

FUJITSU Server BS2000

SE700 / SE500 / SE300

Administration and Operation

User Guide

Valid for:

M2000 V6.2A SP1 (V6.2A05 and higher)

X2000 V6.0A SP1 (V6.2A05 and higher)

HNC V6.2A SP1 (V6.2A05 and higher)

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

Copyright © 2018 Fujitsu Technology Solutions GmbH.

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

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

The Xen® mark is a trademark of Citrix Systems, Inc., which manages the mark on behalf of the Xen open source community. The Xen® mark is registered with the U.S. Patent and Trademark Office, and may also be registered in other countries.

Novell and SUSE are registered trademarks of Novell, Inc. in the USA and other countries.

Linux is a registered trademark of Linus Torvalds.

Windows® is a registered trademark of Microsoft Corporation.

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.

Content

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	18
1.6	Names and abbreviations	19
1.7	Open Source Software	20
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	26
2.2.3.2	Security fix	27
2.2.3.3	Hot fix	27
2.2.3.4	Add-on pack	27
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	External configuration disks	42
2.5	Cluster	44
2.5.1	Management Cluster	44
2.5.2	SU Cluster	45
2.6	Management Unit and SE Manager	47
2.6.1	Role and user strategy	47
2.6.2	IP-based access to the Management Unit	51
2.6.3	Redundant Management Units	52
2.6.4	Central logging	53
2.7	Virtualization	54
2.7.1	Implementing VM2000	54
2.7.2	Virtualization on Server Unit x86	57
2.7.2.1	CPU pool management	58
2.7.2.2	Main memory management	60
2.7.2.3	BS2000 devices	60
2.7.2.4	XenVM devices	61
2.8	Time synchronization	65
2.9	Customer Support and maintenance	69
2.9.1	Tasks of Customer Support	69
2.9.2	Tasks of the customer	69
2.9.3	Maintenance and remote service	71
2.9.4	Handling updates	71
2.9.4.1	Providing updates	71
2.9.4.2	Tasks and responsibilities when installing updates	72
3	Operating the SE Manager	73
3.1	Calling the SE Manager	74
3.1.1	Logging in	75
3.1.2	Logging out	75
3.2	Session management	76
3.2.1	Session timeout	77
3.2.2	Automatic update	78
3.2.3	Restricted operating mode	78

3.3	SE Manager interface	79
3.3.1	Window types	79
3.3.2	Main window	80
3.3.3	Terminal window	83
3.3.4	The dialog	85
3.3.5	The wizard	86
3.3.6	Web UIs of Application Units	87
3.4	Working with the SE Manager	88
3.4.1	Calling an object or function in the SE Manager	88
3.4.2	Navigation	89
3.4.3	Filtering and sorting a table	92
3.4.4	Executing an action	94
3.4.5	Calling the online help	97
3.4.6	Error handling	99
4	Dashboard	101
<hr/>		
5	Operating and managing systems on Server Units	105
<hr/>		
5.1	Setting BS2000 operation mode	108
5.1.1	Server Unit /390	108
5.1.2	Server Unit x86	110
5.2	Opening the BS2000 console and dialog window	112
	Messages on the BS2000 console	112
5.3	SVP console on Server Unit /390	114
5.4	Working in Native BS2000 mode	115
5.4.1	Starting (IPL) and shutting down a BS2000 system, executing an IPL dump and migrating	115
5.4.2	Setting the options (only SU x86)	116
5.4.3	Evaluating KVP logging	117
5.5	Working in VM2000 mode	118
5.5.1	VM administration	118
5.5.2	Managing VM resources	119
5.5.3	Setting VM options	121
5.5.4	Operating a VM	122
5.5.4.1	Start and shut down a BS2000 guest system, create a dump / enable and disable (and delete) a BS2000 VM, migrate	123
5.5.4.2	Managing devices of the VM	125

5.6	Working in XenVM mode (on Server Unit x86)	130
5.6.1	VM administration	130
5.6.2	Managing VM resources	133
5.6.3	Tracking VM installation	134
5.6.4	Setting VM options	136
5.6.4.1	Defining the remaining runtime for shutdown	136
5.6.4.2	Setting VM-specific options (auto start and delay)	137
5.6.5	Operating a VM	138
5.6.5.1	Displaying VM information	138
5.6.5.2	Opening the console of the XenVM	138
5.6.5.3	Starting and shutting down the XenVM	139
5.6.5.4	Changing the configuration of the XenVM	140
5.6.5.5	Managing devices of the XenVM	141
6	Operating and managing systems on Application Units	147
<hr/>		
6.1	Operating a Native system	147
6.2	Operating virtual machines	149
6.3	Installing an operating system on an Application Unit	151
7	Managing applications	155
<hr/>		
7.1	SE management applications	157
7.1.1	BS2000 Backup Monitor	157
7.1.2	openUTM WebAdmin	159
7.1.3	ROBAR	159
7.2	Managing user-defined management applications	161
7.3	Administering user-defined links	162
8	Monitoring performance	163
<hr/>		

9	Managing devices	165
9.1	Managing BS2000 devices	166
9.1.1	Device addresses	166
9.1.2	Device management on Server Unit /390	168
9.1.2.1	Predefined BS2000 devices	168
9.1.2.2	Device connection via Management Unit and HNC	169
9.1.2.3	Configuration in IORSF files	170
9.1.3	Device management on Server Unit x86	171
9.1.3.1	Predefined BS2000 devices	171
9.1.3.2	Connection of peripheral devices	171
9.1.4	Managing disks	173
9.1.4.1	Displaying generated disks on Server Unit /390	173
9.1.4.2	Managing disks on Server Unit x86	174
9.1.5	Managing KVP devices	176
9.1.6	Managing LAN devices	179
9.1.7	Managing tape devices	181
9.1.7.1	Emulated tape devices	183
9.1.7.2	Emulated tape devices from the BS2000 viewpoint	185
9.2	Managing XenVM devices on Server Unit x86	188
9.2.1	Managing disk pools	188
9.2.2	Managing virtual disks	191
9.2.3	Managing virtual switches	193
9.2.4	Managing installation sources	195
10	Managing hardware	197
10.1	Managing units of the SE server	198
10.1.1	Powering a unit on or off, rebooting a unit	198
10.1.2	Managing the SE servers of the Management Cluster	200
10.1.3	Managing the Server Unit /390	201
10.1.3.1	Displaying system information and interfaces of the SU /390	201
10.1.3.2	Displaying the IP configuration of the SU /390	203
10.1.4	Managing the Management Unit	204
10.1.4.1	Displaying system information and interfaces of a Management Unit	204
10.1.4.2	Managing the IP configuration	208
10.1.4.3	Managing routing of the Management Unit	210
10.1.4.4	Managing the DNS configuration	211
10.1.4.5	Managing SNMP	212
10.1.4.6	Setting the system time (time synchronization or local)	214
10.1.4.7	Entering CLI commands	216
10.1.4.8	Managing updates of the Management Unit	217

10.1.4.9	Managing configuration data (CSR) of the MU	220
10.1.4.10	Generating diagnostic data	222
10.1.4.11	Managing service access	223
10.1.5	Managing the HNC	227
10.1.5.1	Displaying system information and interfaces of the HNC	227
10.1.5.2	Managing the IP configuration of the HNC	230
10.1.5.3	Managing routing of the HNC	231
10.1.5.4	Displaying the DNS configuration of the HNC	232
10.1.5.5	Configuring Net-Storage on the HNC	232
10.1.5.6	Managing updates	235
10.1.5.7	Managing configuration data (CSR) of the HNC	235
10.1.5.8	Generating diagnostic data	236
10.1.6	Managing Server Unit x86	237
10.1.6.1	Displaying system information and interfaces of the unit	237
10.1.6.2	Managing the IP configuration of the SU x86	240
10.1.6.3	Managing routing of the SU x86	240
10.1.6.4	Displaying the DNS configuration of the SU x86	241
10.1.6.5	Configuring Net-Storage on the SU x86	241
10.1.6.6	Managing updates of the SU x86	244
10.1.6.7	Managing configuration data (CSR) of the SU x86	244
10.1.6.8	Generating diagnostic data	245
10.1.7	Managing Application Units	246
10.1.7.1	Configuring an Application Unit	246
10.1.7.2	Displaying hardware information of the Application Unit	248
10.1.7.3	Managing the IP configuration of the Application Unit	250
10.2	Managing IP networks	252
10.2.1	Displaying information on networks and switches	252
10.2.1.1	Overview of IP networks	253
10.2.1.2	Configuring SENET	254
10.2.1.3	Information on switches	256
10.2.1.4	Graphical display of the internal IP network topology	257
10.2.1.5	Overview of the performance and utilization of the Net Unit ports	258
10.2.2	Managing a Data Network Public	259
10.2.2.1	Configuring the ACL settings of the DANPU network	261
10.2.2.2	Information on the performance and utilization of the DANPU ports	263
10.2.3	Managing a Data Network Private	265
10.2.3.1	Add network	267
10.2.3.2	Activate RADVD / DNS / NTP server	267
10.2.3.3	Managing members of a DANPR network	268
10.2.3.4	Configuring the ACL settings of the DANPR network	268
10.2.3.5	Information on the performance and utilization of the DANPR ports	268

10.2.4	Managing a Management Network Public	269
10.2.4.1	Configuring the ACL settings of the MANPU network	271
10.2.4.2	Information on the performance and utilization of the MANPU ports	271
10.2.5	Managing a Management Network Private	272
10.2.5.1	Overview over the status of all private management networks	272
10.2.5.2	Information on the performance and utilization of the ports of the private management networks	275
10.2.5.3	Managing members of optional MONPR networks	275
10.2.5.4	Configuring ACL settings of optional MONPR networks	276
10.3	Managing FC networks	277
10.3.1	Overview of FC networks	277
10.3.2	Configuring settings	278
10.3.3	Displaying messages	279
10.3.4	Displaying connections	279
10.4	Managing storage systems	281
10.4.1	Overview of the storage systems of the SE server configuration	281
10.4.2	Overview over the storage systems of an MU	283
10.4.3	Storage Manager	284
10.5	HW inventory	285
10.5.1	Rack view	285
10.5.2	Displaying units	286
10.5.3	Displaying components	288
10.5.4	Administration	289
10.6	Managing energy settings	290
10.6.1	Monitoring energy consumption of the units of the SE server	290
10.6.2	Simulating energy saving scenarios for the SE server	292
10.6.3	Scheduled power on/off of units of the SE server	293
11	Managing a cluster	295
11.1	Overview	295
11.2	Status of the Management Cluster	296
11.3	Managing an SU Cluster	297

12	Managing authorizations	299
12.1	Users	299
12.1.1	Managing accounts	300
12.1.2	Managing passwords	303
12.1.3	Managing individual rights	306
12.1.4	Displaying sessions	308
12.2	Configuration	309
12.2.1	Access to an LDAP server	309
12.2.2	IP-based access restriction to the MUs	311
12.3	Certificates	313
12.3.1	SSL certificate	313
12.3.1.1	Confirming/importing a certificate in the web browser	314
12.3.2	Managing certificates	316
12.3.2.1	Using the standard certificate	317
12.3.2.2	Creating and enabling a new self-signed SSL certificate	319
12.3.2.3	Requesting an SSL certificate	319
12.3.2.4	Uploading and activating a customer-specific certificate	321
13	Managing logging functions	323
13.1	Displaying audit logging	323
13.2	Displaying event logging	325
13.3	Alarm management	327
14	Appendix	331
14.1	Operating BS2000 with PuTTY	331
14.1.1	BS2000 console on MU or SU /390	332
14.1.2	BS2000 dialog on MU or SU /390	337
14.1.3	SVP console on MU or SU /390	340
14.1.4	BS2000 console on SU x86	343
14.1.5	BS2000 dialog on SU x86	348
14.1.6	Information on the user strategy	351
14.2	Working with EMDS	352
14.2.1	Using shortcuts for special characters	352
14.2.2	Using programmable keys (pfkeys)	352

Glossary 355

Related publications 361

Index 365

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:

- Server Unit /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
- Centralized system monitoring of all components
- End-to-end redundancy concept
- 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.

It is possible to combine two SE servers in a management cluster to a management entity and therefore utilize the advantages of the SE Manager for two SE servers at the same time. Every Management Unit can be used to control all components of the cluster, thus enhancing protection against failure. Within an SU Cluster, a live migration can be performed to migrate BS2000 systems without interruption.

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, 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 [1]
 - Server Unit /390 (SE700 / SE500) [2]
 - Server Unit x86 (SE700 / SE500 / SE300) [3]
 - Additive Components (SE700 / SE500 / SE300) [4]
- Operation and Administration [5]
- Quick Guide [6]
- Security Manual [7]
- Cluster Solutions for SE Servers (Whitepaper) [8]

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 V6.2A.

Information on the hardware lifecycle of the FUJITSU Server BS2000 SE Series

With the hardware lifecycle of the SE series, the hardware basis for the Server Unit x86, the Management Unit and the HNC has been renewed. These new generation versions are called SU300 M2, MU M2 and HNC M2. They are supported from basic software V6.2A onwards.

The FUJITSU BS2000 servers of the SE series that are equipped with this hardware generation are called SE300B, SE500B and SE700B.

Functional extensions

The basic software M2000/X2000/HNC V6.2A provides the following functional extensions:

- **MU redundancy**
An SE server may contain two MUs, which are equally ranking in management and operation:
Actions can be executed from each MU.
The add-ons on both MUs are integrated into the SE Manager as links and can therefore be called from each MU.
If the SE Manager is called via DNS, the session is global for all MUs. You can switch from one MU to another without having to log in again. An add-on can be called without having to log in again even if it is installed on the other MU.
- **Support of clusters**
If an SE server configuration consists of two SE servers, the SE servers are managed together in a shared Management Cluster.
Two SUs of the same type (SU /390 or SU x86) can be combined into one SU cluster. SU clusters enable the Live Migration (LM) function for migrating BS2000 systems from one SU to another.
- **Support of LDAP accounts**
LDAP accounts can be used for all user roles. The SE Manager enables the LDAP configuration, which is the prerequisite to use LDAP accounts.
- **Audit logging**
The administrator is able to track changes to objects or to the configuration of the SE server, including the user, time and action involved. The system logs all actions performed in the SE Manager or via the CLI.




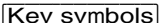


- Event logging
Events in the SE server configuration are logged with a weighting. The logging includes events triggered by the StorMan add-on.
- Alarm management
The administrator can configure the automatic messaging (via SNMP trap or E-Mail) that is triggered for events from a certain weighting.
- For BS2000 devices, the number of free licenses is displayed.
- For SU /390, an emergency system is provided. For this purpose, two emulated disks are provided on the MU.
- For AU PQ with Oracle VM Server, the SE Manager enables direct access to the Oracle VM console.

As of Service Pack 1 of the basic software M2000 / X2000 / HNC V6.2A, the following changes result:

- Additional AU models are supported:
 - the PRIMERGY-based AU25 M4
 - the PRIMEQUEST-based AUQ38E and DBU38E
- With regard to the hardware basis, AUs are generally distinguished by AU PY (PRIMERGY-based) and AU PQ (PRIMEQUEST-based).
- For SU / 390 the dialog box *Initiate IMPL / Change BS2000 operation mode* is now available in the *BS2000 operating mode* tab in the *Actions* group. The dialog permits you to initiate the IMPL and optionally to change the operation mode. After the execution of the IMPL, a BS2000 IPL is always initiated.
- For SU / 390, the *BS2000 operation mode* tab and the VM menus *Disks*, *KVP*, *LAN* and *Tape devices* now also provide links for managing the IORSF files in the *Devices* menu.
- For *Audit Logging* and *Event Logging* in the main menu *Logging*, a new calendar function facilitates the entry of date and time, if the time period for the displayed entries should be changed.

1.5 Notational conventions

The following notational conventions are used in this manual:

	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.
<i>italics</i>	Texts from the SE Manager (e.g. menu name, tab)
monospace	System inputs and outputs
monospaced semi bold	Statements which are entered via the keyboard are displayed in this font.
<abc>	Variables which are replaced by values.
	Keys are displayed as they appear on the keyboard. When uppercase letters need to be entered, the Shift key is specified, e.g.  -  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:
 - **SE700** for FUJITSU Server BS2000 SE700 / SE700B (with SU700, more than one SU300 and AU optional)
 - **SE500** for FUJITSU Server BS2000 SE500 / SE500B (with SU500, more than one SU300 and AU optional)
 - **SE300** for FUJITSU Server BS2000 SE300 / SE300B (with SU300, more than one SU300 and AU optional)
- **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)

Based on the different models, a distinction is made between the following SUs:

- **SU700** for the Server Unit of the unit type SU /390 in SE700 and SE700B
 - **SU500** for the Server Unit of the unit type SU /390 in SE500 and SE500B
 - **SU300** for the Server Unit of the unit type SU x86 in SE300, optionally in SE500 / SE700 or SE500B / SE700B
- **MU** for the Management Unit. The MU enables centralized, user-friendly and cross-system management on the SE server.
 - **AU** for the Application Unit (with x86-based hardware)
A distinction is made between AUs depending on the hardware base:
 - Application Unit PY for a PRIMERGY-based AU (e.g. hardware model AU25 or AU47).
 - Application Unit PQ for a PRIMEQUEST-based AU (e.g. hardware model AU87 or DBU87).
 - **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 operation of the SE server with a single Management Unit is called a "single-MU configuration". The Management Unit can be redundant in design. An SE server configuration with more than one Management Unit (MU redundancy on the SE server or Management Cluster with two SE servers) is called "multi-MU configuration". MU redundancy ensures that the components of the SE server can still be operated if one MU fails. In particular this means that the SKP functionality is then still available for operating an SU /390.
- Server Unit (SU)
 - 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 Unit (AU)
Multiple AUs can be operated on the SE server. An AU enables operation of applications under Linux, Windows or hypervisor-based systems. A distinction is made between AUs depending on the hardware base:
 - Application Unit PY refers to all PRIMERGY-based AUs (e.g. hardware model AU25 or AU47).
 - Application Unit PQ refers to all PRIMEQUEST-based AU (e.g. hardware model AU87 or DBU87).

- Net Unit (NU)

The Net Unit offers maximum performance and security for internal communication in an SE server and for a connection to customer networks (IP networks). For an SU /390, HNC is an additional component of the Net Unit.

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 or multiple racks. 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 285](#)).

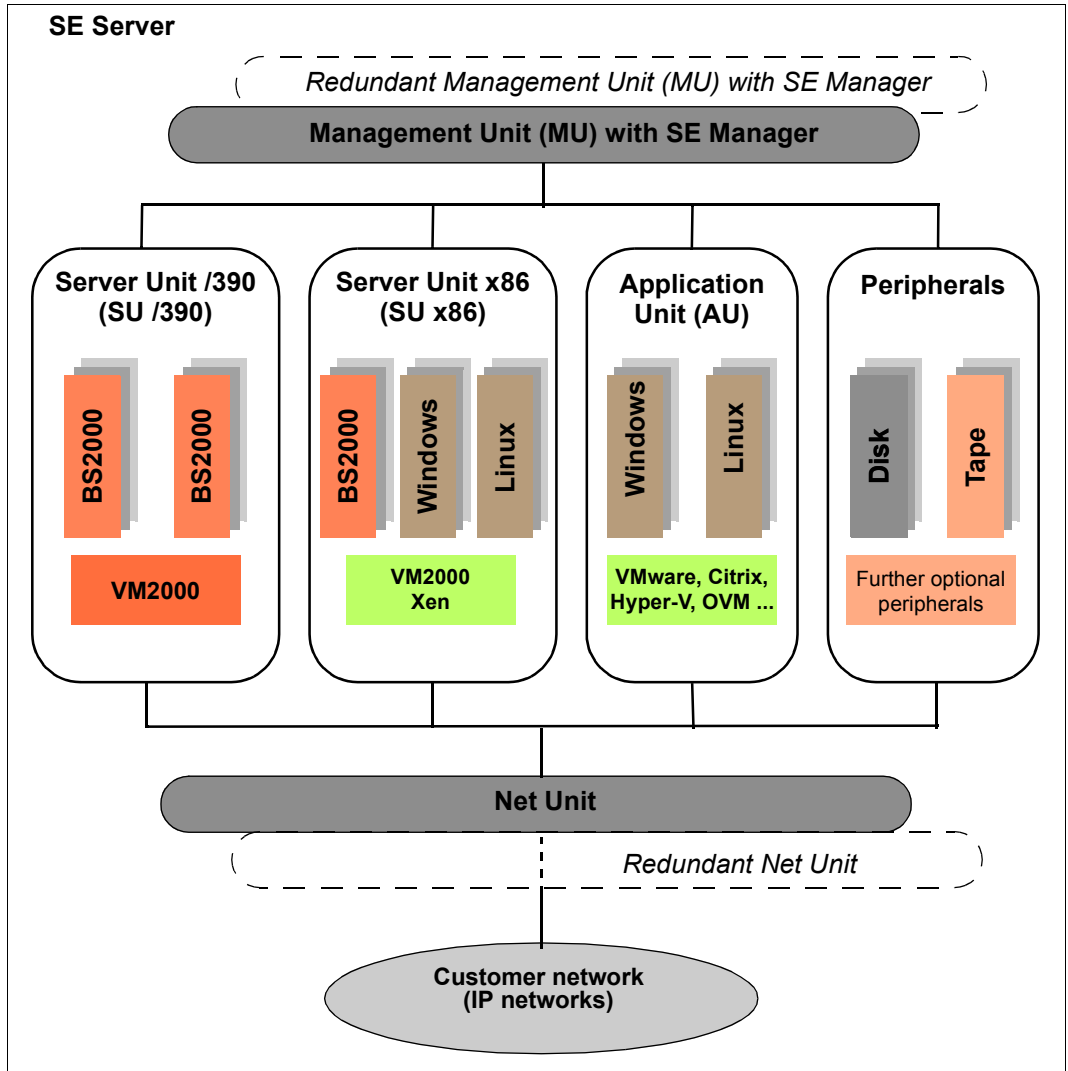


Figure 1: Architecture of SE servers

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 (central operation and administration of the SE servers)
 - Operation and administration of the BS2000 systems on SU /390 and SU x86 (BS2000 console, BS2000 dialog, SVP console on SU /390)
 - Operation and administration of the XenVMs on SU x86
 - Operation and administration of VMs on AUs
 - Realizes the data collection and storage necessary for managing and operating the SE server.
Receives events from all instances of the SE server for displaying, editing and forwarding.
In the case of a multi-MU configuration, these internal functions are coordinated between the MUs.
- Role and user strategy
- Net Unit functions for integration of the SE server into the network world
- SE Desktop for operation on the local console of the Management Unit
- Integration into the Remote Service

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, the 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 or openSM2. See also [section “Add-on pack” on page 27](#).

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 201](#)), but in this case does not support update management.

The software status consequently has the following components:

Component	Example	Description
Version	6.2A	
Revision	REV=0100	Update status
Security fix	6.2A, No.001	<ul style="list-style-type: none"> – Security fixes are assigned to a version and update status. – Security fixes have a sequence number for each version status and each update status (001 in the example)
Hot fix	6.2A, REV=0100, A0603507-H03	<ul style="list-style-type: none"> – Hot fixes are assigned to a version and update status – 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
- 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. MV6.2A.SF.001.iso[.gz] The security fix with the number 001 is assigned to the version and update status 6.2A.
Hot fix	e.g. MV6.2A0100.A0603507-H03.iso[.gz] The hot fix with the name A0603507-H03 is assigned to the version and update status 6.2A REV=0100.
Add-on pack	e.g. MV.STORMAN-7.0.0-12.4.iso This add-on pack contains StorMan V7.0

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. 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 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.

2.2.3.4 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:

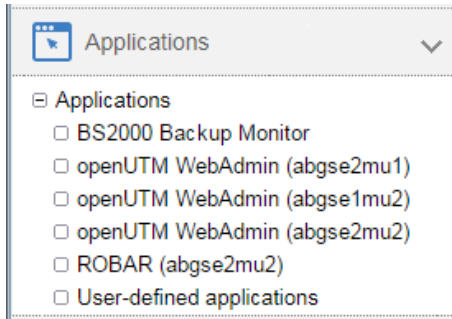
Add-on (product name)	Chargeable	Preinstalled ex works	Integration into the SE Manager
OPENSM2 (openSM2 Performance Monitor)	Yes	Optional	Category: Monitoring → <i>Performance</i>
OPENUTM (openUTM Server Administration)	Yes	No	Category: Application → <i>Applications</i> → <i>SE management application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

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

If there is more than one MU (MU redundancy or Management Cluster):

- Every add-on pack can be installed on any MU or on all MUs.
The recommended use and configuration for multi-installation can be found in the documentation for the add-on.
- All installed add-on packs are integrated into the SE Manager with an MU-specific link.

Example



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 27](#)).

The following SE management applications are currently available:

- BS2000 Backup Monitor
The BS2000 Backup Monitor is a permanent part of the SE Manager.
- Storage Manager
StorMan is implemented as a preinstalled add-on pack.
- openSM2
openSM2 is implemented as an optional add-on pack.
- 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 161](#).



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 162](#).

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 provides a graphical display of the network topology with all the network components and connections of the SE server in the *Topology* tab of the *Hardware → IP networks* menu. See [section “Graphical display of the internal IP network topology” on page 257](#).

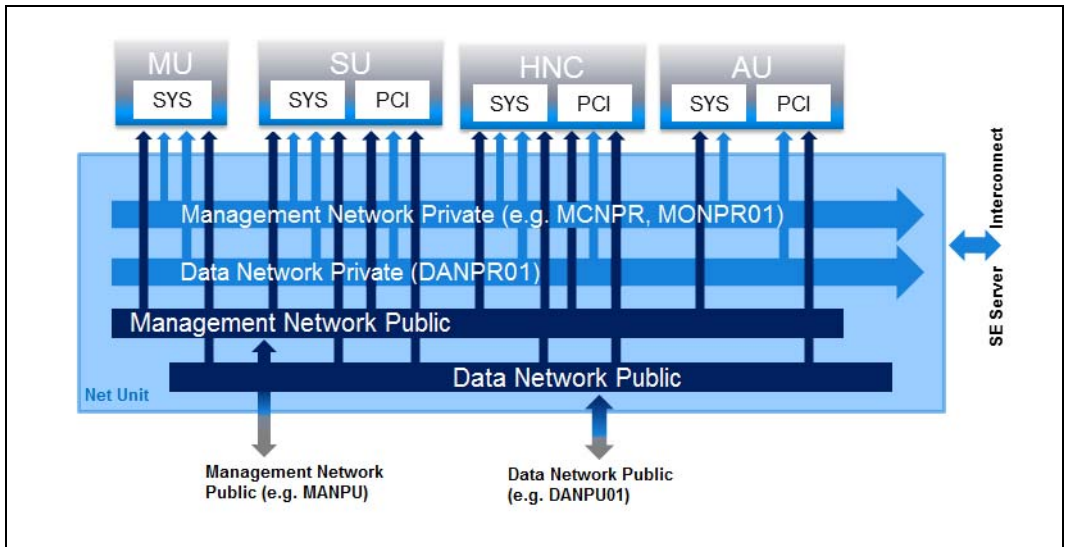


Figure 2: Block diagram of the Net Unit

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 208](#)).

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 254](#)).

The management of the "senet" domain is global. Changes to SE server configurations with more than one MU are automatically aligned in the DNS.

The aliases are assigned according to the following schema:

Component	MCNPR SE alias (x=1..n; y=1..8; z=01..99)	Description
MU	mu<x>-se<y>.senet	M2000
SU /390	su0bs2-se<y>.senet su0vm<z>-se<y>.senet	BS2000 (Native/monitor VM) BS2000 VMs
SU x86	su<x>-se<y>.senet su<x>irmc-se<y>.senet su<x>bs2-se<y>.senet su<x>vm<z>-se<y>.senet	X2000 SU x86 iRMC BS2000 (Native/monitor VM) BS2000 VMs
Managed Switch	nswa<x>-se<y>.senet nswb<x>-se<y>.senet	nswa = 1 Gbit nswb = 10 Gbit
HNC	hnc<x>-se<y>.senet hnc<x>irmc-se<y>.senet	HNC HNC iRMC
AU PY	au<z>-se<y>.senet	System (e.g. VMware)
AU PQ	auc<z>-se<y>.senet auc<z>p<nr>se<y>.senet	Management Board of a PRIMEQUEST 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

Table 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.



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 SU x86 and HNC are configured in such a manner that time synchronization takes place from the local SE server's MU.

In the case of MU redundancy, both MUs of the local SE server are configured as timers.

If external timers are used in a multi-MU configuration, the same external NTP servers must be configured on each MU, so that the time remains accurate even if one MU is switched off.

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

For further details, see [section "Time synchronization" on page 65](#).

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 [13].
- The REWAS subsystem must be active (default).

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 179](#)) 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* → [*<se server>(SE<model>)* →] *<unit> (SU<model>)* → *BS2000 devices on the LAN* tab.



All PCI ports can be used for the ZASLAN connections.

The following must be observed on the SU x86: LAN interfaces cannot be used simultaneously for ZASLAN and virtual switches of XenVMs (see [section “Integration of the XenVM guest systems into the LAN \(only SU x86\)” on page 39](#)).

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 (in case of SU /390) is automatically assigned the addresses 192.168.139.x. If address conflicts occur, the 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 or 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



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.



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 vSwitches:

- **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 *Devices* → [*<se server>(SE<model>)* →] *<unit> (SU<x86>)* → *XenVM devices* on the *Virtual switches* tab. New virtual switches can be created there and unused switches can be deleted.



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](#).

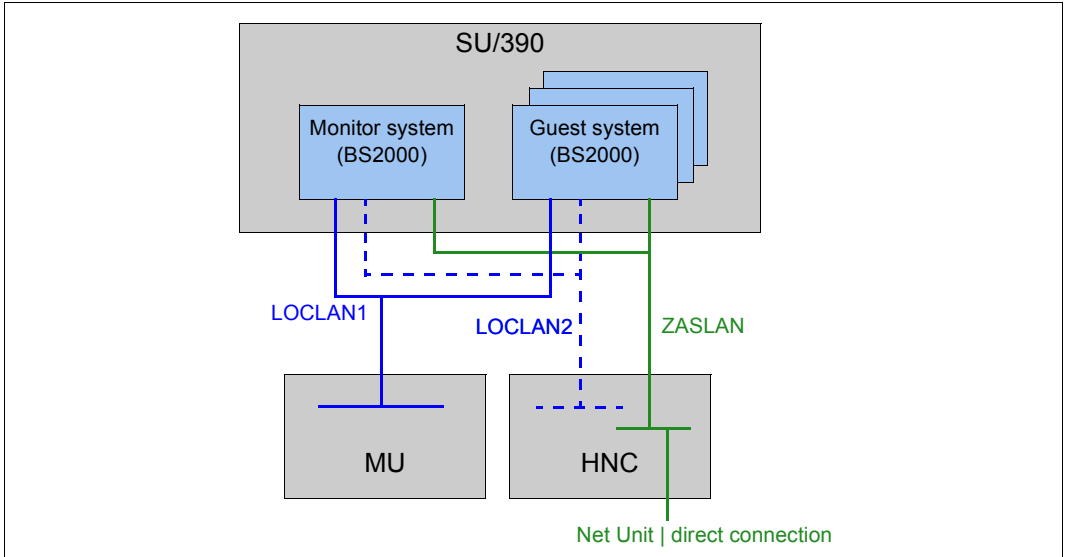


Figure 3: Overview of possible internal and external LAN connections (Server Unit /390)

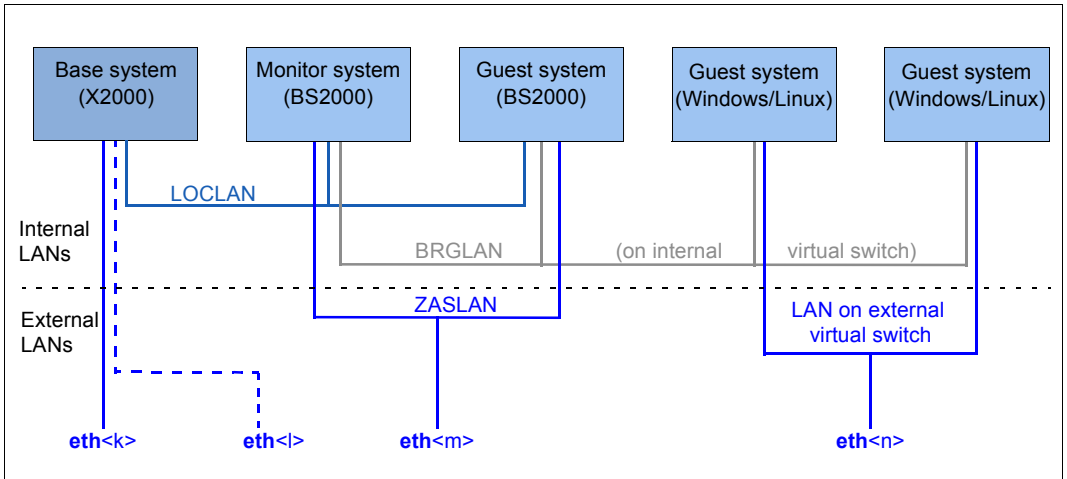


Figure 4: Overview of possible internal and external LAN connections (Server Unit x86)

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 External configuration disks

On a configuration disk of a unit (MU, SU x86, HNC), the following data of the SE server configuration are stored:

- General data of the SE server:
 - Model, name and location
 - Cross-unit data
- Unit-specific data with contents that should remain available even after the Unit fails or is powered off (not for HNC):
 - Model, SW version and host name
 - IP configuration
 - FC configuration
 - VM data for BS2000 (on SU x86 also for Linux and Windows)
- Current configuration of the Net Unit switches

By default, the data are locally stored on an internally mirrored disk of the Unit (MU, SU x86, HNC).

In addition to the internal configuration disk, up to two external configuration disks can be configured on external FC RAID systems, to which all MUs and SU x86 have access via a redundant connection.

This ensures consistency: Every MU and SU x86 reads the data of the SE server in the same way and the actions on these units can be coordinated.

The SE Manager displays information about the configuration disks, e.g. of an MU, in the *Hardware* → *Units* [→ <se server> (SE<model>)] → <unit> (MU) → *Information* menu (see [“Displaying configuration disks of the MU” on page 207](#)):

System | IP interfaces | FC interfaces | Multipath disks | **Configuration disks**

Index	Device	Status	Description
1	raid0d4	✓ NORMAL	intern
2	601225-Disk1183	✓ NORMAL	SE_CRD_OS7_SE1
3	601225-Disk1184	✓ NORMAL	SE_CRD_OS7_SE2

Total: 3

Figure 5: MU with external configuration disks

External configuration disks are required in the following cases:

- MU redundancy
 - On SE700/SE500, external configuration disks are mandatory.
 - On SE300, using them is recommended to avoid restrictions when working with the SE Manager (see below).
- Cluster
 - For the SE Cluster (Management Cluster), external configuration disks are sufficient on the MUs. For SU Clusters, external configuration disks are also required on SU x86.

MU redundancy for SE300 – Restrictions for operation without external configuration disks

In case the customer is unable to provide external configuration disks, working with the SE Manager is still possible but subject to certain restrictions:

- Session management
 - Customer Support has to specify the SEM setting "Working with MU-local sessions" on both MUs.
 - As soon as a function is called on the other MU (upload/download dialog for the other MU, link in the header), the user is redirected to the corresponding main window of that MU. You have to log in on that MU.
- Management of global, i.e. cross-MU, data
 - In this case, these kinds of data only seem to be global. They are actually local data that have to be managed separately on each MU:
 - Accounts, LDAP, IP based access rights
 - Applications and Application Units
- The data collection is not coordinated between the two MUs and therefore a different status of the data may be displayed on each MU.

2.5 Cluster

Two types of clusters are possible in an SE server configuration.

2.5.1 Management Cluster

If two SE servers are combined into one Management Unit, it is called a "Management Cluster" (or "SE Cluster").

A Management Cluster is configured by Customer Support based on the customer's wishes and is used to operate and administrate the two SE servers together.

A Net Unit connection between the two SE servers (ISL-E) and one or two external configuration disks for managing the global data are required to establish a Management Cluster.

See also [section "External configuration disks" on page 42](#).

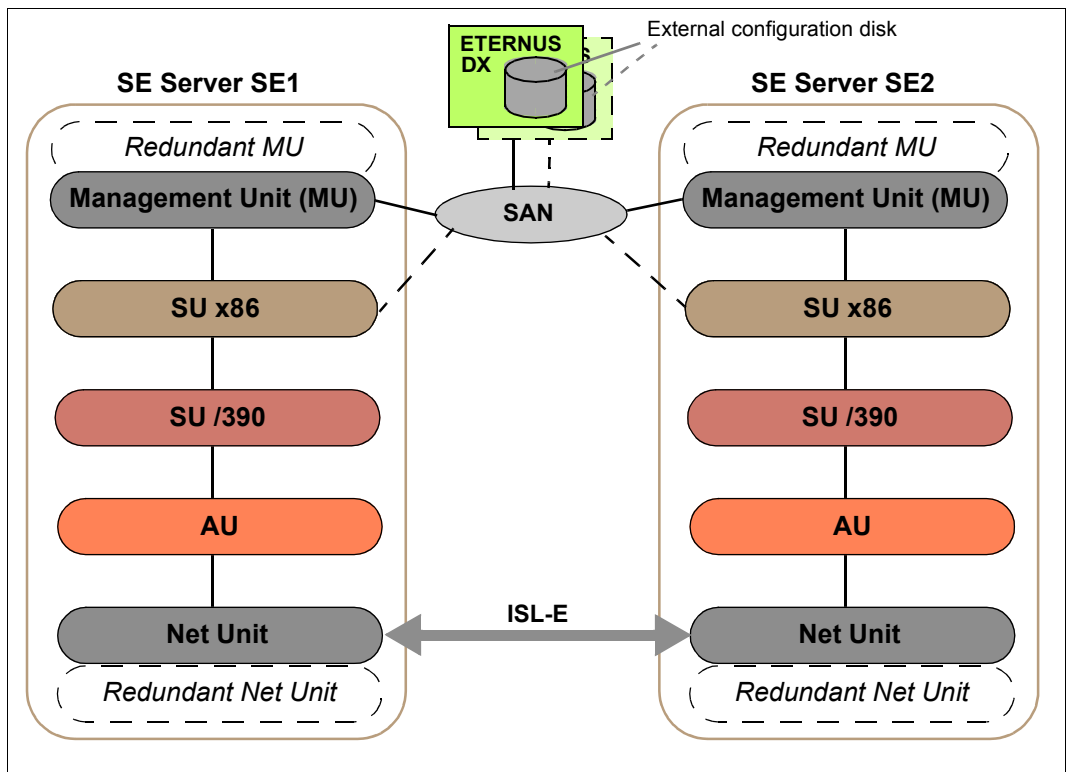


Figure 6: Management Cluster with two SE servers

Regarding administration and operation, all MUs of the Management Cluster are equally ranking. This means you can centrally administer and operate all objects of the whole SE server configuration (in this case: two SE servers) from one MU.

The SE servers can be operated as long as one MU functions. However, an MU of the local SE server is required for the SVP operation of an SU /390 and its correct HW display.

2.5.2 SU Cluster

Two Server Units of the same type (SU /390 or SU x86) can be combined into a logical unit, a so-called "SU Cluster".

An SU Cluster is configured by Customer Support based on the customer's wishes and provides the Live Migration (LM) function for the BS2000 systems of the two Server Units.

Live Migration is used to migrate a BS2000 system from the source SU to another SU (target SU) of the same type and operating mode. This means that a running system can be migrated to a target SU without interruption. A planned operational interruption, e.g. for hardware maintenance, is therefore no longer required. LM can also be used for manual load balancing, e.g. in the event of recurring high-load phases.

An SU Cluster with SU /390 is always cross-server and thus requires a Management Cluster. An SU Cluster with SU x86 may also be configured locally on one server, in case an SE server has more than one SU x86.

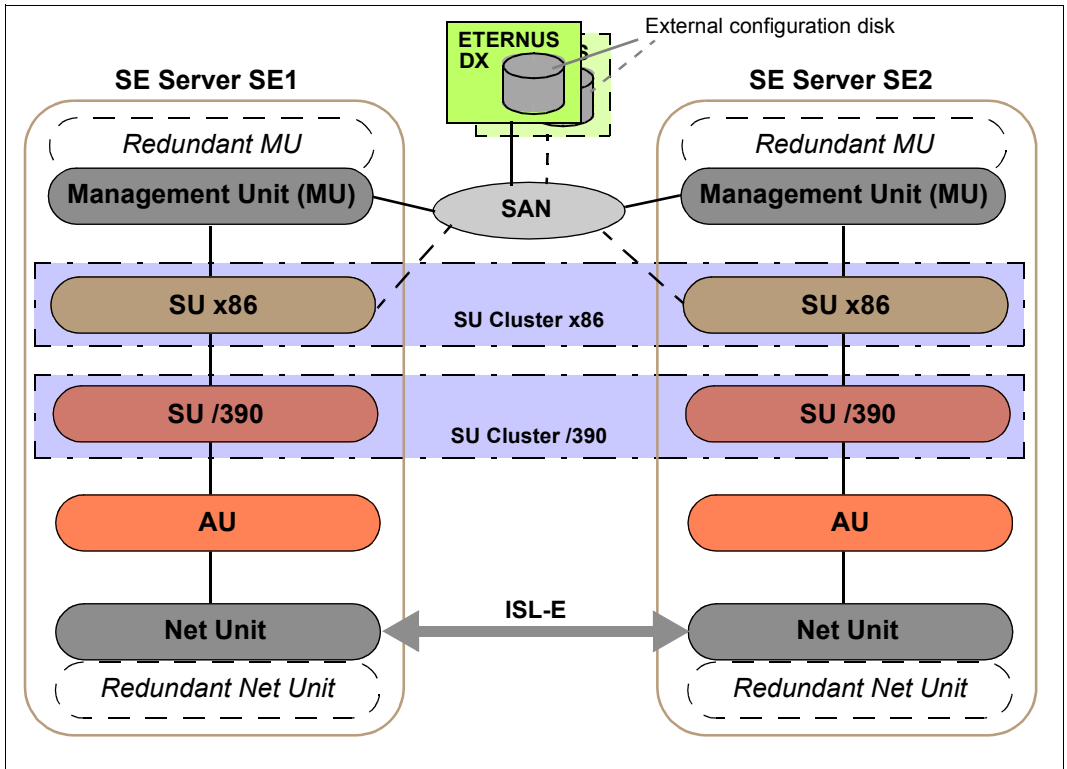


Figure 7: SU Cluster in the Management Cluster with two SE servers

The Live Migration action can be called from the "Operation" main window of the respective BS2000 system. It is only available on SUs that are part of an SU Cluster. Whether or not an LM is possible, depends on the current cluster status. The current status is displayed by the SE Manager in the *Cluster* → <cluster-name> → *SU Cluster* menu, see [section "Managing an SU Cluster" on page 297](#).

LM requires both SUs to have the same operating mode. In case of an SU /390, LM is only possible if the current operating mode is set to *VM2000 mode*.

In order to avoid unwanted fault indications and events over long periods when maintenance takes place (e.g. SU switched off or in error status), the SU Cluster can be temporarily deactivated in the *Cluster* → <cluster-name> → *SU Cluster* menu. LM is not possible in this state as well.

Details on the use of clusters are described in the Whitepaper „Cluster Solutions for SE Servers“ [8].

2.6 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.

2.6.1 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 50](#).

All roles except the *Service* role can be assigned to additional accounts, see [“Further accounts with role assignment” on page 50](#).

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.

In the SE server configuration, the administrator performs, among others, the following tasks:

- Managing all user accounts
- Managing individual authorizations
- LDAP configuration
- Managing the networks
- Monitoring audit and event logging
- The administrator can configure the automatic messaging (via SNMP trap or E-Mail) that is triggered for events with a certain weighting.
- Additional general configurations like installing add-on packs, etc.

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, they 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.

Access to the Linux shell is not possible.

AU administrator

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

All AU administrator accounts are of equal value.

Access to the Linux shell is not possible.

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. An operator 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, they 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 300](#) 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.

Accounts of the add-ons do not correspond to a role in the SE Manager and are therefore not displayed 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.



The accounts are MU-global, i.e. in SE server configurations with more than one MU, all accounts that are added, changed or removed by the administrator are implicitly added, changed or removed on all existing MUs.

An account (locally or centrally managed) must always be unique. If an account is to be added that corresponds to a pre-defined account (e.g. *admin*, *service* or account of an add-on), the SE Manager rejects the action and shows an error message.

Centrally managed accounts

In addition to local accounts, the administrator can also permit LDAP accounts for the various roles. These accounts are managed centrally on an LDAP server (in particular also the password).

In order to use LDAP accounts, the access to an LDAP server must be configured. In the Management Cluster, access to the LDAP server can be configured specifically for one SE server. See [section “Access to an LDAP server” on page 309](#).

When this requirement is satisfied, the administrator, when creating an account, can release an LDAP account by means of the account type for the desired role. If the central account is the same as the existing local account, no LDAP account can be released. When an LDAP account is removed, it is also locked again.

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 for operator accounts, see [section “Managing individual rights” on page 306](#).

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.

2.6.2 IP-based access to the Management Unit

By default, access to the MUs of the SE server is unrestricted 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 explicitly entered IP networks.

In a Management Cluster, the configuration is server-specific.

The current configuration of the access to the MUs is displayed in the *IP-based access rights* tab of the *Authorizations* → *Configuration* menu (see [section “IP-based access restriction to the MUs” on page 311](#)).

2.6.3 Redundant Management Units

Central operation and administration of the SE server is continued after an MU has failed if there is MU redundancy, i.e. if the SE server has a second MU.

Redundancy of the SKP functionality

On an SE server with SU /390, two MUs mean that the SKP functionality is also provided with redundancy. 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* → [*<se server> (SE<model>)* →] *<unit> (SU</390>)*, ["Switching active Management Unit" on page 109](#)).

The SE Manager displays the current status of the SVP network and of the MU connections in the *IP configuration* of the SU /390 (see *Hardware* → *Units*[→ *<se server> (SE<model>)*] → *<unit> (SU</390>)* → *Management*, ["Managing the IP configuration" on page 208](#)).

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 existing MUs and permits a "change" to the SE Manager of the other MU via a link. You do not need to log in again, because, in the default case, a session on the SE Manager is global. For this, the following requirements must be met:

- The MUs are registered at an external DNS domain.
- The connection to the SE Manager was made via the DNS name of the MU (entering the DNS name of the MU as address in the browser).

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.

2.6.4 Central logging

The SE server configuration provides centralized access to the "Audit" and "Event Logging" functions as well as to the alarm management.

Audit logging logs every action that is executed on a Unit (MU, SU, HNC) of the SE server configuration via the SE Manager, an add-on or a CLI command. Thus, every administrator can always see who performed which action with which result and when.

The SE Manager displays all occurring events in the event logging with a timestamp, weight, name of the reporting unit, name of the reporting component and message text. The most recent events are displayed first. To provide a better overview, the recent events that you have not yet seen are also displayed in the *Current events* tab. The Dashboard displays a summary of this overview in a separate tile.

The SE Manager displays the audit and event logging entries in the *Logging → Audit logging* and *Logging → Event logging* menu (see [“Displaying audit logging” on page 323](#) and [“Displaying event logging” on page 325](#)).

With the alarm management you can configure automatic SNMP trap or e-mail messages for events with certain weights; this enables you to recognize important events like error situations earlier and to react quickly if necessary, even in large SE server configurations.

The SE Manager displays the alarm management configuration in the *Logging → Alarm management* menu (see [“Alarm management” on page 327](#)).

2.7 Virtualization

2.7.1 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.

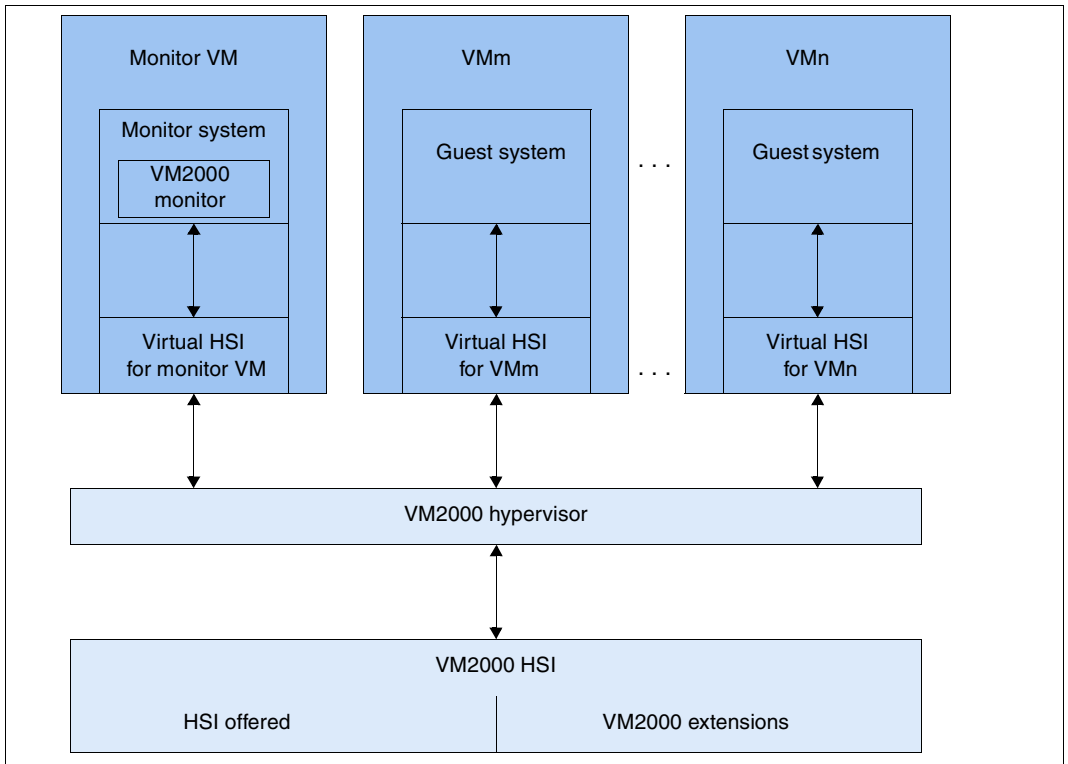


Figure 8: Structure of VM2000 on SU /390

In this case, HSI stands for "Hardware Software Interface". Further information is provided in the "VM2000" manual [12].

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.

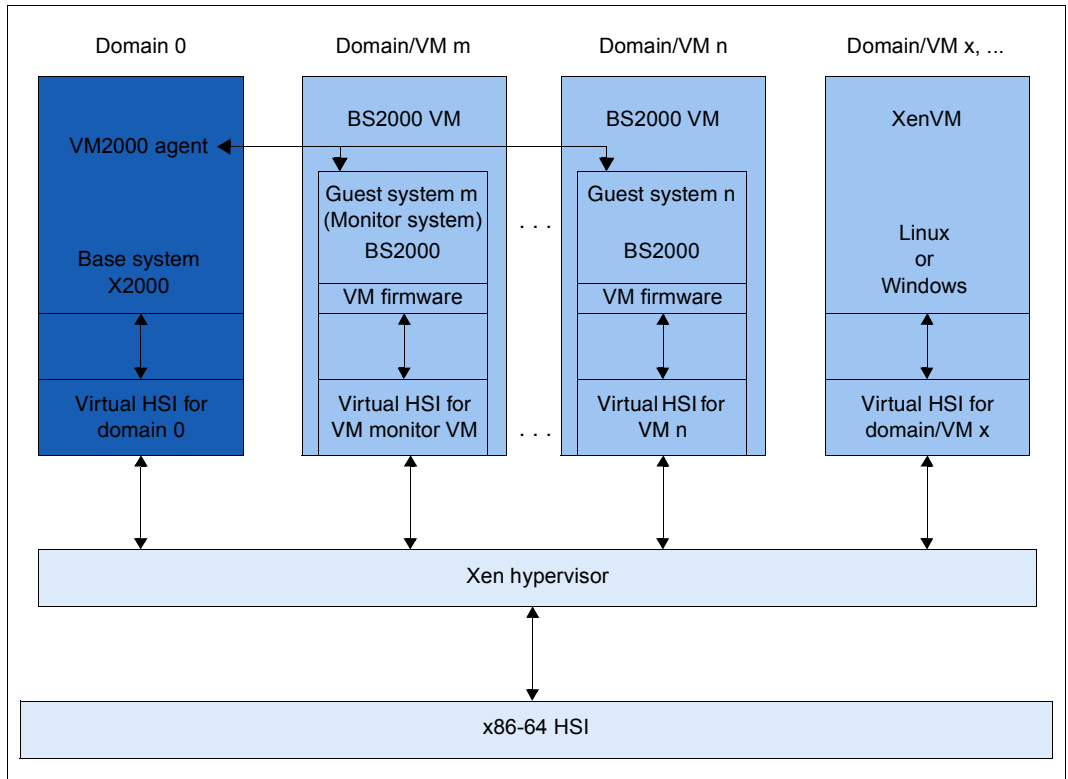


Figure 9: VM2000 on SU x86

Further information is provided in the "VM2000" manual [12].

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 [[12](#)].

2.7.2 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.

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. Additional BS2000 VMs can be created in the SE Manager or 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 generally 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.

2.7.2.1 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	Users	Name in X2000	Name in VM2000
Pool 0	X2000	Pool 0	*POOL0
Standard BS2000 pool	BS2000	bs2_pool co_bs2_pool ¹	*STDPOOL
Pool configured in VM2000	BS2000	<name 1..8> co_<name 1..8> ¹	<name 1..8>
Linux/Windows pool	XenVM	lw_pool	*FOREIGN
Free CPUs (not a pool)			

Table 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 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. Cancellation of the Linux/Windows pool

The SE Manager displays an overview over the available BS2000 CPU pools (including empty pools) and an overview over the BS2000 VMs to which a CPU pool is currently allocated under *Systems* → [*<se server>(SE<model>)* →] *<su-name> (model)* → *Virtual machines* [→ *BS2000*] → *VM resources*.

For information on BS2000 and BS2000 VMs, see also [section “Working in Native BS2000 mode” on page 115](#) and [section “Working in VM2000 mode” on page 118](#), and for information on XenVMs, see also [section “Working in XenVM mode \(on Server Unit x86\)” on page 130](#).

2.7.2.2 Main memory management

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

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 (created/activated in case of BS2000 VM) if the amount of free main memory requested is available.

2.7.2.3 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 166](#).

2.7.2.4 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.

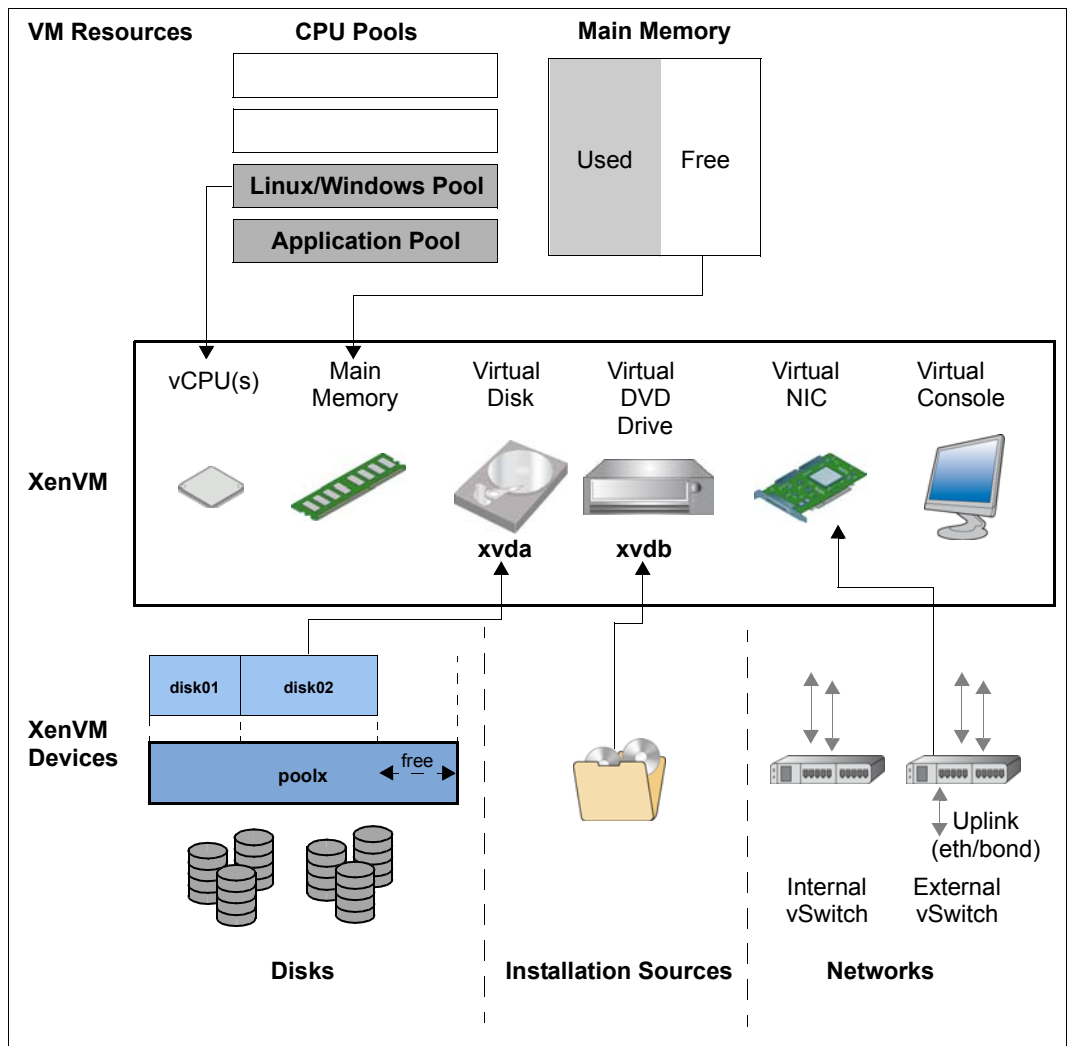


Figure 10: Configuring XenVM devices on the XenVM

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 VMDP¹ 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).

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

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.

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 9](#), 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.

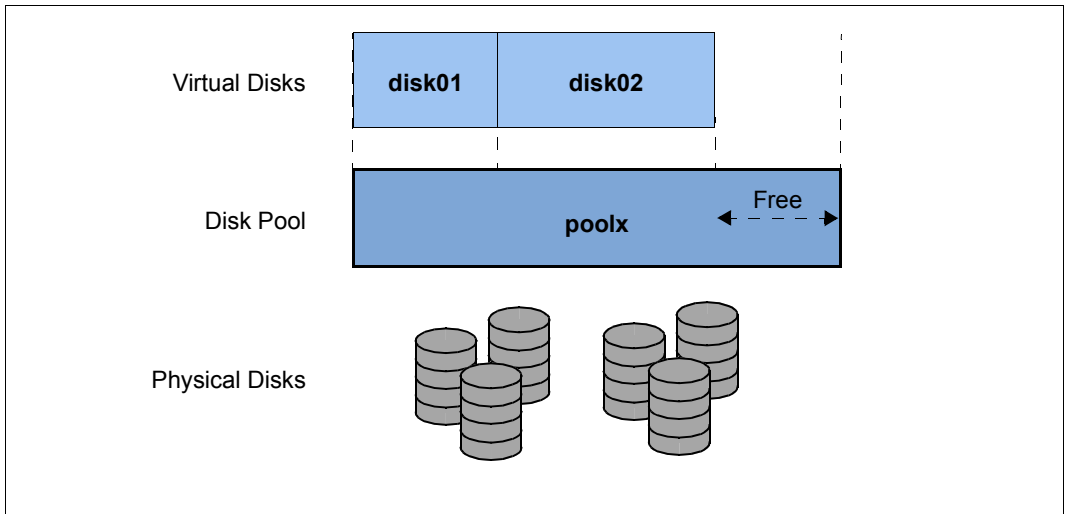


Figure 11: Virtual disks - abstraction level of disk usage

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 188](#).

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 195](#).

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.

2.8 Time synchronization

Basic state without external time synchronization

In the SE server the MU, SU x86, HNC and the optional AUs each have their own time management.

When the SE server is installed, Customer Support sets the exact time in the BIOS setup of each Unit. By default, the MU is configured as the NTP server for SU x86 and HNC via the MCNPR. By default MU and AU use the time set locally in the respective basic system. If differences occur on the MU, SU x86 or HNC, the administrator can correct the local time on the MU manually in the SE Manager.

On an AU the time is corrected with the resources of the operating system used (by default Linux).

The SVP time (on SU /390) and the Linux time of the SU x86 (on SU x86) are important as a time base for the BS2000 systems (see [“Time synchronization in BS2000” on page 67](#)). The Linux time of the SU x86 is important as timebase for operating systems running on XenVMs on SU x86 (see [“Time synchronization in XenVM systems” on page 68](#)).

Consequently, only time synchronization of the SU is examined below.

Time synchronization of an Application Unit is possible with the resources of the operating system used.

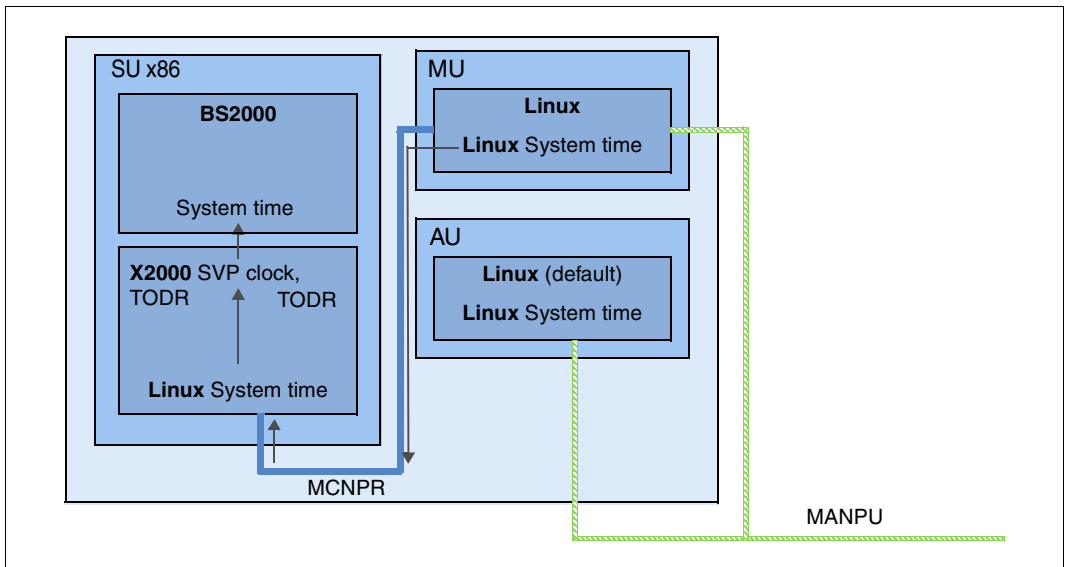


Figure 12: SE300 without external time synchronization (synchronized internally via the MU)

Time synchronization of the SU with an NTP server

If a server with a more accurate system time can be reached over the network MANPU/MONPU, the local system time can be synchronized with this server using NTP (Network Time Protocol). As soon as the administrator has entered this server as the MUs NTP server, an NTP process starts which periodically adjusts the local time to the NTP server's time:

- If at startup time a deviation of more than 0.1 seconds exists, the process sets the time absolutely precisely (accurate to the millisecond).
- In the subsequent time comparison, any time differences are adjusted relatively precisely. The local time thus remains accurate to within a few milliseconds.

This process is restarted if the NTP configuration or the accessibility of the NTP server changes (e.g. reachable again after a connection failure).

By and large it is sufficient to configure one (external) NTP server on the MU.

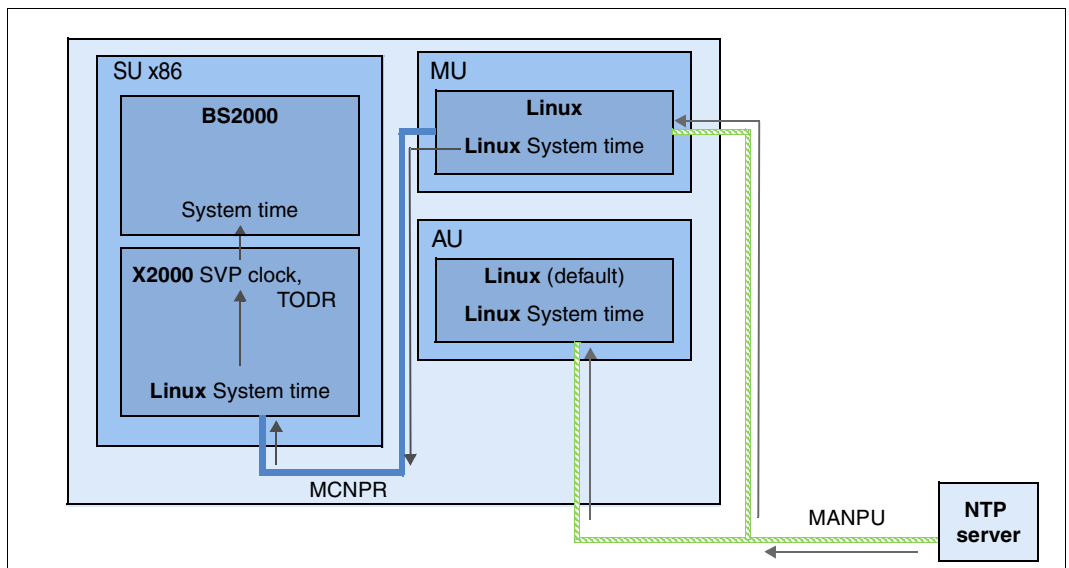


Figure 13: SE300 with external time synchronization

The SE Manager displays the current NTP configuration, see [section “Setting the system time \(time synchronization or local\)” on page 214](#). In addition to the status and the current time difference, the accuracy of the NTP server's time is also displayed. The accuracy of the NTP server's time, the NTP server quality stratum, is specified in quality levels from 1 to 15. The best NTP server quality level 1 has a radio clock.

The administrator can also enter more than one NTP server. In this case the NTP process selects a server which is currently accessible and has the most accurate time.

NTP configuration in the Management Cluster

An external time server should be configured in the MUs of the Management Cluster.

- If no external time server is configured or if it cannot be reached, the time of all units is synchronized with the local time of the MU1 of the local SE server.
- If an external time server is configured (MU1 and MU2) and can be reached, all units (HNC and SU x86) are synchronized with the MU1 of the local SE Server. If the MU1 cannot be reached, all units are synchronized with the MU2 of the local SE server.

In all units, the MUs of the local SE server and the MU1 of the first SE server are entered as NTP server.

- The IPv6 address in the network MCNPR is entered.
- The MU1 in the first SE server receives the stratum value 7.
- Every additional MU1 receives the stratum value 8.
- Every MU2 receives the stratum value 9.

Time synchronization in BS2000

On SU x86, the basic software X2000 is initially responsible for the time synchronization. X2000 emulates the clocks used on /390 architecture, namely the *Time of Day Register* TODR and the SVP clock, for BS2000, the SVP clock always supplying the current Linux time.

On SU /390, the MU communicating with the SVP of the SU /390 is responsible for the time synchronization in BS2000. The SVP clock of the SU /390 always receives the current Linux time from this MU.

BS2000 is automatically synchronized with the SVP clock, and thus with the Linux time. As the command for reading the SVP time ignores the milliseconds, the time can be inaccurate by as much as one second. If this inaccuracy is too great, an NTP connection within BS2000 can also make sense.

If the Linux time is synchronized using an NTP server, this automatically also applies for BS2000. If the NTP server has an NTP server quality with a stratum ≤ 4 and the current time difference is less than one second, BS2000 is shown that the Linux time available is as accurate as the radio clock (see *SYNCHRONIZATION* in the output of the `SHOW-SYSTEM-INFORMATION INFORMATION=*SYSTEM-TIME-PARAMETER` command).

If the Linux time is not synchronized using an NTP server, all the other synchronization instances in BS2000 (NTP or XCS) can apply.

An NTP instance in BS2000 with a stratum ≤ 4 is always higher ranking than an SVP time with a radio clock (which is equivalent to a Linux time with a stratum ≤ 4).

Repercussions of changing the system time on the Server Unit

When changes are made in the Server Unit's time management, greater or lesser leaps in time can occur in the following cases:

- When the local time is set manually (if no NTP server is configured).
- When an NTP server is entered for the first time (possibly also when modifying the NTP configuration).

In the current BS2000 session, leaps in time have the following effects:

- The modified time is forwarded to BS2000. Every 15 minutes BS2000 compares its time with the SVP clock. If a time difference is detected during synchronization, the time is adjusted over a period which is approx. 4 times as large as the time difference (i.e. an adjustment of 2 minutes takes 8 minutes). As a result, time changes on the Server Unit arrive in BS2000 with a corresponding delay.
- BS2000 accepts a time change of at most 15 minutes. If a leap in time is ≤ 15 minutes, the time adjustment is made without issuing any messages. If the leap in time is greater, the time is not adjusted. A console message indicates that from this point the BS2000 session will run only using its own time from the TODR. At intervals of 15 minutes, BS2000 repeatedly compares the times, and synchronizes them only if the time difference is less than 15 minutes.

Details on configuring the system time on the MU are provided in the [section "Setting the system time \(time synchronization or local\)" on page 214](#).

Further details on system time management in BS2000 can be found in the manual "Introduction to System Administration" [10].

Time synchronization in XenVM systems

When the XenVM is started, the operating system which is started on it takes over the current Linux time as its local time setting. In the further operations of the XenVM system the local time is independent of the time configuration of the Server Unit and can be corrected only with the current operating system's means. The time can either be set manually here or be synchronized via an NTP server. However, such settings only ever apply for the active session.

Details on configuring the system time on the MU are provided in the [section "Setting the system time \(time synchronization or local\)" on page 214](#).

Further details on system time management can be found in the documentation of the operation system used.

2.9 Customer Support and maintenance

2.9.1 Tasks of Customer Support

Customer Support has the following tasks:

- Diagnostics and debugging
- Software/hardware maintenance work
 - 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

2.9.2 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 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 your 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* [→ <se server>(SE<model>)] and open the *Units* tab.

Alternatively you can also inquire this information as follows:

- ▶ In the tree structure select *Hardware* → *Units*[→ <se server> (SE<model>)] → <unit> → *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).

2.9.3 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.

2.9.4 Handling updates

2.9.4.1 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 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 [7].

2.9.4.2 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: <ul style="list-style-type: none"> – Clarify requirements – Provide maintenance window (if necessary) – Procure security fix – Transfer security fix to system – Install security fix and, if necessary, activate it explicitly with reboot 	Inform and support the customer when required
Hot fix	<ul style="list-style-type: none"> – Provide maintenance window (if necessary) 	<ul style="list-style-type: none"> – Clarify requirements – Procure hot fix – Transfer hot fix to system (via remote service or on site) – Install hot fix (via remote service or on site)
Add-on pack	<ul style="list-style-type: none"> – Clarify requirements¹ – Procure software – Transfer software to system – Install/uninstall software 	<ul style="list-style-type: none"> – Clarify requirements¹

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(s), one of the following web browsers must be installed on your computer.

The web browsers currently supported are:

- Mozilla Firefox Version 45 (ESR) and higher
- Microsoft Internet Explorer Version 11 or higher and Microsoft Edge

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



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

3.1 Calling the SE Manager

- ▶ As address, enter the FQDN (Fully Qualified Domain Name) of an MU of the SE server into 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:

The screenshot shows a web browser window titled "SE Manager" with the Fujitsu logo in the top right corner. Below the title bar, there is a navigation bar with "Management Unit" on the left and "DE" and "Help" on the right. The main content area is a light gray background with a white login dialog box centered. The dialog box has the title "Login" and the text "System: abgse2mu1.example.net" and "Please log in with your user account and password." Below this text are two input fields: "Account" and "Password". A "Log in" button is located at the bottom of the dialog box.

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 76](#)).

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.

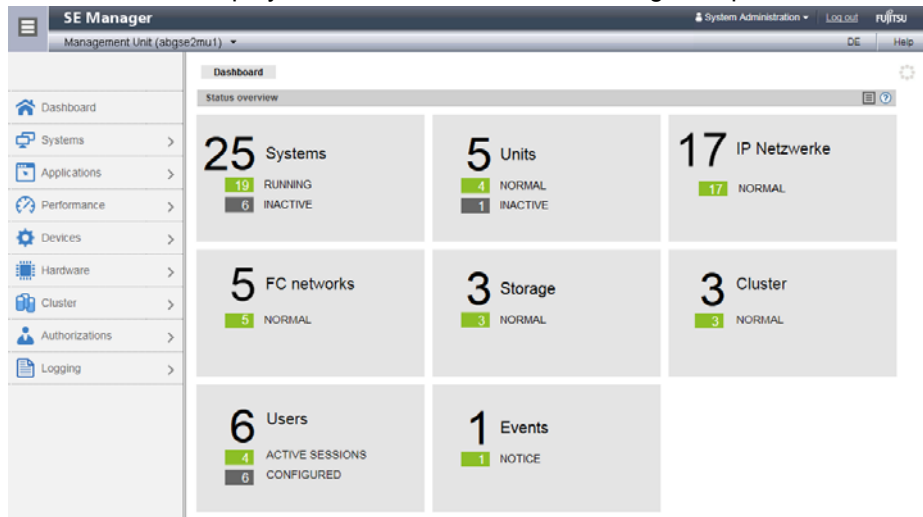


When the SE server is supplied, an initial password is set for standard account *admin*, which can be requested at the service. Change the password immediately after you have logged in for the first time (see [section “Managing passwords” on page 303](#)).

- ▶ Click *Log in*.

The *Dashboard* tab opens as the welcome page. It provides a quick overview of the systems, units/partitions, IP networks, FC networks, storage, users of the SE server and occurred events. If at least one cluster exists, the tab also contains the status of the existing clusters.

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 80](#).

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. The SE Manager displays an overview over the active sessions under *Authorization* → *Users* → *Sessions* (see [section “Displaying sessions” on page 308](#)).

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 main window opened most recently without having to log in once more.

Local and global sessions

From M2000 V6.2A onwards, SE Manager sessions are global under the following conditions:

- The MUs are integrated into an external DNS in the same network domain.
- The SE Manager is called via the DNS name of the MU (entering the FQDN) and not via the IP address.

A global session is a cross-MU session. This means that in SE server configurations with more than one MU (MU redundancy or Management Cluster), you only have to log in at the SE Manager of one MU. After that, you can switch from the SE Manager of the local MU to the SE Manager of another MU without having to log in again.

The same is true for add-on applications, i.e. you can operate the add-on applications on a different MU from the local SE Manager.

A local session is MU local. It is only created if you address an MU via the IP address during login. The name of the MU for which the session is valid, is displayed. You must log in again when you switch to another MU.

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 85](#).

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 80](#).

Main windows with automatic updates are identified by the Update icon (wheel) in the right upper corner of the main page. If there is currently an update in progress, the wheel is rotating. If there is currently no update in progress, the wheel is greyed out. If you drag the mouse cursor over the icon, the "Automatic update follows" tool tip is displayed. All main windows for which an up-to-date status display is important, support automatic updates. You can find the current list of these main windows in the online help.

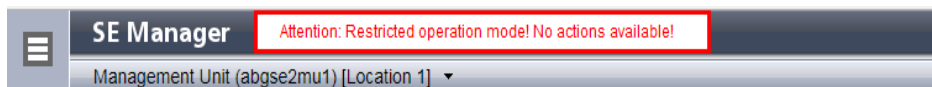
By default an update cycle of 30 seconds is available for each user. Each user can change this setting for himself/herself in the range from 10 through 120 seconds or exclude the automatic update. The setting is specified in the *Change update cycle and session timeout* dialog box (see [section "Session timeout" on page 77](#)). The individual setting is stored on an account-specific basis.

3.2.3 Restricted operating mode

There may be situations in which the SE Manager does not have full access to all resources. This may be the case if an MU is shut down or if time is needed for the reconfiguration of the clusters.

In these situations, the operating mode for the active sessions is restricted for a short period of time and no actions are possible. Access to BS2000 consoles, BS2000 dialogs and the SVP is still possible.

The SE Manager indicates the restricted operating mode in the header of the main window as follows:



In dialogs, the restricted operating mode is reported with the following message:

The functionality of the SE Manager is currently restricted! No actions possible!

As soon as the SE Manager has regained access to all resources, the restricted operating mode is terminated automatically.

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

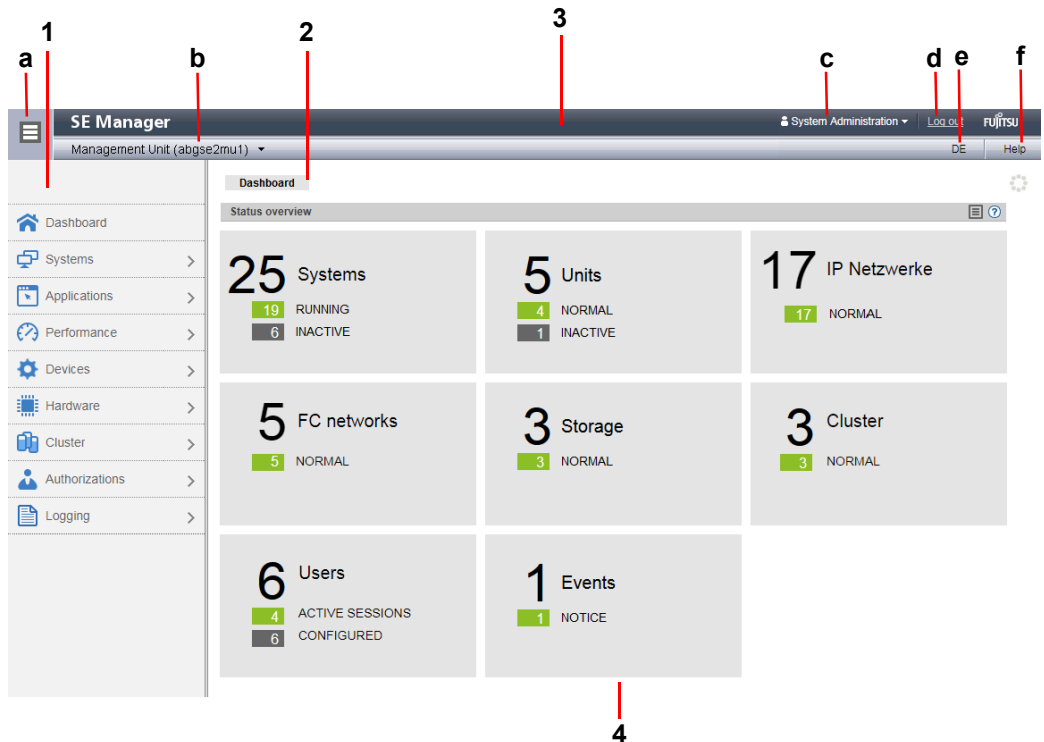
Various window types are used in the SE Manager:

- **Login window:** a window in which you log in using your account and password.
See [section “Logging in” on page 75](#).
- **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 80](#).
- **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 “Terminal window” on page 83](#).
- **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 85](#).
- **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 86](#).
- **Help window:** Window which opens in a separate tab or window of the browser when you call the online help.
See [section “Calling the online help” on page 97](#).

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.

If the main window supports automatic updates, the *Update* icon (wheel) is displayed on the right-hand edge. During an update, the wheel is rotating. Otherwise it is greyed out.

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>)* [*location*] provides information about the Management Unit via which you are currently operating the SE Manager.
<unit> is the name of the Management Unit.
If a location is configured with SYSLOCATION, <location> displays the entry. For the configuration of the local system data see [section "Managing SNMP" on page 212](#).
- c Displays the *login information*: user account or, if defined, the person-related name of the user account.
When you click the field, a selection menu with the following entries opens:
 - *Individual settings*
Opens a dialog box in which you can set the cycle of the automatic updates and the session timeout for your user account.
 - *Reset tables*
Resets all tables of the SE manager back to standard view after confirmation. Changing and resetting the table settings is always MU specific.
A tool tip for login information displays the values currently set.
- d Click *Log out* 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

The screenshot shows the SE Manager interface. The sidebar on the left contains a tree structure of navigation items. The top bar includes the 'SE Manager' title, user information, and navigation buttons. The main content area is divided into several sections: 'Update' with a status bar and a button; 'Add on packs' with a table of software packs and a table of services; and 'Security fixes' and 'Hot fixes' sections at the bottom. Red lines and numbers point to specific UI elements: 1 points to the sidebar menu; 2 points to the 'Update' tab; 3 points to the update refresh icon; 4 points to the help icon; 5a, 5b, 5c, and 5d point to expand/collapse icons in the 'Add on packs' and 'Security fixes' sections; 6 points to action icons in the 'Add on packs' table; 7 points to the 'Total: 11' text; and 8 points to the reset icon below the table.

- 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 78](#)). 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 97](#))
- 5 The information may be subdivided into groups (in the example above, 5a, 5b, 5c, 5d). If the groups can be expanded, the arrow icon in the group header indicates the current status (expanded or collapsed). If collapsed, the group header also contains the number of contained objects: *Total <n>* (see 5c and 5d in the above example). 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>*
- 8 As soon as the settings of a table (e.g. filter or sorting) have been changed, the reset icon is displayed below the table. If you click the icon, the SE Manager again displays the table with the default settings.

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:

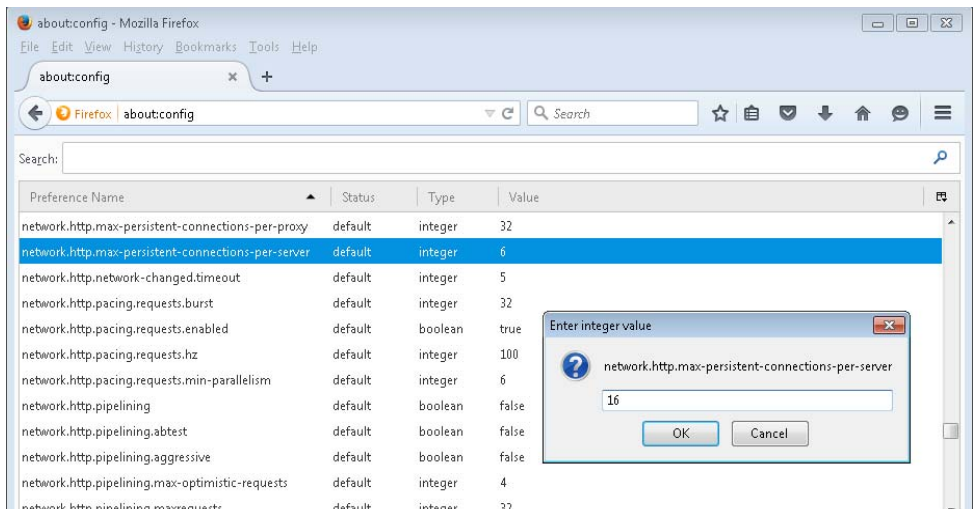
- No further login is required when the terminal window is called.
- The size of the window can be changed flexibly.
- A virtual keyboard (matching the functionality):
The virtual keyboard enables all required characters and function keys to be entered irrespective of the real keyboard's layout.
- Copy & 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.



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.



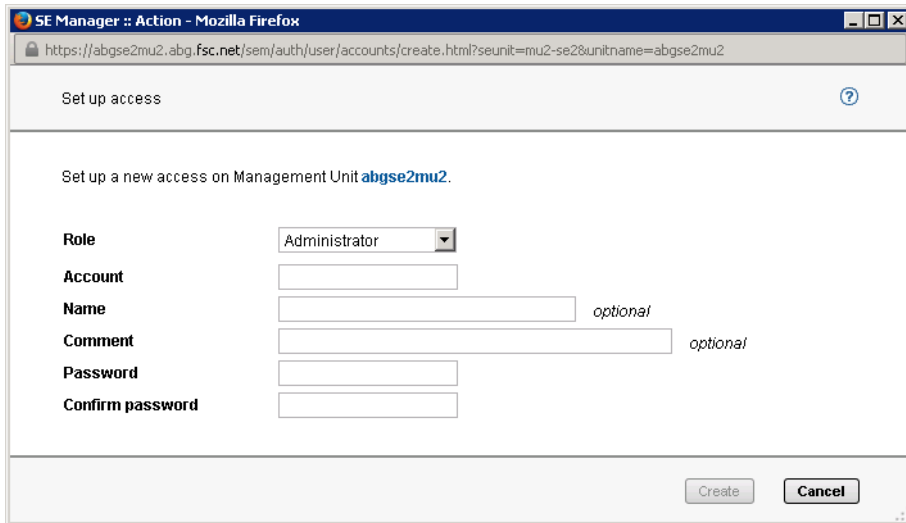
Configuration for Internet Explorer:

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/en-us>

3.3.4 The dialog

A dialog opens as soon as you start an action:



The screenshot shows a web browser window titled "SE Manager :: Action - Mozilla Firefox". The address bar contains the URL: <https://abgse2mu2.abg.fsc.net/sem/auth/user/accounts/create.html?seunit=mu2-se28&unitname=abgse2mu2>. The page content is titled "Set up access" and includes a help icon. Below the title, it says "Set up a new access on Management Unit **abgse2mu2**". The form contains the following fields:

- Role**: A dropdown menu with "Administrator" selected.
- Account**: A text input field.
- Name**: A text input field with "optional" text to its right.
- Comment**: A text input field with "optional" text to its right.
- Password**: A text input field.
- Confirm password**: A text input field.

At the bottom right of the form, there are two buttons: "Create" and "Cancel".

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. An *i* icon is displayed next to entry fields. When you drag the mouse over the *i* icon, possible values or the syntax to be used are displayed.
- Area with the labeled buttons, e.g. *Create* and *Cancel*.

After opening the dialog you have the following options:

- You can use options to control and confirm the action.
- Or you can confirm the action (dialog box with empty parameter area)

Alternatively you can also cancel the action.

You start an action using an icon or button. By pressing only the enter key you activate the default action (highlighted 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.



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.



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 94](#) 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.

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

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 → [*<se server>(SE<model>)* →] *<unit> (AU <model>)* → *Virtual machines* → *<vm-name>* provides you with the *Operation* tab.

Operation

Application Unit **abgqa700** VM **abgqa705-SLE11**: Status ?

VM name	abgqa705-SLE11
Status	▶ RUNNING
Operating system	SUSE Linux Enterprise 11 (64-bit)
Number CPUs	2
Main memory	8192 MB

Application Unit **abgqa700** VM **abgqa705-SLE11**: Operation ?

VMware vSphere Web Client

VMware Host Client

Application Unit **abgqa700** VM : Actions ?

Action Restart VM ▼

The *Open* action opens a separate browser window to execute the required actions. This window 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.

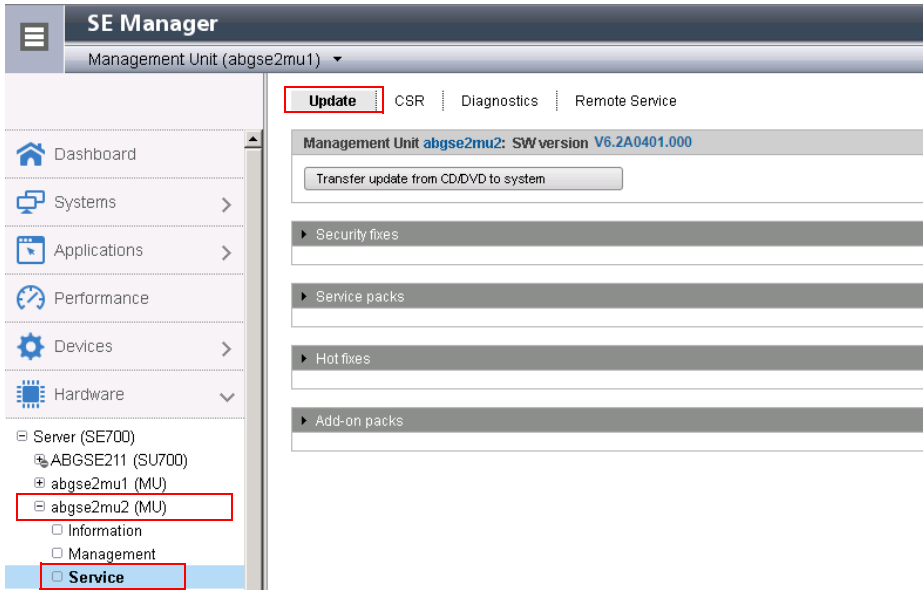
The content of the working area changes if you select another tab.

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 → Units[→ <se server> (SE<model>)] → <unit> (MU) → Service, Update tab

Hardware → *Units*[→ <se server> (*SE*<model>)] → <unit> (*MU*) → *Service* corresponds to a selection in the tree structure, *Update* to a selection in the secondary navigation, also called tab.



i 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*, *Applications*, *Performance*, *Devices*, *Hardware*, *Cluster*, *Authorizations*, and *Logging*. With the exception of *Dashboard*, all main menus can be expanded (the *Performance* main menu only in a multi-MU configuration).

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 menu 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 collapses 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:

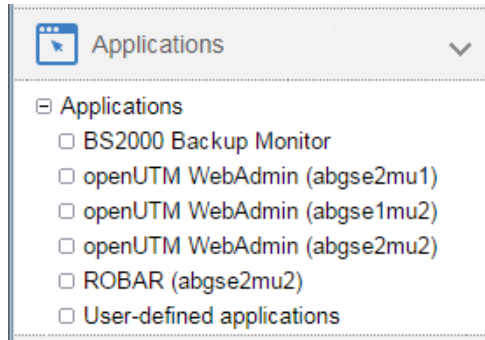
- *Systems* main menu:
 - when creating a BS2000 VM
 - when creating a XenVM
 - after a virtual machine has been created on an AU
- *IP networks* main menu:
 - when creating a new network

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).

Expanded navigation in case of MU redundancy or Management Cluster

In a multi-MU configuration, the tree structure of the SE Manager contains the following additional elements:

- In the *Applications* menu, the openUTM WebAdmin and ROBAR add-ons are displayed MU-specifically in the application overview.
The MU-specific link *<add-on> (<mu-name>)* links to the add-on on the respective MU.
Example:



- In the *Performance* → *Performance (<mu-name>)* menu, the MU-specific link always links to the add-on openSM2 on the respective MU.
- In the *Hardware* → *Storage* menu, the *Overview* tab displays a total overview over the storage systems and management software that the Storage Manager manages on all MUs. Storage systems that are configured on multiple MUs are only displayed once, with the worst status. A tool tip lists the status for each MU.
The *Hardware* → *Storage* → *Storage (<mu-name>)* menu displays an MU-specific overview over the storage systems and management software that the Storage Manager manages on this MU. Additionally, the menu contains the link to the Storage Manager on this MU.
- In the *Authorizations* → *Certificates* → *<mu-name> (MU)* menu, you manage certificates of the respective MU.

3.4.3 Filtering and sorting a table

On the tabs, the properties of the objects are listed in one or more tables. When a tab is called for the first time, all the data available for the function selected is displayed in a default sort (sorting column and sorting direction). The table column according to which the table is sorted is highlighted.



In some cases, the default sorting is neither ascending nor descending but by some other criterium. For example, the units in the unit table may be listed in the same order as in the navigation.

You can change the sorting criteria for the tables (columns) and, by filtering, the volume of displayed data.

The following properties are persistent, i.e. they are retained even when the window is changed and in the case of automatic update.

- Filter and sort
- Scroll position
- Page if scrolling pages is possible
- Status (expanded or collapsed) if expandable elements are contained

As soon as a table is being sorted or filtered, the *Reset table to default view* icon appears beneath it. Click the icon to obtain the table in the default sort and without filters. To obtain all tables in the default sort and without filters, click on *Login information* and select *Reset tables*.



For automatic updates see [section "Automatic update" on page 78](#).

As soon as a table contains more objects than are set in *Per page*, a control bar appears above the table containing the functions for scrolling and for paginating the objects to be displayed. Details for controlling the table view are provided in the online help.

Filtering a table

Filters reduce the number of data displayed in a table based on certain criteria and make handling large tables easier. You can use free text filters and filter lists to filter the data used to build up a table.

The filters for different table columns can be combined.

If a filter is set, the filter's field is highlighted.

A free text filter "<string>" will display hits without regard to capitalization on every position of a line. With "^<string>", only a hit at the start of the cell is searched for. With "<string>\$", only a hit at the end of the cell is searched for. You must escape special characters with a preceding "\".



Detailed information on filtering tables is provided in the SE Manager help. Here, the different filter options are described at the places where they can be used.

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 newly sorted. The selected column is highlighted.

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

Sorting according to a different column cancels the previous sort order.

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 80](#) 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 executed



- ▶ Proceed as follows to log in on the SE Manager:
- ▶ Select *Hardware* → *Units*[→ <se server> (*SE*<model>)] → <unit> (*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	<input type="text" value="host-trap2.example.net"/>
Trap community	<input type="text" value="sdfsd"/>
SNMP version	<input type="text" value="SNMPv1"/>

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

Management Unit **abgse2mu2**.

<input type="text" value="host-trap2.example.net"/>
<input type="text" value="sdfsd"/>
<input type="text" value="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*.

Add new trap receiver

Trap receiver	Trap community
<i>Filter</i>	<i>Filter</i>
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:

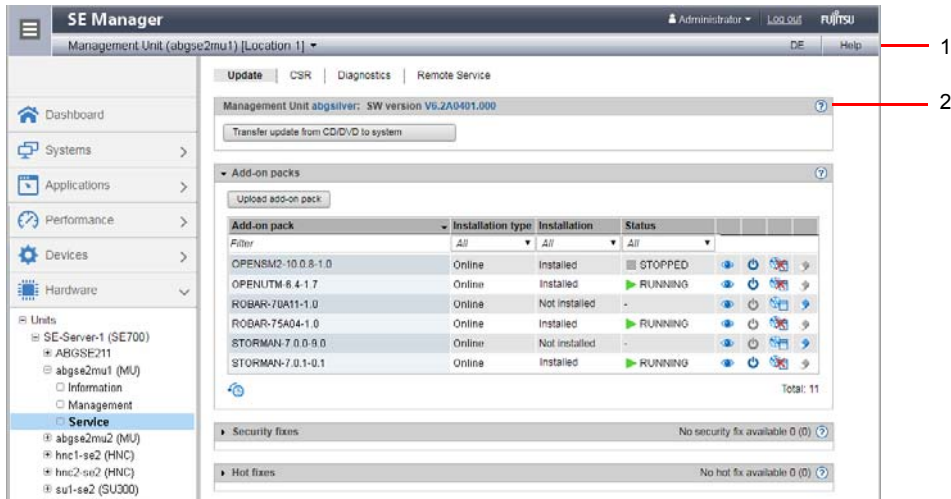


Figure 14: Calling the SE Manager help

- 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:

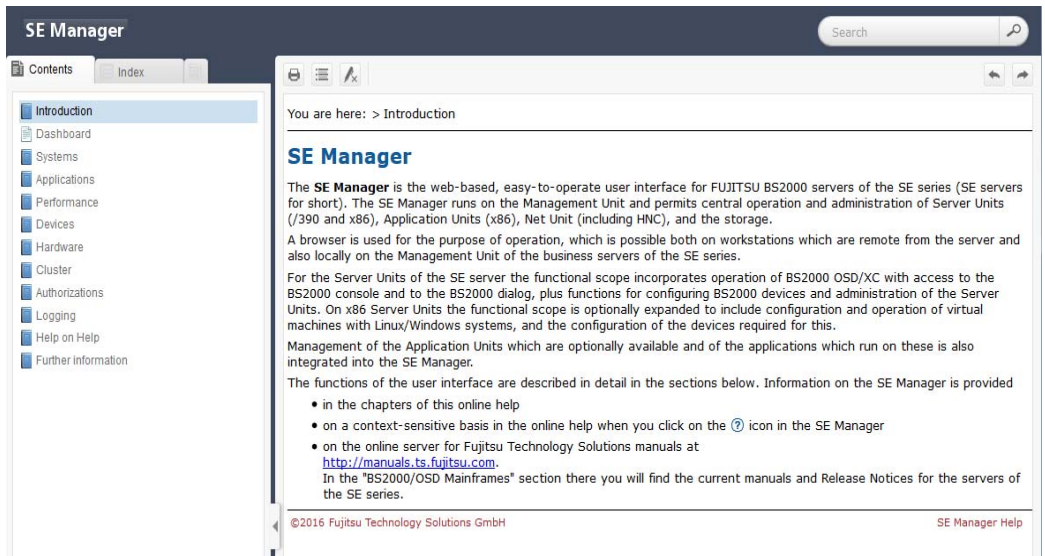


Figure 15: Homepage of the SE Manager help

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 the 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 an 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 information* 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 97](#)).
- ▶ 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, Cluster, Users* and *Events* of the SE server configuration. The *Dashboard* is displayed after you have logged in on the SE Manager.



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

Cluster is displayed only if at least one cluster exists in the SE server configuration.

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.

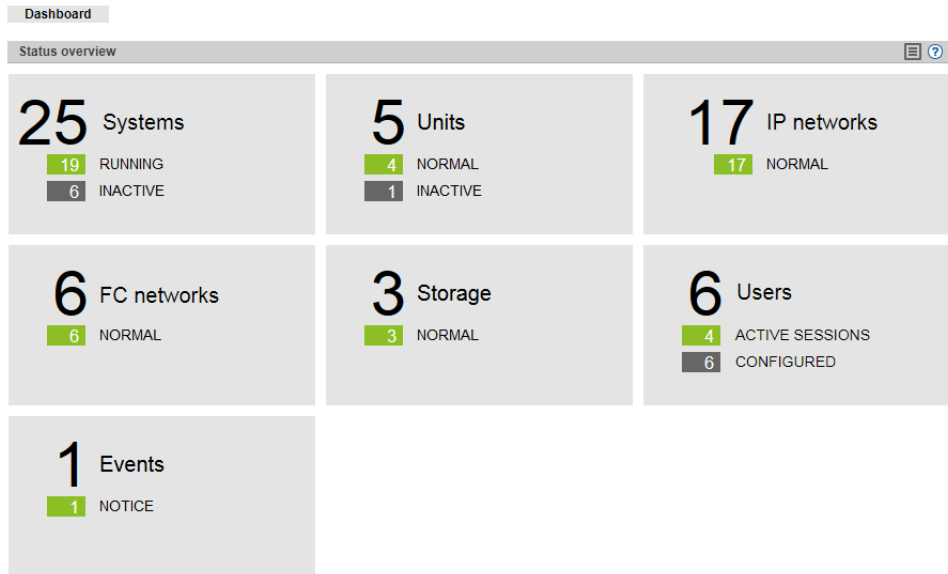
Displaying the status overview in the tile view

- ▶ 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.



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.

Dashboard			
Status overview			
▶	25	Systems	19 RUNNING 6 INACTIVE
▶	5	Units	4 NORMAL 1 INACTIVE
▶	17	IP networks	17 NORMAL
	6	FC networks	6 NORMAL
▶	3	Storage	3 NORMAL
▶	6	Users	4 ACTIVE SESSIONS
	1	Events	1 NOTICE

- ▶ 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.

- ▶ 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*.

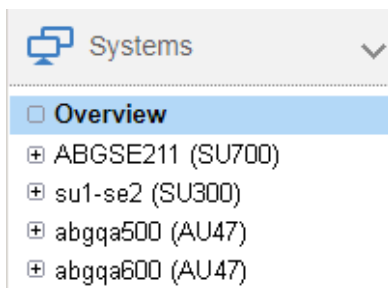
The associated overview page opens with the corresponding filter, in this example the *Systems* main menu with the *Overview* tab. Only the VM2000 systems with the status *INACTIVE* are displayed.

5 Operating and managing systems on Server Units

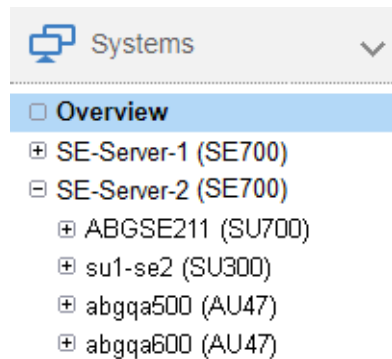
The systems referred to here are the Native and virtual operating systems which run on the various units of the SE server.

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

Managing a single SE server (SE700)



Managing two SE servers in a Management Cluster



In the tree structure displayed, those units are shown on which the so-called "productive systems" with their applications run. These are Server Units with BS2000 systems and XenVMs (only for SU x86) as well as Application Units with Unix, Linux or Windows systems. In each case, the name is followed by the type of 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, AU47 refers to an Application Unit based on an x86-based server.



The operation and administration of the systems on AUs are described in the [chapter "Operating and managing systems on Application Units" on page 147](#).

If you manage a configuration of two SE servers in a Management Cluster, underneath *Systems*, a submenu *<se server> (SE<model>)* will be displayed for each SE server, containing the SUs and AUs of the respective SE server.

Overview of all systems of the SE server configuration

- ▶ Select *Systems* → *Overview*, *Overview* tab.

The *Overview* tab displays information on all systems present on the managed SE server configuration. See the following example for SE700:

Name	Type	Operating system	Server	Unit	Status
M4IVR	VM2000	BS2000 OSD/BC V10.0A	SE-Server-1	D020ZE01	▶ RUNNING
G4IVQ	VM2000	BS2000 OSD/BC V10.0A	SE-Server-1	D020ZE01	▶ RUNNING
G4IVP	VM2000	BS2000 OSD/BC V11.0A	SE-Server-1	D020ZE01	▶ RUNNING
G4IVO	VM2000	BS2000 OSD/BC V10.0A	SE-Server-1	D020ZE01	▶ RUNNING
G4IVJ	VM2000	BS2000	SE-Server-1	D020ZE01	■ INIT_ONLY
TEST1	VM2000	BS2000	SE-Server-1	D020ZE01	■ DEFINED_ONLY
DIO	VM2000	BS2000	SE-Server-1	D020ZE01	■ DEFINED_ONLY
DUBE	VM2000	BS2000	SE-Server-1	D020ZE01	■ DEFINED_ONLY
MONITOR	VM2000	BS2000 OSD/BC V10.0A	SE-Server-1	abgafrica	▶ RUNNING
ABGAFR02	VM2000	BS2000 OSD/BC V10.0A	SE-Server-1	abgafrica	▶ RUNNING
ABGAFR03	VM2000	BS2000 OSD/BC V10.0A	SE-Server-1	abgafrica	▶ RUNNING
ABGAFR04	VM2000	BS2000 OSD/BC V10.0A	SE-Server-1	abgafrica	▶ RUNNING

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

The *Server* column is only displayed if two SE servers are managed together in a Management Cluster. It contains the name of the SE server to which the system belongs.

Overview over the systems of a Server Unit

- ▶ Select *Systems* → [*<se server>(SE<model>)*] → *<unit> (SU<model>)*, *Overview* tab.

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

Overview | BS2000 operation mode

Server Unit **su1-se2**: Main memory (256 GB) ?

Used main memory: 57.7 GB Free main memory: 198.3 GB

22.5 % 77.5 %

Server Unit **su1-se2**: License dependent CPU usage ?

X2000	BS2000	XenVM	Free
6	8 (2)	8	0

Server Unit **su1-se2**: Systems ?

Name	Type	Main memory [MB]	Status
<i>Filter</i>	<i>All</i> ▼	<i>Filter</i>	<i>All</i> ▼
MONITOR	VM2000	4096	▶ RUNNING
VM1	VM2000	16384	▶ RUNNING
VM2	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* → [*se server*] (*SE* <model>) →] <unit> (*SU* </390>), *BS2000 operation mode* tab.

Overview **BS2000 operation mode**

Server Unit ABGSE211: Status ?

Status	▶ RUNNING (since 2017-10-19 11:59:48)
Operation mode	VM2000 mode
Active IORSF file	1 (TYPE-1 IO INITIAL PATTERN CH#00=FCN DATE 14/MAY/2014)

[Management of IORSF files](#)

Server Unit ABGSE211: Actions ?

[Initiate IMPL / Change BS2000 operation mode](#)

Server Unit ABGSE211 SVP Console ?

SVP Console [Open](#)

Server Unit ABGSE211 SVP operation ?

Management Unit	Status	
abgse2mu1	ACTIVE	
abgse2mu2	PASSIVE	✎

The *BS2000 operation mode* tab in the *Status* group displays 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 *Initiate IMPL / Change BS2000 operation mode*. In the subsequent *Initiate IMPL / Change BS2000 operation mode* dialog box, enter the IPL parameters for the IMPL. Optionally, you can change the operating mode.



After the execution of the IMPL, a BS2000 IPL is always initiated. Depending on the set operation mode, either the native BS2000 or the monitor system is started.

If you set a different IORSF file, you have to explicitly update the IORSF file list in the *Devices* menu after the IMPL has been executed.

Switching active Management Unit

If an SE server has redundant Management Units, they are displayed in the *SVP operating* table: One MU is always *ACTIVE* with respect to SVP operating, and the other is *PASSIVE*.

- ▶ Click on the *Change* icon for the passive MU to make it the active MU with respect to SVP operating.



This action may be advisable if the active MU has to be shut down for maintenance reasons and the SVP console has to be available without interruption.

See also [“Redundant Management Units” on page 52](#).

5.1.2 Server Unit x86

- ▶ Select *Systems* → [*<se server>* (*SE<model>*) →] *<unit>* (*SU<x86>*), *BS2000 operation mode* tab.

Overview | **BS2000 operation mode**

Server Unit *su1se2*: BS2000 operation mode ?

Current mode VM2000 mode ✎

Server Unit *su1se2*: Startup settings: Native BS2000 system ?

BS2000 main memory - configured [MB]	32768 (32254)	✎ ✓
BS2000 main memory - possible [MB]	230086	
Total memory [MB]	262144	

Server Unit *su1se2*: Startup settings: Monitor VM ?

Number of virtual CPUs	3	✎ ✓
Main memory - maximum [MB]	5120 (5032)	
Main memory - minimum [MB]	2560 (2472)	
Main memory [MB]	4096 (4008)	
Exclusive devices	9907 9908 9909 CC40 CC41 CC80 CC81 CD40 CD41 Z0 Z1	
Shared devices	34BF 50EA 50EB	
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. In VM2000 mode this applies for all BS2000 VMs.

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



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).



If you change the device configuration of the monitor VM, please note the following:

- If the devices of the monitor VM are assigned or removed using the VM specific tabs *Disks*, *KVP*, *LAN*, *Tape devices* or *All devices*, the changes only remain active until the BS2000 operation mode is reset or until the SU is restarted. The same applies for changes of the device configuration done via VM2000 commands that refer to the monitor VM.
- If changes to the device configuration are to remain active after a change of the BS2000 operation mode or restart of the SU, they have to be entered and activated in the startup configuration of the monitor VM as well (see group *Startup settings: Monitor VM* of the *BS2000 operation mode* tab).
- Changes to the startup configuration of the monitor VM have no immediate effect on the running monitor VM.

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

- ▶ To change the main memory size for the Native BS2000 system, in the *Startup settings: Native BS2000 system* group, click the *Change* icon.
- ▶ To change the number of virtual CPUs, the main memory settings, the device lists or the access password for the monitor VM, in the *Startup settings: Monitor VM* group, click the *Change* icon.

Changes will take effect only after the setting has been activated by clicking the *Activate* 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* → [*<se server>(SE<model>)* →] *<unit> (SU<model>)* → *BS2000, Operation* tab.
 - ▶ VM2000 on SU /390: Select *Systems* → [*<se server>(SE<model>)* →] *<unit> (SU</390>)* → *Virtual machines* → *<bs2000-vm>*, *Operation* tab.
 - ▶ VM2000 on SU x86: Select *Systems* → [*<se server>(SE<model>)* →] *<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.

Alternatively, you can open a BS2000 console or a BS2000 dialog via PuTTY, by using the CLI commands *bs2Console* and *bs2Dialog*. A detailed description is provided in [chapter “Appendix” on page 331](#).

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.

You can inquire response and any meaning texts for messages of M2000/X2000 using the HTML application "System messages". It is available online at <http://manuals.ts.fujitsu.com> or on the "BS2000 SoftBooks" DVD.



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.

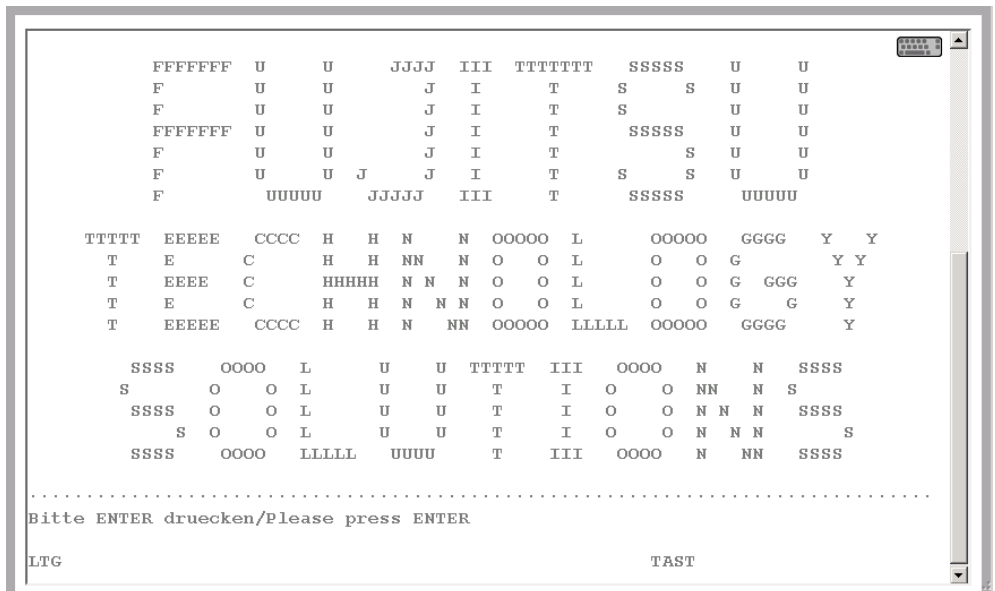
5.3 SVP console on Server Unit /390

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*→[<se server>(SE<model>) →]<unit> (SU</390>), BS2000 operation mode tab.
- ▶ In the *SVP console* group click *Open*.

The SVP console window opens.



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].

Alternatively, you can open the SVP console via PuTTY, by using the CLI command *svpConsole*. A detailed description is provided in [chapter "Appendix", section "SVP console on MU or SU /390" on page 340](#).

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 and migrating](#)
- [Setting the options \(only SU x86\)](#)
- [Evaluating KVP logging](#)

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

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

- ▶ Select *Systems* → [*<se server>(SE<model>)* →] *<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

The following actions are only available for SU x86. The SU x86 also has to form an SU Cluster with another SU x86 of the SE server configuration. Whether or not an LM (Live Migration) is possible, depends on the cluster status. The second SU must also be in the *Native BS2000 mode* operating mode. See also [section “SU Cluster” on page 45](#). Further details are provided in the "Cluster Solutions for SE Servers" whitepaper [8].

- Delete BS2000
This action prepares the SU as target SU for a migration.
- Restore BS2000
This action restores the SU after a failback (BS2000 was deleted).
- Migrate BS2000
Starts the wizard for the migration of the BS2000.

5.4.2 Setting the options (only SU x86)

For SU x86, you manage the options using the *Options* tab of the BS2000 system. You can change the settings for the shutdown, the startup and the Auto IPL.

- ▶ Select *Systems* → [*<se server>(SE<model>)* →] *<unit>(SU<model>)* → *BS2000, Options* tab.

Operation Options KVP logging

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 groups *General options* and *BS2000 options*. The tab provides the following functions:

Defining the remaining runtime for shutdown

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 x86 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 [10]). 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 121](#)).

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.

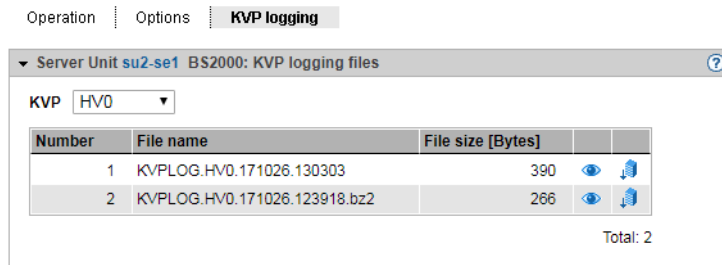
Setting BS2000 options (startup and auto IPL)

- ▶ 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* → [*<se server> (SE<model>)* →] *<unit> (SU<model>)* → *BS2000, KVP logging* tab.



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 in the monitor system when 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 → [*<se server>*(*SE<model>*) →] *<unit>* (*SU</390>*) → *Virtual machines*, *VM administration tab*

or

Systems → [*<se server>*(*SE<model>*) →] *<unit>* (*SU<x86>*) → *Virtual machines* → *BS2000*, *VM administration tab*

VM administration | VM resources | VM options

Server Unit D020ZE01: VM administration (BS2000) Free main memory: 3301 MB (3301 MB)

Create new BS2000 VM

VM name	Host name	VM index	Main memory [MB]	Status
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	All ▾
MONITOR	ABGSE211	1	512	▶ RUNNING
VM03A1	D123ZE02	2 (*ANY)	2048	▶ RUNNING ↗
VM04UV	D123ZE03	3 (*ANY)	3072	▶ RUNNING ↗
VM05	D123ZE04	4 (*ANY)	3072	▶ RUNNING ↗
VM06B5	D123ZE05	5	256	▶ RUNNING ↗
VM10SEGA	-	- (*ANY)	512	■ DEFINED_ONLY ↗
VM11G9	-	- (*ANY)	512	■ DEFINED_ONLY ↗
VM12G8	-	- (*ANY)	512	■ DEFINED_ONLY ↗

Total: 8

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 → [*<se server>(SE<model>)*] → [*<unit> (SU</390>)*] → *Virtual machines, VM resources* tab

or

Systems → [*<se server>(SE<model>)*] → [*<unit> (SU<x86>)*] → *Virtual machines* → *BS2000, VM resources* tab

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

Server Unit **ABGSE211**: CPU pools (BS2000) ?

CPU pool	Attached CPUs	Detached CPUs	Number of VMs
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>
*STDPOOL	2	0	3
USRCPOOL	2	0	2

Total: 2

Server Unit **ABGSE211**: VM resources (BS2000) ?

VM name	VM index	vCPUs	CPU pool	CPU quota	Max. CPU util.	Status
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	All ▼
MONITOR	1	2	*BY_VM_GROUP	1.00	100.00	▶ RUNNING ✎
VM03A1	2 (*ANY)	2	*STDPOOL	25.00	100.00	▶ RUNNING ✎
VM04UV	3 (*ANY)	2	*BY_VM_GROUP	2.00	100.00	▶ RUNNING ✎
VM05	4 (*ANY)	2	*BY_VM_GROUP	2.00	100.00	▶ RUNNING ✎
VM06B5	5	1	*STDPOOL	5.00	100.00	▶ RUNNING ✎
VM10SEGA	- (*ANY)	1	*STDPOOL	1.00	100.00	■ DEFINED_ONLY ✎
VM11G9	- (*ANY)	1	*STDPOOL	1.00	100.00	■ DEFINED_ONLY ✎
VM12G8	- (*ANY)	1	*STDPOOL	1.00	100.00	■ DEFINED_ONLY ✎

Total: 8

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 the automatic IPL for the monitor VM (only SU x86) and persistent BS2000 VMs. For a non-persistent BS2000 VM (except the monitor VM), you can set the persistence attribute. On an SU x86 you can also set the remaining runtime for the shutdown.

- In the tree structure select

Systems → [*<se server>(SE<model>)* →] *<unit> (SU</390>)* → *Virtual machines, VM options tab*

or

Systems → [*<se server>(SE<model>)* →] *<unit> (SU<x86>)* → *Virtual machines* → *BS2000, VM options tab*

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

Server Unit **su2-se1** General options ?

Remaining runtime for shutdown 00:30 (hh:mm) ✎

Server Unit **su2-se1**: VM specific options ?

VM name	Persistence	Auto IPL	Boot disk	Console device	Startup mode	System name	
<i>Filter</i>	<i>All</i> ▼	<i>All</i> ▼	<i>Filter</i>	<i>Filter</i>	<i>All</i> ▼	<i>Filter</i>	
MONITOR	No	Not planned	-	-	AUTOMATIC	-	✎
ABGGOLD2	Yes	Planned	8181	Z2_Z3 (KVP VM2)	FAST	ABGGOLD2	✎
ABGGOLD3	Yes	Planned	8182	Z4_Z5 (KVP VM3)	FAST	ABGGOLD3	✎
VM22	Yes	Not planned	-	-	FAST	-	✎

Total: 3

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 the VM-specific options (persistence, Auto IPL and startup parameters)

- 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.



If you deactivate automatic IPL of a persistent VM, the preset IPL parameters are retained and are available for an explicit IPL in the "Initiate BS2000 IPL" 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 [10]). 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 the options \(only SU x86\)” on page 116](#).

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 → [*<se server>(SE<model>)* →] *<unit> (SU</390>)* → *Virtual machines* → *<bs2000-vm>*

or

Systems → [*<se server>(SE<model>)* →] *<unit > (SU<x86>)* → *Virtual machines* → *BS2000* → *<bs2000-vm>*

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

The following functions are available to you, depending on the situation:

- [Start and shut down a BS2000 guest system, create a dump / enable and disable \(and delete\) a BS2000 VM, migrate](#)
- [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, migrate

► Select:

Systems → [*<se server>(SE<model>)* →] *<unit> (SU</390>)* → *Virtual machines* → *<bs2000-vm>*, *Operation tab*

or

Systems → [*<se server>(SE<model>)* →] *<unit> (SU<x86>)* → *Virtual machines* → *BS2000* → *<bs2000-vm>*, *Operation tab*

Operation | Disks | KVP | LAN | Tape devices | All devices

Server Unit *su1se2* BS2000 VM *ABGSE404*: Status

Host name	ABGQN404
Status	▶ RUNNING (since 2017-08-21 16:11:23)
Operating system	BS2000 OSD/BC V10.0A
Home pubset	QN11
Number of vCPUs	4
Main memory	4000 (3912) MB

	Current	Presetting
Boot disk	29FB	- (not persistent)
Console device	Z6	-
System name	ABGSE404	-

Server Unit *su1se2* BS2000 VM *ABGSE404*: Console and dialog

BS2000 console with KVP VM2 and console mnemonic

BS2000 dialog with connection *MANLO2*

Server Unit *su1se2* BS2000 VM *ABGSE404*: Actions

Action

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

- BS2000 IPL
- BS2000 dump IPL
- BS2000 shutdown
- Activate BS2000 VM (persistent VMs only)
- Deactivate BS2000 VM (persistent VMs only)
- Deactivate and delete BS2000 VM (only non-persistent VMs except the monitor VM)

- Migrate BS2000 VM (except monitor VM)
Starts the wizard for the migration of the BS2000 VM.



This action is only available if the SU is a member of an SU Cluster and LM is possible. The second SU must also be in the *VM2000 mode* operating mode. See also [section “SU Cluster” on page 45](#). Further details are provided in the "Cluster Solutions for SE Servers" whitepaper [8].

The description of the BS2000 console window and dialog is provided in [section “Opening the BS2000 console and dialog window” on page 112](#).

5.5.4.2 Managing devices of the VM

► **Select:**

Systems → [*<se server>(SE<model>)* →] *<unit> (SU</390>)* → *Virtual machines* → *<bs2000-vm>*, tabs *Disks*, *KVP*, *LAN*, *Tape devices* or *All devices*

or

Systems → [*<se server>(SE<model>)* →] *<unit> (SU</x86>)* → *Virtual machines* → *BS2000* → *<bs2000-vm>*, tabs *Disks*, *KVP*, *LAN*, *Tape devices* or *All devices*

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.

Operation | **Disks** | KVP | LAN | Tape devices | All devices

Server Unit **ABGSE211** BS2000-VM **VM08SE2**: Assigned disks ?

➔ Management of BS2000 disks

MN	Type	Usage		
<i>Filter</i>	<i>All</i>	<i>All</i>		
817D	A5	Exclusive		
817D	A5	Exclusive		
FC0D	A5	Exclusive		
FC0E	A5	Exclusive		
FC0F	A5	Exclusive		

Total: 5



The link to IORSF file management and the *PAV* column are displayed for SU / 390 only.

- Click *Assign disk* to assign another disk individually to the VM.
- Click *Management of BS2000 disks* to branch to the device management, see [section “Managing disks” on page 173](#).
- Click the *Change* icon by a disk to change the usage of this disk (Shared/Exclusive).
- Click the *Remove* icon by a disk to *remove* this disk from the VM.

For further information on displaying BS2000 disks, see [section “Displaying generated disks on Server Unit /390” on page 173](#) and [section “Managing disks on Server Unit x86” on page 174](#).

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.

Operation | Disks | **KVP** | LAN | Tape devices | All devices

Server Unit **ABGSE211** BS2000 VM **M41VR**: Assigned KVPs ?

Assign KVP ↗ Management of IORSF files ↗ Management of KVPs

MN	KVP name	Unit	
Filter	Filter	All	
C2_C3	HV0	abgse2mu1	↗
C4_C5	HV0	abgse2mu2	↗

Total: 2

Server Unit **ABGSE211** BS2000 VM **M41VR**: KVP logging files ?

KVP: HV0 (abgse2mu2)

Number	File name	File size [Bytes]		
1	KVPLOG.HV0.180222.085356	947	👁	📄
2	KVPLOG.HV0.180221.121129.bz2	658	👁	📄
3	KVPLOG.HV0.180218.042159.bz2	219	👁	📄
4	KVPLOG.HV0.180215.112955.bz2	1,130	👁	📄
5	KVPLOG.HV0.180214.091222.bz2	383	👁	📄
6	KVPLOG.HV0.180213.082520.bz2	848	👁	📄



The link to IORSF file management link and the *Unit* column in the *Assigned KVPs* group and the MU of the selected KVP in the *KVP logging files* group are displayed for SU / 390 only.

Assigning a KVP

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

Removing a KVP

- ▶ In the *Assigned KVPs* group click the *Remove* icon by a KVP and confirm the action.

Branching to the hardware device management

- ▶ Click *Management of KVPs* to branch to the hardware device management, see [section "Managing KVP devices" on page 176](#).

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 176](#).

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 devices which are assigned to the BS2000 VM.

Operation | Disks | KVP | **LAN** | Tape devices | All devices

Server Unit ABGSE211 BS2000-VM M4IVR: Assigned LAN devices ?

Assign LAN device Management of IORSF files Management of LAN devices

MN	Type	BS2 IP address	BS2 MAC address	Unit	
<i>Filter</i>	<i>All</i>	<i>Filter</i>	<i>Filter</i>	<i>All</i>	
CC40_CC41	ZASLAN	-	00:1...:C0	abgse1mu1	➔
CC80_CC81	LOCLAN	19...3.21	0A:f...:15	abgse2mu1	➔
CD40_CD41	ZASLAN	-	00:1...:50	abgse1mu2	➔
CD80_CD81	LOCLAN	19...9.21	0A:0...:15	abgse2mu2	➔

Total: 4



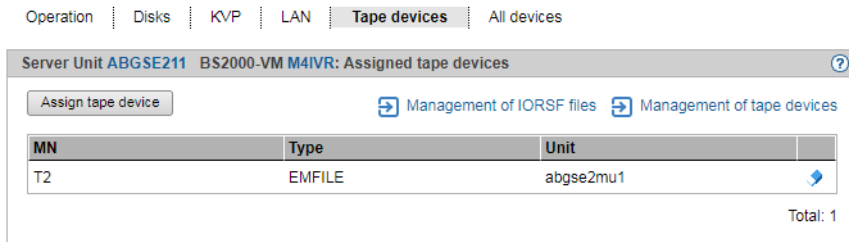
The link to IORSF file management link and the *Unit* column are displayed for SU / 390 only.

- ▶ Click *Assign 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 179](#).

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 devices* tab lists all tape devices which are assigned to the BS2000 VM.



The link to IORSF file management link and the *Unit* column are displayed for SU / 390 only.

- ▶ Click *Assign 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 181](#).

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 devices which are currently assigned to the BS2000 VM.

Operation | Disks | KVP | LAN | Tape devices | **All devices**

Server Unit su1se2 BS2000 VM ABGAFR05: All assigned devices

Assign devices Remove devices

BS2000 mnemonic	Device type	Usage
<i>Filter</i>	<i>All</i>	<i>All</i>
CC48	LAN	Exclusive
CC49	LAN	Exclusive
CC88	LAN	Exclusive
CC89	LAN	Exclusive
K0	Disk	Exclusive
K1	Disk	Exclusive
K2	Disk	Exclusive
Z8	KVP	Exclusive
Z9	KVP	Exclusive

Total: 9

The device mnemonic, device type and device usage are displayed for each assigned BS2000 device (*Exclusive* only for one BS2000 VM or *Shared* for more than one BS2000 VMs usable).

- ▶ 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* → [*<se server>(SE<model>)*] *<unit>* (*SU<x86>*) → *Virtual machines* → *XenVM*, *VM administration* tab.

VM administration | VM resources | VM installation | VM options

Server Unit **su3se1**: VM administration (XenVM)

Create new XenVM Free main m...

VM name	Operating system	Virt.	VNC port	Main memory [MB]	Status
<i>Filter</i>	<i>Filter</i>	<i>All</i>	<i>Filter</i>	<i>Filter</i>	<i>All</i>
ABGEX407	SUSE Linux Enterprise Server 11	Para	5903	4000	▶ RUNNING
ABGEX408	Windows Server 2012 (x64)	Full	5902	8000	▶ RUNNING
Linux_1	SUSE Linux Enterprise Server 11	Para	-	512	■ STOPPED
Windows_1	Windows Server 2012 (x64)	Full	-	1024	■ STOPPED
XenVM_ABGQX502	Windows Server 2012 (x64)	Full	5900	8192	▶ RUNNING
XenVM_ABGQX503	SUSE Linux Enterprise Server 11	Para	5901	8192	▶ RUNNING

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 191](#)), upload ISO image of the required operating system to the local library as an installation source (see [section “Managing installation sources” on page 195](#)).

- ▶ 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 138](#).

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* → [*<se server>(SE<model>)*] *<unit>* (*SU<x86>*) → *Virtual machines* → *XenVM*, *VM resources* tab.

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

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

Server Unit **su3se1**: VM resources (XenVM) ?

VM name	Main memory [MB]	vCPUs	Weight	Limit [%]	
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	
ABGEX407	4000	4	256	0 (Unlimited)	✎
ABGEX408	8000	4	256	0 (Unlimited)	✎
Linux_1	512	1	256	0 (Unlimited)	✎
Windows_1	1024	2	256	0 (Unlimited)	✎
XenVM_ABQQX502	8192	2	256	0 (Unlimited)	✎
XenVM_ABQQX503	8192	2	256	0 (Unlimited)	✎

Total: 6

- ▶ 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 *Change* 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* → [*se server*] (*SE*<*model*>) → <*unit*> (*SU*<*x86*>) → *Virtual machines* → *XenVM*, *VM installation* tab.

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

VM name	Installation status	Last change	Job ID			
XenVM_Index_1	INSTALL	2017-01-20 10:34:23	btpVF_			

Total: 1

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 139](#)).

- ▶ 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)
- Display and change 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* → [*<se server>(SE<model>)* →] *<unit> (SU<x86>)* → *Virtual machines* → *XenVM, VM options* tab.







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

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

Server Unit **su3se1**: General options (XenVM) ?

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

Server Unit **su3se1**: VM-specific options (XenVM) ?

VM name	Auto start	Delay time	
<i>Filter</i>	All		
ABGEX407	Not planned	-	
ABGEX408	Not planned	-	
Linux_1	Not planned	-	
Windows_1	Not planned	-	
XenVM_ABGQX502	Not planned	-	
XenVM_ABGQX503	Not planned	-	

Total: 6

- ▶ 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* → [*<se server>(SE<model>)*] → *<unit>(SU<x86>)* → *Virtual machines* → *XenVM, VM option* 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* → [*<se server>(SE<model>)* →] *<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* → [*<se server>(SE<model>)* →] *<unit> (SU<x86>)* → *Virtual machines* → *XenVM* → *<XenVM-Name>*, *Operation* tab.

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

The screenshot displays the SE Manager interface for a XenVM. At the top, there is a navigation bar with tabs: **Operation** (selected), Configuration, Disks, IP networks, and Installation sources. Below this, the main content area is divided into three sections:

- Server Unit su3se1 XenVM ABGEX407: Status**: A table showing the current status of the VM.

Status	▶ RUNNING (since 2017-08-22 13:30:20)
Number of vCPUs	4
Main memory	4000 MB
- Server Unit su3se1 XenVM ABGEX407: Console**: A section with the text "XenVM console" and an "Open" button.
- Server Unit su3se1 XenVM ABGEX407: Actions**: A section with a dropdown menu set to "Restart XenVM" and an "Execute" button.

5.6.5.2 Opening the console of the XenVM

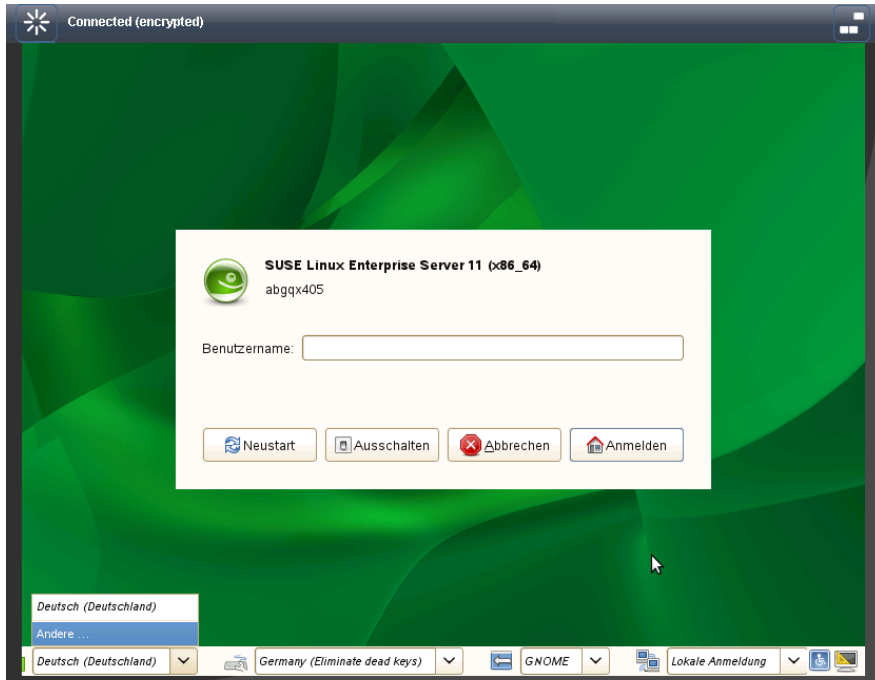
The console window can be opened at any time, i.e. irrespective of the status of the XenVM. You consequently have the option of opening the console before the XenVM is started, to observe the messages during system startup, and to diagnose any errors which may occur.

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

- ▶ Select *Systems* → [*<se server>(SE<model>)* →] *<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.



5.6.5.3 Starting and shutting down the XenVM

- ▶ Select *Systems* → [*<se server>(SE<model>)*] → *<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 130](#). 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* → [*<se server>(SE<model>)*] → *<unit> (SU<x86>)* → *Virtual machines* → *XenVM* → *<XenVM-Name>*, *Configuration* tab.

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

Operation | **Configuration** | Disks | IP networks | Installation sources

Server Unit **su3se1** XenVM **ABGEX407**: Configuration

Name	ABGEX407	
Description		
Operating system	SUSE Linux Enterprise Server 11	
Number of vCPUs	4	
Main memory	4000 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 188](#)). You configure the first virtual disk of the XenVM when you create the XenVM, see [section “VM administration” on page 130](#).

- ▶ Select *Systems* → [*<se server>(SE<model>)*] → *<unit>(SU<x86>)* → *Virtual machines* → *XenVM* → *<XenVM-Name>*, *Disks* tab.

Operation | Configuration | **Disks** | IP networks | Installation sources

Server Unit *su3se1* XenVM *XenVM_ABGQX503*: Virtual disks assigned

Assign virtual disk Management of virtual disks Management of disk pools

Select boot disk

Virtual disk	Disk pool	Size [MB]	Virtual device	Device number	Boot	Accessible		
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>All</i>	<i>All</i>		
DX8400_L024027_1	DX8400_V024027	20480	xvdb	51728	Nein	Ja		
DX8400_L3A2	DX8400_V3A2	47104	xvda	51712	Ja	Ja		

Total: 2

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.

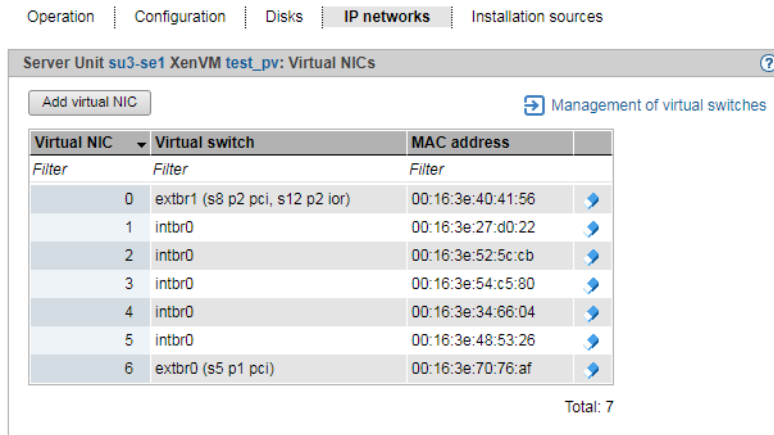
The virtual disk is immediately removed from the configuration of the XenVM. The disk is displayed with the XenVM devices as a free virtual disk.

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 130](#)). The virtual Network Interface Card (NIC) 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 188](#)).

- Select *Systems* → [*<se server>(SE<model>)*] → *<unit>(SU<x86>)* → *Virtual machines* → *XenVM* → *<XenVM-Name>*, *IP networks* tab.



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.

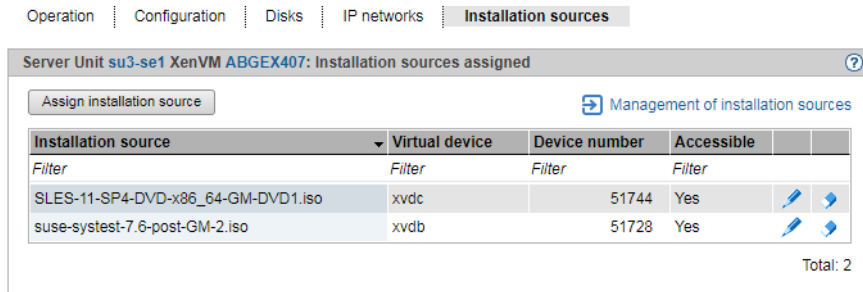
- Click the *Delete* icon by the virtual Network Interface Card to be deleted and confirm the action.

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 130](#)). Possible installation sources are available in the local library on the Server Unit (see [section “Managing XenVM devices on Server Unit x86” on page 188](#)). 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* → [*<se server>(SE<model>)*] → *<unit> (SU<x86>)* → *Virtual machines* → *XenVM* → *<XenVM-Name>*, *Installation sources* tab.



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> (AUxx)* or *<unit> (DBUxx)*.

6.1 Operating a Native system

You operate a Native system via the *Operation* tab.

- ▶ In the tree structure select *Systems* → [*<se server>(SE<model>)* →] *<unit> (AU<model>)*, *Operation* tab.

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

Operation

Application Unit **abgqa700** VM **abgqa705-SLE11**: Status ?

VM name	abgqa705-SLE11
Status	▶ RUNNING
Operating system	SUSE Linux Enterprise 11 (64-bit)
Number CPUs	4
Main memory	2048 MB

Application Unit **abgqa700** VM **abgqa705-SLE11**: Operation ?

VMware vSphere Web Client

VMware Host Client

Operation

- ▶ In the *Operation* tab click *Open* in the *Operation* group.
 - In this way you open the web interface of the iRMC for an AU PY (e.g. AU25 or AU47) .
 - In this way you open the web interface of the Management Board for an AU PQ (e.g. 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 as a VM has been configured, the tree structure below *Systems* → [*<se server>(SE<model>)* →] *<unit> (AU<model>)* → *Virtual machines* is expanded by a VM-specific menu *<VM-Name>*.



In the case of AU PQ, systems run on the individual partitions of the AU. As soon as a VM has been configured, the tree structure below *Systems* → [*<se server>(SE<model>)* →] *<unit> (<AU PQ model>)* → *<unit> (<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* → [*<se server>(SE<model>)* →] *<unit> (AUxx)* → *Virtual machines*, *VM overview* tab.

On AU PQ select *Systems* → [*<se server>(SE<model>)* →] *<unit> (<AU PQ model>)* → *<unit> (<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* → [*<se server>(SE<model>)* →] *<unit> (AUxx)* → *Virtual machines* → *<VM-name>*.

On AU PQ select *Systems* → [*<se server>(SE<model>)* →] *<unit> (<AU PQ model>)* → *<unit> (<partition>)* → *Virtual machines* → *<VM-name>*.

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 161](#).
- A VM with vCenter Server must be running for VMware vSphere on the Application Unit.

Some actions for the VM can also be called directly in the SE Manager:

- ▶ Click *Open* in the *Operation* group VMware vSphere Web Client or Oracle VM Manager.



If VMware ESXi version 6.0.update02 or higher is installed on the AU, the *Open* action is also offered for "VMware Host Client".

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.

- ▶ Only for Oracle VM on AU PQ: In the *Console* group, click *Open Oracle VM Console*.

If it is not already open, the console of the Oracle VM opens in a new window.

Customer Support will install the key required for access.

- ▶ 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*, *Power off VM*, *Pause VM*, *Resume 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 [19].

Further information on modular RAID Controllers is provided in the “LSI Controllers Modular RAID Controller” Installation Guide [20].

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 [13].

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 [17].

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 151).

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 the 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 [18] and [19].

Configuring the network for the administration LAN

For the connection to the MU, AUs must be configured at the administration network. Configure this network when you install the operating system.

Configuring LAN interfaces

The connection can either be made to the public MANPU administration network or to the private MONPR01 administration network.

- For connection to MANPU:
Use Linux resources to configure the IP address, subnetwork and gateway.
- For connection to MONPR01:
Activate Linux for the selected eth interface DHCP for IPv6. The MU then assigns an automatic IPv6 address in the MONPR01 network.

In case your Linux does not support IPv6, you can connect the AU to MONPR01 via a static IPv4 address. To do so, please contact your service technician.

You configure the management network using Linux resources with the appropriate IP addresses, subnetwork masks, and gateways.

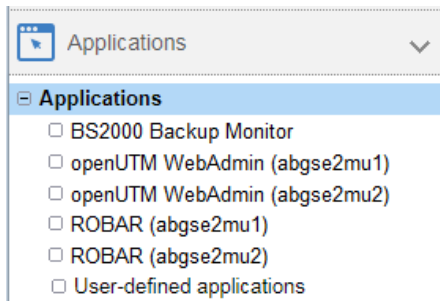
You configure the IP address in the administration network in accordance with your administration network, as defined with Customer Support in the installation checklist.



There is also an option of connecting an AU to private data networks (DANPRnn) or public 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

- ▶ In the tree structure select *Applications* → *Overview*. The *Overview* tab opens.

Overview

▼ SE management applications ?

Name	Description	Management Unit
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>
BS2000 Backup Monitor	Backup Monitor for HSMS and FDDRL in BS2000	- (global)
openUTM WebAdmin	openUTM-Server Administration	abgse2mu1
ROBAR	ROBAR-SV Server	abgse2mu1
ROBAR	ROBAR-SV Server	abgse2mu2

Total: 4

▶ User-defined management applications Total: 2 ?

▶ User-defined links Total: 2 ?

The application list consists of three groups (each as an expandable menu):

- 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 applications currently exist:

- [BS2000 Backup Monitor](#) is a permanent part of the SE Manager
- Storage Manager is a preinstalled add-on pack (in the *Hardware* → *Storage* menu, see [section “Managing storage systems” on page 281](#)).

The following optional SE management applications can be installed as add-on packs:

- openUTM WebAdmin (see [page 159](#))
- ROBAR (see [page 159](#))
- openSM2 (see [chapter “Performance überwachen” on page 163](#))

If the administered SE server configuration has more than one MU (SE server with redundant MU or two SE servers in a Management Cluster), every installation of these SE management applications is listed in the tree structure, with the exception of the BS2000 backup monitor. The name of the MU on which the application is installed is given in brackets after the name of the application. In the table of SE management applications, the name of the respective MU is listed in the *Management Unit* column.

openUTM WebAdmin, ROBAR and openSM2 are chargeable products, each with its own online help, which are realized as add-on packs.

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 configuration 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.

Overview Requests

BS2000 Backup Requests Overview

Get requests

Host name	HSMS Request State							FDDRL Request State				
	ACCEPTED	STARTED	INTERRUPTED	OK	WARNINGS	ERRORS	ACCEPTED	STARTED	OK	ERRORS		
Filter	All	All	All	All	All	All	All	All	All	All		
ABGQN406	-	-	-	-	-	-	-	-	-	-	↻ ↗	
ABGSE211	-	-	-	-	-	-	-	-	-	-	↻ ↗	
ABGSE113	-	-	-	-	-	-	-	-	-	-	↻ ↗	
ABGSE215	-	-	-	-	-	-	-	-	-	-	↻ ↗	
ABGSE217	-	-	-	-	-	-	-	-	-	-	↻ ↗	
ABGSE21A	-	-	-	-	-	-	-	-	-	-	↻ ↗	
ABGSE21B	-	-	-	-	-	-	-	-	-	-	↻ ↗	
ABGSE21C	-	-	-	-	-	-	-	-	-	-	↻ ↗	
ABGSE21D	-	-	-	-	-	-	-	-	-	-	↻ ↗	
ABGSE21F	-	1 ▶	1	30 ✓	1 ⚠	2 ✖	-	-	-	-	↻ ↗	
ABGSE301	-	-	-	-	-	-	-	-	-	-	↻ ↗	
ABGSE308	-	-	-	-	-	-	-	-	-	-	↻ ↗	
ABGSE40	-	-	-	-	-	-	-	-	-	-	↻ ↗	

Total: 13

In the *Overview* tab you can get 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.

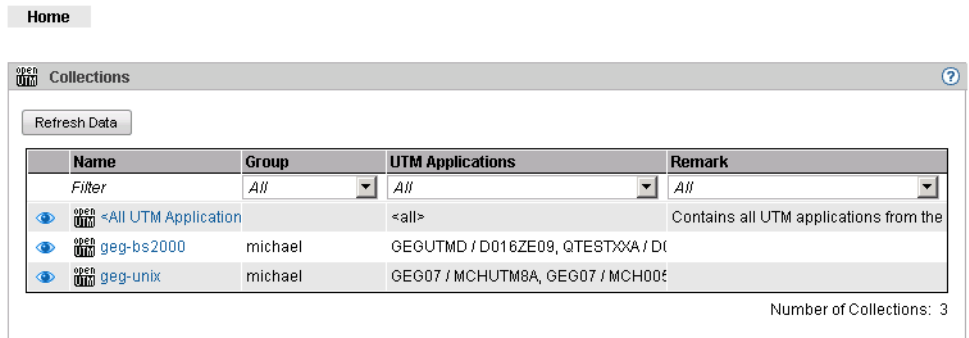
The display of the backup requests for each SE Manager is only possible when REWAS is active, see [section “Integration of BS2000 into the SE Manager” on page 36](#).

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.



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
<i>Filter</i>	<i>All</i>	<i>Filter</i>	<i>All</i>	<i>All</i>	
sci_meise_conf	ABBA	172.17.0.37.75,9058	RUNNING		
sci_meiseu_conf	ABBA	172.17.0.37.75,9059	STOPPED		
sci_meiseu_s	ABBA	172.17.0.37.75,9059	STOPPED		
sci_meise_s	ABBA	172.17.0.37.75,9058	DEFINED		
sci_star_conf	ABBA	172.17.0.36.133,9059	DEFINED		
fink_conf	ABBA	172.17.0.38.128,9058	DEFINED		
sci_i15_conf	ABBA	172.17.0.35.57,3000	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 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		
Filter	Filter	Filter	Filter	Filter		
abgqa500	OVMM	abgqa500.example.net:8001	qa500	admin		
abgqa600	OVMM	abgqa600.example.net:7002	qa600	admin		

Total: 2

- ▶ The *Change* and *Remove* icons enable you to change application properties (e.g. the name or description) 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.
- ▶ *Embed user-defined management application* enables you to integrate further applications into the SE Manager.



Currently, the only available user-defined management application is Oracle VM Manager (Type OVMM). You can use it to operate an Oracle VM Manager via its web interface. When integrating, 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 applications*, *Administration* tab.

In the *User-defined links* group the *Administration* tab displays the list of the user-defined links which are embedded in the SE Manager.

Name and description	URL	Unit	System		
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>		
BS2000-MSG	http://manuals.ts.fujitsu.com/files/html/bs200...	-	-		
OracleDB	https://19... 2.101	abgse1au87-3	linux-u2n4		

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.

- If you have a single-MU configuration and click on *Performance* in the tree structure, the welcome page of the openSM2 Managers opens. The layout is the same as the layout of the SE Manager.

The screenshot displays the openSM2 Manager interface. The top navigation bar includes 'openSM2 Manager', 'System Administrator', 'Log out', and 'FUJITSU'. Below this, the 'Management Unit (abgse2mu1)' is identified, along with 'DE' and 'Help' options. A left sidebar contains navigation links for 'SE Manager', 'Views', 'Overviews', 'Report views', 'Systems', 'System groups', 'Other systems', 'Settings', and 'Administration'. The main content area is divided into three sections:

- Systems**: Includes 'System properties' and 'Alarm messages'.
- Server systems**: Shows 'Showing 1 to 10 of 26 entries'. The table below lists system performance metrics.
- Storage systems**: Shows 'Showing 1 to 8 of 8 entries'. The table below lists storage performance metrics.
- Snmp systems**: Shows 'Showing 1 to 1 of 1 entries'. The table below lists snmp system details.

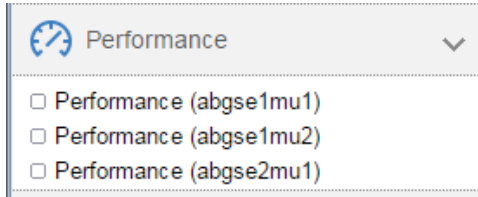
URL: <https://abgse2mu1.abg.fsc.net/opensm2/overview/show/#>

System	System type	CPU[%]		Mem[%]		Disk[IO/s]	
		From	to	From	to	From	to
abgse2mu1	Linux	49.4		39.9		1915.2	
ABOSE217	BS2000	16.0		71.4		136.4	
su1-se2	X2000	8.6		12.5			

System	Model	Data[MB/s]		IO[s]		Time[ms/IO]	
		From	to	From	to	From	to
Eternus+4621349005	STORMAN_STORAGE_MODEL_ETERNUS			621.0		1029.0	0.6
Eternus+4621347002	STORMAN_STORAGE_MODEL_ETERNUS			500.0		522.0	0.2
Eternus+4541142001	STORMAN_STORAGE_MODEL_ETERNUS			491.0		492.0	0.7

System	Description	InReceives[s]		OutRequests[s]	
		From	to	From	to
nswa1-se2	Brocade Communications Systems, Inc. Stacking System ICX8450-24, IronWare Version 08.0.20T31.3 Compiled on Sep 30 2014 at 02:38:23 labeled as ICX84R08020			12.1	12.9

If you have an SE server configuration with multiple MUs (MU redundancy or Management Cluster), the tree structure contains a submenu below *Performance*, which contains an entry *Performance (<mu-name>)* for each MU of the SE server configuration on which openSM2 is installed.



Click on an entry to open the welcome page of the openSM2 Manager of the respective MU.

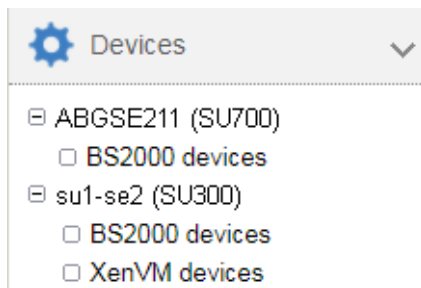
- ▶ You use the tree structure and tabs of openSM2 to call the functions of openSM2.
- ▶ *SE Manager* in the tree structure returns you to the SE Manager.

Further details on openSM2 are contained in the openSM2 User Guide [14].

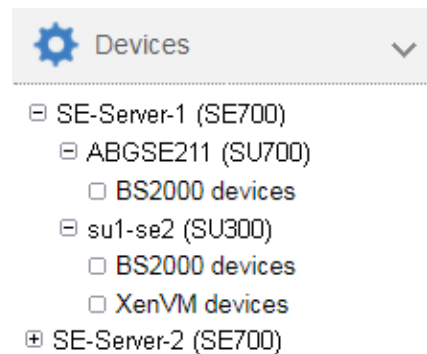
9 Managing devices

You manage the devices of the SE server using the *Devices* menu in the tree structure, see the example below:

Managing a single SE server
(ein SE700)



Managing two SE servers (two SE700)
in a Management Cluster



If you manage an SE server configuration with two SE servers in a Management Cluster, underneath *Devices* there will be a submenu *<se server>* (*SE<model>*) for each SE server, containing the devices of the respective SE server.

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 % NKRO042 'DEVICE   =AF': ATTACH ACCEPTED
%XAAE-000.165608 % NKRO116 ASSIGN FOR 'DEVICE=AF' IN PROCESS
% MSG-000.165608 % NKRO110 'DEVICE   =AF' ATTACHED AND ASSIGNED
! UCO-000.165608 % NBR0740 COMMAND COMPLETED 'ATTACH-DEVICE'; (RESULT:
SC2=000, SC1=000, MC=CMD0001); DATE: 2017-01-09
/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 "normal" disks and real tape devices, the devices visible to BS2000 on an SU /390 are emulated devices and not directly the real devices. The disks for the emergency system are emulated at the MU. On SU x86, all devices visible for BS2000 are emulated. The following designation is more precise than "emulated devices": BS2000 emulations of the real devices.

The device address must be specified when an emulated device is configured for BS2000. The names in X2000/M2000 for the channel path identifier and logical unit number (LUN) are Host Connector and Unit ID, with Unit ID corresponding to the host LUN.

Device address			
BS2000	X2000 / M2000	SU /390 (IORSF)	Periphery
Channel path identifier	Host Connector	Channel path identifier	-
Logical unit number	Unit ID	Logical unit number	Host-LUN or LUN

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. In addition, up to two disks of the type EMDISK are emulated for the emergency system of the SU /390 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. In the device overviews, the *Unit* and *Unit type* columns indicate the unit on which the device is emulated.

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 HNC, 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
EMDISK	CCF0_CCF1	00	F0_F1	2 emulated disks (e.g. for BS2000 emergency system)
KVP	C2_C3	00	C3_C4	Name: HV0
LOCLAN	CC80_CC81	00	80_81	Name: MANLO1 IP address: 192.168.138.21 Address space: 192.168.138.xx
CDROM	T0	00	60	Real CD-ROM drive
EMFILE	T1	00	61	emfile0061

Table 4: Predefined BS2000 devices on SU /390 (MU) (part 1 of 2)

Type	MN	HC	LUN	Details
<i>In the case of MU redundancy on MU2 (MU index 2):</i>				
EMDISK	CDF0_CDF1	00	F0_F1	optional: 2 emulated disks (e.g. for BS2000 emergency system)
KVP	C4_C5	00	C3_C4	Name: HV0
LOCLAN	CD80_CD81	00	80_81	Name: MANLO1 IP address: 192.168.139.21 Address space: 192.168.139.xx
CDROM	TA	00	60	Real CD-ROM drive
EMFILE	TB	00	61	emfile0061

Table 4: Predefined BS2000 devices on SU /390 (MU) (part 2 of 2)

On the HNC the following BS2000 devices are predefined for the SU /390:

Type	MN	HC	LUN	Details
LOCLAN	-	-	-	- Address space: 192.168.151.xx
ZASLAN	CC40_CC41	00	40_41	Name: MCNPR Slot: s2 p0 pci
<i>In the case of HNC redundancy on HNC2:</i>				
LOCLAN	-	-	-	- Address space: 192.168.152.xx
ZASLAN	CD40_CD41	00	40_41	Name: MCNPR Slot: s2 p0 pci

Table 5: Predefined BS2000 devices on SU /390 (HNC)



In case of a Management Cluster, these BS2000 devices are predefined on MU and HNC for the SU /390 on both SE servers as described above.

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 180](#).
- 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 177
- “Removing a KVP” on page 178
- “Add new LAN device” on page 180
- “Removing a LAN device” on page 180
- “Add new tape devices” on page 182
- “Remove tape device” on page 182

9.1.2.3 Configuration in IORSF files

- ▶ Select *Devices* → [*<se server>(SE<model>)* →] *<unit>(SU</390>)*, *ORSF files* tab.

ORSF files

Server Unit ABGSE211: IORSF files

Update IORSF file list

No.	File (description)	Date	Active	Planned
0	SU700001EM-2 29001 26, 10.10.2016	2017-01-10 11:07:30	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
1	SU700001SU700-29001 / AUSTAUSCH VTA500 - C88200 / 21.09.16	2016-10-12 15:23:48	<input type="checkbox"/>	<input type="checkbox"/>
2	SU700001SU700-29001 / CTL B000,B200, DVC FF00-FF67 / 26.07.16	2016-08-29 15:03:14	<input type="checkbox"/>	<input type="checkbox"/>

Total: 3

The *ORSF files* tab provides information about the IORSF files which are available on the MU.

- ▶ Click *Update IORSF file list* to update the file list and the device lists. This action is only possible if at least one of the associated MUs is in normal operation. The previous file list and the previous device lists are deleted and the current data are transferred from the SVP. The active IORSF file is edited implicitly, and the device lists in the *BS2000 devices* menu are refreshed.



The SE Manager always displays the devices which are contained in the current IORSF file on the SVP (*CURRENT level). Dynamic I/O configuration changes are initially performed in the active IORSF. The SE Manager can display these changes only if you write back the changed configuration to the relevant file on the SVP. Use the `/STOP-CONFIGURATION-UPDATE IORSF-UPDATE=*YES(LEVEL=...)` command in the BS2000 to do this. After that you have to run the *Update IORSF file list* action in the SE Manager.

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 Address: 192.168.138.21 Address space: 192.168.138.xx
ZASLAN	CC40_CC41	0C	40_41	Name: MCNPR Slot: s1 p0 pci
CDROM	CD	00	CD	Real CD-ROM drive
EMFILE	EF	00	EF	emfile00ef

Table 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.

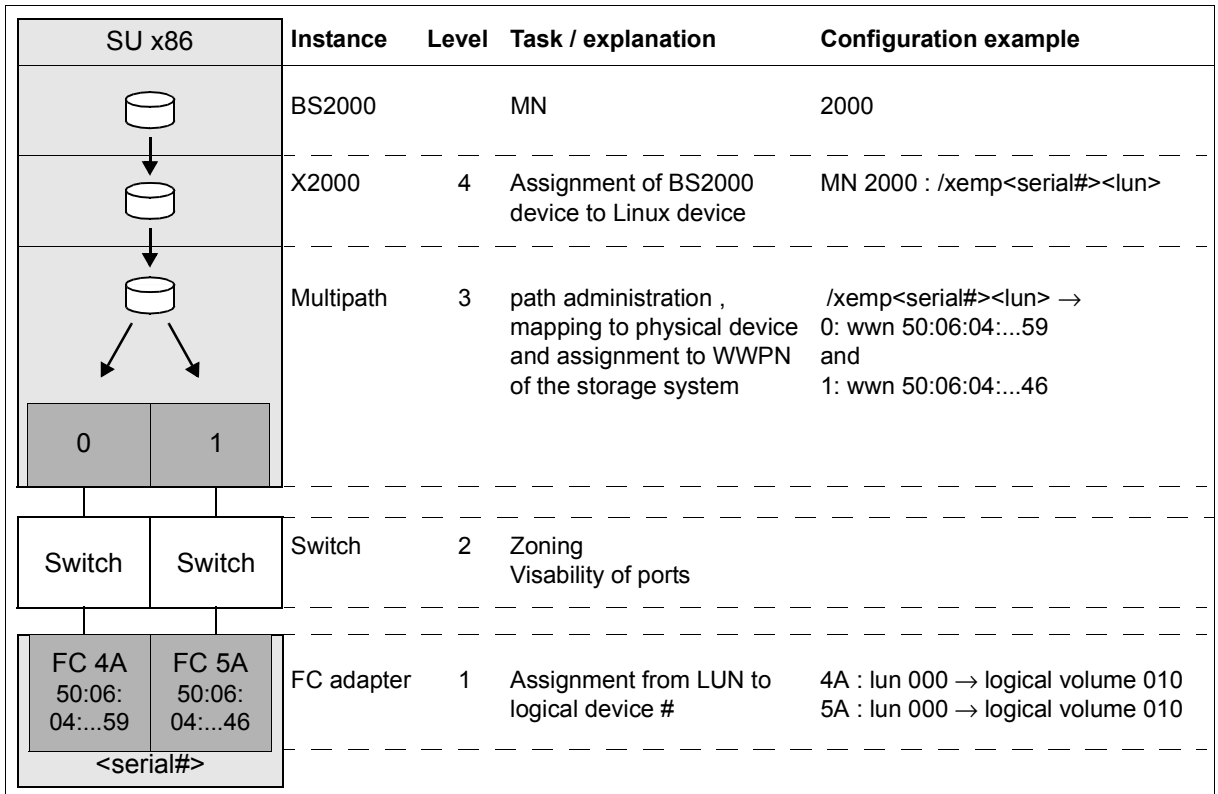


Figure 16: Device configuration on an SU x86 taking a disk storage system as an example

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** → [*<se server>*(SE*<model>*) →] *<unit>* (SU*</390>*) → *BS2000 devices*, *Disks* tab.

Disks | K/V/P | LAN | Tape devices

Server Unit ABGSE211: Disks (IORSF file: #1, 2017-05-14 12:54:17)

1 to 32 from 193 Page 1 from 7 Go to page 1 Per page 32

MN	HC	LUN	CHPID	Type	Code	WWPN	PAV	Unit	Unit type	Assigned
Filter	Filter	Filter	Filter	All	All	Filter	All	All	Filter	
9900	-	0900	70	IORSF	A5	50:06:44:84:52:A7:57:47	-	-	-	-
9900	-	0900	78	IORSF	A5	50:06:44:84:52:A7:57:58	-	-	-	-
9901	-	0901	70	IORSF	A5	50:06:44:84:52:A7:57:47	-	-	-	-
9901	-	0901	78	IORSF	A5	50:06:44:84:52:A7:57:58	-	-	-	-
9902	-	0902	70	IORSF	A5	50:06:44:84:52:A7:57:47	-	-	-	VM02
9902	-	0902	78	IORSF	A5	50:06:44:84:52:A7:57:58	-	-	-	VM02
9903	-	0903	70	IORSF	A5	50:06:44:84:52:A7:57:47	-	-	-	-
9903	-	0903	78	IORSF	A5	50:06:44:84:52:A7:57:58	-	-	-	-
9904	-	0904	70	IORSF	A5	50:06:44:84:52:A7:57:47	-	-	-	VM03
9904	-	0904	78	IORSF	A5	50:06:44:84:52:A7:57:58	-	-	-	VM03

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*, displays the VM.

9.1.4.2 Managing disks on Server Unit x86

Displaying disks

- Select *Devices* → [*<se server>(SE<model>)*] → *<unit> (SU<x86>)* → *BS2000-Geräte, Disks* tab.

MN	HC	Unit ID	Type	Device information	Size [MB]	Usage	Format	IPL	VSN	Assigned
1000	10	00	8F	-(raid0d3-part1)	-	-	-	-	-	-
1001	10	01	8F	raid1d6-part5	8189	Free disk	K2	-	-	-
1002	10	02	8F	raid1d7-part5	8191	Free disk	K2	-	-	-
1003	10	03	8F	raid1d8-part5	8189	Free disk	K2	-	-	-
1004	10	04	8F	raid1d10-part5	8189	Free disk	K2	-	-	-
1005	10	05	A5	601225-Disk115E	-	-	-	-	-	-
1006	10	06	A5	601225-Disk1162	-	-	-	-	-	-
1007	10	07	A5	601225-Disk1164	-	-	-	-	-	-
1008	10	08	A5	601225-Disk1166	-	-	-	-	-	-
1009	10	09	A5	601225-Disk1168	-	-	-	-	-	-
100A	10	0A	A5	601225-Disk116A	-	-	-	-	-	-
100B	10	0B	A5	601225-Disk116D	-	-	-	-	-	-
100C	10	0C	A5	601225-Disk116F	-	-	-	-	-	-
100D	10	0D	A5	DX000E100066-Disk20	20480	Pubset	NK2	/390	FC20.0	-
100E	10	0E	A5	DX000E100066-Disk21	20480	Pubset	NK2	/390	FC21.0	-
100F	10	0F	A5	DX000E100066-Disk22	20480	Pubset	NK2	/390	FC22.0	-

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.

Above the table the number of free licenses is displayed.



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 BS2000 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](#).

Update BS2000 data

- ▶ Click the *Update BS2000 data* icon and confirm the action.

Remove disk

The following requirements must 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 168](#) and [table 6 on page 171](#)). 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 112](#).



Recommendation:

Define precisely one KVP for each VM (in the case of SU /390 for each MU).

- ▶ **Select Devices** → [*<se server>(SE<model>)* →] *<unit> (SU<model>)* → *BS2000 devices, KVP* tab.

Disks | **KVP** | LAN | Tape devices

▼ Server Unit *su1se2*: KVP devices ?

Add new KVP Free licenses: 119

MN	HC	Unit ID	Name	Assigned	Status	Color			
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>All</i>				
AF_AG	00	08_09	HV2	-	UNUSED				
AH_AI	00	0A_0B	HVA	-	UNUSED				
AJ_AK	00	0C_0D	VM7	-	UNUSED				
Z0_Z1	00	04_05	HV0	MONITOR	NORMAL				
Z2_Z3	00	12_13	VM2	ABGAFR02	NORMAL				
Z4_Z5	00	14_15	VM3	ABGAFR03	NORMAL				
Z6_Z7	00	16_17	VM4	ABGAFR04	NORMAL				
Z8_Z9	00	18_19	VM5	ABGAFR05	NORMAL				
ZA_ZB	00	06_07	VM6	-	UNUSED				

Total: 9

▼ Server Unit *su1se2*: KVP logging files ?

KVP *HV0* ▼

Number	File name	File size [Bytes]		
1	KVPLOG.HV0.170821.140912	168,229		
2	KVPLOG.HV0.170821.124758.bz2	14,581		

Total: 2

The *KVP* tab with the *KVP devices* and *KVP logging* groups 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 178](#)).

Above the table the number of free licenses is displayed. Only for SU /390: When you drag the mouse cursor over the information symbol, a tool tip displays the number of licenses per MU.



Information on the generated KVP devices on SU /390

The devices are displayed only if the active 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).



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 *KVP devices* group, 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 *KVP devices* group, click on the *Change* icon by the required KVP and determine a new color code.

Restarting 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



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, click the *Remove* icon by the required KVP.

Displaying KVP logging file selectively



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 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 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 a connection via LOCLAN and the HNC via ZASLAN and LOCLAN.

On an SU x86, the BS2000 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 LAN device per VM.

- In the tree structure select *Devices* → [*<se server>(SE<model>)*] → *<unit> (SU<model>)* → *BS2000 devices, LAN tab*.

Disks | KVP | **LAN** | Tape devices

Server Unit *su1se2*: LAN devices

Add new LAN device Free licenses: 0 / 120 / 512 ⓘ FC interfaces IP interfaces

MN	HC	Unit ID	LAN type	Details	BS2 IP address	BS2 MAC address	Assigned	Status		
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>All</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>All</i>		
-	-	-	LOCLAN	--	192.168.1.38.12	0A:00:11:00:08:FF	-	-		
CC40_CC41	0C	40_41	ZASLAN	s8 p3 pci	-	00:11:00:00:67:00	MONITOR	↑ NORMAL		
CC42_CC43	0C	42_43	ZASLAN	s8 p3 pci	-	00:11:00:00:67:02	ABGAFR02	↑ NORMAL		
CC44_CC45	0C	44_45	ZASLAN	s8 p3 pci	-	00:11:00:00:67:03	ABGAFR03	↑ NORMAL		
CC46_CC47	0C	46_47	ZASLAN	s8 p3 pci	-	00:11:00:00:67:04	ABGAFR04	↑ NORMAL		
CC48_CC49	0C	48_49	ZASLAN	s8 p3 pci	-	00:11:00:00:67:07	ABGAFR05	↑ NORMAL		
CC80_CC81	0C	80_81	LOCLAN	MANLO1	192.168.1.38.21	0A:00:11:00:08:15	MONITOR	↑ NORMAL		
CC82_CC83	0C	82_83	LOCLAN	MANLO2	192.168.1.38.22	0A:00:11:00:08:16	ABGAFR02	↑ NORMAL		
CC84_CC85	0C	84_85	LOCLAN	MANLO3	192.168.1.38.23	0A:00:11:00:08:17	ABGAFR03	↑ NORMAL		
CC86_CC87	0C	86_87	LOCLAN	MANLO4	192.168.1.38.24	0A:00:11:00:08:18	ABGAFR04	↑ NORMAL		
CC88_CC89	0C	88_89	LOCLAN	MANLO5	192.168.1.38.25	0A:00:11:00:08:19	ABGAFR05	↑ NORMAL		
CC8A_CC8B	0C	8A_8B	LOCLAN	MANLO6	192.168.1.38.26	0A:00:11:00:08:1A	-	⊕ UNUSED		
CC8C_CC8D	0C	8C_8D	LOCLAN	MANLO7	192.168.1.38.27	0A:00:11:00:08:1B	-	⊕ UNUSED		
CC8E_CC8F	0C	8E_8F	LOCLAN	MANLO8	192.168.1.38.28	0A:00:11:00:08:1C	-	⊕ UNUSED		
CD40_CD41	0D	40_41	ZASLAN	s5 p0 pci	-	00:11:00:00:67:01	MONITOR	↑ NORMAL		
CD42_CD43	0D	42_43	ZASLAN	s5 p0 pci	-	00:11:00:00:67:06	ABGAFR02	↑ NORMAL		
CD44_CD45	0D	44_45	ZASLAN	s5 p0 pci	-	00:11:00:00:67:05	ABGAFR03	↑ NORMAL		

Total: 17

The *LAN* tab lists the configured LAN devices.

Above the table, the free licenses for LOCLAN, ZASLAN and, for SU x86, for BRGLAN are shown. When you drag the mouse cursor over the information symbol, a tool tip displays detailed license information.



Information on the generated LAN devices on SU /390

The devices are displayed only if the active 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).



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.

Removing 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 provides the following functions:

- ▶ Select *Devices* → [*<se server>(SE<model>)* →] *<unit> (SU<model>)* → *BS2000 devices, Tape devices* tab.

Example for SU x86:

Server Unit su1se2: Tape devices

Add new tape devices Remove real tape devices Free licenses: 128 / 1

MN	HC	Unit ID	Type	Model	Device information	Size [KB]	Assigned				
Filter	Filter	Filter	All	All	Filter	Filter	Filter				
	7C	EC	DATA	-	emfile7cec	331	-				
A9	00	00	EMFILE	-	emfile0000	0	-				
AA	13	12	EMFILE	-	emfile1312	4	-				
AB	00	02	EMFILE	-	emfile0002	170756	-				
AC	00	03	EMFILE	-	emfile0003	94551	-				
AE	7E	BA	EMFILE	-	emfile7eba	3173437	-				
CD	00	CD	CDROM	-	emfile	-	-				
EF55	00	55	EMFILE	-	emfile0055	0	-				

Total: 8

Example for SU /390:

Server Unit ABGSE211: Tape devices (IORSF file: #1, 2017-05-14 12:54:17)

Add new tape device Free licenses: 5

MN	HC	LUN	CHPID	Type	Code	Device information	Size [KB]	Unit	Unit type	Assigned			
Filter	Filter	Filter	Filter	All	All	Filter	Filter	All	All	Filter			
-	00	EB	-	DATA	-	emfile00eb	32	abgse2mu1	MU	-			
AA	00	04	-	EMFILE	-	emfile0004	60	abgse2mu1	MU	-			
AA	00	00	-	EMFILE	-	emfile0000	65	abgse2mu2	MU	-			
AAAA	00	02	-	EMFILE	-	emfile0002	67	abgse2mu1	MU	-			
AB	00	00	-	EMFILE	-	emfile0000	275	abgse2mu1	MU	-			
AB	00	01	-	EMFILE	-	emfile0001	23	abgse2mu2	MU	-			
AC	00	FF	-	EMFILE	-	emfile00ff	32	abgse2mu1	MU	-			
AD	00	03	-	EMFILE	-	emfile0003	71	abgse2mu1	MU	-			
T0	00	60	30	CDROM	-	emfile	-	abgse2mu1	MU	VM04A1			
T1	00	61	30	EMFILE	-	emfile0061	11	abgse2mu1	MU	-			
T2	00	62	30	EMFILE	-	emfile0062	67	abgse2mu1	MU	VM02			
TA	00	60	38	CDROM	-	emfile	-	abgse2mu2	MU	VM03			
TB	00	61	38	EMFILE	-	emfile0061	0	abgse2mu2	MU	-			
TF	00	FF	38	EMFILE	-	emfile00ff	1316	abgse2mu2	MU	-			

Total: 12

The *Tape devices* tab lists the configured tape devices. EMFILES without a tape assignment are displayed with the type DATA.

Above the table, the free licenses for real tape devices (only for SU x86) and CDROMs/EMFILES are displayed. When you drag the mouse cursor over the information symbol, a tool tip displays detailed license information.

*Information on the generated tape devices on SU /390*

The devices are displayed only if the active 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).



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

- ▶ On SU /390, click *Add new tape device* and on SU x86, click *Add new tape devices*.

In the *Add tape device/Add tape devices* wizard you can specify the required properties step by step. In the case of real tape devices of an SU x86, you can also enter 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:

Disks | KVP | LAN | **Tape devices**

Server Unit su2se2: Tape devices

Add new tape devices Remove real tape devices Free licenses: 128 / 4 ⓘ

MN	HC	Unit ID	Type	Model	Device information	Size [KB]	Assigned			
Filter	Filter	Filter	EMFILE	All	Filter	Filter	Filter			
990F	00	0F	EMFILE	-	emfile000f	0	-			
AE	00	0A	EMFILE	-	emfile000a	84419	-			
EF	00	EF	EMFILE	-	emfile00ef	0	-			

Total: 3 from 4

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.



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 [11]. 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-DEVICE 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 [11]. 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
- DVD-RAM
- DVD-RW / DVD+RW
- DVD-RAM

The end-of-tape processing depends on the size of the medium. The maximum net size of the CDRAM 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* → [*<se server> (SE<model>)* →] *<unit> (SU<x86>)* → *XenVM devices, Disk pools* tab.

Disk pools
Virtual disks
Virtual switches
Installation sources

Server Unit **su2-se1**: Disk pools

Disk pool	Storage system	Device information	vDisks	Size [MB]	Free [MB]		
<i>Filter</i>	<i>Filter</i>		<i>Filter</i>	<i>Filter</i>	<i>Filter</i>		
» 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	
» DX440S22_V628	DX000E100002		1	1	40956	0	
» DX8400_V024027	DX0B5D6A1005		4	1	199984	179504	
» 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	4892	
» DX8400_V3A1	DX0B5D6A1005		1	1	47420	0	
» DX8400_V3A2	DX0B5D6A1005		1	1	47420	316	
» aa1tpool1	DX000E10301C		1	3	3596	524	

Total: 25

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.



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



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 141](#)).

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
- Delete unassigned virtual disks
- ▶ **Select Devices** → [*<se server>(SE<model>)* →] *<unit> (SU<x86>)* → *XenVM devices, Virtual disks* tab.

Disk pools **Virtual disks** Virtual switches Installation sources

Server Unit **su2-se1**: Virtual disks

Delete unassigned virtual disks

Virtual disk	Disk pool	Size [MB]	Assigned	Selection
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	
DX440_L0171	DX440_V017	20480	No	<input type="checkbox"/>
DX440_L0172	DX440_V017	19456	No	<input type="checkbox"/>
DX440_L028	DX440_V028	39936	No	<input type="checkbox"/>
DX440_L029_1	DX440_V029	19456	No	<input type="checkbox"/>
DX440_L029_2	DX440_V029	20480	No	<input type="checkbox"/>
DX440S22_L628	DX440S22_V628	40956	No	<input type="checkbox"/>
DX8400_L024027_1	DX8400_V024027	20480	No	<input type="checkbox"/>
DX8400_L03C	DX8400_V03C	39936	No	<input type="checkbox"/>
DX8400_L03E2	DX8400_V03E	39996	No	<input type="checkbox"/>
DX8400_L3A0	DX8400_V3A0	10000	No	<input type="checkbox"/>

The *Virtual disks* tab displays information on all virtual disks.

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*

- ▶ By the required unassigned disk click the *Delete* icon 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* → [*<se server>(SE<model>)*] → *<unit> (SU<x86>)* → *XenVM devices, Virtual switches* tab.

Disk pools | Virtual disks | **Virtual switches** | Installation sources

Server Unit **su2-se1** Virtual switches ?

Create new virtual switch IP interfaces

Name	Slot / port	Assigned	Description	Status
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>
extbr0	s5 p1 pci	Yes	Ext. bridge pci s5p1	Normal
extbr1	s8 p2 pci, s12 p2 ior	Yes	lodtest	Failure
intbr0	-	Yes		Normal
intbr1	-	Yes	intern Test	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 145](#)).

- ▶ **Select Devices** → [`<se server>(SE<model>)`] → `<unit>` (`SU<x86>`) → *XenVM devices, Installation sources* tab.

Disk pools | Virtual disks | Virtual switches | **Installation sources**

Server Unit **su1-se2**: Installation sources Free local memory: 50 GB (from 79 GB)

Name	Assigned	Size	Date	
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	
linuxmint-17.2-cinnamon-64bit.iso	No	1555 MB	2017-03-30 07:03:24	▶
MV6.2A0000.A0606099-H01.iso.10.172.102.48.partial	No	5 MB	2017-07-06 14:33:29	▶
SLES-11-SP4-DVD-x86_64-GM-DVD1.iso	Yes	3228 MB	2017-03-10 10:46:02	▶
sles11.iso	No	2681 MB	2017-03-09 18:14:27	▶
suse-systest-7.6-post-GM-2.iso	Yes	47 MB	2017-03-15 13:26:13	▶

Total: 5

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.

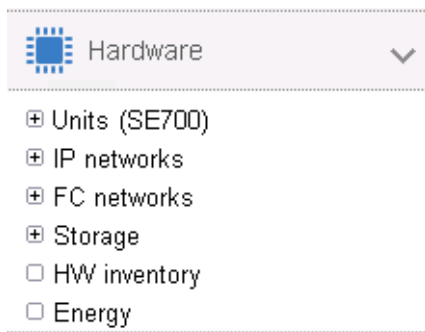
- ▶ Click *Upload information source* and select the required ISO image file in the browser dialog box.

After the update, the updated table displays the newly created ISO image file as an installation source in the local library.

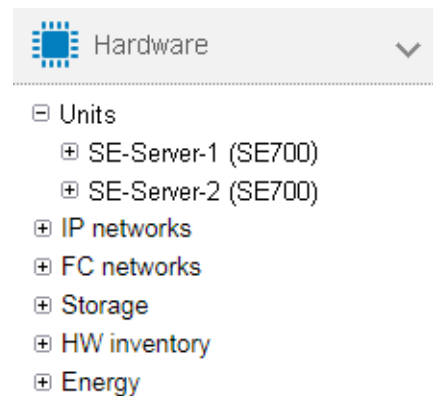
10 Managing hardware

You manage the hardware of the SE server configuration using the *Hardware* menu in the tree structure:

Managing a single SE server
(ein SE700)



Managing two SE servers (two SE700)
in a Management Cluster



The menu has the same layout for all SE servers and contains the following items:

- *Units*: Here you manage all existing units of the SE server configuration, see [section “Managing units of the SE server” on page 198](#).
- *IP networks*: Here you manage all private and public networks of the SE server configuration, see [section “Managing IP networks” on page 252](#).
- *FC networks*: Here you manage the Fibre Channel networks of the SE server configuration, see [section “Managing FC networks” on page 277](#).
- *Storage*: Here you manage the storage components of the SE server configuration, see [section “Managing storage systems” on page 281](#).
- *HW inventory*: Here you can have the hardware configuration displayed on the screen in graphic or tabular form, see [section “HW inventory” on page 285](#).
- *Energy*: Here you manage the energy settings of the SE server configuration, e.g. powering the units on or off automatically, see [section “Managing energy settings” on page 290](#).

10.1 Managing units of the SE server

You manage the units of the SE server using the menu *Hardware* → *Units (SE<model>)*. When you expand this menu, all the existing units are listed.

If you manage a configuration of two SE servers in one Management Cluster, the units are listed underneath *Units* in two SE server-specific submenus *Hardware* → *Units* → *<se server>(SE<model>)*.

10.1.1 Powering a unit on or off, rebooting a unit

- ▶ Select *Hardware* → *Units*, *Units* tab.

The *Units* tab displays information on all Management Units, Server Units, HNCs, and Application Units of the SE server configuration.

Name	HW model	Chassis	Server	Power status	System status	HW status
ABGSE211	SU700	-	SE-Server-1	ON	RUNNING	NORMAL
abgse1mu1	MU	-	SE-Server-1	ON	RUNNING	NORMAL
abgse1mu2	MU	-	SE-Server-1	ON	RUNNING	NORMAL
abgse1hnc1	HNC	-	SE-Server-1	ON	RUNNING	NORMAL
abgse1hnc2	HNC	-	SE-Server-1	ON	RUNNING	NORMAL
su2-se1	SU300	-	SE-Server-1	ON	RUNNING	NORMAL
su3-se1	SU300	-	SE-Server-1	ON	RUNNING	NORMAL
au5-se1	AU20	-	SE-Server-1	ON	RUNNING	NORMAL
au6-se1	AU47	-	SE-Server-1	ON	RUNNING	NORMAL
auc8-se1	DBU87	1541517004	SE-Server-1	ON	RUNNING	NORMAL
abgse1au87-1	DBU87-P	1541517004	SE-Server-1	ON	RUNNING	NORMAL



Notes:

- If, as in the example, at least one AU PQ is available, *HW model* is followed by an additional *Chassis* column. In the case of AU PQ, the chassis of the AU and the partitions are each displayed as single units. Actions are only possible for partitions.
- For a configuration consisting of two SE servers in a Management Cluster:
 - The *Units* menu does not contain a model name (it is displayed in the submenu of the respective SE server instead).
 - The table contains the additional *Server* column. This column contains the name of the SE server to which the respective unit belongs.

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



On an SU /390 without connection to the hardware interface for switching on / off, the *Power on* or *Power off* icon is not active and a tool tip displays the cause.

Powering on the unit

Depending on the situation and the status, the action may not be available. A tooltip then informs about the reason.

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)

Depending on the situation and the status, the action may not be available. A tooltip then informs about the reason.



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

Depending on the situation and the status, the action may not be available. A tooltip then informs about the reason.

Procedure

- ▶ Click the *Power off* icon by the required unit.
- ▶ In the subsequent dialog box, select the option *Shut down* or *Power off immediately* and confirm the action with *Execute*.



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 SE servers of the Management Cluster

If you have a Management Cluster, you can view specific information on each of the SE servers in that cluster.

- ▶ Select *Hardware* → *Units* → *<se server>* (*SE<model>*), *Information* tab.

Information

Server SE-Server-1: Information	
Name	SE-Server-1
Model	SE700B
SE index	1
Location	Location 1

When creating the cluster, Customer Support specifies the name of the SE server, the model, the SE index and the location.

10.1.3 Managing the Server Unit /390

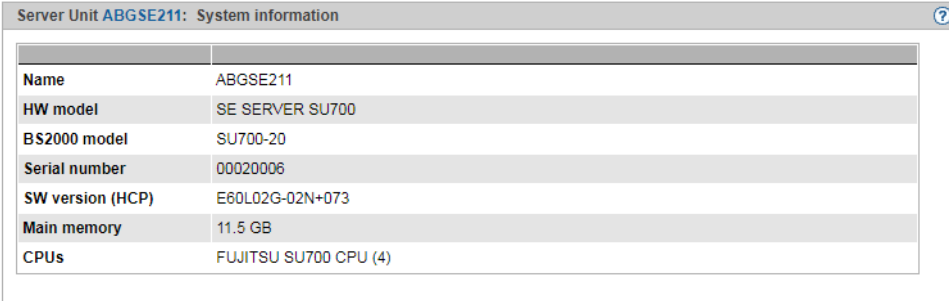
10.1.3.1 Displaying system information and interfaces of the SU /390

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* → *Units*[→ <se server> (*SE*<model>)] → <unit> (*SU*</390>) → *Information*, *System* tab.

System | FC interfaces



Server Unit ABGSE211: System information	
Name	ABGSE211
HW model	SE SERVER SU700
BS2000 model	SU700-20
Serial number	00020006
SW version (HCP)	E60L02G-02N+073
Main memory	11.5 GB
CPUs	FUJITSU SU700 CPU (4)

Displaying FC interfaces of the SU /390

- ▶ Select *Hardware* → *Units* [→ <se server> (SE<model>)] → <unit> (SU</390>) → *Information*, *FC interfaces* tab.

System **FC interfaces**

▼ Server Unit **ABGSE211**: FC interfaces

CHPID	CHE box	Slot / port	WWPN	Status
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>All</i>
00	0	s0 p1	-	-
02	0	s1 p1	20:02:00:.....:00C:E3	UP
03	0	s1 p2	20:03:00:.....:00C:E3	UP
07	0	s3 p2	20:07:00:.....:00C:E3	UP
08	0	s4 p1	20:08:00:.....:00C:E3	UP

Total: 3

▼ Server Unit **ABGSE211**: FC targets

WWPN storage

<i>Filter</i>
10:00:00:.....:AA:2A
10:00:00:.....:E6:00
10:00:00:.....:1A:04
10:00:00:.....:1A:EC
10:00:00:.....:7E:18

Total: 99

▼ Server Unit **ABGSE211**: FC paths

Unit				FC target	
CHPID	CHE box	Slot / port	WWPN	Port address	WWPN
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>
08	0	s4 p1	20:08:00:.....:0C:E4	00 00 E8 ⓘ	10:00:00:.....:7:1A:04
09	0	s4 p2	20:09:00:.....:0C:E4	00 00 E8 ⓘ	10:00:00:.....:B:E6:00
0A	0	s5 p1	20:0A:00:.....:0C:E3	65 08 00	50:00:00:.....:30:1C:80
0A	0	s5 p1	20:0A:00:.....:0C:E3	68 4D 00	50:00:00:.....:4:98:5E
0A	0	s5 p1	20:0A:00:.....:0C:E3	66 12 00	50:00:00:.....:3:25:98
0A	0	s5 p1	20:0A:00:.....:0C:E3	68 2F 00	50:00:00:.....:80:47:21

10.1.3.2 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* → *Units*[→ <se server> (*SE*<model>)] → <unit> (*SU*</390>) → *Management, IP Configuration* tab.

IP configuration

Server Unit ABGSE211: IP configuration (SVP networks)				
SVP network	IP address	Management Unit	Usage	Status
MSNPR0	10.0.1.44	abgse1mu1	ACTIVE	✔ NORMAL
MSNPR0	10.0.1.45	abgse1mu2	PASSIVE	✔ NORMAL
MSNPR1	10.0.2.44	abgse1mu1	PASSIVE	✔ NORMAL
MSNPR1	10.0.2.45	abgse1mu2	PASSIVE	✔ NORMAL

Total: 4

Server Unit ABGSE211: Management Unit connections

SVP network	Status
MSNPR0	✔ NORMAL
MSNPR1	✔ NORMAL

Total: 2

10.1.4 Managing the Management Unit

10.1.4.1 Displaying system information and interfaces of a Management Unit

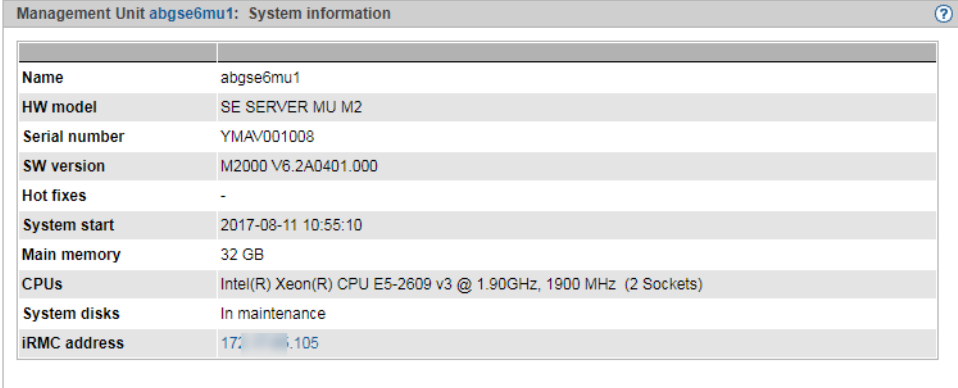
You obtain the system information and interfaces of a Management Unit using the associated *Information* menu. Options provided in this menu:

- [Displaying system information of the MU](#)
- [Displaying and changing IP interfaces of the MU](#)
- [Displaying FC interfaces of the MU](#)
- [Displaying multipath disks of the MU](#)
- [Displaying configuration disks of the MU](#)

Displaying system information of the MU

- Select *Hardware* → *Units*[→ *<se server> (SE<model>)*] → *<unit> (MU)* → *Information*, *System* tab:

System | IP interfaces | FC interfaces | Multipath disks | Configuration disks



Management Unit abgse6mu1 : System information	
Name	abgse6mu1
HW model	SE SERVER MU M2
Serial number	YMAV001008
SW version	M2000 V6.2A0401.000
Hot fixes	-
System start	2017-08-11 10:55:10
Main memory	32 GB
CPUs	Intel(R) Xeon(R) CPU E5-2609 v3 @ 1.90GHz, 1900 MHz (2 Sockets)
System disks	In maintenance
iRMC address	172.16.1.105




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* → *Units* [→ <se server> (SE<model>)] → <unit> (MU) → *Information, IP interfaces* tab:

System | **IP interfaces** | FC interfaces | Multipath disks | Configuration disks

Management Unit **abgse6mu1**: IP interfaces ?

Slot / port	MTU	Type	MAC address	Usage	Status	
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	All ▼	
-	1500	-	0A:00:14:10:20:FF	LOCLAN	-	
s0 p1 onboard	1500	Emulex Corporation OneConnect NIC (Skyhawk) (re...	90:1B:0E:AE:6C:D8	SYS1	 UP	
s0 p2 onboard	1500	Emulex Corporation OneConnect NIC (Skyhawk) (re...	90:1B:0E:AE:6C:D8	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* → *Units*[→ <se server> (*SE*<model>)] → <unit> (*MU*) → *Information*, *FC interfaces* tab:

System | IP interfaces | **FC interfaces** | Multipath disks | Configuration disks

▼ Management Unit **abgse4mu1-1**: FC interfaces ?

HC	Slot / port	Type	WWPN	CHPID	Status
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>All</i>
-	s3 p1 pci	Emulex LPe12002	10.00:.....:37:ae:85	-	UP
00	s3 p0 pci	Emulex LPe12002	10.00:.....:37:ae:84	40	UP

Total: 2

▼ Management Unit **abgse4mu1-1**: FC targets ?

WWPN Storage

Filter

50.00.00:.....:00:02:80
50.00.00:.....:00:54:26

Total: 2

Management Unit **abgse4mu1-1**: FC paths ?

Unit		Storage	
Slot / port	WWPN	Port address	WWPN
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>
s3 p1 pci	10.00:.....:37:ae:85	68 2E 00	50.00:.....:a:80:54:26
s3 p1 pci	10.00:.....:37:ae:85	67 13 00	50.00:.....:4:00:02:80

Total: 2

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 **I**D - 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* → *Units*[→ <se server> (SE<model>)] → <unit> (MU) → *Information*, *Multipath disks* tab:

System | IP interfaces | FC interfaces | **Multipath disks** | Configuration disks

Management Unit **abgse2mu1**: Multipath disks

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:c9:6d:30:bd	33	ALIVE
601225-Disk1184	Symmetrix	c99700	50:00:09:72:08:13:25:21	s3 p1 pci	UP	10:00:00:00:c9:6d:30:bd	34	ALIVE
DX000E2A0761-Disk120	Eternus	3d1500	50:00:00:e0:da:87:61:24	s4 p0 pci	UP	10:00:00:90:fa:a9:be:c4	00	ALIVE
DX000E2A0761-Disk120	Eternus	3d1500	50:00:00:e0:da:87:61:24	s4 p1 pci	UP	10:00:00:90:fa:a9:be:c5	00	ALIVE

Total: 4

Displaying configuration disks of the MU

The *Configuration disks* tab in the *Information* menu displays the status of the internal and, if existing, the external configuration disks of the Management Unit.

Purpose and operation of configuration disks are described in [section “External configuration disks” on page 42](#).

- ▶ Select *Hardware* → *Units*[→ <se server> (SE<model>)] → <unit> (MU) → *Information*, *Configuration disks* tab:

Management Unit **abgse6mu1**: Configuration disks

Index	Device	Status	Description
Filter	Filter	All	Filter
1	raid0d4	NORMAL	intern
2	601225-Disk1183	NORMAL	SE_CRD_OS7_SE1
3	601225-Disk1184	NORMAL	SE_CRD_OS7_SE2

Total: 3

The table lists the configuration disks with the current status. The internal configuration disk is listed before any possibly existing external configuration disks. The *Description* column can contain additional information on the use of the configuration disk.


10.1.4.2 Managing the IP configuration

You manage the IP configuration of the Management Unit using the associated *Management* menu, *IP configuration* tab.





- ▶ Select *Hardware* → *Units*[→ <se server> (SE<model>)] → <unit> (MU) → *Management*, *IP configuration* tab.

IP configuration | Routing & DNS | SNMP | System time | CLI

Management Unit **abgse2mu1**: Host name ?

abgse2mu1.example.net 





Management Unit **abgse2mu1**: Network properties ?

Network	Properties				
<i>Filter</i>					
DANPR01	<input type="checkbox"/> DHCPv4	<input checked="" type="checkbox"/> IPv6	<input checked="" type="checkbox"/> Autoconf	<input type="checkbox"/> DHCPv6	
DANPR04	<input type="checkbox"/> DHCPv4	<input checked="" type="checkbox"/> IPv6	<input checked="" type="checkbox"/> Autoconf	<input type="checkbox"/> DHCPv6	
MANPU	<input type="checkbox"/> DHCPv4	<input checked="" type="checkbox"/> IPv6	<input checked="" type="checkbox"/> Autoconf	<input type="checkbox"/> DHCPv6	
MCNLO	<input type="checkbox"/> DHCPv4	<input checked="" type="checkbox"/> IPv6	<input checked="" type="checkbox"/> Autoconf	<input type="checkbox"/> DHCPv6	
MCNPR	<input type="checkbox"/> DHCPv4	<input checked="" type="checkbox"/> IPv6	<input checked="" type="checkbox"/> Autoconf	<input type="checkbox"/> DHCPv6	
MONPR01	<input type="checkbox"/> DHCPv4	<input checked="" type="checkbox"/> IPv6	<input checked="" type="checkbox"/> Autoconf	<input type="checkbox"/> DHCPv6	
MSNPR0	<input type="checkbox"/> DHCPv4	<input checked="" type="checkbox"/> IPv6	<input checked="" type="checkbox"/> Autoconf	<input type="checkbox"/> DHCPv6	
MSNPR1	<input type="checkbox"/> DHCPv4	<input checked="" type="checkbox"/> IPv6	<input checked="" type="checkbox"/> Autoconf	<input type="checkbox"/> DHCPv6	

Total: 8

Management Unit **abgse2mu1**: Network IP addresses ?

Add new IP address

Network	IP address	Mask	Name	Conf.	
<i>Filter</i>					
DANPR01	fe80::921b:eff:feae:6cd8	/64	-	static	
DANPR04	fd5e:5e5e:804::201	/64	-	static	
DANPR04	fe80::921b:eff:feae:6cd8	/64	-	static	
LOCLAN	192.168.139.12	-	-	-	
MANPU	17. . . . 04	/22	abgse2mu1.example.net	static	

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.

Deleting the IP address

- ▶ In the *Network IP addresses* group click the *Delete* icon by the required IP address and confirm the action.

10.1.4.3 Managing routing of the Management Unit

You manage routing of the Management Unit using the associated *Management* menu, *Routing & DNS* tab.

- ▶ Select *Hardware* → *Units* [→ <se server> (*SE*<model>)] → <unit> (*MU*) → *Management*, *Routing & DNS* tab.

Target	Gateway	Usage
Filter	Filter	Filter
10.0.1.0/24	10.0.1.45	MSNPR0
10.0.2.0/24	10.0.2.45	MSNPR1
10.10.1.0/24	10.10.1.5	MONPR01
127.0.0.0/8	-	-
17...0/22	17...3.104	MANPU
192.168.11.0/24	192.168.11.2	MCNLO
192.168.139.0/24	192.168.139.12	-
default	17...34.1	MANPU

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.

10.1.4.4 Managing the DNS configuration

You manage the DNS configuration of the Management Unit using the associated *Management* menu, *Routing & DNS* tab.

- ▶ Select *Hardware* → *Units* [→ <se server> (*SE*<model>)] → <unit> (*MU*) → *Management*, *Routing & DNS* tab.

The screenshot shows the configuration page for Management Unit **abgse2mu1**. The **Routing & DNS** tab is active. The **DNS configuration: Static** section is expanded, showing two configuration tables. The **DNS name server** table lists three servers: 1. fd5e:5e5e:600::201, 2. 17: : .17, and 3. 17: : 249. The **DNS domain** table lists two domains: 1. abg.example.net and 2. mch.example.net. Buttons for 'Change DNS name servers' and 'Change DNS domains' are visible above the respective tables.

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.



The MU is preconfigured as a DNS server for the internal domain "senet" via the internal LAN (IPv6 address fd5e:5e5e:600::101). This entry cannot be removed.

Changing the DNS domains and DNS search sequence of the MU or removing a domain

- ▶ In the *DNS configuration* group select one of the following procedures:
 - ▶ To change DNS domains or the DNS search sequence, click *Change DNS domains*, and confirm the action after the change.
 - ▶ 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.

10.1.4.5 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`

At the Management Units and Server Units x86, ServerView RAID periodically checks hardware components. These events are reported by trap, even in good case with the weight NOTIFICATION. Text example of such a successful test: "*Patrol Read started*" and "*Patrol Read finished*".

In order for ServerView RAID's traps to be correctly represented by the management station, the MIB `/usr/share/snmp/mibs/FSC-RAID-MIB.txt` must be imported to the management station.



The traps usually contain neither the trap weight nor the message text. This information can only be read from the MIB.

Access to these MIB files on the Management Unit is, for example, possible under any administrator account with `scp` (secure copy).

- ▶ Select *Hardware* → *Units*[→ <se server> (*SE*<model>)] → <unit> (*MU*) → *Management, SNMP* tab:

IP configuration | Routing & DNS | **SNMP** | System time | CLI

Management Unit *abgse2mu1*: Configuration of local system data ?

SYSLOCATION	ABG DC 6a	
SYSCONTACT	Admin Tel. 1234	

Management Unit *abgse2mu1*: Allowed read accesses ?

Read community	Restricted to	
icinga	icinga.example.net	

Total: 1

Management Unit *abgse2mu1*: Trap receiver ?

Trap receiver	Trap community	SNMP version		
<i>Filter</i>	<i>Filter</i>	All		
icinga.example.net	icinga	SNMPv1		
icinga.example.net	icinga	SNMPv2c		

Total: 2

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* icon, and in the subsequent dialog box make changes to the system file.



The SE Manager displays the **SYSLOCATION** in the header. In a Management Cluster, **SYSLOCATION** should be the same as the Location of the Unit's SE server.

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.

Send 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.

10.1.4.6 Setting the system time (time synchronization or local)

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).

The Management Units are available as NTP servers for all units of the server via the private management network **MCNPR**. SU x86 and HNC are preconfigured with respect to NTP; AU configuration must be performed as required by the administrator responsible.

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. Refer to [section "Time synchronization" on page 65](#).

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 [10].

- ▶ Select *Hardware* → *Units*[→ <se server> (*SE*<model>)] → <unit> (*MU*) → *Management, System time* tab:

IP configuration | Routing & DNS | SNMP | **System time** | CLI

Management Unit **abgse2mu2**: Time synchronization with NTP server ?

Host name	IP address	Stratum	Time difference	Status	
abgse2mu1.senet	fd5e:5e5e:600::101	3	-0.002152	Active	✕

Total: 1

Management Unit **abgse2mu2**: Local configuration ?

✎	
Date	2017-08-23
Time	19:01:19
Time zone	CEST (UTC+02:00)
Stratum	9

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.



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 214](#).

- ▶ In the *Local time* group click the *Change* icon, and after making the necessary entries confirm the action.

10.1.4.7 Entering CLI commands

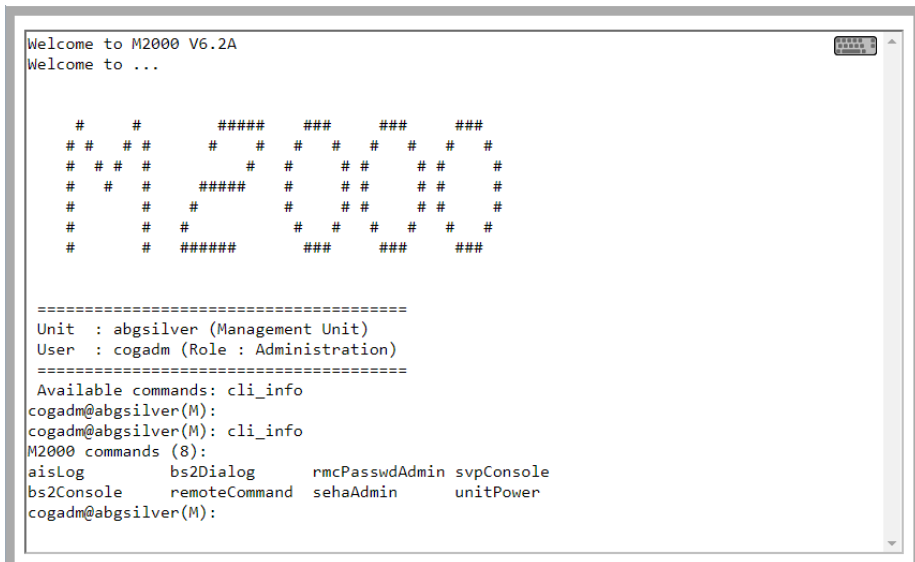
The SE Manager offers the administrator access to the CLI (**C**ommand **L**ine **I**nterface) on the Management Unit.

- ▶ Select *Hardware* → *Units*[→ <se 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 83](#).



```

Welcome to M2000 V6.2A
Welcome to ...

# # ##### ## ## ##
# # # # # # # # # #
# # # # # # # # # #
# # # ##### # # # # #
# # # # # # # # # #
# # # ##### ## ## ##

=====
Unit : abgsilver (Management Unit)
User : cogadm (Role : Administration)
=====
Available commands: cli_info
cogadm@abgsilver(M):
cogadm@abgsilver(M): cli_info
M2000 commands (8):
aisLog      bs2Dialog    rmcPasswdAdmin svpConsole
bs2Console  remoteCommand sehaAdmin      unitPower
cogadm@abgsilver(M):

```

10.1.4.8 Managing updates of the Management Unit

The administrator uses the *Update* tab to manage updates for the Management Units.

Updates extend the system or the M2000 basic software of the MU:

- Add-on packs enhance the basic software and are functional software components which have their own version schema.
- Security fixes contain selected software packages of the basic software and close security gaps.
- Hot fixes solve customer-specific problems.

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 69](#) and [section “Tasks of the customer” on page 69](#)):

- 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 *Update* tab provides you with information on the current status of the updates:

- ▶ Select *Hardware* → *Units* [→ <se server> (SE<model>)] → <unit> (MU) → *Service, Update* tab.

Update | CSR | Diagnostics | Remote Service

Management Unit **abgse2mu1**: SW version **V6.2A0401.000** ?

Transfer update from CD/DVD to system

▼ Add-on packs ?

Upload add-on pack

Add-on pack	Installation type	Installation	Status				
<i>Filter</i>	All	All	All				
OPENSM2-11.0.0-1.0	Online	Not installed	-	👁	🔌	📄	➡
OPENSM2-11.0.0-2.0	Online	Installed	▶ RUNNING	👁	🔌	📄	➡
OPENUTM-6.4-1.7	Online	Installed	▶ RUNNING	👁	🔌	📄	➡
ROBAR-70A11-1.0	Online	Not installed	-	👁	🔌	📄	➡
ROBAR-75A04-1.0	Online	Installed	▶ RUNNING	👁	🔌	📄	➡
STORMAN-7.0.1-2.0	Online	Installed	▶ RUNNING	👁	🔌	📄	➡

Total: 6

▶ Security fixes No security fix available 0 (0) ?

▶ Hot fixes No hot fix available 0 (0) ?

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 *Update* 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.
- *Add-on packs* group
The customer can upload, install, and uninstall add-on packs or delete add-on packs which have not been installed. They can view the readme file for the available add-on packs.
Installation and uninstallation of add-on packs have an immediate effect on the SE Manager (e.g. adjustment of the tree structure). The add-on is started automatically after the installation.
If the add-on supports that functionality, the customer can manually change the status of the add-on pack via the startup-symbol (e.g. Start, Stop, Restart, Reload).

- *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.
- *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 69](#) and [section “Tasks of the customer” on page 69](#)).

10.1.4.9 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 all configuration data that the customer manages themselves via the SE Manager.

Each backup archive has a creation date and an archive name. The backup archive contains MU-specific data (e.g. BS2000 devices or host name) and MU-global data (e.g. accounts). When restoring the data from the backup archive, this distinction **must** be taken into account.



Recommendation: Perform a CSR backup after every configuration change. In a single-MU configuration, you can use a CSR backup to recreate the configuration of the unit as of the time of the backup. In a multi-MU configuration, there is a difference between MU-specific and MU-global data (see the **Important information** under “[Restoring configuration data from a file archive](#)” on page 221).

You manage the configuration data of the Management Unit using the associated *Service* menu, *CSR* tab.

- ▶ Select *Hardware* → *Units*[→ <se server> (*SE*<model>)] → <unit> (*MU*) → *Service*, *CSR* tab.

Update | **CSR** | Diagnostics | Remote Service

Management Unit **abgblack**: Configuration data backup ?

Execute configuration data backup (CSR) Upload configuration data backup (CSR)

Date created	Archive name			
<i>Filter</i>	<i>Filter</i>			
2017-08-11 09:21:53	MU-M2_MV6.2A0400_abgse2mu2__2			
2017-08-11 07:13:28	MU-M2_MV6.2A0400_abgse2mu2__1			
2017-08-10 16:12:13	MU-M2_MV6.2A0400_abgse2mu2__2			
2017-08-08 07:21:18	MU-M2_MV6.2A0400_abgse2mu2			
2017-07-07 06:54:27	MU-M2_MV6.2A0400_abgse2mu2__test2			
2017-07-06 09:06:00	MU-M2_MV6.2A0400_abgse2mu2__test			
2017-06-29 07:26:57	MU-M2_MV6.2A0305_abgse2mu2__before_62A0400			
2017-05-15 16:44:44	MU-M2_MV6.2A0305_abgse2mu2			
2017-05-04 07:40:53	MU-M2_MV6.2A0304_abgse2mu2__before_62A0305			

Total: 9

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.



Ensure to only upload the configuration data backups of the associated unit!

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.



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.



Important information

- For MU-specific data:
The current MU-specific data are replaced by the old data.
- For MU-global data:
The current MU-global data are not changed, only old, no longer existing MU-global data are restored.
The MU-global data are the configured authorizations (accounts, LDAP configuration, IP based access rights), the configuration of the alarm management, the configured Application Units, the configured applications, the configuration of the FC networks, the configured SU Clusters.

10.1.4.10 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* → *Units* [→ *<se 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>.<date>.<time>.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.

10.1.4.11 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).

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.



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.

External assets

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).



External assets are only possible when the MU is connected directly, but not via a gateway.

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* → *Units*[→ *<se server> (SE<model>)*] → *<unit> (MU)* → *Service*, *Remote Service* tab.

The *Remote Service* tab displays the groups *Service access Management Unit*, *Service access external assets* (if at least on service access to an external assets is configured), *AIS Connect Sessions*, *AIS Connect Proxy configuration* and *AIS Connect Service agent*.

Update | CSR | Diagnostics | **Remote Service**

Management Unit **abgse2mu2: AIS Connect** ?

Service access Management Unit

Asset name	Access status	
YLEG001029	Access allowed, shadow possible	

Shadow terminal for: System Administrator (admin)

Service access external assets

Asset name	Description	IP address	Access status	
pig	Eternus DX 410	172.16.174	Access not allowed	
pighthtp	eternus dx 410	172.16.174	Access allowed	
se2mu2lrnc	iRMC abgse2mu2	172.16.97	Access allowed	

AIS Connect Sessions

Asset name	Description	Account	Session ID
-	-	-	-

AIS Connect Proxy configuration

IP address	Port	Account
172.16.9.4	81	-

AIS Connect Service agent

Status	
RUNNING	

Changing the service access

- ▶ In the *Service access Management Unit* or *Service access external assets* group, click on the *Change* icon next to the required asset. In the subsequent dialog box select one of the available access settings and confirm the action.

Opening a shadow terminal

The functionality is restricted for users without administrator rights:

- For AU- and XenVM-administrators, the whole main window is not displayed.
- BS2000 administrators can control the shadow terminal.
- An operator can only control the shadow terminal if he/she has an individual authorization.

- ▶ 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, the process ID (pid) of the AIS Connect session is displayed for you in the format `<pid1>.<pid2>.<pid3>` 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 display open sessions.

Displaying the current usage of the service access / deleting a session

The *AIS Connect Sessions* group displays the sessions that currently use the service accesses to the Management Unit and to the external assets.



External assets are only possible when the MU is connected directly, but not via a gateway.

- ▶ To delete an AIS Connect session (i.e. abort), click the *Delete* icon next to the required AIS Connect session in the *AIS Connect Sessions* group and confirm this action. Deletion takes place asynchronously.

Entering/changing or deleting a proxy configuration

- ▶ To enter or change a proxy configuration, in the *AIS Connect Proxy configuration* group 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 *AIS Connect Proxy configuration* group, click the *Delete* icon by the required proxy server for AIS and confirm the action.

Rebooting a service agent

- ▶ In the *AIS Connect Service agent* group click the *Restart* icon 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 216](#).



The administrator should delete the logging files at regular intervals, to prevent the file system from overflowing.

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.

10.1.5 Managing the HNC

10.1.5.1 Displaying system information and interfaces of the HNC

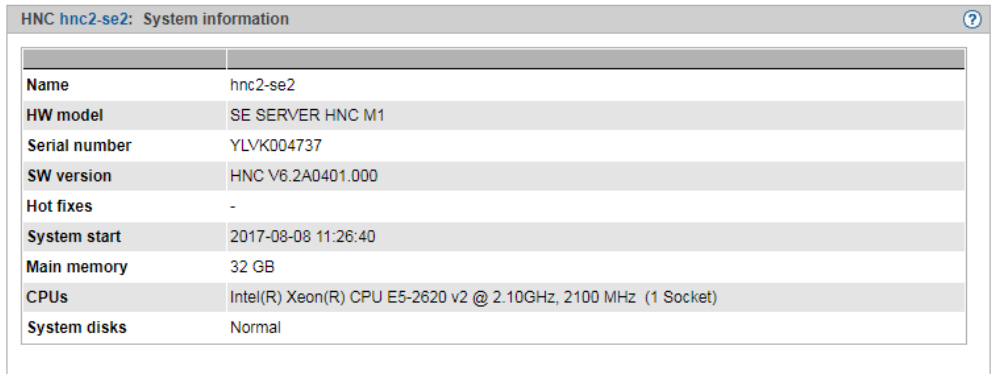
The *Information* menu provides you with information about the HNC and its interfaces.

- [Displaying system information of the HNC](#)
- [Displaying IP interfaces of the HNC](#)
- [Displaying FC interfaces of the HNC](#)
- [Displaying configuration disks of the HNC](#)

Displaying system information of the HNC

- Select *Hardware* → *Units*[→ <se server> (*SE*<model>)] → <unit> (*HNC*) → *Information*, *System* tab:

System | IP interfaces | FC interfaces | Configuration disks



HNC hnc2-se2: System information

Name	hnc2-se2
HW model	SE SERVER HNC M1
Serial number	YLVK004737
SW version	HNC V6.2A0401.000
Hot fixes	-
System start	2017-08-08 11:26:40
Main memory	32 GB
CPUs	Intel(R) Xeon(R) CPU E5-2620 v2 @ 2.10GHz, 2100 MHz (1 Socket)
System disks	Normal

Displaying IP interfaces of the HNC

- ▶ Select *Hardware* → *Units*[→ <se server> (SE<model>)] → <unit> (HNC) → *Information*, *IP interfaces* tab:

System | **IP interfaces** | FC interfaces

HNC hnc1-se2: IP interfaces ?

Slot / port	MTU	Type	MAC address	Usage	Status	
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	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 SFP/SFP+	90:1B:0E:0B:55:E4	ZASLAN	UP	
s1 p1 pci	1500	Intel Corporation 82599EB 10-Gigabit SFP/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* → *Units* [→ <se server> (SE<model>)] → <unit> (HNC) → *Information, FC interfaces* tab:

System | IP interfaces | **FC interfaces** | Configuration disks

▼ HNC hnc2-se2: FC interfaces ?

HC	Slot / port	Type	WWPN	CHPID	Status
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>All</i>
00	s3 p0 pci	Emulex LPe11002	10:00 9:6d:af:40	34	UP
01	s3 p1 pci	Emulex LPe11002	10:00 9:6d: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 plug-in position (slot and port) and the local WWPN (**World Wide Port Number**) are displayed for each FC interface. The hardware status of the FC interface is also displayed (*UP/DOWN*).

Displaying configuration disks of the HNC

The *Configuration disks* tab displays the status of the unit's internal configuration disks.

- Select *Hardware* → *Units* [→ <se server> (SE<model>)] → <unit> (HNC) → *Information, Configuration disks* tab:

The structure of the tab is the same as that for the MU (see [“Displaying configuration disks of the MU” on page 207](#)).

10.1.5.2 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* → *Units*[→ <se server> (*SE*<model>)] → <unit> (*HNC*) → *Management*, *IP configuration* tab.

IP configuration Routing & DNS Net-Storage

HNC hnc2-se2: Host name ?

hnc2-se2.senet ✎

▼ HNC hnc2-se2: Network properties ?

Network	Properties			
<i>Filter</i>				
MCNLO	<input type="checkbox"/> DHCPv4	<input checked="" type="checkbox"/> IPv6	<input checked="" type="checkbox"/> Autoconf	<input type="checkbox"/> DHCPv6
MCNPR	<input type="checkbox"/> DHCPv4	<input checked="" type="checkbox"/> IPv6	<input checked="" type="checkbox"/> Autoconf	<input type="checkbox"/> DHCPv6
MSNPR0	<input type="checkbox"/> DHCPv4	<input checked="" type="checkbox"/> IPv6	<input checked="" type="checkbox"/> Autoconf	<input type="checkbox"/> DHCPv6
MSNPR1	<input type="checkbox"/> DHCPv4	<input checked="" type="checkbox"/> IPv6	<input checked="" type="checkbox"/> Autoconf	<input type="checkbox"/> DHCPv6

Total: 4

▼ HNC hnc2-se2: Network IP addresses ?

Add new IP address

Network	IP address	Mask	Name	Conf.
<i>Filter</i>				
LOCLAN	192.168.151.12	-	-	-
MCNLO	fe80::72e2:84ff:fe0a:3ce8	/64	-	static
MCNPR	fd5e:5e5e:600:0:72e2:84ff:fe0a:3ce8	/64	hnc2-se2.senet	dynamic
MCNPR	fe80::72e2:84ff:fe0a:3ce8	/64	-	static
MSNPR0	fe80::72e2:84ff:fe0a:3ce8	/64	-	static
MSNPR1	fe80::72e2:84ff:fe0a:3ce8	/64	-	static

Total: 6

The *IP configuration* tab displays the host name, network properties, and network IP 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.

10.1.5.3 Managing routing of the HNC

You manage routing of the HNC using the associated *Management* menu, *Routing & DNS* tab.

- ▶ Select *Hardware* → *Units*[→ <se server> (*SE*<model>)] → <unit> (*HNC*) → *Management*, *Routing & DNS* tab.

IP configuration **Routing & DNS** Net-Storage

▼ HNC hnc2-se2: Routing ?

Add new route

Target	Gateway	Usage	
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	
127.0.0.0/8	-	-	
192.168.151.0/24	192.168.151.12	-	
192.168.31.1/32	192.168.40.1	NETSTOR01	↗
192.168.40.0/24	192.168.40.32	NETSTOR01	↗
fd5e:5e5e:600::/64	-	MCNPR	

Total: 5

▶ HNC hnc2-se2: DNS configuration: Static ?

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 210](#)) with the following restriction:



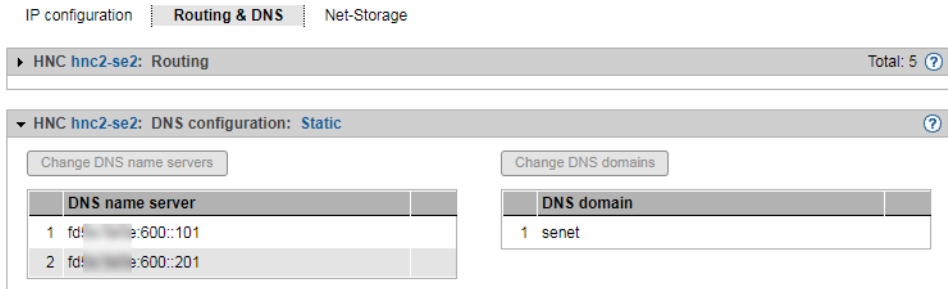
The MANPU and MONPU networks are not available on the HNC.

The *Add new route* and *Delete route* actions are only available for Net-Storage connections.

10.1.5.4 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* → *Units* [→ <se server> (*SE*<model>)] → <unit> (*HNC*) → *Management*, *Routing & DNS* tab.



The *Routing & DNS* tab displays the DNS configuration in the lower group *DNS configuration*.

10.1.5.5 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.

- For administrative access to the Net-Storage server that provides the Net-Storage, the administrator of the Net-Storage server must create an account that is the owner of the directory released via NFS. In the case of Eternus-CS HE NAS, the account must be the owner of the file group of the NAS share. The user ID and group ID must be obtained from the administrator of the Net-Storage server.

The NFSv4 domain must correspond to the domain name set on the Net-Storage server.



The HNC always tries to connect to the Net-Storage via the NFSv4. If the mounting via NFSv4 fails, NFSv3 is used as protocol.

- 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* → *Units* [→ <se server> (SE<model>)] → <unit> (HNC) → *Management, Net-Storage* tab.

IP configuration | Routing & DNS | **Net-Storage**

HNC hnc2-se2: Net-Storage accesses

Access	
User ID	7013
Group ID	2003

Configuration of NFSv4 domain

Domain: localdomain

▼ HNC hnc2-se2: Net-Storage connection properties

Add connection

Connection	Slot / port	VLAN	Properties					
NETSTOR01	s2 p3	-	<input type="checkbox"/> DHCPv4 <input type="checkbox"/> IPv6 <input type="checkbox"/> Autoconf <input type="checkbox"/> DHCPv6					

Total: 1

▼ HNC hnc2-se2: Net-Storage connection addresses

Add IP address

Connection	IP address	Mask	VLAN	MAC address	Conf.	
Filter	Filter	Filter	Filter	Filter	Filter	
LOCLAN	192.168.151.12	-	-	0A:00:14:10:80:FF	-	
NETSTOR01	192.168.40.32	/24	-	A0:36:9F:55:0D:EB	static	

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

In the *Access* table, the current user and group ID that can be used to administrate the Net-Storage access are specified in the form of UNIX userid/groupid. The IDs must be obtained from the system administrator of the Net-Storage server. The default value for both is 0. If the default value is not changed, the access is attempted with root rights, which is not recommended for reasons of data protection.

- 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.



Please note that the following actions will result in the demounting of all mounted Net-Storage devices in the BS2000. You will therefore have to re-mount them afterwards.

Entering or changing configuration data for the NFSv4 domain

- ▶ In the *Net-Storage accesses* group, click on the *Change* icon next to *Configuration of NFSv4 domain* and enter the domain name in the subsequent dialog. Confirm the action.



Please note that the following actions will result in the demounting of all mounted Net-Storage devices in the BS2000. You will therefore have to re-mount them afterwards.

Adding and changing 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.
- ▶ In the *Net-Storage connection properties* group click the *Change* icon by the required Net-Storage connection and enter your changes in the subsequent dialog. Confirm the action.

For further information, see the "Description Paper Net-Storage Guide" [15].

Deleting a Net-Storage connection

- ▶ In the *Net-Storage connection properties* group click the *Delete* 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.

Deleting a Net-Storage connection address

- ▶ In the *Net-Storage connection addresses* group click the *Delete* icon by the required Net-Storage connection and confirm the action.

10.1.5.6 Managing updates

Fundamental information on updates is provided in [section “Maintenance and remote service” on page 71](#).

You manage updates of the HNC using the associated *Service* menu, *Update* tab.

- ▶ Select *Hardware* → *Units*[→ <se server> (*SE*<model>)] → <unit> (*HNC*) → *Service*, *Update* tab.

On the *Update* tab, an expandable group is displayed for the *Security fixes* and *Hot fixes* software updates.

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 217](#)).

10.1.5.7 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* → *Units*[→ <se 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 220](#)).



Recommendation: Perform a CSR backup after each HNC-specific configuration change.

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* → *Units* [→ *<se 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 222](#)).

The file name of the diagnostic data file for the HNC is:

```
DIAGtar.H<software-version><unit-name>.<date>.<time>.gz
```

10.1.6 Managing Server Unit x86

10.1.6.1 Displaying system information and interfaces of the unit

You obtain the system information and interfaces of the Server Unit using the associated *Information* menu.

- [Displaying system information of the SU x86](#)
- [Displaying and changing IP interfaces of the SU x86](#)
- [Displaying FC interfaces of the SU x86](#)
- [Displaying multipath disks of the SU x86](#)
- [Displaying configuration disks of the SU x86](#)

Displaying system information of the SU x86

- ▶ Select *Hardware* → *Units*[→ <se server> (*SE*<model>)] → <unit> (*SU*<x86>) → *Information*, *System* tab.

System Unit su1-se2: System information	
Name	su1-se2
HW model	SE SERVER SU300 M1
BS2000 model	SU300-80F
XenVM license	Existing
Serial number	YL5W001134
SW version	X2000 V6.2A0402.000
Hot fixes	-
System start	2017-08-21 13:59:49
Main memory	256 GB
CPUs	Intel(R) Xeon(R) CPU X7542 @ 2.67GHz, 2666 MHz (4 Sockets, 24 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* → *Units*[→ <se server> (SE<model>)] → <unit> (SU<x86>) → *Information, IP interfaces* tab.

System | **IP interfaces** | FC interfaces | Multipath disks | Configuration disks

Server Unit su1-se2: IP interfaces ?

Slot / port	MTU	Type	MAC address	Usage	Status	
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	All	▼
-	1500	-	0A:00:14:10:08:FF	LOCLAN	-	
s5 p0 pci	1500	Intel(R) 82576NS Gigabit	00:19:99:89:3F:61	ZASLAN	UP	
s5 p1 pci	1500	Intel(R) 82576NS Gigabit	00:19:99:89:3F:60	vSwitch	UP	
s8 p0 pci	1500	Intel(R) 82580 Gigabit	00:19:99:83:A1:AE	-	DOWN	
s8 p1 pci	1500	Intel(R) 82580 Gigabit	00:19:99:83:A1:AF	-	DOWN	
s8 p2 pci	1500	Intel(R) 82580 Gigabit	00:19:99:83:A1:B0	vSwitch	DOWN	
s8 p3 pci	9000	Intel(R) 82580 Gigabit	00:19:99:83:A1:B1	ZASLAN	UP	
s12 p1 ior	1500	Intel(R) 82576NS Gigabit	C8:0A:A9:33:4F:44	SYS1	UP	
s12 p2 ior	1500	Intel(R) 82576NS Gigabit	00:19:99:83:A1:B0	vSwitch	DOWN	
s12 p3 ior	1500	Intel(R) 82576NS Gigabit	C8:0A:A9:33:4F:46	-	DOWN	
s12 p4 ior	1500	Intel(R) 82576NS Gigabit	C8:0A:A9:33:4F:44	SYS2	UP	

Total: 11

The *IP 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* → *Units*[→ <se 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](#)” on page 206.

Displaying multipath disks of the SU x86

For the FC disks of the SU x86 you can view 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* → *Units*[→ <se 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” on page 207](#).

Displaying configuration disks of the SU x86

The *Configuration disks* tab in the *Information* menu displays the status of the internal and, if existing, the external configuration disks of the SU x86.

Purpose and operation of configuration disks are described in [section “External configuration disks” on page 42](#).

- ▶ Select *Hardware* → *Units*[→ <se server> (SE<model>)] → <unit> (SU<x86>) → *Information, Configuration disks* tab:

10.1.6.2 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* → *Units*[→ <se 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 208](#)) with the following restriction:



If only the standard networks LOCLAN, MCNLO, and MCNPR are assigned on the SU x86, the buttons for changes are not enabled.

10.1.6.3 Managing routing of the SU x86

You manage routing of the SU x86 using the associated *Management* menu, *Routing & DNS* tab.

- ▶ Select *Hardware* → *Units*[→ <se server> (*SE*<model>)] → <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 210](#)) with the following restriction:



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.

10.1.6.4 Displaying the DNS configuration of the SU x86

You can inquire information about the DNS configuration of the SU x86 using the associated *Management* menu, *Routing & DNS* tab.

- ▶ Select *Hardware* → *Units* [→ <se server> (*SE*<model>)] → <unit> (*SU*<x86>) → *Management*, *Routing & DNS* tab.

The screenshot shows the 'Routing & DNS' tab for 'Server Unit su1-se2'. The configuration is set to 'Static'. There are two main sections: 'Change DNS name servers' and 'Change DNS domains'. The 'Change DNS name servers' section contains a table with two entries:

	DNS name server
1	fd5:::600::101
2	fd5:::600::201

The 'Change DNS domains' section contains a table with four entries:

	DNS domain
1	abg.example.net
2	mch.example.net
3	example.net
4	senet

The *Routing & DNS* tab displays the DNS configuration in the lower group *DNS configuration*.

The structure of the tab is basically the same as that for the MU (see [section “Managing the DNS configuration” on page 211](#)).

10.1.6.5 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.

- For administrative access to the Net-Storage server that provides the Net-Storage, the administrator of the Net-Storage server must create an account that is the owner of the directory released via NFS. In the case of Eternus-CS HE NAS, the account must be the owner of the file group of the NAS share. The user ID and group ID must be obtained from the administrator of the Net-Storage server.

The NFSv4 domain must correspond to the domain name set on the Net-Storage server.



X2000 always tries to connect to the Net-Storage via NFSv4. If the mounting via NFSv4 fails, NFSv3 is used as protocol.

- 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* → *Units*[→ <se server> (SE<model>)] → <unit> (SU<x86>) → *Management, Net-Storage* tab.

IP configuration | Routing & DNS | **Net-Storage**

Server Unit **su2-se1**: Net-Storage accesses

Access		Configuration of NFSv4 domain	
User ID	7013	Domain	localdomain
Group ID	2003		

▼ Server Unit **su2-se1**: Net-Storage connection properties

Add connection

Connection	Slot / port	VLAN	Properties					
NETSTOR01	s1 p0	-	<input type="checkbox"/> DHCPv4 <input type="checkbox"/> IPv6 <input type="checkbox"/> Autoconf <input type="checkbox"/> DHCPv6					

Total: 1

▼ Server Unit **su2-se1**: Net-Storage connection addresses

Add IP address

Connection	IP address	Mask	VLAN	MAC address	Conf.	
Filter	Filter	Filter	Filter	Filter	Filter	
LOCLAN	192.168.138.12	-	-	0A:00:14:10:08:FF	-	
NETSTOR01	17 4.202	/22	-	A0:36:9F:BF:A5:A0	static	

Total: 2

The *Net-Storage* tab displays the *Net-Storage Authorizations*, *Net-Storage connection properties*, and *Net-Storage connection addresses* groups.

The following functions are available:

Changing accesses for the SU x86

In the *Access* table, the current user and group ID that can be used to administrate the Net-Storage access are specified in the form of UNIX userid/groupid. The IDs must be obtained from the system administrator of the Net-Storage server. The default value for both is 0. If the default value is not changed, the access is attempted with root rights, which is not recommended for reasons of data protection.

- ▶ 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.



Please note that the following actions will result in the demounting of all mounted Net-Storage devices in the BS2000. You will therefore have to re-mount them afterwards.

Entering or changing configuration data for the NFSv4 domain

- ▶ In the *Net-Storage accesses* group, click on the *Change* icon next to *Configuration of NFSv4 domain* and enter the domain name in the subsequent dialog. Confirm the action.



Please note that the following actions will result in the demounting of all mounted Net-Storage devices in the BS2000. You will therefore have to re-mount them afterwards.

Adding and changing 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.
- ▶ In the *Net-Storage connection properties* group click the *Change* icon by the required Net-Storage connection and enter your changes in the subsequent dialog. Confirm the action.

For further information, see the "Description Paper Net-Storage Guide" [15].

Deleting a Net-Storage connection

- ▶ In the *Net-Storage connection properties* group click the *Delete* 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 IP address*, make the required entries in the subsequent dialog box, and confirm the action.

Deleting a Net-Storage connection address

- ▶ In the *Net-Storage connection addresses* group click the *Delete* icon by the required Net-Storage connection and confirm the action.

10.1.6.6 Managing updates of the SU x86

Fundamental information on updates is provided in [section “Maintenance and remote service” on page 71](#).

You manage updates of the SU x86 using the associated *Service* menu, *Update* tab.

- ▶ Select *Hardware* → *Units*[→ <se server> (*SE*<model>)] → <unit> (*SU*<x86>) → *Service*, *Update* tab.

On the *Update* tab, an expandable group is displayed for the *Security fixes* and *Hot fixes* software updates.

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 217](#)).

10.1.6.7 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.



Recommendation: Perform a CSR backup after each SU-specific configuration change.

- ▶ Select *Hardware* → *Units*[→ <se 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 220](#)).

10.1.6.8 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* → *Units* [→ <se 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 222](#)).

The file name of the diagnostic data file for the SU x86 is:

```
DIAGtar.X<software-version><unit-name>.<date>.<time>.gz
```

10.1.7 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 PY (e.g. 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 AU PQ . The access to the console of the Application Unit is also available there.

The iRMC/Management Board is also linked in the system operation of the AU or AU partition.

10.1.7.1 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.



Further information is provided in the appendix of 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 appendix of the online help (see "Further information", "Configuration on the Application Unit").

- ▶ 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.

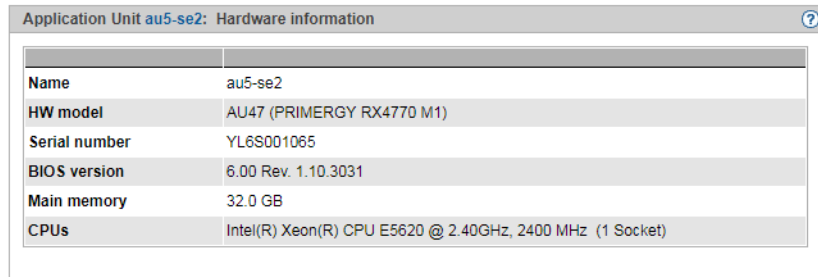
The Application Unit thus reports on hardware errors to the Management Unit in two ways:

- Trap forwarding from the iRMC
- Trap forwarding from the Management Board

10.1.7.2 Displaying hardware information of the Application Unit

- Select *Hardware* → *Units*[→ <se server> (SE<model>)] → <unit> (AU<model>) → *Information, Overview* tab.

Overview



The screenshot shows a window titled 'Application Unit au5-se2: Hardware information'. It contains a table with the following data:

Application Unit au5-se2: Hardware information	
Name	au5-se2
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.

For an AU PQ , information about the chassis, Management Boards, System Boards, IO Units, and Disk Units is displayed. When a partition is selected, information is displayed about the partition, the assigned System Board, and the IO Unit. Example for a DBU87 (only in extracts):

Overview	
Application Unit auc8-se1 : Hardware information ?	
Chassis	
Name	auc8-se1
HW model	DBU87 (PRIMEQUEST 2800E2)
Serial number	1541517004
Management Board 0	
FW version	30.33
Serial number	PP1514036R
Management Board 1	
FW version	30.33
Serial number	PP1411015K
System Board 0	
Serial number	PP160502CV
BIOS version	1.67
BMC version	2.18F
Board revision	CA07777-D010 B3
Main memory	128.0 GB
CPUs	Intel(R) Xeon(R) E7-8867V3, 2500 MHz (2 Sockets)
System Board 1	
Serial number	PP151601YU
BIOS version	1.67

10.1.7.3 Managing the IP configuration of the Application Unit

When managing the IP configuration, there are differences between Application Units PY and Application Units PQ.

Managing IP configuration of an Application Unit PY

You manage the IP configuration of an AU PY using the associated *Management* menu, *IP configuration* tab.

- ▶ Select *Hardware* → *Units*[→ <se server> (SE<model>)] → <unit> (AU<model>) → *Management*, *Configuration* tab.

IP configuration

Application Unit **au5-se2**: Host name ?

Host name	au5-se2
-----------	---------

Application Unit **au5-se2**: IP network ?

IP address	Mask	IP interface	VLAN	Network	
fd5e:5e5e:601:0:250:56ff:fe62:5f62	/ 64	vmk1	601	MONPR01	↻

Application Unit **au5-se2**: Access data ?

Account	Status	
root	✔ VALID	✎

Application Unit **au5-se2**: iRMC Access data ?

IP address iRMC	Account	Status	
17...28	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 network* group click the *Update network data* icon and confirm the action.

A dialog with the *Automatic update* option is opened:

- ▶ If the AU is connected via MONPR01 IPv6, select *Yes* and confirm the action.

- ▶ If the AU is connected via MANPU or MONPR01 IPv4, select *No* and enter the IP address.

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, Microsoft HyperV oder Citrix XenServer operating system.

- ▶ In the *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 IP address and password* icon by the required IP address iRMC, change the *IP address iRMC* or the *Password* and confirm the action.



semuser is permanently assigned as account. An account with this name must be created in the iRMC of the AU. The account must have the *LANchannel privilege Administrator, SerialChannel Privilege user* rights.

Also see "Status monitoring via the iRMC of the Application Unit" in the appendix of the online help.

Managing IP configuration of an Application Unit PQ

IP configuration of an AU PQ is distributed to the *Chassis* and *Partition* levels.

At chassis level, access to the Management Board is configured centrally:

- ▶ Select *Hardware* → *Units*[→ *<se server> (SE<model>)*] → *<unit> (<AU PQ model>)* → *Management, IP configuration tab*.

In the *Management Board access data* area you can change the IP address and password.



The account **semuser** is permanently assigned. The account must be configured in the web UI of the Management Board and have the admin privilege for the Remote Server Management.

At partition level access to the particular partition's system is configured:

- ▶ Select *Hardware* → *Units*[→ *<se server> (SE<model>)*] → *<unit> (<AU PQ model>)* → *<partition>* → *Management, IP configuration tab*.

In the *IP network* area you can update network data analogously to AU PY (see ["Updating network data" on page 250](#)).

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](#)
- [Configuring 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.

Overview | SENE | Switches | Topology | Performance

IP networks overview ?

Network	Status	Description
<i>Filter</i>	All ▼	<i>Filter</i>
DANPU01	✓ NORMAL	Data Network Public 01
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
MANPU	✓ NORMAL	Management Administration Network Public
MCNPR	✓ NORMAL	Management Control Network Private
MONPR01	✓ NORMAL	Management Optional Network Private 01
MONPR02	✓ NORMAL	Management Optional Network Private 02
MCNLO	✓ NORMAL	Management Control Network Local
MSNPR	✓ NORMAL	Management SVP Network Private

Total: 13

The *Overview* tab displays information on all public and private data and management networks of the SE server configuration.

If you manage a configuration of two SE servers in a Management Cluster, an additional *Server* column is displayed. The column contains the name of the SE server to which the network belongs. For non-server-specific networks (DANPR<nn>, MCNPR and MONPR<nn>), - (*global*) is displayed.

10.2.1.2 Configuring SENET

SENET contains the internal DNS configuration of the SE server or the SE servers of a Management Cluster. The IP network SENET is displayed on the *SENET* tab.

- Select *Hardware* → *IP networks*, *SENET* tab.

Overview | **SENET** | Switches | Topology | Performance

IP network SENET (DNS)

Add DNS entry

SENET host name	SENET name	IP address	Network	Registration name		
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>		
-	su3-se1.senet	fd5e:5e5e:600:0:56ab:3aff:fe6f:f4d1	MCNPR	54AB3A6FF4D1		
-	su2-se1.senet	fd5e:5e5e:600:0:ca0a:a9ff:fec8:58c2	MCNPR	C80AA9C858C2		
-	su1-se1.senet	fd5e:5e5e:600:0:ea9a:8ff:fe92:812	MCNPR	E89A8F920812		
-	mu1irmc-se1.senet	fd11: [redacted] c5b0:921b:eff:fea5:8251	-	mu1irmcse1		
-	nswa1-se1.senet	fd5e:5e5e:600::a:101	MCNPR	nswa1se1		
-	su1irmc-se1.senet	fd5e:5e5e:600:0:ea9a:8ff:fe92:816	MCNPR	su1irmcse1		
-	su2irmc-se1.senet	fd5e:5e5e:600:0:ca0a:a9ff:fec8:58c6	MCNPR	su2irmcse1		
-	su3irmc-se1.senet	fd5e:5e5e:600:0:56ab:3aff:fe6f:e678	MCNPR	su3irmcse1		
-	-	17 [redacted] .245	MANPU	au7irmcse1		
-	-	17 [redacted] .7	MANPU	abgqa701		
abgqa700.senet	au7-se1.senet	17 [redacted] .7	MANPU	2C600C82FBDF		
ABGSE704.senet	su3vm04-se1.senet	fd5e:5e5e:600:0:921b:eff:feb2:1404	MCNPR	901B0EB21404		
ABGSE706.senet	su3vm06-se1.senet	fd5e:5e5e:600:0:921b:eff:feb2:1406	MCNPR	901B0EB21406		
ABGSE708.senet	su3vm08-se1.senet	fd5e:5e5e:600:0:921b:eff:feb2:1408	MCNPR	901B0EB21408		
ABGSE709.senet	su3vm09-se1.senet	fd5e:5e5e:600:0:921b:eff:feb2:1409	MCNPR	901B0EB21409		
ABGSE711.senet	su3vm11-se1.senet	fd5e:5e5e:600:0:921b:eff:feb2:140b	MCNPR	901B0EB2140B		
abgsem11.senet	mu1-se1.senet	fd5e:5e5e:600::101	MCNPR	901B0E9A693C		

Total: 94

The *SENET* tab displays all DNS entries of the SENET. In addition to the fixed internal entries, you can add or remove additional DNS entries and change the host name:

Adding a new DNS entry to the SENET

- In the *SENET* tab, click the *Add DNS entry* button and follow the instructions of the wizard.

In the first step of the dialog, you choose between the *IPv6 Discovery* mode or *Manual input of the IP address*.

In case of IPv6 Discovery, select a private management or data network. After that, all IPv6 addresses of this network that are not yet registered in the DNS are displayed. In the "Ports" selection list, select the required address. The registration name is assigned automatically. You can assign the host name.

Manually entering the IP address:

In the following steps of the dialog, you can assign the IP address, the registration name and the host name.

Changing the host name of a DNS entry

- ▶ Click on the *Change* icon next to the DNS entry and change the host name in the subsequent dialog.

Deleting a DNS entry

- ▶ Click the *Remove* icon by the DNS entry you wish to remove.

10.2.1.3 Information on switches

The information on switches is displayed in the *Switches* tab.

- ▶ Select *Hardware* → *IP networks, Switches* tab.

The screenshot shows the 'Switches' tab in a network management interface. It contains two main sections:

IP switch status

Name	Unit	Type	Temperature [°C]	Status	ISL internal
nswa1-se1	1	Stackable ICX6450-48	60.5	NORMAL	NORMAL
nswa1-se1	2	Stackable ICX6450-48	60.5	NORMAL	NORMAL

Total: 2

IP switch port information

Name	Port	Link	Type	Gbit/s	VLAN	Usage	Description
nswa1-se1	1/1/2	UP	RJ45	0.01	MSNPR0	Svp	
nswa1-se1	1/1/3	UP	RJ45	1.00	MANPU	Uplink	
nswa1-se1	1/1/4	DOWN	RJ45	-	MONPU	Uplink	
nswa1-se1	1/1/5	UP	RJ45	1.00	DANPU01	Uplink	
nswa1-se1	1/1/7	UP	RJ45	1.00	MU1SYS1	System	
nswa1-se1	1/1/8	UP	RJ45	1.00	MU2SYS1	System	
nswa1-se1	1/1/9	UP	RJ45	1.00	SU1SYS1	System	
nswa1-se1	1/1/10	UP	RJ45	1.00	SU2SYS1	System	
nswa1-se1	1/1/11	UP	RJ45	1.00	HNC1SYS1	System	

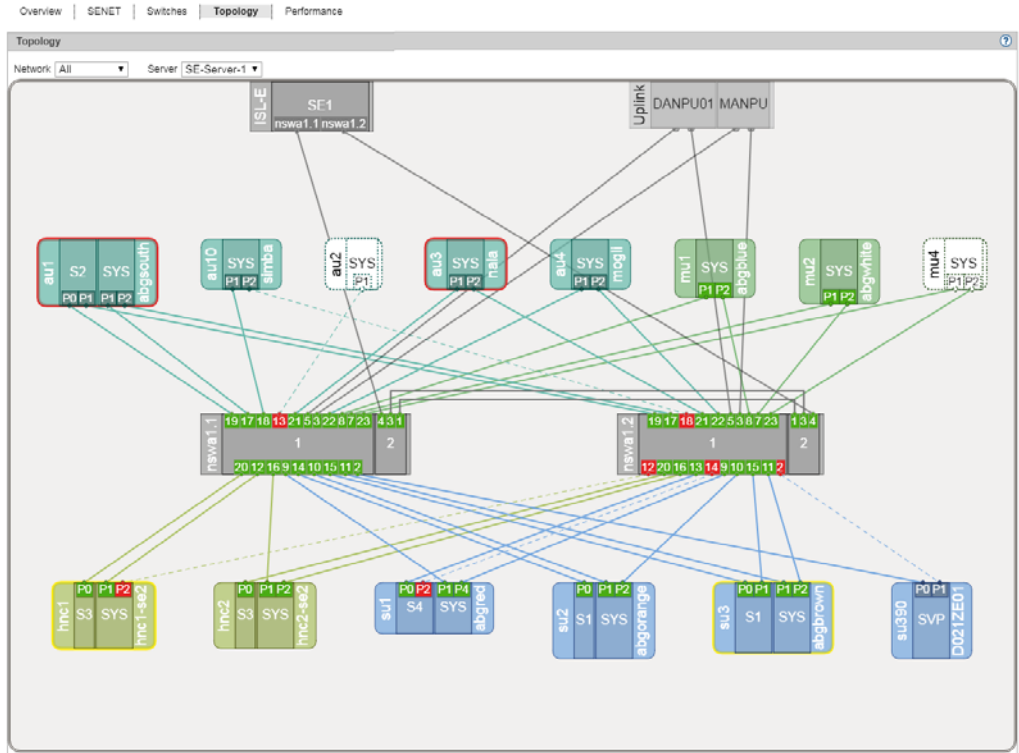
The *Switches* tab displays the status of the switches and information on the ports.

- ▶ If you drag the mouse over the *i* icon next to the temperature value in the *IP switch status* group, a tool tip displays the temperature thresholds for warning and power-off.
- ▶ In the *IP switch port information* group, 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.



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.
- For a Management Cluster, you can select the SE server for which you want to display the topology, from the *Server* list. The default is the SE server of the local MU.



When you drag the mouse cursor over a network component, a tool tip displays detailed information on it (if available).

To view the relevant parts of the graphic, left-click and hold the graphic to drag it into the desired position.

In the case of AU PQ 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.

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	0.16	0.13 %	0.12	0.10 %	MANPU
nswa1-se1	1/1/4	-	-	-	-	-	- MONPU
nswa1-se1	1/1/5	1.00	0.00	0.00 %	0.00	0.00 %	DANPU01
nswa1-se1	1/1/7	1.00	0.34	0.28 %	0.22	0.18 %	MU1SYS1
nswa1-se1	1/1/8	1.00	0.22	0.19 %	0.24	0.20 %	MU2SYS1
nswa1-se1	1/1/9	1.00	0.00	0.00 %	0.02	0.01 %	SU1SYS1
nswa1-se1	1/1/10	1.00	0.00	0.00 %	0.01	0.01 %	SU2SYS1
nswa1-se1	1/1/11	1.00	0.00	0.00 %	0.00	0.00 %	HNC1SYS1
nswa1-se1	1/1/12	1.00	0.00	0.00 %	0.01	0.00 %	HNC2SYS1
nswa1-se1	1/1/13	-	-	-	-	-	- SU1S7P1
nswa1-se1	1/1/14	1.00	0.00	0.00 %	0.00	0.00 %	SU2S1P0

10.2.2 Managing a Data Network Public

You manage the public data networks (Data Network Public, DANPU) using the menu item *Data Network Public* in the *IP networks* menu. Up to eight DANPUs can exist per SE server. These are named DANPU01, DANPU02, etc.



DANPU01 is pre-configured, further DANPU networks are configured by the Customer Support staff.

Overview of all DANPUs

- ▶ Select *Hardware* → *IP networks* → *Data Network Public, Overview* tab.

Overview

Network	Status	Description
<i>Filter</i>	<i>All</i> ▼	<i>Filter</i>
DANPU01	✓ NORMAL	Data Network Public 01
DANPU03	✓ NORMAL	Data Network Public 03
DANPU08	✓ NORMAL	Data Network Public 08

Total: 3

The tab displays information on all existing DANPUs of the SE server configuration.

If managing a Management Cluster, an additional *Server* column is displayed. It lists the SE servers and the DANPUs that belong to it.

All DANPU networks are listed in the tree structure, under the *Hardware* → *IP networks* → *Data Network Public* menu entry. If a Management Cluster is configured, each SE server has a *<se server>(SE<model>)* submenu containing its DANPU. You can use these DANPU entries to obtain detailed information on the various public data networks and manage them.

Overview of the various DANPUs

- Select *Hardware* → *IP networks* → *Data Network Public* → [*<se server>(SE<model>)*] → *DANPU<no>*, *Overview* tab.

Overview | ACL | Performance

IP network DANPU01: general information ?

Property	Value
VLAN ID (NetUnit)	4

▼ IP network DANPU01: IP switch uplinks ?

Name	Port	Link	Mode	Status
<i>Filter</i>	<i>Filter</i>	<i>All</i>	<i>Filter</i>	<i>Filter</i>
nswa1-se1	1/1/5	UP	untagged	NORMAL
nswa1-se1	2/1/5	UP	untagged	NORMAL

Total: 2

▼ IP network DANPU01: IP switch ISL ?

Name	Port	Link	Description
<i>Filter</i>	<i>Filter</i>	<i>All</i>	<i>Filter</i>
nswa1-se1	1/2/1	UP	ISL-S
	1/2/3	UP	
nswa1-se1	2/2/1	UP	ISL-S
	2/2/3	UP	

Total: 2

▼ IP network DANPU01: NetUnit information ?

SENET host name	SENET name	Port name	Port	Link	Mode		
abgsu2se1	su2-se1	SU2S1P1	1/1/16	UP	untagged		
		SU2S2P1	2/1/16	UP	untagged		

Total: 1

The *Overview* tab displays all information on the selected DANPU.

The following functions are available:

Displaying the MAC address

- In the *Net Unit information* group click the *MAC addresses* icon (eye) by the required unit.

The subsequent dialog box *Display MAC addresses* displays the unit's active MAC addresses.

Adding ports

- ▶ In the *Net Unit information* group click *Add ports*, follow the instructions of the wizard, and select the required port.

Removing a port

- ▶ In the *Net Unit information* group click the *Delete* icon by the required unit and confirm the action.

10.2.2.1 Configuring the ACL settings of the DANPU network

The ACL (Access Control List) defines the access settings for the *DANPU<no>*. You can add and delete ACL entries for the *DANPU<no>*.

- ▶ Select *Hardware* → *IP networks* → *Data Network Public* → [*<se server>(SE<model>)*] → *DANPU<no>*, *ACL* tab.

Overview | **ACL** | Performance

IP network DANPU01: ACL settings

Network	ACL	Mode
IPv4	active	deny
IPv6	inactive	-

IP network DANPU01: ACL IPv4 rules

Deny service

TCP / UDP port	TCP / UDP service
49888	

Total: 1

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 IP4 rules* or *ACL IP6 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 IP4 rules* or *ACL IP6 rules* group click the *Remove* icon by the required entry and confirm the action.

10.2.2.2 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* → [*<se server>(SE<model>)*] → *DANPU<no>*, *Performance* tab.

Overview | ACL | **Performance**

▼ IP network DANPU01: uplink performance view ?

SENET name	Port	Gbit/s	Send		Receive	
			MB/s	Utilization	MB/s	Utilization
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 %
Total: 1						

▼ IP network DANPU01: ISL performance view ?

SENET name	Port	Gbit/s	Send		Receive	
			MB/s	Utilization	MB/s	Utilization
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>				
nswa1-se1	1/2/1	10.00	0.00	0.00 %	0.02	0.00 %
	1/2/3	10.00	0.05	0.00 %	0.03	0.00 %
nswa1-se1	2/2/1	10.00	0.02	0.00 %	0.00	0.00 %
	2/2/3	10.00	0.03	0.00 %	0.05	0.00 %
Total: 2						

▼ IP network DANPU01: unit performance view ?

SENET host name	SENET name	Port name	Port	Gbit/s	Send		Receive	
					MB/s	Utilization	MB/s	Utilization
abgsu2se1	su2-se1	SU2S1P1	1/1/16	1.00	0.00	0.00 %	0.00	0.00 %
		SU2S2P1	2/1/16	1.00	0.00	0.00 %	0.00	0.00 %
Total: 1								

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.

10.2.3 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.

Overview

Overview Data Network Private ?

Network	Status	Description
<i>Filter</i>	<i>All</i> ▼	<i>Filter</i>
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

Total: 6



The administrator can create another private network by clicking the *Add network* button.

All existing DANPR networks are listed in the tree structure, under the *Hardware* → *IP networks* → *Data Network Private* menu entry. You can use these DANPR to obtain detailed information on the various private data networks and manage them.

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.

Overview | ACL | Performance

IP network DANPR01: general information ?

Property	Value
IPv6 autoconf. prefix	fd5e:5e5e:801::/64
VLAN ID (NetUnit)	801

IP network DANPR01: RADVD / DNS / NTP server ?

Activate RADVD / DNS / NTP server

SENET host name	IP address		
abgsilver	fd5e:5e5e:801::101	i	↔

Total: 1

IP network DANPR01: IP switch ISL ?

Name	Port	Link	Description
<i>Filter</i>	<i>Filter</i>	<i>All</i>	<i>Filter</i>
nswa1-se1	1/2/1 1/2/3	↑ UP	ISL-S
nswa1-se1	2/2/1 2/2/3	↑ UP	ISL-S
nswa1-se1	1/2/4 2/2/4	↑ UP	ISL-E

Total: 3

IP network DANPR01: NetUnit information ?

Add ports

SENET host name	SENET name	IP switch	Port name	Port	Link	Mode		
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>All</i>	<i>Filter</i>		
abgsu1se1	su1-se1	nswa1-se1	SU1S8P3	2/1/13	↑ UP	tagged	👁	↔
abgse1mu1	mu2-se1	nswa1-se1	MU2SYS1 MU2SYS2	1/1/8 2/1/8	↑ UP	tagged	👁	↔
abgse1mu1	mu1-se1	nswa1-se1	MU1SYS1 MU1SYS2	1/1/7 2/1/7	↑ UP	tagged	👁	↔

Total: 3

10.2.3.1 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.



In the wizard, the available ports of the units (MU, SU x86, HNC) are only offered in the selection list in dependence to the selected mode (*tagged*, *untagged* or *dual*). The ports of the MUs are only offered for selection in the *tagged* mode. If another mode was selected, the ports of the MUs can be added afterwards at the respective DANPR<nn> via *Add ports* (see [“Overview of the various DANPRs” on page 266](#)).

10.2.3.2 Activate RADVD / DNS / NTP server

You can activate the RADVD / DNS / NTP server in the local 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*.



In an SE server configuration with multiple MUs, this action is only available for the local MU (the MU on which you are logged in). To activate another MU, you have to switch to the SE Manager of that MU. In case of a global session: Switching is possible via the link in the header of the SE Manager.

For reasons of redundancy we recommend to activate the RADVD / DNS / NTP server on all MUs of the SE server configuration.

Note:

At least one port of the respective MU must be assigned to the network.

The *IP address* column for already entered MUs displays the IPv6 address of the MU in the network. If you drag the mouse over the *i* icon, a tool tip informs you whether the entry is the local MU or a remote MU.

10.2.3.3 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”](#).



Caution:

After assigning a port of a unit in the *untagged* mode to a network, that port cannot be assigned to an additional network.

In *dual* mode, assigning the port for other networks is only possible as *tagged*.

10.2.3.4 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”](#).

10.2.3.5 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”](#).

10.2.4 Managing a Management Network Public

Each SE server has a public management 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.

Overview over the status of the management networks MANPU and MONPU

- ▶ Select *Hardware* → *IP networks* → *Management Network Public, Overview* tab.

Overview

Network	Status	Description
Filter	All	Filter
MANPU	✓ NORMAL	Management Administration Network Public
MONPU	✓ NORMAL	Management Optional Network Public

Total: 2

In Management Cluster configurations, the *Overview* tab displays the status of the public management networks of both SE servers of the Management Cluster. The *Server* column lists the name of the corresponding SE server with each MANPU/MONPU.

Overview over the network MANPU of an SE server

- ▶ Select *Hardware* → *IP networks* → *Management Network Public* → [*<se server>(SE<model>)*] *MANPU, Overview* tab.

Overview | ACL | Performance

IP network **MANPU**: general information ?

Property	Value
IPv4 gateway	192.168.1.1
IPv4 network	192.168.0.0
IPv6 autoconf. prefix	fd11:fd52:4f34:c5b0::64
VLAN ID (NetUnit)	2

▼ IP network **MANPU**: IP switch uplinks ?

Name	Port	Link	Mode	Status
<i>Filter</i>	<i>Filter</i>	<i>All</i>	<i>Filter</i>	<i>Filter</i>
nswa1-se2	1/1/3	UP	untagged	NORMAL
nswa1-se2	2/1/3	UP	untagged	NORMAL

Total: 2

▼ IP network **MANPU**: IP switch ISL ?

Name	Port	Link	Description
<i>Filter</i>	<i>Filter</i>	<i>All</i>	<i>Filter</i>
nswa1-se2	1/2/1	UP	ISL-S
nswa1-se2	1/2/3	UP	ISL-S
nswa1-se2	2/2/1	UP	ISL-S
nswa1-se2	2/2/3	UP	ISL-S

Total: 2

▼ IP network **MANPU**: NetUnit information ?

SENET host name	SENET name	Port name	Port	Link	Mode		
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>All</i>	<i>Filter</i>		
-	au2-se2	AU2SYS1	1/1/13	DOWN	dual		
-	hnc1-se2	HNC1S3P0	1/1/20	UP	dual		
-	mu4-se2	MU4SYS1	1/1/23	UP	tagged		
		MU4SYS2	2/1/23	UP	tagged		
-	hnc2-se2	HNC2S3P0	2/1/20	UP	dual		
abgse2mu1	mu1-se2	MU1SYS1	1/1/8	UP	tagged		

The *Overview* tab displays all information on the MANPU.

For a Management Cluster, this overview also contains the *IP switch ISL* group.

The following functions are available:

Displaying the MAC address

- ▶ In the *Net Unit information* group click the *MAC addresses* icon by the required unit.
The subsequent dialog box *Display MAC addresses* displays the unit's active MAC addresses.

Adding ports

- ▶ In the *Net Unit information* group click *Add ports*, follow the instructions of the wizard, and select the ports.

Removing a port

- ▶ In the *Net Unit information* group click the *Delete* icon by the required unit and confirm the action.

10.2.4.1 Configuring the ACL settings of the MANPU network

You can add and delete ACL entries for each MANPU.

- ▶ Select *Hardware* → *IP networks* → *Management Network Public* → [*se server*](*SE*[*model*]) →] *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" on page 261](#).

10.2.4.2 Information on the performance and utilization of the MANPU ports

An overview of the performance and utilization of the ports belonging to the public management network is provided by the *Performance* tab.

- ▶ Select *Hardware* → *IP networks* → *Management Network Public* → [*se server*](*SE*[*model*]) →] *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" on page 263](#).

10.2.5 Managing a Management Network Private

An SE server can have the following private 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

You manage the private management networks via the *IP networks* → *Management Network Private* menu. The existing private management networks are listed below *Management Network Private*. You use these menu entries to manage the network and obtain detailed information.

In a Management Cluster configuration, only the globally available private management networks MCNPR and MONPR01 to MONPR08 are listed directly under *IP networks* → *Management Network Private*. The server specific MSNPR and MCNLO networks are each listed in the SE server-specific *<se server> (SE<model>)* menu. Example:

Management Network Private

- MCNPR
- MONPR01
- MONPR02
- SE-Server-1 (SE700B)
 - MCNLO
 - MSNPR
- SE-Server-2 (SE700)
 - MCNLO
 - MSNPR

10.2.5.1 Overview over the status of all private management networks

The *Overview* tab offers an overview over the current status of all private management networks currently existing in the current configuration.

- ▶ Select *Hardware* → *IP networks* → *Management Network Private, Overview* tab.

The screenshot shows a web interface titled "Overview Management Network Private". At the top left is a button labeled "Add network". Below it is a table with the following columns: Network, Status, Server, and Description. The table contains several rows of network configurations.

Network	Status	Server	Description
Filter	All	Filter	Filter
MCNPR	✓ NORMAL	-(global)	Management Control Network Private
MONPR01	✓ NORMAL	-(global)	Management Optional Network Private 01
MONPR02	✓ NORMAL	-(global)	Management Optional Network Private 02
MCNLO	✓ NORMAL	SE-Server-1	Management Control Network Local
MSNPR	✓ NORMAL	SE-Server-1	Management SVP Network Private
MCNLO	✓ NORMAL	SE-Server-2	Management Control Network Local
MSNPR	✓ NORMAL	SE-Server-2	Management SVP Network Private

The *Server* column is only displayed for Management Cluster configurations.

For each SE server-specific network, this column contains the name of the SE server to which the network belongs. For each private cross-SE server management network, the *Server* column displays value *-(global)*.

Add network

An SE server configuration can contain up to 8 Management Optional Network Privates (MONPR01 ... MONPR08). As long as there are fewer than 8 MONPR networks, you can add additional MONPRs:

- ▶ 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.

Overview over a single private management network

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* → *MONPR01, Overview* tab.

The *Overview* tab with all information on the MONPR01 opens.

Overview | ACL | Performance

IP network **MONPR01**: general information ?

Property	Value
IPv4 network	10.10.1.0/24
IPv6 autoconf. prefix	fd5e:5e5e:601::/64
VLAN ID (NetUnit)	601

▼ IP network **MONPR01**: RADVD / DNS / NTP server ?

SENET host name	IP address		
<i>Filter</i>	<i>Filter</i>		
abgse1mu1	fd5e:5e5e:601::102		
abgse1mu2	fd5e:5e5e:601::101		

Total: 6

▼ IP network **MONPR01**: IP switch ISL ?

Name	Port	Link	Description
<i>Filter</i>	<i>Filter</i>	<i>All</i>	<i>Filter</i>
nswa1-se1	1/2/1 1/2/3		ISL-S
nswa1-se1	2/2/1 2/2/3		ISL-S
nswa1-se1	1/2/4 2/2/4		ISL-E

Total: 6

▼ IP network **MONPR01**: NetUnit information ?

SENET host name	SENET name	IP switch	Port name	Port	Link	Mode		
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>All</i>	<i>Filter</i>		
abgse1mu1	mu1-se1	nswa1-se1	MU1SYS1	1/1/8		tagged		
			MU1SYS2	2/1/8		tagged		
abgse1mu2	mu2-se1	nswa1-se1	MU2SYS1	1/1/8		tagged		
			MU2SYS2	2/1/8		tagged		
abgse1au3	au3-se1	nswa1-se1	AU3SYS1	1/1/21		tagged		
			AU3SYS2	2/1/21		tagged		

Displaying the MAC address

- ▶ In the *Net Unit information* group search for the required unit and click the *MAC addresses* icon.

The subsequent dialog box *Display MAC addresses* displays the unit's active MAC addresses.

10.2.5.2 Information on the performance and utilization of the ports of the private management networks

An overview of the performance and utilization of the ports belonging to the selected private management network is provided by the *Performance* tab.

- ▶ For the *MCNPR* or *MONPR*<nn> networks: Select *Hardware* → *IP networks* → *Management Network Private* → <network>, *Performance* tab. Here <network> specifies the private management network *MCNPR* or *MONPR*<nn>.
- ▶ For the *MCNLO* or *MSNPR* networks: Select *Hardware* → *IP network* → *Management Network Private* → [<se server>(SE<model>) →] <network>, *Performance* tab. Here <network> specifies the private management network *MCNLO* or *MSNPR*. Since these networks are server-specific, they are always assigned to a <se server>(SE<model>) menu if they are part of a Management Cluster.

The *Performance* tab is similar for all Management Networks Private. 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” on page 263](#).

10.2.5.3 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 Private* → *MONPR*<no>, *Overview* tab.

Adding ports

- ▶ Select the *Net Unit information* group and click *Add ports*.

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* group, click the *Delete* icon by the required unit and confirm the action.

10.2.5.4 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>*, *ACL* tab.

Proceed as described in [section “Configuring the ACL settings of the DANPU network” on page 261](#).

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.

Overview | Settings | Messages

FC networks: Data ?

Latest Update	Automatic update	Interval	Highest message weight
2017-08-25 09:56:01	▶ ON	30 Minutes	✖ ERROR ?

▼ FC networks: Fabrics ?

Fabric Index	Fabric Name	Fabric WWN	Zones	Switches	Switch States	Paths	Path States	Status
All	All	Filter	Filter	Filter	Filter	Filter	Filter	All
1	fabric10 (Base)	10:00:00:05:33:4F:55:03		8	2 2 0 0 0		0 0 0 0 0	✔ NORMAL
2	fabric2	10:00:00:05:1E:C0:B5:A5		1656	3 3 0 0 0		583 571 0 0 12	✔ NORMAL
3	fabric1	10:00:00:05:33:4F:55:02		1585	2 2 0 0 0		196 95 0 0 101	✔ NORMAL
4	cfg	10:00:00:05:1E:D4:47:F4		1119	5 5 0 0 0		52 52 0 0 0	✔ NORMAL
5	*FAB_05 (Base)	10:00:50:EB:1A:06:24:17		-	1 1 0 0 0		0 0 0 0 0	✔ NORMAL

Total: 5

▼ FC networks: Unassigned paths and switches ?

Description	Total	Status
Generated paths, not assigned to any fabric	38	? UNKNOWN
Registered switches, not assigned to any fabric	9	? UNKNOWN

Total: 2

► FC networks: Switches Total: 22 ?

► FC networks: Inter Switch Links Total: 39 ?

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* tab. The *Settings* tab with all information on FC networks opens.

Index	Agent	VFID	Community	SNMP version	User	Password	Comment	Check
1	17 4.230	10	-	3	sancheck	Yes	switch 12	Yes
2	17 4.235	-	public	1	sancheck	Yes	SW201	Yes
3	17 4.237	-	public	1	sancheck	Yes	SW204	Yes
4	17 4.239	-	public	1	sancheck	Yes	SW203	Yes
5	17 4.5	-	public	1	sancheck	Yes	SW101	No
6	17 4.6	-	public	1	sancheck	Yes	SW103	Yes
7	17 4.6	10	-	3	sancheck	Yes	switch 11	Yes
8	abgfcsw101	128	-	3	sancheck	Yes	test duplicate	No
9	abgfcsw103	128	-	3	sancheck	Yes	test duplicate	Yes
10	abgfcsw104	128	-	3	sancheck	Yes	test duplicate	Yes
11	abgfcsw202	-	public	1	sancheck	No		No
12	ga2.example.net	-	public	1	sancheck	No		Yes
13	ga3.example.net	-	public	1	sancheck	No		Yes
14	ga4.example.net	-	public	1	sancheck	No		Yes

Adding, changing, removing switches

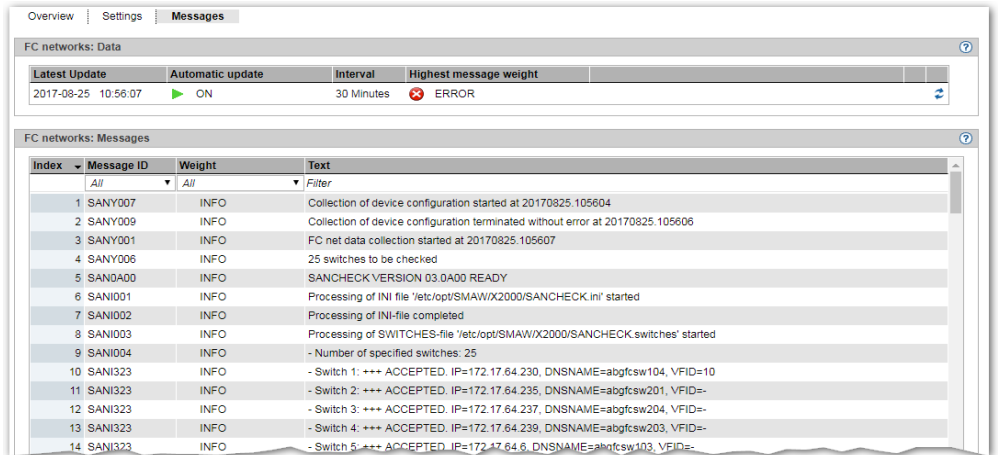
- ▶ To add a switch, in the *Registered switches* group click *Add switch*. In the *Add switch* wizard you can make the required entries step by step.
- ▶ To change a switch, in the *Registered switches* group click the *Change* icon by the required switch, follow the instructions of the subsequent wizard, and confirm the changes.
- ▶ To remove a switch, in the *Registered 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 *Registered switches* group click the *Enable check* or *Disable check* icon by the required switch and confirm the request.

10.3.3 Displaying messages

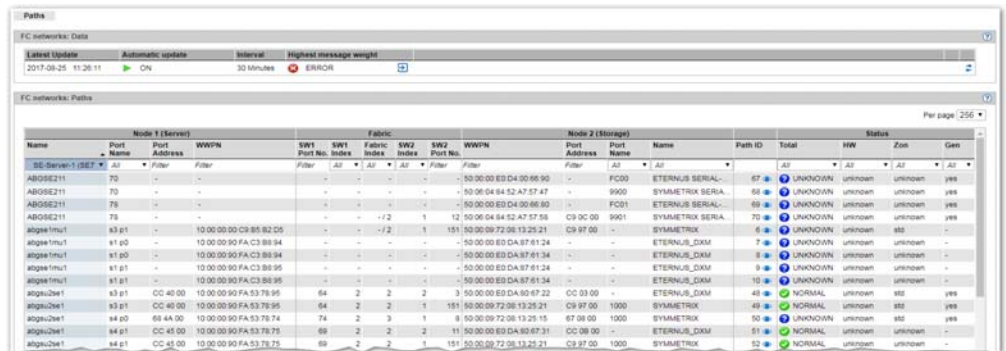
- ▶ Select *Hardware* → *FC networks*, *Messages* tab.



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.



In the *Paths* group, the *Paths* tab displays a table with all connections of the units to FC networks. You can obtain the details for a connection as follows:

- ▶ Click on the *Display* icon (eye) for the required connection in the *Path ID* column. The *Path Detail Information* dialog displays details on the connection in the form of a graphic overview (in the example a connection of the SU abgsu2-se1):

FC networks: Path Detail Information ?

Path ID: 49
 Status: ✔ NORMAL

Node 1: abgsu2se1

HBA

WWPN : 20:00:00:90:FA:53:78:95
 OUI : 0090FA (Emulex)
 Name : -

Port: CC 40 00

WWPN : 10:00:00:90:FA:53:78:95
 OUI : 0090FA (Emulex)
 Name : -
 SlotPort : s3 p1

Fabric: fabric2

Internal Index : fab2

Switch 1: ABGFCSW204

Internal Index : fab2 - swi2
 Domain : 204 (0xCC)

Port: 64

WWPN : 20:40:50:EB:1A:06:24:16
 OUI : 50EB1A (Brocade)
 Speed : 16 Gbit/s

Switch 2: ABGFCSW201

Internal Index : fab2 - swi1
 Domain : 201 (0xC9)

Port: 151

WWPN : 20:97:00:05:1E:36:55:BE
 OUI : 00051E (Brocade)
 Speed : 2 Gbit/s

Node 2: SYMMETRIX

Type : DISK

HBA

WWPN : 50:00:09:72:08:13:24:00
 OUI : 000097 (EMC)
 Name : -

Port: C9 97 00

WWPN : 50:00:09:72:08:13:25:21
 OUI : 000097 (EMC)
 Name : -
 BS2000 MN : 1000

Zone : abgsu2se1_sl3p1_emc38_dir9e1

Close

10.4 Managing storage systems

You manage the storage systems of the SE server in the tree structure: *Hardware* → *Storage*.

The *Storage* menu provides an overview of the storage available, and enables access to the Storage Manager in order to manage the storage.

If the SE server has more than one MU or if more than one SE server form a Management Cluster, the *Storage* menu provides an overview of the storage available in the complete configuration.

If you have an SE server configuration with multiple MUs, a submenu is displayed in the tree structure below *Storage*, which has an entry *Storage* (<mu-name>) for each MU on which the StorMan add-on pack is installed.

These entries give you an MU specific overview over the available storage and the direct access to the Storage Manager on the respective MU.

10.4.1 Overview of the storage systems of the SE server configuration

- ▶ Select *Hardware* → *Storage*, *Overview* tab.

Storage | Storage Manager

▼ Disk storage ?

Name	Vendor	Model	Serial number	Status
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>All</i> ▼
DX500 S3-01	FUJITSU	ETERNUS DX500 S3	4621347002	OK
DX500 S3-02	FUJITSU	ETERNUS DX500 S3	4621349005	OK
ETERNUSJX40(1)@abgafrica	FUJITSU	ETERNUS JX40		OK

Total: 3

▼ Tape storage ?

Name	Vendor	Model	Serial number	Status
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>All</i> ▼
abgsi500	ADIC	Scalar i500	A0C0245B03	OK
FLX13291A	FUJITSU	ETERNUS LT40 S2	LTDE65405932	OK
MONA	FUJITSU	ETERNUS CS HE	YABC000001	OK

Total: 3

▼ Management software ?

Name	Description
No data available	

Total: 0

In a single-MU configuration, the *Overview* tab displays information on the storage systems of the SE server. This information is the same as in the information overview which StorMan displays for storage systems.

In an SE server configuration with multiple MUs, the *Overview* tab informs of the storage systems as well as the management software that the Storage Manager manages on all MUs. Storage-systems which are found on more than one MU are displayed only once, namely with the worst status. A tool tip displays the status of the storage systems on the various MUs.

10.4.2 Overview over the storage systems of an MU

Information on the storage systems of an individual MU of a Management Cluster or an SE server with redundant MU can be obtained as follows:

- ▶ Select *Hardware* → *Storage* → *Storage (mu-name)*, *Storage* tab.

Storage Storage Manager

▼ Management Unit **abgmu1se2**: Disk storage ?

Name	Vendor	Model	Serial number	Status
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>All</i> ▼
DX500 S3-01	FUJITSU	ETERNUS DX500 S3	4621347002	✔ OK
DX500 S3-02	FUJITSU	ETERNUS DX500 S3	4621349005	✔ OK
ETERNUSJX40(1)@abgafrica	FUJITSU	ETERNUS JX40		✔ OK

Total: 3

▼ Management Unit **abgmu1se2**: Tape storage ?

Name	Vendor	Model	Serial number	Status
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>All</i> ▼
abgsi500	ADIC	Scalar i500	A0C0245B03	✔ OK
FLX13291A	FUJITSU	ETERNUS LT40 S2	LTDE65405932	✔ OK
MONA	FUJITSU	ETERNUS CS HE	YABC000001	✔ OK

Total: 3

▼ Management Unit **abgmu1se2**: Management software ?

Name	Description
No data available	

Total: 0

The *Storage* tab provides information about the storage systems and the management software which the Storage Manager manages on this MU.

You obtain direct access to the Storage Manager via the *Storage Manager* tab.

10.4.3 Storage Manager

The Storage Manager **StorMan** is an autonomous product with its own online help. You call StorMan from the SE Manager as follows:

- ▶ In a configuration with a single MU: Select: *Hardware* → *Storage*, *Storage Manager* tab.
- ▶ In an SE server configuration with multiple MUs (MU redundancy on an SE server or Management Cluster): Select *Hardware* → *Storage* → *Storage (<mu-name>)*, *Storage Manager* tab.

The Storage Manager's homepage opens.



If the current account was not entered in StorMan as authorized, the call is rejected.

In configurations with multiple MUs, switch to the GUI of the StorMan instance on the MU *<mu-name>*.



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 SE server displayed on the screen in graphic form and also in various tables:

- [Rack view](#)
- [Displaying units](#)
- [Displaying components](#)
- [Administration](#)

In a Management Cluster, a submenu *<se server>(SE<model>)* for each SE server is displayed below *Hardware* → *HW Inventory*, which contains the hardware equipment of the respective SE server.

10.5.1 Rack view

The rack view displays all integrated components on the screen in graphical form.

- ▶ Select *Hardware* → *HW Inventory* [→ *<se server>(SE<model>)*], *Rack view* tab.

The *Rack view* tab opens, here with an SE 700 as an example.

Rack view | Units | Components | Administration

SE-Server-2 (SE700) at Location 2

Rack 1 (Basic Rack)

Name	Type	Status	Eye Icon
abgse2mu1	MU	✓	👁️
hnc1-se2	HNC	✓	👁️
hnc2-se2	HNC	✓	👁️
su1se2	SU x86	✓	👁️
nswa1-se2 (basic-r)	Switch	✓	
nswa1-se2 (basic)	Switch	✓	
RC 1	RC	-	
ABGSE1BS (CHE-Box 4)	SU /390	✓	
ABGSE1BS (CHE-Box 0)	SU /390	✓	
Shelf 1	Shelf	-	
ABGSE211 (CPU-Box)	SU /390	✓	

The Eye icon allows you to view detailed hardware information about a unit.

10.5.2 Displaying units

The units view displays all integrated units in tabular form. A separate group is displayed for each unit type.

- ▶ Select *Hardware* → *HW Inventory* [→ <se server>(SE<model>)], *Units* tab.

The *Units* tab opens, here with an SE700 as an example.

Rack view | **Units** | Components | Administration

▼ Server Unit /390

Name	ABGSE211
Model	SU700
BS2000 model	SU700-20
Serial number	00020006
SW version (HCP)	E60L02G-02N+073
CPUs	4
Main memory	11.5 GB
CHE boxes	3
Power	▶ ON
HW status	✔ NORMAL
Inventory information	-

▼ Management Unit (2)

Name	iRMC	BIOS	SW version	Power	HW status	Inventory information
abgsu1mu1	8.84F	V5.0.0.9 R1.31.0 for D3279-A1x	M2000 V6.2A0401	▶ ON	✔ NORMAL	-
abgse1mu2	8.84F	V4.6.5.4 R1.16.0 for D3302-A1x	M2000 V6.2A0401	▶ ON	✔ NORMAL	-

Total: 2

▼ HNC (2)

Name	iRMC	BIOS	SW version	Power	HW status	Inventory information
hnc1-se1	5.75A	6.00 Rev. 1.13.2619.N1	HNC V6.2A0401	▶ ON	✔ NORMAL	-
hnc2-se1	8.84F	V4.6.5.4 R1.16.0 for D3302-A1x	HNC V6.2A0401	▶ ON	✔ NORMAL	-

Total: 2

▼ Server Unit x86 (2)

Name	Model	iRMC	BIOS	SW version	Power	HW status	Inventory information
su2-se1	SU300	5.70A	QSSC-S4R.FTS.1.21.2870.062220121315	X2000 V6.2A0402	▶ ON	✔ NORMAL	-
su3-se1	SU300	8.64F	V5.0.0.8 R1.36.0 for D3342-A1x	X2000 V6.2A0402	▶ ON	✔ NORMAL	-

Total: 3

▼ Application Unit x86 (4)

Name	Model	iRMC	BIOS	Power	HW status	Inventory information
<i>Filter</i>	<i>All</i>	<i>Filter</i>	<i>Filter</i>	<i>All</i>	<i>All</i>	<i>Filter</i>
abgqa500	AU20	5.75A	6.00 Rev. 1.16.2786	▶ ON	✔ NORMAL	-
abgse1au25	AU25	8.13F	V5.0.0.9 R1.28.0 for D3279-A1x	▶ ON	✔ NORMAL	-
au5-se1	AU47	-	6.00 Rev. 1.10.3031	▶ ON	✔ NORMAL	-



If at least one AU PQ exists, the properties of these AUs are displayed in a separate table with detailed information on the power status of the Management Boards (MMB), System Boards (SB), IO Units and Disk Units.

Application Unit PQ:

Name	Model	MMB	SB	IO Units	Disk Units	Power	HW status	Inventory information
auc8-se1	DBU87	2	3	3	2	ON	NORMAL	-

Total: 1

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 type.

- ▶ Select *Hardware* → *HW Inventory* [→ <se server>(SE<model>)], *Components* tab.

The *Components* tab opens, here with an SE 700B as an example.

Rack view | Units | **Components** | Administration

Switches

Name	Unit	Model	Serial number	Free ports	SW version	HW status	Inventory information
nswa1-se1 (basic)	1	Stackable ICX6450-48	BZU0433J00V	14 von 48	08.0.30kT313	NORMAL	-
nswa1-se1 (basic-r)	2	Stackable ICX6450-48	BZU0433J00Y	15 von 48	08.0.30kT313	NORMAL	-

Total: 2

Disk Storage Komponenten

Name	Vendor	Model	Serial number	FW version	Location	Contact	Status	Inventory information
DX500 S3-02 (CE)	FUJITSU	ETERNUS DX500 S3	4621349005	V10L70-3160	DC6a_168 Pos 28	Florian	OK	-
DX500 S3-02 (DE 0x00)	FUJITSU	ETERNUS DX500 S3	JWXTP13500029	-	DC6a_168 Pos 28	Florian	OK	-
DX500 S3-02 (DE 0x10)	FUJITSU	ETERNUS DX500 S3	JWXTP13500034	-	DC6a_168 Pos 28	Florian	OK	-
ETERNUSJX40(1)@absu1se2	FUJITSU	ETERNUS JX40	-	2.130.353-1819	absu1se2	-	ERROR	-
ETERNUSJX40(1)@hnc2-se2	FUJITSU	ETERNUS JX40	-	2.130.353-1819	hnc2-se2	-	ERROR	-

Total: 5

Further components

Name	Type	Model	Serial number	Inventory information
Shelf 1	Shelf	-	-	service
RC 1	RC	rc-25	-	service

Total: 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* [→ <se server>(SE<model>)], *Administration* tab.

The *Administration* tab opens, here with an SE 700B as an example.

The screenshot displays the 'Administration' tab of the HW Inventory application. It is divided into two main sections: 'Racks' and 'Units and components'. Both sections have 'Accept changes' and 'Discard changes' buttons.

Racks Section:

No.	Name	Inventory information
1	Rack 1	Basic Rack

Total: 1

Units and components Section:

Name	Type	Model	Rack	HU	IH	Serial number	Inventory information
<i>filter</i>	<i>filter</i>	<i>filter</i>	<i>filter</i>	<i>filter</i>	<i>filter</i>	<i>filter</i>	
abgqa500	AU x86	PRIMERGY RX4770 M1	-	4	-	YLFV001001	test
abgqa600	AU x86	PRIMERGY RX4770 M1	-	4	-	YLFV001002	-
ABGSE211 (CHE-Box 0)	SU i390	SE SERVER SU700	1	2	13	00029001	-
ABGSE211 (CHE-Box 1)	SU i390	SE SERVER SU700	-	2	-	00029001	-
ABGSE211 (CHE-Box 4)	SU i390	SE SERVER SU700	1	2	15	00029001	-
ABGSE211 (CPU-Box)	SU i390	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*.

In a Management Cluster, a submenu *<se server>(SE<model>)* for each SE server is displayed below *Hardware* → *Energy*, which contains the energy settings of the respective SE server.

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).

- ▶ Select *Hardware* → *Energy* [→ *<se server>(SE<model>)*], *Monitoring* tab.

Monitoring Management Scheduled power on/off

SE Server **abgse2**: Energy Monitoring Units

Name	HW model	Rack	Current power consumption	Power status
<i>Filter</i>	<i>All</i>	<i>All</i>		<i>All</i>
abgqa500	AU47	0	372 W (of 3000 W)	ON
abgqa600	AU47	0	372 W (of 3000 W)	ON
ABGSE211 (CHE-Box 0)	SU700	1	188 W (of 267 W)	ON
ABGSE211 (CHE-Box 1)	SU700	0	110 W (of 267 W)	ON
ABGSE211 (CHE-Box 4)	SU700	1	191 W (of 267 W)	ON
ABGSE211 (CPU-Box)	SU700	1	255 W (of 817 W)	ON
abgse2mu1	MU	1	100 W (of 211 W)	ON
abgse2mu2	MU	0	104 W (of 211 W)	ON
hnc1-se2	HNC	1	96 W (of 222 W)	ON
hnc2-se2	HNC	0	96 W (of 222 W)	ON
hnc3-se2	HNC	0	96 W (of 630 W)	ON
su1-se2	SU300	0	450 W (of 1335 W)	ON

Number of Units: 12

Current power consumption: 372 Watt
 equates to 12 % of max. 3000 Watt
 Energymode: 1000 Watts (active)

Using the "percent" icon in the group header you switch between a relative and absolute consumption display. The image above is an example for the absolute display.

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* [→ <se server> (SE<model>)], *Management* tab.
The tab for creating a new template opens. If templates were already stored, these are listed and can be edited.

Monitoring **Management** Scheduled power on/off

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.)
<i>Filter</i>		<i>Filter</i>				
abgqa600	AU47	1848 W	2316 Watts (active)	2316 W	<input type="checkbox"/>	-
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	-	-	<input type="checkbox"/>	-
abgse2mu2	MU	211 W	-	-	<input type="checkbox"/>	-
au5-se2	AU47	1848 W	1000 Watts (active)	1000 W	<input type="checkbox"/>	848 W
hnc1-se2	HNC	222 W	-	-	<input type="checkbox"/>	-
hnc2-se2	HNC	197 W	-	-	<input type="checkbox"/>	-
hnc3-se2	HNC	222 W	-	-	<input type="checkbox"/>	-
su1se2	SU300	1335 W	-	-	<input type="checkbox"/>	-

Total: 12

Summary

Consumption (units)	Power limit savings	Power off savings	Saving (max.)
7712 W	380 W	0 W	380 W

Saving

380 W saved (of 7712 W) → New consumption (units): 7332 W

1.

2.

3.

Three areas are displayed:

1. You can change the settings for the template in the *Energy Templates Units* group.
2. The *Summary* group contains a summary of the total consumption of all units and the maximum energy saving with the saving options simulated in the template implemented.
3. The *Saving* group 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* [→ <se server>(SE<model>)], *Scheduled power on/off* tab.

Monitoring | Management | **Scheduled power on/off**

Server SE-Server-2 (SE700B): Scheduled power on/off of Units

Name	HW model	Monday		Tuesday		Wednesday		Thursday		Friday		Saturday		Sunday		Power status		
		On	Off	On	Off	On	Off	On	Off	On	Off	On	Off	On	Off			
Filter	Filter															All		
abgse2mu1	MU	--	--	--	--	--	--	--	--	--	--	--	--	--	--	▶ ON		
abgse2mu2	MU	--	--	--	--	--	--	--	--	--	--	--	--	--	--	▶ ON		
au5-se2	AU20	--	--	--	--	--	--	--	--	--	--	--	--	--	--	▶ ON		
hnc1-se2	HNC	--	--	--	--	--	--	--	--	--	--	--	--	--	--	▶ ON		
hnc2-se2	HNC	--	--	--	--	--	--	--	--	--	--	--	--	--	--	▶ ON		
su2-se2	SU300	--	--	--	--	--	--	--	--	--	--	--	--	--	--	▶ ON		
su3-se2	SU300	--	--	--	--	--	--	--	--	--	--	--	--	--	--	▶ ON		
test1-au1	AU47	--	--	--	--	--	--	--	--	--	--	--	--	--	--	▶ ON		
test1-au2	AU20	--	--	--	--	--	--	--	--	--	--	--	--	--	--	▶ ON		

Total: 9

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.



The functionality is not supported for SU /390 and AU PQ.

11 Managing a cluster

The *Cluster* main menu is displayed in the tree structure if you manage at least one cluster in your SE server configuration via the SE Manager:

- Two SE servers are always managed in a Management Cluster. Depending on the configuration, there can be one or more additional SU Clusters.
- In an SE server configuration with an SE server that has more than one SU x86s, an SU Cluster can be configured. In that case, only the SU Cluster but no Management Cluster exists.

A cluster is configured by Customer Support as per the customer's request.

11.1 Overview

The *Overview* tab displays all clusters in the server configuration and their status. In the *Dashboard* main menu, the *Cluster* tile displays the status of the clusters in accumulated form, and the link branches to the *Overview* tab.

11.2 Status of the Management Cluster

If an SE server configuration consists of two SE servers, the SE servers are managed together in a shared Management Cluster. The main window provides information on the central resources of the Management Cluster and their status, as well as on the overall status of the Management Cluster.

- ▶ Select *Cluster* → *Management Cluster*, *Management Cluster* tab.

Management cluster

Management cluster overview ?

Status summary ✔ NORMAL

IP networks ISL-E ✔ NORMAL

Cluster manager abgse1mu1 ✔ NORMAL

Management Unit	Server	Power status	Configuration disks	Network heartbeat
abgse1mu1	SE-Server-1	▶ ON	✔ NORMAL	✔ NORMAL
abgse1mu2	SE-Server-1	▶ ON	✔ NORMAL	✔ NORMAL
abgse2mu1	SE-Server-2	▶ ON	✔ NORMAL	✔ NORMAL
abgse2mu2	SE-Server-2	▶ ON	✔ NORMAL	✔ NORMAL

Total: 4

11.3 Managing an SU Cluster

An SU Cluster combines SUs of the same type (SU /390 or SU x86), which enable the Live Migration (LM) for BS2000 systems from one SU to another.

If an LM is currently possible (calling the wizard in the *Operation* main window of the respective BS2000 system), depends on the current status of the SU Cluster.

In order to avoid unwanted fault indications and events over long periods when maintenance takes place (e.g. SU switched off or in error status), the SU cluster can be temporarily deactivated. You can use the checkmark icon to activate or deactivate an SU Cluster.

- Select *Cluster* → <cluster-name>, *SU Cluster* tab.

SU cluster

SU cluster SE1SE2SU390: Status

Cluster name	SE1SE2SU390	<input checked="" type="checkbox"/>
Function	Live migration	
Status summary	NORMAL	

SU cluster SE1SE2SU390: Units

Unit	Model	Server	Operation mode	Power status	Configuration disks	Network heartbeat
ABGSE211	SU700	SE-Server-1	VM2000	ON	NORMAL	NORMAL
abgse1mu1				ON	NORMAL	NORMAL
abgse1mu2				ON	NORMAL	NORMAL
ABGSE221	SU700	SE-Server-2	VM2000	ON	NORMAL	NORMAL
abgse2mu1				ON	NORMAL	NORMAL
abgse2mu2				ON	NORMAL	NORMAL

Total: 2

In the example, the *SU Cluster* tab shows the current state of an SU Cluster with SU /390.

A detailed description of the cluster functionality is provided in the "Cluster Solutions for SE Servers" whitepaper [8].

12 Managing authorizations

12.1 Users

You use the *Authorizations* → *Users* menu to manage the local user accounts of all MUs of the SE server configuration and the attributes of the accounts (exception: service account). Accounts are MU-global, i.e. every account exists on every MU of the SE server configuration and always has the same attributes.

In addition to local accounts, you can also release or lock LDAP accounts for usage on the MUs of the SE server configuration, which are centrally managed on a connected LDAP server (see [section “Managing accounts” on page 300](#)).

For the administration and operation of the SE server, the administrator can assign the following roles to the accounts:

- 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 47](#).

12.1.1 Managing accounts

The administrator manages all accounts on the SE server or the SE servers of a Management Cluster, with the exception of the service accounts. He/She creates new accounts and changes or deletes existing accounts. There are local accounts and LDAP accounts:

- A local account is created on the MUs of the SE server configuration and is completely managed in the SE Manager.
- An LDAP account is created on an LDAP server and is also managed from there. For an LDAP account, "Add new account" means that the account is released for usage on the SE server and enables access to the SE Manager just like a local account. "Remove account" means the account gets locked and is no longer available for use on the SE server.

The local 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 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 local accounts, see [section "Managing passwords" on page 303](#)

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 for your local account yourself, see [section "Managing passwords" on page 303](#).

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 307](#).

On the *Accounts* tab you can create and manage accounts:



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.

Accounts | Password management | Individual rights | Sessions

Accounts

Add new account

Type	Account	Role	Name	Comment		
All	Filter	All	Filter	Filter		
🏠	admin	Administrator	System Administrator		✎	🔄
🏠	admpavel	Administrator	Admin	test2	✎	🔄
🏠	autoadm	Administrator	AutoSEM	Automatic testing	✎	🔄
🏠	brun	Administrator	Horst		✎	🔄
🏠	bs2opr	Operator	AW	BS2000 Operator	✎	🔄
🏠	bs2pavel	BS2000-Administrator	Bs2Admin		✎	🔄
🏠	btadm	Administrator	Thomas	Testkennung admin	✎	🔄
🏠	btopr	Operator	Thomas	Testkennung opr	✎	🔄
🌐	cinapa	Administrator		test	✎	🔄

An administrator can use the *Accounts* tab to view all accounts in the server configuration. Every account is available on every MU of the managed SE server configuration. A BS2000 administrator, operator, XenVM administrator or AU administrator sees only his/her own account.

Local accounts and LDAP accounts can be distinguished via the icon in the *Type* tab.

The Customer Support account *service* (*Service* role) is only displayed. You cannot administer service accounts.

Add new account

- ▶ Select *Add new account*.
- ▶ In the following dialog, select whether you want to create a local account or release an LDAP account. You only have this option if an LDAP server is configured.
- ▶ Enter all required information for the new account.



The following is required to release an LDAP account:

- On the SE server of the MU on which the LDAP is to be released, access to the LDAP server is configured and active.
- If you have activated the check in the LDAP directory tree, the account is only created if it exists in the LDAP. If you have not activated the check, you can also add an account that does not exist in the LDAP (yet).
- There must be no local account with the same name.

Note:

Access to BS2000 dialog and BS2000 console is not supported for LDAP accounts which are longer than 8 characters or contain uppercase letters.



You can create an account for the *XenVM administrator* role only if at least one SU x86 with a XenVM license exists in the SE server configuration.
You can create an account for the *AU administrator* role only if at least one AU exists in the SE server configuration.

Change account

You can change the *Name* and *Comment* properties of an account.



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 account properties.

Removing an account



Every user with the *administrator* role can remove any other user. Only the predefined accounts *admin* and *service* cannot be deleted.

- ▶ Click the *Remove* icon by the required account. Confirm the action.

The removed account is no longer displayed in the *Accounts* tab. An LDAP account is locked for use on the SE server but still exists on the LDAP server.

12.1.2 Managing passwords

In the *Password management* tab you manage the passwords of all defined local accounts.

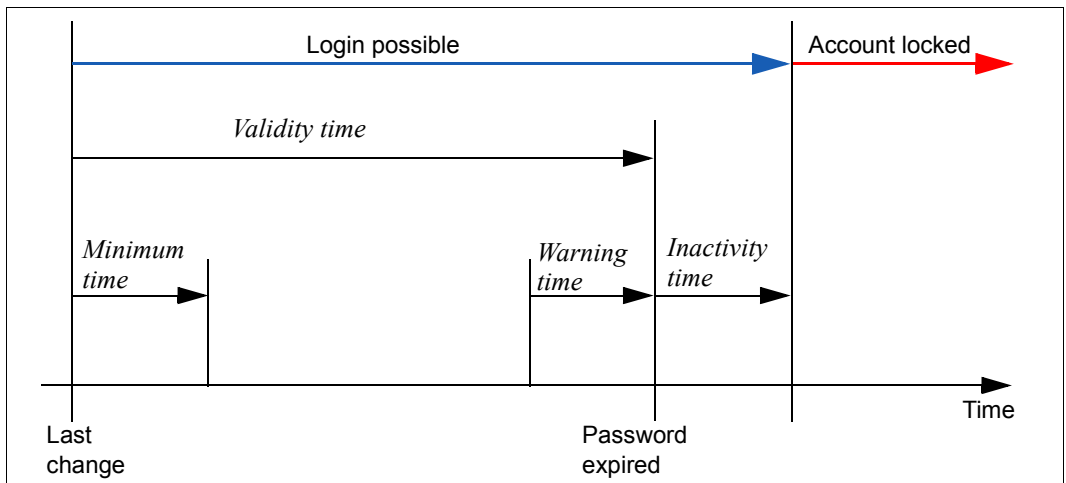


(The passwords of LDAP accounts are only managed on the LDAP server.)

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, AU administrator or XenVM administrator cannot change their 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

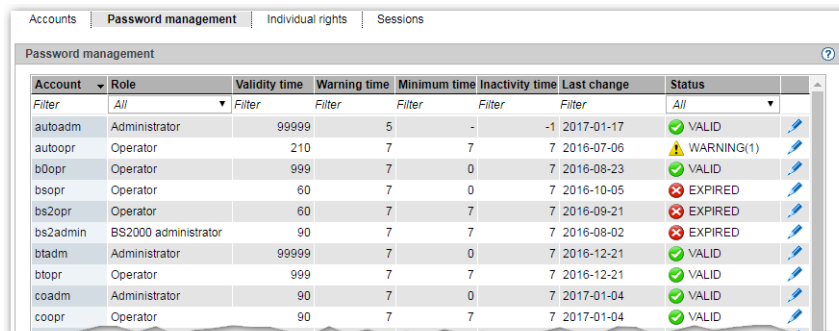
The minimum time is not relevant for an administrator account and the value 0 is therefore displayed for it.

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.

Displaying password attributes

- In the tree structure select *Authorizations* → *Users*, *Password management* tab.



The screenshot shows the 'Password management' window with a table of user accounts. The table has columns for Account, Role, Validity time, Warning time, Minimum time, Inactivity time, Last change, and Status. The status column includes icons for valid (green checkmark), warning (yellow triangle), and expired (red X) accounts.

Account	Role	Validity time	Warning time	Minimum time	Inactivity time	Last change	Status
autoadm	Administrator	99999	5	-	-1	2017-01-17	VALID
autoopr	Operator	210	7	7	7	2016-07-06	WARNING(1)
b0opr	Operator	999	7	0	7	2016-08-23	VALID
bsopr	Operator	60	7	0	7	2016-10-05	EXPIRED
bs2opr	Operator	60	7	7	7	2016-09-21	EXPIRED
bs2admin	BS2000 administrator	90	7	7	7	2016-08-02	EXPIRED
btadm	Administrator	99999	7	0	7	2016-12-21	VALID
btopr	Operator	999	7	7	7	2016-12-21	VALID
coadm	Administrator	90	7	0	7	2017-01-04	VALID
coopr	Operator	90	7	7	7	2017-01-04	VALID

The *Password management* tab displays the defined local accounts with their password attributes.

Changing passwords or password attributes



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.

Only an administrator can change password attributes.

- ▶ Click the *Change* icon for the required account and change the properties as required. In configurations with multiple MUs, the password attributes of the account are changed on all MUs.

12.1.3 Managing individual rights

The *Individual rights* tab displays all operator accounts (local accounts and LDAP accounts with the *Operator* role) and their current individual rights.

For individual rights, a distinction is made between global (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* → *Users, Individual rights* tab.

Account	On/Off	Shadow	SVP	Unit	Console rights	Dialog
bs2opr	Denied	Granted	Denied	-	-	-
btopr	Denied	Denied	Denied	-	-	-
co2opr	Denied	Denied	Denied	-	-	-
in2opr	Denied	Denied	Denied	ABGSE211 (abgse1mu1) ABGSE211 (abgse1mu2)	HV0 (M4IVR), C0 HV0 (M4IVR), C1	Granted Granted
le1opr	Granted	Denied	Granted	ABGSE211 (abgse1mu1) ABGSE211 (abgse1mu2) abgsu2se1	HV0 (M4IVR), AB VM2 (G4IVQ), C1 VM3 (G4IVP), CD VM3 (G4IVP), CD HV0 (M4IVV), CD VM2 (ABGRED02), GH	Granted Denied Granted Granted Granted
le2su390	Granted	Granted	Granted	ABGSE211 (abgse1mu1) ABGSE211 (abgse1mu2)	VM2 (G4IVQ), C0 VM2 (G4IVQ), C1	Granted Denied
le3x86	Denied	Denied	Denied	abgsu3se1 abgsu2se1	HV0 (MONITOR), C0 VM2 (ABGAFR02), C0 HV0 (MONITOR), C0 HV1, C1 VM2 (ABGRED02), C0	Denied Denied Denied Denied Denied
oop	Denied	Denied	Denied	-	-	-
oprtest2	Granted	Denied	Granted	ABGSE211 (abgse1mu1) abgsu4se1	VM2 (G4IVQ), CC VM2 (ABGGOLD2), AB VM3 (ABGGOLD3), AC	Denied Denied Granted
test1op	Denied	Denied	Denied	-	-	-

The *Individual rights* tab lists all operator accounts together with their individual rights.

Changing global rights



Only the administrator can make changes.

- In the required account click the *Change global rights* icon on the right of the *SVP* column. In the subsequent dialog, assign the required global operator rights.

Changing system-related rights

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.

12.1.4 Displaying sessions

The *Sessions* tab informs the administrator about all sessions of users who are currently logged in on the SE Manager of a Management Unit of the SE server or Management Cluster.

- Select *Authorizations* → *Users, Sessions* tab.

Accounts | Password management | Individual rights | **Sessions**

Management Unit	Account	Name	Role	IP address	Language	Autom. upd.	Timeout
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>All</i>	<i>Filter</i>	<i>All</i>	<i>Filter</i>	<i>Filter</i>
-(global)	admin	Std. Administrator	Administrator	10.172.1.270	German	10 s	-
-(global)	admin	Std. Administrator	Administrator	Lokale Konsole	English	-	-
-(global)	admin01	User AAA	Administrator	10.172.1.242	German	-	10 min
-(global)	admin02	Admin BBB	Administrator	21.172.1.18	German	-	20 min
-(global)	admb1	Admin FF	BS2000 administrator	10.172.1.28	German	60 s	60 min
-(global)	oper01	User CC	Operator	10.172.1.154	German	60 s	45 min
-(global)	service	System Service	Service	10.172.1.142	German	30 s	-
-(global)	wro	User ABC	Operator	10.172.1.277	English	-	20 min

Total: 8

The *Sessions* tab provides information on the sessions of the users currently logged in. The local *Session* is highlighted.

In addition to the information on the user and IP address of the PC, the current individual settings for the session are also displayed.

The *Management Unit* column is only displayed for multi-MU configurations. It informs on the scope of the session:

- For a global session, which is valid for all MUs of the SE server configuration, *-(global)* is displayed. No new login is required for switching to one of the other MUs.
- In a local session, the name of the MU for which the session is valid, is displayed. You must log in again when you switch to another MU. When logging in on the SE Manager, a local session is only created if the MU is addressed via the IP address or if it has not been entered in the DNS.

12.2 Configuration

The *Authorizations* → *Configuration* menu is used to manage the access to an LDAP server, which provides centrally managed accounts for use on an SE server as well as IP based access restrictions to the MUs.

12.2.1 Access to an LDAP server

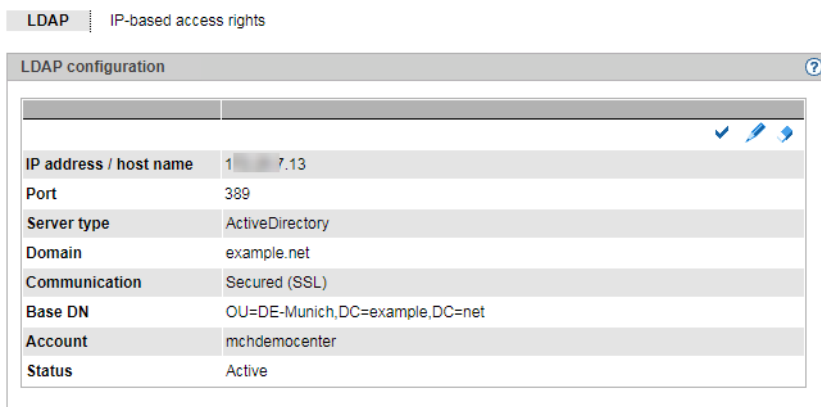
The *LDAP* tab enables you to configure and edit the access to an LDAP server on which the LDAP accounts are managed that can be released for the MUs of the SE server.



In a Management Cluster, you can configure one LDAP server per SE server. Two redundant MUs in one SE server share the same LDAP server.

The LDAP server and the MU(s) must synchronize their time via the same NTP server.

- ▶ In the tree structure select *Authorizations* → *Configuration*, *LDAP* tab.



On the *LDAP* tab, the configuration data of the currently configured LDAP server are displayed. The *Status* field informs you whether the LDAP configuration was activated or only created.



In a Management Cluster, the configurations for each SE server are displayed in individual groups. The LDAP configuration is SE server-specific, but in the default mode it is configured for both SE servers together (i.e. both get the same configuration). For more information on the LDAP configuration in the Management Cluster, see the "Cluster Solutions for SE Servers" whitepaper [8].

The following options are available to you:

Configuring access to the LDAP server

To access the LDAP server, you need a valid account on an LDAP server (Bind DN) with a password.

- ▶ Click on the *Change LDAP configuration* button, in the subsequent dialog enter the access data for the LDAP server or change the existing data. This button is only available if there is no LDAP configuration (yet) or the LDAP configuration is the same for both SE servers. You can test the new setting (*Test* button) before you confirm the configuration. By selecting the *Active* option, you can specify whether the LDAP configuration should be activated directly after creation.

Testing the LDAP configuration

- ▶ In the displayed *LDAP configuration* of the SE server, click the corresponding *Test LDAP configuration* icon. The test commences immediately and is followed by a dialog that informs you whether the LDAP configuration was successfully tested. You can only work with LDAP accounts if the test was successful.

Changing the access data of LDAP configurations

You can change individual parameters of the displayed LDAP configuration, e.g. activate or deactivate the access to the LDAP server:

- ▶ In the displayed *LDAP configuration* of the SE server, click the corresponding *Change LDAP configuration* icon and change the data of the currently entered access as you require. To activate or deactivate the access to the LDAP server, activate or deactivate the *Active* option. Confirm the action. If the access is activated and a connection to the LDAP server is established, you can use the released LDAP accounts to log in to the SE server.

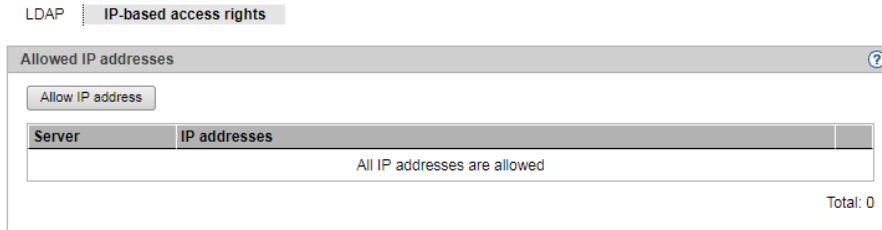
Delete LDAP configuration

- ▶ In the displayed *LDAP configuration* of the SE server, click the corresponding *Delete LDAP configuration* icon and confirm the action. On the *LDAP* tab, no configuration data are displayed (in the group) anymore.

12.2.2 IP-based access restriction to the MUs

The administrator can configure the access to the MUs (applies for access via SE Manager and CLI) of the SE server in such a manner that it is possible only for explicitly entered IP addresses or for IP addresses from an explicitly entered IP network.

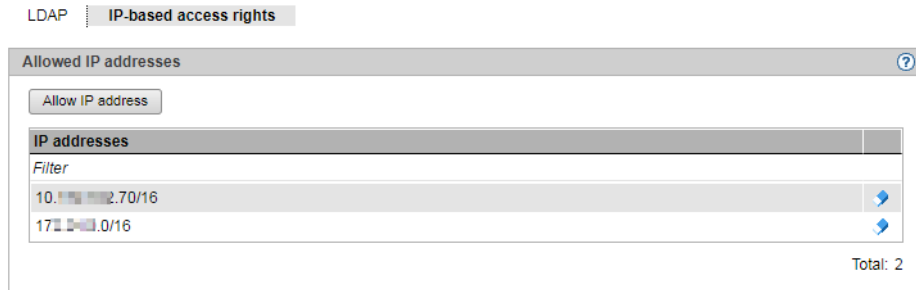
By default the list for access restrictions is empty, and access is permitted without restriction for all IP addresses and networks.



The access restriction is server-specific. In case of MU redundancy, the access restriction is valid for both MUs of the SE server.

In a Management Cluster, you can specify different IP-based access restrictions for each SE server.

- In the tree structure select *Authorizations* → *Configuration*, *IP-based access rights* tab.



The *IP-based access rights* tab displays the IP addresses and networks for which access to the MUs of the SE server is allowed.

If two SE servers form a Management Cluster, the additional *Server* column indicates for which SE server the access authorization is defined.

The following options are available to you:

Allow IP address or network

- ▶ Click *Allow IP address* and enter the IP address or network in the subsequent dialog box. Syntax: *<ip address>[/<network mask>]*

For a Management Cluster, you also have to determine whether the access restriction is valid for all SE servers or only for a single SE server. The default is *All*.



With the first entry (IP address or IP network) you enable IP-based access restriction to the MUs of the SE server. Access is then only possible for IP addresses which are entered either explicitly or via an IP network. Because of that, the IP address of your administration PC, from which you have logged on to the SE Manager, should be part of the first entry.

Remove IP address or network

- ▶ By the required IP address or network, click the *Remove* icon and confirm the action.



As soon as you delete the last entry from the list for access restrictions, access to the MUs of the SE server is once again possible for all IP addresses without restriction. You should delete the entry that contains the address of your administration PC last.

12.3 Certificates

12.3.1 SSL 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.

12.3.1.1 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.

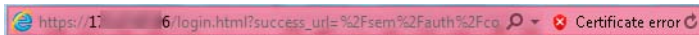
We recommend that you close this webpage and do not continue to this website.

- 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.

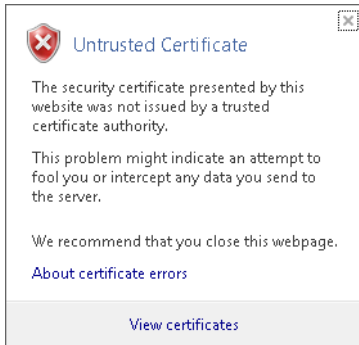
You are shown the login page. The browser's address bar displays *Certificate Error* as a warning.



The certificate has now been temporarily accepted for this session, and you can now work with the SE Manager of this system.

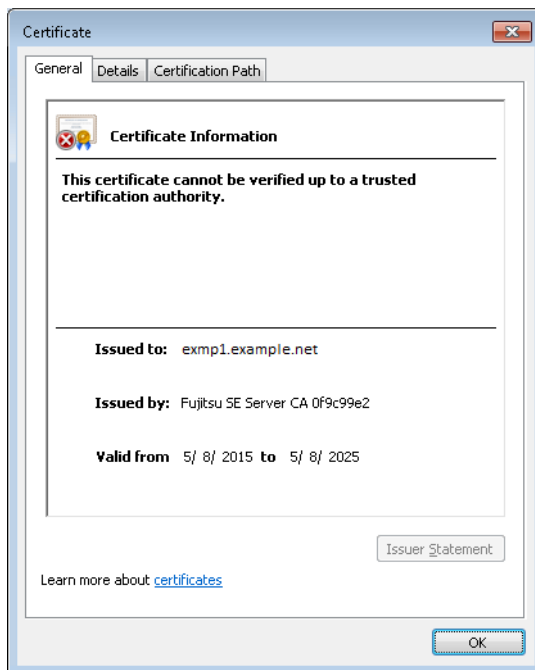
To prevent this browser message from being displayed in future, you can also import the certificate.

- ▶ Click *Certificate Error* in the browser's address bar.



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*.



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 through installation of the certificate step by step.



You have to explicitly select "Trusted root certification authorities" as certificate memory (for details, see "Security Manual" [6]).

Alternatively or for other browsers, you can also download and install the CA certificate, see [page 322](#).

12.3.2 Managing certificates

The *Certificates* menu option enables you to create and manage SSL certificates. 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* menu option 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 SSL 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 option is provided in the SE Manager help.



Digital certificates are system-specific, i.e. they are managed MU-specifically. In an SE server configuration with multiple MUs (MU redundancy on an SE server or Management Cluster with two SE servers) there is a submenu for each MU beneath *Certificates* in the tree structure, named `<mu-name>` (*MU*).

12.3.2.1 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* → *Certificates* [→ <mu-name> (MU)].

The *Certificates* tab with the *Current SSL certificate* and *Current request for an SSL certificate* groups opens.

Certificates

Management Unit **abgsilver**: Current SSL certificate ?

Create and enable new SSL certificate

Upload and enable SSL certificate

Certificate	Standard certificate
Issued for (CN)	abqse2mu2.abq.fsc.net, abqse2mu2, 172.17.0.67, 111, localhost
Issued by (CN)	Fujitsu SE Server CA 9e2e65b5
Valid from	2017-08-10
Valid to	2027-08-10
Validity period in days	3652

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* → *Certificates* [→ <mu-name> (MU)].

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.

12.3.2.2 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.



Notes:

- 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 314](#)).
- ▶ In the tree structure select *Authorizations* → *Certificates* [→ <mu-name> (MU)].
 - ▶ 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.

12.3.2.3 Requesting an SSL certificate



Any existing request is overwritten.

For the following reasons you should not perform reinstallation or change the host name between requesting an SSL certificate (creation of the certificate signing request) and entering the signed certificate into 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* → *Certificates* [→ <mu-name> (MU)].
- ▶ 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 320.
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 321 and section “[Using the standard certificate](#)” on page 317.

Displaying details of the current SSL certificate request

- ▶ In the tree structure select *Authorizations* → *Certificates* [→ <mu-name> (MU)].
- ▶ In the *Current request for an SSL certificate* group, click the *Details* icon.
The *Detailed display of the current SSL certificate request* dialog box opens. The information displayed is described in the SE Manager help.

Downloading the SSL certificate request

- ▶ In the tree structure select *Authorizations* → *Certificates* [→ <mu-name> (MU)].
- ▶ 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.

12.3.2.4 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 SSL certificate” on page 319](#)) 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.



Notes:

- 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 314](#)).
-
- ▶ In the tree structure select *Authorizations* → *Certificates* [→ <mu-name> (MU)].
 - ▶ 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* → *Certificates* [→ <mu-name> (MU)], *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.

13 Managing logging functions

The *Logging* menu comprises the functions for central management of the audit and event logging and the configuration of the alarm management of the SE server configuration.



In a multi-MU configuration, the following must be observed when displaying audit logging records and events on an MU:

In normal operation, the displayed entries are the same at each MU.

However, if an MU is not available during the generation of an entry (e.g. switched off), the entry cannot be propagated to that MU. Because of that, the displayed entries and the date of the oldest entries can differ between the MUs.

Especially the MUs in a Management Cluster will always show differences.

13.1 Displaying audit logging

The logging records from the audit logging are displayed in the *Audit Logging* tab.

Audit logging logs every action that is executed on a Unit (MU, SU, HNC) of the SE server configuration via the SE Manager, an add-on or a CLI command. This enables you as administrator to trace at all times who performed which action and when.

- ▶ Select *Logging* → *Audit Logging*, *Audit Logging* tab.

The screenshot shows the 'Audit logging' tab in a software interface. At the top, there's a search bar for 'Period' set to '2017-08-24 00:00:00 -'. Below it, navigation controls show '1 to 256 from 874', 'Page 1 from 4', and 'Go to page 1'. The table below lists logging entries with the following columns: Date, Unit, Account, Component, Type, and Message. The entries are sorted by date and time, with the most recent at the top.

Date	Unit	Account	Component	Type	Message
2017-08-24 16:57:09	abgsu2se1	root	CLI	OK	vmManage vm-last-ipl-set -d ABGAFR03 --activate no
2017-08-24 16:57:09	abgsu2se1	root	CLI	Start	vmManage vm-last-ipl-set -d ABGAFR03 --activate no
2017-08-24 17:45:59	abgsu2se1	root	CLI	OK	vmManage vm-last-ipl-set -d ABGAFR02 -a yes -y 9924 -c Z2 --system-name=ABGAFR02 -u FAST
2017-08-24 17:45:59	abgsu2se1	root	CLI	Start	vmManage vm-last-ipl-set -d ABGAFR02 -a yes -y 9924 -c Z2 --system-name=ABGAFR02 -u FAST
2017-08-24 16:57:07	abgsu2se1	root	CLI	OK	vmManage vm-last-ipl-set -d ABGAFR02 --activate no
2017-08-24 16:57:07	abgsu2se1	root	CLI	Start	vmManage vm-last-ipl-set -d ABGAFR02 --activate no
2017-08-24 17:58:13	abgsu2se1	root	CLI	Start	vmManage vm-aset-set -d 2 *STDSET
2017-08-24 17:42:12	abgsu2se1	root	CLI	OK	vmManage vm-aset-set -d 2 *STDSET
2017-08-24 17:42:12	abgsu2se1	root	CLI	Start	vmManage vm-aset-set -d 2 *STDSET
2017-08-24 17:51:17	abgsu2se1	root	CLI	Start	vmManage vm-aset-set -d 2 *STDSET
2017-08-24 17:51:17	abgsu2se1	root	CLI	OK	vmManage vm-aset-set -d 2 *STDSET
2017-08-24 17:58:13	abgsu2se1	root	CLI	OK	vmManage vm-aset-set -d 2 *STDSET
2017-08-24 16:15:46	abgse1mu2	service	CLI	OK	system
2017-08-24 16:15:16	abgse1mu2	service	CLI	Start	system
2017-08-24 19:07:24	abgse1mu1	wwwrun	CLI	Start	svp.org ipl fast 9904 -m vm2000
2017-08-24 19:08:33	abgse1mu1	wwwrun	CLI	OK	svp.prr.inl fast 9904 -m vm2000

The *Audit Logging* tab lists the logging entries sorted according to their time stamps (newest action first).

You can use the *Period:* field to filter for entries from a certain time.

A log entry contains the following information:

- Time stamp with date and time at which the action was executed



In order for the time stamp to be consistent, it is assumed that all units (MU, SU x86, HNC, etc.) are synchronized with an NTP server.

- Name of the unit on which the action was executed
- Account under which the action was executed
- Component on which the action was started: *SEM* (SE Manager), *<add-on name>* or *CLI* (Command Line Interface)
- Type of the log entry or executed action, e.g. login or start
- Message with details on the action, e.g. parameter values, result message

13.2 Displaying event logging

The *Event Logging* function displays the logged events in the *Current events* and *All events* tab.



The dashboard of the SE Manager contains the *Events* tile, on which the number of currently pending events is displayed, depending on their weights (NOTICE, WARNING, ERROR etc.). The tile is linked to the *Current events* tab of the *Event Logging*.

Current events

- ▶ Select *Logging* → *Event Logging*, *Current events* tab.

Timestamp	Weight	Unit	Component	Message
2017-08-27 20:47:16	NOTICE	abgse1mu1	Sys-Mgmt	VM 'G4IVO' on Server Unit 'ABGSE211' started
2017-08-27 20:45:19	NOTICE	abgse1mu1	Sys-Mgmt	VM 'G4IVO' on Server Unit 'ABGSE211' stopped
2017-08-27 20:45:16	NOTICE	abgse1mu1	Sys-Mgmt	VM 'G4IVO' on Server Unit 'ABGSE211' paused
2017-08-27 20:43:53	NOTICE	abgsu2se1	Sys-Mgmt	VM 'ABGAFR05' on Server Unit 'abgsu2se1' started
2017-08-27 20:43:38	NOTICE	abgsu2se1	Sys-Mgmt	VM 'ABGAFR05' on Server Unit 'abgsu2se1' stopped
2017-08-27 20:42:21	NOTICE	abgsu2se1	Sys-Mgmt	VM 'ABGAFR05' on Server Unit 'abgsu2se1' started
2017-08-27 20:42:13	NOTICE	abgsu2se1	Sys-Mgmt	VM 'ABGAFR05' on Server Unit 'abgsu2se1' stopped
2017-08-27 20:42:12	NOTICE	abgsu2se1	Sys-Mgmt	VM 'ABGAFR05' on Server Unit 'abgsu2se1' paused
2017-08-27 20:40:10	NOTICE	abgse1mu1	Sys-Mgmt	VM 'G4IVO' on Server Unit 'ABGSE211' started
2017-08-27 20:40:06	NOTICE	abgse1mu1	Sys-Mgmt	VM 'G4IVO' on Server Unit 'ABGSE211' stopped
2017-08-27 20:40:02	NOTICE	abgse1mu1	Sys-Mgmt	VM 'G4IVO' on Server Unit 'ABGSE211' paused
2017-08-25 19:27:24	NOTICE	abgse1mu1	Sys-Mgmt	VM 'G4IVN' on Server Unit 'ABGSE211' deleted
2017-08-25 19:27:20	NOTICE	abgse1mu1	Sys-Mgmt	VM 'G4IVN' on Server Unit 'ABGSE211' paused
2017-08-25 19:27:18	NOTICE	abgse1mu1	Sys-Mgmt	VM 'G4IVN' on Server Unit 'ABGSE211' created
2017-08-25 15:33:50	NOTICE	abgse1mu2	abgse1mu2	M2000 activated
2017-08-25 15:28:00	NOTICE	abgse1mu2	M2000	M2000 deactivated
2017-08-25 15:18:52	NOTICE	abgse1mu1	Sys-Mgmt	VM 'TESTVM1' on Server Unit 'ABGSE211' activated

The *Current events* tab contains a list of all events that have occurred since the last time you acknowledged events. You can only acknowledge the whole table:

- ▶ Click on the *Acknowledge current events* tab and confirm the action.

All currently displayed events are removed from the table and are now only visible in the *All events* tab.

All events

- ▶ Select *Logging* → *Event Logging*, *All events* tab.

Timestamp	Weight	Unit	Component	Message
2017-08-27 20:47:16	NOTICE	abgse1mu1	Sys-Mgmt	VM 'G4IVO' on Server Unit 'ABGSE211' started
2017-08-27 20:45:19	NOTICE	abgse1mu1	Sys-Mgmt	VM 'G4IVO' on Server Unit 'ABGSE211' stopped
2017-08-27 20:45:16	NOTICE	abgse1mu1	Sys-Mgmt	VM 'G4IVO' on Server Unit 'ABGSE211' paused
2017-08-27 20:43:53	NOTICE	abgsu2se1	Sys-Mgmt	VM 'ABGAFR05' on Server Unit 'abgsu2se1' started
2017-08-27 20:43:38	NOTICE	abgsu2se1	Sys-Mgmt	VM 'ABGAFR05' on Server Unit 'abgsu2se1' stopped
2017-08-27 20:42:21	NOTICE	abgsu2se1	Sys-Mgmt	VM 'ABGAFR05' on Server Unit 'abgsu2se1' started
2017-08-27 20:42:13	NOTICE	abgsu2se1	Sys-Mgmt	VM 'ABGAFR05' on Server Unit 'abgsu2se1' stopped
2017-08-27 20:42:12	NOTICE	abgsu2se1	Sys-Mgmt	VM 'ABGAFR05' on Server Unit 'abgsu2se1' paused
2017-08-27 20:40:10	NOTICE	abgse1mu1	Sys-Mgmt	VM 'G4IVO' on Server Unit 'ABGSE211' started
2017-08-27 20:40:06	NOTICE	abgse1mu1	Sys-Mgmt	VM 'G4IVO' on Server Unit 'ABGSE211' stopped
2017-08-27 20:40:02	NOTICE	abgse1mu1	Sys-Mgmt	VM 'G4IVO' on Server Unit 'ABGSE211' paused
2017-08-25 19:27:24	NOTICE	abgse1mu1	Sys-Mgmt	VM 'G4IVN' on Server Unit 'ABGSE211' deleted
2017-08-25 19:27:20	NOTICE	abgse1mu1	Sys-Mgmt	VM 'G4IVN' on Server Unit 'ABGSE211' paused
2017-08-25 19:27:18	NOTICE	abgse1mu1	Sys-Mgmt	VM 'G4IVN' on Server Unit 'ABGSE211' created
2017-08-25 15:33:50	NOTICE	abgse1mu2	abgse1mu2	M2000 activated
2017-08-25 15:28:00	NOTICE	abgse1mu2	M2000	M2000 deactivated
2017-08-25 15:18:52	NOTICE	abgse1mu1	Sys-Mgmt	VM 'TESTVM1' on Server Unit 'ABGSE211' activated

In this group, all occurred events are listed.

Default sorting and scope of the listed results

In both tabs, the default sorting is by the time stamp of the events, with the newest event listed first.

In the *All Events* tab you can use the *Period:* field to filter for entries from a certain time.



To ensure that the time stamps are consistent, it is required that all units (MU, SU x86, HNC etc.) are synchronized with an NTP server.

See also [section "NTP server" on page 36](#).

To restrict the number of displayed results, you can filter by the following criteria:

- Weight of the event (e.g. >=WARNING, >=ERROR, >=CRITICAL)
- Name of the unit on which the message was issued
- Component that issued the warning (e.g. M2000, X2000, Sys-Mgmt, cluster or name of an installed add-on)
- Message text



The currently possible events with messages are listed in the online help of the SE Manager under "Further information".

13.3 Alarm management

As administrator, you can use the *Alarm management* tab to configure rules for the automatic messaging in case of events on the units of the SE server configuration. There are two possible types of messages:

- A management station can be informed via SNMP trap. Traps are unsolicited messages of the SNMP agent.
- A user can be informed via e-mail.

You decide which servers are informed via SNMP trap and which users are informed via e-mail. You decide for each receiver, which weight an event must have to trigger a message.

- ▶ Select *Logging* → *Alarm management*, *Alarm management* tab.

Alarm management

SNMP trap receivers

Add new trap receiver

Receiver	Community	SNMP version	Weight			
Filter	Filter	All	All			
172.17.0.139	icinga	SNMPv2c	>= ERROR			
172.17.0.139	icinga2	SNMPv2c	>= CRITICAL			
icinga.example.net	icinga	SNMPv2c	ANY			

Total: 3

Mail configuration

Create mail configuration

SMTP server	Return address		
mail.example.net	se-alarm-mgmt@reply.no		

Mail receivers

Add new mail receiver

Receiver	Weight			
Filter	All			
abc.user1@example.com	ANY			
def.user2@example.com	>= WARNING			
info.admin@example.com	>= CRITICAL			

Total: 6

The *Alarm management* tab contains information on the receivers of messages via SNMP trap, the e-mail configuration and the receivers of messages via e-mail.

A message via e-mail has the following properties:

- Subject: *SE server alarm management notification (<weight>)*
- The content of the mail shows the event or a list of the events of the last minute in the following format:

`<timestamp>;<weight>;<management-unit>;<component>;<message>`

For a list of possible events, see *Further information* → *Events* in the online help.

The following functions are available in the *Alarm management* tab:

Add a new SNMP trap receiver:

- ▶ In the *SNMP trap receiver* group, click the *Add new trap receiver* tab and in the subsequent dialog, enter the required information for the trap receiver. Define a threshold weight, starting from which messages should be triggered, and confirm the action.

Change the properties of an SNMP trap receiver

- ▶ In the *SNMP trap receiver* group click the *Change* icon by the required receiver. Modify the weight and confirm the action.

Remove an SNMP trap receiver from the list

- ▶ In the *SNMP trap receiver* group click the *Delete* icon by the required receiver and confirm the action.

Test the messages for an SNMP trap receiver

You can send a test trap to a receiver. If the test trap is successfully received, the properties of the receiver are ok.

- ▶ In the *SNMP trap receiver* group click the *Test* icon by the required receiver and confirm the action.

Create mail configuration

For messaging via e-mail, you need an SMTP server that sends the e-mails. There should also be a return address entered in the sent e-mails. If there is no e-mail configuration configured yet, proceed as follows:

- ▶ In the *mail configuration* group, click the *Create mail configuration* button and in the subsequent dialog, enter the required information. Then confirm the action.

Change mail configuration

If you want to change the data of an existing e-mail configuration, proceed as follows:

- ▶ In the *mail configuration*, click the *Change* icon. Modify the required properties and confirm the action.

Delete mail configuration

- ▶ In the *Mail configuration* group click on the *Remove* icon by the entered SMTP server and confirm the action.

Add new email receiver

- ▶ In the *Mail receiver* group, click the *Add new mail receiver* button and in the subsequent dialog enter the e-mail address of the receiver. Define a threshold weight, starting from which messages should be triggered, and confirm the action.

Change the properties of a mail receiver

- ▶ In the *Mail receiver* group click the *Change* icon by the required receiver. Modify the weight and confirm the action.

Remove a mail receiver from the list

- ▶ In the *Mail receiver* group click the *Delete* icon by the required receiver and confirm the action.

Test the messages for an e-mail receiver

You can send a test mail to a receiver. If the e-mail is successfully received, the mail configuration and the e-mail address of the receiver are in order.

- ▶ In the *Mail receiver* group click the *Test* icon by the required receiver and confirm the action.

14 Appendix

The sections below describe the alternative BS2000 operation using PuTTY and the key assignments of the EMDS application of the operation instance BS2000 terminal.

14.1 Operating BS2000 with PuTTY

Users with the roles administrator, BS2000 administrator or operator have access to the CLI commands *bs2Console*, *bs2Dialog* and *svpConsole* on the Management Unit (MU). Upon entering the correct parameters, these commands open the correct operation instance (BS2000 console, BS2000 terminal or SVP console) on the specified Server Unit.

Below, we will use a few examples to quickly outline how you can use these commands for the alternate BS2000 operation under PuTTY.

In general:

- A prerequisite for this is a valid account for the role administrator, BS2000 administrator or operator on the Management Unit. Both local accounts and LDAP accounts can be used.
- The respective command is specified in PuTTY as follow-up command.



An administrator has access to the CLI and can therefore use the commands directly in the shell.

- Some special settings are required for an ideal display and the use of specific shortcuts.

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.

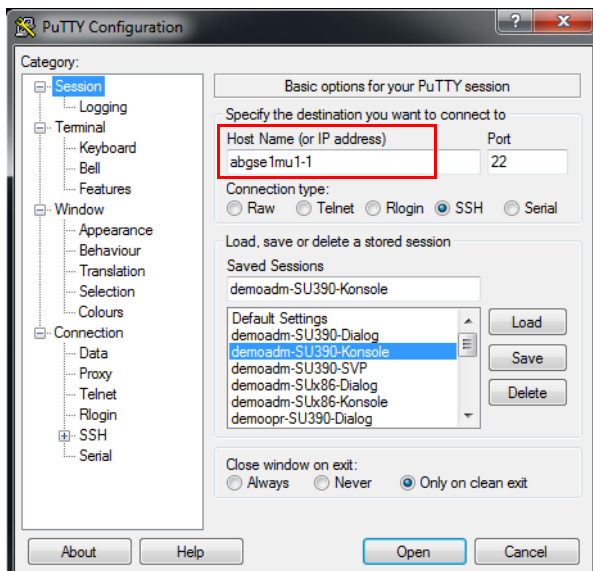
A detailed syntax description of the CLI commands is provided in the CLI command reference, see the online help under *Further information* → *PDF documents*.

Notes on PuTTY

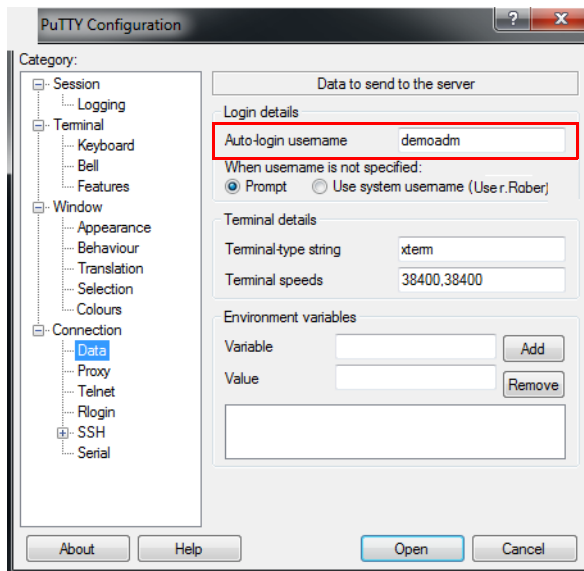
- Access to the Management Unit is only possible with the most recent PuTTY versions (from version 0.63 onwards).
- You can find the most recent version on the PuTTY download page:
<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>

14.1.1 BS2000 console on MU or SU /390

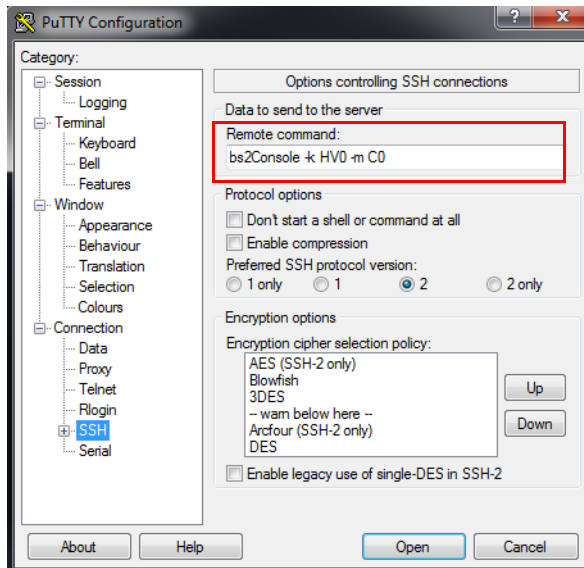
- ▶ Address the MU via hostname or IP address.
- ▶ Optional: Save the session under a meaningful name (*Session* menu).
- ▶ Optional: Set a meaningful name for the title bar (*Window* → *Behaviour* menu).



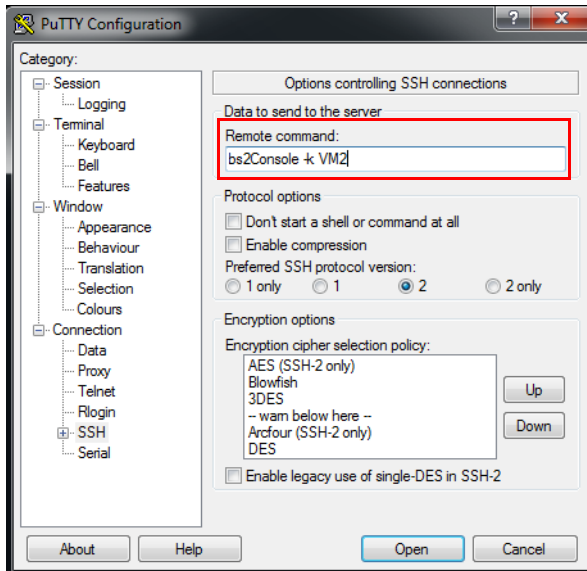
- ▶ Enter your own account (*Connection* → *Data* menu):



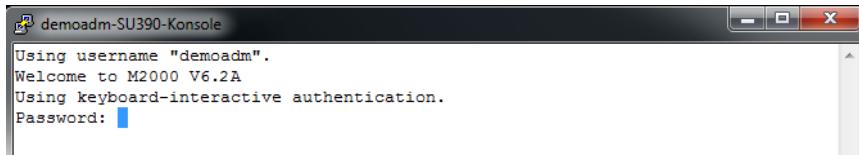
- ▶ Enter the *bs2Console* follow-up command with the following parameters:
 - the KVP of the local or explicitly addressed MU
 - only as administrator or BS2000 administrator: the console MN



As operator, you may not enter the console MN! It is defined in the individual rights and will be determined:



- In the console window, enter the password for the specified account:



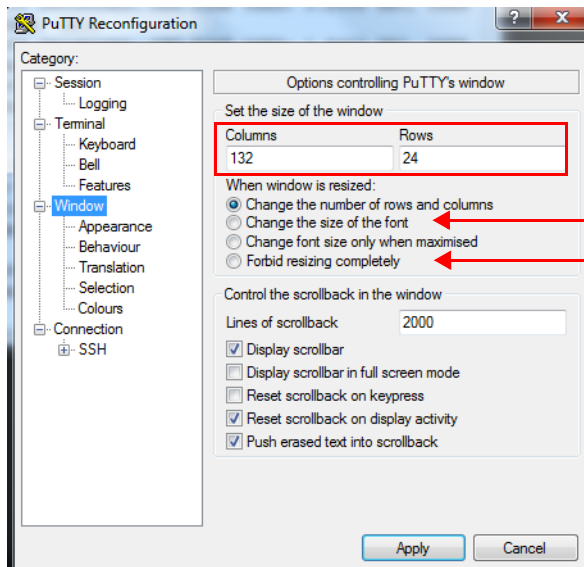
After successful login, the connection to the console of the BS2000 system to which the specified KVP is assigned, is opened:

```

demoadm-SU390-Konsole
%1J0U-000.161837 % EXC0420 /LOGOFF PROCESSED. CPU TIME USED: 0.2008 SEC, USER
ID: TSOS, TASK ID: 00020E1E, JOB NAME: HAUS
%1J0V-000.161847 % EXC0420 /LOGOFF PROCESSED. CPU TIME USED: 1.9383 SEC, USER
ID: TSOS, TASK ID: 00020E1B, JOB NAME: HAUS
%1J0W-000.161857 % EXC0420 /LOGOFF PROCESSED. CPU TIME USED: 0.2952 SEC, USER
ID: TSOS, TASK ID: 00020E1A, JOB NAME: HAUS
% UCO-000.161857 % NBR1201 TASK '1J0W' OF OPERATOR 'TSOS' DISCONNECTED FROM SU
BSYSTEM OPERATING
KVP0002 NEW KVP PARAMETER FILE ACTIVATED
%1J00-000.172553 % JMS0154 'TSOS' LOGGED ON FOR 'P#MANL01/DSS007'. JOB NAME 'D
EMOADM'. CALLER '(NONE)'. TID 00020DD2
%1J00-000.200648 % EXC0736 ABNORMAL TASK TERMINATION. ERROR CODE 'SSM1015': /H
ELP-MSG SSM1015
%1J00-000.200648 % EXC0420 /LOGOFF PROCESSED. CPU TIME USED: 0.0042 SEC, USER
ID: TSOS, TASK ID: 00020DD2, JOB NAME: DEMOADM
%1J01-000.202302 % JMS0154 'TSOS' LOGGED ON FOR 'P#MANL01/DSS007'. JOB NAME 'D
EMOADM'. CALLER '(NONE)'. TID 00020DC1
%1J01-000.202320 % BLS0519 PROGRAM 'EDTSTART' LOADED
%1J01-000.202330 % BLS0519 PROGRAM 'IMSSDF' LOADED
%1J01-000.202343 % EXC0420 /LOGOFF PROCESSED. CPU TIME USED: 0.0901 SEC, USER
ID: TSOS, TASK ID: 00020DC1, JOB NAME: DEMOADM
KVP0002 NEW KVP PARAMETER FILE ACTIVATED
SYS HVO DEMOADM C0 abgse1mu1-1 2015-03-06 10:02

```

- Choose an alternative setting for the window size (the default size is 80 x 24). To avoid line breaks, we recommend using 132 columns:



When operating the BS2000 console, you can change the size by dragging; the number of columns and lines is automatically adapted, based on the settings. Some other potentially useful settings for the window size are:

- Changing the font size together with the window size: *Change size of the font* (see above)
- Set a fixed window size: *Forbid resizing completely* (see above)

The console window with 132 columns:

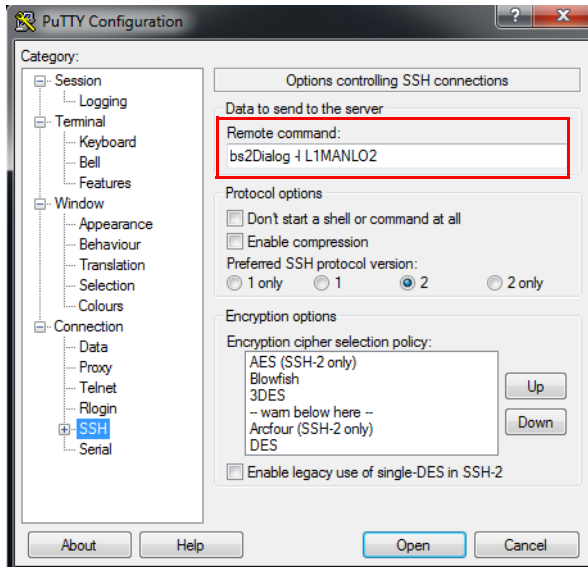
```

demoadm-SU390-Konsole
%1J0W-000.161857 % EXC0420 /LOGOFF PROCESSED. CPU TIME USED: 0.2952 SEC, USER ID: TSOS, TASK ID: 00020E1A, JOB NAME: HAUS
% UCO-000.161857 % NBR1201 TASK '1J0W' OF OPERATOR 'TSOS' DISCONNECTED FROM SUBSYSTEM OPERATING
KVP0002 NEW KVP PARAMETER FILE ACTIVATED
%1J00-000.172553 % JMS0154 'TSOS' LOGGED ON FOR 'P#MANLO1/DSS007'. JOB NAME 'DEMOADM'. CALLER '(NONE)'. TID 00020DD2
%1J00-000.200648 % EXC0736 ABNORMAL TASK TERMINATION. ERROR CODE 'SSM1015': /HELP-MSG SSM1015
%1J00-000.200648 % EXC0420 /LOGOFF PROCESSED. CPU TIME USED: 0.0042 SEC, USER ID: TSOS, TASK ID: 00020DD2, JOB NAME: DEMOADM
%1J01-000.202302 % JMS0154 'TSOS' LOGGED ON FOR 'P#MANLO1/DSS007'. JOB NAME 'DEMOADM'. CALLER '(NONE)'. TID 00020DC1
%1J01-000.202320 % BLS0519 PROGRAM 'EDTSTART' LOADED
%1J01-000.202330 % BLS0519 PROGRAM 'LMSDF' LOADED
%1J01-000.202343 % EXC0420 /LOGOFF PROCESSED. CPU TIME USED: 0.0901 SEC, USER ID: TSOS, TASK ID: 00020DC1, JOB NAME: DEMOADM
KVP0002 NEW KVP PARAMETER FILE ACTIVATED
/sta m
+ UCO-000.100416 ? VMM-001.110515 % EXC0889 MAXIMUM REACHED IN SLOT POOL WITH SPID AT 71FE9BD8
! UCO-000.100416 % NBR0740 COMMAND COMPLETED 'STA'; (RESULT: SC2=000, SC1=000, MC=CMD0001); DATE: 2015-03-06
SYS HVO DEMOADM CO abgse1mu1-1 2015-03-06 10:04

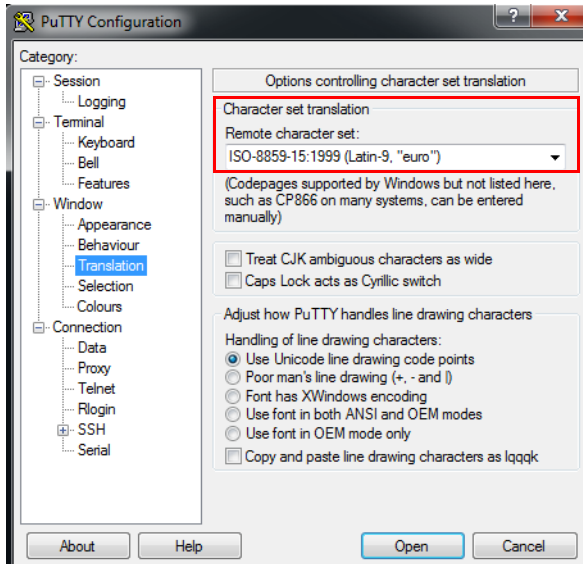
```

14.1.2 BS2000 dialog on MU or SU /390

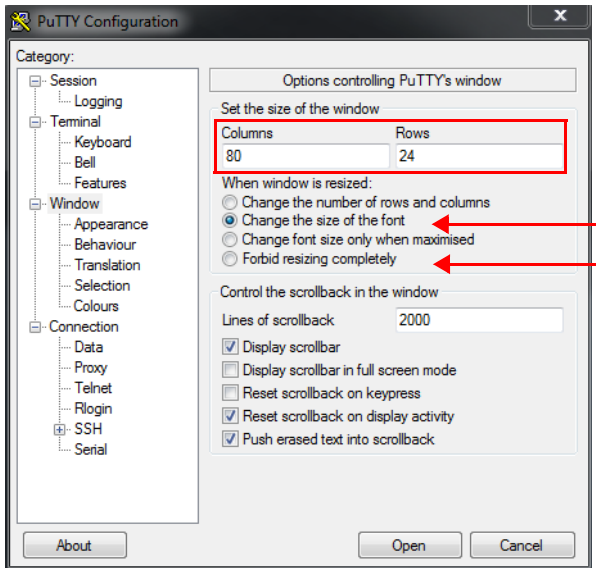
- ▶ Enter the *bs2Dialog* follow-up command with the following parameters:
 - a LOCLAN connection of the local or explicitly addressed MU



- ▶ Specify a character set that supports the display and the keyboard shortcuts required in the BS2000 dialog (*Window* → *Translation* menu):

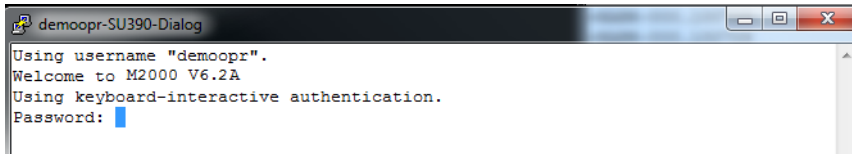


- ▶ Make sure to retain the default window size of 80 columns and 24 lines!



The number of columns and lines may not change when the dialog window is dragged, as this would disrupt the display. Therefore, select one of the following settings for window size:

- Changing the font size together with the window size: *Change size of the font* (see above)
 - Set a fixed window size: *Forbid resizing completely* (see above)
- ▶ In the dialog window, enter the password for the specified account:

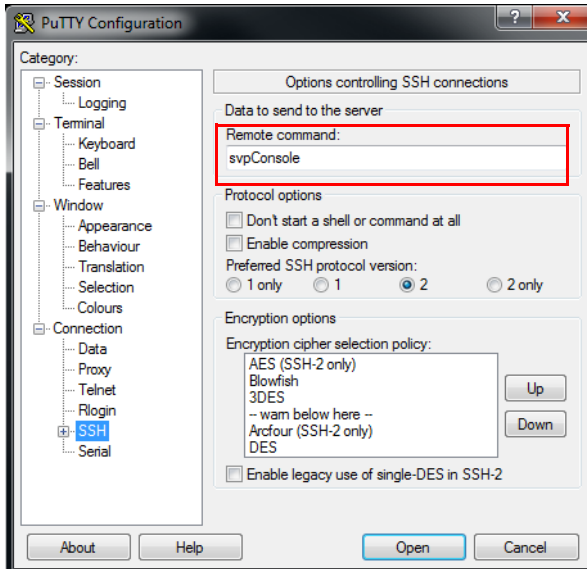


After successful login, the connection to the BS2000 dialog is opened and you can login to BS2000. Important keys:

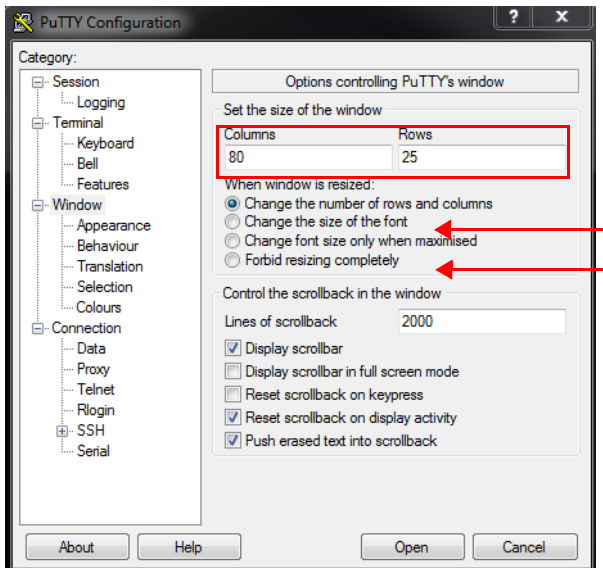
- K1 F5
- K2 F6
- EM F11
- DUE F12

14.1.3 SVP console on MU or SU /390

- ▶ Enter the *svpConsole* follow-up command:

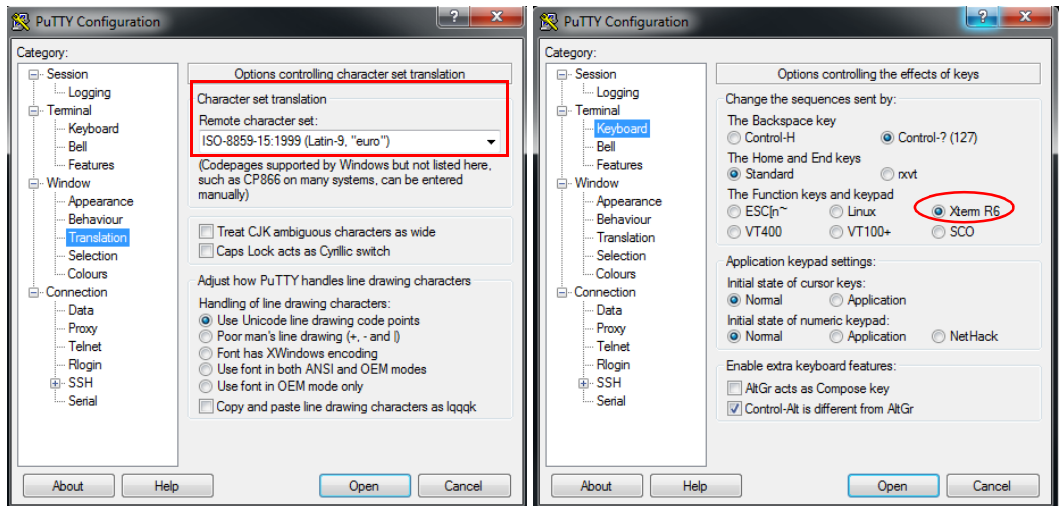


- ▶ Specify a window size of 80 columns and 25 lines. This setting must be kept at all times!



The number of columns and lines may not change when the dialog window is dragged, as this would disrupt the display. Therefore, select one of the following settings for window size:

- Changing the font size together with the window size: *Change size of the font* (see above)
- Set a fixed window size: *Forbid resizing completely* (see above)
- Specify a character set (*Window* → *Translation* menu) and a keyboard (*Terminal* → *Keyboard* menu) that support the display and keys required on the SVP console:



- In the console window, enter the password for the specified account:

```

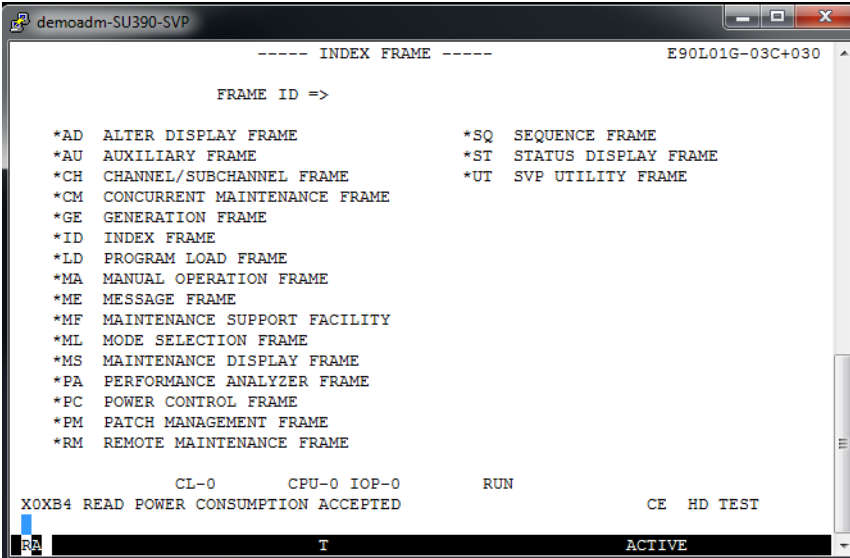
demoadm-SU390-SVP
Using username "demoadm".
Welcome to M2000 V6.2A
Using keyboard-interactive authentication.
Password: █

```

After successful login, the connection to the SVP console is opened. Important keys:

PF3 ESC + F3 (in this order)

INDEX ESC + F2 (in this order)

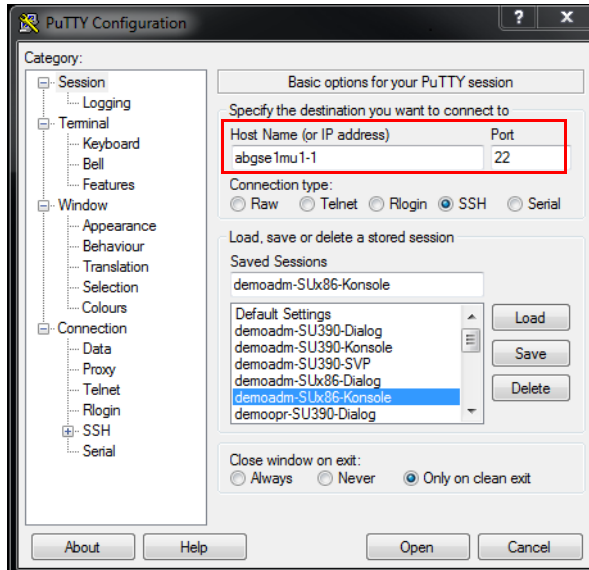


```
----- INDEX FRAME -----                                E90L01G-03C+030
      FRAME ID =>
*AD ALTER DISPLAY FRAME                                *SQ SEQUENCE FRAME
*AU AUXILIARY FRAME                                  *ST STATUS DISPLAY FRAME
*CH CHANNEL/SUBCHANNEL FRAME                        *UT SVP UTILITY FRAME
*CM CONCURRENT MAINTENANCE FRAME
*GE GENERATION FRAME
*ID INDEX FRAME
*LD PROGRAM LOAD FRAME
*MA MANUAL OPERATION FRAME
*ME MESSAGE FRAME
*MF MAINTENANCE SUPPORT FACILITY
*ML MODE SELECTION FRAME
*MS MAINTENANCE DISPLAY FRAME
*PA PERFORMANCE ANALYZER FRAME
*PC POWER CONTROL FRAME
*PM PATCH MANAGEMENT FRAME
*RM REMOTE MAINTENANCE FRAME

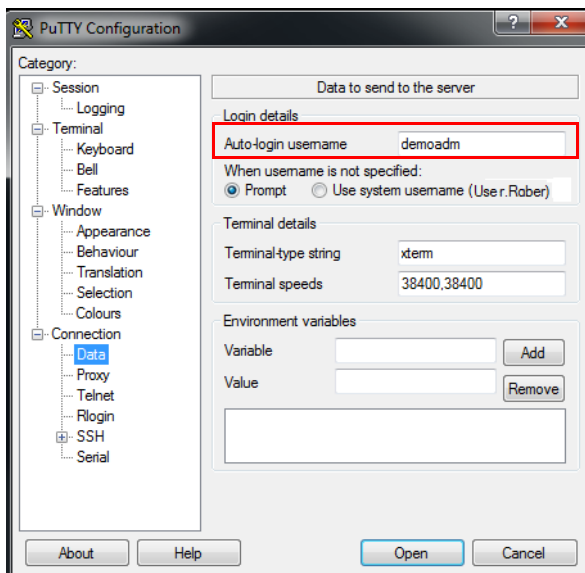
          CL-0      CPU-0 IOP-0      RUN
X0XB4 READ POWER CONSUMPTION ACCEPTED                CE HD TEST
RM T ACTIVE
```


14.1.4 BS2000 console on SU x86

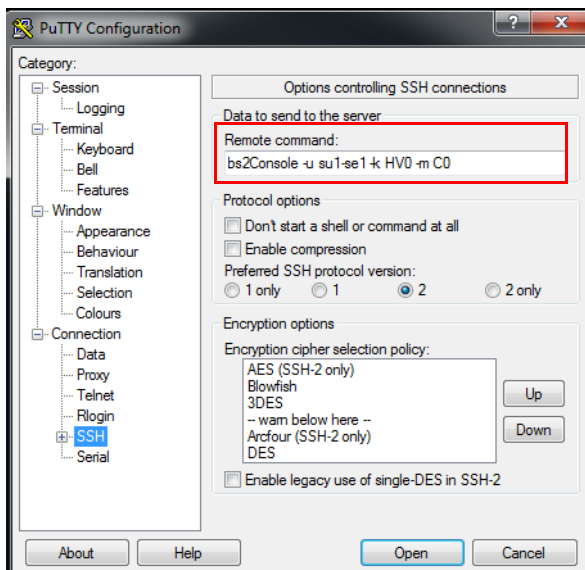
- ▶ Address the MU via hostname or IP address.
- ▶ Optional: Save the session under a meaningful name (*Session* menu).
- ▶ Optional: Set a meaningful name for the title bar (*Window* → *Behaviour* menu).



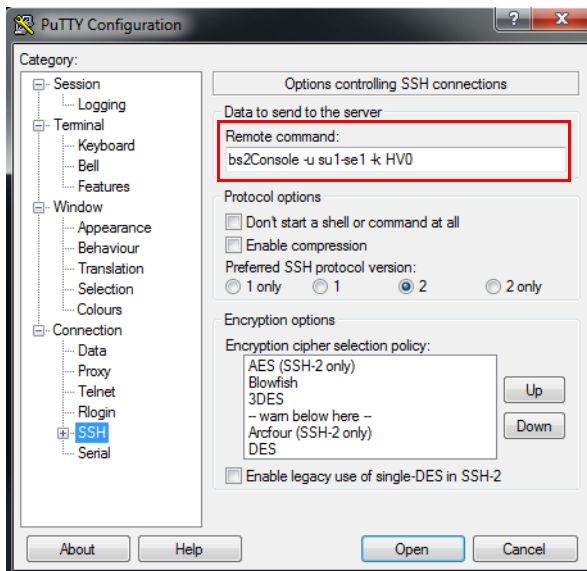
- ▶ Enter your own account (*Connection* → *Data* menu):



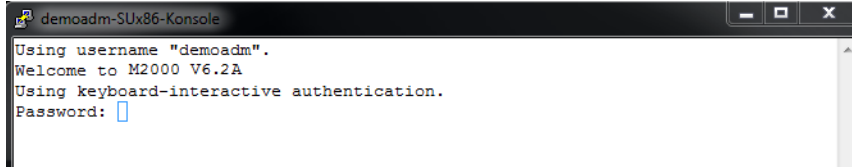
- ▶ Enter the *bs2Console* follow-up command with the following parameters:
 - the unit: external or internal name of the SU x86
 - the KVP
 - only as administrator or BS2000 administrator: the console MN



As operator, you may not enter the console MN! It is defined and will be determined:



► In the console window, enter the password for the specified account:



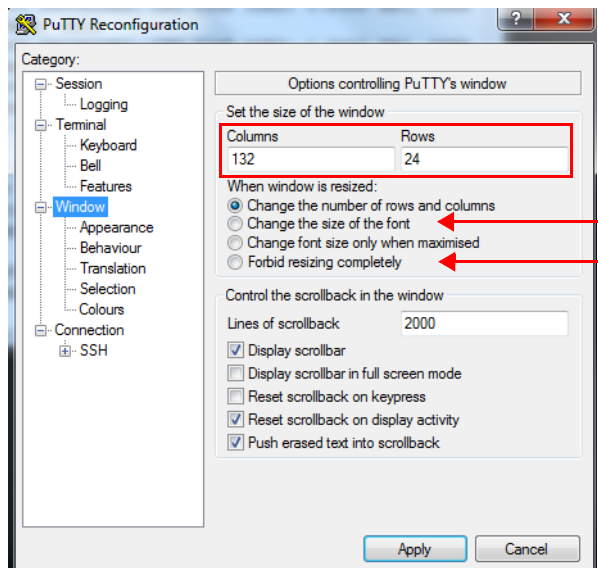
After successful login, the connection to the console of the BS2000 system to which the specified KVP is assigned, is opened:

```

demoadm-SUx86-Konsole
%VM2E-000.134502 % VMS2023 CPU 02 OF VIRTUAL MACHINE (4,ABGAFR04) STARTED
%VM2E-000.134502 % VMS2023 CPU 03 OF VIRTUAL MACHINE (3,ABGAFR03) STARTED
%VM2E-000.134503 % VMS2023 CPU 05 OF VIRTUAL MACHINE (2,ABGAFR02) STARTED
%VM2E-000.134506 % VMS2023 CPU 03 OF VIRTUAL MACHINE (4,ABGAFR04) STARTED
%VM2E-000.134507 % VMS2023 CPU 06 OF VIRTUAL MACHINE (2,ABGAFR02) STARTED
%VM2E-000.134510 % VMS2023 CPU 04 OF VIRTUAL MACHINE (4,ABGAFR04) STARTED
%VM2E-000.134511 % VMS2023 CPU 07 OF VIRTUAL MACHINE (2,ABGAFR02) STARTED
%VM2E-000.134514 % VMS2023 CPU 05 OF VIRTUAL MACHINE (4,ABGAFR04) STARTED
%VM2E-000.134518 % VMS2023 CPU 06 OF VIRTUAL MACHINE (4,ABGAFR04) STARTED
%VM2E-000.134523 % VMS2023 CPU 07 OF VIRTUAL MACHINE (4,ABGAFR04) STARTED
%VM2E-000.134553 % VMS2050 GUEST SYSTEM ON VM (3,ABGAFR03) READY
%VM2E-000.134603 % VMS2050 GUEST SYSTEM ON VM (5,ABGAFR05) READY
%VM2E-000.134636 % VMS2050 GUEST SYSTEM ON VM (4,ABGAFR04) READY
%VM2E-000.134656 % VMS2050 GUEST SYSTEM ON VM (2,ABGAFR02) READY
%UCO-000.134905 % NBR1201 TASK 'LHYX' OF OPERATOR 'TSOS' DISCONNECTED FROM SU
BSYSTEM OPERATING
%1HYX-000.134905 % EXC0420 /LOGOFF PROCESSED. CPU TIME USED: 0.1812 SEC, USER
ID: TSOS, TASK ID: 0001007D, JOB NAME: VERNER
%1HYY-000.134905 % EXC0420 /LOGOFF PROCESSED. CPU TIME USED: 0.0302 SEC, USER
ID: TSOS, TASK ID: 0001007F, JOB NAME: UEST1HYX
%VM2E-000.112001 % VMS2033 'PSC0177 2015-03-10 11:19:00 RS-TEST ABGAFR03 LOCL
NO CONNECT: 0C5C2C00' FROM VM (3,ABGAFR03) VIA SVP
SYS HVO DEMOADM C0 abgafrika 2015-03-10 15:21

```

- Choose an alternative setting for the window size (the default size is 80 x 24). To avoid line breaks, we recommend using 132 columns:



When operating the BS2000 console, you can change the size by dragging; the number of columns and lines is automatically adapted, based on the settings. Some other potentially useful settings for the window size are:

- Changing the font size together with the window size: *Change size of the font* (see above)
- Set a fixed window size: *Forbid resizing completely* (see above)

The console window with 132 columns:

```

demoadm-SUX86-Konsole
%VM2E-000.134506 % VMS2023 CPU 03 OF VIRTUAL MACHINE (4,ABGAFR04) STARTED
%VM2E-000.134507 % VMS2023 CPU 06 OF VIRTUAL MACHINE (2,ABGAFR02) STARTED
%VM2E-000.134510 % VMS2023 CPU 04 OF VIRTUAL MACHINE (4,ABGAFR04) STARTED
%VM2E-000.134511 % VMS2023 CPU 07 OF VIRTUAL MACHINE (2,ABGAFR02) STARTED
%VM2E-000.134514 % VMS2023 CPU 05 OF VIRTUAL MACHINE (4,ABGAFR04) STARTED
%VM2E-000.134518 % VMS2023 CPU 06 OF VIRTUAL MACHINE (4,ABGAFR04) STARTED
%VM2E-000.134523 % VMS2023 CPU 07 OF VIRTUAL MACHINE (4,ABGAFR04) STARTED
%VM2E-000.134553 % VMS2050 GUEST SYSTEM ON VM (3,ABGAFR03) READY
%VM2E-000.134603 % VMS2050 GUEST SYSTEM ON VM (5,ABGAFR05) READY
%VM2E-000.134636 % VMS2050 GUEST SYSTEM ON VM (4,ABGAFR04) READY
%VM2E-000.134656 % VMS2050 GUEST SYSTEM ON VM (2,ABGAFR02) READY
% UCO-000.134905 % NBR1201 TASK '1HYX' OF OPERATOR 'TSOS' DISCONNECTED FROM SUBSYSTEM OPERATING

%1HYX-000.134905 % EXC0420 /LOGOFF PROCESSED. CPU TIME USED: 0.1812 SEC, USER ID: TSOS, TASK ID: 0001007D, JOB NAME: VERNER
%1HYX-000.134905 % EXC0420 /LOGOFF PROCESSED. CPU TIME USED: 0.0302 SEC, USER ID: TSOS, TASK ID: 0001007F, JOB NAME: UEST1HYX

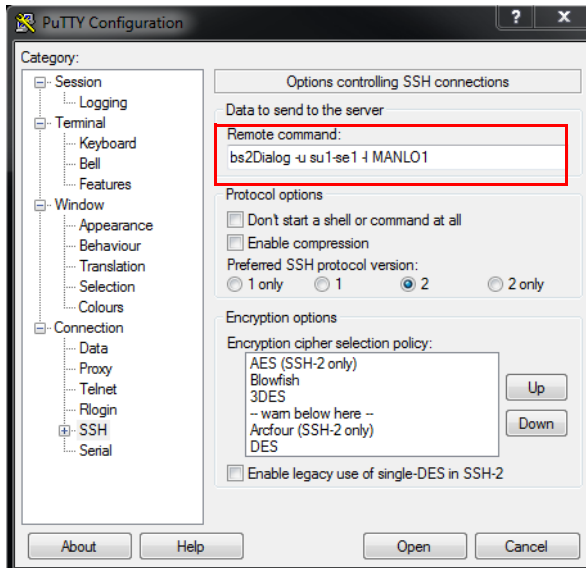
%VM2E-000.112001 % VMS2033 'PSC0177 2015-03-10 11:19:00 RS-TEST ABGAFR03 LOCL NO CONNECT: 0C5C2C00' FROM VM (3,ABGAFR03) VIA S
VF
%1HY4-000.152353 % JMS0154 'TSOS' LOGGED ON FOR 'P#MANLO1/DSS015'. JOB NAME 'DEMOADM'. CALLER '(NONE)'. TID 00020077
%1HY4-000.152400 % BLS0519 PROGRAM 'EDITSTART' LOADED
%1HY4-000.152411 % EXC0420 /LOGOFF PROCESSED. CPU TIME USED: 0.2483 SEC, USER ID: TSOS, TASK ID: 00020077, JOB NAME: DEMOADM

SYS HVO DEMOADM C0 abgafrica 2015-03-10 15:24

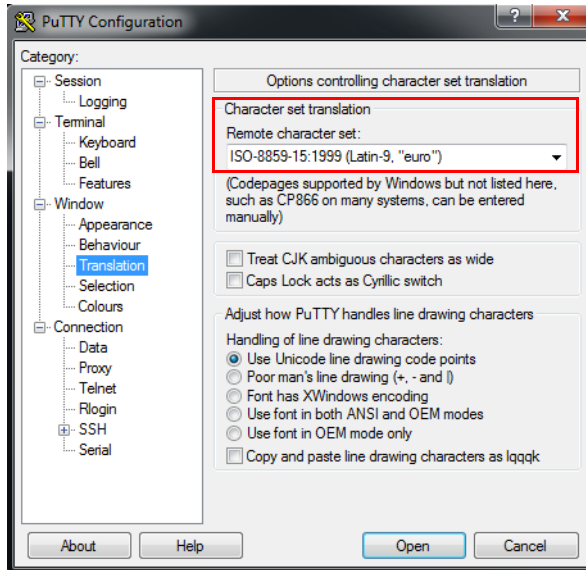
```

14.1.5 BS2000 dialog on SU x86

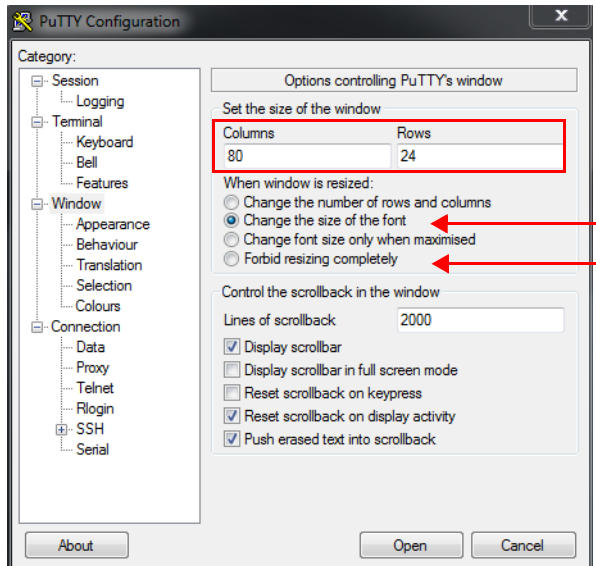
- ▶ Enter the *bs2Dialog* follow-up command with the following parameters:
 - the unit: external or internal name of the SU x86
 - a LOCLAN connection



- Specify a character set that supports the display and the keyboard shortcuts required in the BS2000 dialog (*Window* → *Translation* menu):

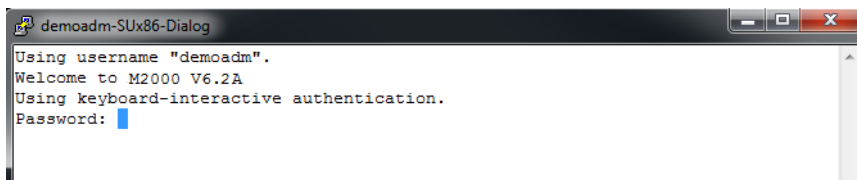


- Make sure to retain the default window size of 80 columns and 24 lines!



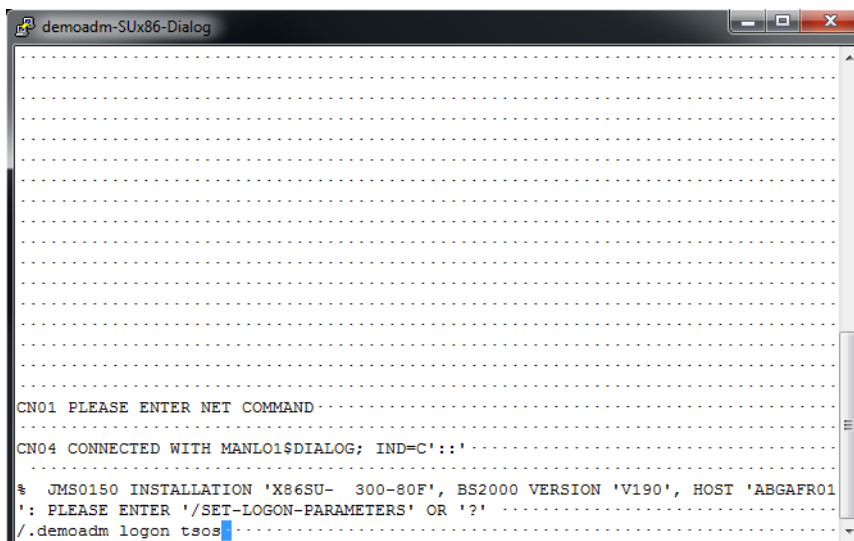
The number of columns and lines may not change when the dialog window is dragged, as this would disrupt the display. Therefore, select one of the following settings for window size:

- Changing the font size together with the window size: *Change size of the font* (see above)
- Set a fixed window size: *Forbid resizing completely* (see above)
- ▶ In the dialog window, enter the password for the specified account:



After successful login, the connection to the BS2000 dialog is opened and you can login to BS2000. Important keys:

K1	F5
K2	F6
EM	F11
DUE	F12



14.1.6 Information on the user strategy

For administrators and BS2000 administrators, the accesses described are unrestricted. For XenVM administrators and AU administrators none of the accesses is possible.

For an operator, their individual settings apply, as specified by an administrator (also see the following example):

- BS2000 console/console rights:
Access to the fixed KVPs of the individual SUs is only possible with fixed console MNs.
- BS2000 dialog/dialog authorization:
The access to the BS2000 dialog of the BS2000 systems accessible as per console rights (see above) is possible.
- SVP console (SU /390):
Access is possible via individually specified authorizations. This is only possible if at least one console authorization is specified for the SU /390.

Example for an operator with individual authorizations (*Authorizations* → *User* menu):

Account	On/Off	Shadow	SVP	Unit	Console rights	Dialog
bs2opr	Denied	Granted	Denied	-	-	-
btopr	Denied	Denied	Denied	-	-	-
demoopr	Granted	Denied	Granted	ABGSE211 (abgse1mu1)	HVD (M4IVR), AB	Granted
				ABGSE211 (abgse1mu2)	VM2 (G4IVQ), C1	Denied
					VM3 (G4IVP), CD	Denied
					HVD (M4IV), CD	Granted
				abgsu2se1	VM2 (ABGRED02), GH	Granted

The authorizations are tested, the call is rejected:

```

demoopr-SU390-Dialog
Using username "demoopr".
Welcome to M2000 V6.2A
Using keyboard-interactive authentication.
Password:
Access to BS2000 dialog not granted on unit su1se1

```



Information on logging in with an ssh key:

For a more comfortable access, the user may generate an ssh key pair and store the public key in their account.

When storing the public key, it is important to note that the file *authorized_keys* may already contain ssh keys, which are used internally by the SE Manager. These keys must remain as is under all circumstances!

14.2 Working with EMDS

If you open an operation instance BS2000 terminal in the SE Manager or via PuTTY, after successful authentication the EMDS application will start automatically and provide the "terminal" functionality. Alternative accesses are available in addition to the accesses to the BS2000 console and BS2000 dialog using the SQ Manager:

14.2.1 Using shortcuts for special characters

When you work with EMDS, special characters are available which you can access by means of shortcuts. The table below shows the most important shortcuts:

Keys	F1	F2	F3	F4	F5	F6	F7	F8	F9	F10	F11	F12
		NIL	LZF	LVD	K1	K2	K3	MAR	ED		EM	DUE1
Shift	EFZ	AFZ	LZE	LSP	F1	F2	F3	RS	WAZ	SY	AM	DUE2
Esc	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	LA1	HC
Esc Shift	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20	PP	SC

Table 7: EMDS – Shortcuts for special characters

Hold down the **Shift** key when you press an **Fn** key. Press the **Esc** key once briefly before you press **Fn** or **Shift - Fn**.

14.2.2 Using programmable keys (pfkeys)

You can use programmable keys (pfkeys) when you work with EMDS. Proceed as follows to assign values to the pfkeys:

- ▶ Press **Esc Shift - F11** in the EMDS window (PP in the table above).

The pfkey menu is displayed:



- ▶ Press the pfkey to which you want to assign a value twice. To do this, use the key shortcuts from the table on page [page 352](#), for example **[Esc] [F7]**, **[Esc] [F7]** for *P7*, *P7*.
- ▶ Now assign a value to the selected pfkey, e.g. a frequently used command.
- ▶ Terminate the entry by pressing the selected pfkey again, for example **[Esc] [F7]** for *P7*.
- ▶ Press **[Esc] [Shift] - [F11]** (PP in the table above) to return to the EMDS window.

Proceed as follows if you want to change an existing pfkey assignment:

- ▶ Press the pfkey to which you want to change once. To do this, use the shortcuts from the table on [page 352](#), for example **[Esc] [F7]** for *P7*.
- ▶ Position the cursor with the arrow keys on a character in the existing assignment.
 - ▶ Press the **[Del]** key to delete the character.
 - ▶ Press the pfkey again (in the example **[Esc] [F7]** for *P7*) and enter a character which will overwrite the existing character. Press the pfkey once again to terminate assignment.
 - ▶ Press the **[Enter]** key and then the pfkey again (in the example **[Esc] [F7]** for *P7*) and enter a character which will overwrite the existing one. Press the pfkey once again to terminate assignment.

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 \(AU\)](#).

CSR

See [Configuration Save and Restore \(CSR\)](#).

Configuration disk

Internally mirrored disk of the Unit (MU, SU x86, HNC) where the data of the SE server configuration are locally stored. In addition to the internal configuration disk, up to two external configuration disks can be configured on external FC RAID systems, to which all MUs and SU x86 have access via a redundant connection.

Configuration Save and Restore (CSR)

Sichert die Konfigurationsdaten der Management Unit in einem Archiv. Das Sicherungsarchiv enthält alle Konfigurationsdaten, die der Kunde über den SE Manager selbst verwaltet.

Data Network Private (DANPR)

Private data network for use as SE server-internal private customer network. When required, you can configure up to 99 networks DANPR<n> (with <n>= 01..99).

Data Network Public (DANPU)

Public data network for connecting applications to the public customer network. You can configure up to 8 networks DANPU<n> (with <n>= 01..08).

DANPR

See [Data Network Private \(DANPR\)](#).

DANPU

See [Data Network Public \(DANPU\)](#).

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.

IOCF

See [IO Configuration File \(IOCF\)](#).

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.

IORSF

Input/Output Resource File

An IORSF contains a BS2000 device configuration, which is required to start up an SU /390.

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 Admin Network Public (MANPU)

Public management network for the administrative access to MU, BS2000 systems and AUs.

Management Control Network Local (MCNLO)

Private management network for the local SE server communication

Management Control Network Private (MCNPR)

Private management network for the SE server communication

Management Optional Network Private (MONPR)

Private management network for the SE server communication. When required, you can configure up to 8 additive networks MONPR<n> (with <n>= 01..08).

Management Optional Network Public (MONPU)

Public management network, which can be configured as the additive administration network when required (e.g. when AIS Connect is not to be operated via MANPU but over a separate network).

Management SVP Network Private (MSNPR)

Private management network, which enables the SVP communication to the SU /390 on SE700/SE500.

Management Unit (MU)

Component of the SE server; with the help of the SE Manager, enables central, web-based management of all units of an SE server.

MANPU

See [Management Admin Network Public \(MANPU\)](#).

MCNLO

See [Management Control Network Local \(MCNLO\)](#).

MCNPR

See [Management Control Network Private \(MCNPR\)](#).

MONPR

See [Management Optional Network Private \(MONPR\)](#).

MONPU

See [Management Optional Network Public \(MONPU\)](#).

MSNPR

See [Management SVP Network Private \(MSNPR\)](#).

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-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.

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).

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.

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:

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).

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.

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 all manuals that are displayed with the order number.

- [1] **FUJITSU Server BS2000
SE700 / SE500 / SE300
Basic Operating Manual**
- [2] **FUJITSU Server BS2000
SE700 / SE500
Server Unit /390
Operating Manual**
- [3] **FUJITSU Server BS2000
SE700 / SE500 / SE300
Server Unit x86
Operating Manual**
- [4] **FUJITSU Server BS2000
SE700 / SE500 / SE300
Additive Components
Operating Manual**
- [5] **FUJITSU Server BS2000
SE700 / SE500 / SE300
Administration and Operation
User Guide**
- [6] **FUJITSU Server BS2000
SE700 / SE500 / SE300
Quick Guide
User Guide**
- [7] **FUJITSU Server BS2000
SE700 / SE500 / SE300
Security Manual
User Guide**

- [8] **FUJITSU Server BS2000
SE700 / SE500 / SE300
Cluster Solutions for SE Servers**
Whitepaper



This document is not available online. If required, Customer Support can provide you with a copy of this manual.

- [9] **BS2000 OSD/BC
System Installation (SE Server)**
User Guide
- [10] **BS2000 OSD/BC
Introduction to System Administration (SE Server)**
User Guide
- [11] **BS2000 OSD/BC
Utility Routines**
User Guide
- [12] **VM2000 (BS2000)
Virtual Machine System**
User Guide
- [13] **openNet Server
BCAM Volume 1/2**
User Guide
- [14] **openSM2
Software Monitor**
User Guide
- [15] **Net-Storage Guide**
Description Paper
- You can find this product on the BS2000 product page under <http://www.fujitsu.com> (select *Products* → *IT Products and Systems* → *Servers* → *BS2000* → *Software* → *BS2000 Operating System* → *BS2000 OSD/BC V11.0, Documents* tab).
- [16] **ServerView Suite
iRMC S2 - integrated Remote Management Controller**
User Guide
- [17] **ServerView Suite
ServerView Operation Manager**
Installation for Linux / Installation for Windows (one Installation Guide for each)

- [18] **ServerView Suite**
ServerView Operation Manager
Installation of the ServerView agents for Linux / Installation of the ServerView agents for Windows (one Installation Guide for each)

- [19] **LSI MegaRAID**
SAS Software
User Guide

- [20] **LSI Controllers**
Modular RAID Controller
Installation Guide

Index

A

Access authorization
 Net-Storage 233, 242
account 75
 admin 300
 LDAP 301
 local 300
 managing 300
 service 300
account management 300
Accounts 301
accounts 300
ACL
 DANPU 261
 Management Networks Private 276
 MANPU 271
ACL (Access Control List) 35
action, executing 94
add
 account 301
add-on pack 25, 26, 27
admin (administrator role) 50, 300
administrator 300
 role 48
AIS agent
 displaying 224
AIS Connect
 reading log 226
Application Unit 21, 246
 configuring 246
 installing 151
Application Unit PQ 19, 21
Application Unit PY 19, 21
architecture of SE server 23
asset, external 223

ATTACH-DEVICE 185
AU administrator 300
AU PQ
 IP configuration 251
AU PY
 IP configuration 250
Autoconf 41
automatic startup
 XenVM 137
automatic update 78
AutoYAST XML file 195

B

basic software
 HNC 25
 M2000 24
 X2000 24
boot disk
 XenVM 142
BRGLAN 38, 179
BS2000
 remaining runtime 116, 122
BS2000 administrator 300
 role 48
BS2000 console 332, 343
 messages 112
BS2000 dialog 337, 348
BS2000 operation via PuTTY 331
BS2000 pool 58
BS2000 VM
 operating menu 122
BS2000 ZASLAN 37
bs2Console 331
bs2Dialog 331
burning CD/DVD 186

C

- CA certificate downloading [322](#)
- CD
 - burning [186](#)
 - taking over files (BS2000) [183](#)
- CDROM files [183](#)
- certificate
 - confirming [314](#)
 - server's own CA certificate certificate
 - downloading [322](#)
- Channel path identifier [167](#)
- CHECK-TAPE [185](#)
- CLI [216](#)
- Cluster [295](#)
- Command Line Interface [216](#)
- components
 - displaying [288](#)
- Configuration
 - XenVM [140](#)
- configuration data backup
 - downloading/deleting [221](#)
 - executing [220](#)
 - executing (HNC) [235](#), [244](#)
 - performing (MU) [220](#)
 - performing (SU x86) [244](#)
 - uploading [221](#)
- Configuration disks
 - HNC [229](#)
 - MU [207](#)
- Configuration disks (SU x86) [239](#)
- configuration errors (XenVM) [131](#)
- Configuration Save and Restore [220](#), [235](#), [244](#)
- connections, displaying [279](#)
- console
 - XenVM [138](#)
- console distribution program [176](#)
- CPU
 - real [58](#)
- CPU assignment [58](#)
- CPU pool [58](#)
- CSR (Configuration Save and Restore) [355](#)
- CSR (HNC) [235](#)
- CSR (MU) [220](#)
- CSR (SU x86) [244](#)

- CSR backup
 - managing (MU) [220](#)
 - managing (SU x86) [244](#)
- Customer Support
 - tasks [69](#)

D

- D3435 (disk type) [173](#)
- D3475-8F (disk type) [173](#)
- DANPR [32](#), [265](#), [355](#)
- DANPU [32](#), [259](#), [355](#)
- Dashboard [101](#)
- data network
 - private [32](#)
 - public [32](#)
- Data Network Private (DANPR) [32](#), [355](#)
- Data Network Public (DANPU) [32](#), [355](#)
- database
 - for virtual disks [190](#)
 - for virtual disks (XenVM) [190](#)
- Deleting a DNS entry [255](#)
- DETACH-DEVICE [185](#), [186](#)
- device addressing, BS2000 [166](#)
- DHCPv4 [41](#)
- DHCPv6 [41](#)
- diagnosis (MU) [222](#)
- diagnosis (SU x86) [245](#)
- diagnostic data (MU) [222](#)
- diagnostic data (SU x86) [245](#)
- diagnostic data, generating [222](#), [236](#)
- Diagnostics (HNC) [236](#)
- dialog [85](#), [94](#)
- disk pool [63](#), [191](#)
 - creating [189](#)
 - deleting [190](#)
 - displaying information [189](#)
 - extending [190](#)
- Disk pool (XenVM)
 - managing [189](#)
- Disk pools (XenVM) [188](#)
 - displaying [189](#)
- disk, virtual [63](#)
- disks (BS2000)
 - managing [173](#)

- Displaying sessions 308
- DNS configuration
 - SE server 254
- DNS configuration (HNC) 232
- DNS configuration (MU) 211
- DNS configuration (SU x86) 241
- DNS entry
 - changing host name 255
- DNS entry, adding
 - SENET 254
- DNS server 34
- domain, changing
 - MU 208
- download server 26
- DVD
 - taking over files (BS2000) 183
- DVD burner 183
- DVD drive
 - physical 196
 - virtual 195
- E**
- EMDS
 - operating 352
- EMFILES 183
- errors
 - while creating the XenVM 131
 - while installing the XenVM 134
- external virtual switch 193
- F**
- FC interfaces
 - HNC 229
 - MU 206
 - SU /390 202
- filter 92
- full virtualization 57
- G**
- generating diagnostic data (SU x86) 245
- Global session 76
- graphics card, changing 140
- H**
- HAL (message class) 113
- hardware virtualization 57
- high availability
 - LAN connection 193
- HNC 19, 356
 - basic software 25
 - Open Source licenses 20
- host name, changing
 - MU 208
- hot fix 25, 26, 27
- HV0 176
- I**
- icon 94
- import filter 92
- inactivity time 303
- Individual settings 81
- INIT 185, 186
- initial password 75
- Input/Output Resource File (IORSF file) 357
- installation configuration file 195
- installation information
 - deleting 135
 - history 134
- installation log
 - displaying content 135
 - viewing 134
- installation medium
 - reading in 195
- installation process
 - aborting 134
 - monitoring 134
- installation source 63
 - adding 145
 - assigning 145
 - managing 195
 - removing 146
 - switching 145
- Installation sources (XenVM) 195
- internal virtual switch 193
- inventory information
 - changing 289
- IOD (message class) 113

- IP address, adding
 - MU [209](#)
- IP address, changing
 - Application Unit [247](#)
- IP address, deleting
 - MU [209](#)
- IP configuration
 - AU PQ [251](#)
 - AU PY [250](#)
 - AU25/AU47 [250](#)
- IP configuration (HNC) [230](#)
- IP configuration (MU) [208](#)
- IP configuration (SU /390) [203](#)
- IP interfaces
 - HNC [228](#)
 - MU [205](#)
- IP networks
 - XenVM [144](#)
- IP-based access restriction [51, 311](#)
- IPv6 autoconfiguration [33](#)
- IPv6 log [41](#)
- ISO image file [195](#)

K

- keyboard language
 - changing [140](#)
- KVP (message class) [113](#)
- KVP device, managing [176](#)

L

- LAN configuration
 - Application Unit [247](#)
- LDAP account [301](#)
- licenses for Open Source Software [20](#)
- Linux time [65](#)
- Linux/Windows pool [59](#)
- list view [103](#)
- local library [145](#)
- local session [76](#)
- local system data for SNMP
 - changing [213](#)
- LOCLAN [37, 179](#)
- LOCLAN (MU)
 - changing packet length [205](#)

- logging in
 - SE Manager [75](#)
 - XenVM console [138](#)
- logical unit number [167](#)
- Logical Unit Number (LUN) [167](#)
- login window [74](#)
- logs
 - AIS Connect [226](#)
- LUN (Logical Unit Number) [167](#)

M

- M2000
 - basic software [24](#)
 - Open Source licenses [20](#)
- MAC address
 - DANPR [260](#)
 - Management Networks Private [274](#)
 - MANPU [271](#)
- main memory [60](#)
- main window [80](#)
- maintenance window [71](#)
- Management Admin Network Public (MANPU) [32, 357](#)
- Management Cluster [295](#)
 - status [296](#)
- Management Control Network Local (MCNLO) [32, 357](#)
- Management Control Network Private (MCNPR) [32, 357](#)
- management network
 - private [32](#)
 - public [32, 357](#)
- Management Network LOCLAN (MANLO) [37](#)
- Management Optional Network Private (MONPR) [32, 357](#)
- Management Optional Network Public (MONPU) [32, 357](#)
- management station [212](#)
- Management SVP Network Private (MSNPR) [32, 357](#)
- Management Unit [21](#)
- Managing XenVM devices [141](#)
- MANLO [37](#)
- MANPU [32, 357](#)

- MCNLO [32, 357](#)
- MCNPR [32, 357](#)
- messages
 - displaying (FC networks) [279](#)
- messages of M2000/X2000 [112](#)
- metalanguage [18](#)
- MIB-II [212](#)
- minimum time [303](#)
- MN [166](#)
- MNEM [166](#)
- mnemonic [166](#)
- mnemonic name [166](#)
- MONPR [32, 357](#)
- MONPU [32, 357](#)
- MSNPR [32, 357](#)
- MU
 - restricting IP-based access [51, 311](#)
- MU redundancy [52](#)
- Multi-MU configuration [21](#)
- Multipath disks
 - MU [207](#)
- Multipath disks (SU x86) [239](#)
- N**
- Net Storage (HNC)
 - configuring [232](#)
 - connecting [234](#)
- Net Storage (SU x86)
 - configuring [241](#)
 - connecting [243](#)
- Net Unit [22, 31](#)
- Net-Storage (HNC)
 - Access authorization [233](#)
- Net-Storage (SU x86)
 - Access authorization [242](#)
- network connection
 - BS2000 [37, 179](#)
- network connection, XenVM [39, 64](#)
- Network Interface Card
 - displaying [144](#)
 - removing [144](#)
- network properties, changing
 - MU [209](#)
- Network Time Protocol [66](#)
- network, adding
 - DANPR [267](#)
 - MONPR [273](#)
- notational conventions [18](#)
- NTP (Network Time Protocol) [214](#)
- NTP server [36, 66](#)
- NTP server quality [66](#)
- O**
- online help [97](#)
- Open Source Software
 - licenses [20](#)
- opening XenVM console [138](#)
- operating mode, restricted [78](#)
- operation
 - XenVM [138](#)
- operator [300](#)
 - role [49](#)
- P**
- P-keys
 - EMDS [352](#)
- packet length
 - changing for MU [205](#)
- parameter area [85](#)
- paravirtualization [57](#)
- password [75](#)
- password administration [303](#)
- PCI interfaces (MU)
 - changing packet length [205](#)
- physical volume [191](#)
- pool 0 [58](#)
- port, removing
 - DANPR [261](#)
 - Management Networks Private [275](#)
 - MANPU [271](#)
- ports, adding
 - DANPR [261](#)
 - Management Networks Private [275](#)
 - MANPU [271](#)
- powering off
 - unit [200](#)
- powering on
 - unit [199](#)

- private networks [31](#)
- programmable keys
 - EMDS [352](#)
- proxy configuration
 - displaying [224](#)
 - entering/changing or deleting [226](#)
- public networks [31](#)
- PuTTY
 - BS2000 operation [331](#)

R

- rack view [285](#)
- RADVD / DNS / NTP server
 - activating (DANPR) [267](#)
- Readme file [15](#)
- rebooting
 - unit [199](#)
- redundancy
 - MU [52](#)
 - SKP functionality [52](#)
- remaining runtime
 - BS2000 [116](#), [122](#)
 - XenVM [136](#)
- Remote Service [71](#)
- remote service
 - process [71](#)
- Remote Service (MU) [224](#)
- reset
 - tables to default view [92](#)
- reset tables [81](#), [92](#)
- restricting MU access [311](#)
- revision [25](#)
- REWAS [36](#)
- role [299](#)
 - administrator [48](#)
 - BS2000 administrator [48](#)
 - operator [49](#)
 - service [50](#)
- Routing & DNS (HNC) [231](#)
- Routing & DNS (MU) [210](#)
- Routing & DNS (SU x86) [240](#)

S

- S server [20](#)
- SE Manager [23](#), [56](#)
 - interface [79](#)
 - logging in [75](#)
- SE server [21](#)
 - architecture [23](#)
- sealing off [58](#)
- security fix [25](#), [26](#)
- SENET
 - configuring [254](#)
 - DNS entry, adding [254](#)
- senet [34](#)
- Server Unit [21](#)
- service
 - role [50](#)
- service (service role) [300](#)
- service access
 - changing [224](#)
 - displaying [224](#)
- session [76](#)
 - restricted operating mode [78](#)
- session ID [76](#)
- sessions
 - displaying [224](#)
- shadow terminal
 - AIS Connect [223](#)
 - opening [225](#)
- Simple Network Management Protocol (see SNMP) [212](#)
- Single-MU configuration [21](#)
- SKP functionality, redundancy [52](#)
- SNMP [212](#)
 - changing local system data [213](#)
 - read accesses [213](#)
 - security [212](#)
 - testing traps [214](#)
 - trap receiver [214](#)
- SNMP (MU) [213](#)
- SNX (message class) [113](#)
- software status [25](#)
- software update [26](#)
- standard account, password [75](#)
- starting and shutting down the XenVM [139](#)

Storage Manager 284
storage system (external asset) 223
Storman 284
stratum 66
SU /390 19
 implementation of VM2000 54
SU Cluster 295, 297
SU x86 19
 implementation of VM2000 55
SVP clock 67
SVP console 340
svpConsole 114, 331
SVR (message class) 113
switch
 virtual 39, 64
switch, adding 278
switch, changing 278
switch, removing 278
SYSLOCATION (MU)
 system data, local 213
system information
 HNC 227
 MU 204
 SU /390 201
system initialization
 automatic 137
system version 25

T

terminal window 83
test
 SNMP traps 214
tile view 101
time management 65
Time of Day Register 67
time synchronization 66
 BS2000 67
 X2000 67
 XenVM system 68
TODR 67
trap receiver
 SNMP 214

U

unit
 powering off 200
 powering on 199
 rebooting 199
unit ID 166
units
 displaying 286
UNLOAD-TAPE 186
update 25
 providing 71
 responsibilities 72
 tasks 72
Update (HNC) 235
Update (SU x86) 244
update status 25, 26
Updates
 displaying (HNC) 235
updates
 displaying (SU x86) 244
user account see account
user management 300

V

validity 303
virtual disk 63
 changing size 142
 displaying disks of the XenVM 141
 displaying XenVM assignment of all
 disks 191
 removing 143
 updating data base 190
Virtual disks (XenVM) 191
virtual DVD device 145
virtual DVD drive 195
virtual Network Interface Card 144
virtual switch
 external 193
 internal 193
 removing from the configuration 194
Virtual switches (XenVM) 193
VM administration (XenVM) 130
VM installation (XenVM) 134
VM options (XenVM) 137

VM resources (XenVM) [133](#)
VM type [58](#)
VM2000 [57](#)
volume group [191](#)
vSwitch [39](#), [64](#)
 external [39](#)
 internal [39](#)

W

warning time [303](#)
welcome page SE Manager [75](#)
wildcards
 device specifications [129](#)
window type [79](#)
wizard, Create new XenVM [131](#)

X

X2000
 basic software [24](#)
 Open Source licenses [20](#)
 time synchronization [67](#)
Xen hypervisor [55](#)
XenVM
 configuring Network Interface Card [144](#)
 displaying configuration [140](#)
 displaying installation sources [145](#)
 displaying virtual disks [141](#)
 handling configuration errors [131](#)
 opening console [138](#)
 operating menu [138](#)
 powering off [139](#)
 remaining runtime [136](#)
 removing Network Interface Card [144](#)
 removing virtual disk [143](#)
 restarting [139](#)
 shutting down [139](#)
 starting [139](#)
 starting automatically [137](#)
 stopping [139](#)
 unpausing [139](#)
XenVM administrator [300](#)
XenVM license [57](#)

Z

ZASLAN [37](#), [179](#)