 10.1.3.10 Generating diagnostic data

To support error diagnosis by Customer Support, the administrator or operator can generate diagnostic data when an error situation occurs and send this to the Support Center.

- ▶ Select *Hardware → Server (SE<model>) → <unit>(MU) → Service*, *Diagnostics* tab.

A diagnostic data file which already exists is displayed. You can generate new diagnostic data, in which case an existing diagnostic data file is overwritten. The file name shows the basic software for which and when the diagnostic data was generated:

```
DIAGtar.M<software-version><unit-name>.<datum>.<uhrzeit>.gz
```

As administrator, you can download the diagnostic data file on the local MU as a compressed archive file in order to send it to the Support Center if necessary.

### 10.1.3.11 Managing service access

#### Remote Service

Customer Support activities on the SE server are monitored with the help of the shadow terminal. Configuration can be implemented in such a manner that you as administrator, for instance, observe all the Customer Support activities (mandatory use of a so-called shadow terminal).

AIS Connect enables Customer Support connections to be configured via the Management Unit to selected storage systems which in this context are referred to as **external assets**. These connections are configured by Customer Support in agreement with the customer. As administrator you can at all times modify the Customer Support access to specific external assets (allow or not allow).

Remote service ensures that a service call is sent to the Support Center when a problem occurs (outgoing connection).

Customer Support can establish the connection to the SE server itself (incoming connection) if it wants to correct the problem or take preventive measures (changes, updates, diagnostics, etc.).
If it is absolutely essential, as an administrator (and to a lesser extent as an operator) you can change the remote service configuration or intervene in a service operation which is currently running.

ℹ **Important!**
Please discuss every change to the remote service configuration with the Support Center, otherwise you will put the serviceability of your SE server at risk.
Aspects of remote service which are relevant to security are described in the Security Manual.

#### Service accounts

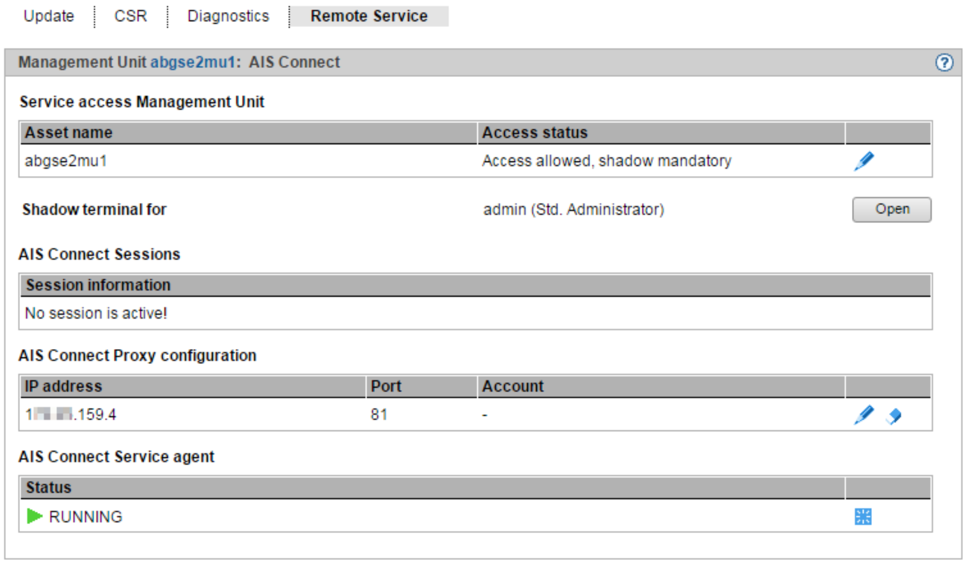
To perform its work, Customer Support logs in (remotely via Teleservice or locally) under the service account provided for this purpose. On the units the protected account *service* is available to Customer Support in the operating system.

#### Remote Service tab

Service access is managed via the Management Unit. The *Remote Service* tab is provided in the *Service* menu for this purpose:

► Select *Hardware → Server (SE<model>) → <unit> (MU) → Service*, *Remote Service* tab.

The *Remote Service* tab displays the *Service access*, *Sessions*, *Proxy configuration*, and *AIS agent* groups.



Management Unit abgse2mu1: AIS Connect

Service access Management Unit

| Asset name | Access status | |
|---|---|---|
| abgse2mu1 | Access allowed, shadow mandatory | ✎ |

Shadow terminal for admin (Std. Administrator) Open

AIS Connect Sessions

| Session information |
|---|
| No session is active! |

AIS Connect Proxy configuration

| IP address | Port | Account | |
|---|---|---|---|
| 1[redacted] [redacted].159.4 | 81 | - | ✎ |

AIS Connect Service agent

| Status | |
|---|---|
| ▶ RUNNING | |

*Changing the service access*

► In the *Service access* group click the *Change* icon by the required asset. In the subsequent dialog box select one of the available access settings and confirm the action.

*Opening a shadow terminal*

► Click the *Open* button after *Shadow terminal for <account>* in order to open a terminal window.

The account tele is switched to automatically and a shadow is opened. You can follow the activities of Customer Support in this window.

Depending on the current setting of the Customer Support access (see *Access status*), you have the following options:

– With the *Allow access, shadow mandatory* setting Customer Support is blocked until you have opened the shadow terminal. Only then can Customer Support work. You can now follow every step taken by Customer Support on the opened shadow terminal and can intervene actively yourself, i.e. enter commands yourself.

– With the *Allow access, shadow possible* setting Customer Support can work independently of the customer. When Customer Support is active (see also *Session information)*, the process ID (pid) of the AIS Connect session is displayed for you in the format <pid$_1$>.<pid$_2$>.<pid$_3$> after you have logged in on the shadow terminal.

- ► Enter the `screen -x <pid1>.<pid2>.<pid3>` command to establish a connection to this AIS Connect session.
- ► Enter `screen -ls` to also display open sessions.

*Entering/changing or deleting a proxy configuration*

- ► To enter or change a proxy configuration, in the *Proxy configuration* click the *Change* icon by the required proxy server for AIS. Define the properties of the proxy configuration and confirm the action.
- ► To delete a proxy configuration, in the *Proxy configuration* group click the *Delete* icon by the required proxy server for AIS and confirm the action.

*Rebooting an AIS agent*

- ► In the *AIS agent* group click the *Reboot* icon by the required AIS agent and confirm the action.

### Reading logs

AIS Connect writes the Customer Support activities to logging files. The files have different formats depending on the type of session:

- SSH sessions: logging files in text format
- VNC sessions: html and swf logging files; here an html file and an swf file with the same timestamp always belong together

You can list and delete the logging files using the `aisLog` command. You can also view the logging files of SSH sessions with `aisLog`. As operator you enter the command on the shadow terminal, and as administrator you can also enter it in the terminal window of the Management Unit using the *CLI* tab, see section “Entering CLI commands” on page 201.

You can only read the logging files of VNC sessions on a PC. Transfer the required logging file pair to your PC (e.g. with `scp` under an administrator account) and open the html file in the browser.

## 10.1.4 Managing the HNC

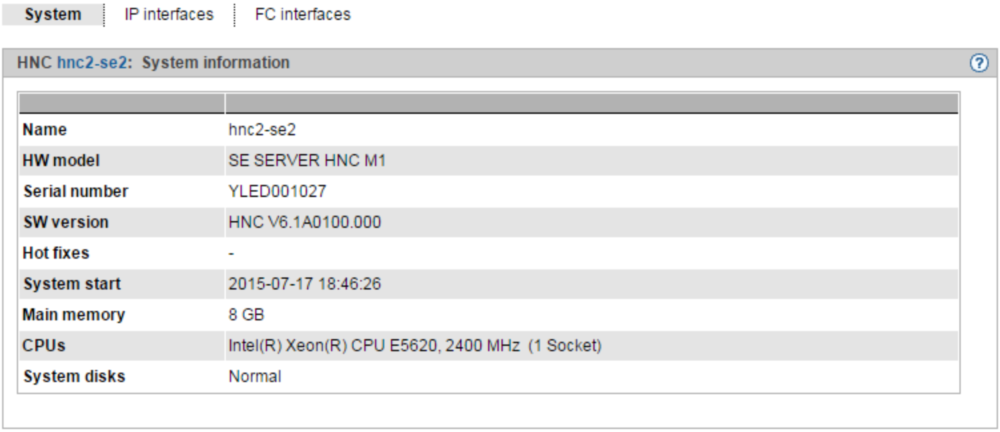
### 10.1.4.1 Displaying system information and interfaces of the HNC

The *Information* menu provides you with information about the HNC and its interfaces.

- Displaying system information of the HNC
- Displaying IP interfaces of the HNC
- Displaying FC interfaces of the HNC

### Displaying system information of the HNC

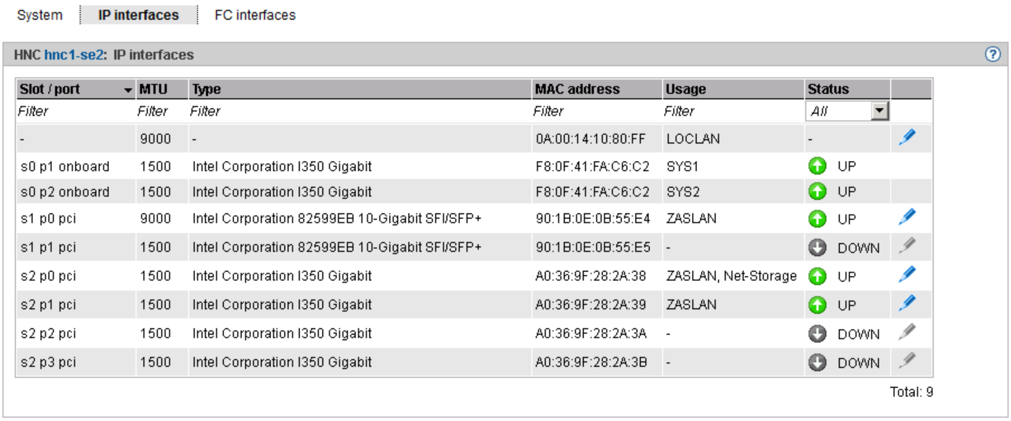
► Select *Hardware* → *Server (SE<model>)* → *<unit> (MU)* → *Information*, *System* tab:



| | |
|---|---|
| Name | hnc2-se2 |
| HW model | SE SERVER HNC M1 |
| Serial number | YLED001027 |
| SW version | HNC V6.1A0100.000 |
| Hot fixes | - |
| System start | 2015-07-17 18:46:26 |
| Main memory | 8 GB |
| CPUs | Intel(R) Xeon(R) CPU E5620, 2400 MHz (1 Socket) |
| System disks | Normal |

## Displaying IP interfaces of the HNC

► Select *Hardware* → *Server (SE<model>)* → *<unit> (HNC)* → *Information*, *IP interfaces* tab



HNC hnc1-se2: IP interfaces

| Slot / port | MTU | Type | MAC address | Usage | Status | |
|---|---|---|---|---|---|---|
| *Filter* | *Filter* | *Filter* | *Filter* | *Filter* | *All* | |
| - | 9000 | - | 0A:00:14:10:80:FF | LOCLAN | - | ✎ |
| s0 p1 onboard | 1500 | Intel Corporation I350 Gigabit | F8:0F:41:FA:C6:C2 | SYS1 | ⬆ UP | |
| s0 p2 onboard | 1500 | Intel Corporation I350 Gigabit | F8:0F:41:FA:C6:C2 | SYS2 | ⬆ UP | |
| s1 p0 pci | 9000 | Intel Corporation 82599EB 10-Gigabit SFI/SFP+ | 90:1B:0E:0B:55:E4 | ZASLAN | ⬆ UP | ✎ |
| s1 p1 pci | 1500 | Intel Corporation 82599EB 10-Gigabit SFI/SFP+ | 90:1B:0E:0B:55:E5 | - | ⬇ DOWN | ✎ |
| s2 p0 pci | 1500 | Intel Corporation I350 Gigabit | A0:36:9F:28:2A:38 | ZASLAN, Net-Storage | ⬆ UP | ✎ |
| s2 p1 pci | 1500 | Intel Corporation I350 Gigabit | A0:36:9F:28:2A:39 | ZASLAN | ⬆ UP | ✎ |
| s2 p2 pci | 1500 | Intel Corporation I350 Gigabit | A0:36:9F:28:2A:3A | - | ⬇ DOWN | ✎ |
| s2 p3 pci | 1500 | Intel Corporation I350 Gigabit | A0:36:9F:28:2A:3B | - | ⬇ DOWN | ✎ |

Total: 9

The *IP interfaces* tab provides information about the HNC's LAN interfaces.

The following function is available:

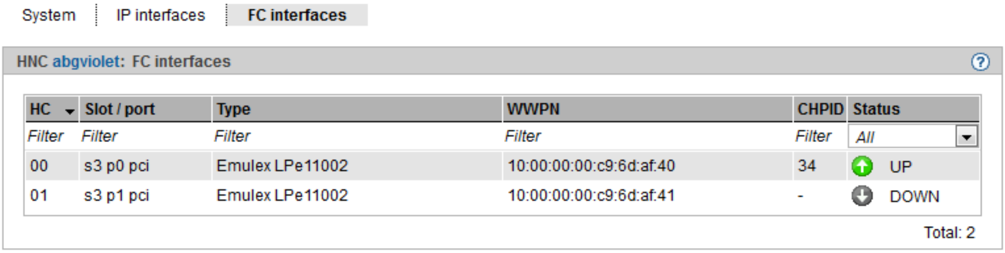
*Changing the packet length in the case of LOCLAN and PCI interfaces*

In the case of a PCI interface you can only change the packet length in normal operation, i.e. the *Status UP* is displayed for the interface.

► Click the *Change* icon by the required IP interface, select the required packet length in the subsequent dialog box, and confirm the action.

### Displaying FC interfaces of the HNC

► Select *Hardware → Server (SE<model>) → <unit> (HNC) → Information*, *FC interfaces* tab.



HNC abgviolet: FC interfaces

| HC | Slot / port | Type | WWPN | CHPID | Status |
|---|---|---|---|---|---|
| *Filter* | *Filter* | *Filter* | *Filter* | *Filter* | *All* |
| 00 | s3 p0 pci | Emulex LPe11002 | 10:00:00:00:c9:6d:af:40 | 34 | UP |
| 01 | s3 p1 pci | Emulex LPe11002 | 10:00:00:00:c9:6d:af:41 | - | DOWN |

Total: 2

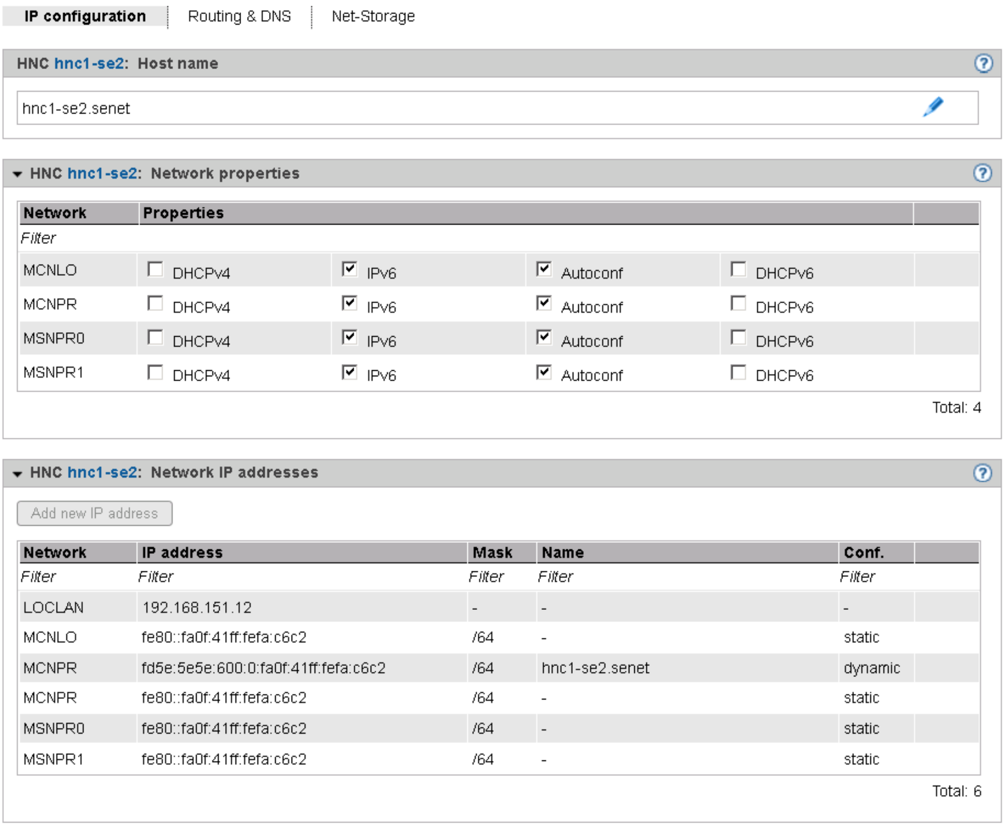
The *FC interfaces* tab provides information on the Fibre Channel interface of the HNC to the SU /390.

The host controller used, the local WWPN (**W**orld **W**ide **P**ort **N**umber) and the plug-in position (slot and port) are displayed for each FC interface. The hardware status of the FC interface is also displayed (*UP*/*DOWN*).

### 10.1.4.2 Managing the IP configuration of the HNC

You manage the IP configuration of the HNC using the associated *Management* menu, *IP configuration* tab.

► Select *Hardware* → *Server (SE<model>)* → *<unit> (HNC)* → *Management*, *IP configuration* tab.



**HNC hnc1-se2: Host name**

hnc1-se2.senet

**HNC hnc1-se2: Network properties**

| Network | Properties | | | |
|---|---|---|---|---|
| *Filter* | | | | |
| MCNLO | □ DHCPv4 | ☑ IPv6 | ☑ Autoconf | □ DHCPv6 |
| MCNPR | □ DHCPv4 | ☑ IPv6 | ☑ Autoconf | □ DHCPv6 |
| MSNPR0 | □ DHCPv4 | ☑ IPv6 | ☑ Autoconf | □ DHCPv6 |
| MSNPR1 | □ DHCPv4 | ☑ IPv6 | ☑ Autoconf | □ DHCPv6 |

Total: 4

**HNC hnc1-se2: Network IP addresses**

| Network | IP address | Mask | Name | Conf. |
|---|---|---|---|---|
| *Filter* | *Filter* | *Filter* | *Filter* | *Filter* |
| LOCLAN | 192.168.151.12 | - | - | - |
| MCNLO | fe80::fa0f:41ff:fefa:c6c2 | /64 | - | static |
| MCNPR | fd5e:5e5e:600:0:fa0f:41ff:fefa:c6c2 | /64 | hnc1-se2.senet | dynamic |
| MCNPR | fe80::fa0f:41ff:fefa:c6c2 | /64 | - | static |
| MSNPR0 | fe80::fa0f:41ff:fefa:c6c2 | /64 | - | static |
| MSNPR1 | fe80::fa0f:41ff:fefa:c6c2 | /64 | - | static |

Total: 6

The *IP configuration* tab displays the host name, network properties, and network addresses of the HNC in three groups.

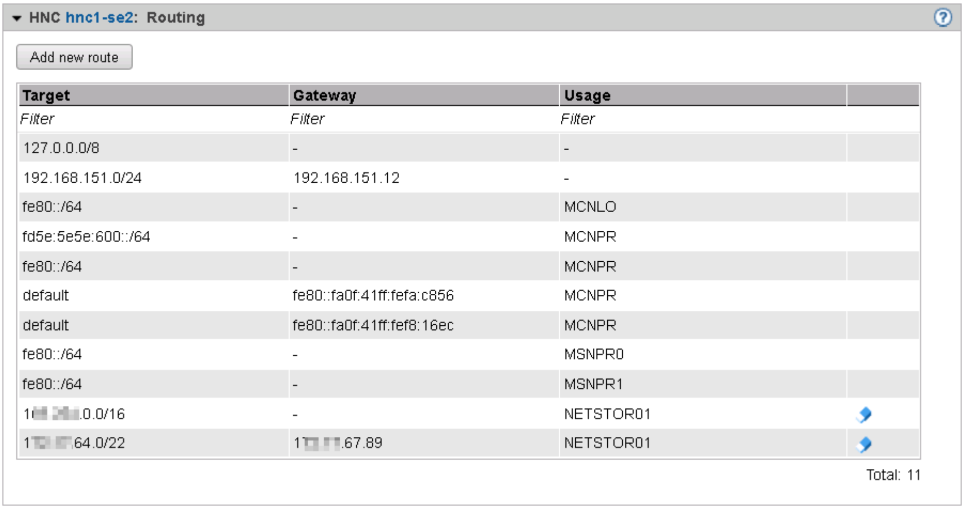
*Changing the host name and domain of the HNC*

► In the *Host name* group click the *Change* icon, in the subsequent dialog box change the host name and domain, and confirm the action.

### 10.1.4.3 Managing routing of the HNC

You manage routing of the HNC using the associated *Management* menu, *Routing & DNS.* tab

▶ Select *Hardware* → *Server* → *<unit name> (HNC)* → *Management*, *Routing & DNS* tab.



| Target | Gateway | Usage | |
|---|---|---|---|
| *Filter* | *Filter* | *Filter* | |
| 127.0.0.0/8 | - | - | |
| 192.168.151.0/24 | 192.168.151.12 | - | |
| fe80::/64 | - | MCNLO | |
| fd5e:5e5e:600::/64 | - | MCNPR | |
| fe80::/64 | - | MCNPR | |
| default | fe80::fa0f:41ff:fefa:c856 | MCNPR | |
| default | fe80::fa0f:41ff:fef8:16ec | MCNPR | |
| fe80::/64 | - | MSNPR0 | |
| fe80::/64 | - | MSNPR1 | |
| 1[redacted].0.0/16 | - | NETSTOR01 | ◆ |
| 1[redacted]64.0/22 | 1[redacted].67.89 | NETSTOR01 | ◆ |

Total: 11

The *Routing & DNS* tab displays the routing in the upper group *Routing*.

The functionality of the tab is the same as that for the MU (see section “Managing routing of the Management Unit” on page 195) with the following restriction:

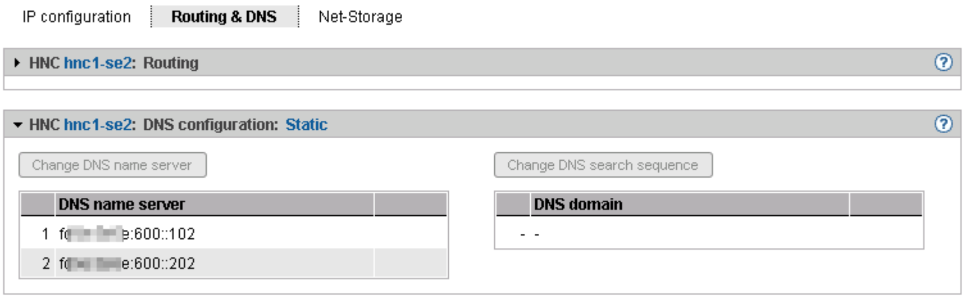
i The MANPU and MONPU networks are not available on the HNC.

The *Add new route* and *Delete route* actions are only available for Net-Storage connections.

### 10.1.4.4 Displaying the DNS configuration of the HNC

You can inquire information about the DNS configuration of the HNC using the associated *Management* menu, *Routing & DNS* tab.

► Select *Hardware* → *Server* → *<unit name> (HNC)* → *Management*, *Routing & DNS* tab.



▸ HNC hnc1-se2: Routing

▾ HNC hnc1-se2: DNS configuration: Static

| | DNS name server | |
|---|---|---|
| 1 | f[redacted]e:600::102 | |
| 2 | f[redacted]e:600::202 | |

| | DNS domain | |
|---|---|---|
| | - - | |

The *Routing & DNS* tab displays the DNS configuration in the lower group *DNS configuration*.

### 10.1.4.5 Configuring Net-Storage on the HNC

Access to Net-Storage (storage access via NFS) is possible for BS2000 systems (for Native BS2000 and the BS2000 VMs) of the SU /390 provided the prerequisites are fulfilled in the HNC.

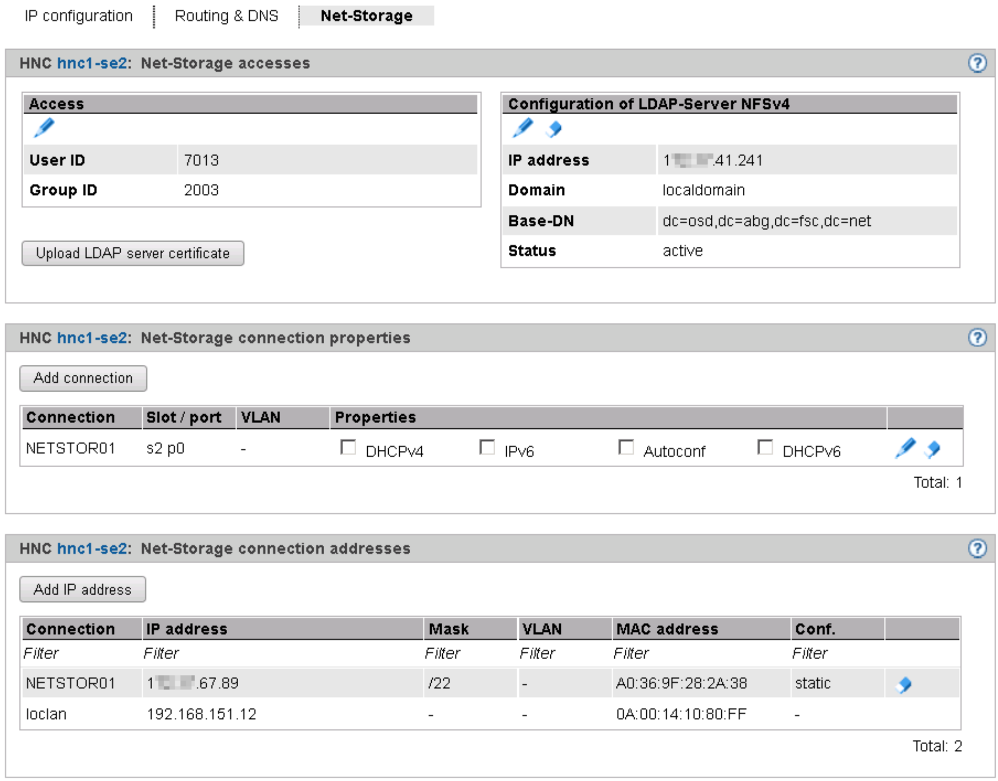
– As net client the HNC requires access rights for the net server which provides the Net-Storage. Authentication takes place either via user and group IDs or via an LDAP server NFSv4.

> **i** Access via an LDAP server is only possible if the LDAP server's certificate has been downloaded to the unit.
>
> If the LDAP server's configuration is not active or invalid or is being deleted, authentication takes place using the local user and group.

– Each Net-Storage connection must be configured in the network.

You configure Net-Storage in the HNC using the *Management* menu, *Net-Storage* tab.

► Select *Hardware* → *Server (SE<model>)* → *<unit> (HNC)* → *Management*, *Net-Storage* tab.



HNC hnc1-se2: Net-Storage accesses

| Access | |
|---|---|
| User ID | 7013 |
| Group ID | 2003 |

| Configuration of LDAP-Server NFSv4 | |
|---|---|
| IP address | 1[redacted].41.241 |
| Domain | localdomain |
| Base-DN | dc=osd,dc=abg,dc=fsc,dc=net |
| Status | active |

HNC hnc1-se2: Net-Storage connection properties

| Connection | Slot / port | VLAN | Properties | | | | |
|---|---|---|---|---|---|---|---|
| NETSTOR01 | s2 p0 | - | □ DHCPv4 | □ IPv6 | □ Autoconf | □ DHCPv6 | |

Total: 1

HNC hnc1-se2: Net-Storage connection addresses

| Connection | IP address | Mask | VLAN | MAC address | Conf. | |
|---|---|---|---|---|---|---|
| *Filter* | *Filter* | *Filter* | *Filter* | *Filter* | *Filter* | |
| NETSTOR01 | 1[redacted].67.89 | /22 | - | A0:36:9F:28:2A:38 | static | |
| loclan | 192.168.151.12 | - | - | 0A:00:14:10:80:FF | - | |

Total: 2

The *Net-Storage* tab displays the *Net-Storage accesses*, *Net-Storage connection properties*, and *Net-Storage connection addresses* groups.

The following functions are available to you:

*Changing access right for the HNC*

The *Access right* table displays the current user and group IDs for Net-Storage access. If no LDAP configuration is active, authentication takes place using this entry.

► In the *Net-Storage accesses* group click the *Change* icon by *Access*. In the subsequent dialog box change the user and/or group ID and confirm the action.

*Uploading an LDAP server certificate to the HNC*

► In the *Net-Storage accesses* group click *Upload LDAP server certificate*, select the certificate file in the subsequent dialog box, and confirm the action.

*Entering or changing configuration data for the LDAP server*

► In the *Net-Storage accesses* group click the *Change* icon by *Configuration of LDAP-Server <server>*, enter the required properties in the subsequent dialog box, and confirm the action.

*Deleting configuration data for the LDAP server*

► In the *Net-Storage accesses* group click the *Delete* icon by *Configuration of LDAP-Server <server>* and confirm the action.

> ℹ Following deletion, authentication takes place using the user and group IDs entered. Net-Storage access is then only possible if valid values are entered.

*Adding a Net-Storage connection to the HNC*

► In the *Net-Storage connection properties* group click *Add connection*. Make the required entries in the subsequent dialog box and confirm the action.

*Removing the Net-Storage:connection*

► In the *Net-Storage connection properties* group click the *Remove* icon by the required Net-Storage connection and confirm the action.

*Adding a Net-Storage connection address (HNC)*

► In the *Net-Storage connection addresses* group click *Add IP address*. Make the required entries in the subsequent dialog box and confirm the action.

*Removing a Net-Storage connection address*

► In the *Net-Storage connection addresses* group click the *Remove* icon by the required Net-Storage connection and confirm the action.

### 10.1.4.6 Managing updates

Fundamental information on updates is provided in section “Maintenance and remote service” on page 62.

You manage updates of the HNC using the associated *Service* menu, *Update* tab.

► Select *Hardware* → *Server (SE<model>)* → *<unit> (HNC)* → *Service*, *Update* tab.

An expandable group is displayed on the *Update* tab for each of the software updates *Security Fixes*, *Service Packs* and *Hot Fixes*.

With the exception of the *Add-on Packs*, the functionality of the tab is the same as that for the MU (see section “Managing updates of the Management Unit” on page 202).

### 10.1.4.7 Managing configuration data (CSR) of the HNC

You use a CSR backup (CSR = Configuration Save and Restore) to back up the configuration data of the HNC in an archive. The backup archive contains the entire configuration of the basic system. Each backup archive has a creation date and an archive name.

A CSR backup enables the configuration of the HNC at the time the backup was made to be restored.

► Select *Hardware* → *Server (SE<model>)* → *<unit> (HNC)* → *Service*, *CSR* tab.

You can use the *CSR* tab to upload, download, and delete configuration data backups.

The functionality of the tab is the same as that for the MU (see section “Managing configuration data (CSR) of the MU” on page 204).

ℹ Perform a CSR backup after each configuration change.

### 10.1.4.8 Generating diagnostic data

To support error diagnosis by Customer Support, the administrator or operator can generate diagnostic data when an error situation occurs and send this to the Support Center.

► Select *Hardware* → *Server (SE<model>)* → *<unit>(HNC)* → *Service*, *Diagnostics* tab.

The functionality of the tab is the same as that for the MU (see section “Generating diagnostic data” on page 205).

The file name of the diagnostic data file for the HNC is:

```
DIAGtar.H<software-version><unit-name>.<datum>.<uhrzeit>.gz
```

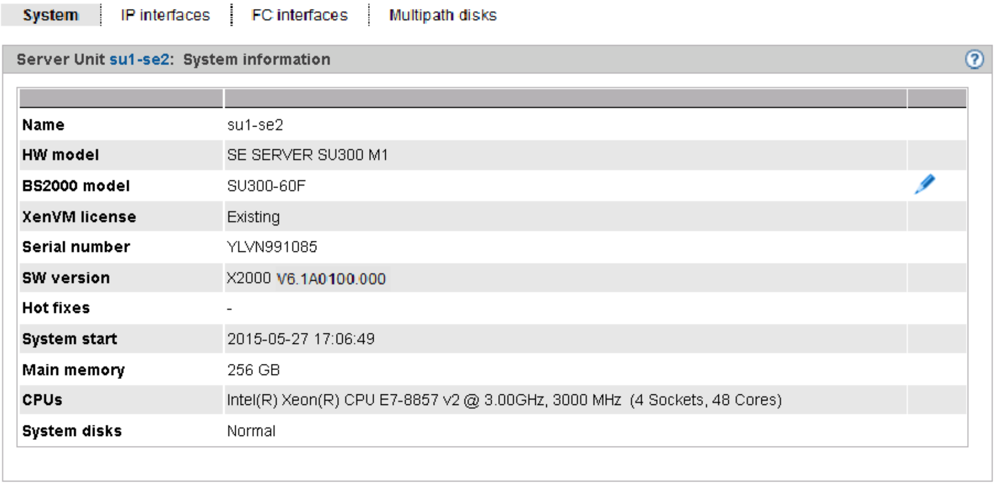
## 10.1.5 Managing Server Unit x86

### 10.1.5.1 Displaying system information and interfaces of the unit

You obtain the system information and interfaces of the <unit> using the associated *Information* menu.

#### Displaying system information of the SU x86

► Select *Hardware* → *Server (SE<model>)* → *<unit> (SU<x86>)* → *Information*, *System* tab.



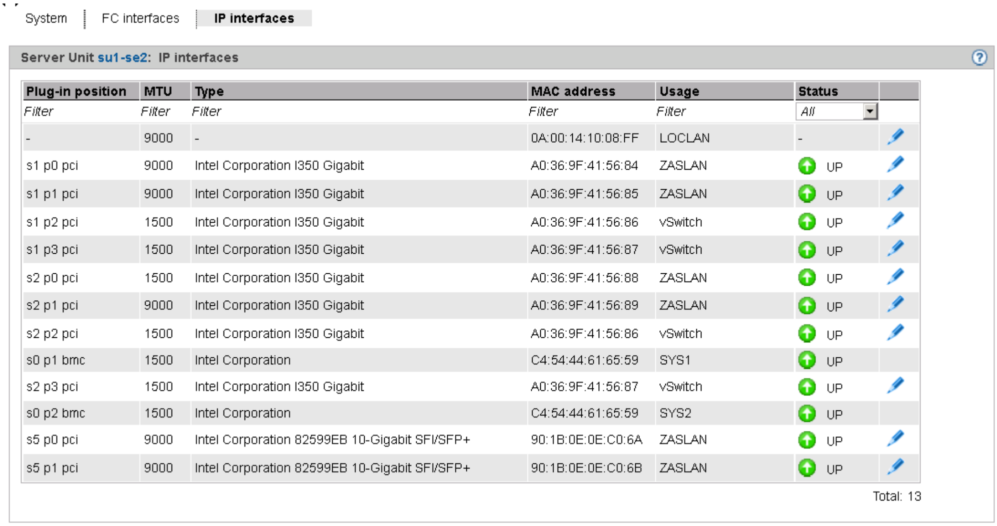
Server Unit su1-se2: System information

| | | |
|---|---|---|
| **Name** | su1-se2 | |
| **HW model** | SE SERVER SU300 M1 | |
| **BS2000 model** | SU300-60F | ✎ |
| **XenVM license** | Existing | |
| **Serial number** | YLVN991085 | |
| **SW version** | X2000 V6.1A0100.000 | |
| **Hot fixes** | - | |
| **System start** | 2015-05-27 17:06:49 | |
| **Main memory** | 256 GB | |
| **CPUs** | Intel(R) Xeon(R) CPU E7-8857 v2 @ 3.00GHz, 3000 MHz (4 Sockets, 48 Cores) | |
| **System disks** | Normal | |

If more than one license is installed on the unit, you can change the *BS2000 model*.

## Displaying and changing IP interfaces of the SU x86

- ► Select *Hardware → Server (SE<model>) → <unit> (SU<x86>) → Information, IP interfaces* tab.



Server Unit su1-se2: IP interfaces

| Plug-in position | MTU | Type | MAC address | Usage | Status | |
|---|---|---|---|---|---|---|
| Filter | Filter | Filter | Filter | Filter | All | |
| - | 9000 | - | 0A:00:14:10:08:FF | LOCLAN | - | ✎ |
| s1 p0 pci | 9000 | Intel Corporation I350 Gigabit | A0:36:9F:41:56:84 | ZASLAN | UP | ✎ |
| s1 p1 pci | 9000 | Intel Corporation I350 Gigabit | A0:36:9F:41:56:85 | ZASLAN | UP | ✎ |
| s1 p2 pci | 1500 | Intel Corporation I350 Gigabit | A0:36:9F:41:56:86 | vSwitch | UP | ✎ |
| s1 p3 pci | 1500 | Intel Corporation I350 Gigabit | A0:36:9F:41:56:87 | vSwitch | UP | ✎ |
| s2 p0 pci | 1500 | Intel Corporation I350 Gigabit | A0:36:9F:41:56:88 | ZASLAN | UP | ✎ |
| s2 p1 pci | 9000 | Intel Corporation I350 Gigabit | A0:36:9F:41:56:89 | ZASLAN | UP | ✎ |
| s2 p2 pci | 1500 | Intel Corporation I350 Gigabit | A0:36:9F:41:56:86 | vSwitch | UP | ✎ |
| s0 p1 bmc | 1500 | Intel Corporation | C4:54:44:61:65:59 | SYS1 | UP | |
| s2 p3 pci | 1500 | Intel Corporation I350 Gigabit | A0:36:9F:41:56:87 | vSwitch | UP | ✎ |
| s0 p2 bmc | 1500 | Intel Corporation | C4:54:44:61:65:59 | SYS2 | UP | |
| s5 p0 pci | 9000 | Intel Corporation 82599EB 10-Gigabit SFI/SFP+ | 90:1B:0E:0E:C0:6A | ZASLAN | UP | ✎ |
| s5 p1 pci | 9000 | Intel Corporation 82599EB 10-Gigabit SFI/SFP+ | 90:1B:0E:0E:C0:6B | ZASLAN | UP | ✎ |

Total: 13

The *FC interfaces* tab provides information about the unit's LAN interfaces. The following function is available to you:

*Changing the packet length in the case of LOCLAN and PCI interfaces*

In the case of a PCI interface you can only change the packet length in normal operation, i.e. the *Status UP* is displayed for the interface.

- ► Click on the *Change* icon by the required IP interface and select the required package length in the subsequent dialog box.

## Displaying FC interfaces of the SU x86

The **FC interfaces** tab provides information about the unit's Fibre Channel interfaces.

- ► Select *Hardware → Server (SE<model>) → <unit> (SU<x86>) → Information, FC interfaces* tab.

Detailed information on the output is provided in the section Displaying FC interfaces of the MU.

### Displaying multipath disks of the SU x86

For the FC disks of the SU x86 you can display the status of the paths between the SU x86 and the storage system and also of their end points on the storage system and the SU x86.

► Select *Hardware* → *Server (SE<model>)* → *<unit> (SU<x86>)* → *Information*, *Multipath disks* tab.

Detailed information on the output is provided in the section Displaying multipath disks of the MU.

### 10.1.5.2 Managing the IP configuration of the SU x86

You manage the IP configuration of the SU x86 using the associated *Management* menu, *IP configuration* tab.

► Select *Hardware* → *Server (SE<model>)* → *<unit> (SU<x86>)* → *Management*, *IP configuration* tab.

Using the *IP configuration* tab you can change the host name and network properties and add network addresses.

The functionality of the tab is the same as that for the MU (see section “Managing the IP configuration” on page 193) with the following restriction:

i If only the standard networks LOCLAN, MCNLO, and MCNPR are assigned on the SU x86, the buttons for changes are not enabled.

### 10.1.5.3 Managing routing of the SU x86

You manage routing of the SU x86 using the associated *Management* menu, *Routing & DNS* tab.

► Select *Hardware* → *Server* → *<unit> (SU<x86>)* → *Management*, *Routing & DNS* tab.

The routing is displayed in the upper *Routing* group on the tab.

The functionality of the tab is the same as that for the MU (see section “Managing routing of the Management Unit” on page 195) with the following restriction:

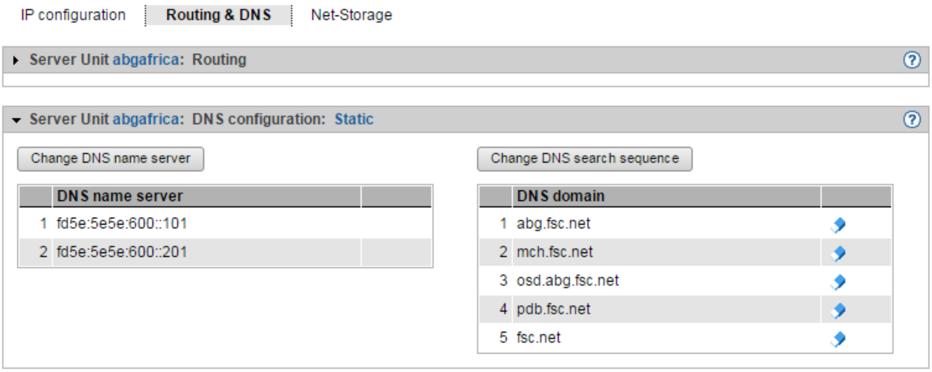
i The MANPU and MONPU networks are not available on an SU x86.

The *Add new route* and *Delete route* actions are only available for Net-Storage connections.

### 10.1.5.4 Managing the DNS configuration of the SU x86

You manage the DNS configuration of the SU x86 using the associated *Management* menu, *Routing & DNS* tab.

► Select *Hardware* → *Server* → *<unit> (SU<x86>)* → *Management*, *Routing & DNS* tab.



▸ Server Unit abgafrica: Routing

▾ Server Unit abgafrica: DNS configuration: Static

| | DNS name server | |
|---|---|---|
| 1 | fd5e:5e5e:600::101 | |
| 2 | fd5e:5e5e:600::201 | |

| | DNS domain | |
|---|---|---|
| 1 | abg.fsc.net | ✎ |
| 2 | mch.fsc.net | ✎ |
| 3 | osd.abg.fsc.net | ✎ |
| 4 | pdb.fsc.net | ✎ |
| 5 | fsc.net | ✎ |

The *Routing & DNS* tab displays the DNS configuration in the lower group *DNS configuration*.

The functionality of the tab is largely the same as that for the MU (see section “Managing the DNS configuration” on page 196).

### 10.1.5.5 Configuring Net-Storage on the SU x86

Access to Net-Storage (storage access via NFS) is possible for BS2000 systems (for Native BS2000 and the BS2000 VMs) of the SU x86 provided the prerequisites are fulfilled in X2000.

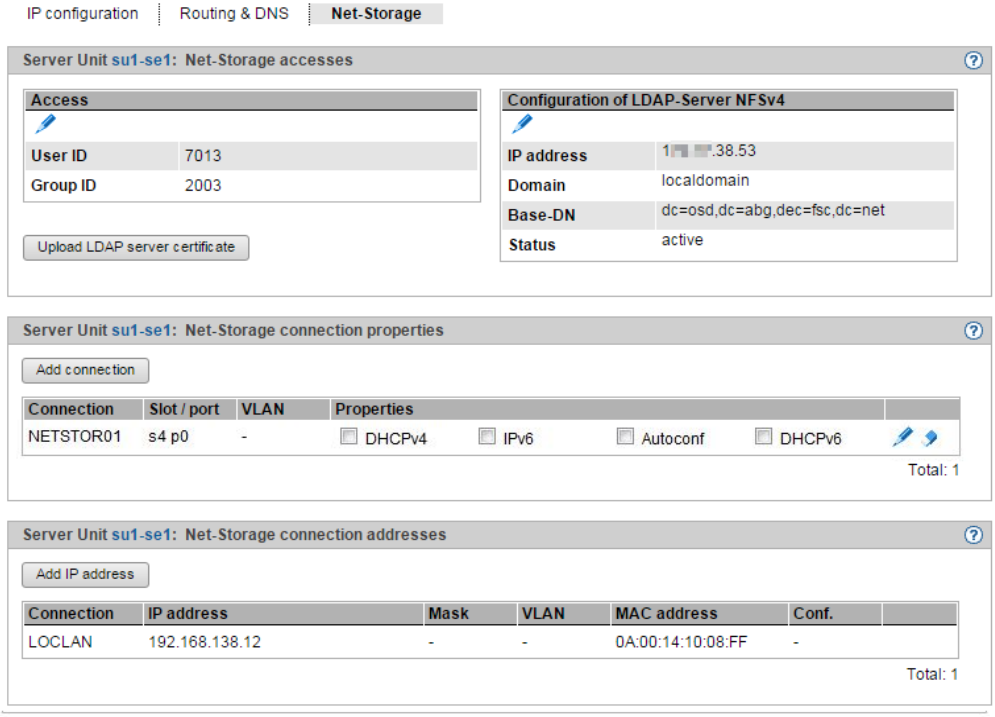
– As net client the SU x86 requires access rights for the net server which provides the Net-Storage. Authentication takes place either via user and group IDs or via an LDAP server NFSv4.

> **i** Access via an LDAP server is only possible if the LDAP server's certificate has been downloaded to the unit.
>
> If the LDAP server's configuration is not active or invalid or is being deleted, authentication takes place using the local user and group.

– Each Net-Storage connection must be configured in the network.

You configure Net-Storage in X2000 of the SU x86 using the *Management* menu, *Net-Storage* tab.

► Select *Hardware* → *Server(SE<model>)* → *<unit>(SU<x86>)* → *Management*, *Net-Storage* tab.



Server Unit su1-se1: Net-Storage accesses

| Access | |
|---|---|
| User ID | 7013 |
| Group ID | 2003 |

| Configuration of LDAP-Server NFSv4 | |
|---|---|
| IP address | 1[redacted].38.53 |
| Domain | localdomain |
| Base-DN | dc=osd,dc=abg,dec=fsc,dc=net |
| Status | active |

Server Unit su1-se1: Net-Storage connection properties

| Connection | Slot / port | VLAN | Properties | | | | |
|---|---|---|---|---|---|---|---|
| NETSTOR01 | s4 p0 | - | □ DHCPv4 | □ IPv6 | □ Autoconf | □ DHCPv6 | |

Total: 1

Server Unit su1-se1: Net-Storage connection addresses

| Connection | IP address | Mask | VLAN | MAC address | Conf. | |
|---|---|---|---|---|---|---|
| LOCLAN | 192.168.138.12 | - | - | 0A:00:14:10:08:FF | - | |

Total: 1

The *Net-Storage* tab displays the *Net-Storage accesses*, *Net-Storage connection properties*, and *Net-Storage connection addresses* groups.

The following functions are available:

*Changing accesses for the SU x86*

The *Access right* table displays the current user and group IDs for Net-Storage access. If no LDAP configuration is active, authentication takes place using this entry.

► In the *Net-Storage accesses* group click the *Change* icon by *Access*. In the subsequent dialog box change the user and/or group ID and confirm the action.

*Uploading an LDAP server certificate to the SU x86*

► In the *Net-Storage accesses* group click *Upload LDAP server certificate*, select the certificate file in the subsequent dialog box, and confirm the action.

*Entering or changing the LDAP configuration of the SU x86*

► In the *Net-Storage accesses* group click the *Change* icon by *Configuration of LDAP-Server <server>*, enter the required properties in the subsequent dialog box, and confirm the action.

*Deleting configuration data for the LDAP server*

► In the *Net-Storage accesses* group click the *Delete* icon by *Configuration of LDAP-Server <server>* and confirm the action.

i Following deletion, authentication takes place using the user and group IDs entered. Net-Storage access is then only possible if valid values are entered.

*Adding a Net-Storage connection to the SU x86*

► In the *Net-Storage connection properties* group click *Add connection*, make the required entries in the subsequent dialog box, and confirm the action.

*Removing the Net-Storage:connection*

► In the *Net-Storage connection properties* group click the *Remove* icon by the required Net-Storage connection and confirm the action.

*Adding a Net-Storage connection address (SU x86)*

► In the *Net-Storage connection addresses* group click *Add new IP address*, make the required entries in the subsequent dialog box, and confirm the action.

*Removing a Net-Storage connection address*

► In the *Net-Storage connection addresses* group click the *Remove* icon by the required Net-Storage connection and confirm the action.

### 10.1.5.6 Managing updates of the SU x86

Fundamental information on updates is provided in section “Maintenance and remote service” on page 62.

You manage updates of the SU x86 using the associated *Service* menu, *Update* tab.

▶ Select *Hardware* → *Server (SE<model>)* → *<unit> (SU<x86>)* → *Service*, *Update* tab.

An expandable group is displayed on the *Update* tab for each of the software updates *Security Fixes*, *Service Packs* and *Hot Fixes*.

With the exception of the *Add-on Packs*, the functionality of the tab is the same as that for the MU (see section “Managing updates of the Management Unit” on page 202).

### 10.1.5.7 Managing configuration data (CSR) of the SU x86

You use a CSR backup (CSR = Configuration Save and Restore) to back up the configuration data of the Server Unit in an archive. The backup archive contains the complete configuration of the basic system, e.g. the devices (BS2000 and XenVM), the XenVMs, and the Net-Storage configuration. Each backup archive has a creation date and an archive name.

A CSR backup enables the configuration of the unit concerned at the time the backup was made to be restored.

i Perform a CSR backup after each configuration change.

▶ Select *Hardware* → *Server (SE<model>)* → *<unit> (SU<x86>)* → *Service*, *CSR* tab.

You can use the *CSR* tab to upload, download, and delete configuration data backups.

The functionality of the tab is the same as that for the MU (see section “Managing configuration data (CSR) of the MU” on page 204).

### 10.1.5.8 Generating diagnostic data

To support error diagnosis by Customer Support, the administrator or operator can generate diagnostic data when an error situation occurs and send this to the Support Center.

► Select *Hardware → Server (SE<model>) → <unit> (SU<x86>) → Service*, *Diagnostics* tab.

The functionality of the tab is the same as that for the MU (see section “Generating diagnostic data” on page 205).

The file name of the diagnostic data file for the SU x86 is:

```
DIAGtar.X<software-version><unit-name>.<datum>.<uhrzeit>.gz
```

## 10.1.6 Managing Application Units

An SE server can optionally contain autonomous high-end x86-64 servers, so-called Application Units (AUs).

The Application Units are integrated into the rack of the SE server when it is supplied, the internal network is preconfigured, and if requested the operating system is also installed. The Application Units are incorporated in the status display of the SE Manager and in the remote service procedure for SE servers.

As administrator you install your own software (e.g. Networker StorageNode or Oracle products) on the Application Units and perform other administration and configuration tasks. You add installed applications with web interfaces to the list of applications in the SE Manager, which enables you to call these applications directly from the SE Manager.

You can access the applications with all roles. As operator or XenVM administrator the administration functions for modifying the data for accessing Application Units are not available to you.

**Remote access to the console of the Application Unit**

For Application Units of the type AU25 and AU47, the iRMC function *Video Redirection* enables remote access to the console of the Application Unit. The console has the same functions as the local console.

The web interface of the Management Board can be opened in the same way for partitions of AU87/DBU87.

The iRMC/Management Board is also linked in the system operation of the AU or AU partition.

### 10.1.6.1 Configuring an Application Unit

Application Units are integrated into the status monitoring and display of the SE Manager and the remote service procedure of the SE server. The connection to these procedures is established via basic mechanisms of the operating system on the Application Unit (SNMP query). No further software is required on the Application Units for the connection.

You check and modify the configuration of the Application Unit in the following cases:

- You (re)install the Application Unit.
- You change the IP address space of MANPU
- You change the IP address of the MU in MANPU.

i Further information is provided in the online help under "Configuration on the Application Unit."

### Change LAN configuration of the Application Unit

If your Application Unit is connected or is to be connected via MANPU, you must change or set the IP addresses of the Application Unit for MANPU in the following cases:

- You (re)install the Application Unit.
- You change the IP address space of MANPU

You must perform the following steps to do this:

1. Use operating system resources on the Application Unit to change or set the LAN configuration of the LAN interface for the MANPU.
2. On the Application Unit, use the Linux and Windows operating systems to change or set the SNMP configuration according to the (new) IP address space of the MANPU.
3. Only when you are modifying the IP address space of the MANPU:

   Modify the LAN configuration of the MU using the SE Manager.

### Integrating an Application Unit into status monitoring

The hardware status of the Application Unit is determined by means of an SNMP query from the Management Unit to the ServerView agent on the Application Unit via the management LAN. To permit this the ServerView agents must be installed and SNMP must be configured on the Application Unit.

Detailed and operating-system-specific information about the SNMP configuration is available in the online help system.

► Check the implemented configuration.

  The configuration is correct when the following conditions are satisfied:
  – The Application Unit in the SE server overview on the Management Unit is displayed with the status *Running*.
  – The hardware information of the Application Unit is displayed in the information for the Application Unit.

### Integrating an Application Unit into the remote service procedure

An Application Unit is integrated into the remote service procedure with reporting of hardware errors to the Service Center (call home) by forwarding hardware error messages to the Management Unit. For Application Units with the Linux and Windows operating systems, ServerView agents and the ServerView RAID Manager must also be installed for the purpose of hardware monitoring.

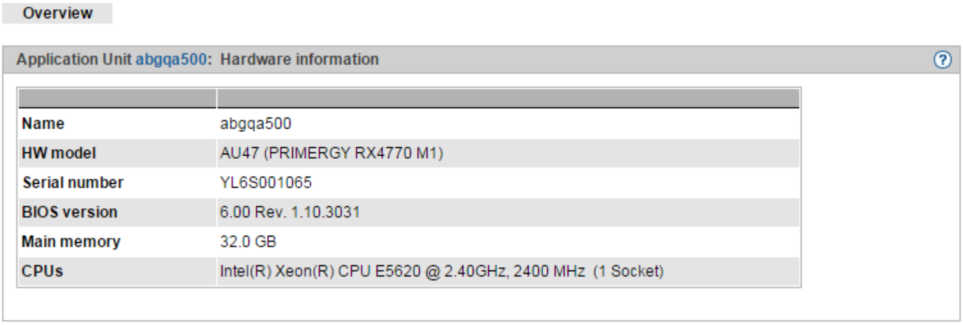
On the Management Unit the messages forwarded from the Application Units are filtered further and sent to the Service Center using the remote service procedure AIS Connect.

The Application Unit thus reports on hardware errors to the Management Unit in two ways:

- Trap forwarding from the iRMC
- Trap forwarding from the Management Board

### 10.1.6.2 Displaying hardware information of the Application Unit

► Select *Hardware* → *Server (SE<model>)* → *<unit> (AU<model>)* → *Information*, *Overview* tab.



Application Unit abgqa500: Hardware information

| | |
|---|---|
| **Name** | abgqa500 |
| **HW model** | AU47 (PRIMERGY RX4770 M1) |
| **Serial number** | YL6S001065 |
| **BIOS version** | 6.00 Rev. 1.10.3031 |
| **Main memory** | 32.0 GB |
| **CPUs** | Intel(R) Xeon(R) CPU E5620 @ 2.40GHz, 2400 MHz (1 Socket) |

The *Overview* tab displays hardware information on the selected unit.

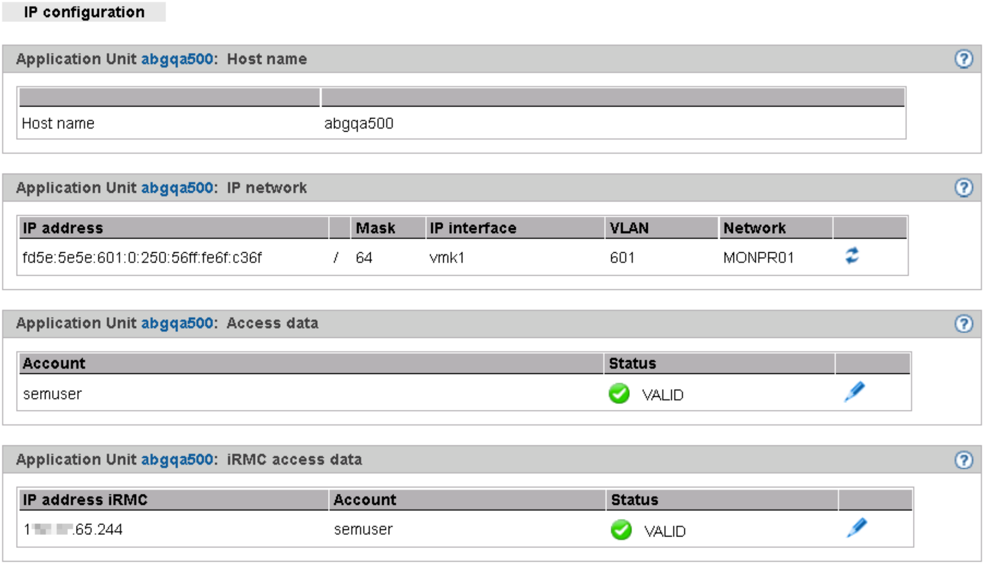
### 10.1.6.3 Managing the IP configuration of the Application Unit

When managing the IP configuration, there are differences between Application Units of the type AU25/AU47 and Application Units of the type AU87/DBU87.

#### Managing IP configuration of the Application Unit type AU25/AU47

You manage the IP configuration of an AU25 and AU47 using the associated *Management* menu, *IP configuration* tab.

► Select *Hardware → Server (SE<model>) → <unit> (AU<model>) → Management*, *IP configuration* tab.



**IP configuration**

**Application Unit abgqa500: Host name**

| | |
|---|---|
| Host name | abgqa500 |

**Application Unit abgqa500: IP network**

| IP address | | Mask | IP interface | VLAN | Network | |
|---|---|---|---|---|---|---|
| fd5e:5e5e:601:0:250:56ff:fe6f:c36f | / | 64 | vmk1 | 601 | MONPR01 | ⟳ |

**Application Unit abgqa500: Access data**

| Account | Status | |
|---|---|---|
| semuser | ✓ VALID | ✎ |

**Application Unit abgqa500: iRMC access data**

| IP address iRMC | Account | Status | |
|---|---|---|---|
| 1[redacted].65.244 | semuser | ✓ VALID | ✎ |

The *IP configuration* tab displays the groups *Host name, IP network, Access data* (only for AU with the VMware vSphere operating system), and *iRMC access data*.

The following functions are available:

*Updating network data*

You can cause the current data to be determined again and the display to be updated.

► In the *IP networks* group click the *Update network data* icon and confirm the action.

*Changing access data of the Application Unit*

You can change the access data of the Application Unit only if the Application Unit is operated with the VMware vSphere operating system.

► In the *Application Unit <unit> Access data* group, click the *Change AU password* icon for the required account, change the account/password in the subsequent dialog box, and confirm the action.

*Changing access data of the Application Unit's iRMC access*

The hardware status is determined for all Application Units using the iRMC. When the password on the iRMC is changed, you must also change the password here.

► In the *iRMC access data* group, click the *Change iRMC address and password* icon by the required IP address iRMC, change the *IP address iRMC* or the *Account* and confirm the action.

### Managing IP configuration of the Application Unit type AU87/DBU87

IP configuration of an AU87 or DBU87 is distributed to the *Chassis* and *Partition* levels.

At chassis level, access to the Management Board is configured centrally:

► Select *Hardware → Server (SE<model>) → <unit> (AU87/DBU87) → Management*, *IP configuration* tab.

In the *Management Board access data* area you can change the IP address and password.

At partition level access to the particular partition's system is configured:

► Select *Hardware → Server (SE<model>) → <unit> (AU87/DBU87) → <partition> → Management*, *IP configuration* tab.

In the *IP networks* area you can update network data.

# 10.2 Managing IP networks

You manage the IP networks of the SE server using the tree structure: *Hardware → IP networks*. All IP networks are listed in this menu.

## 10.2.1 Displaying information on networks and switches

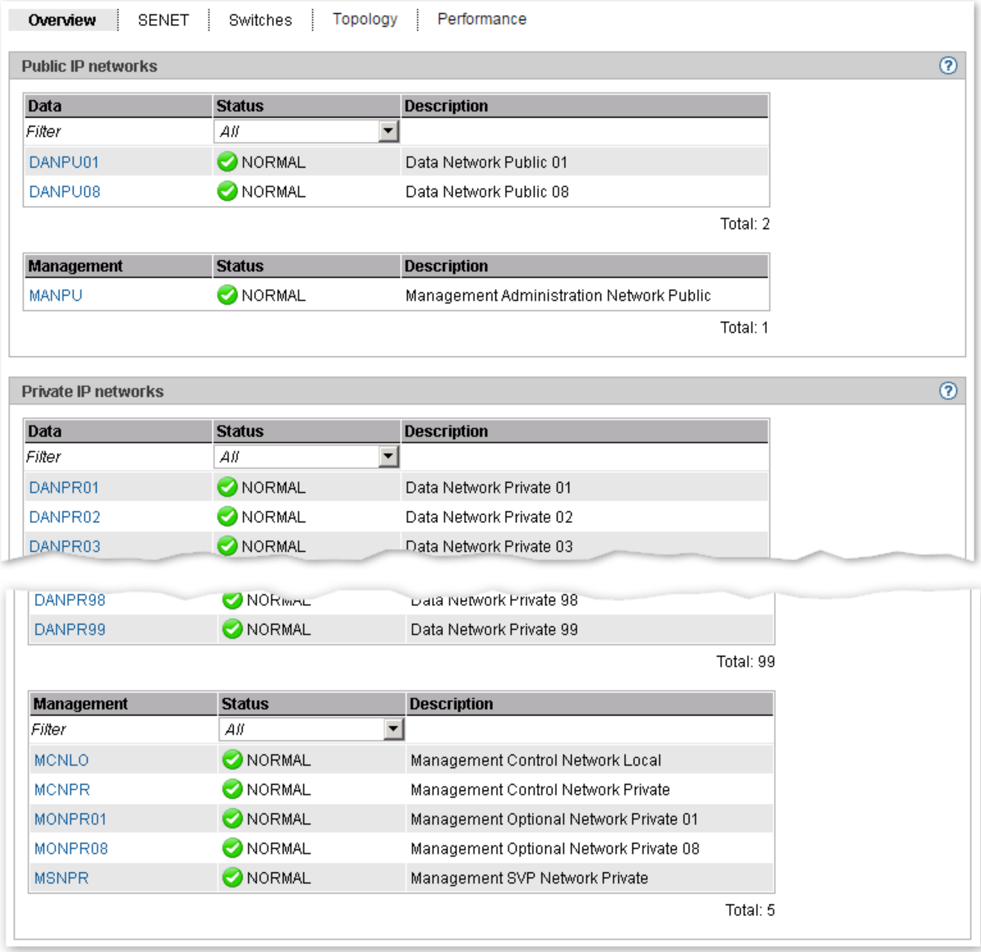
You can display the following information on IP networks:

- Overview of IP networks
- Information on the IP network SENET
- Information on switches
- Graphical display of the internal IP network topology
- Overview of the performance and utilization of the Net Unit ports

### 10.2.1.1 Overview of IP networks

You obtain the overview of the public and private IP networks using the associated *Overview* tab.

► Select *Hardware* → *IP networks*, *Overview* tab.



Public IP networks

| Data | Status | Description |
|---|---|---|
| *Filter* | *All* | |
| DANPU01 | ✓ NORMAL | Data Network Public 01 |
| DANPU08 | ✓ NORMAL | Data Network Public 08 |

Total: 2

| Management | Status | Description |
|---|---|---|
| MANPU | ✓ NORMAL | Management Administration Network Public |

Total: 1

Private IP networks

| Data | Status | Description |
|---|---|---|
| *Filter* | *All* | |
| DANPR01 | ✓ NORMAL | Data Network Private 01 |
| DANPR02 | ✓ NORMAL | Data Network Private 02 |
| DANPR03 | ✓ NORMAL | Data Network Private 03 |
| DANPR98 | ✓ NORMAL | Data Network Private 98 |
| DANPR99 | ✓ NORMAL | Data Network Private 99 |

Total: 99

| Management | Status | Description |
|---|---|---|
| *Filter* | *All* | |
| MCNLO | ✓ NORMAL | Management Control Network Local |
| MCNPR | ✓ NORMAL | Management Control Network Private |
| MONPR01 | ✓ NORMAL | Management Optional Network Private 01 |
| MONPR08 | ✓ NORMAL | Management Optional Network Private 08 |
| MSNPR | ✓ NORMAL | Management SVP Network Private |

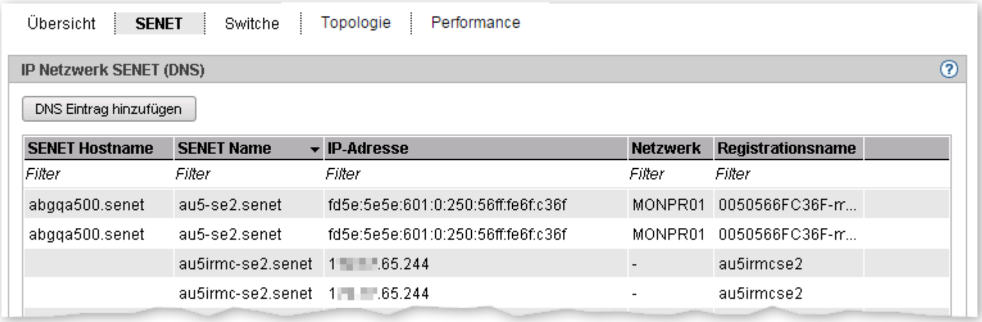
Total: 5

The *Overview* tab displays information on public and private networks.

### 10.2.1.2 Information on the IP network SENET

SENET contains the internal DNS configuration of the SE server. The IP network SENET is displayed on the *SENET* tab.

► Select *Hardware → IP networks, SENET* tab.



| SENET Hostname | SENET Name | IP-Adresse | Netzwerk | Registrationsname |
|---|---|---|---|---|
| *Filter* | *Filter* | *Filter* | *Filter* | *Filter* |
| abgqa500.senet | au5-se2.senet | fd5e:5e5e:601:0:250:56ff:fe6f:c36f | MONPR01 | 0050566FC36F-rr... |
| abgqa500.senet | au5-se2.senet | fd5e:5e5e:601:0:250:56ff:fe6f:c36f | MONPR01 | 0050566FC36F-rr... |
| | au5irmc-se2.senet | 1[redacted].65.244 | - | au5irmcse2 |
| | au5irmc-se2.senet | 1[redacted].65.244 | - | au5irmcse2 |

The *SENET* tab displays all DNS entries of the SENET.

The following function is available:

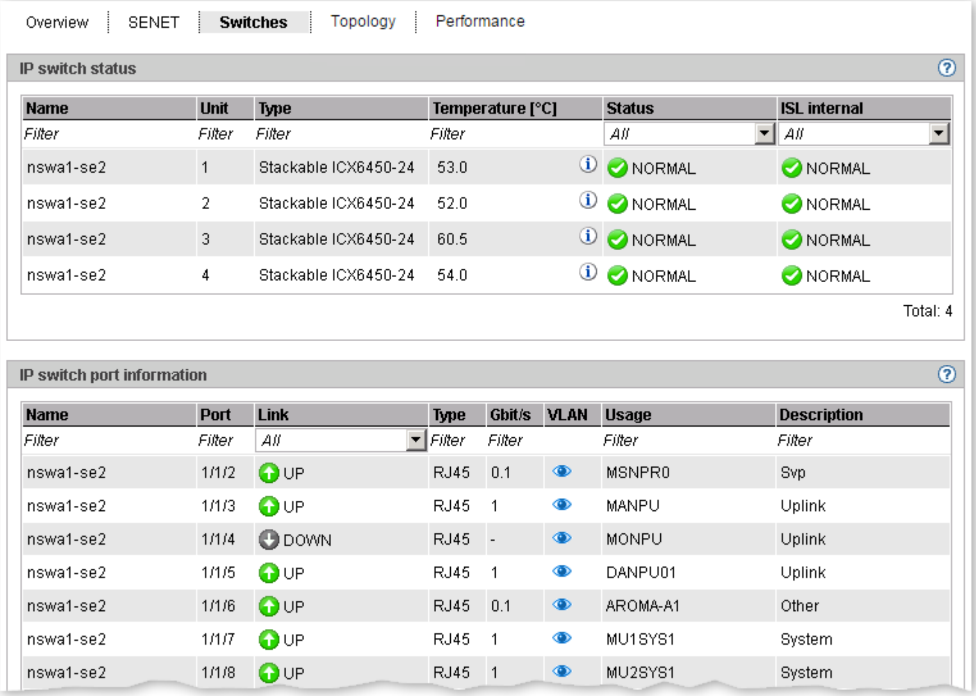
*Adding a new DNS entry to the SENET*

► In the *SENET* tab click *Add DNS entry* and proceed as described in section “Configuring SENET”.

### 10.2.1.3 Information on switches

The information on switches is displayed in the *Switches* tab.

► Select *Hardware → IP networks, Switches* tab.



IP switch status

| Name | Unit | Type | Temperature [°C] | Status | ISL internal |
|---|---|---|---|---|---|
| *Filter* | *Filter* | *Filter* | *Filter* | *All* | *All* |
| nswa1-se2 | 1 | Stackable ICX6450-24 | 53.0 ⓘ | ✓ NORMAL | ✓ NORMAL |
| nswa1-se2 | 2 | Stackable ICX6450-24 | 52.0 ⓘ | ✓ NORMAL | ✓ NORMAL |
| nswa1-se2 | 3 | Stackable ICX6450-24 | 60.5 ⓘ | ✓ NORMAL | ✓ NORMAL |
| nswa1-se2 | 4 | Stackable ICX6450-24 | 54.0 ⓘ | ✓ NORMAL | ✓ NORMAL |

Total: 4

IP switch port information

| Name | Port | Link | Type | Gbit/s | VLAN | Usage | Description |
|---|---|---|---|---|---|---|---|
| *Filter* | *Filter* | *All* | *Filter* | *Filter* | | *Filter* | *Filter* |
| nswa1-se2 | 1/1/2 | ⬆ UP | RJ45 | 0.1 | 👁 | MSNPR0 | Svp |
| nswa1-se2 | 1/1/3 | ⬆ UP | RJ45 | 1 | 👁 | MANPU | Uplink |
| nswa1-se2 | 1/1/4 | ⬇ DOWN | RJ45 | - | 👁 | MONPU | Uplink |
| nswa1-se2 | 1/1/5 | ⬆ UP | RJ45 | 1 | 👁 | DANPU01 | Uplink |
| nswa1-se2 | 1/1/6 | ⬆ UP | RJ45 | 0.1 | 👁 | AROMA-A1 | Other |
| nswa1-se2 | 1/1/7 | ⬆ UP | RJ45 | 1 | 👁 | MU1SYS1 | System |
| nswa1-se2 | 1/1/8 | ⬆ UP | RJ45 | 1 | 👁 | MU2SYS1 | System |

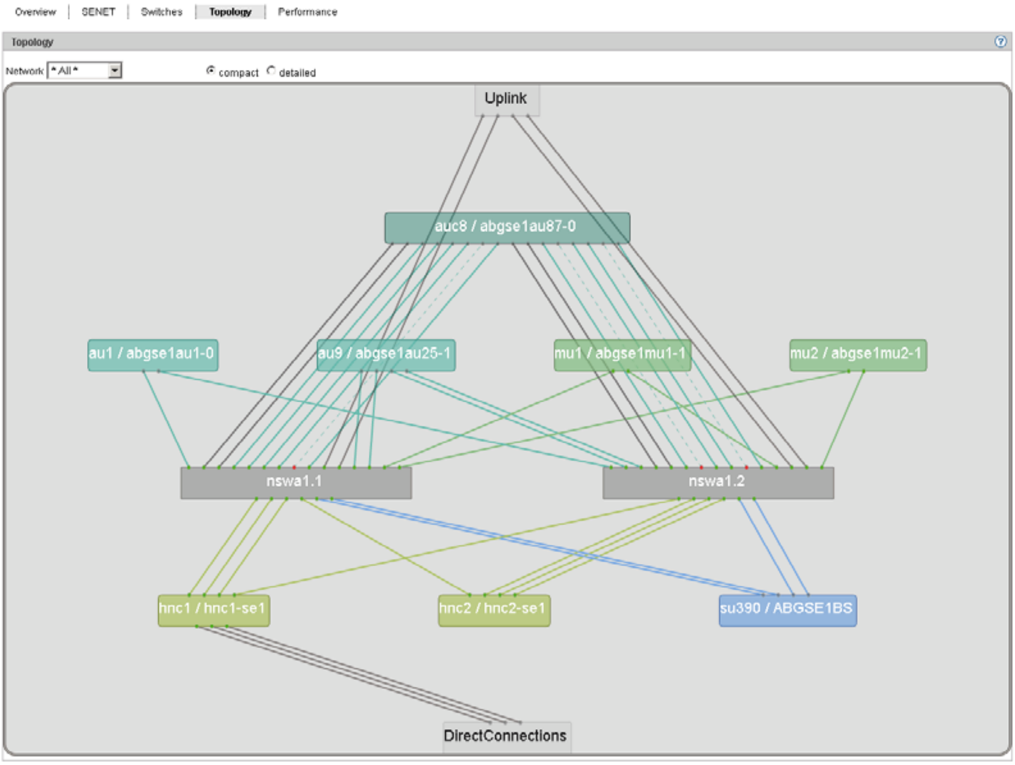
The *Switches* tab displays information on switches and port information.

► Click the *Display/Details* icon (eye) in the entry for a switch port. The VLAN connection for this switch port is displayed in a dialog box.

### 10.2.1.4 Graphical display of the internal IP network topology

A graphical display of the network topology with all the network components and connections is displayed in the *Topology* tab.

► Select *Hardware → IP networks*, *Topology* tab.

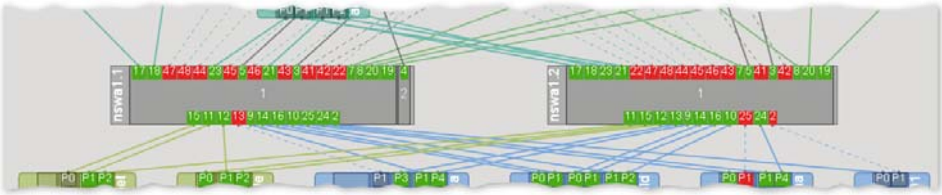


Network * All *

◉ compact ○ detailed

You can influence the display:

- In the display of the topology of all IP networks you can have a selected network highlighted, i.e. this network is displayed normally and the components of all other IP networks are grayed out.
- You can choose between the compact (simple) display and the detailed display in which the interfaces of the various slots and ports of a unit are shown (in the figure below you will find a section of the display as an example).



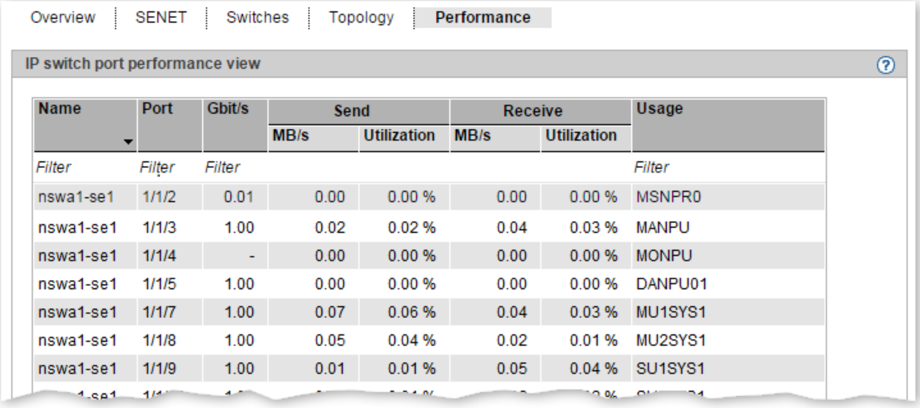
When you drag the mouse cursor over a network component, a tool tip displays detailed information on it (if available).

In the case of AU87 or DBU87, the chassis and system components IO Unit and Management Board are displayed together as one unit.

### 10.2.1.5 Overview of the performance and utilization of the Net Unit ports

An overview of the performance and utilization of the switches in the Net Unit is supplied by the *Performance* tab. The maximum and current data throughput rate (in MB/s) and the utilization (in %) are displayed for each Net Unit port (for each of the Net Unit's connections). A distinction is made between the send and receive directions for data throughput and utilization.

- ► Select *Hardware → IP networks*, *Performance* tab.



IP switch port performance view

| Name | Port | Gbit/s | Send | | Receive | | Usage |
|---|---|---|---|---|---|---|---|
| | | | MB/s | Utilization | MB/s | Utilization | |
| Filter | Filter | Filter | | | | | Filter |
| nswa1-se1 | 1/1/2 | 0.01 | 0.00 | 0.00 % | 0.00 | 0.00 % | MSNPR0 |
| nswa1-se1 | 1/1/3 | 1.00 | 0.02 | 0.02 % | 0.04 | 0.03 % | MANPU |
| nswa1-se1 | 1/1/4 | - | 0.00 | 0.00 % | 0.00 | 0.00 % | MONPU |
| nswa1-se1 | 1/1/5 | 1.00 | 0.00 | 0.00 % | 0.00 | 0.00 % | DANPU01 |
| nswa1-se1 | 1/1/7 | 1.00 | 0.07 | 0.06 % | 0.04 | 0.03 % | MU1SYS1 |
| nswa1-se1 | 1/1/8 | 1.00 | 0.05 | 0.04 % | 0.02 | 0.01 % | MU2SYS1 |
| nswa1-se1 | 1/1/9 | 1.00 | 0.01 | 0.01 % | 0.05 | 0.04 % | SU1SYS1 |

## 10.2.2 Configuring SENET

The *SENET* tab enables you to add or remove a DNS entry and change the host name.

► Select *Hardware → IP networks, SENET* tab.

The *SENET* tab displays all the SENET's DNS entries.

The following functions are available:

*Adding a DNS entry*

► Click the *Add DNS entry* tab and follow the instructions of the wizard.

*Removing a DNS entry*

► Click the *Remove* icon by the DNS entry you wish to remove.

*Changing a host name*

► Click the *Change* icon by the DNS entry whose host name you wish to change and enter the new host name in the subsequent dialog box.

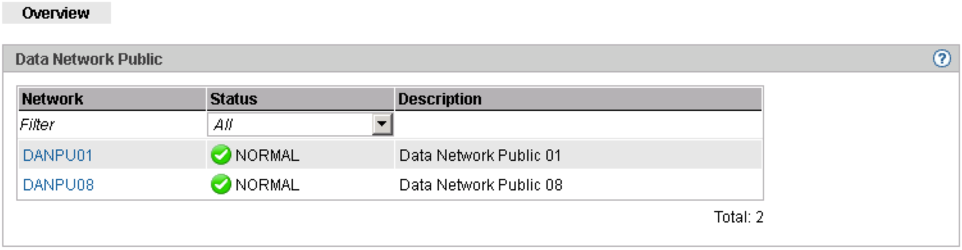
### 10.2.3 Managing a Data Network Public

You manage a Data Network Public (DANPU) using the menu item *Data Network Public* in the *IP networks* menu. Up to eight DANPUs can exist. These are named DANPU01, DANPU02, etc.

i Further DANPU networks are configured by the Customer Support staff.

#### Overview of all DANPUs

► Select *Hardware → IP networks → Data Network Public, Overview* tab.



Data Network Public

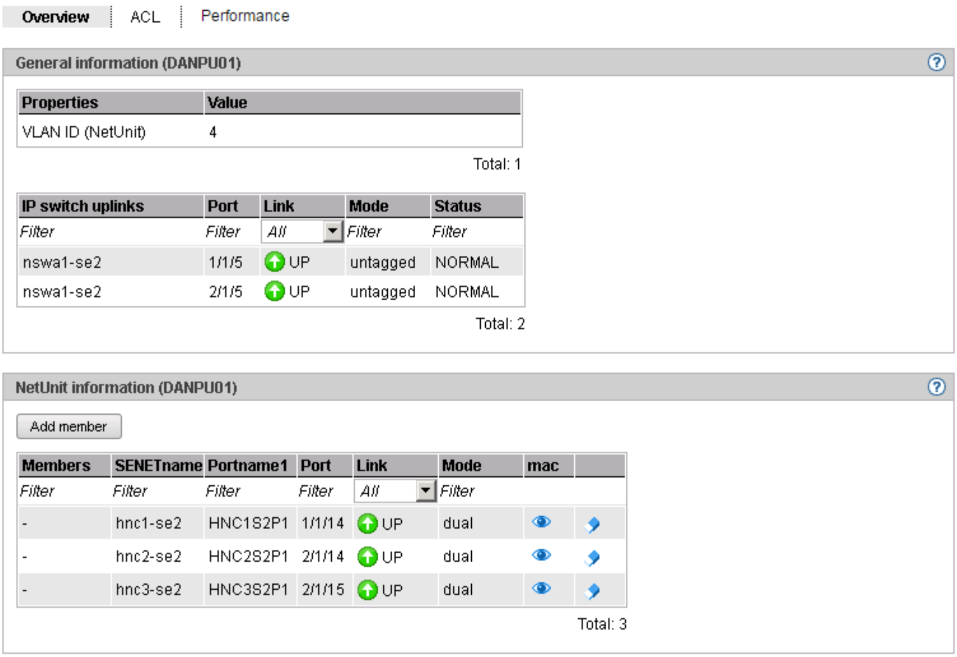
| Network | Status | Description |
|---|---|---|
| *Filter* | *All* ▼ | |
| DANPU01 | ✓ NORMAL | Data Network Public 01 |
| DANPU08 | ✓ NORMAL | Data Network Public 08 |

Total: 2

The tab displays all information on the existing DANPUs.

### Overview of the various DANPUs

► Select *Hardware → IP networks → Data Network Public → DANPU<no>*, *Overview* tab.



General information (DANPU01)

| Properties | Value |
|---|---|
| VLAN ID (NetUnit) | 4 |

Total: 1

| IP switch uplinks | Port | Link | Mode | Status |
|---|---|---|---|---|
| *Filter* | *Filter* | *All* | *Filter* | *Filter* |
| nswa1-se2 | 1/1/5 | ⬆ UP | untagged | NORMAL |
| nswa1-se2 | 2/1/5 | ⬆ UP | untagged | NORMAL |

Total: 2

NetUnit information (DANPU01)

| Members | SENETname | Portname1 | Port | Link | Mode | mac | |
|---|---|---|---|---|---|---|---|
| *Filter* | *Filter* | *Filter* | *Filter* | *All* | *Filter* | | |
| - | hnc1-se2 | HNC1S2P1 | 1/1/14 | ⬆ UP | dual | 👁 | ✎ |
| - | hnc2-se2 | HNC2S2P1 | 2/1/14 | ⬆ UP | dual | 👁 | ✎ |
| - | hnc3-se2 | HNC3S2P1 | 2/1/15 | ⬆ UP | dual | 👁 | ✎ |

Total: 3

The *Overview* tab displays all information on the selected DANPU.

The following functions are available:

*Displaying the MAC address*

► In the *Net Unit information (DANPU<no>)* group click the *MAC addresses* icon (eye) by the required unit.

The subsequent dialog box *Display MAC address* displays the unit's active address.

*Adding ports*

► In the *Net Unit information (DANPU<no>)* group click *Add member*, follow the instructions of the wizard, and select the required port.

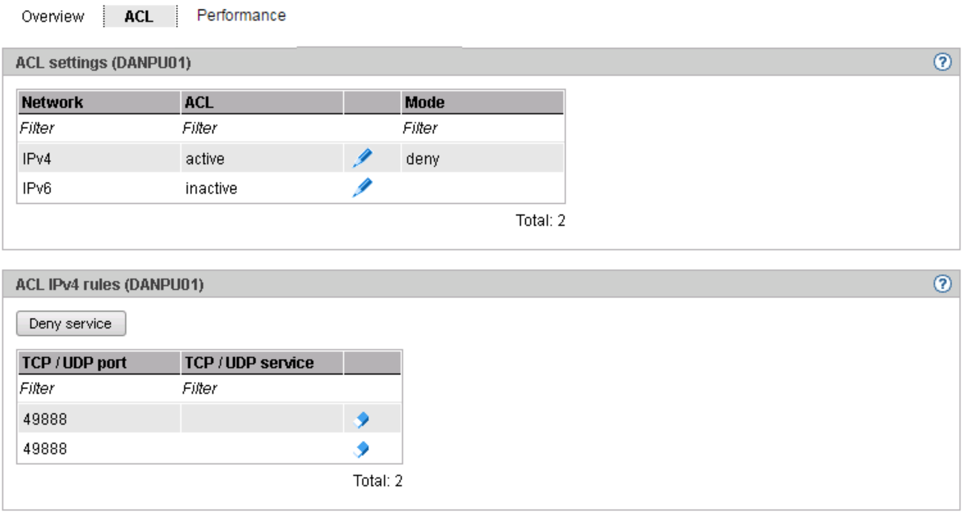
*Removing a port*

► In the *Net Unit information (DANPU<no>)* group click the *Remove* icon by the required unit, follow the instructions of the wizard, and confirm the action.

### 10.2.3.1 Configuring the ACL settings of the DANPU network

The ACL (Access Control List) defines the access settings for the DANPUs. You can add and delete ACL entries for each *DANPU<no>*.

► Select *Hardware → IP networks → Data Network Public → DANPU<no>*, *ACL* tab.



ACL settings (DANPU01)

| Network | ACL | | Mode |
|---|---|---|---|
| *Filter* | *Filter* | | *Filter* |
| IPv4 | active | ✎ | deny |
| IPv6 | inactive | ✎ | |

Total: 2

ACL IPv4 rules (DANPU01)

| TCP / UDP port | TCP / UDP service | |
|---|---|---|
| *Filter* | *Filter* | |
| 49888 | | ◆ |
| 49888 | | ◆ |

Total: 2

The *ACL* tab displays a list of the ACL settings.

*Changing an ACL setting*

You can:

– enable or disable an ACL and associated network access control on a network-specific basis,

– select the ACL mode (*permit* or *deny*). In *permit* mode only the ports/services contained in the ACL are permitted network access. All other services are locked. In *deny* mode only the ports/services contained in the ACL are locked.

► In the ACL settings group click the *Change* icon by the required entry and enter the new settings in the subsequent dialog box.

⚠ If you set *permit* mode and enable ACL without entering services in the list, network access is locked for all services.

*Adding a service to the ACL*

► In the *ACL rules* group click *Deny service* (in the case of ACL mode *deny*) or *Permit service* (in the case of ACL mode *permit*) and select the ports and the services associated with them which are to be added to the ACL.

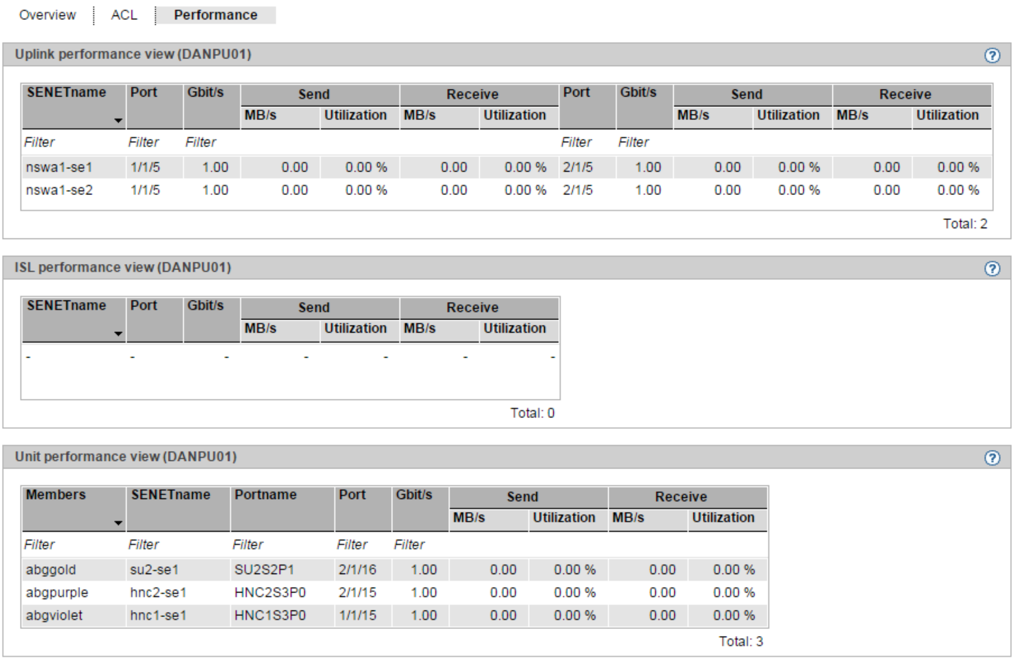
*Removing a service from the ACL*

► In the *ACL rules* group click the *Remove* icon by the required entry and confirm the action.

### 10.2.3.2 Information on the performance and utilization of the DANPU ports

An overview of the performance and utilization of the ports belonging to the network is provided by the *Performance* tab.

► Select *Hardware* → *IP networks* → *Data Network Public* → *DANPU<no>*, *Performance* tab.



Overview | ACL | **Performance**

**Uplink performance view (DANPU01)**

| SENETname | Port | Gbit/s | Send | | Receive | | Port | Gbit/s | Send | | Receive | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | MB/s | Utilization | MB/s | Utilization | | | MB/s | Utilization | MB/s | Utilization |
| Filter | Filter | Filter | | | | | Filter | Filter | | | | |
| nswa1-se1 | 1/1/5 | 1.00 | 0.00 | 0.00 % | 0.00 | 0.00 % | 2/1/5 | 1.00 | 0.00 | 0.00 % | 0.00 | 0.00 % |
| nswa1-se2 | 1/1/5 | 1.00 | 0.00 | 0.00 % | 0.00 | 0.00 % | 2/1/5 | 1.00 | 0.00 | 0.00 % | 0.00 | 0.00 % |

Total: 2

**ISL performance view (DANPU01)**

| SENETname | Port | Gbit/s | Send | | Receive | |
|---|---|---|---|---|---|---|
| | | | MB/s | Utilization | MB/s | Utilization |
| - | - | - | - | - | - | - |

Total: 0

**Unit performance view (DANPU01)**

| Members | SENETname | Portname | Port | Gbit/s | Send | | Receive | |
|---|---|---|---|---|---|---|---|---|
| | | | | | MB/s | Utilization | MB/s | Utilization |
| Filter | Filter | Filter | Filter | Filter | | | | |
| abggold | su2-se1 | SU2S2P1 | 2/1/16 | 1.00 | 0.00 | 0.00 % | 0.00 | 0.00 % |
| abgpurple | hnc2-se1 | HNC2S3P0 | 2/1/15 | 1.00 | 0.00 | 0.00 % | 0.00 | 0.00 % |
| abgviolet | hnc1-se1 | HNC1S3P0 | 1/1/15 | 1.00 | 0.00 | 0.00 % | 0.00 | 0.00 % |

Total: 3

Three views are displayed on the *Performance* tab:

- The *Uplink Performance view* provides information relating to the performance and utilization of the connection ports to customer networks.
- The *ISL Performance view* provides information relating to the performance and utilization of the network's ISL ports (ISL = Inter Switch Link Protocol).
- The *Unit Performance view* provides information relating to the performance and utilization of the network's units (members).

The maximum and the current data throughput rate (in MB/s) and the utilization (in %) are displayed for each port (for each connection) listed in the various views. A distinction is made between the send and receive directions for data throughput and utilization.

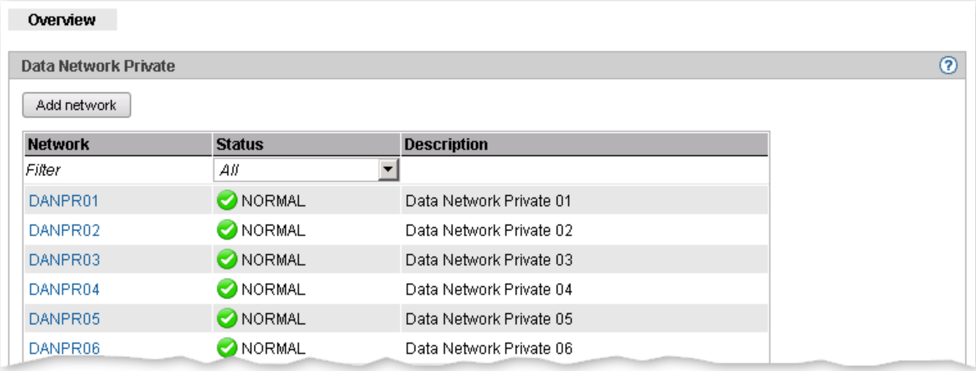
In the case of redundant networks the two ports used for the redundant connections and their performance are displayed one after the other in a table row.

## 10.2.4 Managing a Data Network Private

You manage a Data Network Private (DANPR) using the menu item *Data Network Private* in the *IP networks* menu. Up to 99 DANPRs can exist. These are named DANPR01, DANPR02, etc.

### Overview of all DANPRs

► Select *Hardware → IP networks → Data Network Private, Overview* tab. The *Overview* tab with all information on the existing DANPRs opens.

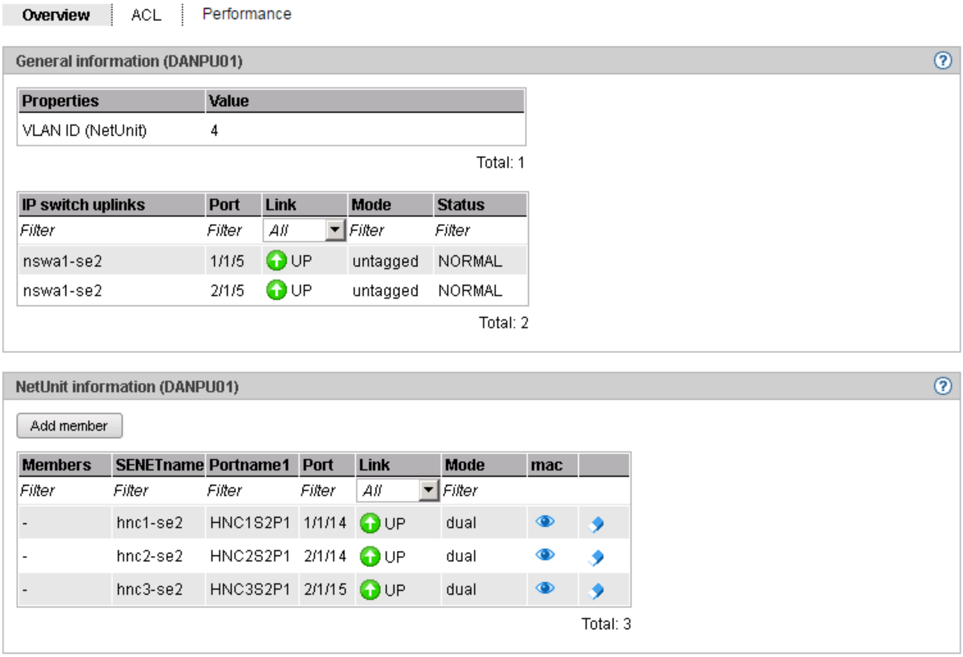


| Network | Status | Description |
|---|---|---|
| *Filter* | *All* | |
| DANPR01 | ✓ NORMAL | Data Network Private 01 |
| DANPR02 | ✓ NORMAL | Data Network Private 02 |
| DANPR03 | ✓ NORMAL | Data Network Private 03 |
| DANPR04 | ✓ NORMAL | Data Network Private 04 |
| DANPR05 | ✓ NORMAL | Data Network Private 05 |
| DANPR06 | ✓ NORMAL | Data Network Private 06 |

i The administrator can create another private network by clicking the *Add network* button.

### Overview of the various DANPRs

- ► Select *Hardware → IP networks → Data Network Private → <DANPR<no>*, *Overview* tab. The *Overview* tab with all information on the selected DANPR opens.



General information (DANPU01)

| Properties | Value |
|---|---|
| VLAN ID (NetUnit) | 4 |

Total: 1

| IP switch uplinks | Port | Link | Mode | Status |
|---|---|---|---|---|
| *Filter* | *Filter* | *All* | *Filter* | *Filter* |
| nswa1-se2 | 1/1/5 | UP | untagged | NORMAL |
| nswa1-se2 | 2/1/5 | UP | untagged | NORMAL |

Total: 2

NetUnit information (DANPU01)

| Members | SENETname | Portname1 | Port | Link | Mode | mac | |
|---|---|---|---|---|---|---|---|
| *Filter* | *Filter* | *Filter* | *Filter* | *All* | *Filter* | | |
| - | hnc1-se2 | HNC1S2P1 | 1/1/14 | UP | dual | 👁 | ✎ |
| - | hnc2-se2 | HNC2S2P1 | 2/1/14 | UP | dual | 👁 | ✎ |
| - | hnc3-se2 | HNC3S2P1 | 2/1/15 | UP | dual | 👁 | ✎ |

Total: 3

### 10.2.4.1 Add network

- ► Select *Hardware → IP networks → Data Network Private → Overview* tab. The *Overview* tab with all information on the existing DANPRs opens.
- ► Click *Add network*.

  The *Add network* dialog box opens and the first free network name is reserved.
- ► Follow the instructions of the wizard and enter the network data. Detailed information is provided in the SE Manager help.

### 10.2.4.2 Activate RADVD / DNS / NTP server

You can activate the RADVD / DNS / NTP server in the MU for each DANPR:

- ► Select *Hardware → IP networks → Data Network Private → DANPR<no>*, *Overview* tab.
- ► Click *Activate RADVD / DNS / NTP server*.
- ► The *Activate RADVD / DNS / NTP server* dialog box opens. Click *Activate.*

i In the case of multiple MUs, this action must be performed on all MUs.

### 10.2.4.3 Managing members of a DANPR network

You can display the active MAC addresses and add or remove ports (members of the network) for each DANPR.

Proceed as described in section “Managing a Data Network Public”.

### 10.2.4.4 Configuring the ACL settings of the DANPR network

You can add and delete ACL entries for each DANPR.

- ► Select *Hardware → IP networks → Data Network Private → DANPR<no>*, *ACL* tab.

  Proceed as described in section “Configuring the ACL settings of the DANPU network”.

### 10.2.4.5 Information on the performance and utilization of the DANPR ports

An overview of the performance and utilization of the ports belonging to the network is provided by the *Performance* tab.

- ► Select *Hardware → IP networks → Data Network Private → DANPR<no>*, *Performance* tab.

The *Performance* tab displays the *ISL Performance view* and *Unit Performance view* tables.

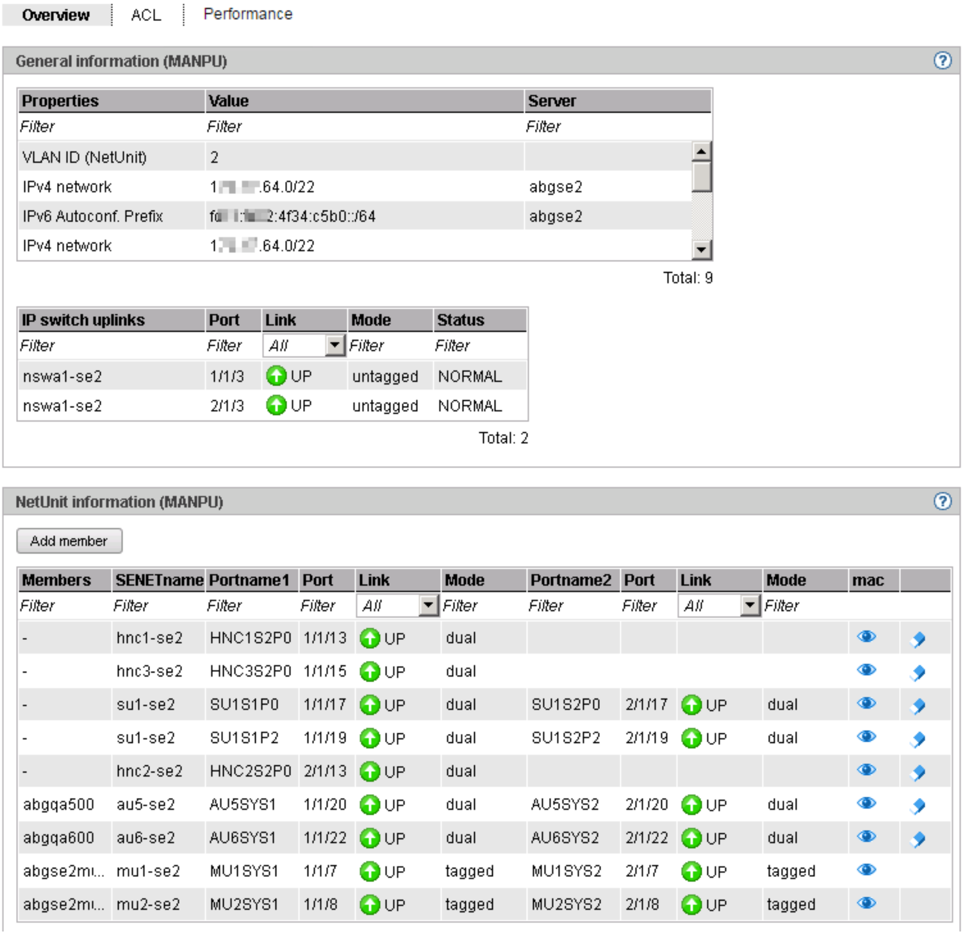
Detailed information is provided in section “Information on the performance and utilization of the DANPU ports”.

## 10.2.5 Managing a Management Network Public

Each SE server has a public administration network, the so-called Management Network Public (MANPU). There can also be a second optional network (Management Optional Network Public, MONPU for short).

You manage the Management Network Public (MANPU) using the menu item *Management Network Public* in the *IP networks* menu.

► Select *Hardware → IP networks → Management Network Public, → MANPU*, *Overview* tab.



General information (MANPU)

| Properties | Value | Server |
|---|---|---|
| *Filter* | *Filter* | *Filter* |
| VLAN ID (NetUnit) | 2 | |
| IPv4 network | 1[redacted].64.0/22 | abgse2 |
| IPv6 Autoconf. Prefix | fd[redacted]2:4f34:c5b0::/64 | abgse2 |
| IPv4 network | 1[redacted].64.0/22 | |

Total: 9

| IP switch uplinks | Port | Link | Mode | Status |
|---|---|---|---|---|
| *Filter* | *Filter* | *All* | *Filter* | *Filter* |
| nswa1-se2 | 1/1/3 | UP | untagged | NORMAL |
| nswa1-se2 | 2/1/3 | UP | untagged | NORMAL |

Total: 2

NetUnit information (MANPU)

| Members | SENETname | Portname1 | Port | Link | Mode | Portname2 | Port | Link | Mode | mac | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| *Filter* | *Filter* | *Filter* | *Filter* | *All* | *Filter* | *Filter* | *Filter* | *All* | *Filter* | | |
| - | hnc1-se2 | HNC1S2P0 | 1/1/13 | UP | dual | | | | | 👁 | ✎ |
| - | hnc3-se2 | HNC3S2P0 | 1/1/15 | UP | dual | | | | | 👁 | ✎ |
| - | su1-se2 | SU1S1P0 | 1/1/17 | UP | dual | SU1S2P0 | 2/1/17 | UP | dual | 👁 | ✎ |
| - | su1-se2 | SU1S1P2 | 1/1/19 | UP | dual | SU1S2P2 | 2/1/19 | UP | dual | 👁 | ✎ |
| - | hnc2-se2 | HNC2S2P0 | 2/1/13 | UP | dual | | | | | 👁 | ✎ |
| abgqa500 | au5-se2 | AU5SYS1 | 1/1/20 | UP | dual | AU5SYS2 | 2/1/20 | UP | dual | 👁 | ✎ |
| abgqa600 | au6-se2 | AU6SYS1 | 1/1/22 | UP | dual | AU6SYS2 | 2/1/22 | UP | dual | 👁 | ✎ |
| abgse2m... | mu1-se2 | MU1SYS1 | 1/1/7 | UP | tagged | MU1SYS2 | 2/1/7 | UP | tagged | 👁 | |
| abgse2m... | mu2-se2 | MU2SYS1 | 1/1/8 | UP | tagged | MU2SYS2 | 2/1/8 | UP | tagged | 👁 | |

The tab displays all information on the MANPU.

The following functions are available:

*Displaying the MAC address*

► In the *Net Unit information (MANPU)* group click the *MAC addresses* icon by the required unit.

The subsequent dialog box *Display MAC address* displays the unit's address.

*Adding ports*

► In the *Net Unit information (MANPU)* group click *Add member* for the required unit, follow the instructions of the wizard, and select the port.

*Removing a port*

► In the *Net Unit information (MANPU)* group click the *Remove* icon by the required unit, follow the instructions of the wizard, and confirm the action.

### 10.2.5.1 Configuring the ACL settings of the MANPU network

You can add and delete ACL entries for each MANPU.

► Select *Hardware* → *IP networks* → *Data Network Private* → *MANPU*, *ACL* tab.

⚠ If you set *permit* mode and enable ACL without entering services in the list, network access is locked for all services. For the MANPU network this means that you, as administrator, "lock yourself out."

Proceed as described in section "Configuring the ACL settings of the DANPU network".

### 10.2.5.2 Information on the performance and utilization of the MANPU ports

An overview of the performance and utilization of the ports belonging to the public administration network is provided by the *Performance* tab.

► Select *Hardware* → *IP networks* → *Management Network Public,* → *MANPU*, *Performance* tab.

The *Performance* tab displays the *Uplink Performance view, ISL Performance view* and *Unit Performance view* tables.

Detailed information is provided in section "Information on the performance and utilization of the DANPU ports".

## 10.2.6 Management Network Private

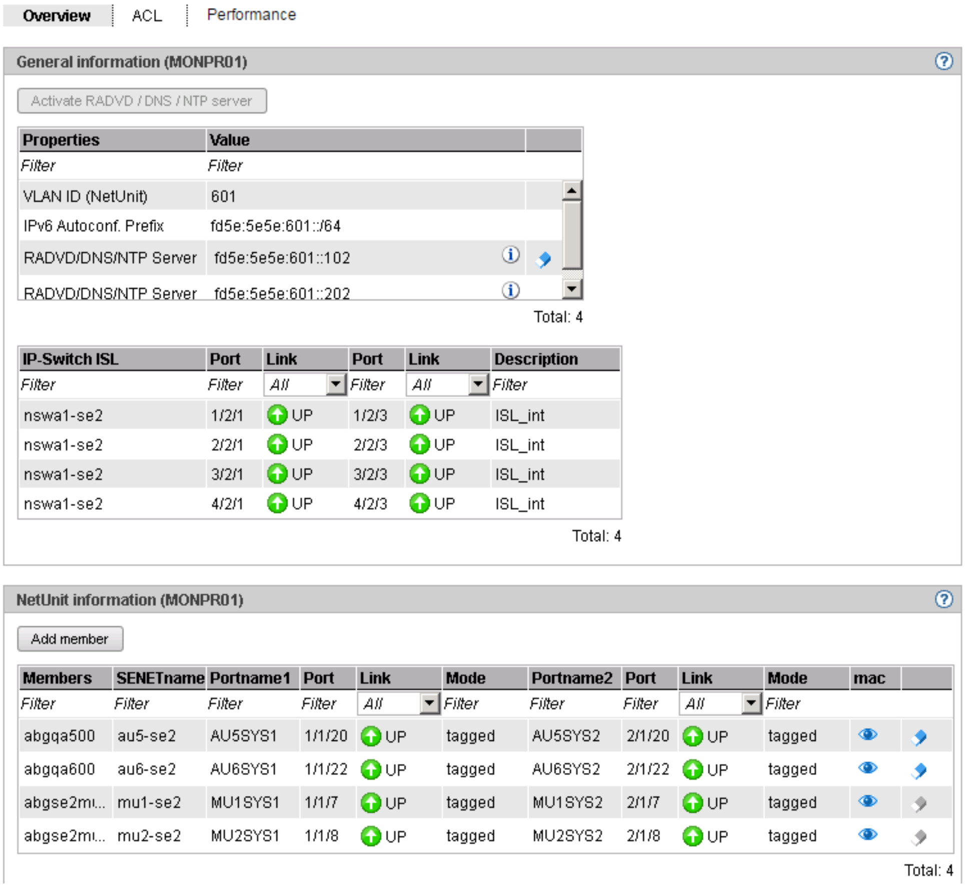
An SE server can have the following internal management networks:

- MCNLO: Management Control Network Local
- MCNPR: Management Control Network Private
- MONPR01 to up to MONPR08: Management Optional Network Private, optional
- MSNPR: Management SVP Control Network Private, optional

### Overview

The overview is similar for all Management Networks Private. Consequently only the MONPR01 is shown here. You can display the MAC addresses for all Management Networks Private. Detailed information on tabs and the subsequent dialog boxes is provided in the SE Manager help.

- ► Select *Hardware → IP networks → Management Network Private* and click *MONPR01*. The *Overview* tab with all information on the MONPR01 opens.


Overview
ACL
Performance
General information (MONPR01)
?
Activate RADVD / DNS / NTP server

| Properties | Value | |
|---|---|---|
| *Filter* | *Filter* | |
| VLAN ID (NetUnit) | 601 | |
| IPv6 Autoconf. Prefix | fd5e:5e5e:601::/64 | |
| RADVD/DNS/NTP Server | fd5e:5e5e:601::102 ⓘ | ✎ |
| RADVD/DNS/NTP Server | fd5e:5e5e:601::202 ⓘ | |

Total: 4

| IP-Switch ISL | Port | Link | Port | Link | Description |
|---|---|---|---|---|---|
| *Filter* | *Filter* | *All* ▾ | *Filter* | *All* ▾ | *Filter* |
| nswa1-se2 | 1/2/1 | UP | 1/2/3 | UP | ISL_int |
| nswa1-se2 | 2/2/1 | UP | 2/2/3 | UP | ISL_int |
| nswa1-se2 | 3/2/1 | UP | 3/2/3 | UP | ISL_int |
| nswa1-se2 | 4/2/1 | UP | 4/2/3 | UP | ISL_int |

Total: 4

| Members | SENETname | Portname1 | Port | Link | Mode | Portname2 | Port | Link | Mode | mac | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| *Filter* | *Filter* | *Filter* | *Filter* | *All* ▾ | *Filter* | *Filter* | *Filter* | *All* ▾ | *Filter* | | |
| abgqa500 | au5-se2 | AU5SYS1 | 1/1/20 | UP | tagged | AU5SYS2 | 2/1/20 | UP | tagged | 👁 | ✎ |
| abgqa600 | au6-se2 | AU6SYS1 | 1/1/22 | UP | tagged | AU6SYS2 | 2/1/22 | UP | tagged | 👁 | ✎ |
| abgse2mı... | mu1-se2 | MU1SYS1 | 1/1/7 | UP | tagged | MU1SYS2 | 2/1/7 | UP | tagged | 👁 | ✎ |
| abgse2mı... | mu2-se2 | MU2SYS1 | 1/1/8 | UP | tagged | MU2SYS2 | 2/1/8 | UP | tagged | 👁 | ✎ |

Total: 4

*Displaying the MAC address*

- ► In the *Net Unit information (MANPU)* group search for the required unit and click the *MAC addresses* icon.

  The subsequent dialog box *Display MAC address* displays the unit's address.

### 10.2.6.1 Information on the performance and utilization of the ports of the internal management networks

An overview of the performance and utilization of the ports belonging to the selected internal management network is provided by the *Performance* tab.

► Select *Hardware → IP networks → Management Network Private → <network>*, *Performance* tab. Here *<network>* specifies the internal management network *MCNLO, MCNPR, MONPR<no>* or *MSNPR.*

The *Performance* tab looks similar for all internal administration networks. The *ISL Performance view* and *Unit Performance view* tables are displayed. Detailed information is provided in section “Information on the performance and utilization of the DANPU ports”.

### 10.2.6.2 Managing members of optional MONPR networks

You can add or remove ports for each optional MONPR (MONPR01, MONPR02, etc.):

► Select *Hardware → IP networks → Management Network Public → MONPR<no>*. The *Overview* tab opens.

*Adding ports*

► In the *Net Unit information (MONPR<no>)* group search for the required unit and click *Add member*.

The *Add ports* dialog box opens. Follow the instructions of the wizard and select the ports.

► Confirm the action in the last step with *Add*.

*Removing a port*

► In the *Net Unit information (MONPR<no>)* group search for the required unit and click the *Remove* icon.

The *Remove ports* dialog box opens. Follow the instructions of the wizard and confirm the dialog box with *Remove*.

### 10.2.6.3 Configuring ACL settings of optional MONPR networks

You can add and delete ACL entries for each optional MONPR.

► Select *Hardware* → *IP networks* → *Data Network Private* → *MONPR<no>* and click the *ACL* tab.

Proceed as described in section “Configuring the ACL settings of the DANPU network”.

# 10.3 Managing FC networks

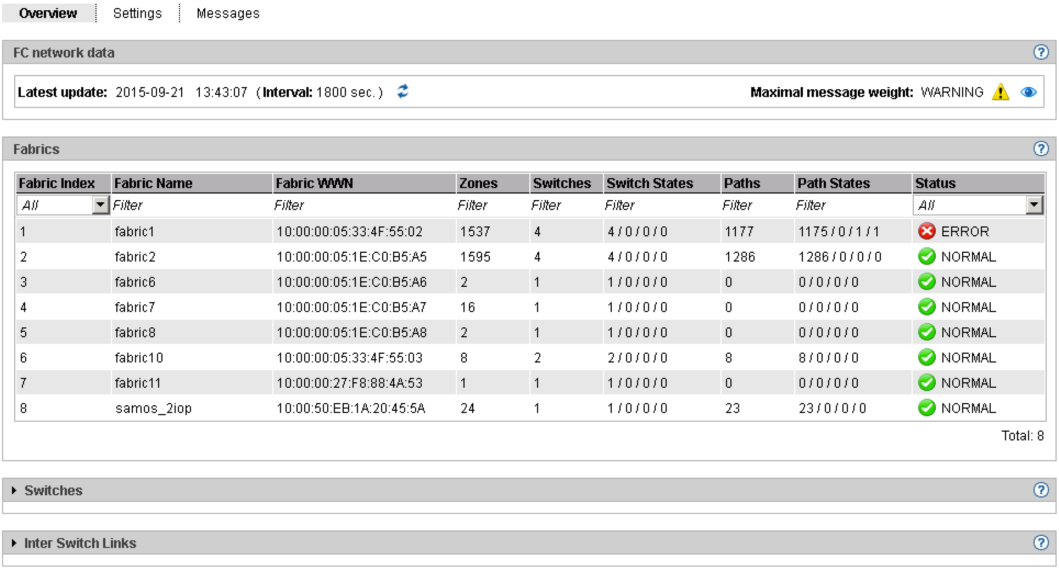
You manage the Fibre Channel networks of the SE server using the tree structure: *Hardware → FC networks*. All FC networks are listed in this menu.

The following options for information and settings are available to you:

- Overview of FC networks
- Configuring settings
- Displaying messages
- Displaying connections

## 10.3.1 Overview of FC networks

► Select *Hardware → FC networks*, *Overview* tab.



FC network data

**Latest update:** 2015-09-21 13:43:07 (**Interval:** 1800 sec.) **Maximal message weight:** WARNING ⚠

Fabrics

| Fabric Index | Fabric Name | Fabric WWN | Zones | Switches | Switch States | Paths | Path States | Status |
|---|---|---|---|---|---|---|---|---|
| *All* | *Filter* | *Filter* | *Filter* | *Filter* | *Filter* | *Filter* | *Filter* | *All* |
| 1 | fabric1 | 10:00:00:05:33:4F:55:02 | 1537 | 4 | 4 / 0 / 0 / 0 | 1177 | 1175 / 0 / 1 / 1 | ✗ ERROR |
| 2 | fabric2 | 10:00:00:05:1E:C0:B5:A5 | 1595 | 4 | 4 / 0 / 0 / 0 | 1286 | 1286 / 0 / 0 / 0 | ✓ NORMAL |
| 3 | fabric6 | 10:00:00:05:1E:C0:B5:A6 | 2 | 1 | 1 / 0 / 0 / 0 | 0 | 0 / 0 / 0 / 0 | ✓ NORMAL |
| 4 | fabric7 | 10:00:00:05:1E:C0:B5:A7 | 16 | 1 | 1 / 0 / 0 / 0 | 0 | 0 / 0 / 0 / 0 | ✓ NORMAL |
| 5 | fabric8 | 10:00:00:05:1E:C0:B5:A8 | 2 | 1 | 1 / 0 / 0 / 0 | 0 | 0 / 0 / 0 / 0 | ✓ NORMAL |
| 6 | fabric10 | 10:00:00:05:33:4F:55:03 | 8 | 2 | 2 / 0 / 0 / 0 | 8 | 8 / 0 / 0 / 0 | ✓ NORMAL |
| 7 | fabric11 | 10:00:00:27:F8:88:4A:53 | 1 | 1 | 1 / 0 / 0 / 0 | 0 | 0 / 0 / 0 / 0 | ✓ NORMAL |
| 8 | samos_2iop | 10:00:50:EB:1A:20:45:5A | 24 | 1 | 1 / 0 / 0 / 0 | 23 | 23 / 0 / 0 / 0 | ✓ NORMAL |

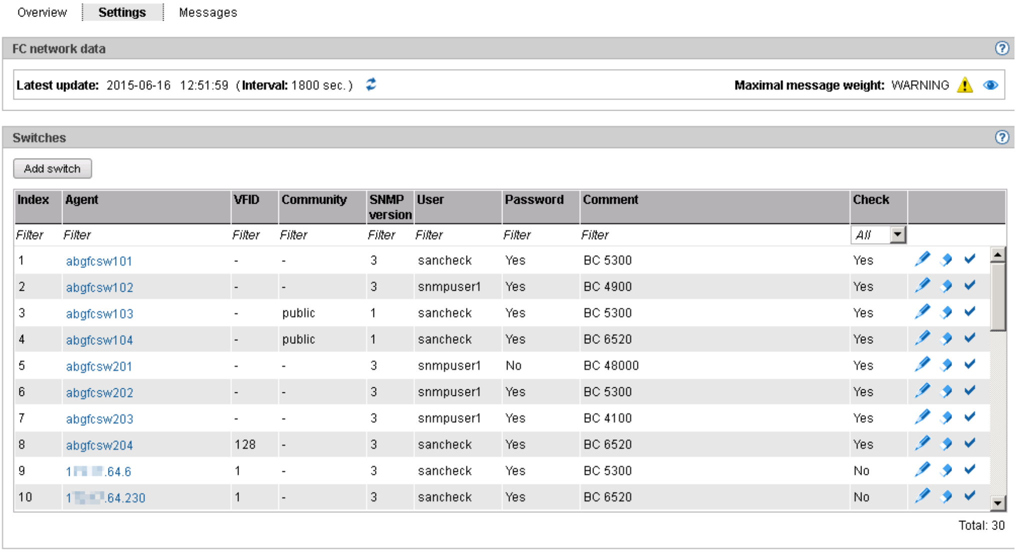
Total: 8

The *Overview* tab displays all information on the FC networks.

## 10.3.2 Configuring settings

You can add, change or remove switches.

► Select *Hardware* → *FC networks* → *Settings*. The *Settings* tab with all information on FC networks opens.



**Latest update:** 2015-06-16 12:51:59 (**Interval:** 1800 sec.) **Maximal message weight:** WARNING

| Index | Agent | VFID | Community | SNMP version | User | Password | Comment | Check | |
|---|---|---|---|---|---|---|---|---|---|
| *Filter* | *Filter* | *Filter* | *Filter* | *Filter* | *Filter* | *Filter* | *Filter* | *All* | |
| 1 | abgfcsw101 | - | - | 3 | sancheck | Yes | BC 5300 | Yes | ✎ ◆ ✓ |
| 2 | abgfcsw102 | - | - | 3 | snmpuser1 | Yes | BC 4900 | Yes | ✎ ◆ ✓ |
| 3 | abgfcsw103 | - | public | 1 | sancheck | Yes | BC 5300 | Yes | ✎ ◆ ✓ |
| 4 | abgfcsw104 | - | public | 1 | sancheck | Yes | BC 6520 | Yes | ✎ ◆ ✓ |
| 5 | abgfcsw201 | - | - | 3 | snmpuser1 | No | BC 48000 | Yes | ✎ ◆ ✓ |
| 6 | abgfcsw202 | - | - | 3 | snmpuser1 | Yes | BC 5300 | Yes | ✎ ◆ ✓ |
| 7 | abgfcsw203 | - | - | 3 | snmpuser1 | Yes | BC 4100 | Yes | ✎ ◆ ✓ |
| 8 | abgfcsw204 | 128 | - | 3 | sancheck | Yes | BC 6520 | Yes | ✎ ◆ ✓ |
| 9 | 1[redacted].64.6 | 1 | - | 3 | sancheck | Yes | BC 5300 | No | ✎ ◆ ✓ |
| 10 | 1[redacted].64.230 | 1 | - | 3 | sancheck | Yes | BC 6520 | No | ✎ ◆ ✓ |

Total: 30

*Adding, changing, removing switches*

► To add a switch, in the *Switches* group click *Add switch*. In the *Add switch* wizard you can make the required entries step by step.

► To change a switch, in the *Switches* group click the *Change* icon by the required switch, follow the instructions of the subsequent wizard, and confirm the changes.

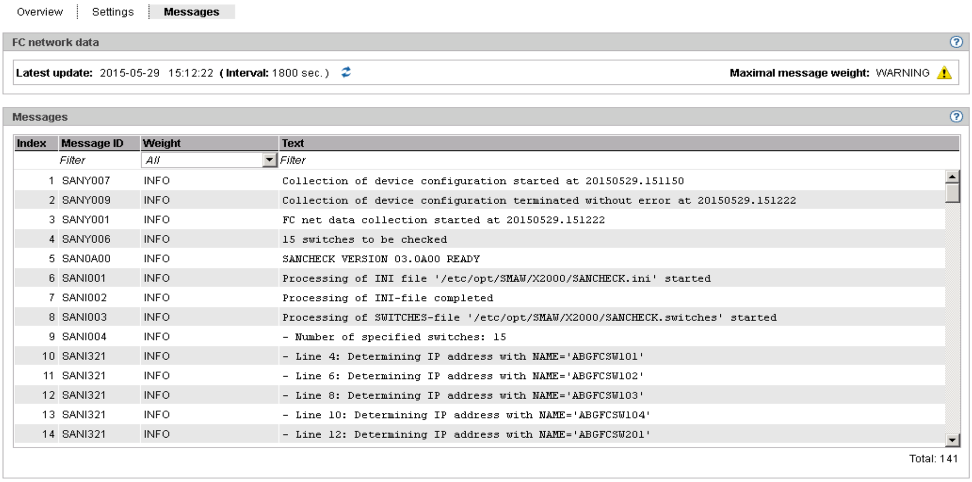
► To remove a switch, in the *Switches* group click the *Remove* icon by the required switch and confirm the action in the subsequent dialog box.

*Enabling/disabling switch check*

► In the *Switches* group click the *Enable* or *Disable* icon by the required switch and confirm the request.

## 10.3.3 Displaying messages

► Select *Hardware* → *FC networks*, *Messages* tab.



**Latest update:** 2015-05-29 15:12:22 ( **Interval:** 1800 sec. )

**Maximal message weight:** WARNING

Messages

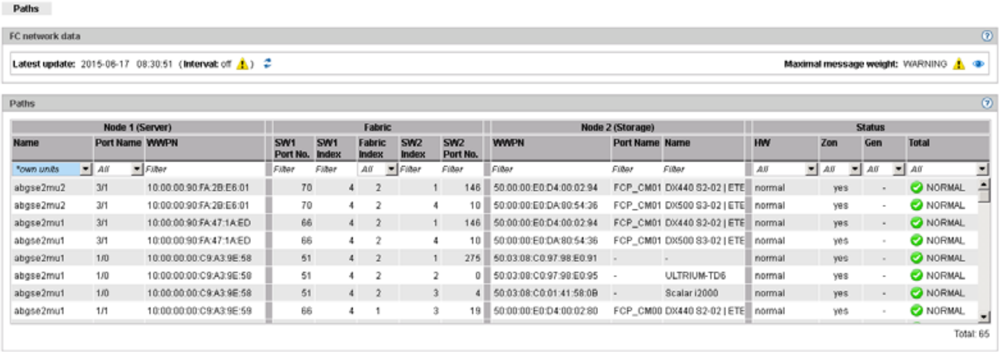
| Index | Message ID | Weight | Text |
|---|---|---|---|
| | Filter | All | Filter |
| 1 | SANY007 | INFO | Collection of device configuration started at 20150529.151150 |
| 2 | SANY009 | INFO | Collection of device configuration terminated without error at 20150529.151222 |
| 3 | SANY001 | INFO | FC net data collection started at 20150529.151222 |
| 4 | SANY006 | INFO | 15 switches to be checked |
| 5 | SAN0A00 | INFO | SANCHECK VERSION 03.0A00 READY |
| 6 | SANI001 | INFO | Processing of INI file '/etc/opt/SMAW/X2000/SANCHECK.ini' started |
| 7 | SANI002 | INFO | Processing of INI-file completed |
| 8 | SANI003 | INFO | Processing of SWITCHES-file '/etc/opt/SMAW/X2000/SANCHECK.switches' started |
| 9 | SANI004 | INFO | - Number of specified switches: 15 |
| 10 | SANI321 | INFO | - Line 4: Determining IP address with NAME='ABGFCSW101' |
| 11 | SANI321 | INFO | - Line 6: Determining IP address with NAME='ABGFCSW102' |
| 12 | SANI321 | INFO | - Line 8: Determining IP address with NAME='ABGFCSW103' |
| 13 | SANI321 | INFO | - Line 10: Determining IP address with NAME='ABGFCSW104' |
| 14 | SANI321 | INFO | - Line 12: Determining IP address with NAME='ABGFCSW201' |

Total: 141

The *Messages* tab displays a list containing all messages for the FC networks.

## 10.3.4 Displaying connections

► Select *Hardware* → *FC networks* → *Connections*, *Paths* tab.



**Latest update:** 2015-06-17 08:30:51 ( **Interval:** off )

**Maximal message weight:** WARNING

Paths

| Node 1 (Server) | | | Fabric | | | | | Node 2 (Storage) | | | Status | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Name | Port Name | WWPN | SW1 Port No. | SW1 Index | Fabric Index | SW2 Index | SW2 Port No. | WWPN | Port Name | Name | HW | Zon | Gen | Total |
| *own units | All | Filter | Filter | Filter | All | Filter | Filter | Filter | Filter | Filter | All | All | All | All |
| abgse2mu2 | 3/1 | 10:00:00:90:FA:2B:E6:01 | 70 | 4 | 2 | 1 | 146 | 50:00:00:E0:D4:00:02:94 | FCP_CM01 | DX440 S2-02 \| ETE | normal | yes | - | ✓ NORMAL |
| abgse2mu2 | 3/1 | 10:00:00:90:FA:2B:E6:01 | 70 | 4 | 2 | 4 | 10 | 50:00:00:E0:DA:80:54:36 | FCP_CM01 | DX500 S3-02 \| ETE | normal | yes | - | ✓ NORMAL |
| abgse2mu1 | 3/1 | 10:00:00:90:FA:47:1A:ED | 66 | 4 | 2 | 1 | 146 | 50:00:00:E0:D4:00:02:94 | FCP_CM01 | DX440 S2-02 \| ETE | normal | yes | - | ✓ NORMAL |
| abgse2mu1 | 3/1 | 10:00:00:90:FA:47:1A:ED | 66 | 4 | 2 | 4 | 10 | 50:00:00:E0:DA:80:54:36 | FCP_CM01 | DX500 S3-02 \| ETE | normal | yes | - | ✓ NORMAL |
| abgse2mu1 | 1/0 | 10:00:00:00:C9:A3:9E:58 | 51 | 4 | 2 | 1 | 275 | 50:03:08:C0:97:98:E0:91 | - | - | normal | yes | - | ✓ NORMAL |
| abgse2mu1 | 1/0 | 10:00:00:00:C9:A3:9E:58 | 51 | 4 | 2 | 2 | 0 | 50:03:08:C0:97:98:E0:95 | - | ULTRIUM-TD6 | normal | yes | - | ✓ NORMAL |
| abgse2mu1 | 1/0 | 10:00:00:00:C9:A3:9E:58 | 51 | 4 | 2 | 3 | 4 | 50:03:08:C0:01:41:58:0B | - | Scalar i2000 | normal | yes | - | ✓ NORMAL |
| abgse2mu1 | 1/1 | 10:00:00:00:C9:A3:9E:59 | 66 | 4 | 1 | 3 | 19 | 50:00:00:E0:D4:00:02:80 | FCP_CM00 | DX440 S2-02 \| ETE | normal | yes | - | ✓ NORMAL |

Total: 65

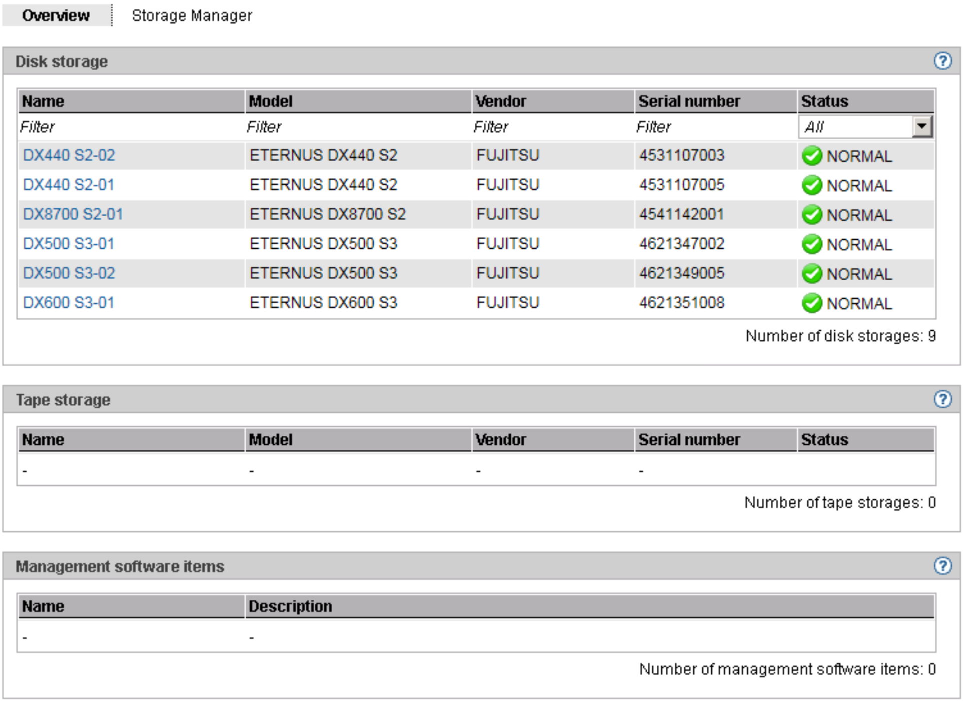
The *Paths* tab displays a list containing all connections to FC networks.

# 10.4 Managing storage systems

You manage the storage systems of the SE server in the tree structure: *Hardware* → *Storage*.

## 10.4.1 Overview of the storage systems

► Select *Hardware* → *Storage*, *Overview* tab.



Disk storage

| Name | Model | Vendor | Serial number | Status |
|---|---|---|---|---|
| *Filter* | *Filter* | *Filter* | *Filter* | *All* |
| DX440 S2-02 | ETERNUS DX440 S2 | FUJITSU | 4531107003 | ✓ NORMAL |
| DX440 S2-01 | ETERNUS DX440 S2 | FUJITSU | 4531107005 | ✓ NORMAL |
| DX8700 S2-01 | ETERNUS DX8700 S2 | FUJITSU | 4541142001 | ✓ NORMAL |
| DX500 S3-01 | ETERNUS DX500 S3 | FUJITSU | 4621347002 | ✓ NORMAL |
| DX500 S3-02 | ETERNUS DX500 S3 | FUJITSU | 4621349005 | ✓ NORMAL |
| DX600 S3-01 | ETERNUS DX600 S3 | FUJITSU | 4621351008 | ✓ NORMAL |

Number of disk storages: 9

Tape storage

| Name | Model | Vendor | Serial number | Status |
|---|---|---|---|---|
| - | - | - | - | |

Number of tape storages: 0

Management software items

| Name | Description |
|---|---|
| - | - |

Number of management software items: 0

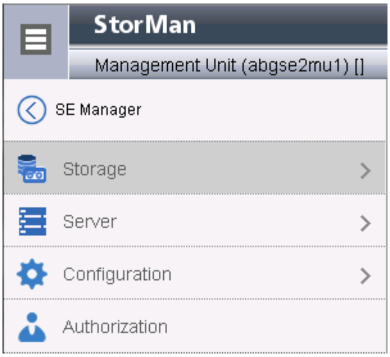
The *Overview* tab displays information on the storage systems. This information is the same as in the information overview which StorMan displays for storage systems.

### 10.4.2 Storage Manager

The Storage Manager **StorMan** is an autonomous product with its own online help. You call Storman from the SE as follows:

- ► Select *Hardware* → *Storage*, *Storage Manager* tab.

The Storage Manager's homepage opens.



Further details on using the Storage Manager are provided in the online help and documentation for StorMan.

When you click *SE Manager*, you return to the SE Manager.

## 10.5 HW inventory

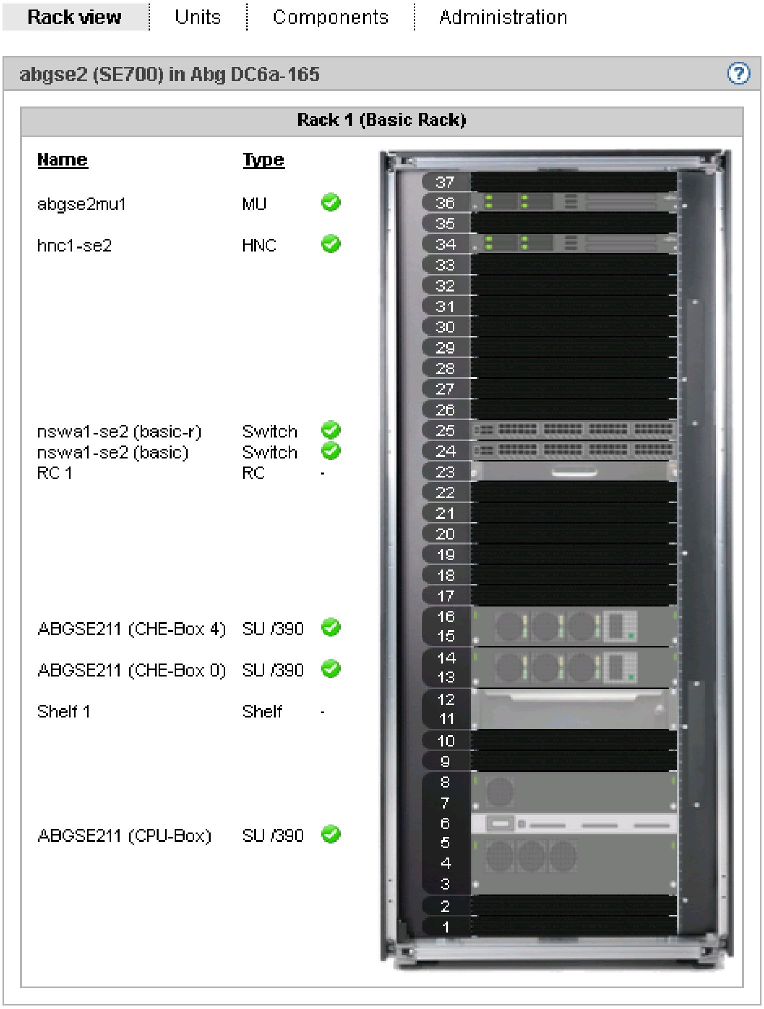
In the *Hardware → HW inventory* menu you can have the hardware configuration of your SW server displayed on the screen in graphic form and also in various tables:

- Rack view
- Displaying units
- Displaying components
- Administration

### 10.5.1 Rack view

The rack view displays all integrated components on the screen in graphical form.

► Select *Hardware → HW inventory* and click *Rack view*. The *Rack view* tab opens, here with an SE 700 as an example.



Rack view | Units | Components | Administration

abgse2 (SE700) in Abg DC6a-165

Rack 1 (Basic Rack)

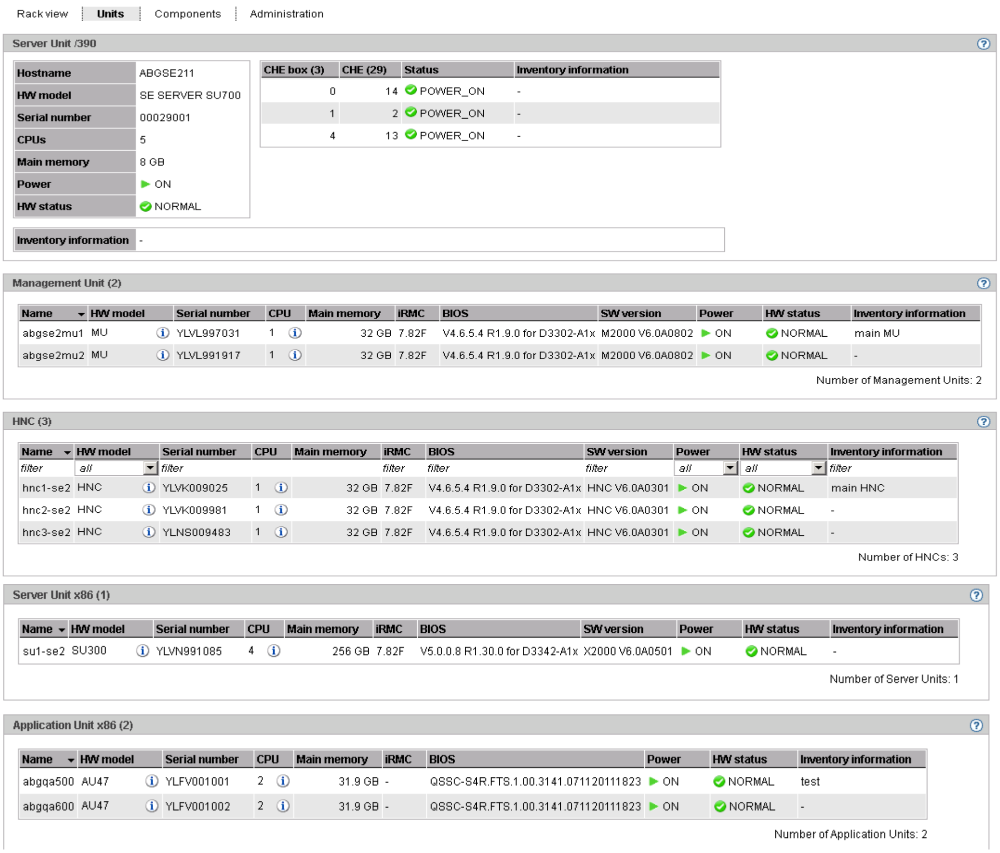
| Name | Type | |
|---|---|---|
| abgse2mu1 | MU | ✓ |
| hnc1-se2 | HNC | ✓ |
| nswa1-se2 (basic-r) | Switch | ✓ |
| nswa1-se2 (basic) | Switch | ✓ |
| RC 1 | RC | - |
| ABGSE211 (CHE-Box 4) | SU /390 | ✓ |
| ABGSE211 (CHE-Box 0) | SU /390 | ✓ |
| Shelf 1 | Shelf | - |
| ABGSE211 (CPU-Box) | SU /390 | ✓ |

## 10.5.2 Displaying units

The units view displays all integrated units in tabular form. A separate group is displayed for each unit.

► Select *Hardware* → *HW inventory*, *Units* tab.

The *Units* tab opens, here with an SE 700 as an example.



Rack view | **Units** | Components | Administration

**Server Unit /390**

| | |
|---|---|
| Hostname | ABGSE211 |
| HW model | SE SERVER SU700 |
| Serial number | 00029001 |
| CPUs | 5 |
| Main memory | 8 GB |
| Power | ▶ ON |
| HW status | ✓ NORMAL |

| CHE box (3) | CHE (29) | Status | Inventory information |
|---|---|---|---|
| 0 | 14 | ✓ POWER_ON | - |
| 1 | 2 | ✓ POWER_ON | - |
| 4 | 13 | ✓ POWER_ON | - |

| | |
|---|---|
| Inventory information | - |

**Management Unit (2)**

| Name | HW model | Serial number | CPU | Main memory | iRMC | BIOS | SW version | Power | HW status | Inventory information |
|---|---|---|---|---|---|---|---|---|---|---|
| abgse2mu1 | MU ⓘ | YLVL997031 | 1 ⓘ | 32 GB | 7.82F | V4.6.5.4 R1.9.0 for D3302-A1x | M2000 V6.0A0802 | ▶ ON | ✓ NORMAL | main MU |
| abgse2mu2 | MU ⓘ | YLVL991917 | 1 ⓘ | 32 GB | 7.82F | V4.6.5.4 R1.9.0 for D3302-A1x | M2000 V6.0A0802 | ▶ ON | ✓ NORMAL | - |

Number of Management Units: 2

**HNC (3)**

| Name | HW model | Serial number | CPU | Main memory | iRMC | BIOS | SW version | Power | HW status | Inventory information |
|---|---|---|---|---|---|---|---|---|---|---|
| *filter* | *all* | *filter* | | | *filter* | *filter* | *filter* | *all* | *all* | *filter* |
| hnc1-se2 | HNC ⓘ | YLVK009025 | 1 ⓘ | 32 GB | 7.82F | V4.6.5.4 R1.9.0 for D3302-A1x | HNC V6.0A0301 | ▶ ON | ✓ NORMAL | main HNC |
| hnc2-se2 | HNC ⓘ | YLVK009981 | 1 ⓘ | 32 GB | 7.82F | V4.6.5.4 R1.9.0 for D3302-A1x | HNC V6.0A0301 | ▶ ON | ✓ NORMAL | - |
| hnc3-se2 | HNC ⓘ | YLNS009483 | 1 ⓘ | 32 GB | 7.82F | V4.6.5.4 R1.9.0 for D3302-A1x | HNC V6.0A0301 | ▶ ON | ✓ NORMAL | - |

Number of HNCs: 3

**Server Unit x86 (1)**

| Name | HW model | Serial number | CPU | Main memory | iRMC | BIOS | SW version | Power | HW status | Inventory information |
|---|---|---|---|---|---|---|---|---|---|---|
| su1-se2 | SU300 ⓘ | YLVN991085 | 4 ⓘ | 256 GB | 7.82F | V5.0.0.8 R1.30.0 for D3342-A1x | X2000 V6.0A0501 | ▶ ON | ✓ NORMAL | - |

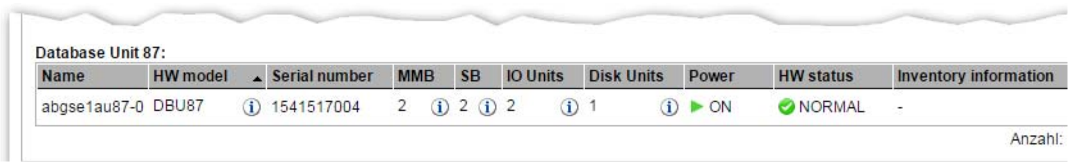
Number of Server Units: 1

**Application Unit x86 (2)**

| Name | HW model | Serial number | CPU | Main memory | iRMC | BIOS | Power | HW status | Inventory information |
|---|---|---|---|---|---|---|---|---|---|
| abgqa500 | AU47 ⓘ | YLFV001001 | 2 ⓘ | 31.9 GB | - | QSSC-S4R.FTS.1.00.3141.071120111823 | ▶ ON | ✓ NORMAL | test |
| abgqa600 | AU47 ⓘ | YLFV001002 | 2 ⓘ | 31.9 GB | - | QSSC-S4R.FTS.1.00.3141.071120111823 | ▶ ON | ✓ NORMAL | - |

Number of Application Units: 2

i If AUs of the type AU87 or DBU87 exist, the properties of these AUs are displayed in a separate table with detailed information on the power status of the Management Boards, system boards, IO Units and Disk Units.



**Database Unit 87:**

| Name | HW model | Serial number | MMB | SB | IO Units | Disk Units | Power | HW status | Inventory information |
|---|---|---|---|---|---|---|---|---|---|
| abgse1au87-0 | DBU87 ⓘ | 1541517004 | 2 ⓘ | 2 ⓘ | 2 ⓘ | 1 ⓘ | ▶ ON | ✓ NORMAL | - |

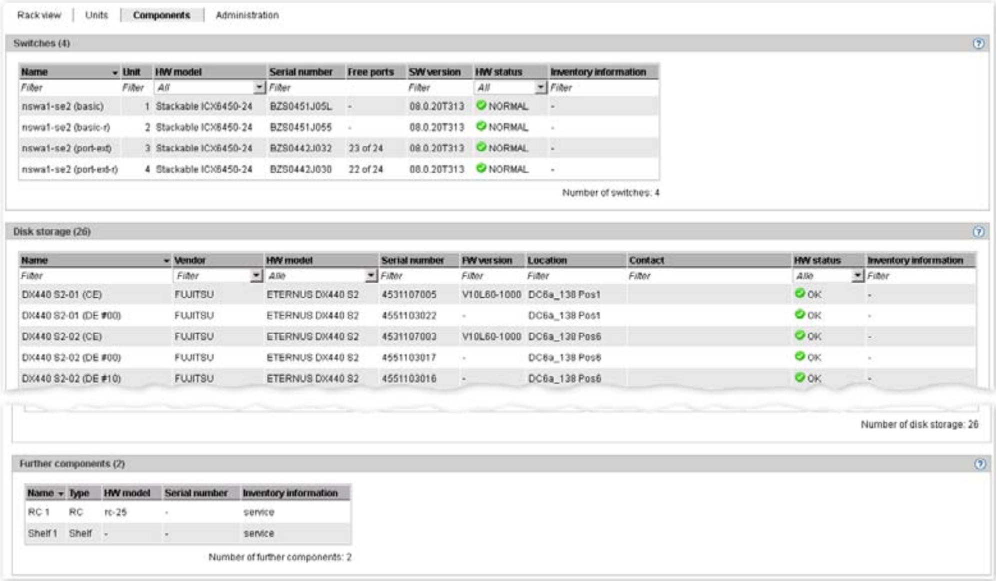
Anzahl:

## 10.5.3 Displaying components

In the components view all integrated add-on components, e.g. switches and storage systems, are displayed in tabular form. A separate group is displayed for each component.

► Select *Hardware* → *HW inventory* , *Components* tab.

The *Components* tab opens, here with an SE 700 as an example.



Switches (4)

| Name | Unit | HW model | Serial number | Free ports | SW version | HW status | Inventory information |
|---|---|---|---|---|---|---|---|
| Filter | Filter | All | Filter | | Filter | All | Filter |
| nswa1-se2 (basic) | 1 | Stackable ICX6450-24 | BZS0451J05L | - | 08.0.20T313 | ✓ NORMAL | - |
| nswa1-se2 (basic-r) | 2 | Stackable ICX6450-24 | BZS0451J055 | - | 08.0.20T313 | ✓ NORMAL | - |
| nswa1-se2 (port-ext) | 3 | Stackable ICX6450-24 | BZS0442J032 | 23 of 24 | 08.0.20T313 | ✓ NORMAL | - |
| nswa1-se2 (port-ext-r) | 4 | Stackable ICX6450-24 | BZS0442J030 | 22 of 24 | 08.0.20T313 | ✓ NORMAL | - |

Number of switches: 4

Disk storage (26)

| Name | Vendor | HW model | Serial number | FW version | Location | Contact | HW status | Inventory information |
|---|---|---|---|---|---|---|---|---|
| Filter | Filter | Alle | Filter | Filter | Filter | Filter | Alle | Filter |
| DX440 S2-01 (CE) | FUJITSU | ETERNUS DX440 S2 | 4531107005 | V10L60-1000 | DC6a_138 Pos1 | | ✓ OK | - |
| DX440 S2-01 (DE #00) | FUJITSU | ETERNUS DX440 S2 | 4551103022 | - | DC6a_138 Pos1 | | ✓ OK | - |
| DX440 S2-02 (CE) | FUJITSU | ETERNUS DX440 S2 | 4531107003 | V10L60-1000 | DC6a_138 Pos6 | | ✓ OK | - |
| DX440 S2-02 (DE #00) | FUJITSU | ETERNUS DX440 S2 | 4551103017 | - | DC6a_138 Pos6 | | ✓ OK | - |
| DX440 S2-02 (DE #10) | FUJITSU | ETERNUS DX440 S2 | 4551103016 | - | DC6a_138 Pos6 | | ✓ OK | - |

Number of disk storage: 26

Further components (2)

| Name | Type | HW model | Serial number | Inventory information |
|---|---|---|---|---|
| RC 1 | RC | rc-25 | - | service |
| Shelf 1 | Shelf | - | - | service |

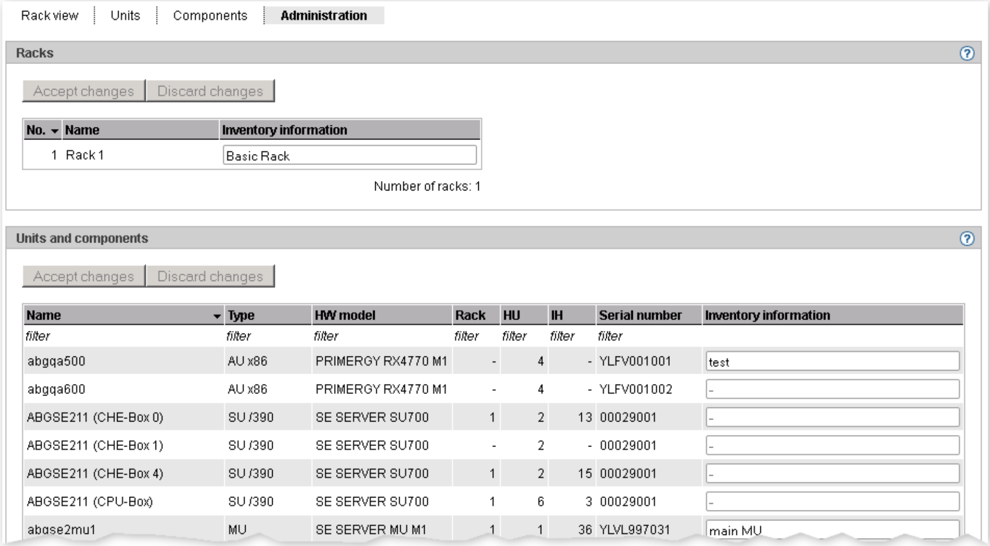
Number of further components: 2

## 10.5.4 Administration

In the administration view all racks and hardware components are displayed in tabular form. One group is displayed for each rack and other hardware components.

► Select *Hardware → HW inventory*, *Administration* tab.

The *Administration* tab opens, here with an SE 700 as an example.



Racks

| No. | Name | Inventory information |
|---|---|---|
| 1 | Rack 1 | Basic Rack |

Number of racks: 1

Units and components

| Name | Type | HW model | Rack | HU | IH | Serial number | Inventory information |
|---|---|---|---|---|---|---|---|
| filter | filter | filter | filter | filter | filter | filter | |
| abgqa500 | AU x86 | PRIMERGY RX4770 M1 | - | 4 | - | YLFV001001 | test |
| abgqa600 | AU x86 | PRIMERGY RX4770 M1 | - | 4 | - | YLFV001002 | - |
| ABGSE211 (CHE-Box 0) | SU /390 | SE SERVER SU700 | 1 | 2 | 13 | 00029001 | - |
| ABGSE211 (CHE-Box 1) | SU /390 | SE SERVER SU700 | - | 2 | - | 00029001 | - |
| ABGSE211 (CHE-Box 4) | SU /390 | SE SERVER SU700 | 1 | 2 | 15 | 00029001 | - |
| ABGSE211 (CPU-Box) | SU /390 | SE SERVER SU700 | 1 | 6 | 3 | 00029001 | - |
| abgse2mu1 | MU | SE SERVER MU M1 | 1 | 1 | 36 | YLVL997031 | main MU |

► In the *Inventory information* column you can enter a comment or change the existing comment. You accept the comment with *Accept changes*.

# 10.6 Managing energy settings

You manage the energy settings of the SE server using the tree structure: *Hardware* → *Energy*.

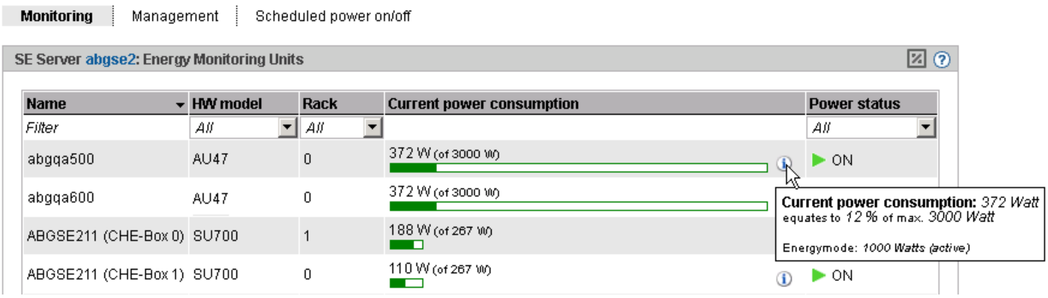
The following options for information and settings are available to you:

- Monitoring energy consumption of the units of the SE server
- Simulating energy saving scenarios for the SE server
- Scheduled power on/off of units of the SE server

## 10.6.1 Monitoring energy consumption of the units of the SE server

The *Monitoring* tab displays the current energy consumption, the hardware-specific maximum performance, and the power status for all units of the SE server (SU, MU, HNC, and AU). In the case of an AU, the energy saving mode enabled is also displayed.

► Select *Hardware* → *Energy*, *Monitoring* tab.



SE Server abgse2: Energy Monitoring Units

| Name | HW model | Rack | Current power consumption | Power status |
|---|---|---|---|---|
| Filter | All | All | | All |
| abgqa500 | AU47 | 0 | 372 W (of 3000 W) | ON |
| abgqa600 | AU47 | 0 | 372 W (of 3000 W) | |
| ABGSE211 (CHE-Box 0) | SU700 | 1 | 188 W (of 267 W) | |
| ABGSE211 (CHE-Box 1) | SU700 | 0 | 110 W (of 267 W) | ON |

**Current power consumption:** *372 Watt*
equates to *12 %* of max. *3000 Watt*

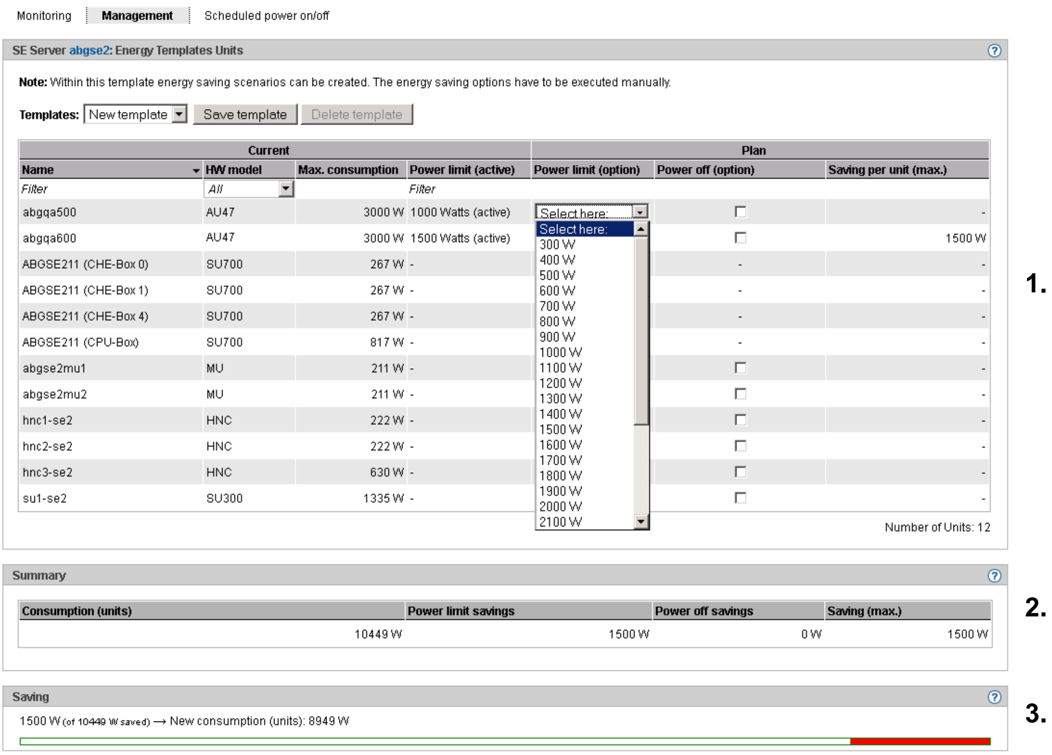
Energymode: *1000 Watts (active)*

## 10.6.2 Simulating energy saving scenarios for the SE server

You can create planning templates for defining energy saving scenarios and have energy saving options calculated.

You can set the power off option for the various units of the SE server. There is no power off option for the components of the SU /390 (CPU and channel boxes).

► Select *Hardware → Energy*, *Management* tab.
The tab for creating a new template opens. If templates are already stored, these are listed and can be edited.



SE Server abgse2: Energy Templates Units

**Note:** Within this template energy saving scenarios can be created. The energy saving options have to be executed manually.

**Templates:** New template ▾ Save template Delete template

| Current | | | | Plan | | |
|---|---|---|---|---|---|---|
| Name | HW model | Max. consumption | Power limit (active) | Power limit (option) | Power off (option) | Saving per unit (max.) |
| Filter | All ▾ | | Filter | | | |
| abgqa500 | AU47 | 3000 W | 1000 Watts (active) | Select here: ▾ | □ | - |
| abgqa600 | AU47 | 3000 W | 1500 Watts (active) | | □ | 1500 W |
| ABGSE211 (CHE-Box 0) | SU700 | 267 W | - | | - | - |
| ABGSE211 (CHE-Box 1) | SU700 | 267 W | - | | - | - |
| ABGSE211 (CHE-Box 4) | SU700 | 267 W | - | | - | - |
| ABGSE211 (CPU-Box) | SU700 | 817 W | - | | - | - |
| abgse2mu1 | MU | 211 W | - | | □ | - |
| abgse2mu2 | MU | 211 W | - | | □ | - |
| hnc1-se2 | HNC | 222 W | - | | □ | - |
| hnc2-se2 | HNC | 222 W | - | | □ | - |
| hnc3-se2 | HNC | 630 W | - | | □ | - |
| su1-se2 | SU300 | 1335 W | - | | □ | - |

Number of Units: 12

Summary

| Consumption (units) | Power limit savings | Power off savings | Saving (max.) |
|---|---|---|---|
| 10449 W | 1500 W | 0 W | 1500 W |

Saving

1500 W (of 10449 W saved) → New consumption (units): 8949 W

Three areas are displayed:

1. An area in which you can make settings for the template.
2. An area containing a summary of the total consumption of all units and the maximum energy saving when the saving options simulated in the template are implemented.
3. This area displays the maximum total saving with respect to the total consumption in the form of a red bar. The saving, the total consumption and the newly calculated consumption (total consumption - maximum saving) are also displayed.

### 10.6.3 Scheduled power on/off of units of the SE server

► Select *Hardware → Energy*, *Scheduled power on/off* tab.

A list is displayed containing all the units of the SE server which can be powered on and off on a scheduled basis.

The power on/off times currently set and the current power status are displayed for each unit of the type MU, HNC, SU, and AU. You can define, change, and reset new power on/off times for each day of the week.

ℹ The functionality is not supported for AU87 and DBU87.

# 11 Managing authorizations

## 11.1 User

The following roles exist for administering and operating the SE server:

- Administrator
- BS2000 administrator
- Operator
- XenVM administrator
- AU administrator
  This role is used to configure and manage the Application Units and the systems which run on them.
- Service
  The SE Manager only displays this role or the user accounts with this role. A service account cannot be administered in the SE Manager.

Detailed information on the various roles is provided in section "Role and user strategy" on page 42.

### 11.1.1 Managing accounts

The administrator manages all accounts on the SE server with the exception of the service accounts. He/She creates new accounts and changes or deletes existing accounts.

The accounts *admin* for the administrator and *service* for Customer Support are predefined and cannot be deleted.

As administrator you can create, modify and delete further local accounts for the *administrator, BS2000 administrator, operator, XenVM administrator* and *AU administrator* roles.
You cannot administer the *service* account (*Service* role).
You can also manage passwords and password attributes (e.g. Validity time) for the accounts, see section "Managing passwords" on page 272

As BS2000 administrator, operator, XenVM administrator or AU administrator you are authorized to manage your own account, i.e. you can change the access password yourself, see section “Managing passwords” on page 272.

A XenVM administrator has access to XenVM systems and to XenVM devices.

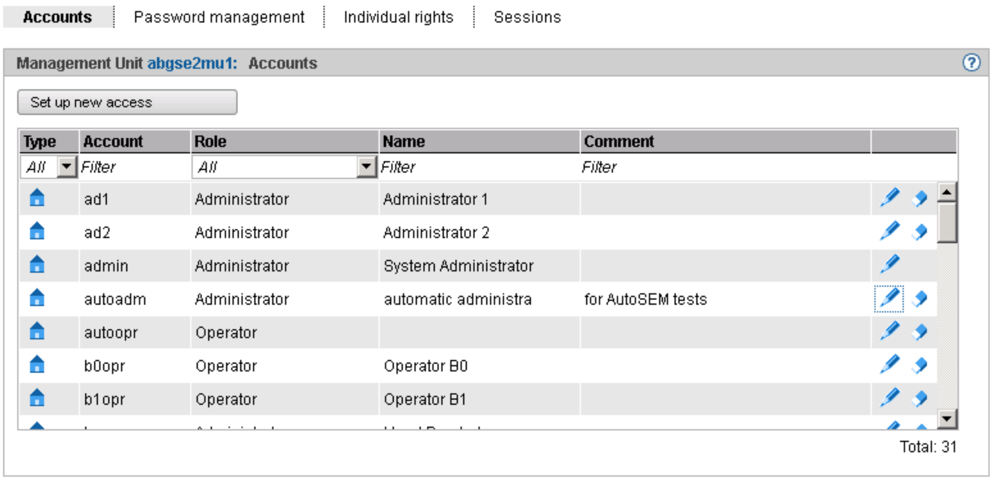
The operator obtains access to BS2000 systems and the corresponding BS2000 devices only in accordance with his/her individual authorizations which are assigned by the administrator, see section “Managing access to the BS2000 console and dialog” on page 276.

In the *Accounts* tab you can create and manage local accounts.

i For the BS2000 administrator, operator, XenVM administrator and AU administrator the functionality is limited to displaying his/her own account and changing the name and comment.

### Displaying accounts

► Select *Authorizations* → *User, Accounts* tab.



| Type | Account | Role | Name | Comment |
|---|---|---|---|---|
| All ▾ | Filter | All ▾ | Filter | Filter |
| ⌂ | ad1 | Administrator | Administrator 1 | |
| ⌂ | ad2 | Administrator | Administrator 2 | |
| ⌂ | admin | Administrator | System Administrator | |
| ⌂ | autoadm | Administrator | automatic administra | for AutoSEM tests |
| ⌂ | autoopr | Operator | | |
| ⌂ | b0opr | Operator | Operator B0 | |
| ⌂ | b1opr | Operator | Operator B1 | |

Total: 31

The *Accounts* tab displays the existing accounts. A BS2000 administrator, operator, XenVM administrator or AU administrator sees only his/her own account.

The Customer Support account *service* (*Service* role) is only displayed. You cannot administer service accounts.

*Set up new access*

► Click *Set up new access* and make the required entries for the new account in the subsequent dialog.

ℹ You can create an account for the *XenVM administrator* role only if at least one SU x86 with a XenVM license exists on the SE server.
You can create an account for the *AU administrator* role only if at least one AU exists on the SE server.

*Change account*

ℹ For the BS2000 administrator, operator, XenVM administrator and AU administrator the functionality is restricted to his/her own account:

► In the required account click the *Change* icon and change the required access properties.

*Delete account*

ℹ Every user with the *administrator* role can remove any other user. Only the predefined accounts *admin* and *service* and other service accounts cannot be deleted.

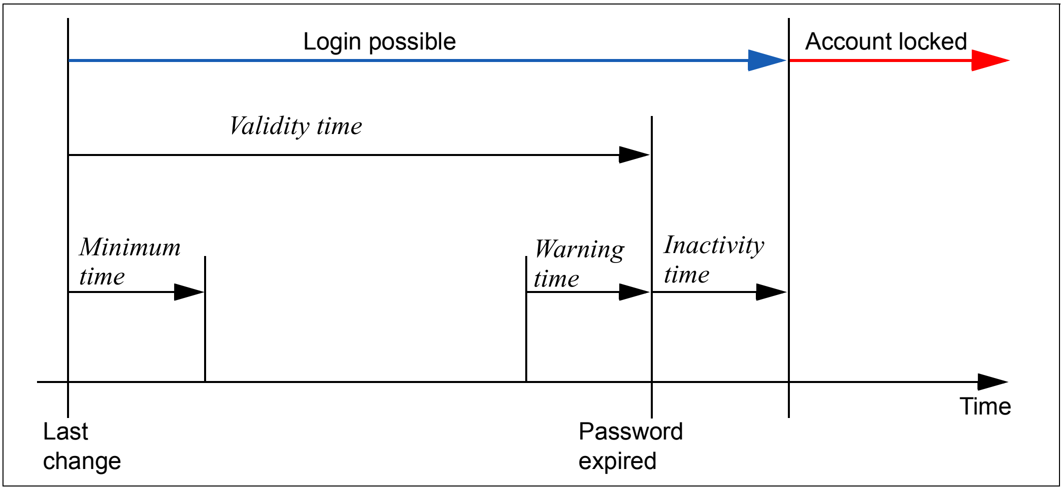
► On the *Accounts* tab click the *Delete* icon and confirm the action.

## 11.1.2 Managing passwords

The passwords of the local accounts have the attributes *Validity time*, *Warning time*, *Minimum time*, and *Inactivity time*:

- During the Validity time, which applies from the last time the password was set, it is possible to log in without restriction.
- During the *Minimum time* which is defined by the administrator; the BS2000 administrator, operator or XenVM administrator cannot change his/her own password.
- During the warning time, a warning is issued that the password will soon no longer be valid. However, it is possible to log in without restrictions.
- During the inactivity time, the password is no longer valid, but it is still possible to log in. Directly after a user has logged in, a request to change the password is issued.
- After the inactivity time has elapsed, the account is locked. It can be opened again from an(other) administration account or, if necessary, by Customer Support.
- The value *-1* for the *Inactivity time* results in the inactivity time not elapsing.
- The value *99999* for the *Validity time* means, in practice, that you need not change the password.

The figure below shows the relationship between these times.



When the SE server is supplied, the following values are predefined for the *Validity time*, *Warning time, Minimum time*, and *Inactivity time* for the standard account *admin*:

| **Account** | **Minimum time** | **Validity time** | **Warning time** | **Inactivity time** | **Comment** |
|---|---|---|---|---|---|
| admin | 0 | 60 | 7 | -1 | The account is never locked, it is always possible to log in with the old password. The value -1 for the inactivity time means that it never expires. |

When you create another local account using the SE Manager, the passwords you specify are initially assigned the following attributes:

| **Account** | **Minimum time** | **Validity time** | **Warning time** | **Inactivity time** |
|---|---|---|---|---|
| <name> | 7 | 60 | 7 | 7 |

The minimum time is not relevant for an administrator account and the value 0 is therefore displayed for it.

As administrator you can disable an account in the password management. You can only log in under this account again if you activate the account.

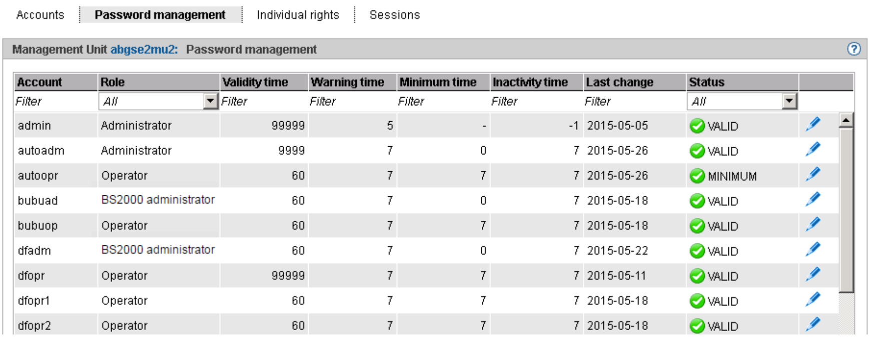
You can also force a change of password. When you force a change of password for an account which is locked by the system, you permit a one-off login using the previous password.

On the *Password management* tab you manage the passwords of the defined accounts.

i For the BS2000 administrator, operator, XenVM administrator and AU administrator the functionality is restricted to his/her own account: He/She can change his/her own password if it has not yet expired and the minimum time between two changes has been reached.

### Displaying passwords

► In the tree structure select *Authorizations* → *User*, *Password management* tab.



Management Unit abgse2mu2: Password management

| Account | Role | Validity time | Warning time | Minimum time | Inactivity time | Last change | Status | |
|---|---|---|---|---|---|---|---|---|
| Filter | All | Filter | Filter | Filter | Filter | Filter | All | |
| admin | Administrator | 99999 | 5 | - | -1 | 2015-05-05 | ✓ VALID | ✎ |
| autoadm | Administrator | 9999 | 7 | 0 | 7 | 2015-05-26 | ✓ VALID | ✎ |
| autoopr | Operator | 60 | 7 | 7 | 7 | 2015-05-26 | ✓ MINIMUM | ✎ |
| bubuad | BS2000 administrator | 60 | 7 | 0 | 7 | 2015-05-18 | ✓ VALID | ✎ |
| bubuop | Operator | 60 | 7 | 7 | 7 | 2015-05-18 | ✓ VALID | ✎ |
| dfadm | BS2000 administrator | 60 | 7 | 0 | 7 | 2015-05-22 | ✓ VALID | ✎ |
| dfopr | Operator | 99999 | 7 | 7 | 7 | 2015-05-11 | ✓ VALID | ✎ |
| dfopr1 | Operator | 60 | 7 | 7 | 7 | 2015-05-18 | ✓ VALID | ✎ |
| dfopr2 | Operator | 60 | 7 | 7 | 7 | 2015-05-18 | ✓ VALID | ✎ |

The *Password management* tab displays defined accounts with their password data.

*Changing password data*

i You can only change the password attributes if you are an administrator. For the BS2000 administrator, operator, XenVM administrator and AU administrator the functionality is restricted to his/her own account: He/She can change his/her own password if it has not yet expired and the minimum time between two changes has been reached.

► Click the *Change* icon for the required account and change the properties as required.

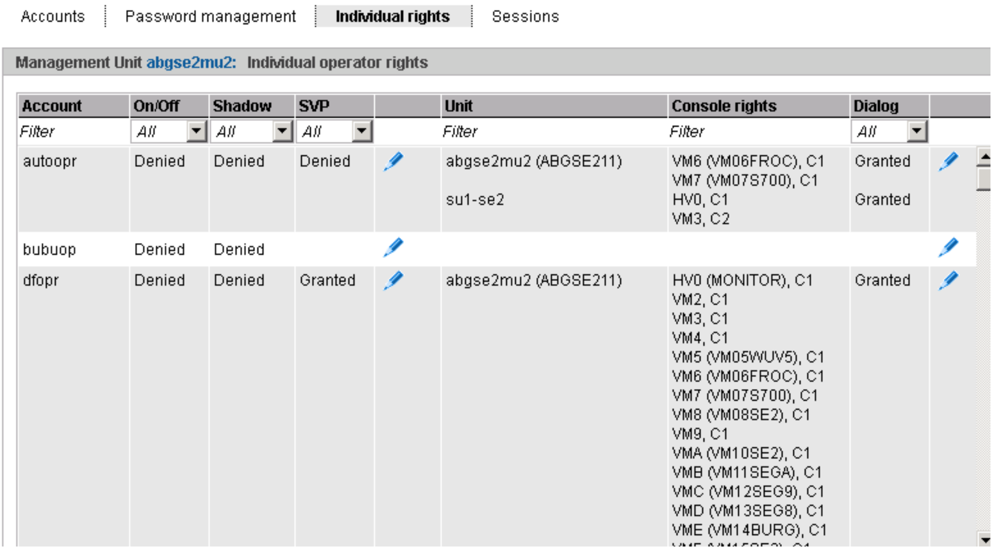
### 11.1.3 Managing individual rights

The *Individual rights* tab displays the operator accounts and their individual rights which are currently assigned. With individual rights a distinction is made between server-related rights (e.g. powering Units on/off) and system-related rights (access to particular BS2000 systems).

The tag is not available to a BS2000 administrator, XenVM administrator or AU administrator.

For an operator the functionality is restricted to his/her own account. He/She only sees his/her own rights. Only an administrator can make changes.

► Select *Authorizations* → *User*, *Individual rights* tab.



Management Unit abgse2mu2: Individual operator rights

| Account | On/Off | Shadow | SVP | | Unit | Console rights | Dialog | |
|---|---|---|---|---|---|---|---|---|
| Filter | All | All | All | | Filter | Filter | All | |
| autoopr | Denied | Denied | Denied | ✎ | abgse2mu2 (ABGSE211)<br>su1-se2 | VM6 (VM06FROC), C1<br>VM7 (VM07S700), C1<br>HV0, C1<br>VM3, C2 | Granted<br>Granted | ✎ |
| bubuop | Denied | Denied | | ✎ | | | | ✎ |
| dfopr | Denied | Denied | Granted | ✎ | abgse2mu2 (ABGSE211) | HV0 (MONITOR), C1<br>VM2, C1<br>VM3, C1<br>VM4, C1<br>VM5 (VM05WUV5), C1<br>VM6 (VM06FROC), C1<br>VM7 (VM07S700), C1<br>VM8 (VM08SE2), C1<br>VM9, C1<br>VMA (VM10SE2), C1<br>VMB (VM11SEGA), C1<br>VMC (VM12SEG9), C1<br>VMD (VM13SEG8), C1<br>VME (VM14BURG), C1 | Granted | ✎ |

The *Individual rights* tab lists all operator accounts together with their individual rights.

*Change server-related rights*

i Only the administrator can make changes.

► In the required account click the *Change server-related rights* icon after the *SVP* column. In the subsequent dialog, assign the required server-related operator rights.

*Change system-related rights*

ℹ Only the administrator can make changes.

► In the required account, click the *Change system-related rights* icon in the rightmost column. In the subsequent dialog, assign the required system-related operator rights.

*Managing access to the BS2000 console and dialog*

An operator can access the console of a BS2000 system solely by means of individual authorizations.

BS2000 communicates with KVPs using the mnemonic names of the KVP devices concerned. In addition, consoles to be used by operators and administrators in BS2000 must be configured with a mnemonic console name and assigned rights must be configured in the OPR parameter record of the parameter service (see the manual “Introduction to System Administration”, DEFINE-CONSOLE and SET-CODE instructions). When a KVP is configured, the mnemonic console names *C0* and *C1* which are by default configured in BS2000 are automatically assigned. These console names can be changed in BS2000. However, changes become effective only after the BS2000 system has been started up again.

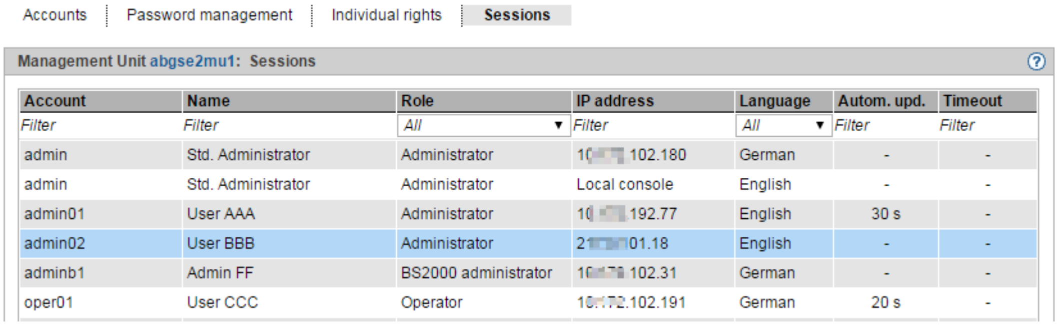
An administrator can always access the BS2000 consoles. An operator can only access BS2000 consoles for which he/she has an individual right,see section “Change system-related rights” on page 276.

## 11.1.4 Displaying sessions

The Sessions tab informs the administrator about all session of users who are currently logged in on the SE Manager of the local Management Unit.

In addition to the information on the user and IP address of the PC, the current individual setting for the session is also displayed.

► Select *Authorizations* → *User*, *Sessions* tab.



Management Unit abgse2mu1: Sessions

| Account | Name | Role | IP address | Language | Autom. upd. | Timeout |
|---|---|---|---|---|---|---|
| *Filter* | *Filter* | *All* ▼ | *Filter* | *All* ▼ | *Filter* | *Filter* |
| admin | Std. Administrator | Administrator | 1[redacted]102.180 | German | - | - |
| admin | Std. Administrator | Administrator | Local console | English | - | - |
| admin01 | User AAA | Administrator | 1[redacted]192.77 | English | 30 s | - |
| admin02 | User BBB | Administrator | 2[redacted]01.18 | English | - | - |
| adminb1 | Admin FF | BS2000 administrator | 1[redacted]102.31 | German | - | - |
| oper01 | User CCC | Operator | 1[redacted]72.102.191 | German | 20 s | - |

The *Sessions* tab provides information on the users currently logged in. The local session is highlighted.

# 11.2 Configuration

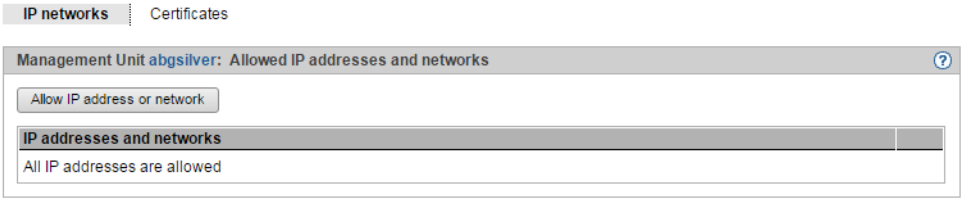
In the *Authorizations→ Configuration* menu you manage the IP-based access restrictions to the MU and digital certificates.

## 11.2.1 IP-based access restriction to the MU

In M2000 V6.1A and higher the administrator can configure access to the MU (applies for the SE Manager and CLI) in such a manner that it is possible only for explicitly entered IP addresses or for IP addresses from an explicitly entered IP network.

By default the list for access restrictions is empty, and access is permitted without restriction for all IP addresses and networks.

► In the tree structure select *Authorizations→ Configuration*, *IP networks* tab.



IP networks
Certificates
Management Unit abgsilver: Allowed IP addresses and networks
Allow IP address or network

| IP addresses and networks | |
|---|---|
| All IP addresses are allowed | |

The *IP networks* tab displays the IP addresses and networks access to the MU is allowed.

The following options are available to you:

*Allow IP address or network*

► Click *Allow IP address or network* and enter the IP address or network in the subsequent dialog box.

> i With the first entry (IP address or IP network) you enable IP-based access restriction to the MU. Access is then only possible for IP addresses which are entered either explicitly or via an IP network.

*Remove IP address or network*

► By the required IP address or network, click the *Remove* icon and confirm the action.

> i When you delete the last entry from the list for access restriction, access to the MU is once again possible for all IP addresses without restriction.

### 11.2.2 Digital certificate

To use HTTPS/SSL, not only an SSL key pair is required on the system, but also a (digital) SSL certificate. This server certificate performs the following two tasks:

- The certificate is always system-specific (contains the FQDN) and proves the online identity of the system concerned for the browser on the administration PC.
- The certificate provides the public key with which the browser encrypts its messages to the server on the administration PC.

A self-signed, system-specific certificate which was generated on the system is preinstalled as the standard certificate on each of the systems.

You can also use other certificates on your SE server instead of the preinstalled self-signed certificate. The following options are available:

- Use of a self-signed certificate

  A certificate of this type is preinstalled on the system as the standard certificate. It must be explicitly confirmed or imported on any browser with which the SE Manager operates.

- Use of a customer-specific certificate (signed by a customer CA)

  If the customer-specific policy specifies the use of such a certificate, it can simply be installed.

  The certificate is as a rule derived from a customer-specific root certificate. Such a certificate is known to the browsers the customer uses and is accepted without an inquiry (i.e. without being confirmed or imported).

- Use of a commercial certificate (signed by a root CA)

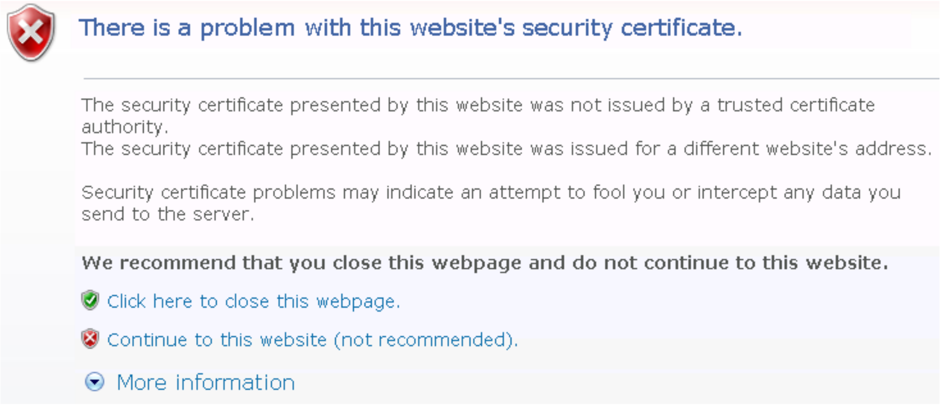
  A certificate of this type is created for a fee by a trusted root certification authority (CA) and is therefore known to all browsers. Consequently every browser accepts such certificates without an inquiry.

### 11.2.2.1 Confirming/importing a certificate in the web browser

If the web interface called uses a self-signed certificate (i.e., for example, the preinstalled standard certificate), web browsers reject the call for the page because, from their viewpoint, the certificate is not trusted. To permit pages of the SE Manager to be loaded in the browser at all, you must either temporarily accept the certificate error or import the certificate permanently in the browser.

The procedure described in principle below is based on Internet Explorer Version 11 or higher and differs according to the browser used and the version. You will find details of the specific procedure in your browser’s online help.

- ► Open your web browser.
- ► In the browser window call the SE Manager of the required system.



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

**We recommend that you close this webpage and do not continue to this website.**

Click here to close this webpage.

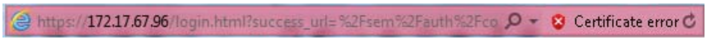
Continue to this website (not recommended).

More information

The web browser reports a certificate error.

- ► Confirm that the website should be loaded.

You are shown the login page. The browser’s address bar displays *Certificate Error* as a warning.



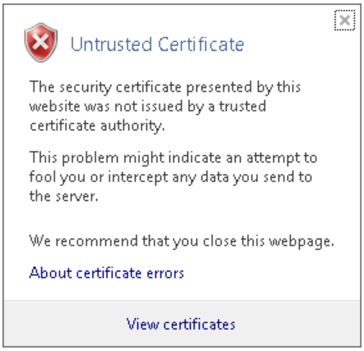
https://172.17.67.96/login.html?success_url=%2Fsem%2Fauth%2Fco

Certificate error

The certificate has now been temporarily accepted for this session, and you can now work with the SE Manager of this system.

To prevent this browser message from being displayed in future, you can also import the certificate.

► Click *Certificate Error* in the browser's address bar.



Untrusted Certificate

The security certificate presented by this website was not issued by a trusted certificate authority.

This problem might indicate an attempt to fool you or intercept any data you send to the server.

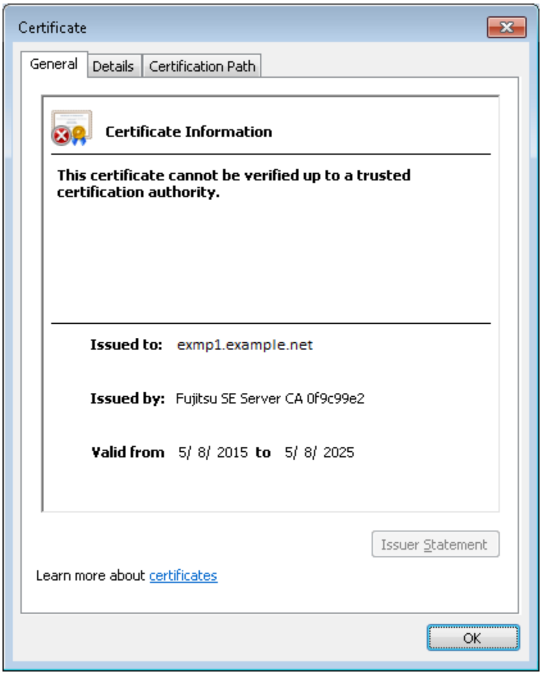
We recommend that you close this webpage.

About certificate errors

View certificates

You are shown information about the potential security risk, and *About certificate errors* enables you to view more detailed information in the browser's online help.

► Click *View Certificates*.



Certificate

General | Details | Certification Path

Certificate Information

This certificate cannot be verified up to a trusted certification authority.

Issued to: exmp1.example.net

Issued by: Fujitsu SE Server CA 0f9c99e2

Valid from 5/ 8/ 2015 to 5/ 8/ 2025

Issuer Statement

Learn more about certificates

OK

Check the certificate (further details are provided on the *Details* and *Certification Path* tabs).
Continue only if no doubts exist about the certificate.

► Click *Install Certificate*.

The certificate import wizard starts and guides you though installation of the certificate step by step.

i Alternatively or for other browsers, you can also download and install the CA certificate, see page 287.

### 11.2.3 Managing certificates

You can create and manage new SSL certificates on the *Certificates* tab. In the case of HTTPS communication a server identifies itself to its client with an SSL certificate. An SSL certificate is only ever issued for a server, an organization and a particular period. This information is contained in the certificate and can be viewed in a certificate viewer (e.g. browser). The validity of this information is confirmed by a trusted certification authority (CA) by means of the authority's digital signature.

The *Certificates*tab provides the following functions for managing certificates:

- Using the standard certificate
  - Displaying the current SSL certificate
  - Displaying details of the current SSL certificate
- Creating and enabling a new self-signed SSL certificate
- Requesting an SLL certificate
  - Displaying details of the current SSL certificate request
  - Downloading the SSL certificate request
- Uploading and activating a customer-specific certificate
- Downloading a CA certificate and installing it in the browser

Detailed information on the tab is provided in the SE Manager help.

### 11.2.3.1 Using the standard certificate

A self-signed, system-specific certificate is preinstalled on the SE server. This is not known directly by the web browsers, nor is it derived from a known root certificate.

A standard certificate is automatically generated and activated each time the system is renamed (the FQDN is changed). The new standard certificate must then of course be accepted by or imported to the browsers.

The main features of this certificate are:

- The *common name (CN)* is identical to the fully qualified domain name (FQDN) of the base operating system.
- The Validity time is 10 years.
- The fingerprint which unambiguously identifies the certificate is generated using the SHA-1 algorithm and RSA encryption.

As the browser does not know the self-signed certificate, when the SE Manager is called it requests the user to accept the certificate temporarily for the current session or to import it permanently.
If you call the SE Manager on the local console, you must also confirm or import the standard certificate, because the browser used on the Gnome desktop does not know the certificate, either.

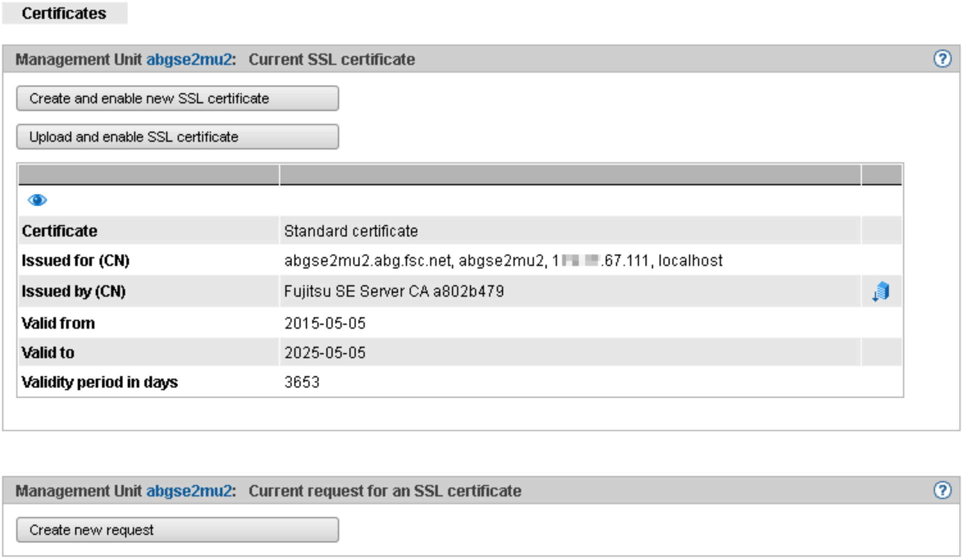
You are granted access to the SE Manager of the system component only if the certificate is temporarily accepted or permanently imported.

If in doubt, you should first read and cross check the certificate before accepting it temporarily or importing it permanently.

### Displaying the current SSL certificate

► In the tree structure select *Authorizations > Configuration.*

The *Certificates* tab with the *Current SSL certificate* and *Current request for an SSL certificate* groups opens..



Certificates

Management Unit abgse2mu2: Current SSL certificate

Create and enable new SSL certificate

Upload and enable SSL certificate

| | | |
|---|---|---|
| Certificate | Standard certificate | |
| Issued for (CN) | abgse2mu2.abg.fsc.net, abgse2mu2, 1[redacted].67.111, localhost | |
| Issued by (CN) | Fujitsu SE Server CA a802b479 | |
| Valid from | 2015-05-05 | |
| Valid to | 2025-05-05 | |
| Validity period in days | 3653 | |

Management Unit abgse2mu2: Current request for an SSL certificate

Create new request

The information displayed is described in the SE Manager help.

### Displaying details of the current SSL certificate

► In the tree structure select *Authorizations → Configuration.*

The *Certificates* tab opens.

► To display further details, click the *Details* icon in the *Current SSL certificate* group.

The *Detailed display of the current SSL certificate* dialog box opens. The information displayed is described in the SE Manager help.

### 11.2.3.2 Creating and enabling a new self-signed SSL certificate

The preinstalled standard certificate contains data which is naturally not customer-specific.

If you want to work with a certificate with customer-specific data, you can at any time create and use such a certificate. This action can also be necessary when you want to renew a certificate.

> - When a certificate is activated, the web server is also automatically rebooted.
> - As the web browser does not know how trustworthy the new certificate is, like the standard certificate it must be explicitly accepted or imported (see the section "Confirming/importing a certificate in the web browser" on page 280).

► In the tree structure select *Authorizations → Configuration.*

► In the *Current SSL certificate* group, click *Create and enable new SSL certificate.*

The *Create and enable SSL certificate* dialog box opens.

► Make the necessary entries. Detailed information on the entries is provided in the SE Manager help.

► Click *Create and enable*.

The certificate is created, activated immediately and displayed as the current certificate.

### 11.2.3.3 Requesting an SLL certificate

> Any existing request is overwritten.
>
> For the following reasons you should not perform reinstallation or change the host name between the certificate signing request being created and the signed certificate being entered in the system:
>
> – When the certificate signing request is created, it is linked to the system's standard SSL key. If this key is changed in the system in the time between the certificate signing request being created and the signed certificate being entered in the system, the certificate cannot be used.
>
> – A new standard SSL key is created when reinstallation takes place or when the host name is changed.

- ► In the tree structure select *Authorizations → Configuration.*
- ► In the *Current request for an SSL certificate* group, click *Create new request.*

  The *Create SSL certificate request* dialog box opens.
- ► Make the necessary entries. Detailed information on the entries is provided in the SE Manager help.
- ► Click *Create*.

  The request is created and displayed as the current request. To send the request to the certification authority by email, first download the request to your administration PC, see section “Downloading the SSL certificate request” on page 286.

  When the signed certificate is returned to you, enter the certificate in the system: see the “Uploading and activating a customer-specific certificate” on page 286 and section “Using the standard certificate” on page 283.

#### Displaying details of the current SSL certificate request

- ► In the tree structure select *Authorizations → Configuration.*
- ► In the *Current request for an SSL certificate* group, click the *Details* icon.

  The *Detailed display of the current SSL certificate* dialog box opens. The information displayed is described in the SE Manager help.

#### Downloading the SSL certificate request

- ► In the tree structure select *Authorizations → Configuration.*
- ► In the *Current request for an SSL certificate* group, click the *Download request.* symbol.

  The file with the current request for the SSL certificate is downloaded in the browser.

### 11.2.3.4 Uploading and activating a customer-specific certificate

Instead of a self-signed certificate generated in the system (standard certificate or user-defined certificate), you can use a certificate of your own to access the system’s SE Manager.

*Requirement*

A certificate signing request was generated in the system for the certificate (see section “Requesting an SLL certificate” on page 285) and sent to a certification authority.

*Procedure*

As soon as the certificate signed by the CA (certification authority) is available to you, you can upload and activate it.

> **i**
> - When a certificate is activated on the target system, the web server is also automatically rebooted with the new certificate. A brief interruption of the SE Manager's connection to the system can occur.
> - If the web browser used (on the administration PC or local console) knows that the new certificate is trusted or knows its root certificate, no further action is required.
> - If the web browser does not know that a certificate is trusted, the certificate must be explicitly confirmed or imported (see the section “Confirming/importing a certificate in the web browser” on page 280).

► In the tree structure select *Authorizations* → *Configuration.*

► In the *Current SSL certificate* group, click *Create and enable new SSL certificate.*

The *Create and enable SSL certificate* dialog box opens.

► Make the necessary entries. Detailed information on the entries is provided in the SE Manager help.

► Click *Upload*.

The files specified are uploaded into the target system, activated immediately and displayed as the current SSL certificate.

### Downloading a CA certificate and installing it in the browser

To prevent a certificate error, you can download the SE server's CA certificate and install it in the browser.

► Select *Authorizations* → *Configuration*, *Certificates* tab. The table displays the current certificate:

► In the *Issued by (CN)* row click the *Download CA certificate* icon.

After the download, you can install the certificate in your browser.

► Open the certificate file and click *Install Certificate*.

The browser's certificate import wizard takes you through certificate installation step by step.

# Glossary

**Application Unit (AU)**

Component of the SE server; with the help of the SE Manager, enables central, web-based management of customer applications. An AU permits operation of applications under Linux, Windows, VMware or other hypervisors.

**AU**

See Application Unit (AU).

**FDDRL job**

For each FDDRL function statement, one FDDRL job is defined per single or pubset disk. Another FDDRL job is defined per disk set. Each FDDRL job can be handled either under the calling task (FDDRL maintask) or under a separate task (FDDRL subtask).

**FDDRL subtask**

FDDRL jobs can be processed by a subtask generated by FDDRL.

**HAL**

See Hardware Abstraction Layer (HAL).

**Hardware Abstraction Layer (HAL)**

Firmware component on SU x86 for mapping privileged /390 interfaces to the basic machine code. This mapping is required, for example, when handling exceptions, managing memory and also for system diagnostics.

**HNC**

High Speed Net Connect

HNC implements the connection from an SU /390 to a LAN. HNC designates both the Linux-based basic software which is integrated into the SE Manager and the hardware unit on which this basic software runs. As a hardware unit, the HNC is a component part of the Net Unit on SE servers which have an SU / 390.

**Initial Program Load (IPL)**

First phase of system initialization after booting. IPL reads in the CLASS1-EXEC, system parameters, and REPs.

**IO Configuration File (IOCF)**

Contains information on the configuration of the input/output devices of an SU / 390. The IOCF must be installed in the service processor.

**IOCF**

See IO Configuration File (IOCF).

**IPL**

See Initial Program Load (IPL).

**KVP**

console distribution program
Access to a BS2000 console window takes place via a KVP (console distribution program).
The KVP performs the following tasks, among others:

- Authorization checks
- Distribution of the BS2000 tasks to multiple console windows
- Short- and long-term storage of the console communication logs (KVP logging)

BS2000 sees a KVP as two (emulated) KVP devices (or a device pair) which are identified by their mnemonic names.

**Management Unit (MU)**

Component of the SE server; with the help of the SE Manager, enables central, web-based management of of all units of an SE server.

**MU**

See Management Unit (MU).

**net client**

Implements access to Net-Storage for the operating system using it.
In BS2000/OSD the net client, together with the BS2000 subsystem ONETSTOR, transforms the BS2000 file accesses to corresponding UNIX file accesses and executes these using NFS on the net server.

**net server**

File server in the worldwide computer network which provides storage space (Network Attached Storage, NAS) for use by other servers and offers corresponding file server services.

**Net Unit**

Component of the SE server; enables an SE server to be connected to customer networks (LAN/SAN). The Net Unit incorporates High Speed Net Connect (HNC).

**Net-Storage**

The storage space provided by a new server in the computer network and released for use by foreign servers. Net-Storage can be a file system or also just a node in the net server's file system.

**Parallel Access Volume (PAV)**

Multiple I/O requests can be executed simultaneously to a logical volume. A logical PAV volume is represented by a basic device and up to seven alias devices.

**PAV**

See Parallel Access Volume (PAV).

**SE Manager**

Web-based user interface for SE servers. The SE Manager runs on the Management Unit and permits central operation and administration of Server Units (SU /390 and SU x86), Application Units (x86), Net Unit (including HNC), and the storage.

**Server Unit /390 (SU /390)**

Component of the SE server; Server Unit with /390 architecture. A /390-based Server Unit (SU /390) enables operation of BS2000 (Native BS2000 or VM2000).

**Server Unit x86 (SU x86)**

Component of the SE server; Server Unit with x86 architecture. An x86-based Server Unit (SU x86) enables operation of BS2000 (Native BS2000 or VM2000). XenVM operation with Linux or Windows guest systems is also possible as an option.

**SKP**

service and console processor
An SKP enables servers with /390 architecture to be operated, the connected devices to be managed, and remote service to be supported.
The term **SKP** is used in the three views hardware functionality, software functionality, and device type:
The term **SKP** is used in the three views hardware functionality, software functionality, and device type:
**Hardware functionality**
To operate, S servers require an SKP as a Hardware Unit. The SKP Hardware Unit SKP is a PRIMERGY server which has a local console, a Host Controller, and various ports for LAN connection and supporting remote service.
On the SE server the Management Unit (MU) provides this hardware functionality for operating SU /390.
**Software functionality**
On an SKP Hardware Unit the SKP Manager provides the SKP functionality for operating the S server and managing the devices and remote service.
On the SE server the SKP functionality is integrated into the SE Manager.
**Device type**
In BS2000 an SKP device type is used (e.g. SKP2).

**SVP**

service processor

**SVP clock**

Autonomous clock which supplies the TODR with the real time at system startup. In SU /390 the SVP clock is part of the SVP. In SU x86 the SVP clock is emulated via the basic software X2000.

# Related publications

You will find the manuals on the internet at *http://manuals.ts.fujitsu.com*. You can order printed versions of manuals which are displayed with the order number.

[1] **FUJITSU Server BS2000**<br>
**SE700 / SE500 / SE300**<br>
Basic Operating Manual

[2] **FUJITSU Server BS2000**<br>
**SE700 / SE500**<br>
Server Unit /390<br>
Operating Manual

[3] **FUJITSU Server BS2000**<br>
**SE700 / SE500 / SE300**<br>
Server Unit x86<br>
Operating Manual

[4] **FUJITSU Server BS2000**<br>
**SE700 / SE500 / SE300**<br>
Additive Components<br>
Operating Manual

[5] **FUJITSU Server BS2000**<br>
**SE700 / SE500 / SE300**<br>
Administration and Operation User Guide<br>
User Guide

[6] **FUJITSU Server BS2000**<br>
**SE700 / SE500 / SE300**<br>
Security Manual<br>
User Guide

[7] **FUJITSU Server BS2000**<br>
**SE700 / SE500 / SE300**<br>
Quick Guide<br>
User Guide

[8] **BS2000 OSD/BC V10.0**
**System Installation (SE Server)**
User Guide

[9] **BS2000 OSD/BC V10.0**
**Introduction to System Administration (SE Server)**
User Guide

[10] **BS2000 OSD/BC**
**Utility Routines**
User Guide

[11] **VM2000** (BS2000)
**Virtual Machine System**
User Guide

[12] **openNet Server**
**BCAM Volume 1/2**
User Guide

[13] **openSM2**
**Software Monitor**
User Guide

[14] **ServerView Suite**
**iRMC S2 - integrated Remote Management Controller**
User Guide

[15] **ServerView Suite**
**ServerView Operation Manager**
Installation for Linux / Installation for Windows (one Installation Guide for each)

[16] **ServerView Suite**
**ServerView Operation Manager**
Installation of the ServerView agents for Linux / Installation of the ServerView agents for Windows (one Installation Guide for each)

[17] **LSI MegaRAID**
**SAS Software**
User Guide

[18] **LSI Controllers**
**Modular RAID Controller**
Installation Guide

# Index

**A**

account 67
- admin 269
- managing 269
- service 269

account management 269
accounts 269
ACL
- DANPU 243
- Management Networks Private 254
- MANPU 250

ACL (Access Control List) 35
action, executing 83
add-on pack 25, 26, 28
admin (administrator role) 44, 269
administrator 269
- role 43

AIS agent
- displaying 206

AIS Connect
- reading log 208

Application Unit 21, 228
- configuring 228
- installing 137

architecture of SE server 23
asset, external 206
ATTACH-DEVICE 172
AU administrator 269
Autoconf 41
automatic startup
- XenVM 122

automatic update 69
AutoYAST XML file 182

**B**

basic software
- HNC 25
- M2000 24
- X2000 24

boot disk
- XenVM 127

BRGLAN 38, 166
BS2000
- remaining runtime 103, 108

BS2000 administrator 269
- role 43

BS2000 console
- messages 99

BS2000 pool 53
BS2000 VM
- operating menu 108

BS2000 ZASLAN 37
burning
- CD/DVD 173

burning DVD 173

**C**

CA certificate downloading 287
CD
- burning 173
- taking over files (BS2000/OSD) 170

CDROM files 170
certificate
- confirming 280
- server's own CA certificate certificate downloading 287

channel path identifier 153
CHECK-TAPE 172
CLI 201

Command Line Interface 201
components
  displaying 263
configuration data backup
  downloading/deleting 205
  executing 204
  executing (HNC) 217, 226
  uploading 205
configuration errors (XenVM) 116
Configuration Save and Restore 204, 217, 226
connections, displaying 257
console
  XenVM 123
console distribution program 162
CPU
  real 53
CPU assignment 53
CPU pool 53
CSR 204
CSR (SU x86) 226
CSR backup
  managing (HNC) 217
  managing (MU) 204
  managing (SU x86) 226
Customer Support
  tasks 60

**D**
D3435 (disk type) 159
D3475-8F (disk type) 159
DANPR 32, 246
DANPU 32, 241
data network
  private 32
  public 32
Data Network Private (DANPR) 32
Data Network Public (DANPU) 32
database
  for virtual disks 177
  for virtual disks (XenVM) 177
DETACH-DEVICE 172, 173
device addressing, BS2000 152
DHCPv4 41
DHCPv6 41
diagnostic data, generating 205, 218, 227
dialog 76, 83
disk pool 58, 178
  creating 177
  deleting 177
  displaying information 176
  extending 177
disk, virtual 58
disks (BS2000/OSD)
  managing 159
DNS entry
  adding to SENET 235
DNS entry, adding
  SENET 240
DNS server 34
domain, changing
  MU 193
download server 27
DVD
  taking over files (BS2000/OSD) 170
DVD burner 170
DVD drive
  physical 182
  virtual 182

**E**
EMFILEs 170
errors
  while creating the XenVM 116
  while installing the XenVM 119
external virtual switch 180

**F**
FC interfaces
  HNC 211
  MU 191
  SU /390 187
filter 82
full virtualization 52

**G**
graphics card, changing 125

**H**
HAL (message class) 99
hardware virtualization 52
high availability
    LAN connection 180
HNC 18, 289
    Open Source licenses 19
HNC (basic software) 25
host name, changing
    MU 193
hot fix 26, 28
HV0 162

**I**
icon 83
import filter 82
inactivity time 272
INIT 172, 173
initial password 67
installation configuration file 182
installation information
    deleting 120
    history 119
installation log
    displaying content 120
    viewing 119
installation medium
    reading in 182
installation process
    aborting 119
    monitoring 119
installation source 59
    adding 130
    assigning 130
    managing 182
    removing 131
    switching 130
internal virtual switch 180
inventory information
    changing 264
IOD (message class) 99
IP address, adding
    MU 194
IP address, changing
    Application Unit 229
IP configuration
    AU25/AU47 231
    AU87/DBU87 232
IP interfaces
    HNC 210
    MU 190
IP-based access restriction 45, 278
IPv6 autoconfiguration 33
IPv6 log 41
ISO image file 182

**K**
keyboard language
    changing 125
KVP (message class) 99
KVP device, managing 162

**L**
LAN configuration
    Application Unit 229
licenses for Open Source Software 19
Linux/Windows pool 54
local library 130
local system data for SNMP
    changing 198
LOCLAN 37, 166
LOCLAN (MU)
    changing packet length 190
logging in
    SE Manager 67
    XenVM console 123
logical unit number 153
login window 66
logs
    AIS Connect 208

**M**
M2000
    Open Source licenses 19
M2000 (basic software) 24

MAC address
  DANPR 242
  Management Networks Private 252
  MANPU 250
main memory 55
main window 71
maintenance window 62
Management Admin Network Public
  (MANPU) 32
Management Control Network Local
  (MCNLO) 32
Management Control Network Private
  (MCNPR) 32
management network
  private 32
  Public 32
Management Network LOCLAN (MANLO) 37
Management Optional Network Private
  (MONPR) 32
Management Optional Network Public
  (MONPU) 32
management station 197
Management SVP Network Private (MSNPR) 32
Management Unit 21
MANLO 37
MANPU 32
MCNLO 32
MCNPR 32
messages
  displaying (FC networks) 257
messages of M2000/X2000 99
metalanguage 17
MIB-II 197
minimum time 272
MN 152
MNEM 152
mnemonic 152
mnemonic name 152
MONPR 32
MONPU 32
MSNPR 32
MU
  restricting IP-based access 45, 278
MU redundancy 46

N
Net Unit 21, 31
network connection
  BS2000 37, 166
network connection, XenVM 39, 59
Network Interface Card
  displaying 129
  removing 129
network properties, changing
  MU 194
network, adding
  DANPR 247
notational conventions 17
NTP (Network Time Protocol) 199
NTP server 36

O
online help 85
Open Source Software
  licenses 19
operator 269
  role 43
Oracle VM Manager 146

P
packet length
  changing for MU 190
parameter area 76
paravirtualization 52
password 67
PCI interfaces (MU)
  changing packet length 190
physical volume 178
pool 0 53
port, removing
  DANPR 242
  Management Networks Private 253
  MANPU 250
ports, adding
  DANPR 242
  Management Networks Private 253
  MANPU 250
powering off
  unit 186

powering on
  unit 185
private networks 31
proxy configuration
  displaying 206
  entering/changing or deleting 208
public networks 31

R
rack view 260
RADVD / DNS / NTP server
  activating (DANPR) 248
Readme file 15
rebooting
  unit 185
redundancy
  MU 46
  SKP functionality 46
remaining runtime
  BS2000 103, 108
  XenVM 121
remote service 62
  process 62
restricting MU access 278
revision 25
REWAS 36
role 269
  administrator 43
  BS2000 administrator 43
  operator 43
  service 44

S
S server 18
SE Manager 23, 50
  interface 70
  logging in 67
SE server 21
  architecture 23, 51
sealing off 53
security fix 25, 26
SENET
  DNS entry, adding 240
senet 34
Server Unit 21
service
  role 44
service (service role) 269
service access
  changing 207
  displaying 206
service pack 25, 26, 28
session 68
session ID 68
sessions
  displaying 206
shadow terminal
  AIS Connect 206
  opening 207
Simple Network Management Protocol (see SNMP) 197
SKP functionality
  redundancy 46
SNMP 197
  changing local system data 198
  read accesses 198
  security 197
  testing traps 199
  trap receiver 199
SNX (message class) 99
software status 25
software update 27
standard account, password 67
Storage Manager 259
storage system (external asset) 206
Storman 259
SU /390 18
  implementation of VM2000 48
SU x86 18
  implementation of VM2000 49
SVR (message class) 99
switch
  virtual 39, 59
switch, adding 256
switch, changing 256
switch, removing 256

system information
  HNC 209
  MU 189
  SU /390 187
system initialization
  automatic 122
system version 25

**T**
tab
  Accounts 270
  Configuration 125
  CSR 204, 226
  Diagnostics 205, 218, 227
  Disk pools 175, 176
  Installation sources 182
  IP configuration (HNC) 212
  IP configuration (MU) 193
  IP configuration (SU /390) 187
  IP networks 129
  Net-Storage (HNC) 214
  Net-Storage (SU x86) 223
  Operation 123, 124
  Remote Service 206
  Routing & DNS 195, 196
  Routing & DNS (HNC) 213
  Routing & DNS (MU) 214
  Routing & DNS (SU x86) 222, 223
  SNMP 198, 205, 218, 227
  Update (HNC) 217
  Update (SU x86) 226
  Virtual disks 178
  Virtual switches 180
  VM administration 115
  VM installation 119
  VM options 121
  VM resources 118
terminal window 74
test
  SNMP traps 199
trap receiver
  SNMP 199

**U**
unit
  powering off 186
  powering on 185
  rebooting 185
unit ID 152
units
  displaying 262
UNLOAD-TAPE 173
update 25
  providing 62
  responsibilities 63
  tasks 63
update status 25, 27
Updates
  displaying (HNC) 217
updates
  displaying (SU x86) 226
user account see account
user management 269

**V**
validity 272
virtual disk 58
  changing size 127
  displaying disks of the XenVM 126
  displaying XenVM assignment of all disks 178
  removing 128
  updating data base 177
virtual DVD device 130
virtual DVD drive 182
virtual Network Interface Card 129
virtual switch
  external 180
  internal 180
  removing from the configuration 181
VM type 53
VM2000 52
volume group 178
vSwitch 39, 59
  external 39
  internal 39

**W**
warning time 272
welcome page SE Manager 67
wildcards
    device specifications 114
window type 70
wizard, Create new XenVM 116

**X**
X2000
    Open Source licenses 19
X2000 (basic software) 24
Xen hypervisor 49
XenVM
    configuring Network Interface Card 129
    displaying configuration 125
    displaying installation sources 130
    displaying virtual disks 126
    handling configuration errors 116
    opening console 123
    operating menu 123
    powering off 124
    remaining runtime 121
    removing Network Interface Card 129
    removing virtual disk 128
    restarting 124
    shutting down 124
    starting 124
    starting automatically 122
    stopping 124
    unpausing 124
XenVM administrator 269
XenVM console
    opening 123
XenVM devices
    managing 126
XenVM license 52

**Z**
ZASLAN 37, 166