English

Fujitsu Server BS2000 SE Series

Administration and Operation

User Guide

Valid for:
M2000 V6.5A
X2000 V6.5A
HNC V6.5A

Edition December 2023

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: bs2000services@fujitsu.com.

Certified documentation according to DIN EN ISO 9001:2015

To ensure a consistently high quality standard and user-friendliness, this documentation was created to meet the regulations of a quality management system which complies with the requirements of the standard DIN EN ISO 9001:2015.

Copyright and Trademarks

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 brands of Novell, Inc. in the USA and other countries.

Linux is a registered brand 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.

Table of Contents

Administration and Operation

1 Introduction

The Fujitsu Server BS2000 SE series with its innovative HW and SW features forms the proven mainframe line from Fujitsu. Designed as hybrid systems, the SE servers create a new quality of openness and integration capability of different server and peripheral systems with simultaneous comprehensive and cross-system manageability.

Under the umbrella of the SE infrastructure, multiple application scenarios are possible in various combinations for both mainframe applications and applications of the open world. The server architecture offers comprehensive 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 of the SE servers is 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 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.
In addition to their high system performance, the servers of the SE series offer enhanced configuration options, maximum availability and, not least of all, significantly reduced power consumption compared with predecessors.

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

Main features of an SE server are:

- 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 for all units
- Various options for consolidation through virtualization
- SE components and infrastructure are preconfigured and supplied to customers ready to use.

Regarding customer's requirements, SE servers enable a flexible and application-specific implementation which fulfills high SLAs (Service Level Agreements) through the use of high-end components and an end-to-end redundancy concept. This permits cost-effective operation of the overall system with few resources thanks to its uniformity.

Intel x86-based Application Units with their systems 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
- High level of proven quality through extensive testing before release
- Comprehensive service concept.

The uniform management interface, the SE Manager, permits a simultaneous view of all the system components of the SE servers 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 up to eight SE servers in a Management Cluster to one management entity and therefore utilize the advantages of the central administration with the SE Manager for several SE servers at the same time. Every Management Unit can be used to control all components of the cluster, thus enhancing protection against failure.

Two Server Units can be combined in an SU Cluster. Thus, live migration (LM) allows to relocate BS2000 systems between the units without interruption.

SE servers consequently permit very stable system operation which includes not only the mainframe platforms which have to date been known to be particularly failsafe, but also the other 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.

In this manual, abbreviations are used to describe the SE server models and their components. These are explained in the introduction to the Basic Operating Manual [1] in the section "Models, Names, Abbreviations".

You will find information on these topics in the following sections:

1.1 Documentation for the Fujitsu Server BS2000 SE Series

A wide range of documentation is available for the SE servers on the manual server at https://bs2manuals.ts.fujitsu.com.

- The manuals on BS2000 OS DX, which provide the basic literature.
- The manuals for the system-related software products also apply.

Any additions to the manuals are described in the Readme files for the various product versions. These Readme files are also available on the manual server with the BS2000 documentation 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 OS DX, M2000, X2000, and HNC, are available on the manual server.

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

- Operating manual (consisting of a number of modules):
  - Basic Operating Manual [1]
  - Server Unit /390 [2]
  - Server Unit x86 [3]
  - Additive Components [4]
- Operation and Administration [5] (this manual)
- Quick Guide [6]
- Security Manual [7]
- Cluster Solutions for SE Servers (Whitepaper) [8]

1.2 Objective and concept of this manual

The chapter "Architecture and strategies" contains fundamental information regarding the SE server which is relevant for all readers (e.g. architecture, fundamental operating functions).

The chapter "Operating the SE Manager" 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.

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 on the manual server with the BS2000 documentation (https://bs2manuals.ts.fujitsu.com).

Target groups of this manual

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

- Administrator
  - 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 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).
  - As administrator you can manage by default all add-on packs.
- For other users, roles are provided with a customized (reduced) selection of functions (e.g. BS2000 operator, AU administrator, etc.) to permit the assigned tasks to be performed.

1.3 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 V6.5A.

Functional extensions

The basic software M2000/X2000/HNC V6.5A provides the following functional extensions:

BS2000-supporting functions

- Global and system-specific display of pending BS2000 messages for all BS2000 systems of the SE administration area
- Display and possibility of download for C2H files (reports and tables) of all BS2000 systems of the SE administration area
- Unification of storage displays in SEM windows with disk display
- Generation of IOGEN sources from IORSF files
- A user-defined name can be specified for the monitor VM on SU x86.

FC networks

- Redesign of the functions for the integration and display of FC switches
- Introduction of performance and topology displays for FC networks
- Display of BS2000 paths

Tracking of asynchronous processes

- Display of transition states when starting and stopping systems
- Display of transition states when starting and stopping units

Maintainability

- Advanced display of remote service configuration
- Enhanced display and management of remote service sessions and logging files
- Enhancement of the SE operating state and introduction of the maintenance state
- Restructuring of the SEM menu Service
- Introduction of the SEFW add-on, which is used for firmware upgrades of the units and their components

Security

- Introduction of a new RBAC-based role concept with basic roles and user-defined roles based on these roles
- Introduction of a new authorization assignment for BS2000 operators aimed at BS2000 systems, with independent authorizations for console and dialog
- Introduction of the Security Monitor (SecMon), which regularly checks the security settings and guidelines and generates appropriate events if necessary

- Extension of the Resource Monitor (ResMon), which regularly checks the currently available resources
- Support of multi-factor authentication (MFA) for login at the SE Manager
- Replacement of security fixes and hot fixes by updates

SEM graphical user interface

- Introduction of an AU-optimized view of the systems and units, which can be used especially for configurations with many AUs
  For configurations with many AUs, an AU-optimized view of the systems and units is supported.
- Exporting SEM tables in XLSX format
  SEM tables can be exported in XLSX format.
- Direct integration of the Storage Manager into the SEM GUI (depending on the version of the Storage Manager)

1.4 Notational conventions

The following notational conventions are used in this manual:

italics	Texts from the SE Manager (e.g. menu name, tab)
`monospace`	System inputs and outputs
<abc>	Variables which are replaced by values.
Key symbols	Keys are displayed as they appear on the keyboard. When uppercase letters need to be entered, the Shift key is specified, e.g. SHIFT - A for A. If two keys need to be pressed at the same time, this is indicated by a hyphen between the key symbols.
>	An action which you must perform is indicated by this symbol.
i	This symbol indicates information and notes that you should observe.
i	This symbol indicates further instructions for action and tips that you should observe.
!	This symbol indicates particularly important notes and instructions for action which you should observe.
!	This symbol and the word "ATTENTION!" or "CAUTION!" precede warning information. In the interests of system and operating security you should always observe this information.
[ ]	The titles of related publications in the text are generally 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.

2 Architecture and strategies

The description is divided into the following sections:

2.1 Architecture

A Fujitsu Server BS2000 of the SE Series (SE server for short) can consist 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 enables operation of BS2000 (Native BS2000 or VM2000). Depending on the model family, the following combinations are possible:
  - SE servers SE7xx are equipped with an SU /390
  - SE servers SE3xx each contain an 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 (AU PY) refers to all PRIMERGY-based AUs (e.g. hardware model AU25 or AU47).
  - Application Unit PQ (AU PQ) refers to all PRIMEQUEST-based AUs (e.g. hardware model AUQ38E or DBU38E).
- 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 SE server with an SU /390 the Net Unit is always redundant in design. In the case of SE server with SU x86 only 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
- Optional hardware components / peripherals integrated into the rack:
  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").

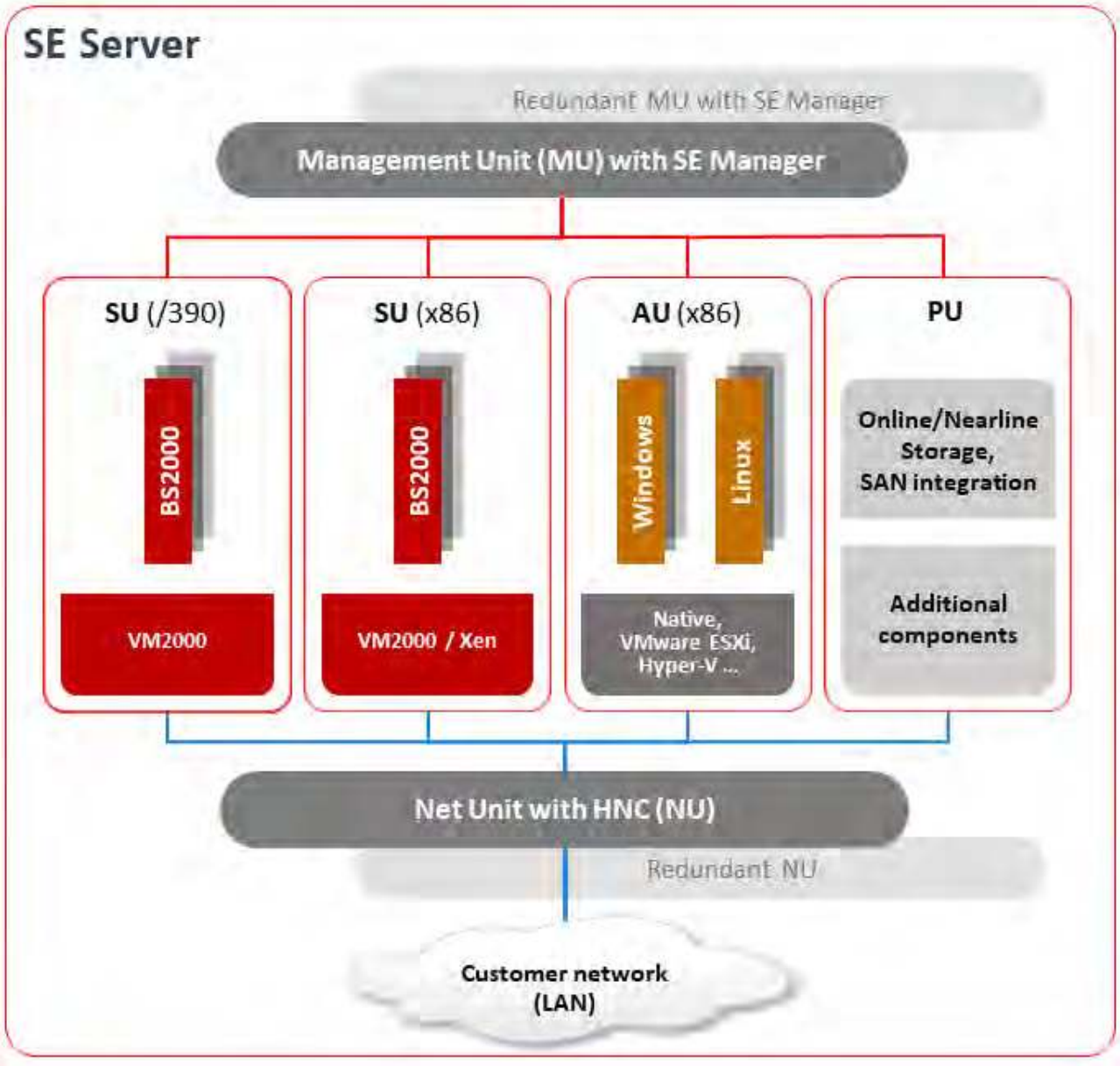


Figure 1: Architecture of SE servers

The SE Manager (also called SEM for short) 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

The description is divided into the following sections:

- Structure of the software
- Software status, system version and update status
- Updates to the basic software
- Add-on packs

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 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 customer network
- SE Desktop for operation on the local console of the Management Unit
- Integration into the Remote Service of Fujitsu

X2000

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

- Execution system for BS2000 systems (including I/O system)
- Management functions for administering the BS2000 VMs in the SE Manager
- Management functions for administering the BS2000 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.

See also section "Add-on packs".

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 "Name, system information and interfaces of the SU /390"), but in this case does not support update management.

The software status consequently has the following components:

Component	Example	Description
Version	`6.5A`	
Revision	`REV=0206`	Update status
Update	`6.5A, No.010`	• Updates are assigned to a version and update status. • Updates have a sequence number for each version status and each update status (`010` in the example)

In contrast to the other updates, add-on packs are autonomous software products which Fujitsu provides 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

You can transfer updates to the basic software as well as add-on packs to the Management Unit, the SU x86 and the HNC and manage them there.

An update to the basic software contains a patch with which an urgent problem in your system can be rectified as quickly as possible.

An update can only be installed by Customer Support. Installation can only be performed using a CLI command under the Customer Support account.

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

Naming conventions

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

Update	e.g. `MV6.5A0206U010.iso[.gz]` The update with number `010` is assigned to the version and update status `6.5A REV=0206`.
Add-on pack	e.g. `MV.STORMAN-10.3.0-0.0.iso` This add-on pack contains STORMAN V10.3.

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 High-speed Net Connect

2.2.4 Add-on packs

Add-on packs are software components on a unit which generally 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.

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.

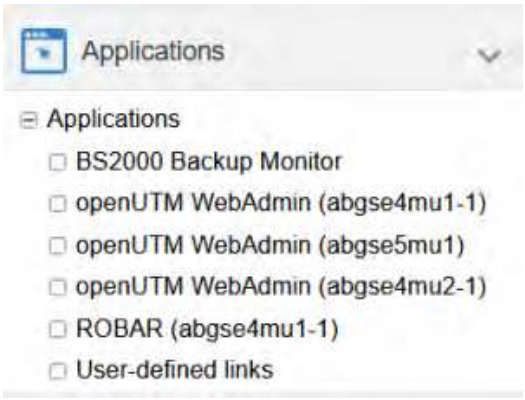
Add-on packs have their own online help systems and, when necessary, are described in separate product manuals. These online helps are integrated into that of the SE Manager, but can also be called separately.

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.

An exception applies to the Storage Manager: For STORMAN versions V10.3 and higher on the local MU, the Storage Manager is directly integrated into the SE Manager. The STORMAN user interface is accessible immediately below the Hardware -> Storage menu.

Example with the add-on packs OPENUTM and ROBAR:



Overview of the add-on packs with own GUI in the SE Manager on the MU:

Add-on (product name)	**Chargeable**	**Preinstalled ex works**	**Integration into the SE Manager**
OPENSM2 (openSM2 Manager)	Yes	Optional	Category: Performance -> *Performance*
OPENUTM (openUTM WebAdmin)	No *)	No	Category: Applications -> *Applications* -> *openUTM WebAdmin (<mu>)*
ROBAR (ROBAR-SV Manager)	Yes	Optional	Category: Applications -> *Applications* -> *ROBAR (<mu>)*
STORMAN (StorMan Storage Management)	No	Yes	Category: Hardware -> *Hardware* -> *Storage* -> *Storage (<mu>)* -> *Storage Manager*

Table 1: Add-on packs (with own GUI) in the SE Manager on the MU

*) The add-on OPENUTM is not chargeable, but the basic product openUTM is.

Add-on pack NUX

The add-on pack NUX occupies a special position. NUX stands for Net Unit eXtension and the add-on serves to connect the SE server to the customer networks via Cisco switches.
If a suitable Cisco infrastructure is available, the NUX add-on is installed and configured as part of a service.
In the SE Manager, the NUX-specific menus extend the Hardware -> IP Networks menu.
The online help for NUX is included in the online help of the SE Manager.
For more details on NUX, please contact customer support or service.

SE management applications

SE management applications run on the Management Units and are fully integrated into the SE Manager. These include the above-mentioned add-on packs OPENSM2, OPENUTM, ROBAR and STORMAN.

As a further SE Management application, which in contrast to the add-on packs is implemented as a permanent part of the SE Manager, also the BS2000 Backup Monitor is currently available. It can be found in the SE Manager under the Applications category: -> *Applications -> BS2000 Backup Monitor*.

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, SE server with an SU /390 incorporate a redundant Net Unit. Redundancy can be ordered as an option for SE x86.

The BS2000 systems communicate with the MU over a private network, see section "Integration of BS2000 into the SE Manager".

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 SE server with an SU /390.

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".

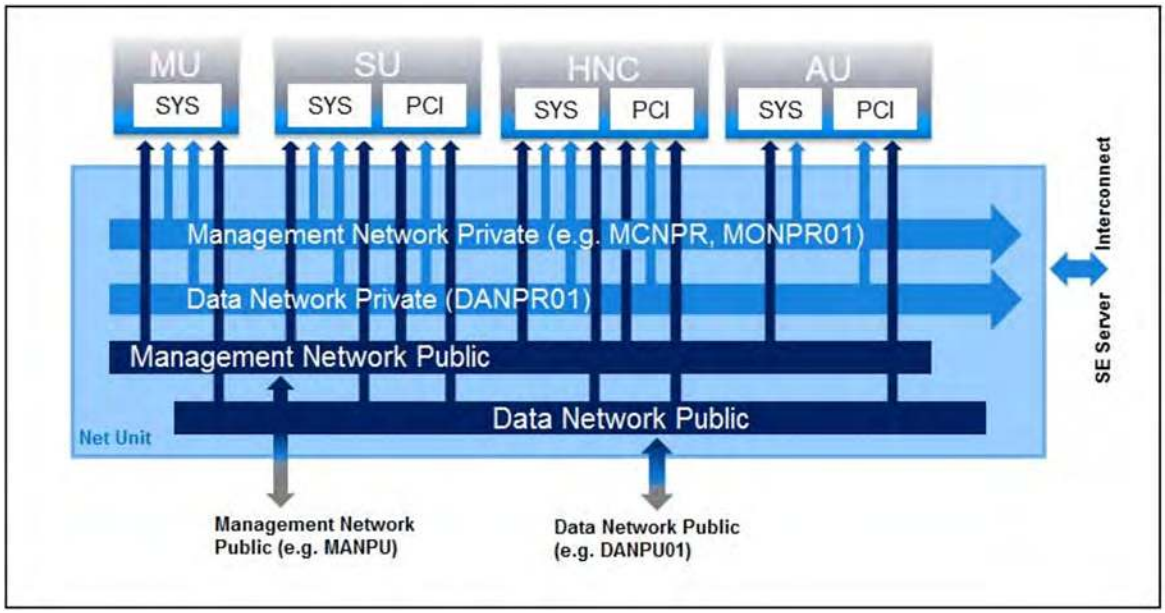


Figure 2: Block diagram of the Net Unit

> This description refers to the internal Net Unit and the internal networks and connection possibilities of the SE Server to the public customer network realized with it.
> If the optional add-on NUX (Net Unit eXtension) is installed on the Management Unit, there are further connection possibilities to the public customer network.
> For further details on NUX, please contact customer service.

2.3.1 Services

The description is divided into the following sections:

- IPv6 autoconfiguration
- Domain Name System (DNS)
- Managing the "senet" domain
- ACL functionality
- NTP server

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>::<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").

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").

The management of the "senet" domain is global for the SE server resp. SE cluster. 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
Net Unit (Managed switch)	nswa<x>-se<y>.senet	1 Gbit NU switch
HNC	hnc<x>-se<y>.senet hnc<x>irmc-se<y>.senet	HNC HNC iRMC
AU PY	au<i>-se<y>.senet (i=1..9999)	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.

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

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

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

2.3.1.5 NTP server

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

The units 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".

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.

For SU /390 as well as for SU x86, communication is required between the MU and the BS2000 systems concerned in the following cases:

- For the BS2000 Backup Monitor to communicate with the BS2000 systems on which the backup requests take place
- For the display of pending BS2000 messages in SEM
- For the display of C2H data of BS2000 systems in SEM
- For the display of BCAM networks in SEM

The communication uses the internal network MCNPR (see Figure 2 in section "Networks") 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 and LOCLAN 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") 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>)* on the *LAN* tab.

> ¡ All PCI ports can be used for the ZASLAN connections.

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 in section "Networks"). 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, Customer Support can configure other address ranges.

2.3.4 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 BS2000 VMs running on the Server Unit. Physical network integration is shown in Figure 2 in section "Networks".

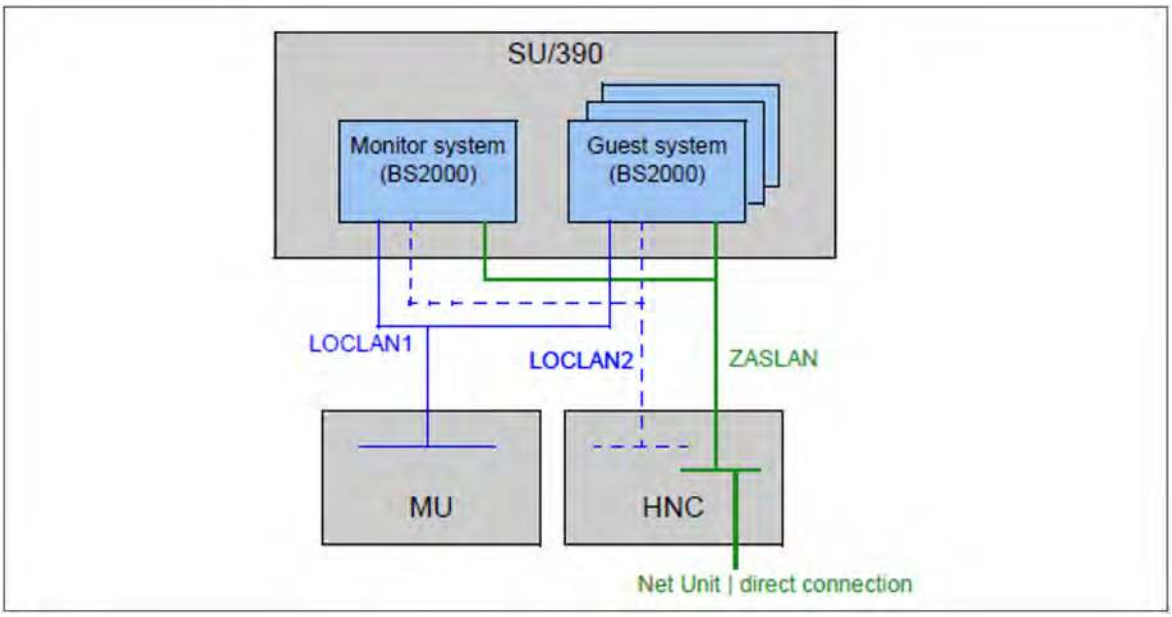


Figure 3: Overview of possible internal and external LAN connections (Server Unit /390)

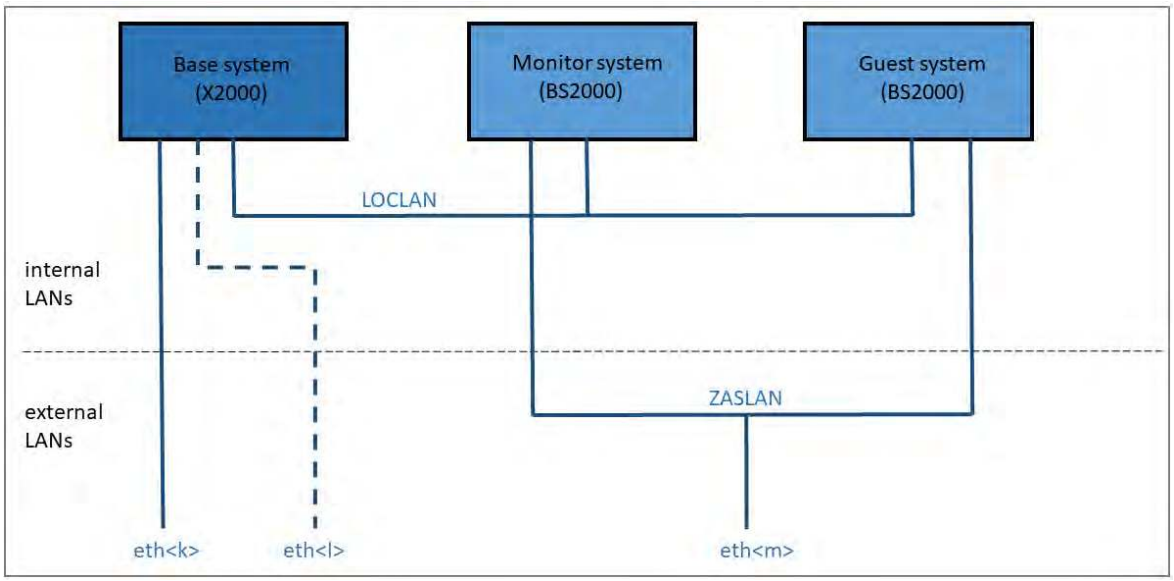


Figure 4: Overview of possible internal and external LAN connections (Server Unit x86)

2.3.5 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:

- 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 CRD disks

On a CRD disk (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 CRD 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 CRD disks, e.g. of an MU, in the *Hardware* -> *Units* -> [*<se server> (SE<model>)* ->] *<unit> (MU)* -> *Information* menu (see "Displaying CRD disks of the MU"):

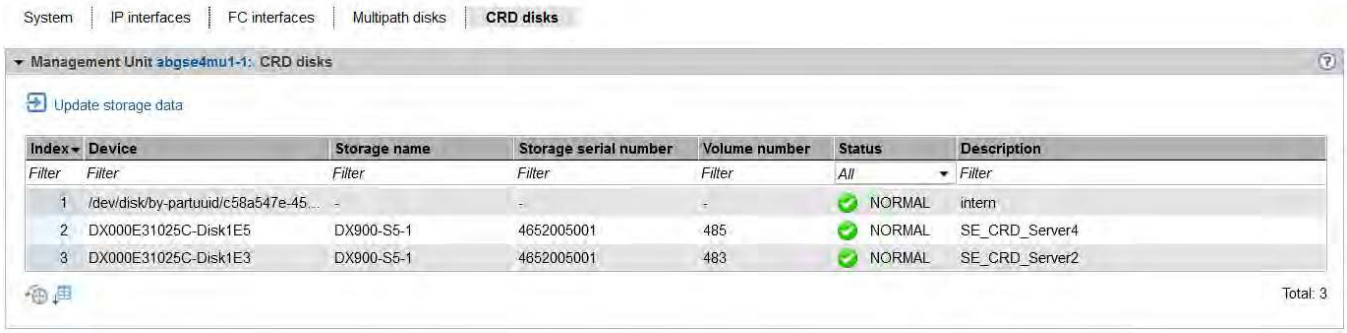


Figure 5: MU with external CRD disks

External CRD disks are required in the following cases:

- MU redundancy
- Cluster
  For the SE Cluster (Management Cluster), external CRD disks are sufficient on the MUs. For SU Clusters, external CRD disks are also required on SU x86.

2.5 Cluster

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

- Management Cluster
- SU Cluster

2.5.1 Management Cluster

If two or more SE servers are combined into one management entity, this is called a "Management Cluster" (or "SE Cluster").

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

A Net Unit connection between the 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 CRD disks".

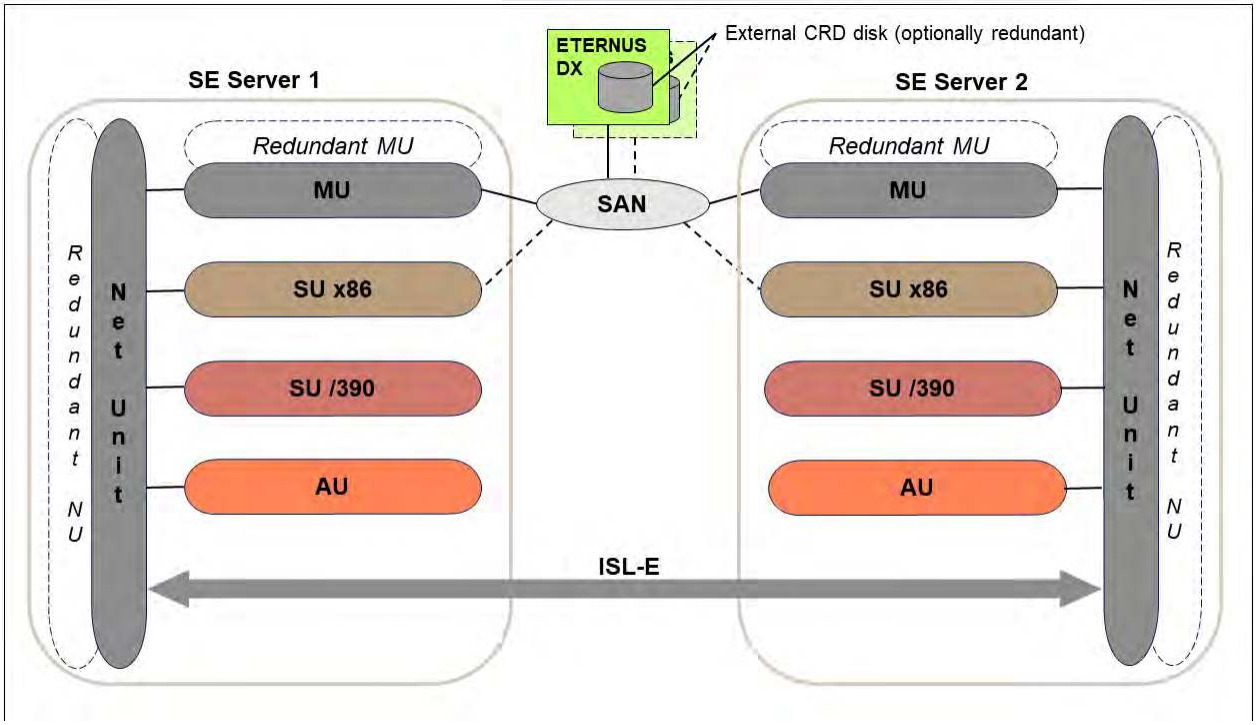


Figure 6: Management Cluster with two SE servers

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 each 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.

Figure 6 shows a Management Cluster with two SE /390 and additional SU x86 in each SE server. A Management Cluster can also be formed with two SE x86.

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.

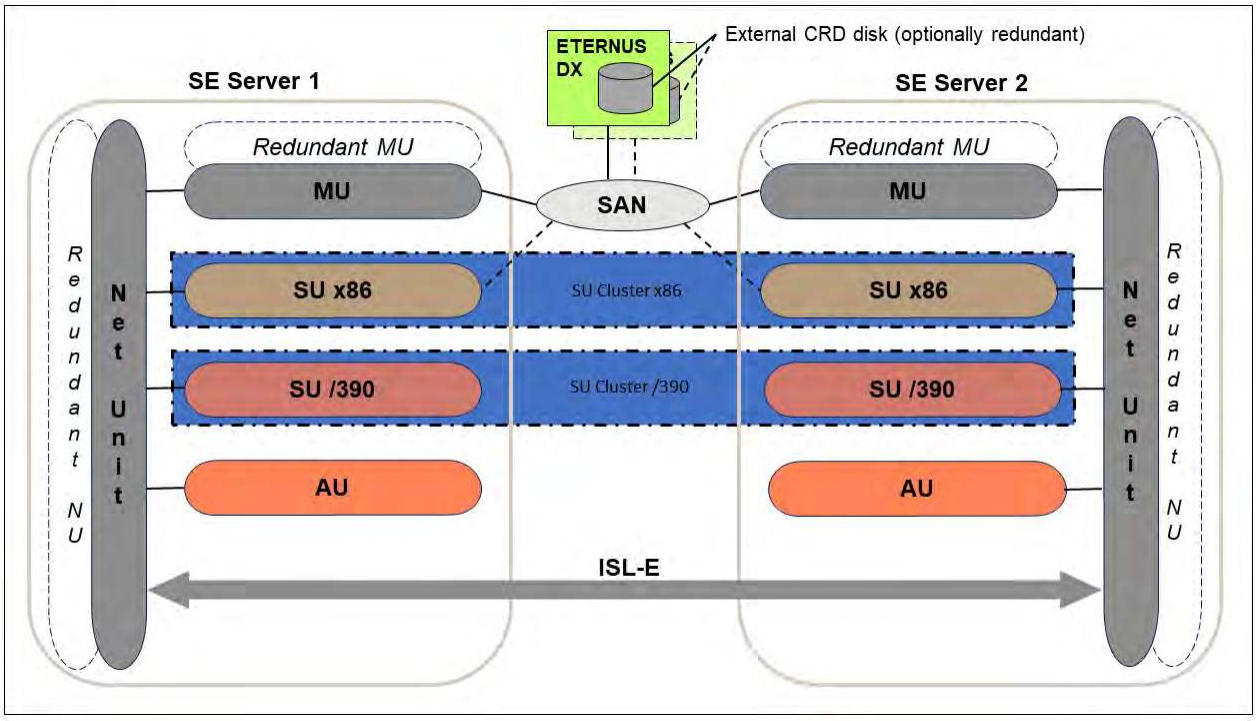


Figure 7: SU Cluster in a Management Cluster with two SE servers

Figure 7 shows a Management Cluster with two SE /390 and additional SU x86 in each SE server. A Management Cluster can also be formed with two SE x86.

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".

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.

These topics are described below:

- Role and user strategy
- IP-based access to the Management Unit
- Redundant Management Units
- Central logging

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 predefined basic roles. In addition, basic roles (except *Administrator* and *Service*) can be combined to user-defined roles.

In addition to the SEM functionality described below, each basic role also has access to some further SEM windows like the main windows *Dashboard* and *Certificates* and may change its own password on main window *Password management*, download the CA certificate of the MU and access the event logging.

The roles are tied to an account. In other words, users take over a role when they log 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".

All roles except the *Service* role can be assigned to additional accounts, see "Further accounts with role assignment".

All accounts to which the same role is assigned are equivalent. The only exception in this respect is for accounts with the *BS2000 operator* role. These are also initially equivalent. However, an administrator or security administrator can additionally assign them individual rights for access to BS2000 or the individual BS2000 VMs.

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.
- 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.

BS2000 administrator

Comprises (largely) the subset of the Administrator task area which refers to BS2000 systems (BS2000 systems, BS2000 devices, Backup Monitor, Net-Storage, Cluster, …).

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.

BS2000 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.

General access to the Linux shell is not possible. A BS2000 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.

AU administrator

An AU administrator has the authorization for functions of the SE Manager which are necessary to operate the systems on AUs. In addition, they also have some administrator authorizations: switching the AUs on/off, read access to the hardware inventory, and configuration of scheduled power on/off of the AUs.
Access to the Linux shell is not possible.

Read-only administrator

A Read-only administrator has the right to view all windows of the SE Manager, however modifying actions are not allowed.

Security administrator

A Security administrator has full authorization for the windows and functions of the SE Manager under the categories *Authorizations* and *Logging*.

Hardware administrator

A Hardware administrator has full authorization for the windows and functions of the SE Manager under the categories *Hardware -> Units, Hardware -> HW inventory, Hardware -> Energy* and *Service -> Units.*

Storage administrator

A Storage administrator has full authorization for the windows and functions of the SE Manager under the categories *Devices -> … -> IORSF files | Disks | Tape devices, Hardware -> Units -> … -> FC interfaces | Multipath disks | CRD disks* as well as *Hardware -> Storage* (without STORMAN!).

Power operator

A Power operator has authorization for the main window *Units* under the category *Hardware* and the functions for powering units on and off.

IP networks administrator

An IP network administrator has full authorization for the windows and functions of the SE Manager under the categories *Hardware -> Units -> … -> IP interfaces, Hardware -> Management -> … -> IP configuration | Routing & DNS* as well as *Hardware -> IP networks*.

FC networks administrator

An FC network administrator has full authorization for the windows and functions of the SE Manager under the categories *Hardware -> FC networks* and *Devices -> BS2000 paths*.

Shadow terminal operator

A *Shadow terminal operator* has authorization for access to the main window *Service -> Units -> <MU> -> Remote Service*, wherefrom a shadow terminal can be opened.

Add-on-specific roles

- OPENSM2
  - OPENSM2 administrator
    An OPENSM2 administrator has authorization for access to the add-on OPENSM2 and to its administration on all Management Units.
  - OPENSM2 information
    A user with role OPENSM2 information has authorization for access to the add-on OPENSM2. The administration of the add-on is not allowed.

- OPENUTM
  - OPENUTM administrator
    An OPENUTM administrator has authorization for access to the add-on OPENUTM and to its administration on all Management Units (Master and Administration Write privileges).
  - OPENUTM operator
    An OPENUTM operator has authorization for access to the add-on OPENUTM including administration (Administration Write privilege).
  - OPENUTM information
    A user with role OPENUTM information has authorization for read access to the add-on OPENUTM (Administration Read privilege).

- ROBAR
  - ROBAR administrator
    A ROBAR administrator has authorization for access to the add-on ROBAR and to its administration on all Management Units.
  - ROBAR operator
    A ROBAR operator has authorization for access to the add-on ROBAR. The administration of the add-on is not allowed.

- STORMAN
  - STORMAN administrator
    A STORMAN administrator has authorization for access to the add-on STORMAN and to its administration on all Management Units.
  - STORMAN information
    A user with role STORMAN information has authorization for access to the add-on STORMAN. The administration of the add-on is not allowed.

Service

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

When special basic roles are mentioned below, such as BS2000 administrator or Security administrator, this also refers to those user-defined roles which contain these basic roles.

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" 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 are internal function accounts, do not correspond to a role in the SE Manager and are therefore not displayed in the SE Manager.

Further accounts with role assignment

An administrator or security administrator can configure further accounts for all basic roles except *Service* and for user-defined roles. They assign the role during creation of an account. 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, an administrator or security 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". When this requirement is satisfied, the administrator resp. security 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 or security administrator can assign these authorizations individually also to a BS2000 operator account, in VM2000 mode specifically for particular guest systems.

For information on accesses to BS2000 for BS2000 operator accounts, see section "Managing individual rights".

Accesses to the operating system on Application Units

The customer is responsible for configuring accounts in the operating systems on 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").

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. The two MUs are equivalent in this case and each of them can be used for administration.

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 *SVP console* 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").

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").

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 redundant MU is the remote MU.

2.6.4 Central logging

The SE server configuration provides centralized access to the Audit logging 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" and "Displaying event logging").

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").

2.7 Virtualization

The description is divided into the following sections:

- Implementation of VM2000
- Virtualization on Server Unit x86

2.7.1 Implementation of 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.

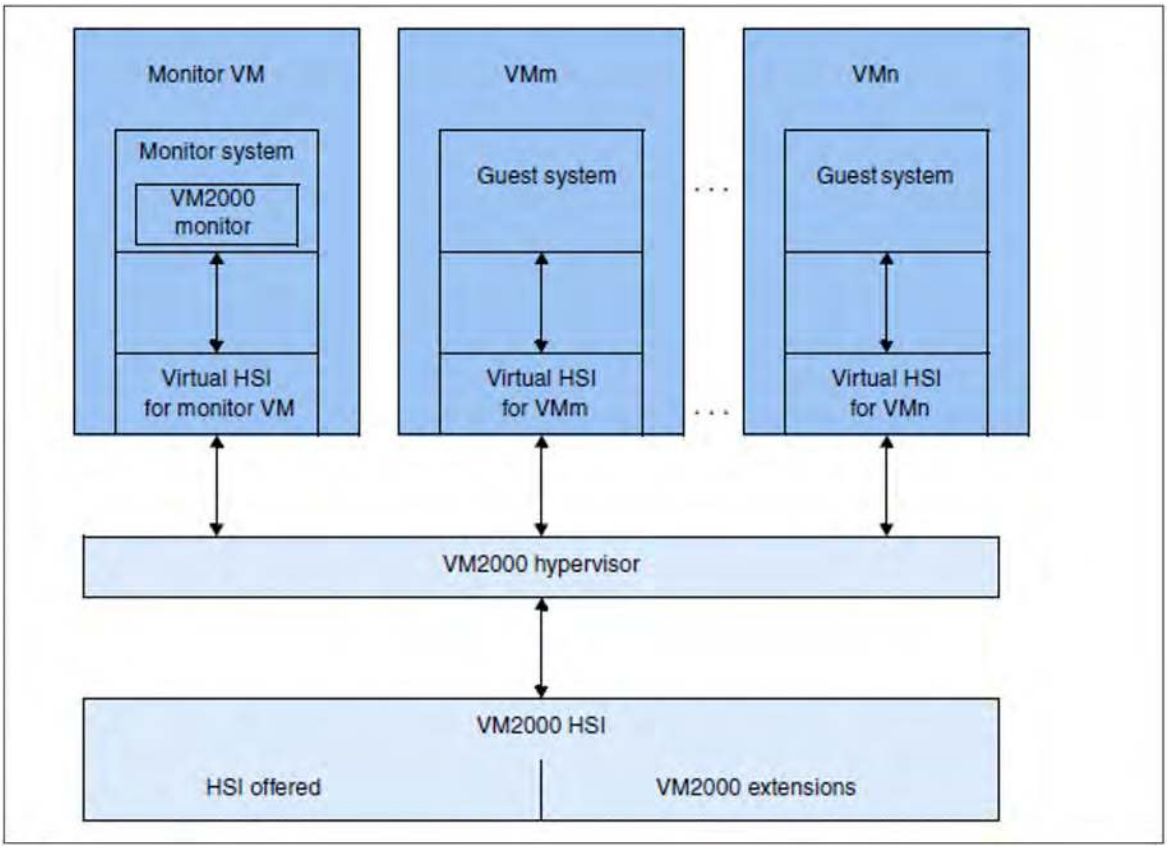


Figure 8: Structure of VM2000 on SU /390

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.

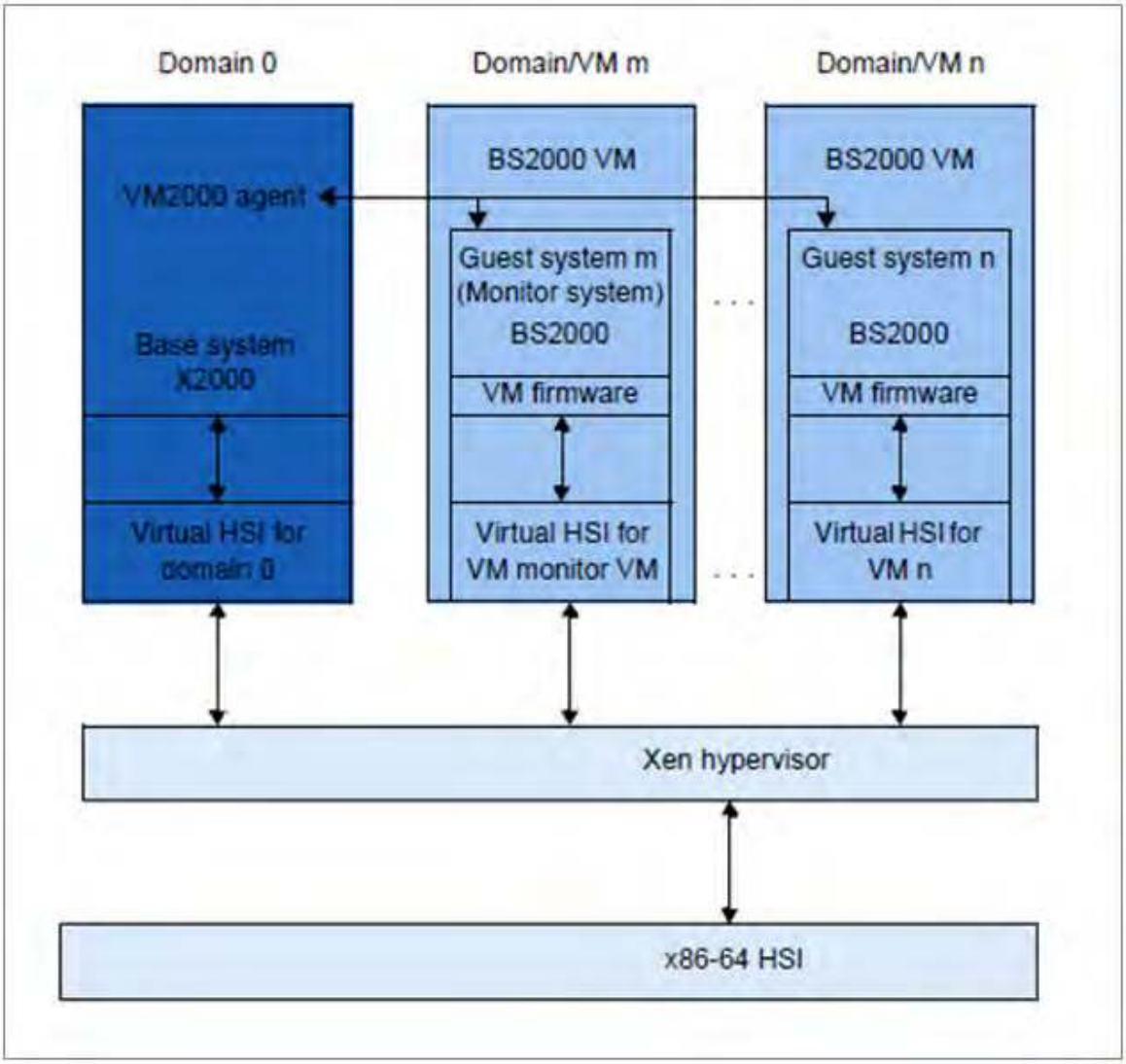


Figure 9: VM2000 on SU x86

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 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.

Main memory management

32 GB of the existing main memory is reserved for the X2000 carrier system. In addition, memory for the firmware of the individual BS2000 systems is needed.

BS2000 can use the remaining main memory on the Native system or on the BS2000 VMs.

The main memory is always allocated to the respective guest system only when a virtual machine is started (or when a BS2000 VM is created/activated), provided that free main memory is still available in the requested amount.

CPU pool management

The real CPUs of the Server Unit x86 are allocated to groups, 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 X2000 from the other 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 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.
- 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>
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. The BS2000 CoD CPUs are omitted (CoD means Capacity on Demand)
3. Alternating omission of one CPU of the BS2000 pool down to 2 CPUs
4. Pool 0 is reduced to 1 CPU
5. The last but one CPU of the BS2000 pool is omitted

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 as well as their current assignment to the defined CPU pools under *Systems* -> [*<se server> (SE<model>)* ->] *<su-name> (model) -> VM resources*.

For information on BS2000 and BS2000 VMs, see also section "Working in Native BS2000 mode" and section "Working in VM2000 mode".

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 devices".

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 (under *Hardware –> Units [–> <se server> (SE<model>)] –> <mu> –> Management –> System time*).

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"). 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.

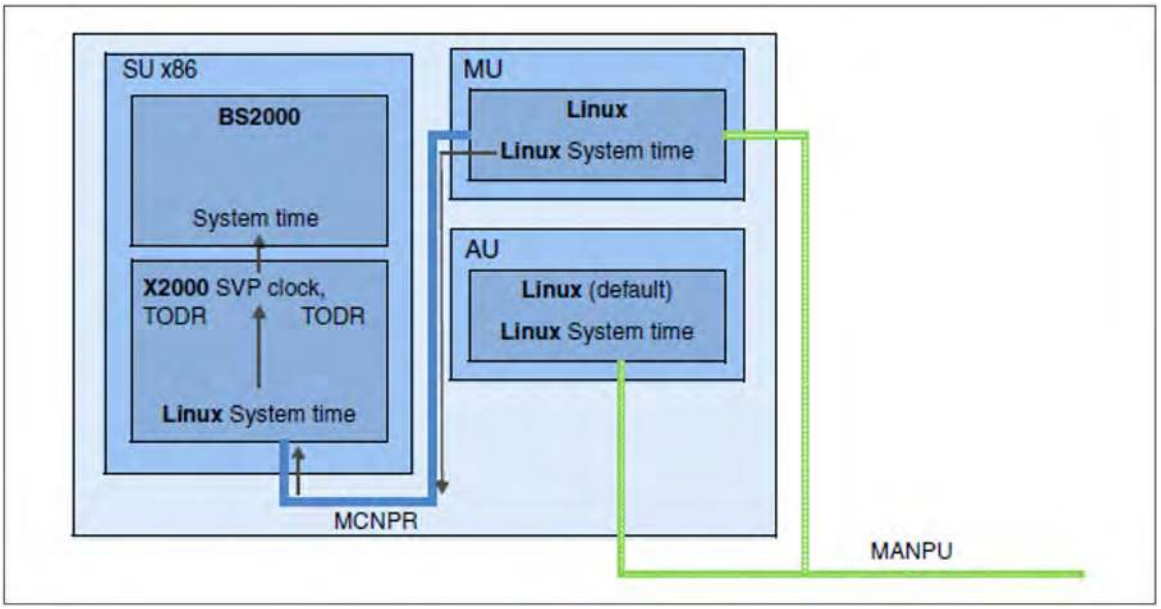


Figure 12: SE server with SU x86 only without external time synchronization (synchronized internally via the MU)

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.

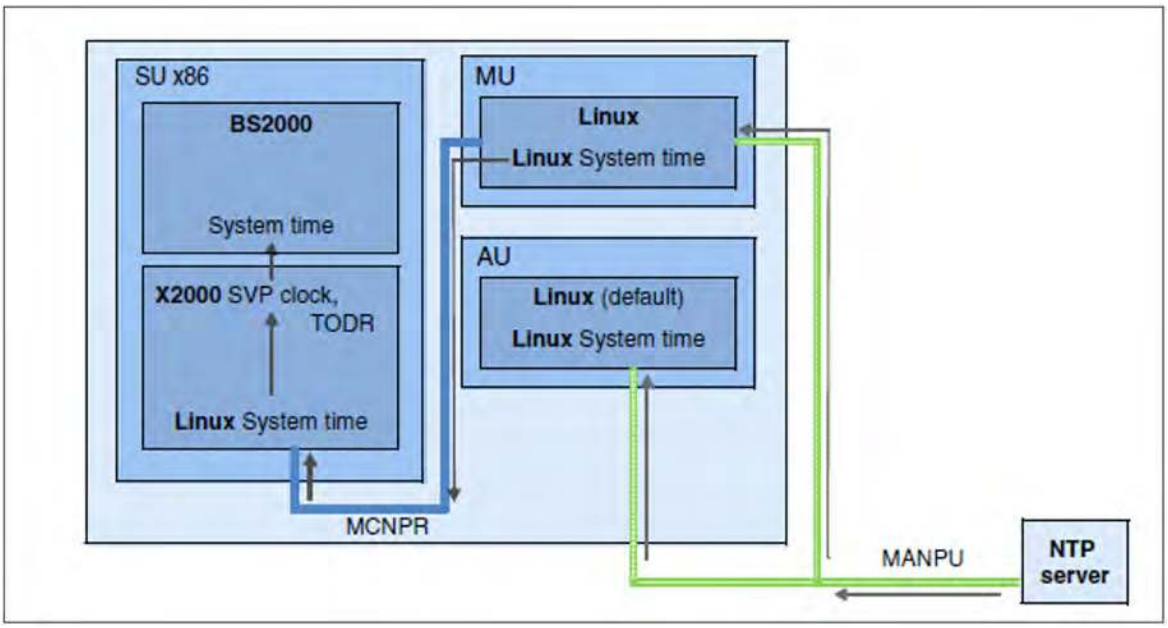


Figure 13: SE server with SU x86 only with external time synchronization

The SE Manager displays the current NTP configuration, see section "Setting the system time (time synchronization or local)". 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)".

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

2.9 Customer Support and maintenance

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.

In the SE Manager, the pages under the *Service* category serve as an interface between customers and Customer Support. You can also find more details on this under Managing service-related functions.

These topics are dealt with below:

- Tasks of Customer Support
- Tasks of the customer
- Handling updates

2.9.1 Tasks of Customer Support

Customer Support has the following tasks:

- Diagnostics and debugging
- Software/hardware maintenance work
  - Installation of updates
  - 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

> **Maintenance state**
>
> During maintenance work, you or the service team set the maintenance status (SE operating state Maintenance) to make all users aware of the special situation.
> See also the "Information" section in the "Managing service-related functions" chapter.

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 the updates
  - Uploading, installing and uninstalling add-on packs
  - Deleting update files which are not installed
- Generating and supplying diagnostic documentation
  For the standard generation of diagnostic documents, see the chapter Generating diagnostic data.
  Other diagnostic documents available on the Management Unit in file form can be made available to the service with the command `aisTransfer`. Its description can be found in the online help.
  Other diagnostic documents such as screenshots can be sent directly to the service by mail.
- Scheduled provision of an annual maintenance window of approximately 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.

Customer ID and serial numbers

When communicating with Customer Support, always specify the customer ID of your SE server that allows the service to identify your server configuration unambiguously. Determine the customer ID as follows:

> In the tree structure select *Service -> Information*.

  The *Information* tab shows the customer ID for the SE server.

In addition specify where appropriate 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.

> Then click the *Details* ( ) icon by the desired unit. The *Show details* dialog box informs among other things about the unit's serial number.

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).

Maintenance state

During maintenance work, you or the service team set the maintenance status (SE operating state Maintenance) to make all users aware of the special situation.
See also the "Information" section in the "Managing service-related functions" chapter.

2.9.3 Handling updates

Providing updates

Updates of the basic system you can receive by email, on CD/DVD or by means of remote service.

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
Update	• Provide maintenance window (if necessary)	• Clarify requirements • Procure update • Transfer update to system (via remote service or on site) • Install update (via remote service or on site)
Add-on pack	• Clarify requirements[1] • Procure software • Transfer software to system • Install/uninstall software	• Clarify requirements[1]

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

3 Operating the SE Manager

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

Requirement:

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

The web browsers currently supported are:

- Mozilla Firefox Version 102.5.0 (ESR) and higher
- Microsoft Edge
- Google Chrome

Restrictions can apply when other browsers are used (e.g. for uploads, downloads, display of certain pages like *Hardware inventory*).

The chapter is subdivided as follows:

3.1 Calling the SE Manager, logging in and logging out

> As address, enter the FQDN (Fully Qualified Domain Name) of an MU of the SE server into the address bar of the browser.

> Press the ENTER key.

> **i** If the browser now displays a warning about the security certificate, click *Continue to this website*. The procedure for confirming or importing a certificate is described in more detail in Section "Confirming/importing a certificate in the web browser".

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:

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

> Enter your account in the login window.

> Enter your password.

> **i** When the SE server is supplied, 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").
>
> 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").

> Click *Log in*.

To increase security, multi-factor authentication (MFA) can be configured for accounts. In this case, a one-time password has to be entered additionally in a second step. This password is generated using an authentication app. For more details, please refer to section Managing multi-factor authentication and to the SE Manager help.

The *Dashboard* tab opens as the welcome page. It provides a quick overview of the systems, BS2000 messages, 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.

Logging out

> In the header area of the SE Manager main window click *Log out* to terminate the session. See section "Main window".

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 they are assigned to your account. The SE Manager displays an overview over the active sessions under *Authorizations* -> *Users* -> *Sessions* (see section "Displaying sessions").

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

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. The session expires without explicit logout if you are inactive for a longer period of time, i.e. if the SE Manager does not register any action within a certain period of time. The default setting for this time is 20 minutes after creating an account.

Users can change this setting for themselves in the range from 5 through 60 minutes or disable the session timeout at all:

> Click in the login information in the header area. A list containing the menu item *Individual settings* opens.

> Click *Individual settings*. The *Change individual settings* 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".

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".

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 the automatic update is switched off for each user. Each user can change this setting for themself so that an automatic update takes place every 10 to 120 seconds or switch off the automatic update again. The setting is specified in the *Change individual settings* dialog box (see section "Session timeout"). The individual setting is stored on an account-specific basis.

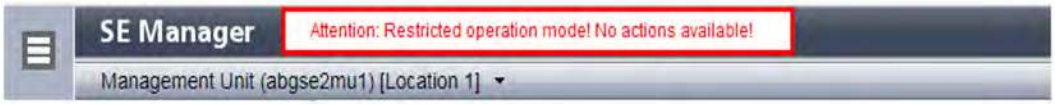
The automatic update is suspended as soon as an action is selected in the main window (e.g. when an action is selected in the *Actions* group in the *Operation* main window for a BS2000 system). In this case, the *Continue with automatic update* icon () is displayed instead of the update icon. Clicking this icon continues the suspended automatic update.

3.2.3 Restricted operation mode

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

In these situations, the operation 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 operation mode in the header of the main window as follows:



In dialog boxes, the restricted operation 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 its resources, the restricted operation mode terminates 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.

- Window types
- Main window
- Terminal window
- The dialog
- The wizard
- Web UIs of Application Units

3.3.1 Window types

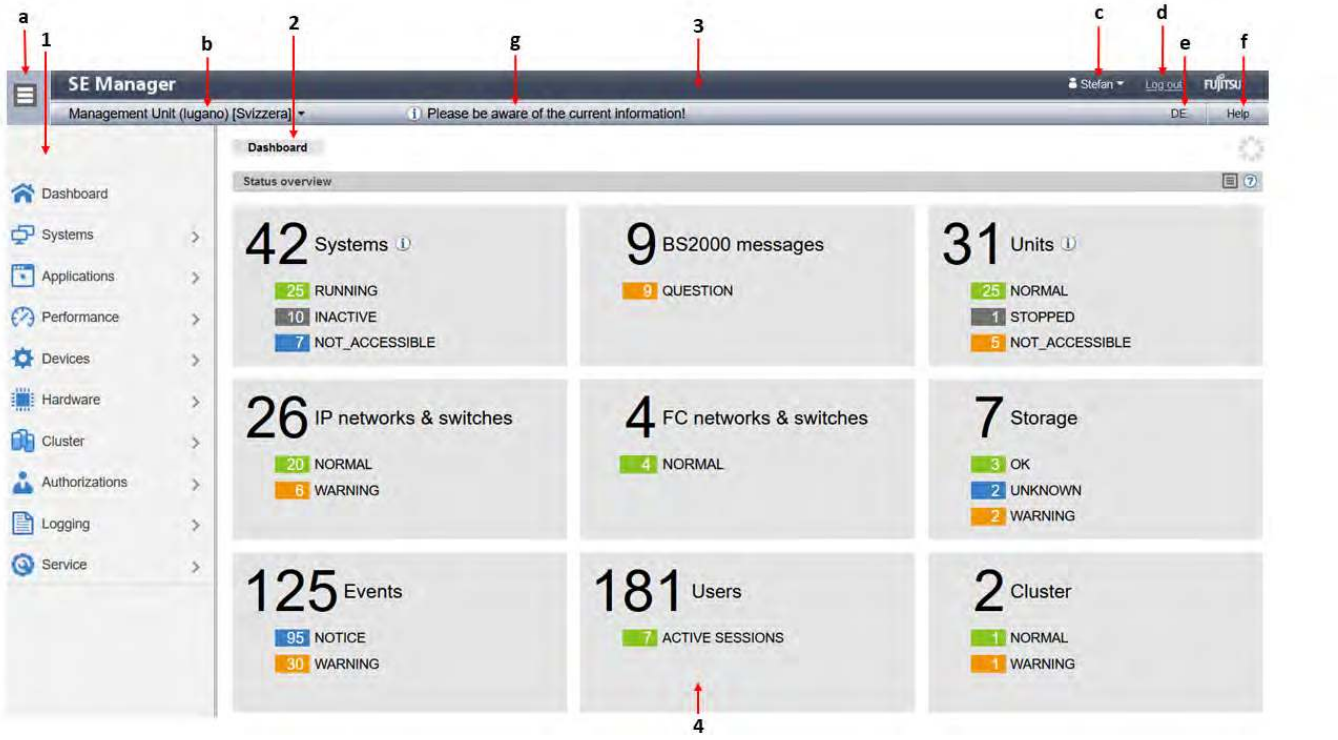
Various window types are used in the SE Manager:

- **Login window**: a window in which you log in using your account and password. See section "Calling the SE Manager, logging in and logging out".
- **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".
- **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".
- **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".
- **Wizard**: a utility which guides you step by step through a sequence of windows (dialogs) to perform a task.
  See section "The wizard".
- **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".

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 (see "Automatic update"), the *Update* icon (wheel) is displayed on the right-hand edge. During an update, the wheel is rotating. Otherwise it is greyed out. When the automatic update is suspended, the icon *Continue with automatic update* ( ) is displayed instead.

3: Header area

Contains general information and settings for the SE Manager:

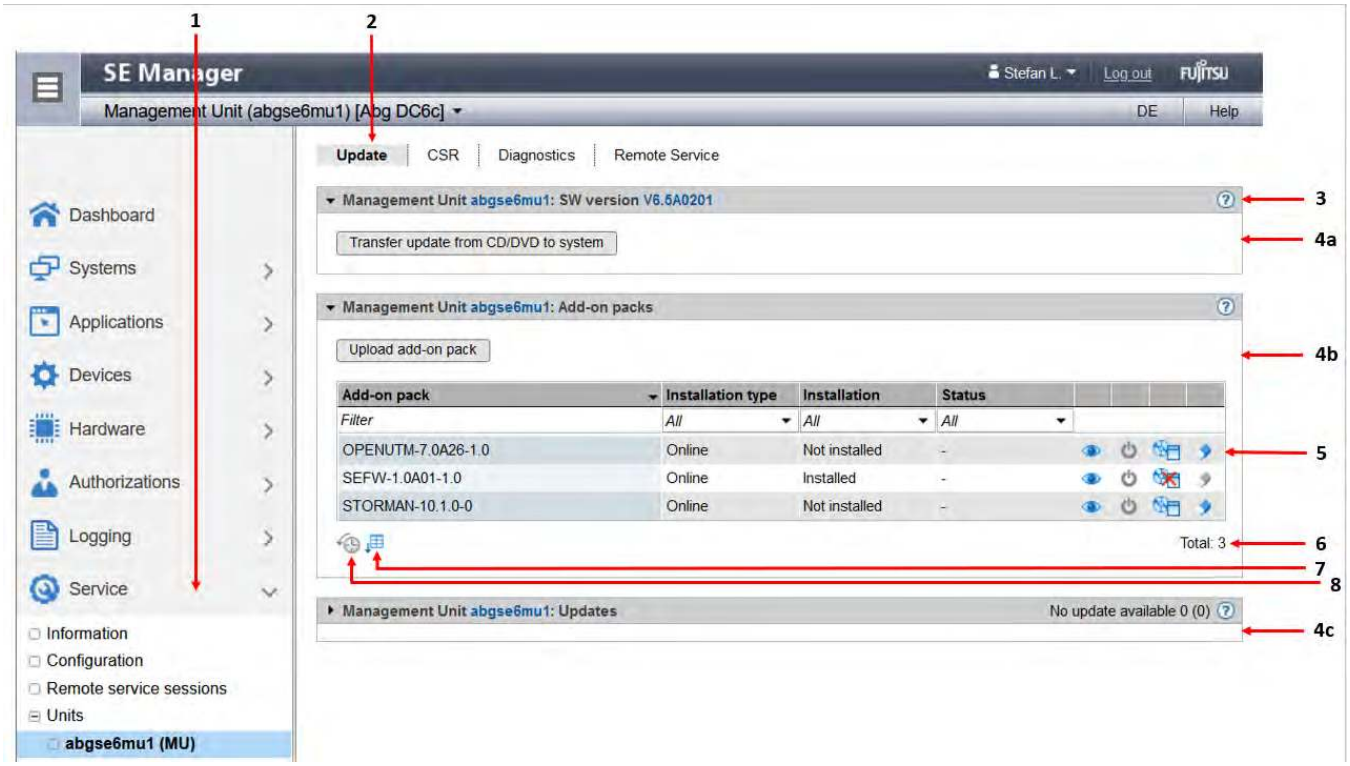
a	Click the icon to hide or display the tree structure again.
b	*Management Unit (<unit>) [location]* provides information about the Management Unit via which you are currently operating the SE Manager. *<unit>* is the name of the Management Unit. If a location is configured with SYSLOCATION, *<location>* displays the entry. For the configuration of the local system data see section "Managing SNMP".

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.
g	This hint is displayed regardless of the currently called main page, if an information has been configured (see "Information").

4: Working area

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

SE Manager: elements of the main window

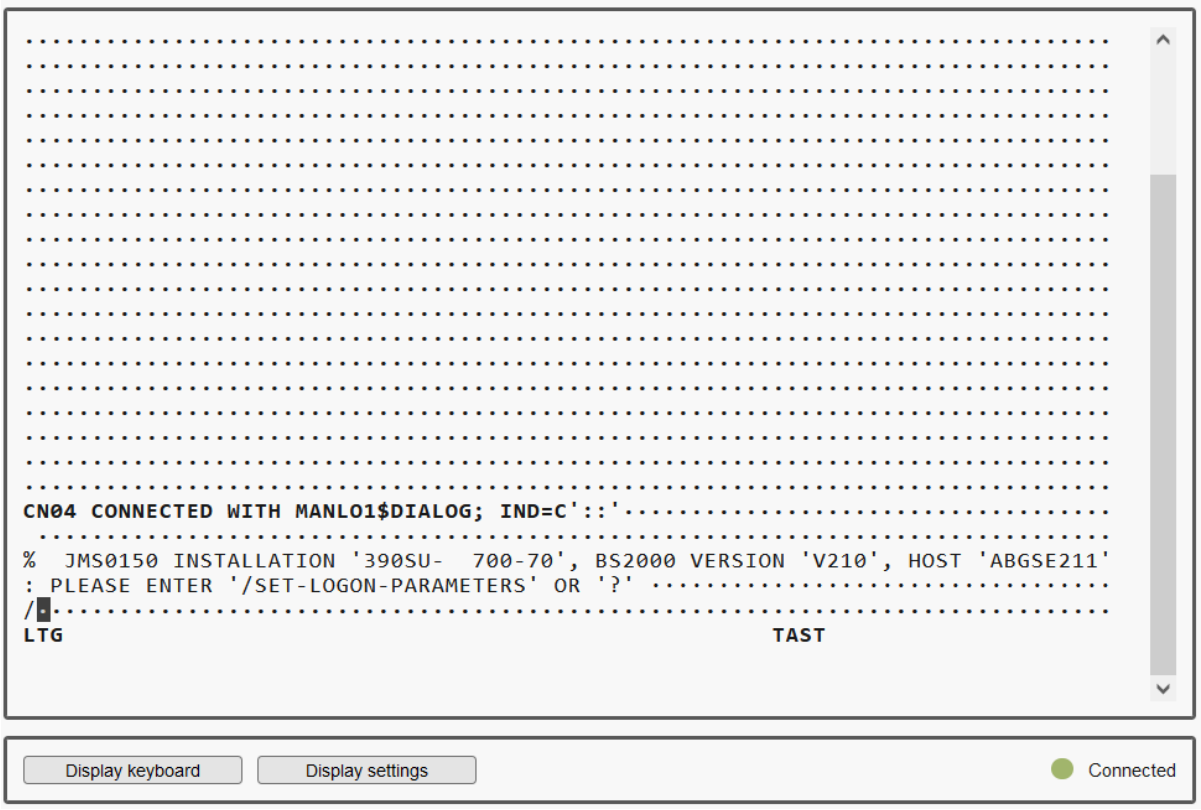


1	Active main menu of the tree structure

2	Active tab
3	*Help* icon for calling the SE Manager help on a context-sensitive basis (see "Calling the online help")
4a, 4b, 4c	The information may be subdivided into groups (in the example above, 4a, 4b, 4c). 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 4c in the above example). Each group contains one or more tables with properties of the objects displayed.
5	Icons for triggering actions. Depending on the situation, icons may be deactivated (greyed out); in such situations the corresponding action cannot be triggered.
6	Number of entries in the table *Total: <n>* or *Total <objects>: <n>*
7	The *Export of table* icon allows to export or print the table data.
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 window, SVP console window, AIS Connect shadow terminal, and shell terminal (CLI) on an MU are opened in a separate terminal window (SE Manager's Virtual terminal, SEMVT) after they are called in the SE Manager. Subsequently the terminal window remains open irrespective of the SE Manager's session. The following example shows a terminal window with a BS2000 dialog:



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) can be displayed or hidden as needed: The virtual keyboard enables all required characters and function keys to be entered irrespective of the real keyboard's layout.
- Several properties of the terminal window are configurable.
- You can transfer text between Windows and SEMVT via Copy & Paste. In SEMVT this functionality is available from the context menu (right mouse button).
- The current status of the connection is displayed in the lower right corner of the terminal window:

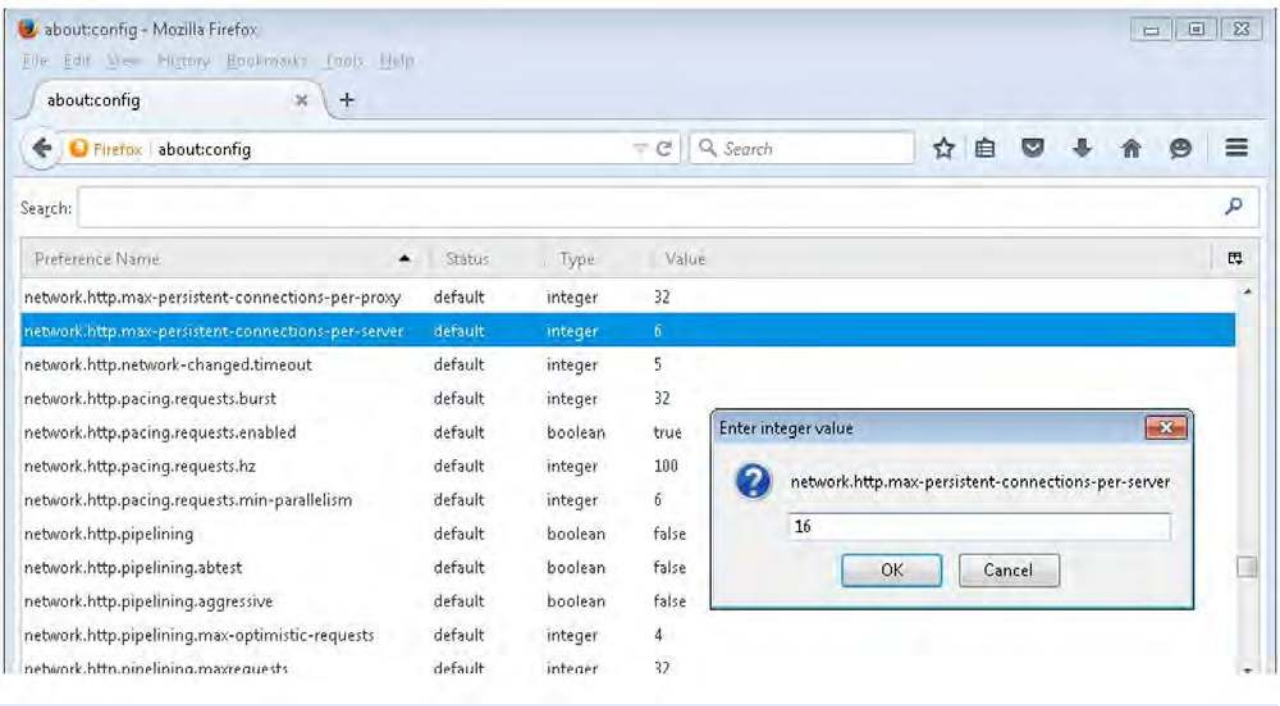
  During initialization of the terminal window, a yellow status icon and the text **Initializing...** is displayed.

  A green status icon and the text **Connected** indicates that a connection exists. The terminal window can be used normally.

  A red status icon and the text **Disconnected** indicates that the connection has been terminated or is broken. In this case, a message describing the reason for the loss of connection is displayed. In addition, in front of the icon the button **Reconnect** is offered to restore the connection (a prerequisite for this is that the SE Manager session in which the terminal window was opened is still active), and another button **Hide message** resp. **Show message** allows for hiding or showing the message. The terminal window is closed by pressing the Enter key.

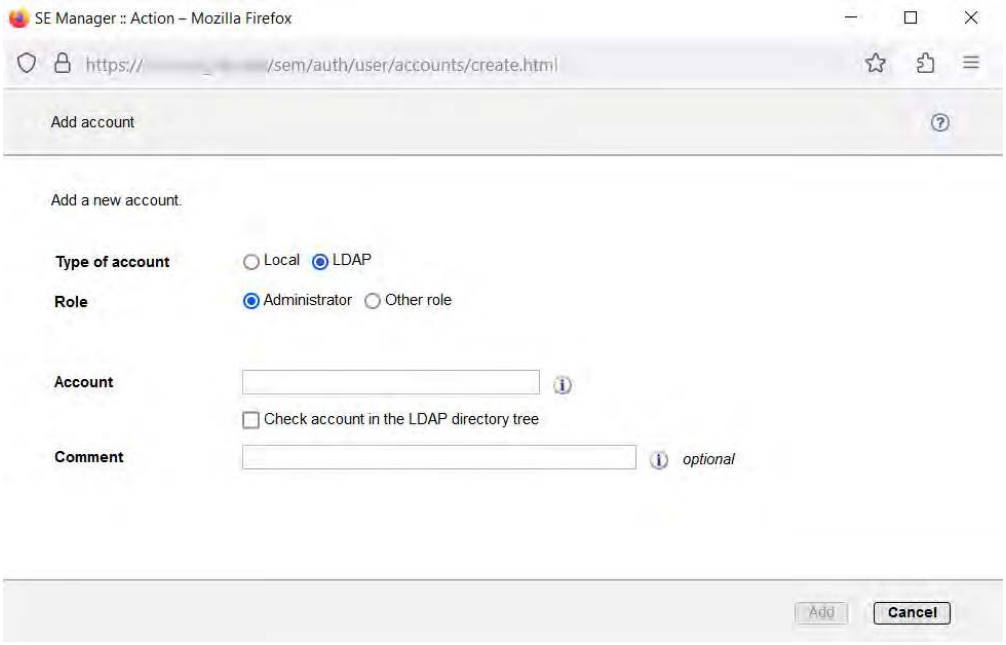
If you want more than one terminal window to remain open in parallel (e.g. with BS2000 console windows), this must be supported on the client side by the number of possible connections to a server. To achieve this, you must configure your browser to support the desired number of parallel connections, if necessary.

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



3.3.4 The dialog

A dialog opens as soon as you start an action. Example:



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 when a value is entered in a field. An info icon ( ) is displayed next to entry fields. When you drag the mouse over the info icon, possible values or the syntax to be used are displayed.
- Area with the labeled buttons, e.g. *Add* 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" describes what you must take into account when executing an action.

3.3.5 The wizard

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

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

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

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

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

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

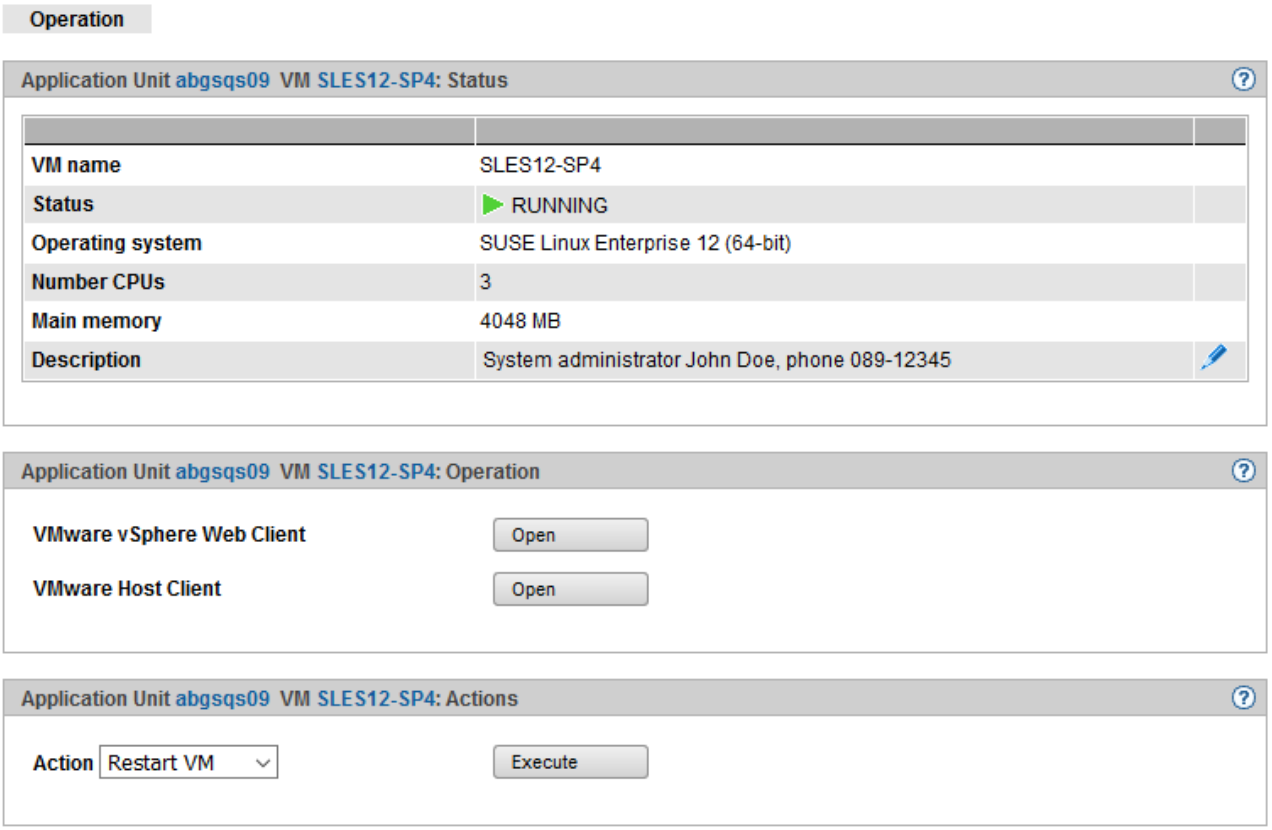
3.3.6 Web UIs of Application Units

On Application Units, web applications such as a VMware ESXi Server 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>)* –> *<vm-name>* leads to the *Operation* tab.



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

The following sections describe aspects of 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.

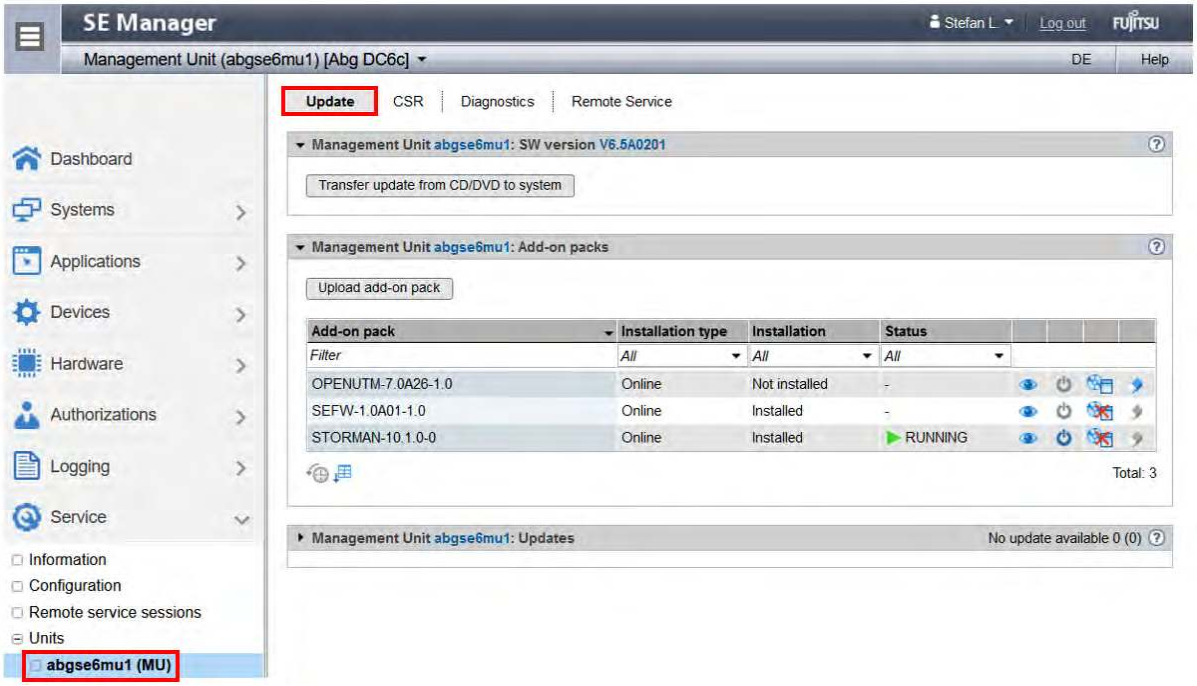
The content of the working area changes if you select another tab.

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

Example

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

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



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*, *Logging*, and *Service*. 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 menus is also referred to as the primary navigation.

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

A main menu collapses in the following cases:

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

Dynamic extensions of the navigation

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

- *Systems* main menu:
  - when creating a BS2000 VM
  - after a virtual machine has been created on an AU
- *IP networks* main menu:
  - when creating a new network
- when installing an add-on - see the text below
- when creating a SU cluster or a management cluster - see for this also the text below

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*. For STORMAN versions V10.3 and higher on the local MU, the Storage Manager is directly integrated into the SE Manager. The STORMAN user interface is accessible immediately below the *Storage* menu.

The links to the add-ons ROBAR and openUTM are available under the *Applications* main menu.

Authorizations

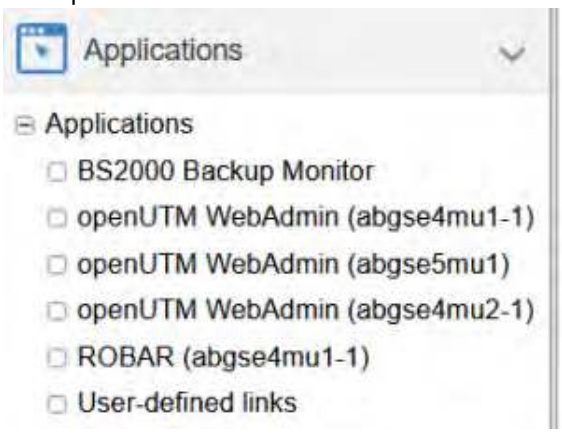
The scope and thus the visibility of the functions depends on the role which is assigned to your account.

In the SE Manager, each user sees only those functions to which the role assigned to their account entitles them.

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 *Hardware -> HW inventory* menu, the *Units* tab displays in case of a Management Cluster a total overview of all units of the participating SE servers.
  The *Hardware -> HW inventory -> <se server> (SE<model>)* menu in this case displays the SE server-specific tabs *Rack view*, *Units*, *Components,* and *Administration*.
- In the *Authorizations -> Certificates -> <mu-name> (MU)* menu, you manage certificates of the respective MU.

Expanded navigation in case of installed add-on NUX

If the add-on pack NUX is installed on at least one MU, the structure of the primary navigation beneath the main menus *Systems* and *Hardware -> Units* is extended: Both main menus receive rack-specific substructures *SE<se-index> AU<rack-index>xx* corresponding to the name scheme of the AUs, under which the links to the individual AUs of the rack (with a corresponding submenu if necessary) can be found.

3.4.3 Filtering, sorting and exporting 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".

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 SE Manager 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.

With a free-text filter, hits are searched for at every position of a cell without differentiating between upper and lower case. Otherwise, the rules for the so-called regular expressions apply when searching.

> ¡ 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.

Export of table data

You can either print the data of a table or export it in XLSX format. To do this, choose the icon  below the table to call up the *Export of table* dialog. Details can be found in the online help.

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 "The dialog" for the layout.

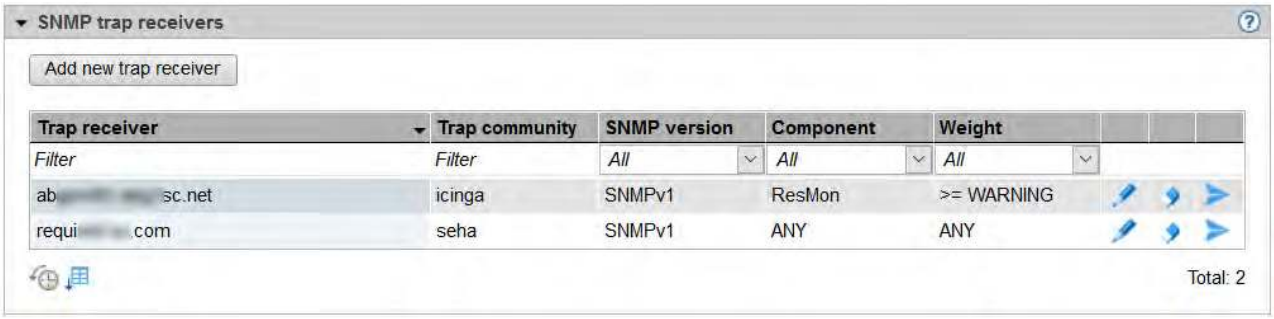
Within the dialog proceed as follows:

> 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.

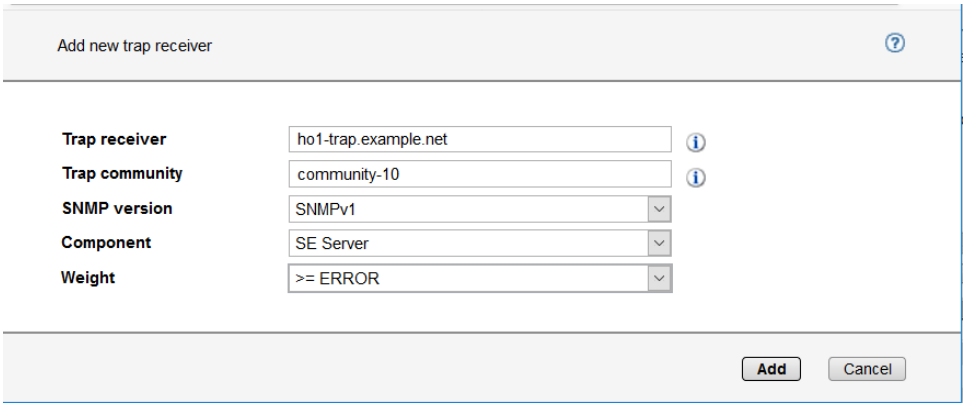
Example of how an action is executed



> Log in to the SE Manager.

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

> In the *SNMP trap receivers* group click *Add new trap receiver*.
A dialog with a parameter area opens.



> Enter an IP address or an FQDN as trap receiver.

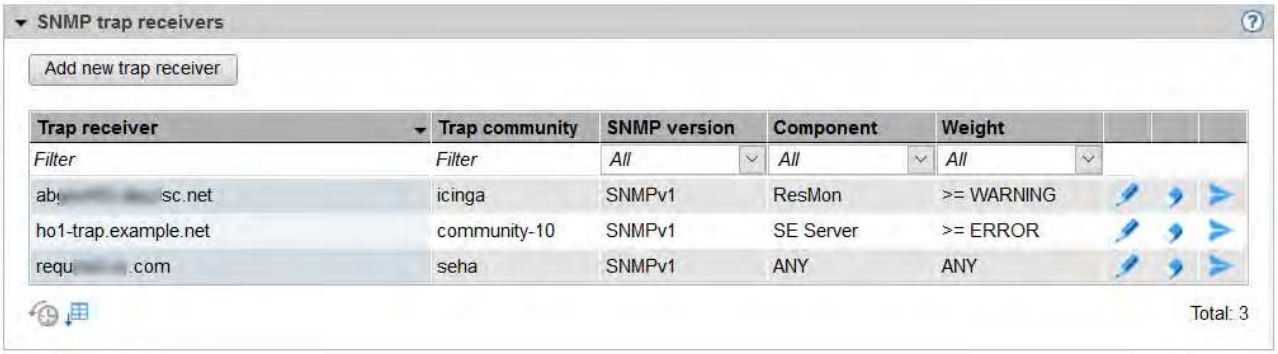
> Enter a trap community.

> Select component, SNMP version, and weight.

> Click *Add*.

After execution of the action, the message that the trap receiver has been successfully added appears.

> Click *Close*.



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 (?) 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:

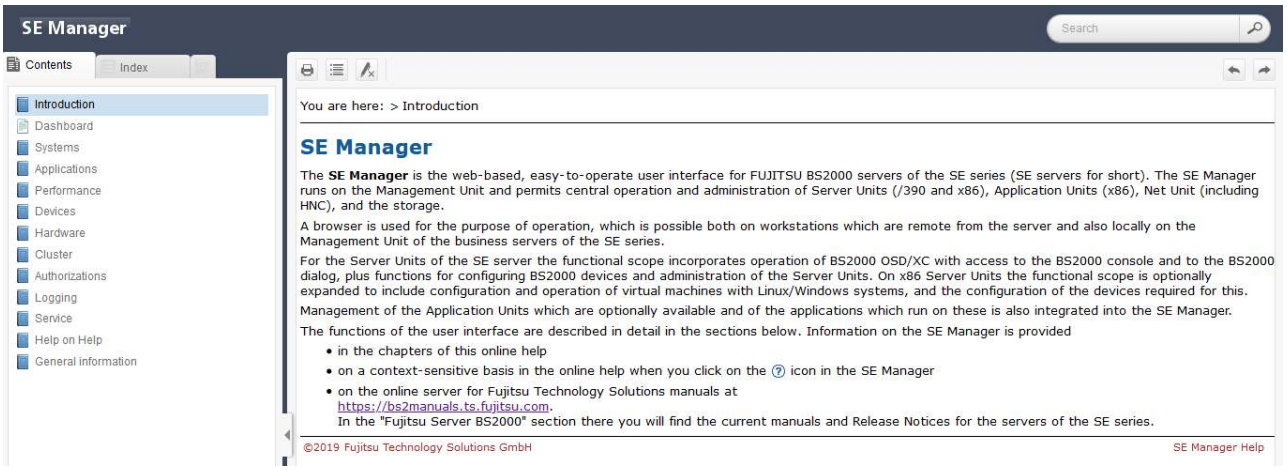


Figure 15: Homepage of the SE Manager help

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 *General 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 IP-based access rights are configured: Make sure that access is allowed for the IP address of your computer.

> 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").

> 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, BS2000 messages, Units*, *IP networks & switches*, *FC networks & switches*, *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 three status classes are displayed per object type. If more than three 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.

> 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 three status classes are displayed. If more than three status classes are currently assigned, the last line displays the status class with the highest priority level. The sum display also contains the less urgent problematical states that 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.*

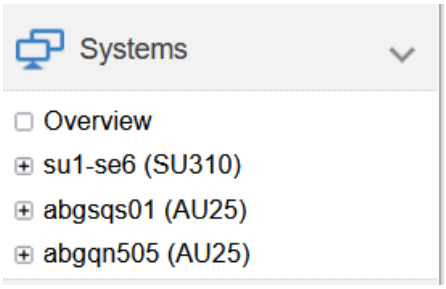
    The associated overview page opens with the corresponding filter, in this example the *Systems* main menu with the *Overview* tab. Only the VM2000 systems with the status *INACTIVE* are displayed.

5 Operating and managing systems on Server Units

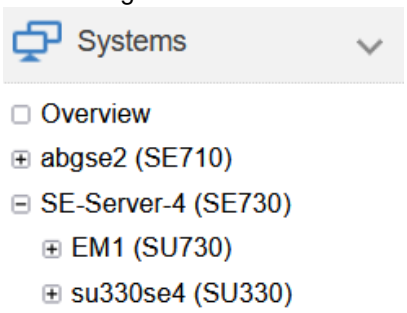
The systems referred to here are the Native and virtual operating systems which run on the various units of the SE server.

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

Managing a single SE server
(with SU x86 and AUs)



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 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, SU730 refers to a Server Unit of the type /390.
- In the example, SU310 refers to a Server Unit of the type x86.
- In the example, AU25 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".

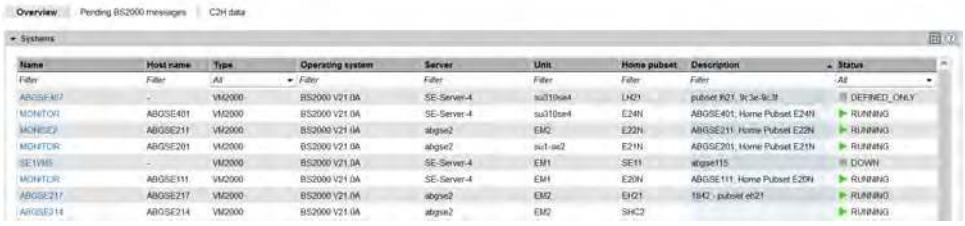
If you manage a configuration of two or more SE servers in a Management Cluster, underneath *Systems*, a submenu *<se server> (SE<model>)* will be displayed for each SE server, containing the SUs and AUs of the respective SE server.

Also, if the add-on pack NUX is installed on at least one MU, the structure of the primary navigation underneath *Systems* is extended: The main menu receives rack-specific substructures *SE<se-index> AU<rack-index>xx* corresponding to the name scheme of the AUs, under which the links to the individual AUs of the rack (with a corresponding submenu if necessary) can be found:

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:



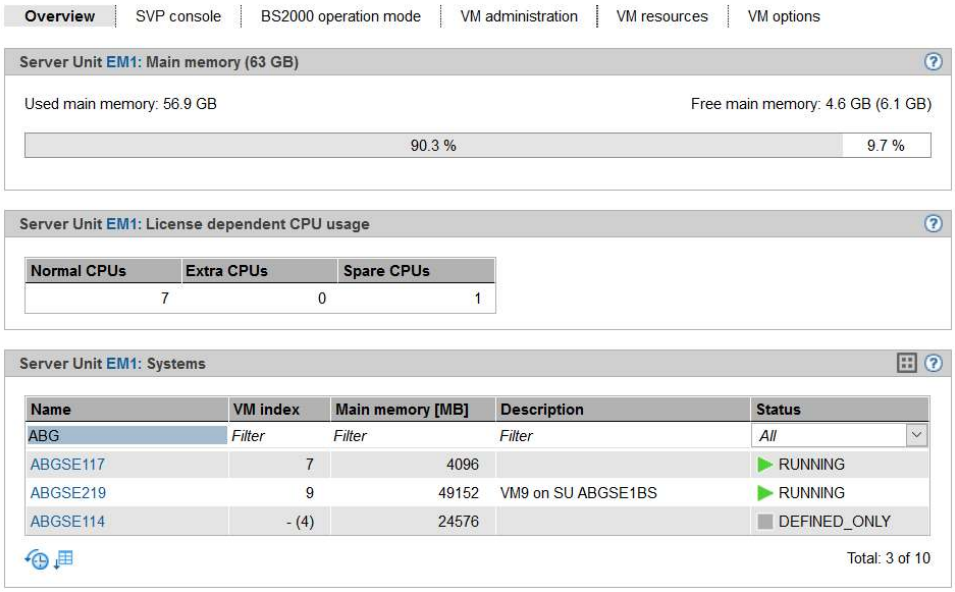
> When you click on a system in the *Name* column, the *Operation* tab of the selected system opens.

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

Under the category *Systems* -> *Overview,* the *Pending BS2000 messages* and *C2H data* tabs also display messages waiting for a response of all BS2000 systems of the SE administration area and output data of the BS2000 tool C2H (C2H reports and global C2H tables).

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 SU /390:



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

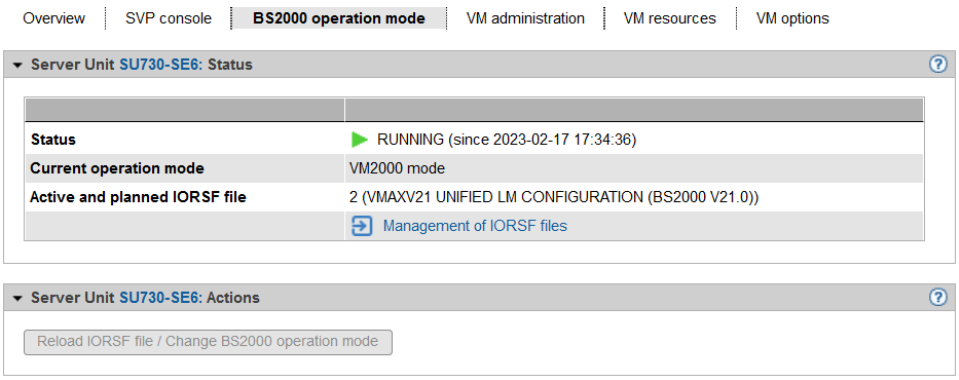
5.1 Setting BS2000 operation mode

You set BS2000 operation mode on a unit-specific basis. The procedure differs depending on the type of the Server Unit.

- Server Unit /390
- Server Unit x86

5.1.1 Server Unit /390

> Select *Systems* -> [*<se server> (SE<model>)* ->] *<unit> (SU</390>)*, *BS2000 operation mode* tab.



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:

Reload IORSF file / Change BS2000 operation mode

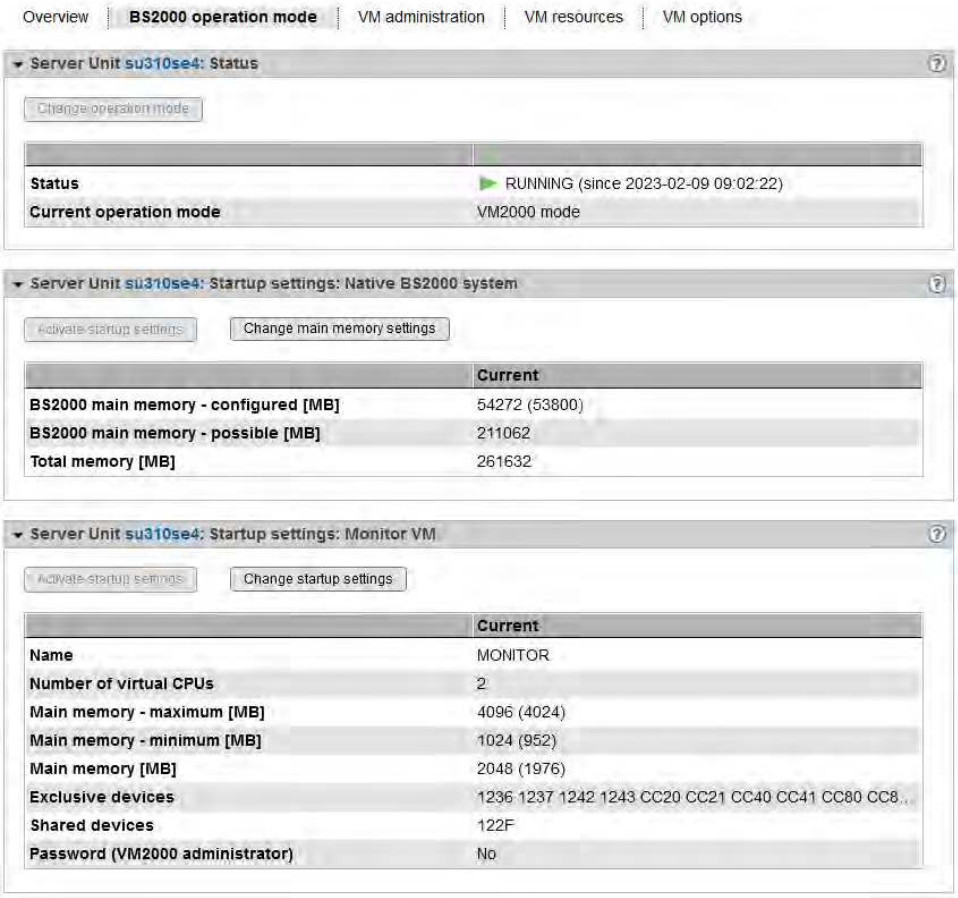
You can change the operation mode only when no BS2000 system is active.

> In the *Actions* group click *Reload IORSF file / Change BS2000 operation mode*. In the subsequent dialog box, enter the IPL parameters for the IMPL. Optionally, you can change the operating mode.

> ℹ 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.

5.1.2 Server Unit x86

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



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 *Change operation mode* and confirm the switch to the other operation mode.

> **i** When you switch mode, the *Automatic IPL* option is implicitly set to *Not planned*. 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 *Change main memory settings*.

> To change the name of the monitor VM, 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 *Change startup settings*.

> To activate the startup settings of the respective operation mode, click *Activate startup settings* in the corresponding group. The function is only available if BS2000 is not active.

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), 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<model>) -> <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 "Operating BS2000 with PuTTY".

5.2.1 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 (on SU x86 only)
IOD	Messages of the I/O handler for bus devices (on SU x86 only)
HAL	Messages of the Hardware Abstraction Layer (on SU x86 only)
SNX	Messages for write operations to 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 https://bs2manuals.ts.fujitsu.com or on the "BS2000 SoftBooks" DVD.

> In BS2000 you can 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.

5.2.2 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. The dialog with BS2000 is started and you are prompted to login with BS2000 command /SET-LOGON-PARAMETERS.

The following sections describe shortcuts and programmable keys:

- Using shortcuts for special characters
- Using programmable keys (pfkeys)

5.2.2.1 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 4: 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.

5.2.2.2 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 "Using shortcuts for special characters", 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 "Using shortcuts for special characters", 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.

5.3 SVP console on Server Unit /390

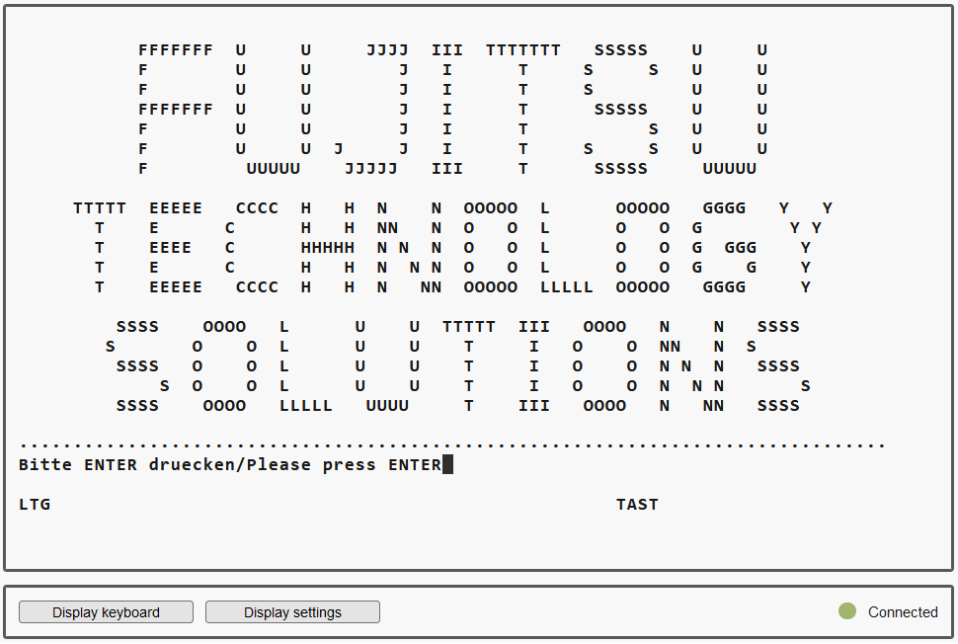
A Server Unit /390 is operated via the SVP (service processor). Some important SVP functions, for instance for IPL or IORSF, are also available directly on the SE Manager.

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>)*, *SVP console* 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].

SVP console via PuTTY

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".

SVP connection in case of redundant Management Units

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

Switching active Management Unit

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

> **i** 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".

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 Start/shut down a BS2000 system, execute an IPL dump and migrate

You perform these actions from 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

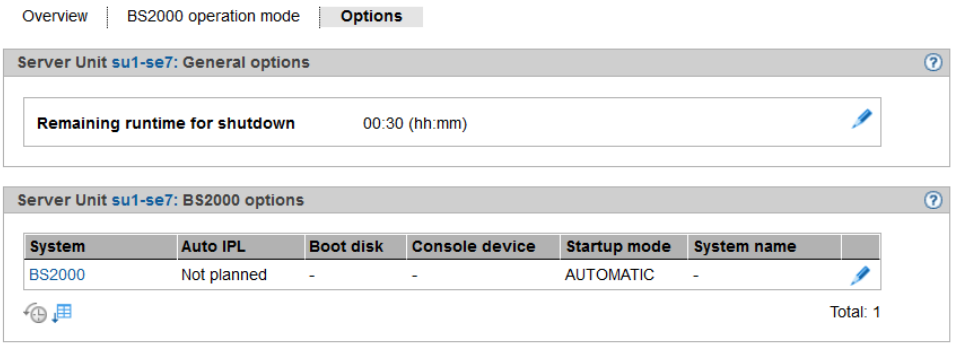
The following actions are only available for SU x86. The SU x86 also has to form an SU Cluster with another SU x86 of the SE server configuration. Whether or not an LM (Live Migration) is possible, depends on the cluster status. The second SU must also be in the *Native BS2000 mode* operating mode. See also section "SU Cluster". 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>)* , *Options* tab.



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").

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 the *Change* icon and set the required remaining runtime.

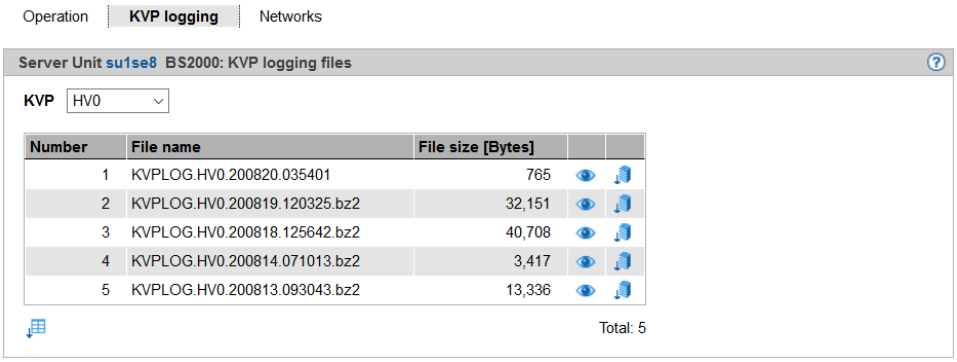
Setting BS2000 options (startup and auto IPL)

> In the *BS2000 options* group click the *Change* icon 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 a KVP logging file

> 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* dialog box in which the logging records of the selected file are displayed. You can limit the time range for the logging records to be displayed and filter the output.

Downloading a 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.

5.5 Working in VM2000 mode

You manage the BS2000 VMs of a Server Unit using the menu item *Systems* -> [*<se server> (SE<model>)* ->] *<unit> (SU<model>)*.

> For an SU /390, the VM2000 management by SE Manager is only possible when REWAS is active in the monitor system, see also section "Integration of BS2000 into the SE Manager".

Working in VM2000 mode is described in the following sections:

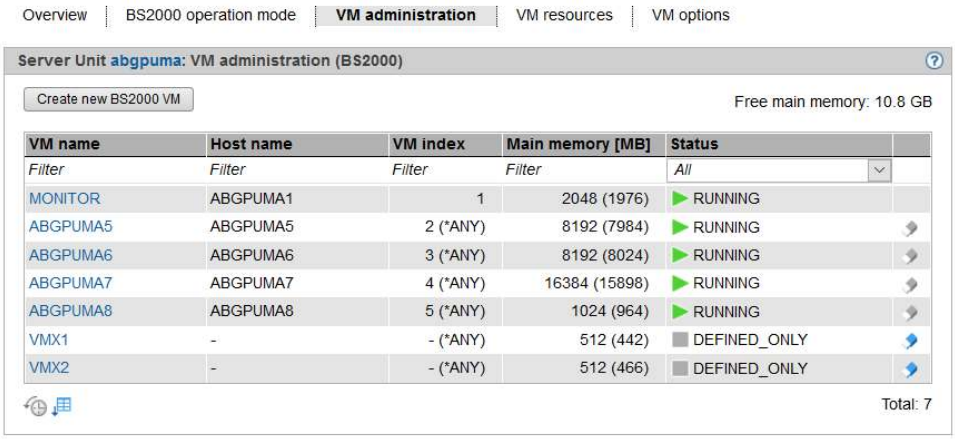
- VM administration
- Managing VM resources
- Setting VM options
- Operating a VM
  - BS2000 guest system - Information and Operation
  - Managing devices of the VM

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<model>) , VM administration tab



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.

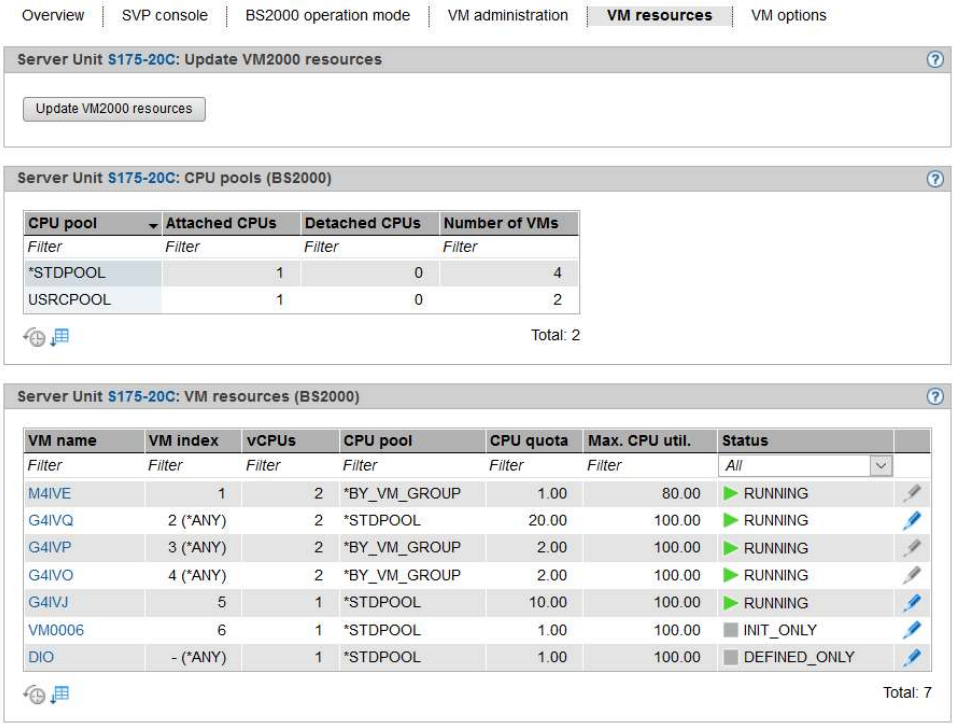
BS2000 VMs can only be deleted if they are in DEFINED_ONLY status.

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<model>)* , *VM resources* tab



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 functions are available:

Update VM2000 resources (for SU /390 only)

> You should use this action if you have carried out preparatory measures in VM2000 and want to continue work in the SE Manager. This ensures that the VM resource data such as main memory and CPU pools displayed in the SE Manager are up-to-date.

Change resources of a BS2000 VM

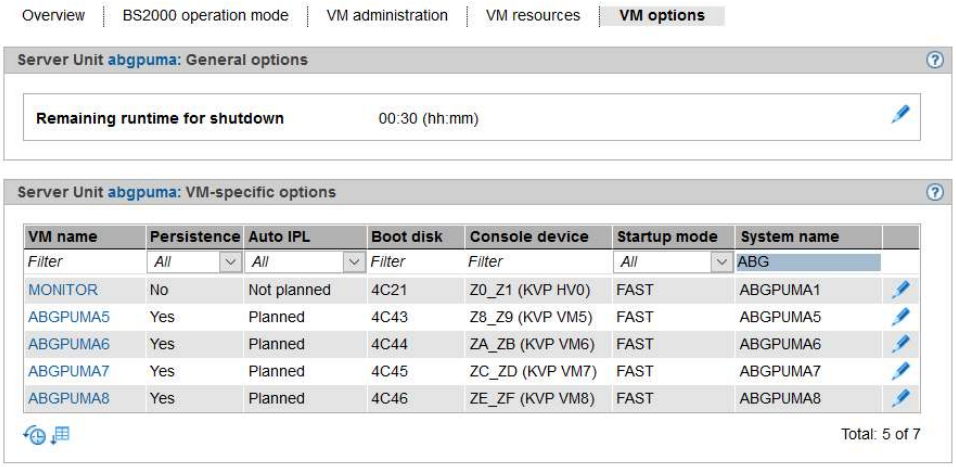
> By the required BS2000 VM click the *Change* icon and make the requisite changes in the *Change resources* dialog box.

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<model>) , VM options tab



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 above.

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.

> **i** 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 of the remaining runtime for Native mode, see section "Setting the options (only SUx86)".

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 the *Change* icon 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<model>)* -> *<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:

- BS2000 guest system - Information and Operation
- Managing devices of the VM

5.5.4.1 BS2000 guest system - Information and Operation

> Select: *Systems* -> [*<se server> (SE<model>)* ->] *<unit> (SU<model>)* -> *<bs2000-vm>*, *Operation* tab

The *Operation* tab displays the status of the VM, enables you to enter or change a description of the VM, displays pending BS2000 messages, offers access to the BS2000 console and BS2000 dialog, and allows 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.

> The action *Migrate BS2000 VM* is only available if the SU is a member of an SU Cluster and Live Migration is possible. The second SU must also be in the *VM2000 mode* operating mode. See also section "SU Cluster". 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".

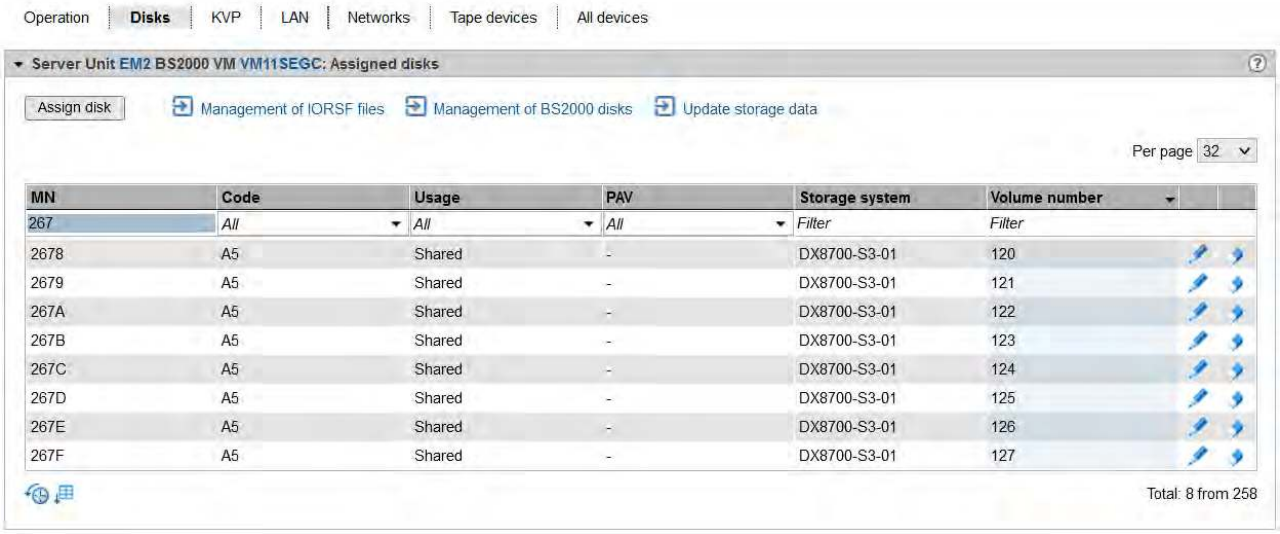
5.5.4.2 Managing devices of the VM

> Select: *Systems* -> [*<se server> (SE<model>)* ->] *<unit> (SU<model>)* -> *<bs2000-vm>*, tabs *Disks*, *KVP*, *LAN*, *Networks*, *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.



> 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".

> Click the *Change* icon by a disk to change the usage of this disk (Shared/Exclusive).

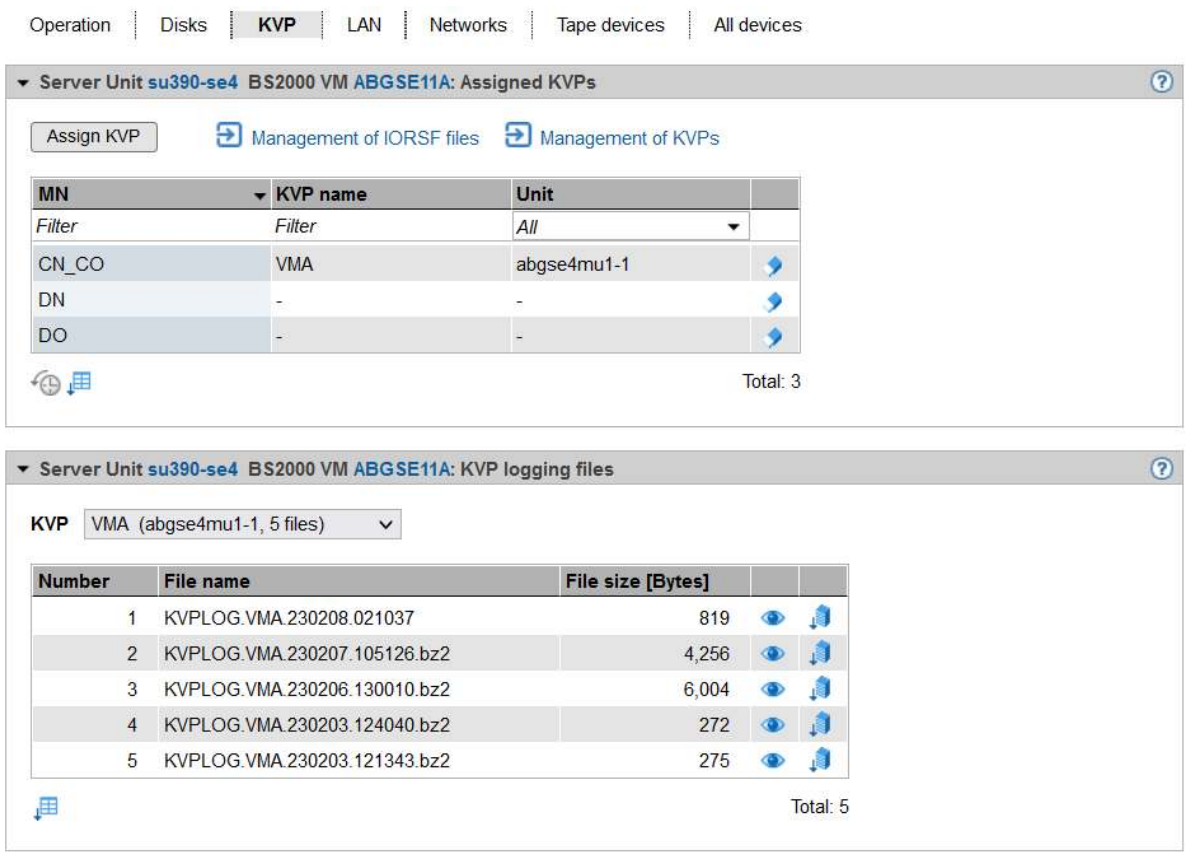
> Click the *Remove* icon by a disk to remove this disk from the VM.

For further information on displaying BS2000 disks, see section "Displaying generated disks on Server Unit /390" and section "Managing disks on Server Unit x86" .

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.



> The link to IORSF file management 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"

Displaying KVP logging file

> 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* window for the chosen logging file. You can restrict the time period of the logging records to be displayed and filter the output.

Downloading the KVP logging file

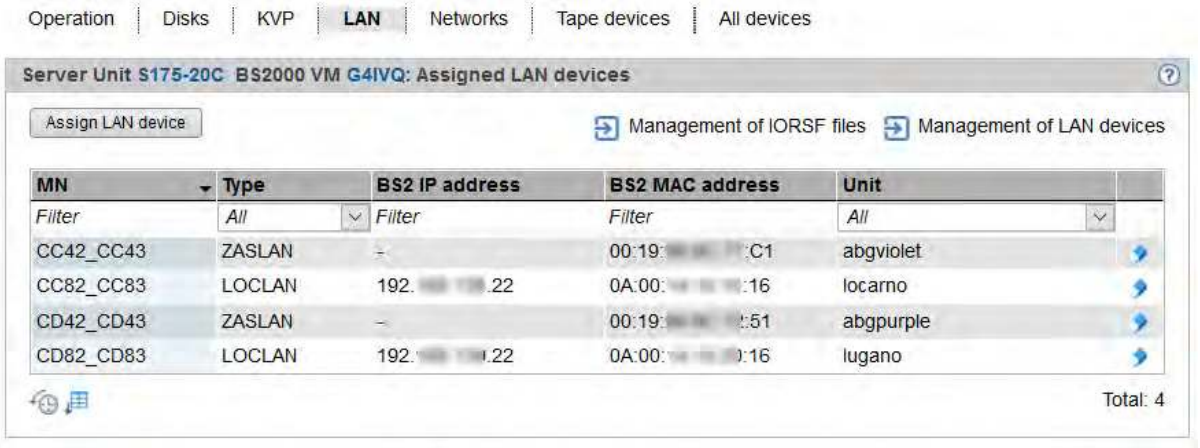
> In the *KVP logging files* group select the required KVP from the *KVP* list. Click the *Download* icon by the required KVP logging file, enter the path name and file name in the system-specific Explorer window, and save the file.

Further details on KVPs are contained in the section "Managing KVP devices".

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.



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

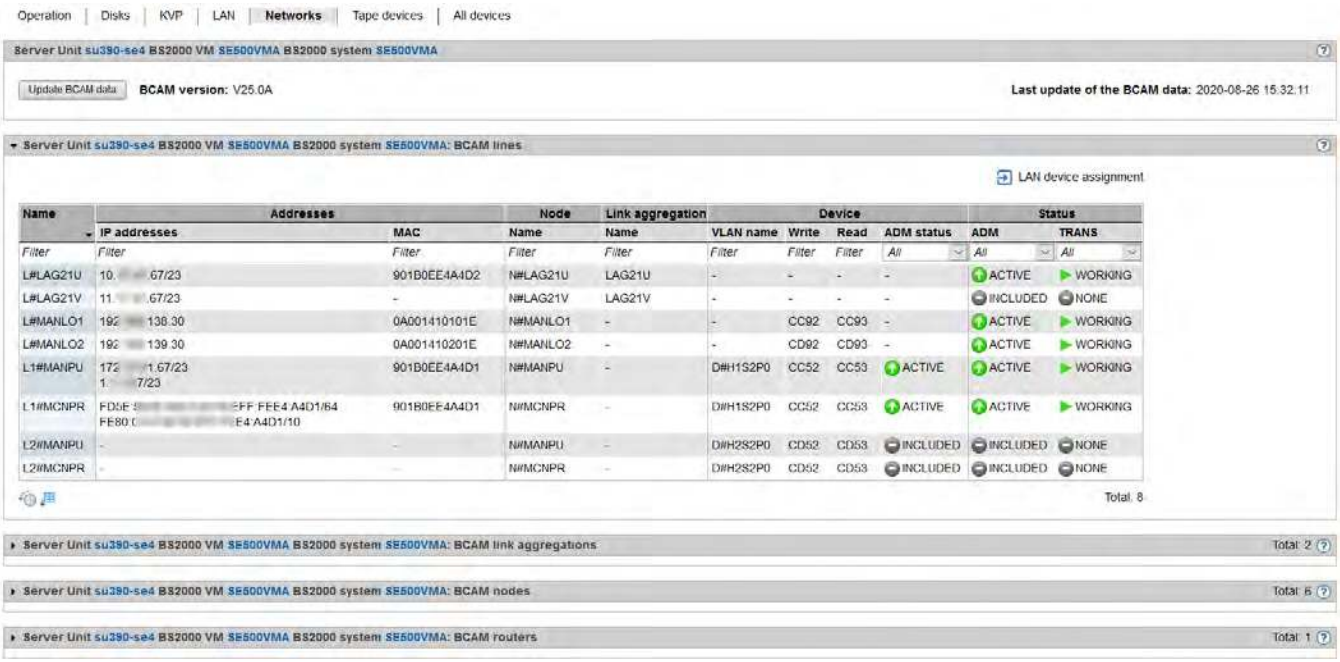
> Click *Assign LAN device* to assign another LAN device pair to the VM.

> 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".

Networks tab

This tab gives you an overview of the BS2000 VM's BCAM data and allows you to update the displayed BCAM data.



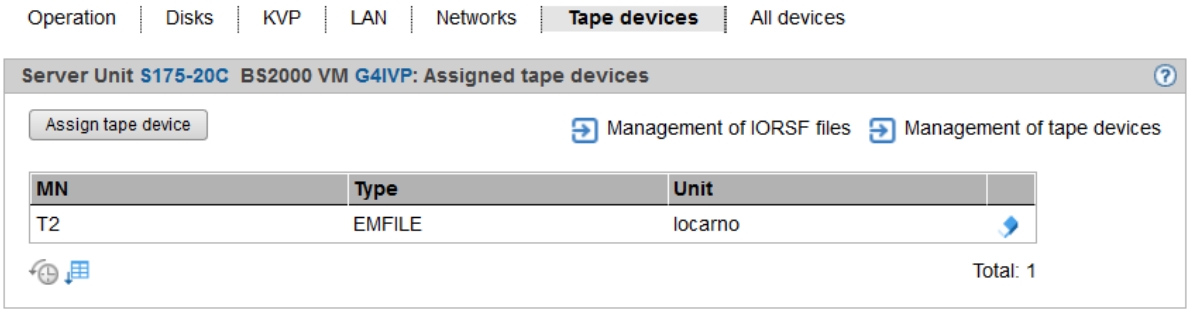
> The *Link aggregation* column of the *BCAM lines* table and the *BCAM link aggregations* group are displayed only if at least one link aggregation exists.

- Click *Update BCAM data* to retrieve the BCAM data again.

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.



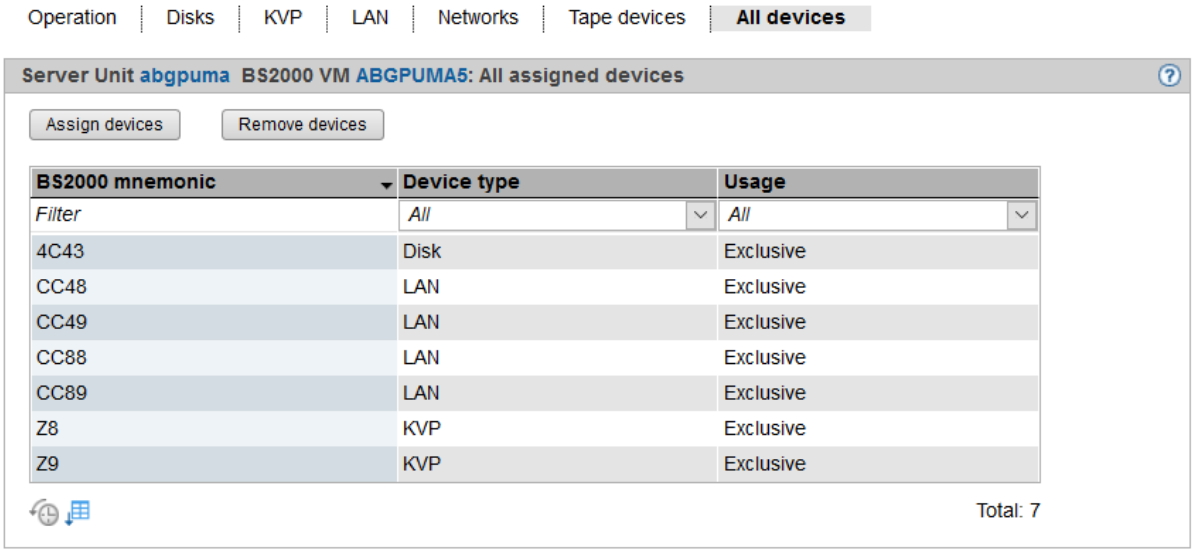
> The link to IORSF file management and the *Unit* column are displayed for SU /390 only.

- 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".

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.



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.

6 Operating and managing systems on Application Units

An operating system from another vendor (Windows, Linux or Unix systems) usually 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: VMware vSphere ESXi or HyperV Windows Server.

Application Units are displayed in the tree structure as *<unit> (AU...)* or *<unit> (DBU...)*.

For deployment scenarios with many Application Units, the standard view of the systems in the SE Manager can become confusing. For such cases, the AU optimized view, which can be selected in the user's individual settings, is suitable. In the navigation, the AU optimized view displays only one *System AU* menu in the *Systems* main menu for all AUs of an SE server, which provides access to the *Operation* main page of the AUs.

If the add-on pack NUX is installed on at least one MU, the structure of the primary navigation underneath *Hardware –> Units* is extended: The main menu receives rack-specific substructures *SE<se-index> AU<rack-index>xx* corresponding to the name scheme of the AUs, under which the links to the individual AUs of the rack (with a corresponding submenu if necessary) can be found.

> If an AU is only integrated at hardware level, its VMs are not enquired and are therefore not displayed. For such an AU, only the basic system resp. Native-AU system is displayed.

The following description is divided into these sections:

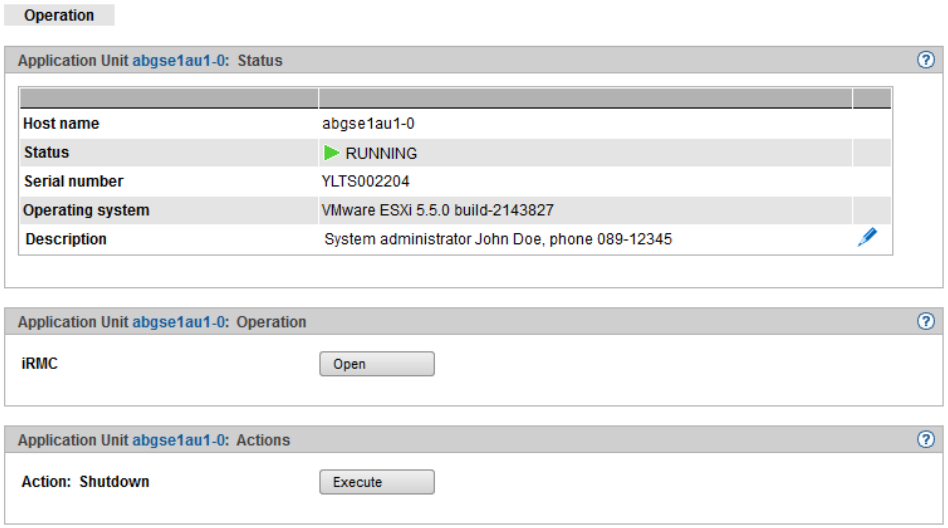
- Operating a Native system
- Operating virtual machines
- Installing an operating system on an Application Unit

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 VMware system).



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. AUQ38E or DBU38E).

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.

For AUs that are only embedded at hardware level, only the Native System is displayed, as follows:

- The SENET name is displayed as the host name (e.g. au1-se1).
- *NOT_MONITORED* is displayed as the status.
- There is no shutdown action available.

For more information, refer to the online help.
Please contact Customer Support for further details.

6.2 Operating virtual machines

When an AU is operated with a hypervisor system, VMs can be configured (via this hypervisor system).
As soon as a VM has been configured, the tree structure below *Systems* -> [*<se server>(SE<model>)* ->] *<unit> (AU<model>)* 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>)* 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 (VMware vSphere ESXi or HyperV Windows Server).

> Select *Systems* -> [*<se server> (SE<model>)* ->] *<unit> (AU<model>)*, *VM overview* tab.
>
> On AU PQ select *Systems* -> [*<se server> (SE<model>)* ->] *<unit> (<AU PQ model>)* -> *<unit> (<partition>)*, *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. start the VM).

> In the tree structure select *Systems* -> [*<se server> (SE<model>)* ->] *<unit> (AU<model>)* -> *<VM-name>*.
>
> On AU PQ select *Systems* -> [*<se server> (SE<model>)* ->] *<unit> (<AU PQ model>)* -> *<unit> (<partition>)* -> *<VM-name>*.
>
> The *Operation* tab opens and in the *Status* group displays the properties and current status of the VM.
>
> For the hypervisor VMware vSphere ESXi, the *Operation* group is also displayed provided the associated hypervisor is active and can be reached by the Management Unit. That means a VM with vCenter Server must be running on the Application Unit.

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

> Click *Open* for VMware vSphere Web Client in the *Operation* group.
> The VM Manager opens in a new window. After logging in successfully, you obtain access there to manage the VMware hosts/systems.
>
> Additionally, the group also offers the *Open* action for VMware Host Client.

> 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 with the hypervisor 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 S<n> - integrated Remote Management Controller” manual [16].

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 hardwarespecific 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").

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 [17] and [18].

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.

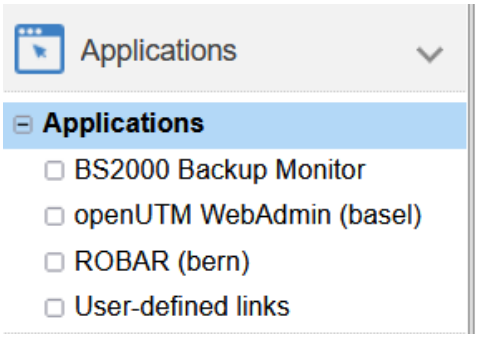
You configure the management network using Linux resources with the appropriate IP addresses, subnetwork masks, and gateways.

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.

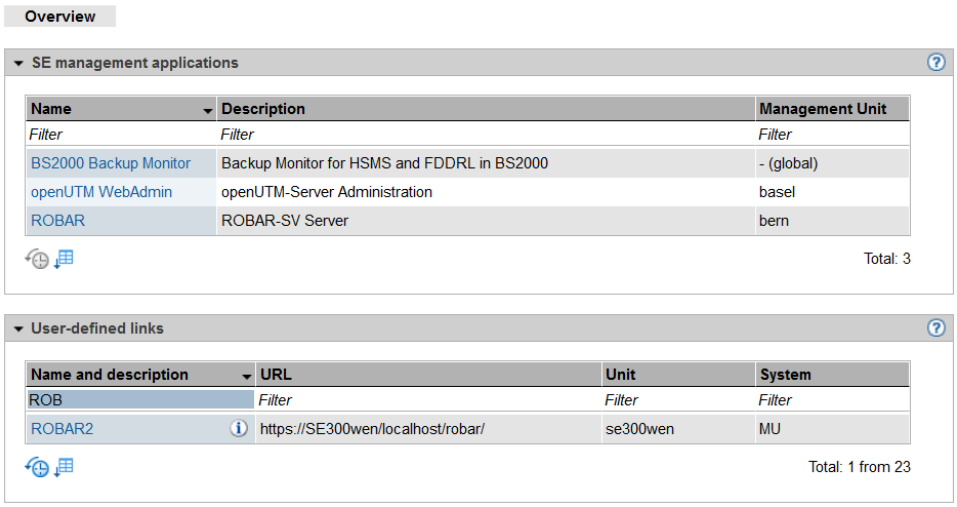
7 Managing applications

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.



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

- SE management applications are fully integrated into the SE Manager.
- 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 under "Management applications" in section "Add-on packs".

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").

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

- openUTM WebAdmin (see "openUTM WebAdmin")
- ROBAR (see "ROBAR")
- openSM2 (see chapter "Monitoring performance")

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.

ROBAR and openSM2 are chargeable products, each with its own online help, which are realized as add-on packs. openUTM WebAdmin also is a product with its own online help and realized as add-on pack, but it is not chargeable. The basic product openUTM, however, is chargeable.

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.

In the *Overview* tab you can retrieve requests (via the *Get requests* button above the table or for a specific syste the  icon) as well as delete requests.

> The *Requests* tab provides you with detailed information on the various requests and, when necessary, enables 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".

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 *Home* tab displays the homepage of openUTM WebAdmin.

The menus of openUTM WebAdmin are displayed in the tree structure.

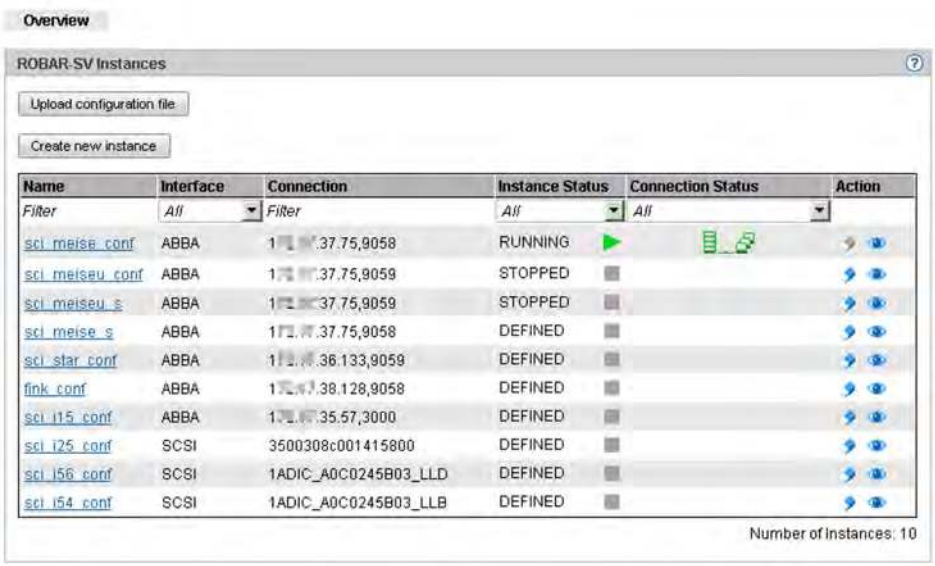
> Clicking *SE Manager* in the tree structure returns you to the SE Manager.

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.



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.

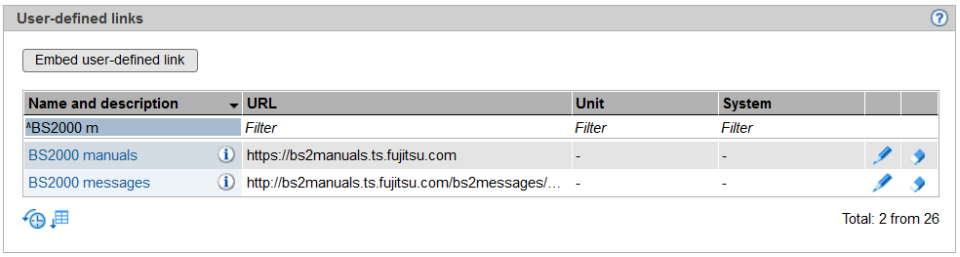
The menus of the ROBAR-SV instances and of the ROBAR-SV management are displayed in the tree structure.

> Clicking *SE Manager* in the tree structure returns you to the SE Manager.

7.2 Administering user-defined links

> Select *Applications -> User-defined links, 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.



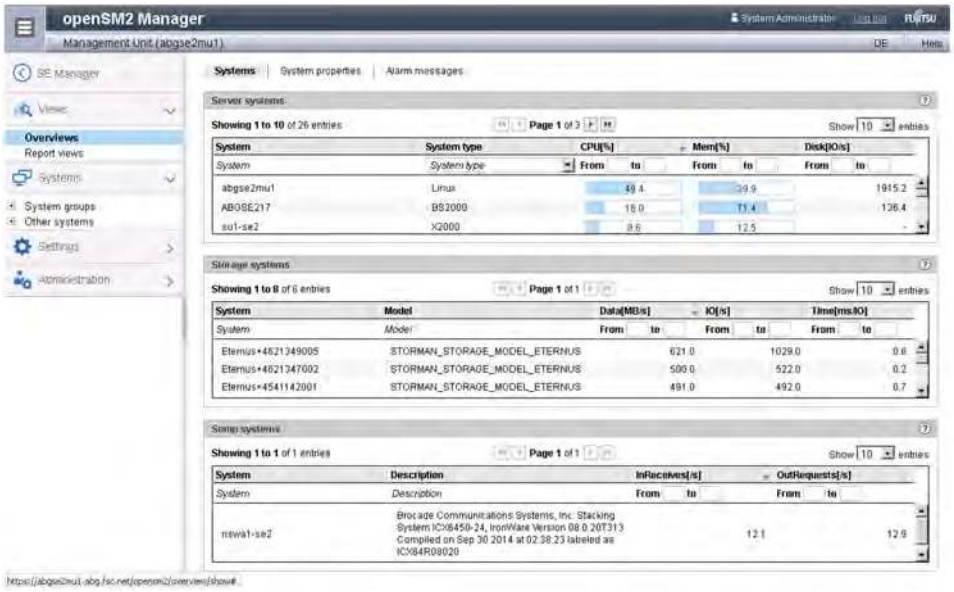
> The *Change* and *Remove* icons enable you to change application properties (e.g. a URL) or remove the link to an application from the SE Manager.

> *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 Manager opens. The layout is the same as the layout of the SE Manager.



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.

If you manage an SE server configuration with two or more 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.

For an SU x86 you manage BS2000 devices via the SU itself. 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.

Emergency system

A new SE server is prepared by the manufacturer so that it is ready for use by the customer. The Server Units are delivered with a pregenerated and preinstalled emergency system. The emergency system is IPL-capable. It is intended for installation and maintenance only, should not be used for everyday operation, and should not be newly installed by the customer. The pubset with the emergency system can be kept as a stand-by pubset or for diagnosis. You can find more information in the "System Installation (SE Server)" [9] user guide.

The description is divided into the following sections:

9.1 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 output sometimes also abbreviated with MNEM).

Example

On the BS2000 console an emulated tape drive with the mnemonic AF is addressed in the /SHOW-DEVICE-STATUS and /ATTACH-DEVICE commands:

```
/SHOW-DEVICE-STATUS AF
%  MNEM DEV-TYPE CONF-STATE POOL VSN   DEV-A    PHASE    ACTION
%  AF   BM1662FS DETACHED    SW         FREE           NO ACTION
/ATTACH-DEVICE AF
% MSG-000.165608  %  NKR0042 'DEVICE     =AF': ATTACH ACCEPTED
%XAAE-000.165608  %  NKR0116 ASSIGN FOR 'DEVICE=AF' IN PROCESS
% MSG-000.165608  %  NKR0110 'DEVICE     =AF' ATTACHED AND ASSIGNED
! UCO-000.165608  %  NBR0740 COMMAND COMPLETED 'ATTACH-DEVICE'; (RESULT:
SC2=000, SC1=000, MC=CMD0001); DATE: 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 DETACHED status (CONF-STATE); 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.

BS2000	**Device address X2000 / M2000**	**Device address SU /390 (IORSF)**	**Device address 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 (SE Server)” manual [9].

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.

9.2 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.

FC-SCSI channels have a Channel Path ID (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.

- Predefined BS2000 devices
- Device connection via Management Unit and HNC
- Configuration in IORSF files

9.2.1 Predefined BS2000 devices

The following BS2000 devices are predefined for the SU /390:

Type	MN	HC	LUN	Details
EMDISC	CCF0, CCF1	00	30, 31	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
In the case of MU redundancy on MU2 (MU index 2):				
EMDISC	CDF0, CDF1	00	30, 31	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 5: Predefined BS2000 devices on SU /390 (MU)

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

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

Table 6: 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.

9.2.2 Device connection via Management Unit and HNC

You manage the devices of an SU /390 via the Management Unit. The devices are emulated on the MU or, in the case of LAN devices, alternatively on the HNC. When adding a device, the first step is to specify the MU or HNC where the device will be emulated. LAN devices of type ZASLAN or LOCLAN can be emulated on an HNC, only those of type LOCLAN can be emulated on an MU.

You can manage (add, change, remove) KVP devices, LAN devices and emulated tape devices via the Management Unit. Disks and real tape devices are only displayed.

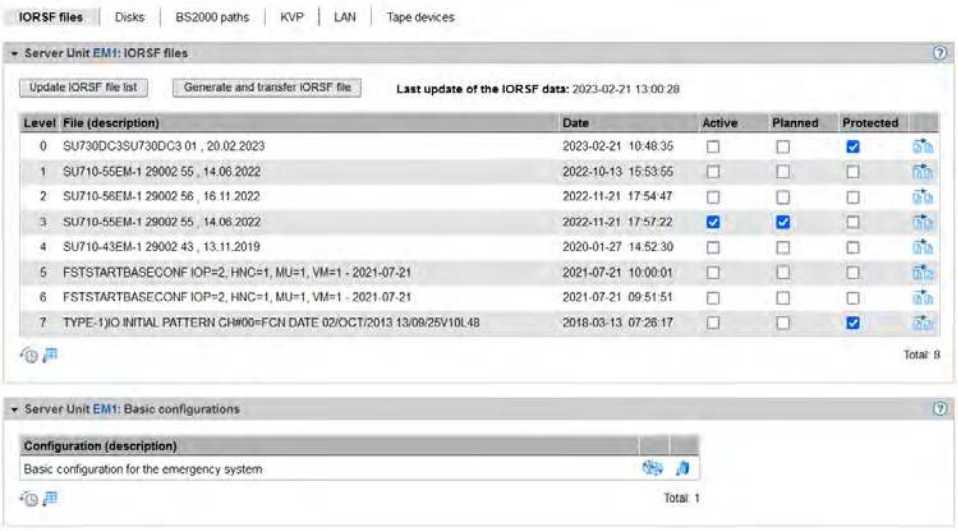
Details are provided in the sections below:

- Managing KVP devices
- Managing LAN devices
- Managing tape devices

9.2.3 Configuration in IORSF files

Creating the current device lists for SU /390

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



The *IORSF files* tab provides information about the IORSF files which are available on the SU /390.

> 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 of the Server Unit 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.

Creating an I/O configuration for SU /390

In SEM, actions are available with which IO configurations (IORSF files) can be created and transferred to the SVP:

- Generate and transfer IORSF file
- Generate and transfer the basic configuration

The actions are executed on the MU and do not require an active BS2000.
The generated configurations and log files are no longer accessible after the respective action has been completed.
The actions must be repeated completely if they fail or are not completed.

> Click button *Generate and transfer IORSF file* in group *IORSF files*

The individual steps for generating and transferring the IORSF file on the SEM are as follows:

- Upload the file(s) with the IOGEN instructions from the PC to the MU;
  then select the start file and the configuration, if necessary.
- Generating an IORSF file (on the MU)
  It is possible to download the log file to the MU. The generated log file contains the data of the IOGEN and IOCGEN runs in the form as they are created in BS2000 with the option PROT=*SPOOL in the SYSLST file. (The IOGEN and IOCGEN protocols are not separated.)
- Transferring the IORSF file to a selected SVP level

> Click *Generate and transfer basic configuration* () icon in the *Basic configurations* group

Without existing IOGEN instructions the generation and transfer to the SVP of a basic I/O configuration is possible.
The basic configuration can be used for an initial installation or as an emergency system.
The basic configuration includes the following devices:

- Via the channel with CHPID 40 at the MU (first MU):
  - EMDISKS CCF0, CCF1
  - KVP main consoles C2, C3
  - LOCLAN connection (dialog) CC80, CC81
  - CDROM T0
  - EMFILE T1
- Via the channel with CHPID 08 on the HNC (first HNC):
  - ZASLAN (Data LAN) CC00, CC01
  - ZASLAN (Control LAN for REWAS) CC40, CC41

The corresponding IOGEN instructions can be downloaded in a file to the PC for further use.
The name in the basic configuration is "FSTSTART".

Creating an IOGEN source

From an existing IORSF file, the corresponding IOGEN source can also be created again in the SE Manager.

> Click the *Create IOGEN source* () icon by the desired IORSF file

This invokes a wizard that calls IOGEN, displays the IOGEN job messages, and offers to download the generated IOGEN source.

Details on the I/O configuration and the IOGEN utility can be found in the manual "System Installation (SE Server)" [9].

9.3 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.

- Predefined BS2000 devices
- Connection of peripheral devices

9.3.1 Predefined BS2000 devices

The following BS2000 devices are predefined on SU x86:

Type	MN	HC	Unit ID	Details
EMDISC	D0	00	30	Emulated disk; generated as standby pubset with the emergency system
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 7: Predefined BS2000 devices on SU x86

9.3.2 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.

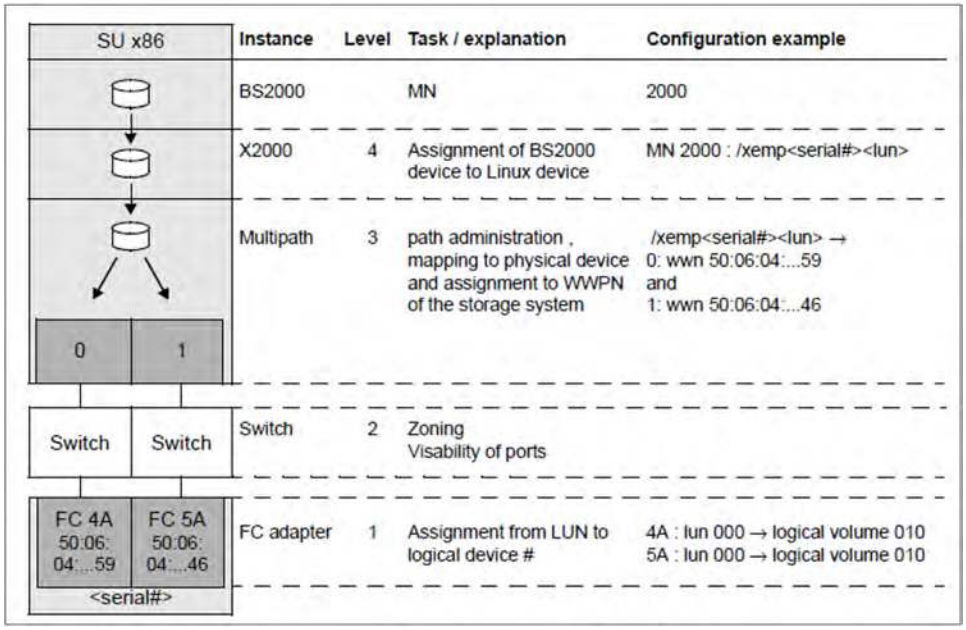


Figure 16: Device configuration on an SU x86 taking a disk storage system as an example

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.

9.4 Managing disks

Disks of the type A5 (D3435) or A6 (D3435-FP, for SU /390 only) are connected to an SE server. The disks are connected either internally (within the SE server) or externally (in other storage systems or cabinets).

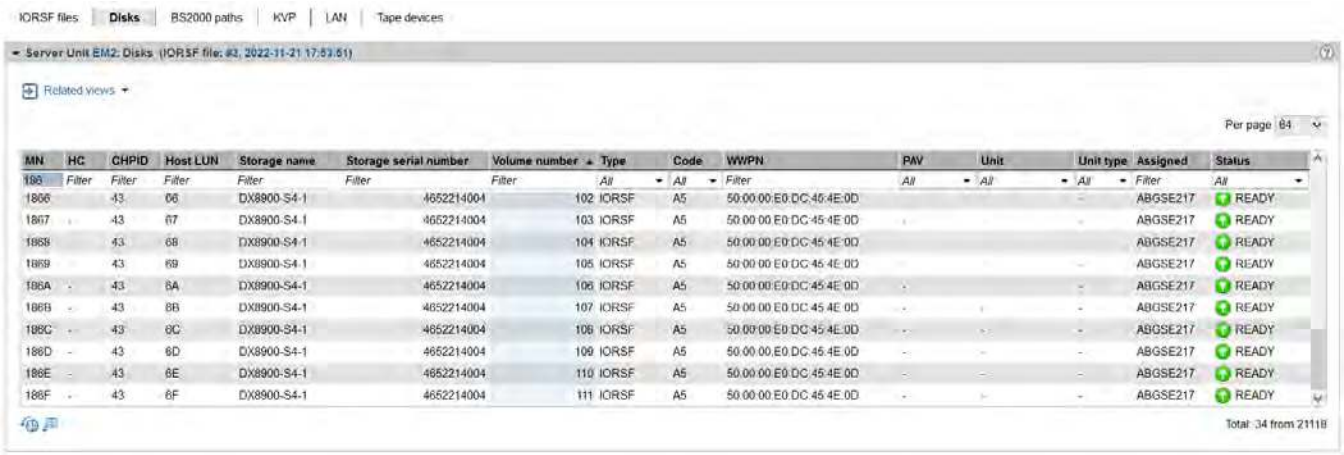
For the Server Units, the *Disks* tab offers the following functionality for managing disks. Functions above and beyond the displaying of disks are only available for the Server Unit x86.

- Displaying generated disks on Server Unit /390
- Managing disks on Server Unit x86

9.4.1 Displaying generated disks on Server Unit /390

> The devices are displayed completely only if the data of the active IORSF file are available at the MU. If necessary, execute action *Update IORSF file list* on tab *IORSF files* for this purpose.

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



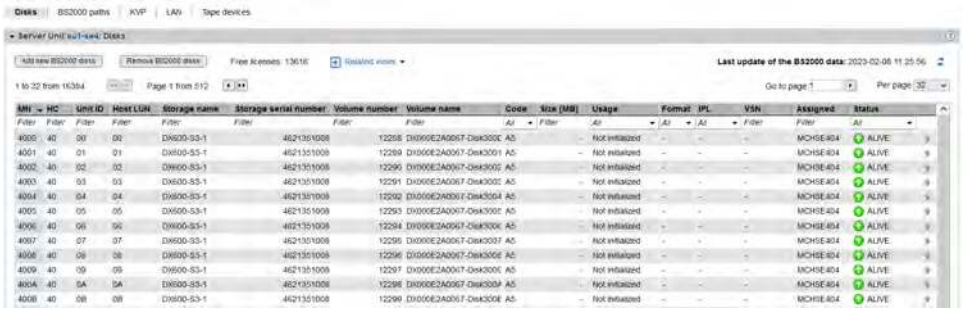
The *Disks* tab provides information about the BS2000 disks which are configured in the active IORSF file.

> In VM2000 mode the table contains an additional column: if a device assignment exists, the column *Assigned* displays the VM name.
>
> The columns *Host LUN, Storage name, Storage serial number, Volume number, Volume name* and *Status* are supplied only, if STORMAN is properly configured and the storage data is updated. For this, the *Update storage data* dialog in the *Hardware -> Storage* menu must be called.

9.4.2 Managing disks on Server Unit x86

Displaying disks

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



The *Disks* tab displays the configured BS2000 disks.

Above the table the number of free licenses is displayed.

> Only in VM2000 mode the table contains the column *Assigned* (see the picture): if a device assignment exists, this column displays the VM name.
>
> The columns *Host LUN, Storage name, Storage serial number, Volume number, Volume name* and *Status* are supplied only, if STORMAN is properly configured and the storage data is updated. For this, the *Update storage data* dialog in the *Hardware -> Storage* menu must be called.

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* (see below).

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.

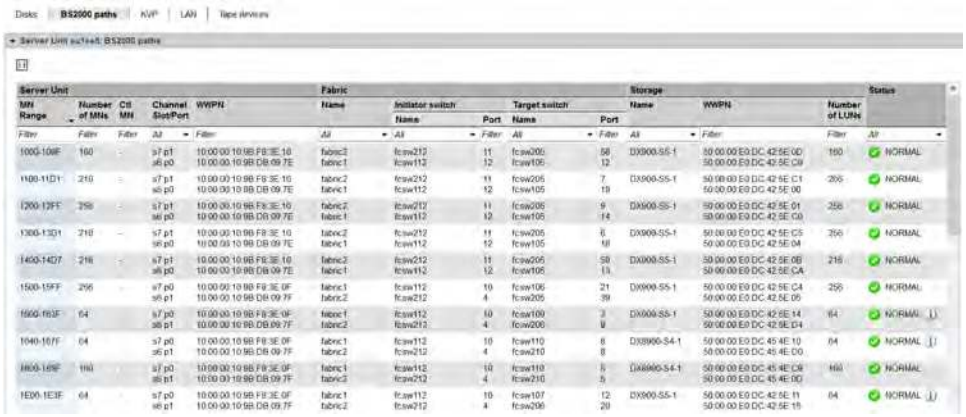
> By the required disk, click the *Remove* icon and confirm the action.

9.5 BS2000 paths

In the *BS2000 paths* tab the configured paths between server and storage are shown.

The prerequisite for this is that the FC network data and in addition also the storage systems in StorMan are configured correctly. If necessary, these must first be updated. Information on updating the FC network configuration can be found under Configuring settings (Administration and Operation, #213).

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



The *BS2000 paths* tab opens. A table displays the entries grouped according to the MN range. The icon resp. above the table makes it possible to switch between the default view and an alternative view of the columns.

9.6 Managing KVP devices

A KVP (console distribution program) with the name *HV0* is preconfigured on the MU and SU x86 (see table 5 and table 7). You can delete the existing KVP and then define a new one with different values.

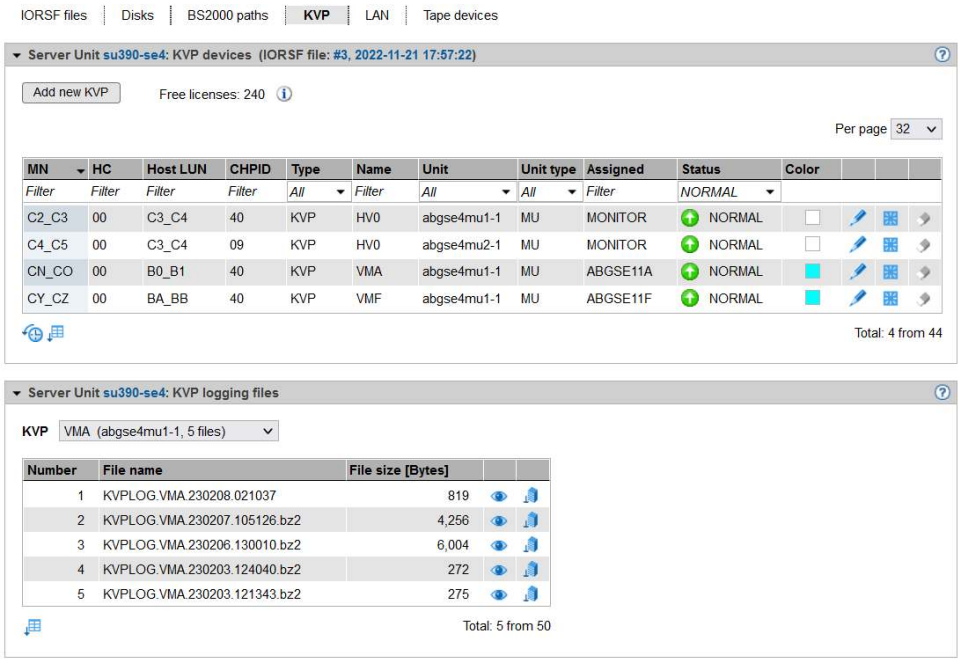
BS2000 sees a KVP as two (emulated) KVP devices (or a device pair) which are identified by their mnemonic names.

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".

> **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>)*, *KVP* tab.



The *KVP* tab with the *KVP devices* and *KVP logging files* groups opens. When expanded, the groups display a table containing the current KVPs and the logging files of the selected KVP.

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 completely only if the data of the active IORSF file are available at the MU. If necessary, execute action *Update IORSF file list* on tab *IORSF files* for this purpose.

- 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 name.

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

> 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* window for the chosen logging file. You can restrict the time period of the logging records to be displayed and filter the output.
>
> 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.

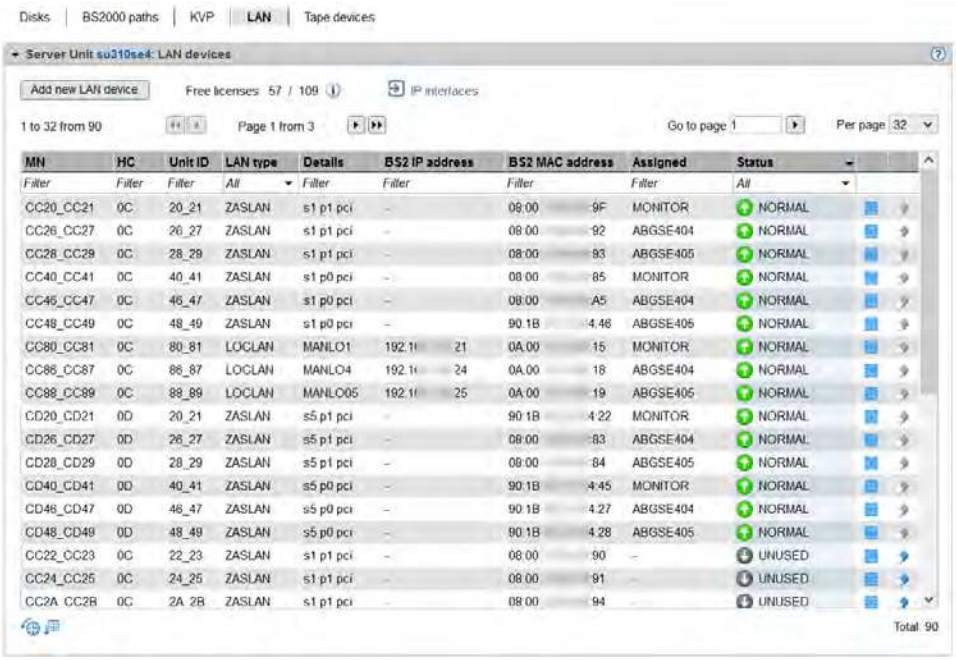
9.7 Managing LAN devices

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 and LOCLAN.

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>)*, *LAN* tab.



The *LAN* tab lists the configured LAN devices.

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

> **i** In VM2000 mode the table contains an additional column: if a device assignment exists, the *Assigned* column displays the VM name.

> *Information on the generated LAN devices on SU /390*
>
> The devices are displayed completely only if the data of the active IORSF file are available at the MU. If necessary, execute action *Update IORSF file list* on tab *IORSF files* for this purpose.
>
> - 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).

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

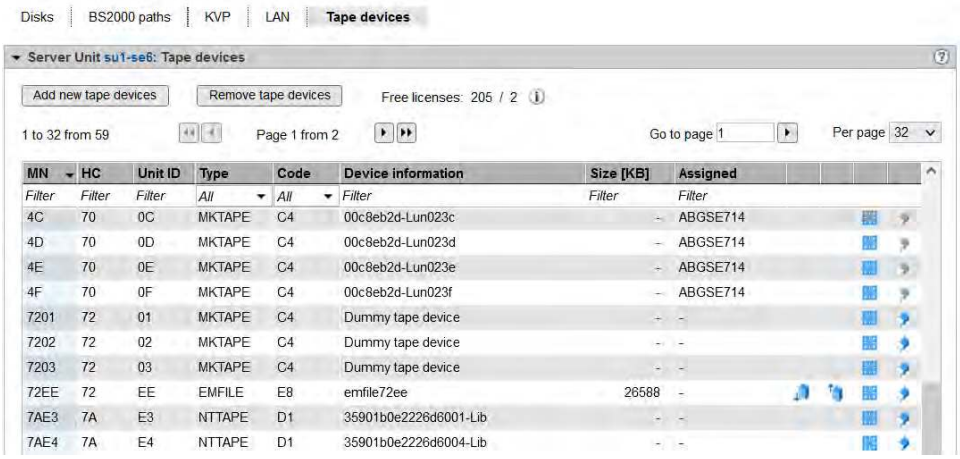
> Click the *Remove* icon by the required LAN device and confirm the action.

9.8 Managing tape devices

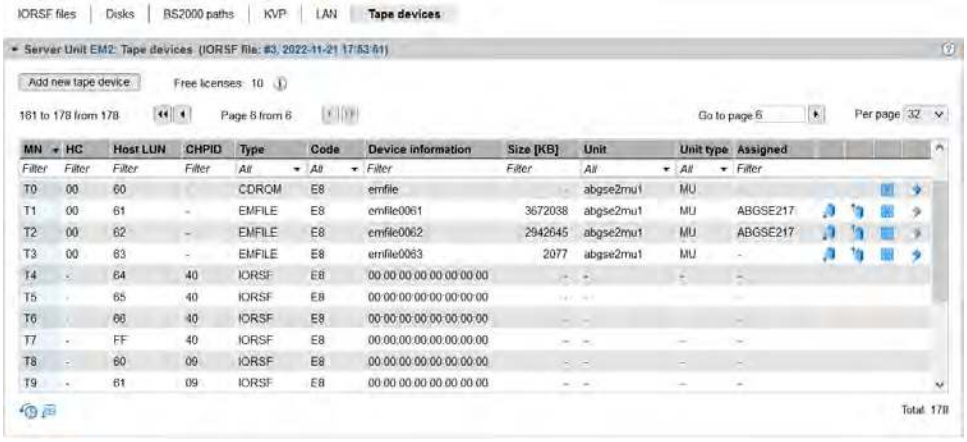
The *Tape devices* tab provides the following functions:

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

Example for SU x86:



Example for SU /390:



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 icon, a tool tip displays detailed license information.

> **i** In VM2000 mode the table contains an additional column: if a device assignment exists, the *Assigned* column displays the VM name.

> *Information on the generated tape devices on SU /390*
>
> The devices are displayed completely only if the data of the active IORSF file are available at the MU. If necessary, execute action *Update IORSF file list* on tab *IORSF files* for this purpose.
>
> - 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).

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 or dummy tape devices of an SU x86, you can also enter the required number of tape devices.

Remove tape devices (SU x86 only)

> Click *Remove tape devices*.
>
> In the *Remove tape devices* wizard you can specify an interval of MNs for the real and dummy 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.

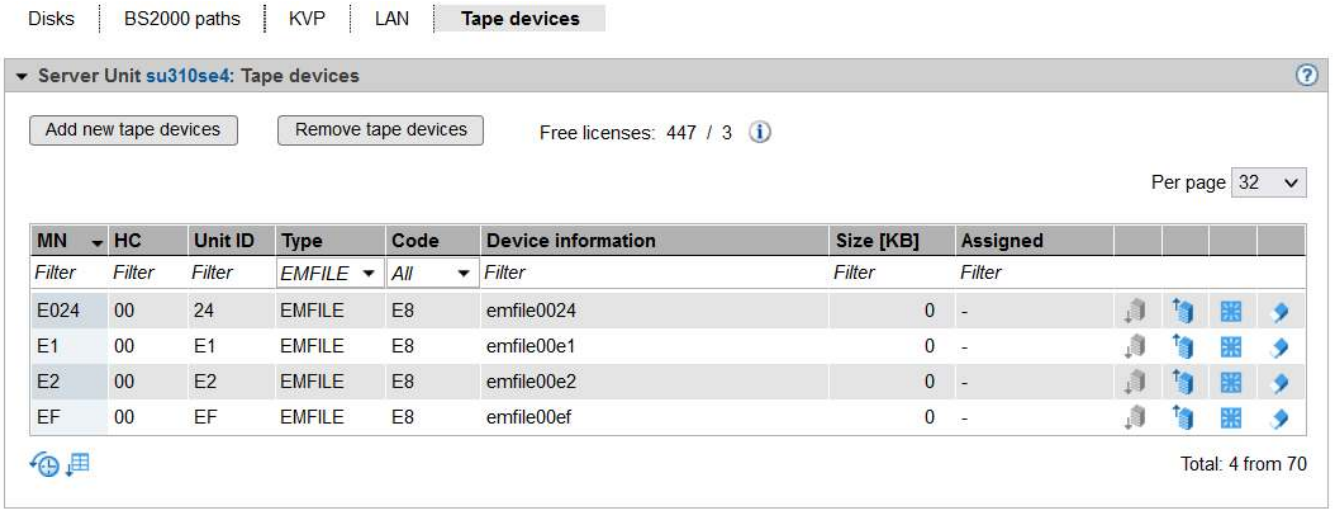
9.8.1 Emulated tape devices

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 manage emulated tape devices using the *Tape devices* tab of the SU /390 or SU x86, see the example below for an SU x86:



> 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.

9.8.2 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

> Initialize the CDROM file with the INIT utility routine and assign a VSN.
All data on a rewritable medium will be deleted.

> 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
- CD-RW (minimum speed 4x)
- DVD-R / DVD+R
- DVD-RW / DVD+RW
- DVDRAM

The end-of-tape processing depends on the size of the medium. The maximum net size of the CDROM file is 4200 MB and is correspondingly lower in the case of a smaller medium since the space for the table of contents and lead-in / lead-out is deducted (CD: up to 32 MB / DVD: up to 128 MB).

Times of different CD/DVD media

The burning times (or initialization times) depend on the medium used and the possible speed for burning/deleting. The table below provides some information for estimating roughly how long the procedure will take (tests with a few different media).

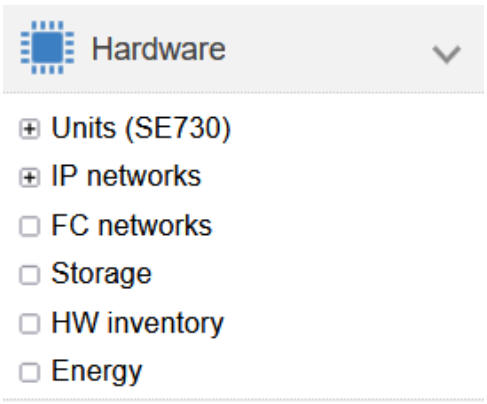
Medium	Time INIT	Time INIT ... ERASE	Time /UNLOAD-TAPE (burn)
DVD-R 8x	2 sec	-	11 min (4200 MB)
CD-R 52x	2 sec	-	7 min (650 MB)
CD-RW 4x-10x	130 sec	10 min	10 min (650 MB)

DVD+RW 1x-4x	30 sec	16 min	15 min (4200 MB)
DVDRAM 3x-20x	20 sec	40 min	37 min (4200 MB)

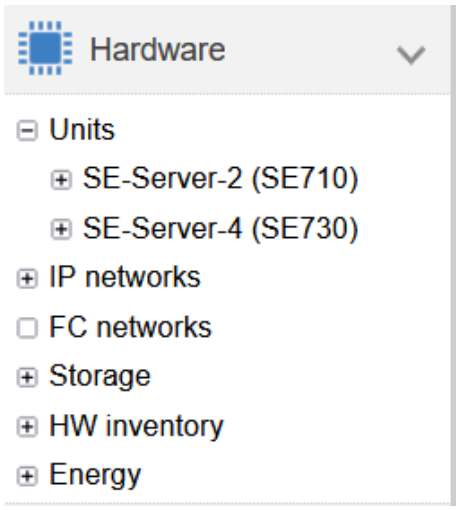
10 Managing hardware

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

Managing a single SE server
(with an SU /390)



Managing two SE servers
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".
- *IP networks*: Here you manage all private and public networks of the SE server configuration, see section "Managing IP networks".
- *FC networks*: Here you manage the Fibre Channel networks of the SE server configuration, see section "Managing FC networks".
- *Storage*: Here you manage the storage components of the SE server configuration, see section "Managing storage systems".
- *HW inventory*: Here you can have the hardware configuration displayed on the screen in graphic or tabular form, see section "HW inventory".
- *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".

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 or more SE servers in one Management Cluster, the units are listed underneath *Units* in SE server-specific submenus *Hardware -> Units -> <se server> (SE<model>)*.

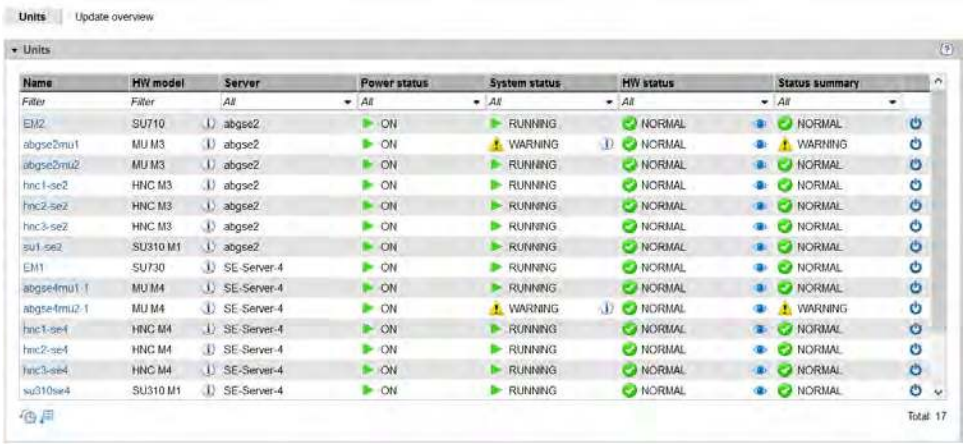
If the add-on pack NUX is installed on at least one MU, the structure of the primary navigation underneath *Hardware -> Units (SE<model>)* resp. *Hardware -> Units -> <se server> (SE<model>)* is extended: The main menu receives rack-specific substructures *SE<se-index> AU<rack-index>xx* corresponding to the name scheme of the AUs, under which the links to the individual AUs of the rack (with a corresponding submenu if necessary) can be found.

The description is divided into the following sections:

- Units - Information, powering on/off, etc.
- Overview of the software versions of the units
- Managing the SE servers of the Management Cluster
- Managing the Server Unit /390
  - Name, system information and interfaces of the SU /390
  - Displaying the IP configuration of the SU /390
- Managing the Management Unit
  - Displaying system information and interfaces of an MU
  - Managing the IP configuration
  - Managing routing of the Management Unit
  - Managing the DNS configuration
  - Managing SNMP
  - Setting the system time (time synchronization or local)
  - Entering CLI commands

10.1.1 Units - Information, powering on/off, etc.

> 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.



Notes:

- If at least one AU PQ is available, the column *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, as in the example, consisting of two or more 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.

Hardware details for unit

By clicking the *Hardware details* ( ) icon in the *HW status* column, you can view details about the status of the single hardware components of a unit.

Actions: Power on, reboot, shut down or power off immediately a unit

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 tool tip then informs about the reason.

> 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 tool tip 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 of the MU.

> 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 tool tip then informs about the reason.

> 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*.

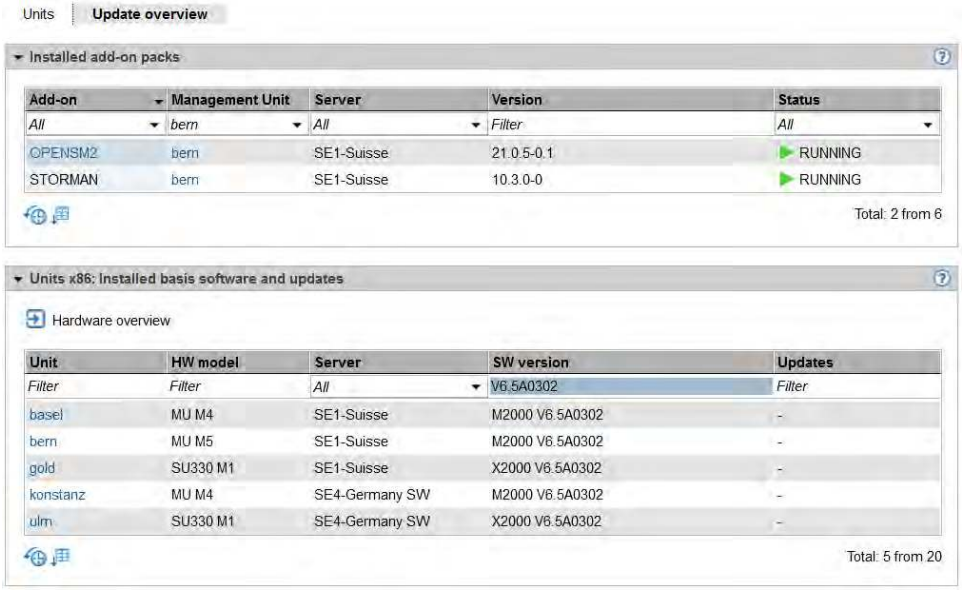
> ℹ Only *Power off immediately* is available for the SU /390.

The unit is shut down or powered off immediately. You will receive a message when the operation has been completed.

10.1.2 Overview of the software versions of the units

> Select *Hardware* -> *Units*, *Update overview* tab.

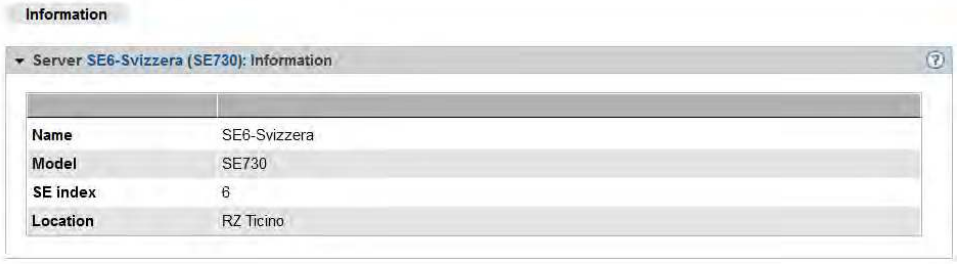
The *Update overview* tab displays information about add-on packs installed on Management Units of the SE server configuration in the first table and information about the basic software and updates installed on the x86-based units of the SE server configuration in the second table.
Links allow easy navigation to the individual add-ons, to the update windows of the individual units and to the units overview in the HW inventory.



10.1.3 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.



Customer Support configures the displayed data in consultation with the customer.

10.1.4 Managing the Server Unit /390

The administration of an SU /390 is described in the following sections:

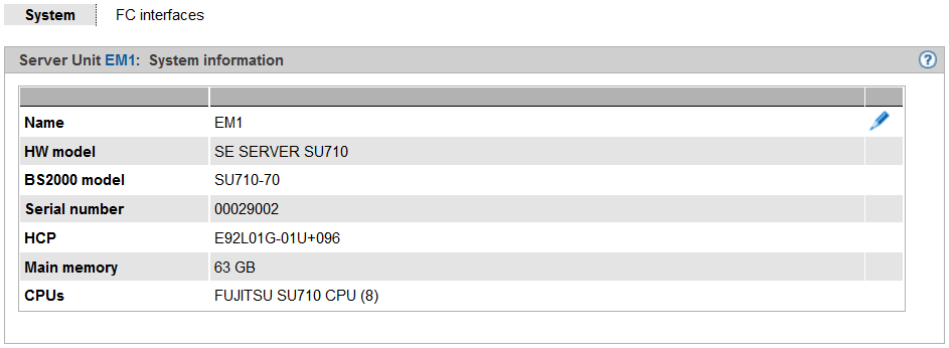
- Name, system information and interfaces of the SU /390
- Displaying the IP configuration of the SU /390

10.1.4.1 Name, system information and interfaces of the SU /390

You obtain the system information and interfaces of the SU /390 using the associated *Information* menu.
You may change the name of the SU /390.

Displaying system information of the SU /390

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



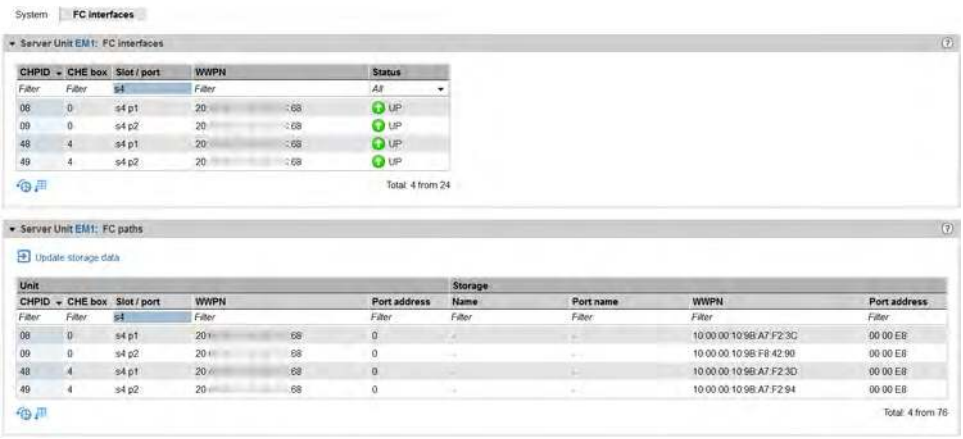
Changing the name of the SU /390

In the *System* tab for the SU /390 you may change the name of this SU.

> Click the *Change* icon in the line containing the name and enter the desired name in the dialog that opens.

Displaying FC interfaces of the SU /390

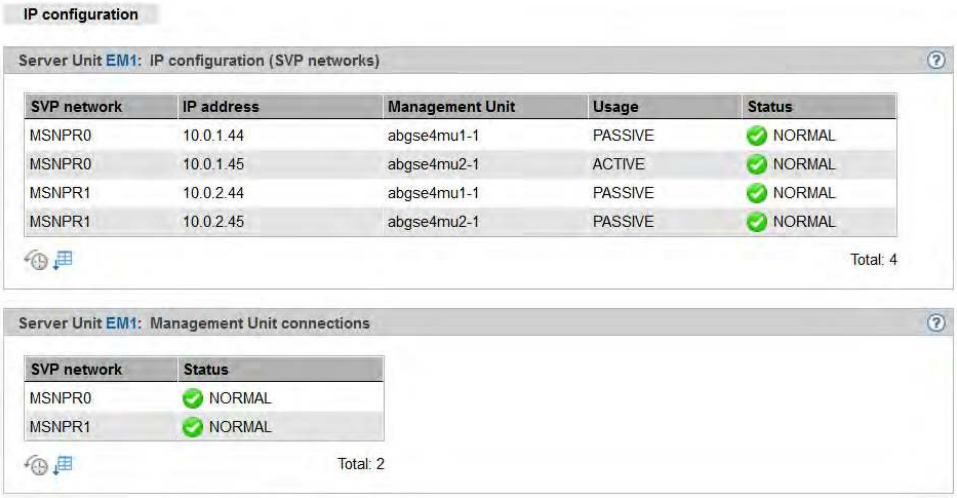
> Select *Hardware -> Units ->* [*<se server> (SE<model>) ->*] *<unit> (SU</390>) -> Information*, *FC interfaces* tab.



10.1.4.2 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.



10.1.5 Managing the Management Unit

The administration of a Management Unit is described in the following sections:

- Displaying system information and interfaces of an MU
- Managing the IP configuration
- Managing routing of the Management Unit
- Managing the DNS configuration
- Managing SNMP
- Setting the system time (time synchronization or local)
- Entering CLI commands

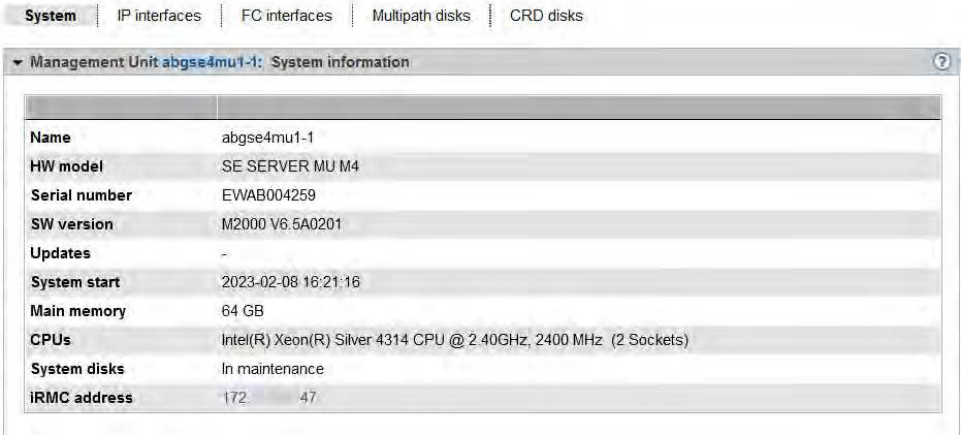
10.1.5.1 Displaying system information and interfaces of an MU

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 and resetting FC interfaces of the MU
- Displaying multipath disks of the MU
- Displaying CRD disks of the MU

Displaying system information of the MU

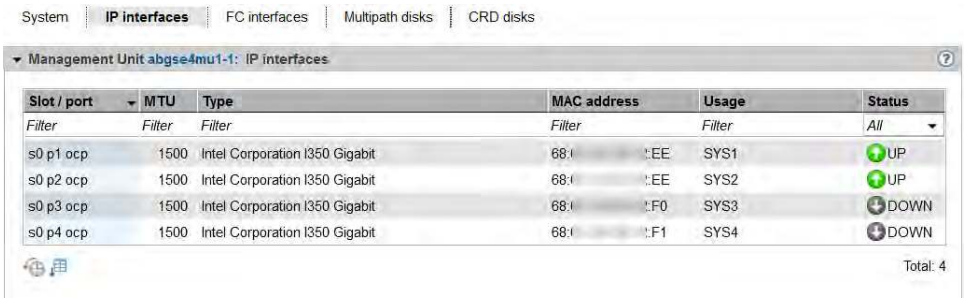
> Select *Hardware* -> *Units* -> [*<se server> (SE<model>)* ->] *<unit> (MU)* -> *Information*, *System* tab:



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:



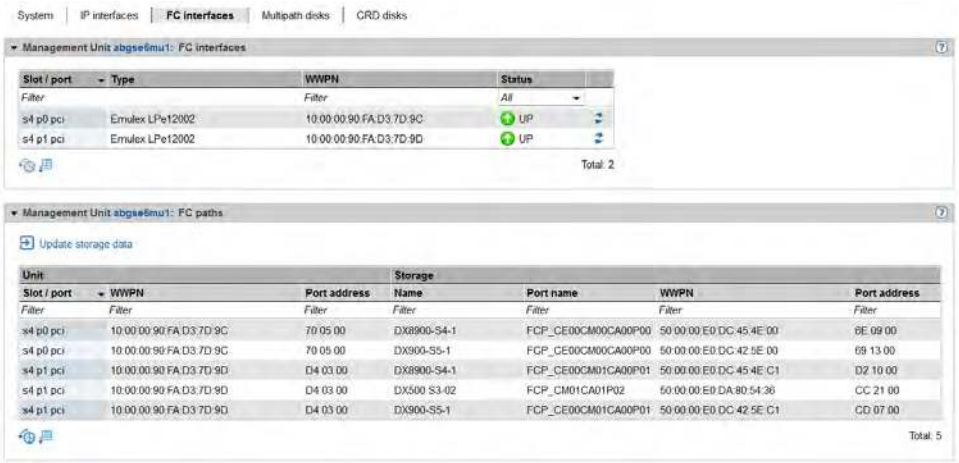
Changing the packet length in the case of LOCLAN and PCI interfaces

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 and resetting FC interfaces of the MU

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



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 (**Ch**annel **P**ath **ID -** CHPID). The hardware status of the FC interface is also displayed (*UP* / *DOWN*). For MUs without SKP functionality the columns *HC* and *CHPID* are not displayed.
- *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.

Resetting the FC interface

On the *FC interfaces* tab of the management unit, you can reset the individual single FC interfaces. The devices connected to the FC interface are rescanned. After this action, the displayed number of connected devices to this interface can change.

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. The columns *Name* and *Serial number* of the storage system are supplied only, if STORMAN is properly configured and the storage data is updated. For this, the *Update storage data* dialog in the *Hardware -> Storage* menu must be called.

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

Displaying CRD disks of the MU

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

Purpose and operation of CRD disks are described in section "External CRD disks".

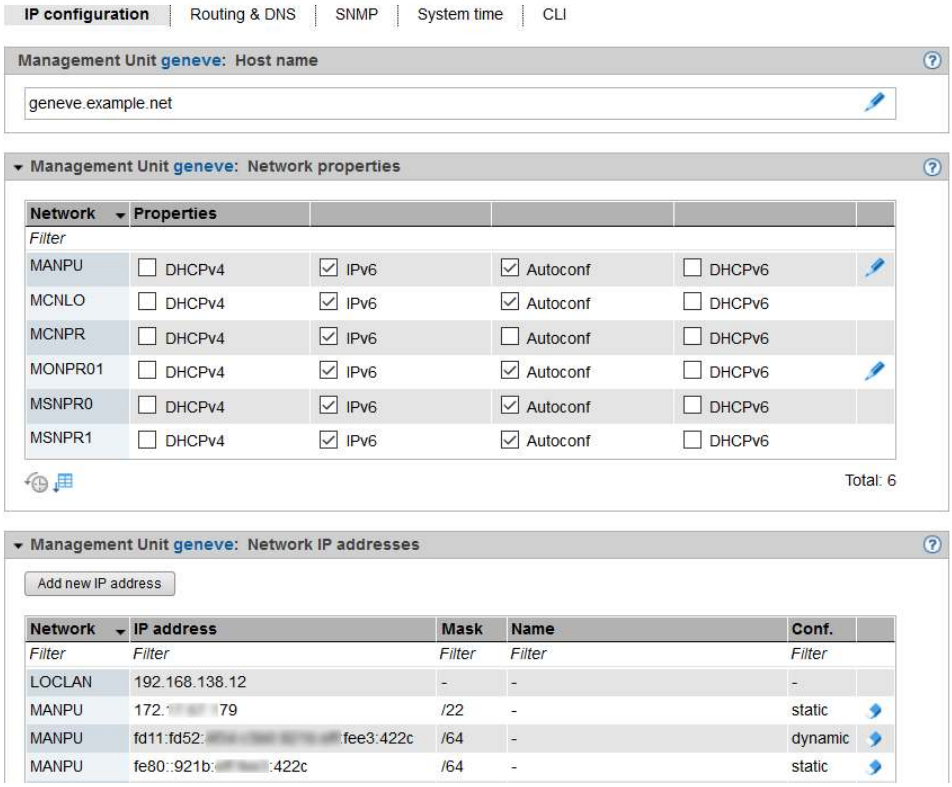
> Select *Hardware* -> *Units* -> [*<se server> (SE<model>)* ->] *<unit> (MU)* -> *Information*, *CRD disks* tab:

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

10.1.5.2 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.



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.

Adding a 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.

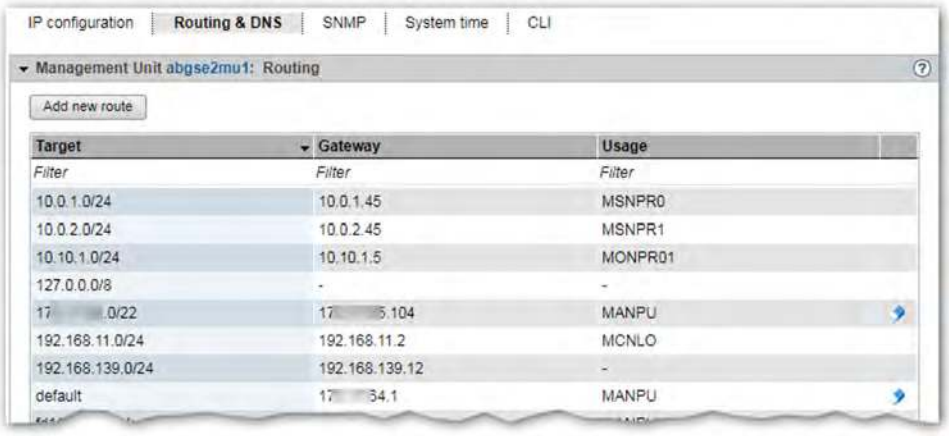
Deleting the IP address

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

10.1.5.3 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.



You use the *Routing & DNS* tab with the *Routing*, *DNS name servers* and *DNS domains* 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.

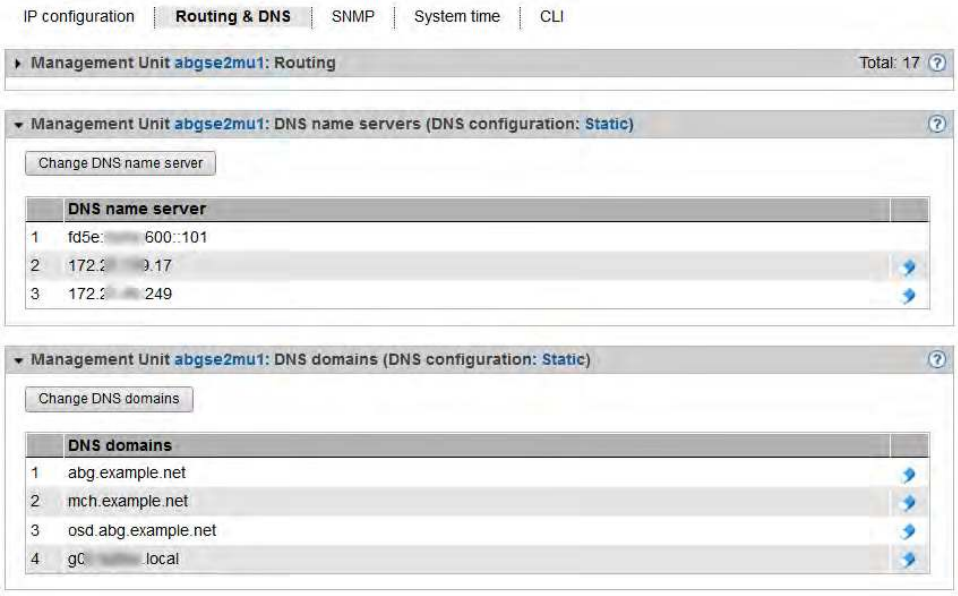
Deleting a route on MU (only for MANPU or MONPU networks)

> In the *Routing* group click the *Delete* icon by the required route and confirm the action.

10.1.5.4 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 DNS configuration is displayed in the two groups *DNS name servers* and *DNS domains*. The title bar of the group shows whether DNS is configured and whether static or dynamic DNS configuration is involved. 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 servers*, 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::<nnn>). This entry cannot be removed.

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

- In the *DNS domains* 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.

10.1.5.5 Managing SNMP

SNMP integration of the SE Server

SNMP (Simple Network Management Protocol) is a communication protocol for network, system and application management and enables the SE server to be monitored over a LAN. From a management station (customer's own computer), a system monitoring application can communicate with the SNMP agent present on the MU.

You administer central SNMP integration of the SE server using the SE Manager on the Management Unit. In the case of an SE server configuration with several MUs, redundant SNMP integration is recommended: The MUs must be integrated independently of each other in order to be used for SNMP monitoring, with the same functionality for the same SNMP integration.
The preconfiguration on MU, HNC and SU x86 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).
On AUs, on the other hand, you have to configure SNMP by yourself. The online help of SEM contains instructions.

The following monitoring functions are possible:

- Queries
  - Queries regarding the Server Unit /390 are possible at the MU (see the MIBs provided for this purpose).
  - Queries regarding the individual BS2000 systems and the applications running there are possible (see BS2000's own MIBs and the measures and prerequisites required for SNMP communication in the corresponding BS2000 documentation).
  - Management stations cannot address the SNMP agent on the SU x86 or HNC directly, but only via the MU. The SNMP agent on MU, HNC and SU x86 supports MIB-II and private MIBs for queries.
  - The host name of the system or the SENET name of the unit must be used for the query - see the examples below.
- Traps
  - 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 traps generated by applications in the individual BS2000 systems are also forwarded via the MU to the external management stations.
  - The sender of the trap is always the Management Unit.
  - In the case of two MUs (integrated in SNMP) in an SE server, traps are sent twice.

MIB files (MIBs) must be used to read and interpret the output.
The traps usually contain neither the trap weight nor the message text. This information can only be read from the MIB.

Therefore at least the following MIBs should be imported at the management station:

- `/usr/share/snmp/mibs/FUJITSU-SESERVER-MIB.txt`
- `/usr/share/snmp/mibs/FUJITSU-SU390-MIB.txt`

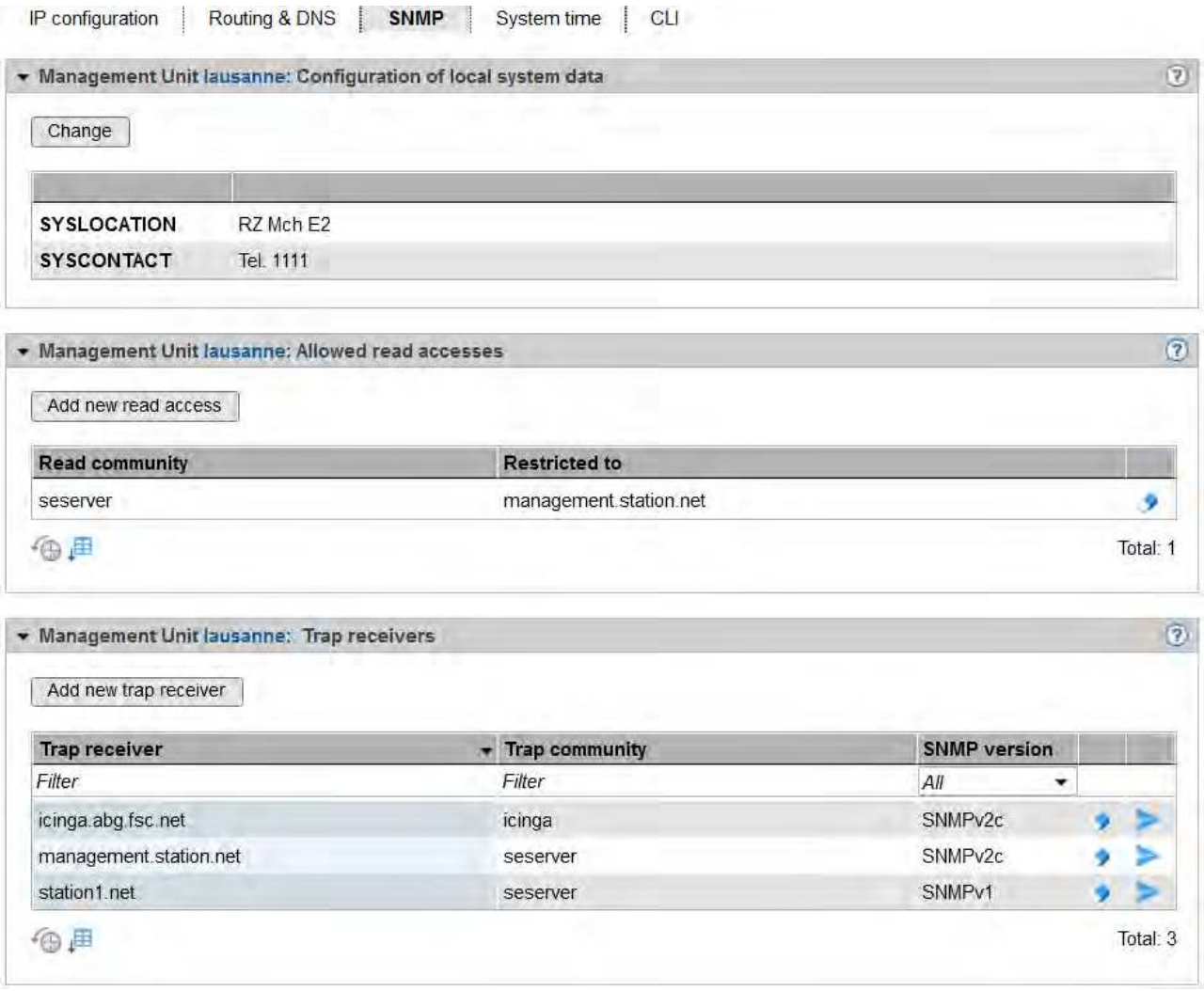
- `/usr/share/snmp/mibs/FSC-RAID-MIB.txt`
  At the Management Units and Server Units x86, ServerView RAID periodically checks hardware components. These events are reported by trap, even in good case with the weight `NOTIFICATION`. Text example of such a successful test: "*Patrol Read started*" and "*Patrol Read finished*".
  In order for ServerView RAID's traps to be correctly represented by the management station, this MIB must be imported to the management station.
- Access to the above MIBs is possible on the Management Unit, e.g. with scp (secure copy) under any administrator ID.
- The corresponding MIBs from BS2000 should be used to interpret the SNMP data from the BS2000 systems. Details can be found in the manual "SNMP Management" for BS2000.

The following examples with standard SNMP commands are intended to illustrate the addressing of the units or systems and the use of the MIBs. In a system monitoring application this is to be done analogously.

- Determining the SE server-specific data:
  - ```
    admin@abgsilver(M): snmpwalk -v 2c -m +FUJITSU-SU390-MIB:FUJITSU-SESERVER-MIB -c
    seserver abgblack.abg.fsc.net 1.3.6.1.4.1.fujitsu.product.se-server
    ...
    FUJITSU-SU390-MIB::Model = STRING: "SU710-20"
    ...
    ```
  - The read community (in this case "seserver") must be configured on the MU to be queried (in this case on abgblack) and allowed for the requesting side (in this case abgsilver).
  - The MIBs must be accessible on the requesting side (in this case on abgsilver).
  - The OIDs are usually documented in the MIBs.
- Determination of data from an SU x86:
  - ```
    admin@abgsilver(M): snmpget -v 2c -c su1-se1.seserver abgblack.abg.fsc.net
    sysName.0
    SNMPv2-MIB::sysName.0 = STRING: abgafrica
    ```
  - As read community <senet-name>.<read-community> has to be specified, “`su1-se1.seserver`” in this case.
- Determination of openSM2 data from a BS2000 system:
  - ```
    admin@abgsilver(M): snmpwalk -v 2c -m FJ-OPENSM2-MIB -c D020ZE01.seserver
    abgblack.abg.fsc.net .1.3.6.1.4.1.231
    FJ-OPENSM2-MIB::sm2Status.0 = INTEGER: running(1)
    FJ-OPENSM2-MIB::sm2Version.0 = STRING: "V20.0A04"
    ...
    ```
  - As read community <hostname>.<read-community> has to be specified, “`D020ZE01.seserver`” in this case.

SNMP integration of the SE server via SEM

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



Example of an SNMP configuration

The *SNMP* tab displays information for the selected MU 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

  Click on the *Change* icon in the *Configuration of local system data* group and make the changes to the system file in the following dialog.

  Hints:
  The SE Manager displays the SYSLOCATION in the header line.
  In a management cluster, SYSLOCATION should match the location of the SE server of the unit.

- Adding or removing allowed read accesses

  In the *Allowed read accesses* group select one of the following procedures:

  > To add a new read access, click *Add new read access*, and confirm the action after entering the necessary information.
  You can restrict the read access to a management station by specifying its host name or IP address.

> 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 confirm the action after entering the necessary information.

  > To remove a trap receiver, click the *Remove* icon by the required trap receiver and confirm the action.

- Sending a test trap

  > To send a test trap, click the *Send test trap* icon by the required trap receiver and confirm the action.

10.1.5.6 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.

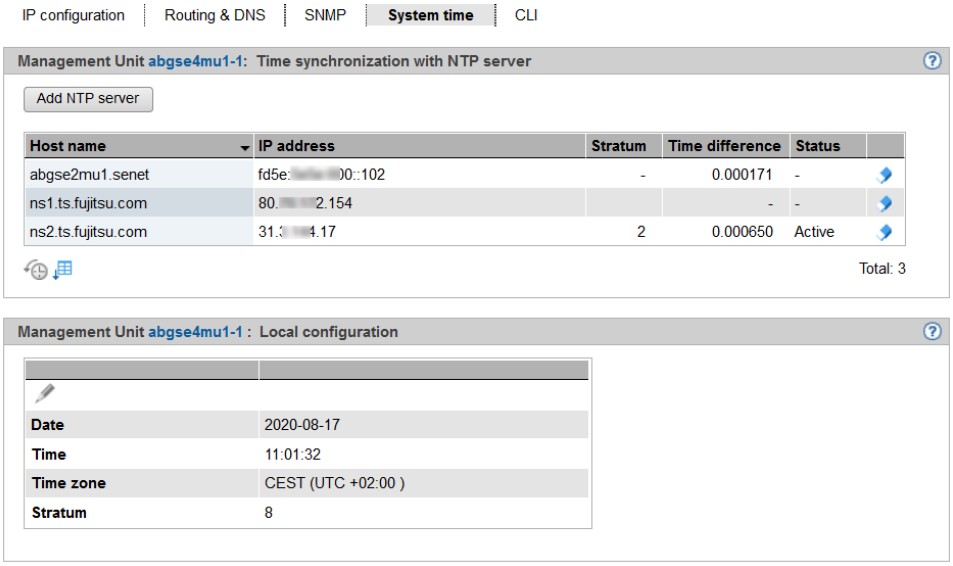
Effect on the time setting of the systems on the SE server

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".

When changes are made to the time management which affect the Server Unit, bear in mind that the time settings in BS2000 systems 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 OS DX Introduction to System Administration" manual [10].

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



The *System time* tab displays the NTP servers which are configured 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".

> In the *Local configuration* group click the *Change* icon, and after making the necessary entries confirm the action.

10.1.5.7 Entering CLI commands

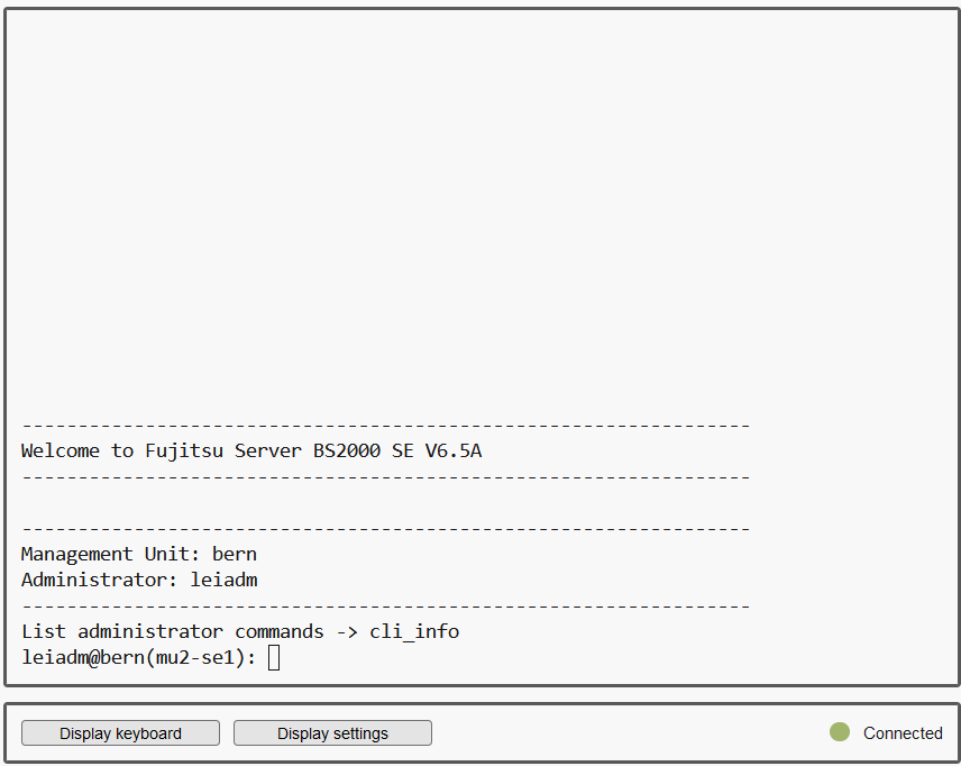
The SE Manager offers the administrator access to the CLI (**C**ommand **L**ine **I**nterface) on the Management Unit.

> 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 textbased 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 in section "Terminal window".



The available commands are described in the online help of the SE Manager.

10.1.6 Managing the HNC

The administration of an HNC is described in the following sections:

- Displaying system information and interfaces of the HNC
- Managing the IP configuration of the HNC
- Managing routing of the HNC
- Managing the DNS configuration of the HNC
- Configuring Net-Storage on the HNC

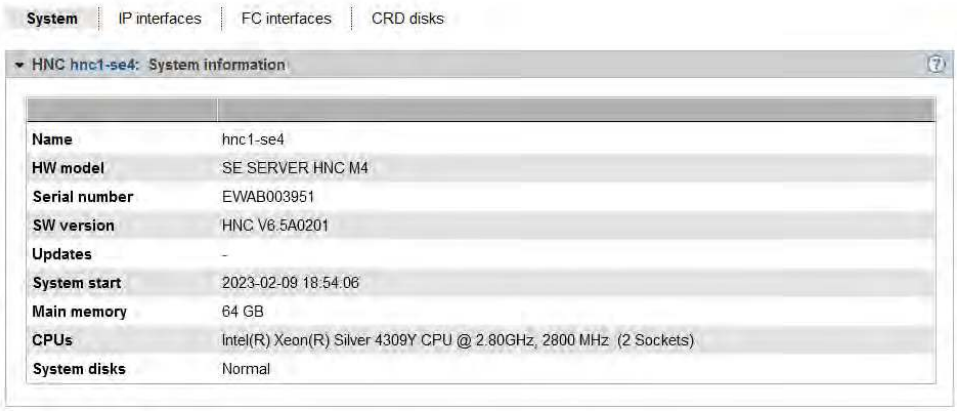
10.1.6.1 Displaying system information and interfaces of the HNC

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 CRD disks of the HNC

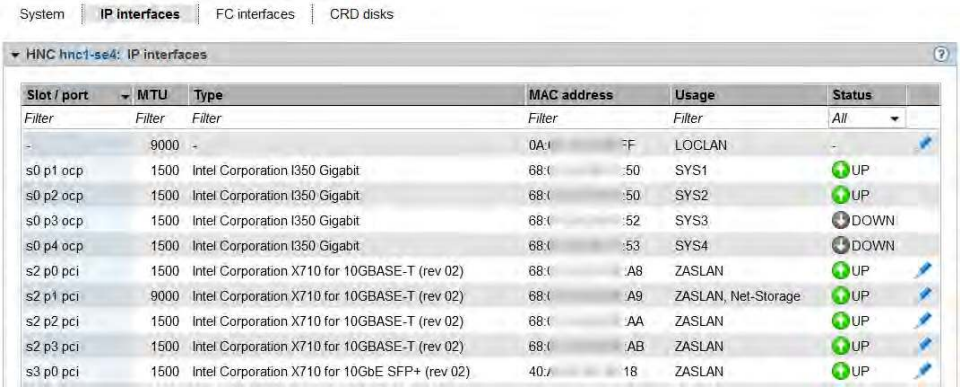
Displaying system information of the HNC

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



Displaying IP interfaces of the HNC

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



The *IP interfaces* tab provides information about the HNC's LAN interfaces.

The following function is available:

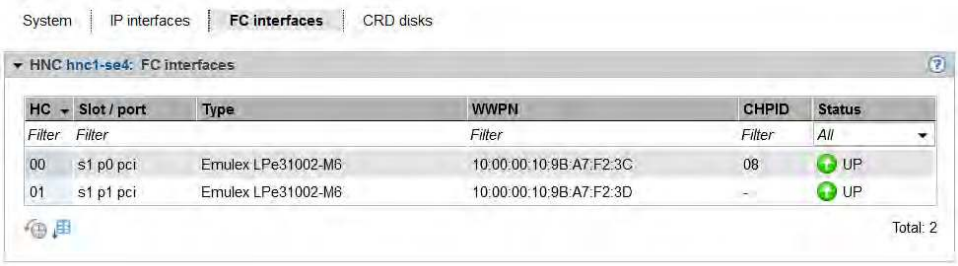
Changing the packet length in the case of LOCLAN and PCI interfaces

In the case of a PCI interface you can only change the packet length in normal operation, i.e. when *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:



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 (**W**orld **W**ide **P**ort **N**umber) are displayed for each FC interface. The hardware status of the FC interface is also displayed (*UP* / *DOWN*).

Displaying CRD disks of the HNC

The *CRD disks* tab displays the status of the unit's internal CRD disks (configuration disks).

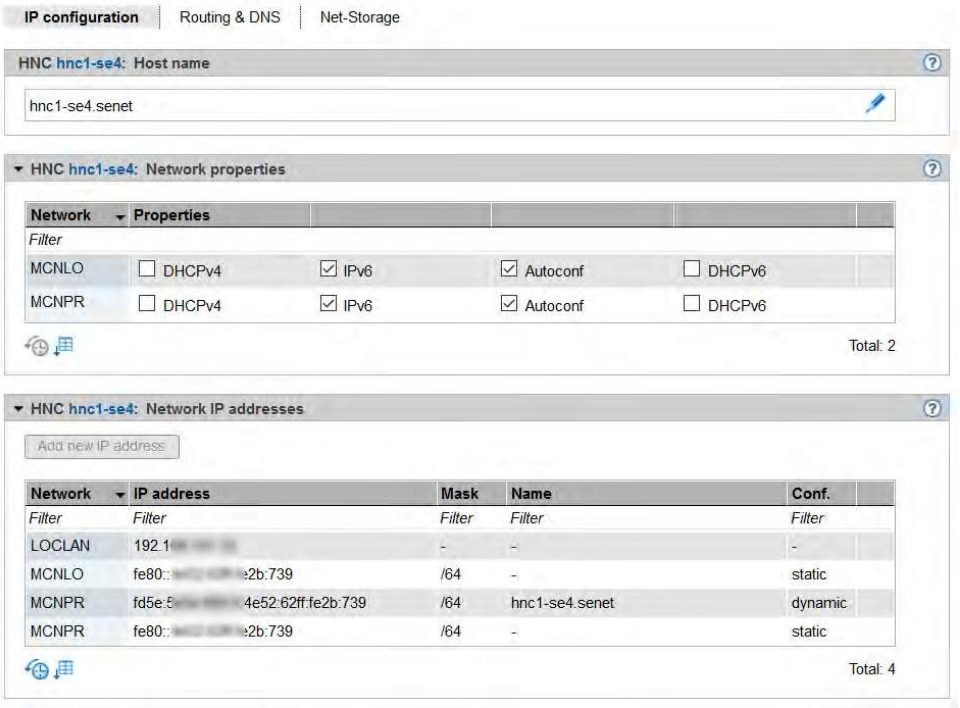
> Select *Hardware -> Units ->* [*<se server> (SE<model>) ->*] *<unit> (HNC) -> Information*, *CRD disks* tab:

The structure of the tab is the same as that for the MU (see "Displaying CRD disks of the MU").

10.1.6.2 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.



The *IP configuration* tab displays the host name, network properties, and network IP addresses of the HNC in three groups.

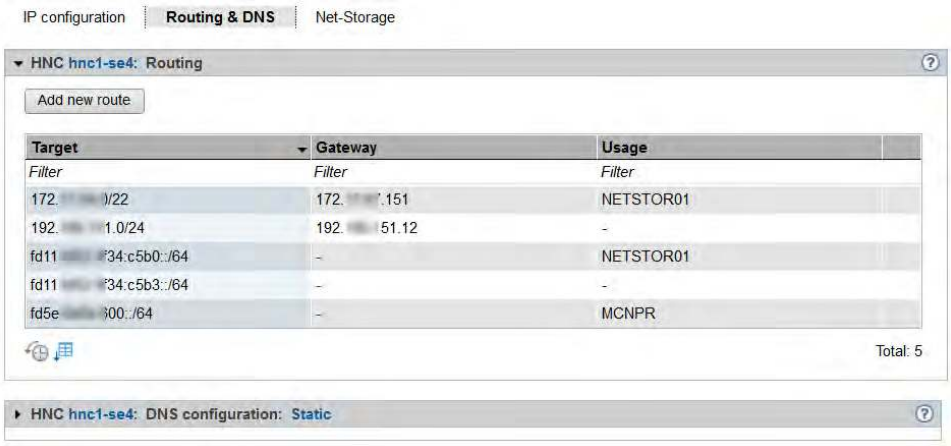
Changing the host name and domain of the HNC

> In the *Host name* group click the *Change* icon, in the subsequent dialog box change the host name and domain, and confirm the action.

10.1.6.3 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.



The *Routing & DNS* tab displays the routing in the upper group *Routing*.

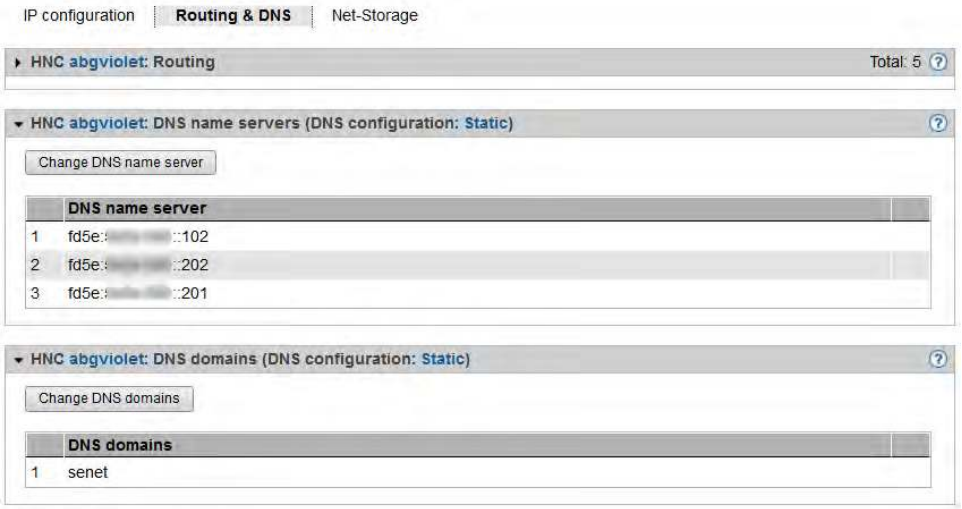
The functionality of the tab is the same as that for the MU (see section "Managing routing of the Management Unit") with the following restriction:

> 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.

10.1.6.4 Managing 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 DNS configuration is displayed in the two groups *DNS name servers* and *DNS domains*. The title bar of the group shows whether DNS is configured and whether static or dynamic DNS configuration is involved.

10.1.6.5 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.

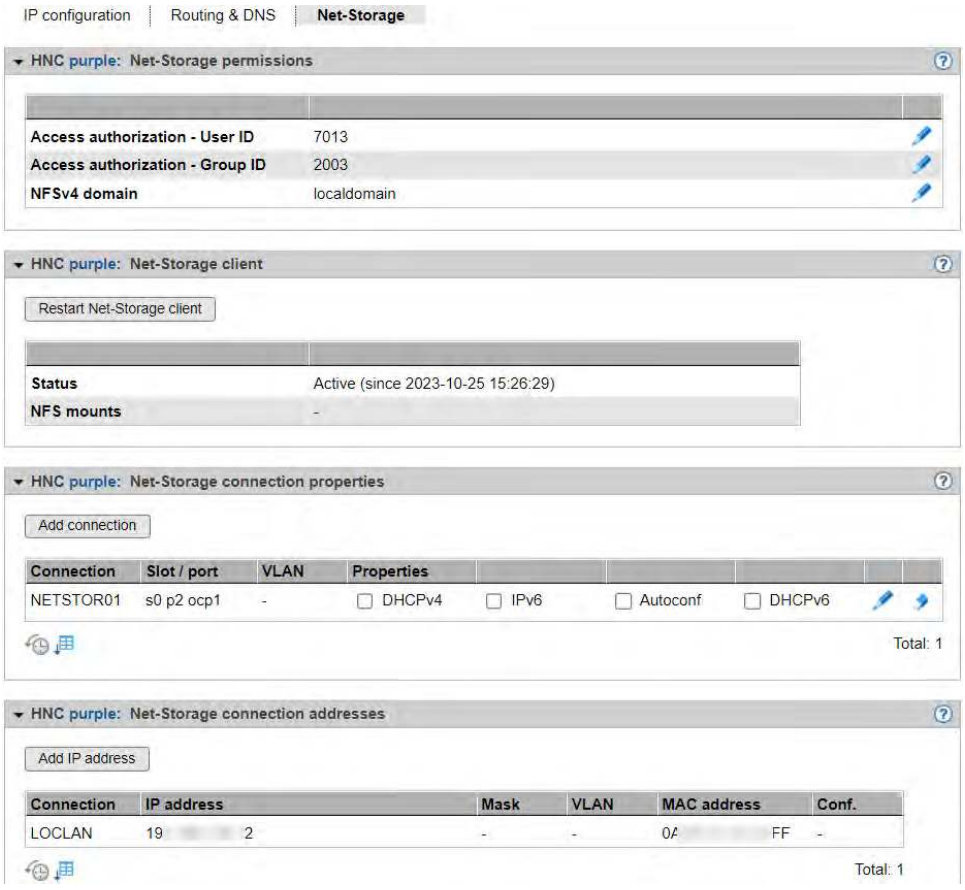
  The NFSv4 domain must correspond to the domain name set on the Net-Storage server.

  > **i** The HNC 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 the HNC using the *Management* menu, *Net-Storage* tab.

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



The *Net-Storage* tab displays the *Net-Storage permissions*, *Net-Storage client, 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 *Net-Storage permissions* group, the current user and group ID that can be used to administrate the Net-Storage access are specified in the form of userid/groupid. The IDs must be obtained from the system administrator of the Net-Storage server. The default value for both is 0.

> In the *Net-Storage permissions* group click the *Change* icon by *Access authorization - User ID* or *Group ID*. In the subsequent dialog box change the user and/or group ID and confirm the action.

! If the default value is not changed, the access is attempted with root rights, which is not recommended for reasons of data protection.

¡ Please note that as a result of this action, all mounted Net-Storage devices in the BS2000 will be unmounted. You will therefore have to re-mount them afterwards.

Entering or changing configuration data for the NFSv4 domain

> In the *Net-Storage permissions* group, click on the *Change* icon by *NFSv4 domain* and enter the domain name in the subsequent dialog. Confirm the action.

¡ Please note that as a result of this action, all mounted Net-Storage devices in the BS2000 will be unmounted. You will therefore have to re-mount them afterwards.

Restarting the Net-Storage client

The *Net-Storage client* group displays the current status of the Net-Storage client and the mounted directories.

> In the *Net-Storage client* group, click on *Restart Net-Storage client* and confirm the action.

¡ Please note that as a result of this action, all mounted Net-Storage devices in the BS2000 will be unmounted. 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.

10.1.7 Managing the Server Unit x86

The administration of an SU x86 is described in the following sections:

- System information and interfaces of the unit
- Managing the IP configuration of the SU x86
- Managing routing of the SU x86
- Managing the DNS configuration of the SU x86
- Configuring Net-Storage on the SU x86

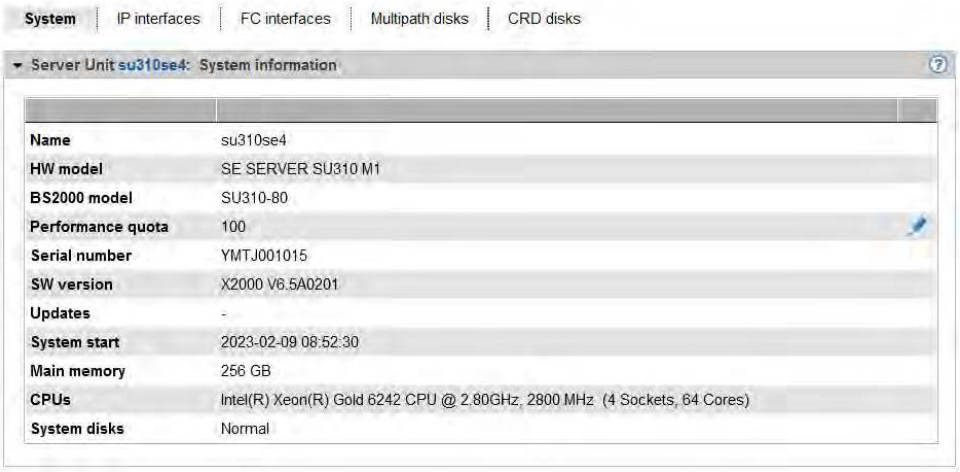
10.1.7.1 System information and interfaces of the unit

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

- Displaying system information of the SU x86
- Displaying and changing IP interfaces of the SU x86
- Displaying and resetting FC interfaces of the SU x86
- Displaying multipath disks of the SU x86
- Displaying CRD disks of the SU x86

Displaying system information of the SU x86

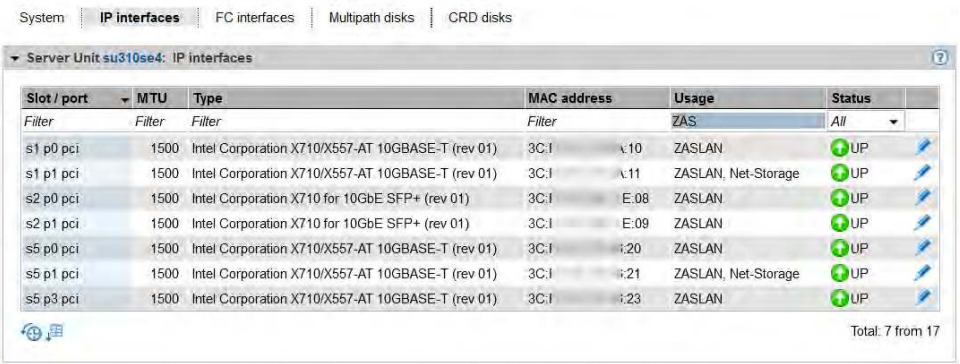
> Select *Hardware -> Units ->* [*<se server> (SE<model>) ->*] *<unit> (SU<x86>) -> Information*, *System* tab.



> *Performance quota* is displayed and can be changed only when a license for dynamic performance control (a so-called performance quota key) is installed on the unit.

Displaying and changing IP interfaces of the SU x86

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



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 and resetting 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 tab is provided in the section "Displaying and resetting FC interfaces of the MU".

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".

Displaying CRD disks of the SU x86

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

Purpose and operation of configuration disks are described in section "External CRD disks".

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

10.1.7.2 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") 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.

10.1.7.3 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.

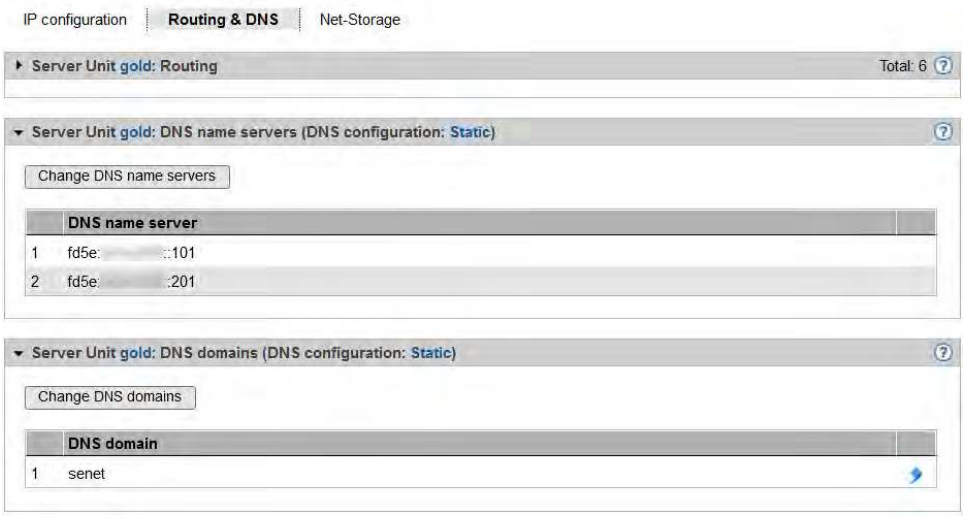
The functionality of the tab is the same as that for the MU (see section "Managing routing of the Management Unit") with the following restriction:

> ¡ 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.

10.1.7.4 Managing 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 DNS configuration is displayed in the two groups *DNS name servers* and *DNS domains*. The title bar of the group shows whether DNS is configured and whether static or dynamic DNS configuration is involved.

The structure of the tab is basically the same as that for the MU (see section "Managing the DNS configuration").

10.1.7.5 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 following 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.

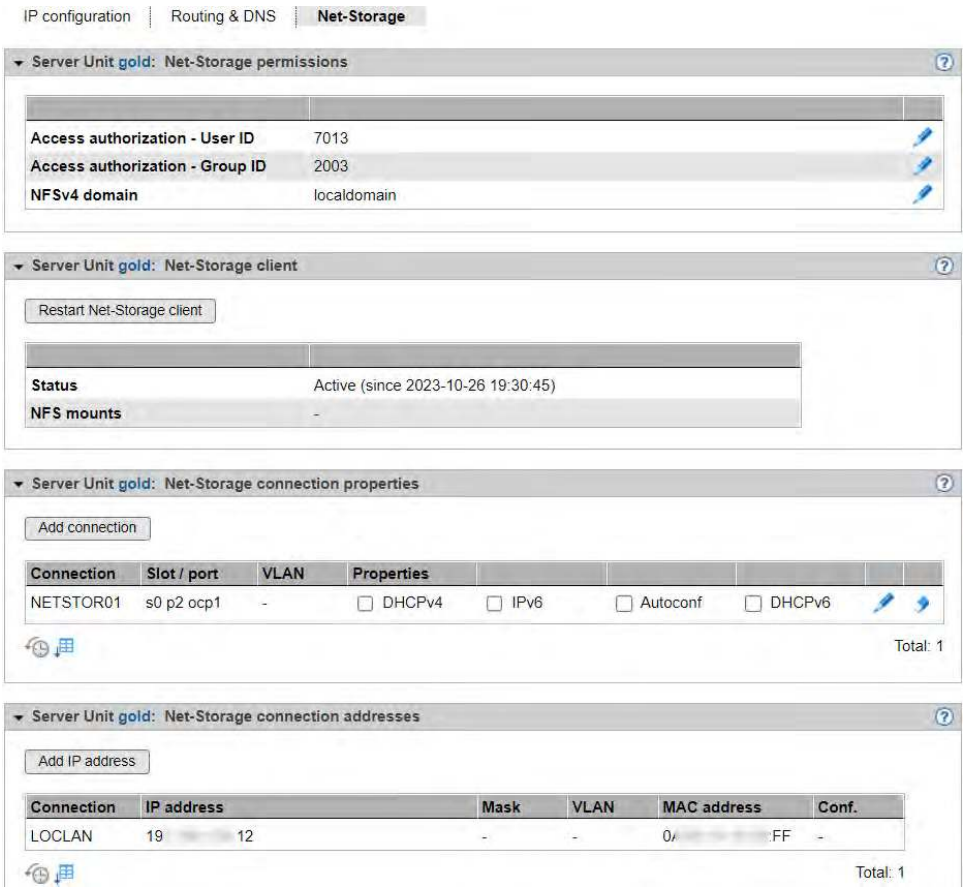
  The NFSv4 domain must correspond to the domain name set on the Net-Storage server.

  > **i** 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.



The *Net-Storage* tab displays the *Net-Storage permissions*, *Net-Storage client*, *Net-Storage connection properties*, and *Net-Storage connection addresses* groups. The following functions are available:

Changing access for the SU x86

In the *Net-Storage permissions* group, the current user and group ID that can be used to administrate the Net-Storage access are specified in the form of userid/groupid. The IDs must be obtained from the system administrator of the Net-Storage server. The default value for both is 0.

> In the *Net-Storage permissions* group click the *Change* icon by *Access authorization - User ID* or *Group ID*. In the subsequent dialog box change the user and/or group ID and confirm the action.

! If the default value is not changed, the access is attempted with root rights, which is not recommended for reasons of data protection.

¡ Please note that as a result of this action, all mounted Net-Storage devices in the BS2000 will be unmounted. You will therefore have to re-mount them afterwards.

Entering or changing configuration data for the NFSv4 domain

> In the *Net-Storage permissions* group, click the *Change* icon by *NFSv4 domain* and enter the domain name in the subsequent dialog. Confirm the action.

¡ Please note that as a result of this action, all mounted Net-Storage devices in the BS2000 will be unmounted. You will therefore have to re-mount them afterwards.

Restarting the Net-Storage client

The *Net-Storage client* group displays the current status of the Net-Storage client and the mounted directories.

> In the *Net-Storage client* group, click on *Restart Net-Storage client* and confirm the action.

¡ Please note that as a result of this action, all mounted Net-Storage devices in the BS2000 will be unmounted. 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.

10.1.8 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 (and into additional racks, if needed) 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 (or AU administrator) you install your own software (e.g. Networker StorageNode) 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.

Many roles are entitled to access the applications. Only as administrator or AU administrator, however, the administration functions for modifying the data for accessing Application Units are 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 (e.g. AUQ38E /DBU38E). 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.

The following sections describe the management of an AU in more detail:

- Configuring an Application Unit
- Displaying hardware information of the Application Unit
- Managing the IP configuration of the Application Unit

10.1.8.1 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 system status *Running*.
  - The hardware information of the Application Unit is displayed in the information for the Application Unit.

> It is possible to integrate an AU only at hardware level.
> In this case, systems resp. VMs are not enquired and therefore not displayed, *NOT_MONITORED* is displayed as the system status of the AU, and the hardware displays are subject to certain restrictions.
> For more information, see the online help.
> For details, please contact Customer Support.

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 (teleservice call) by forwarding hardware error messages to the Management Unit. For Application Units with the Linux and Windows operating systems, ServerView agents must also be installed for the purpose of hardware monitoring.

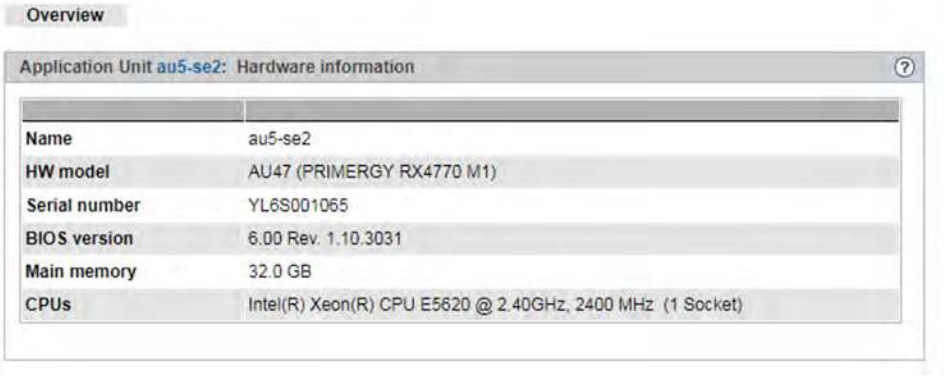
On the Management Unit the messages forwarded from the Application Units are filtered further and sent to the Service Center using the remote service procedure AIS Connect.

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

10.1.8.2 Displaying hardware information of the Application Unit

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



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):

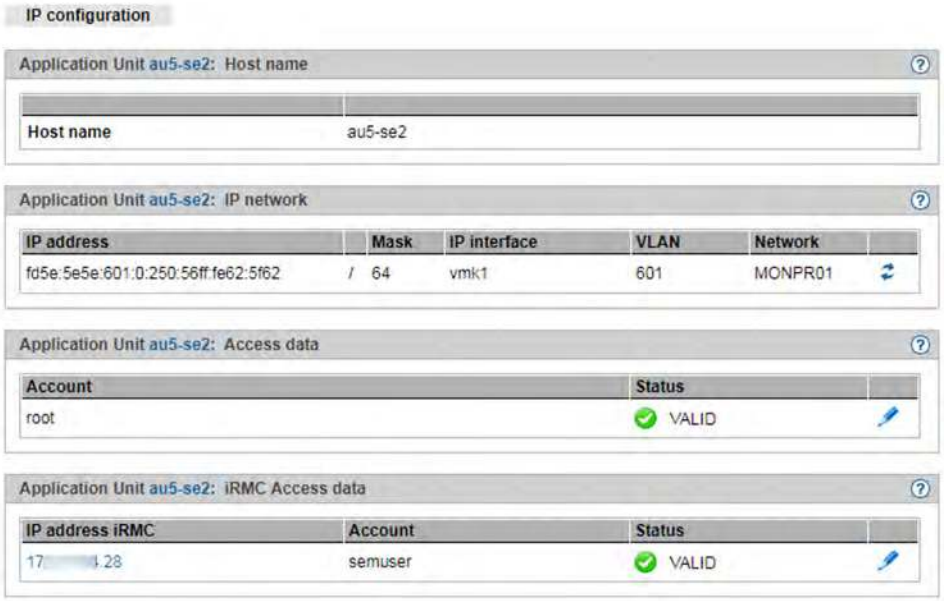
10.1.8.3 Managing the IP configuration of the Application Unit

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



The *IP configuration* tab displays the groups *Host name, IP network, Access data* (only for AU with the VMware vSphere ESXi or Microsoft HyperV 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 ESXi or Microsoft HyperV 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 has been changed (outside of the SE Manager), you must also change the password here in SEM.

> 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 *LAN Channel Privilege Administrator* and *Serial Channel 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").

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.

The following description refers to the internal Net Unit and the networks realized with it. If the optional add-on NUX (Net Unit eXtension) is installed on your Management Unit, SEM's menu structure will be adapted to the extended connectivity of the SE server.
For more details on NUX, please contact the customer service.

The following sections describe the management of IP networks:

10.2.1 Displaying information on networks and switches

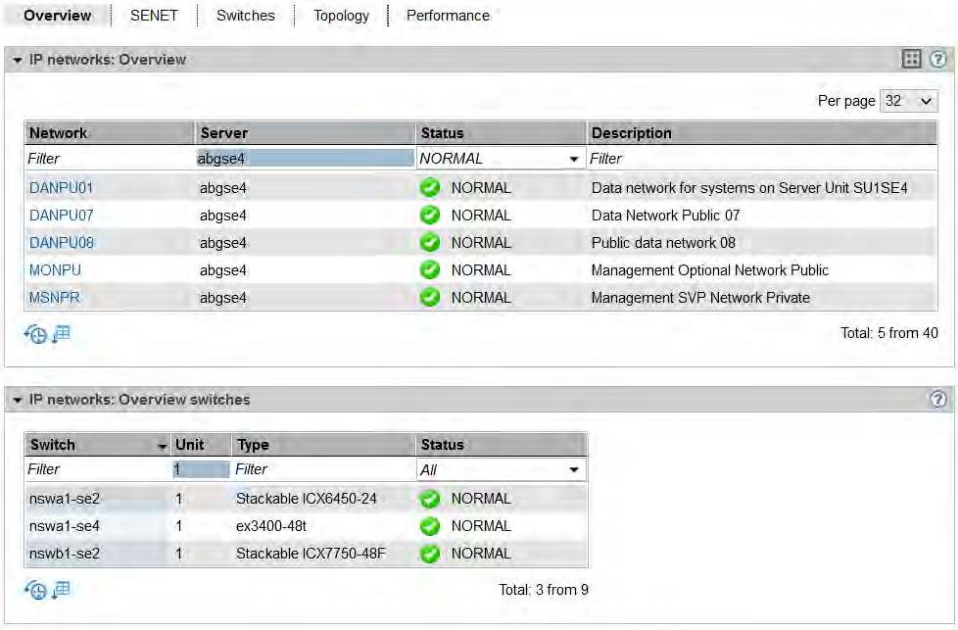
You can display the following information on IP networks and switches:

- 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 and switches

You obtain the overview of the public and private IP networks and switches using the associated *Overview* tab.

> Select *Hardware -> IP networks*, *Overview* tab.



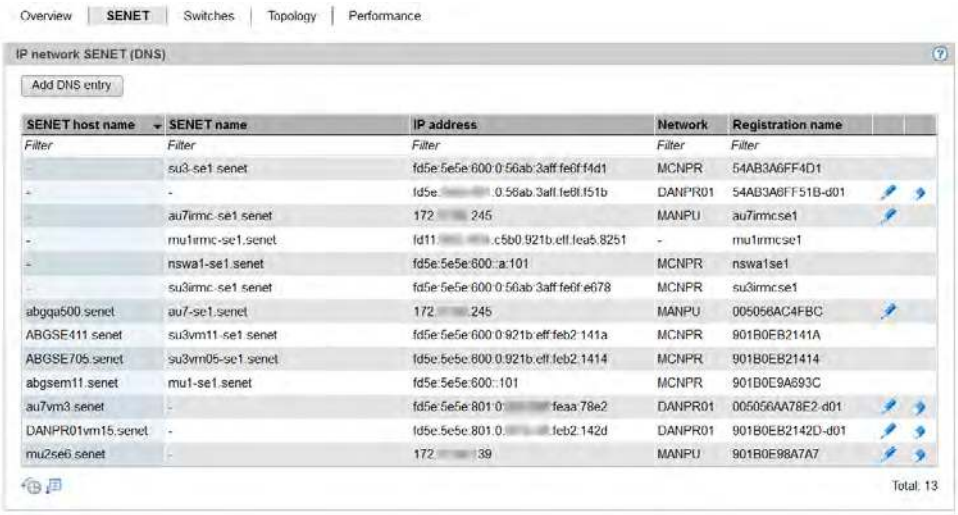
The *Overview* tab displays information on all public and private data and management networks of the SE server configuration as well as information on the switches in the second table.

If you manage a configuration of two SE servers in a Management Cluster, an additional *Server* column is displayed in the first table. 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.



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.

In case of *Manual input of 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.

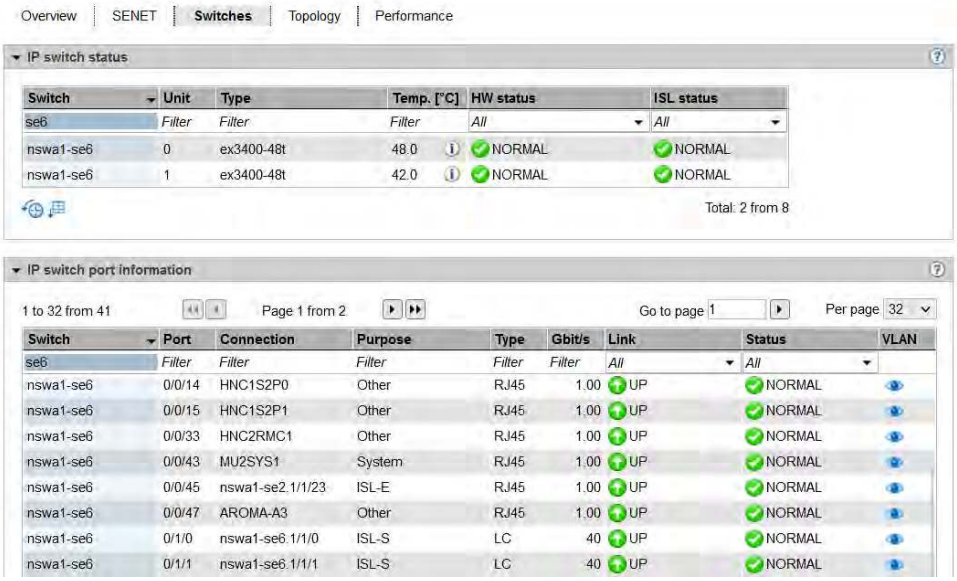
Deleting a DNS entry

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

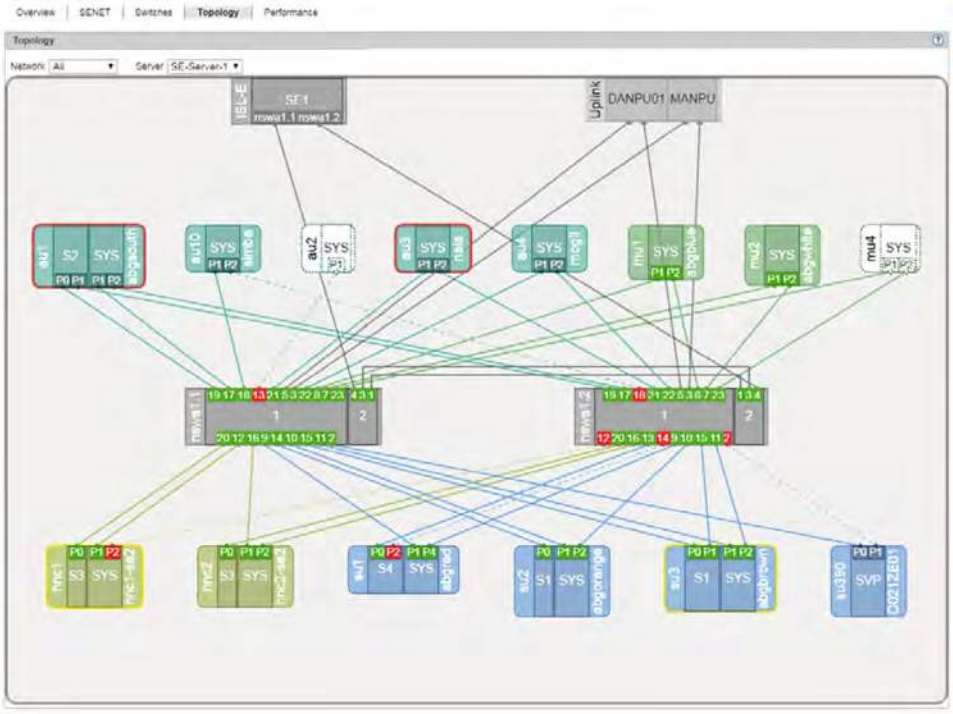
> If you drag the mouse over the icon next to the temperature value in the *IP switch status* group, a tool tip displays the temperature thresholds for warning and power-off.

> In the *IP switch port information* group, click the *Display/Details* icon ( ) in the entry for a switch port; The VLAN connections for this switch port are displayed in a dialog box.

10.2.1.4 Graphical display of the SE 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:

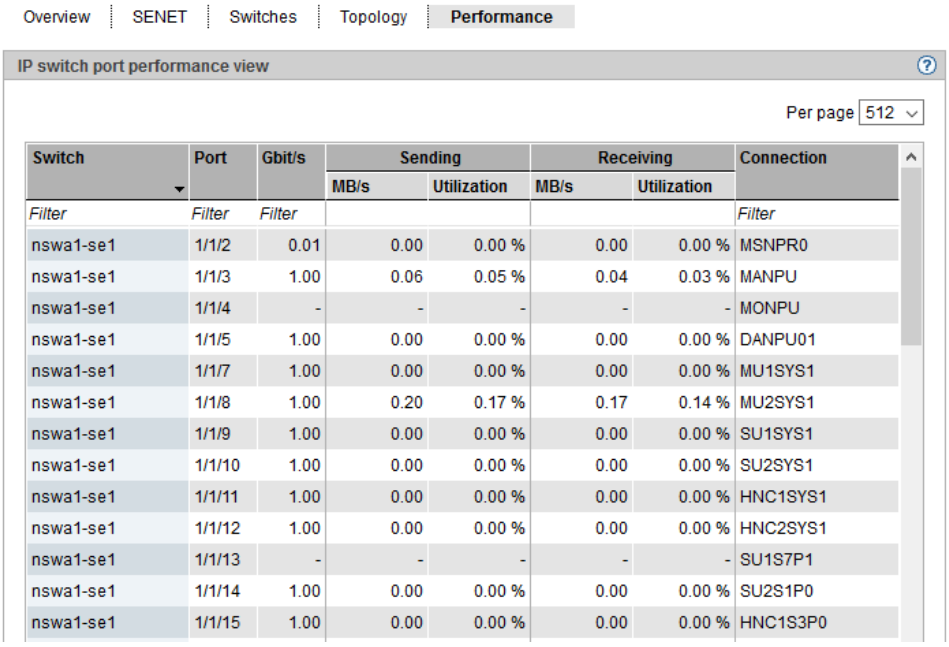
- In the display of the topology you can have a selected network highlighted, i.e. this network is displayed normally and the components of all other IP networks are grayed out.
- For a Management Cluster, you can select the SE server for which you want to display the topology, from the *Server* list. 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.
>
> Further information can be found in the online help.

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 active connections). A distinction is made between the send and receive directions for data throughput and utilization.

> Select *Hardware -> IP networks*, *Performance* tab.



Switch	Port	Gbit/s	Sending		Receiving		Connection
			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	0.06	0.05 %	0.04	0.03 %	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	0.00	0.00 %	0.00	0.00 %	MU1SYS1
nswa1-se1	1/1/8	1.00	0.20	0.17 %	0.17	0.14 %	MU2SYS1
nswa1-se1	1/1/9	1.00	0.00	0.00 %	0.00	0.00 %	SU1SYS1
nswa1-se1	1/1/10	1.00	0.00	0.00 %	0.00	0.00 %	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 %	0.00	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
nswa1-se1	1/1/15	1.00	0.00	0.00 %	0.00	0.00 %	HNC1S3P0

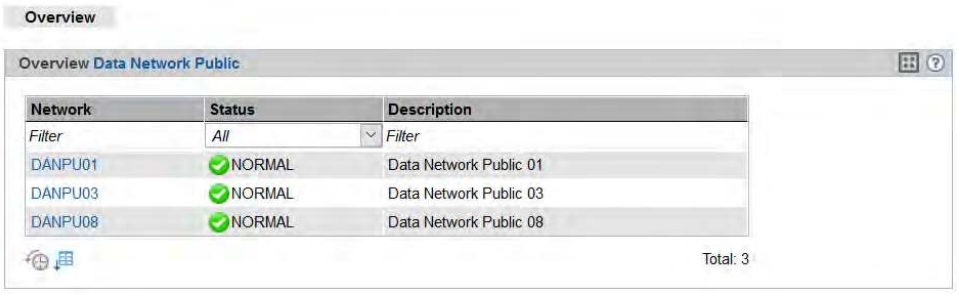
10.2.2 Managing a Data Network Public

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.



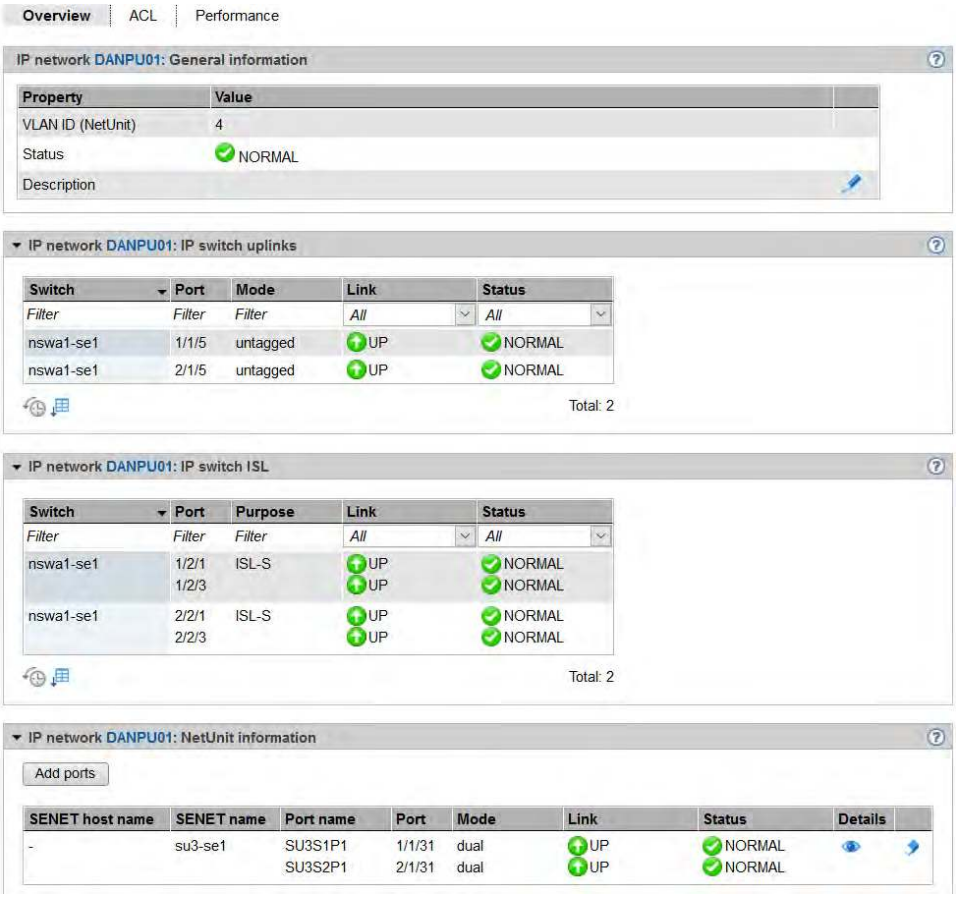
The tab displays information on all existing DANPUs of the SE server configuration.

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 DANPUs. 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.



The *Overview* tab displays all information on the selected DANPU. The table in the *NetUnit information* group contains the additional *Switch* column with the name of the switch, if more than one logical switch exists.

The following functions are available:

Modifying the description

> In the *General information* group click the *Change* icon ( ) in row *Description*.
>
> The subsequent dialog box *Change description* allows to enter resp. modify the description of the network.

Displaying the MAC address

> In the *NetUnit 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 *NetUnit information* group click *Add ports*, follow the instructions of the wizard, and select the required port.

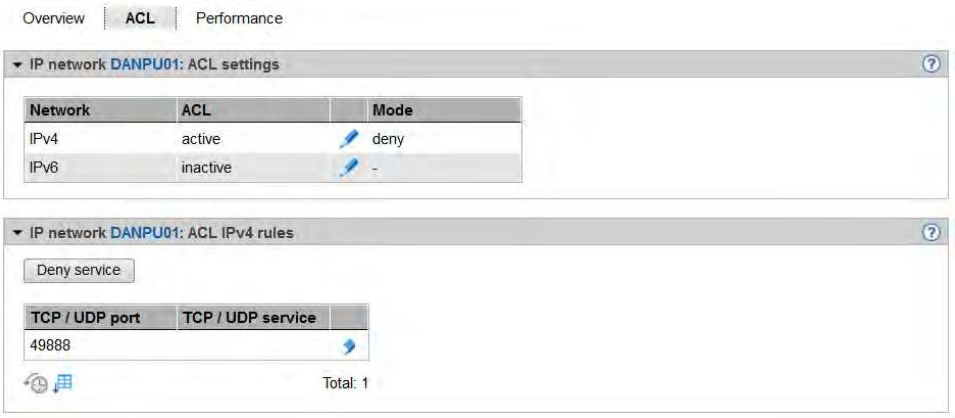
Removing a port

> In the *NetUnit 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.



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 (for IPv4 and IPv6 separately),
- select the ACL mode (*permit* or *deny*). In *permit* (whitelist) mode only the ports/services contained in the ACL are permitted network access. All other services are locked. In *deny* (blacklist) 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 IPv4 rules* or *ACL IPv6 rules* group click *Deny service* (in the case of ACL mode *deny*) or *Grant 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.

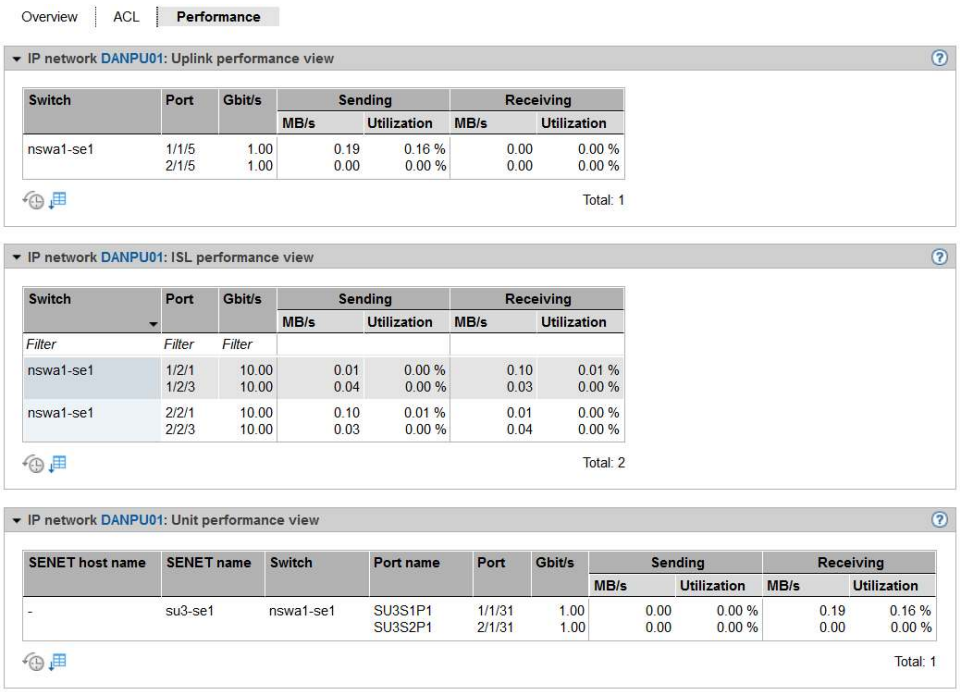
Removing a service from the ACL

> In the *ACL IPv4 rules* or *ACL IPv6 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.



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).
- 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.

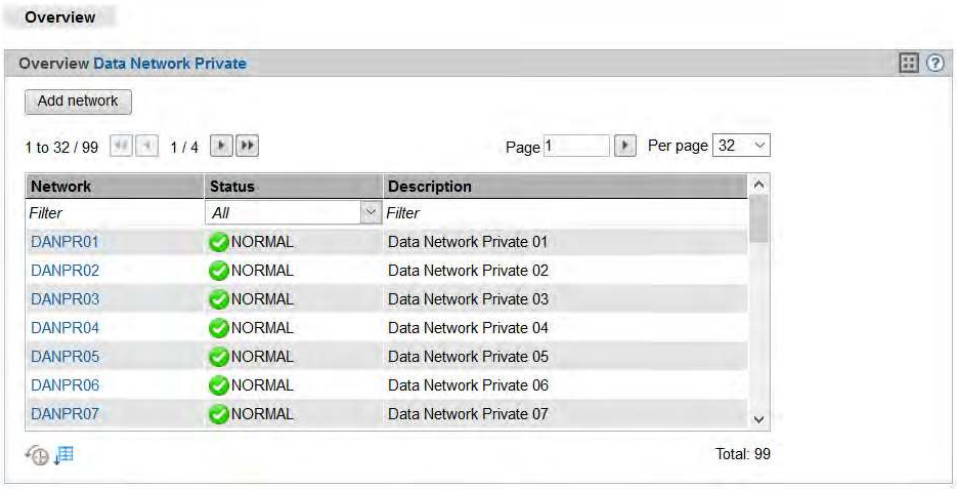
In the case of redundant networks the two ports used for the redundant connections and their performance are displayed one after the other in a table row.

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.

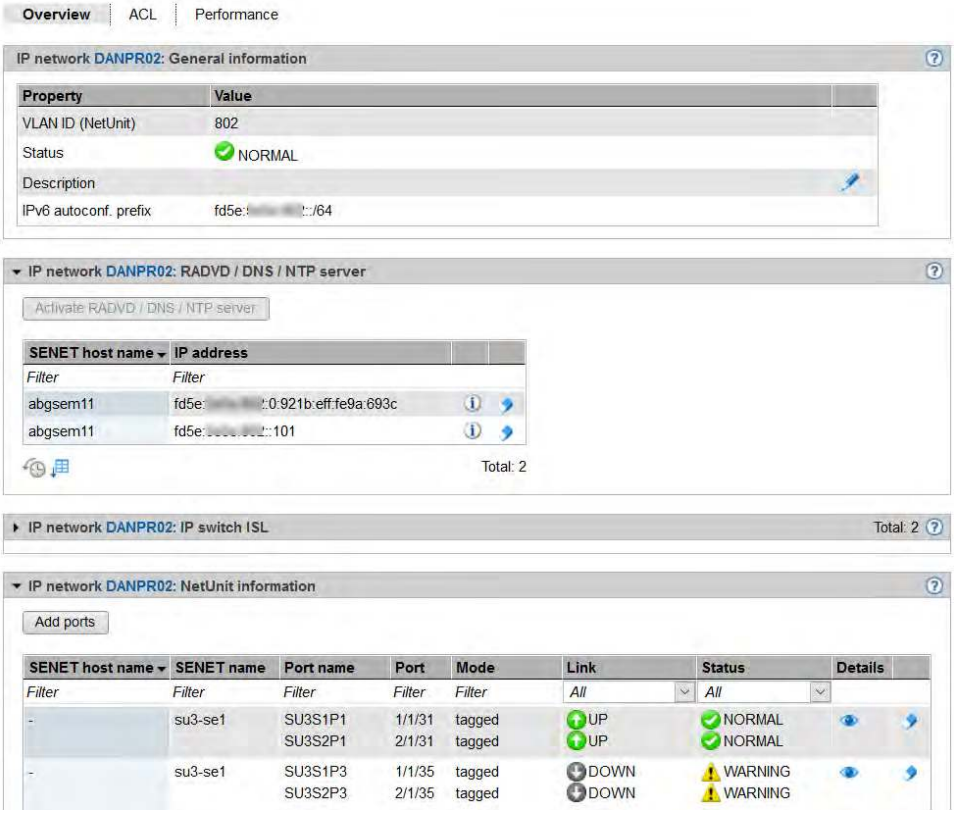


> The administrator can create another private network by clicking the *Add network* button.

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 entries 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.



The *Overview* tab displays all information on the selected DANPR. The table in the *NetUnit information* group contains the additional *Switch* column with the name of the switch, if more than one logical switch exists.

The following functions are available:

Modifying the description

> In the *General information* group click the *Change* icon ( ) in row *Description*.

The subsequent dialog box *Change description* allows to enter resp. modify the description of the network.

Activating the RADVD/DNS/NTP server

> In the *RADVD / DNS / NTP server* group click the *Activate RADVD / DNS / NTP server* button.

A dialog box opens in which you can enable the RADVD/DNS/NTP server on the MU resp. the desired MUs of the SE administration area.

Only those MUs can be selected which are connected to the network and on which the RADVD/DNS /NTP server is not yet activated.

Deactivating the RADVD/DNS/NTP server

> In the *RADVD / DNS / NTP server* group click the icon *Deactivate RADVD / DNS / NTP server* ( ) by an IP address of the local MU.

After confirmation, disables the RADVD/DNS/NTP server. The function is available only for the local MU.

Displaying the MAC address

> In the *NetUnit 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 *NetUnit information* group click *Add ports*, follow the instructions of the wizard, and select the required port.

Removing a port

> In the *NetUnit information* group click the *Delete* icon ( ) by the required unit and confirm the action.

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 preselected.

> Follow the instructions of the wizard and enter the network data. Detailed information is provided in the SE Manager help.

i In the wizard, the available ports of the units (MU, SU x86, HNC) are only offered in the selection list subject 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").

10.2.3.2 Activate RADVD / DNS / NTP server

For each DANPR, you can activate the RADVD / DNS / NTP server on the MUs of the SE administration area connected to the network:

> 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.
Select the desired MUs, if necessary, and click *Activate.*

i For reasons of redundancy we recommend to activate the RADVD / DNS / NTP server on all MUs of the SE administration area.

Note: At least one port of the respective MU must be assigned to the network.

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".

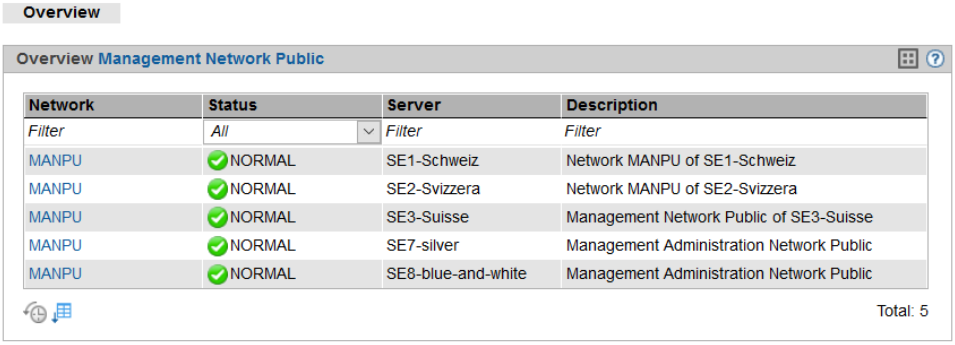
10.2.4 Managing a Management Network Public

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 public management networks (MANPU and MONPU) using the menu item *Management Network Public* in the *IP networks* menu.

Overview over the status of the management networks MANPU and MONPU

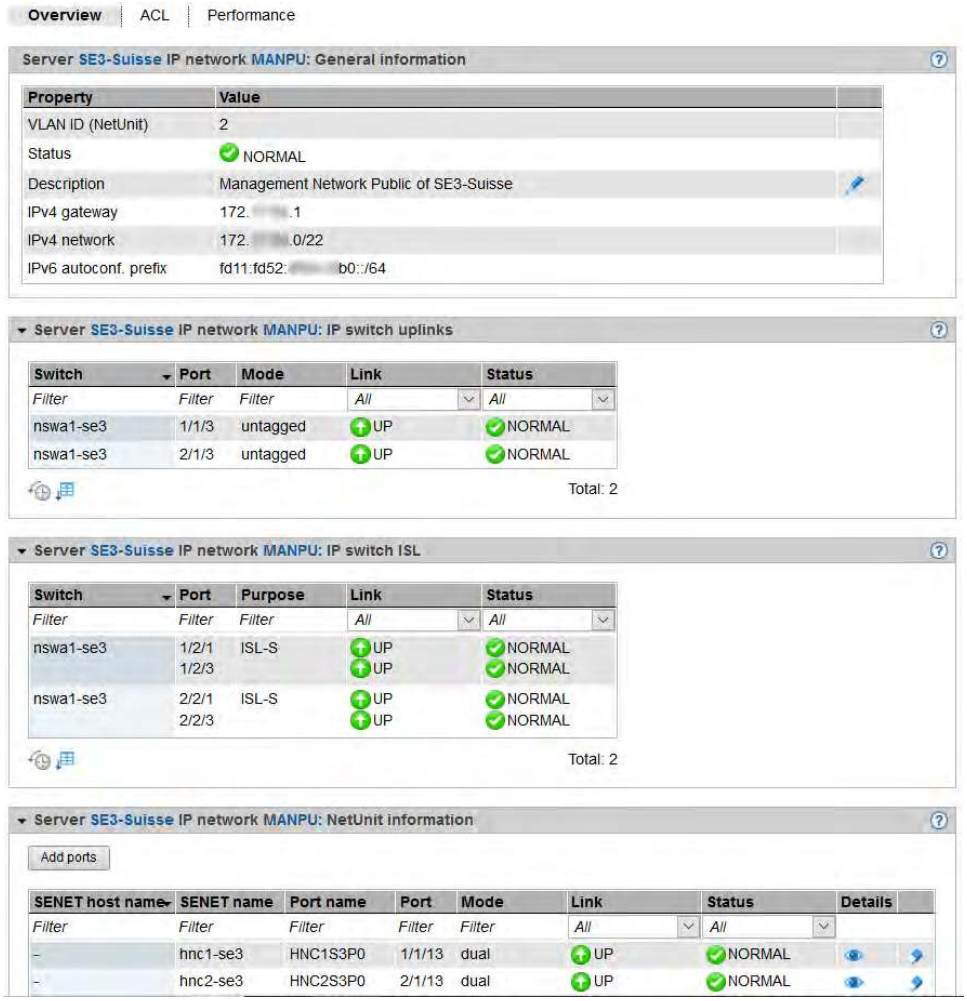
> Select *Hardware* -> *IP networks* -> *Management Network Public, Overview* tab.



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.



The *Overview* tab displays all information on the MANPU. Information on a MONPU network is displayed in the same way.

For a Management Cluster, this overview also contains the *IP switch ISL* group.

The following functions are available:

Displaying the MAC addresses

> In the *NetUnit 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 *NetUnit information* group click *Add ports*, follow the instructions of the wizard, and select the ports.

Removing a port

> In the *NetUnit 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".

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".

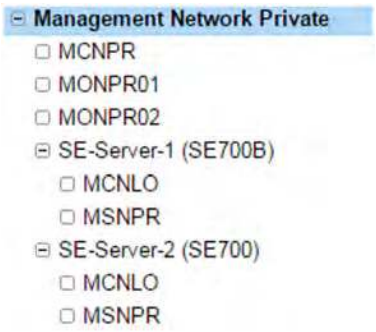
10.2.5 Managing a Management Network Private

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.

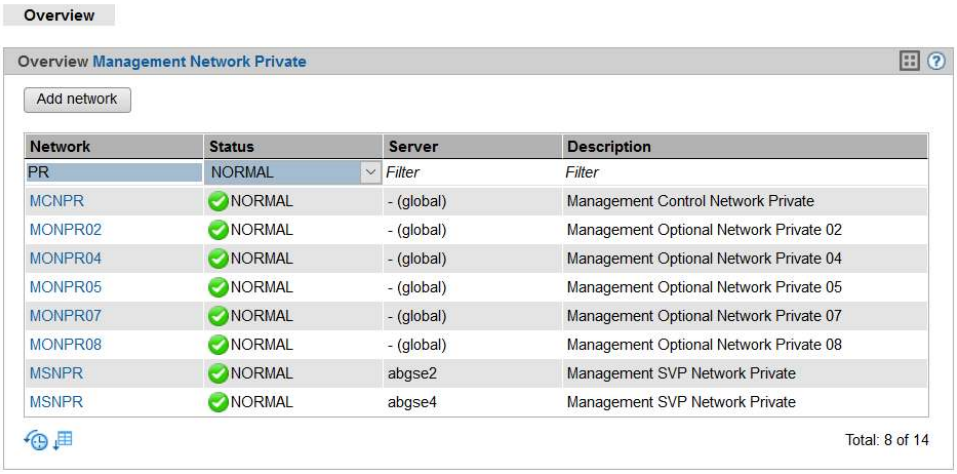
In a Management Cluster configuration, only the globally available private management networks MCNPR and MONPR01 to MONPR08 are listed directly under *IP networks -> Management Network Private*. The server specific MSNPR and MCNLO networks are each listed in the SE server-specific *<se server> (SE<model>)* menu.
Example:



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 existing in the current configuration.

> Select *Hardware -> IP networks -> Management Network Private*, *Overview* tab.



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 preselected.

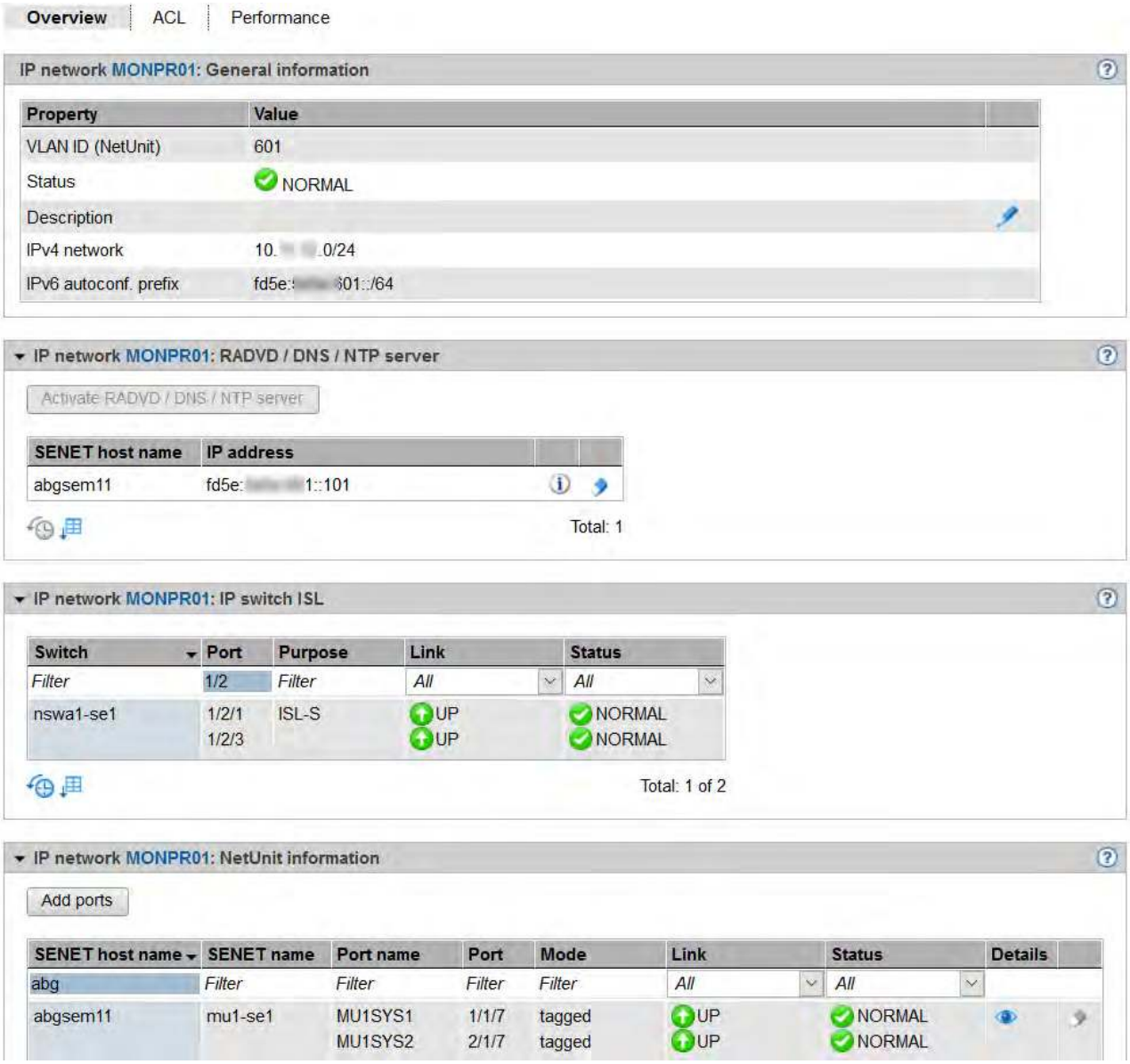
> Follow the instructions of the wizard and enter the network data. Detailed information is provided in the SE Manager help.

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.



Displaying the MAC addresses

> In the *NetUnit 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 Performance 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".

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 *NetUnit 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 *NetUnit 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.

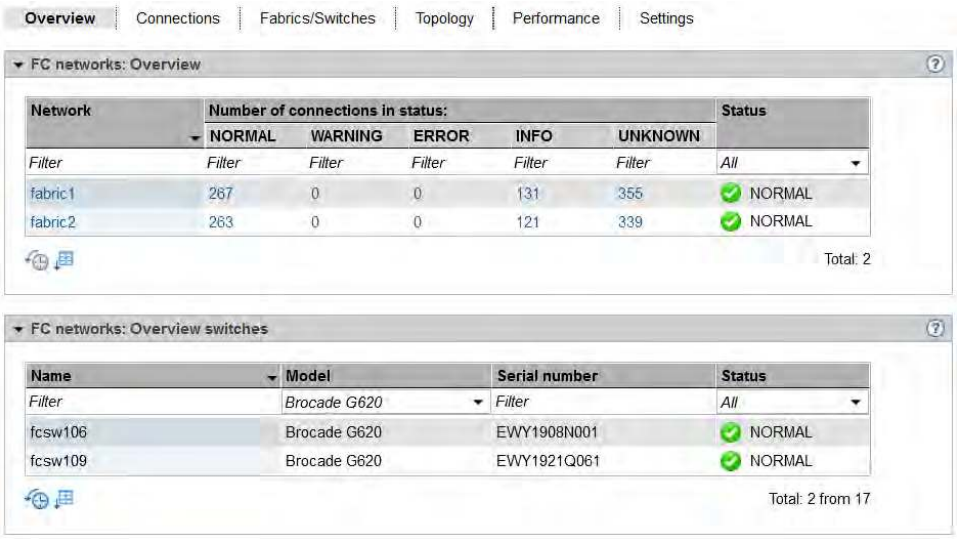
Proceed as described in section "Configuring the ACL settings of the DANPU network".

10.3 Managing FC networks

You manage the Fibre Channel networks of the SE server using the tree structure *Hardware -> FC networks*. Information about all FC networks and switches is accessible via this menu.

The *Overview* tab provides a summary overview of the connections per FC network (fabric) and of the switches.

> Select *Hardware -> FC networks*, *Overview* tab.



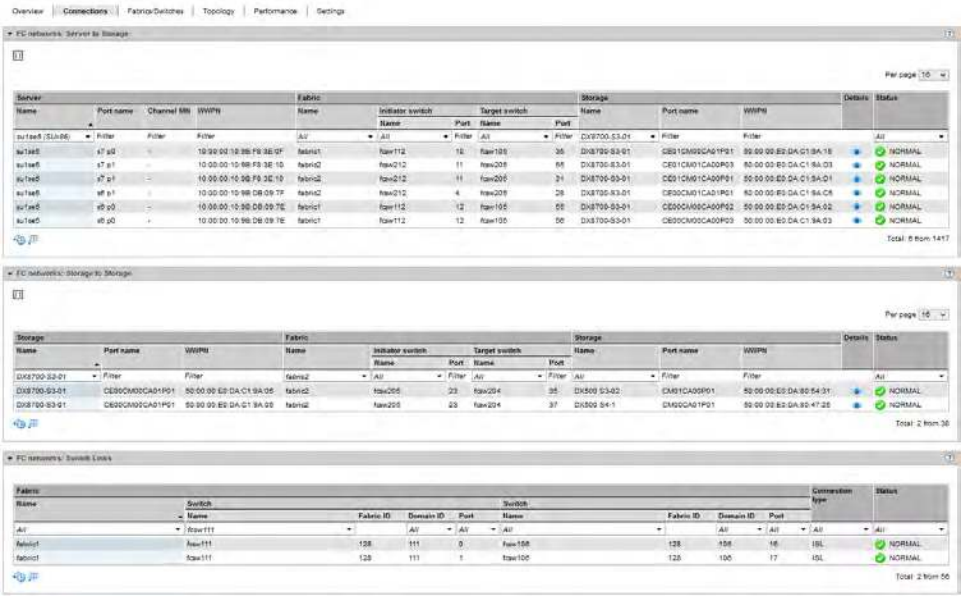
The following options for information and settings are available to you:

- Displaying connections
- Displaying fabrics and switches
- Displaying topology
- Displaying performance
- Configuring settings

10.3.1 Displaying connections

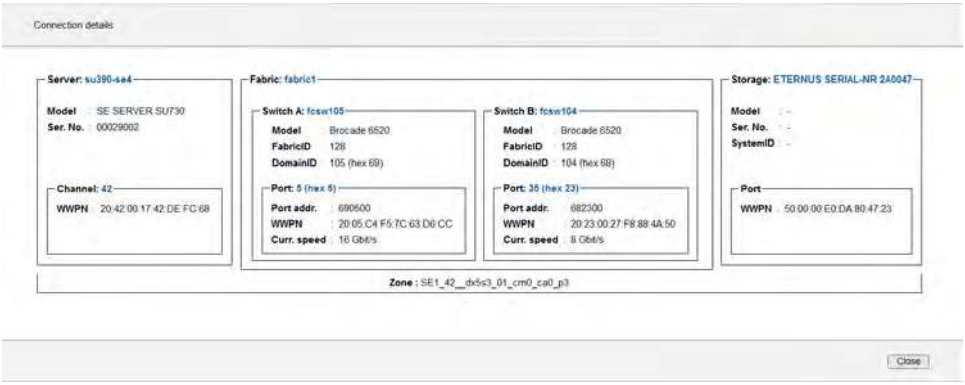
The *Connections* tab provides an overview of all connections. Three different tables of connections are shown: Between server and storage, storage and storage, and between two switches (ISL).

> Select *Hardware -> FC networks*, *Connections* tab.



You can obtain the details for a connection as follows:

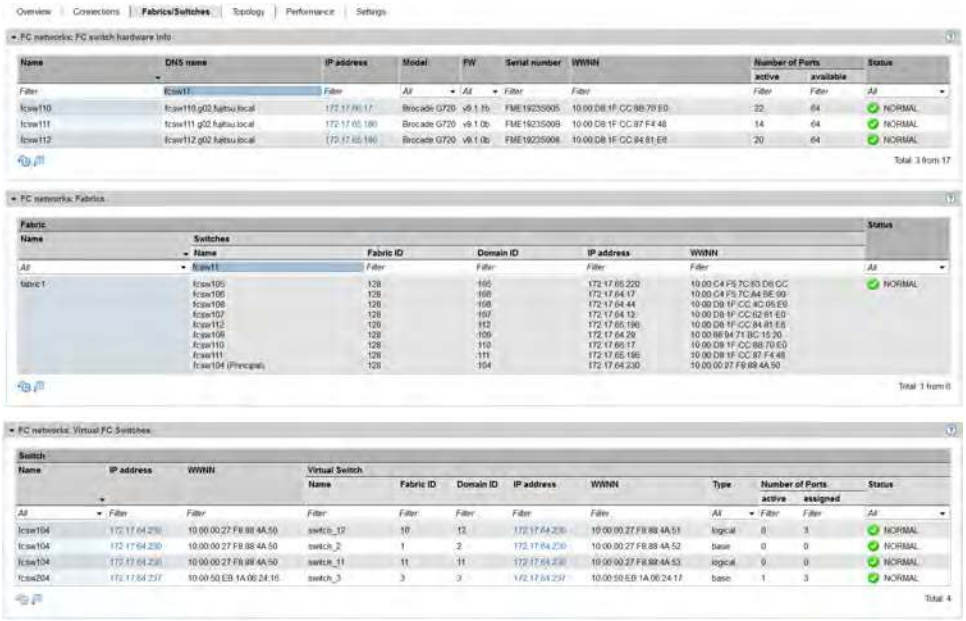
> Click on the *Display* icon ( ) for the required connection in the *Details* column. The *Connection details* dialog displays details of the connection as an overview (in the example a connection of the SU su390-se4):



10.3.2 Displaying fabrics and switches

In the *Fabrics/Switches* tab all configured switches are shown.

> Select *Hardware* -> *FC networks*, *Fabrics/Switches* tab.



The *FC switch hardware info* table displays the hardware switches with their properties. Virtual switches will not be shown.

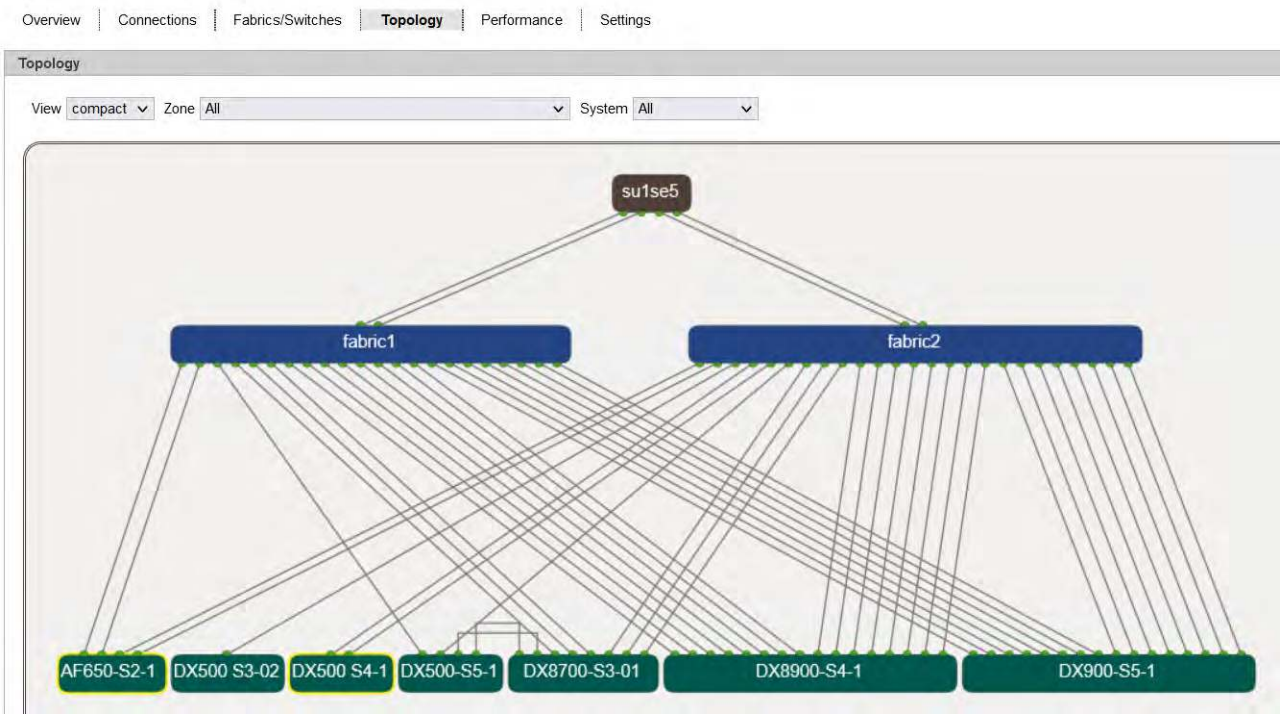
The *Fabrics* table displays the fabrics with their associated switches.

The *Virtual switches* table displays the virtual switches with the corresponding hardware switches. If no virtual switch is configured, the table will not be shown.

10.3.3 Displaying topology

The *Topology* tab displays all connections of the FC networks of the SE administration area in graphical form. When you drag the mouse cursor over a network component, a tool tip displays detailed information on it.

> Select *Hardware -> FC networks*, *Topology* tab.



View

The view can be switched between *detailed* and *compact*. In the *compact* mode, only the main components like fabrics, servers and storage systems are visible.

Zone

List of the zones. The default is *All*, i.e. all zones are displayed. When you select a zone, all other components apart from the selected zone are grayed out.

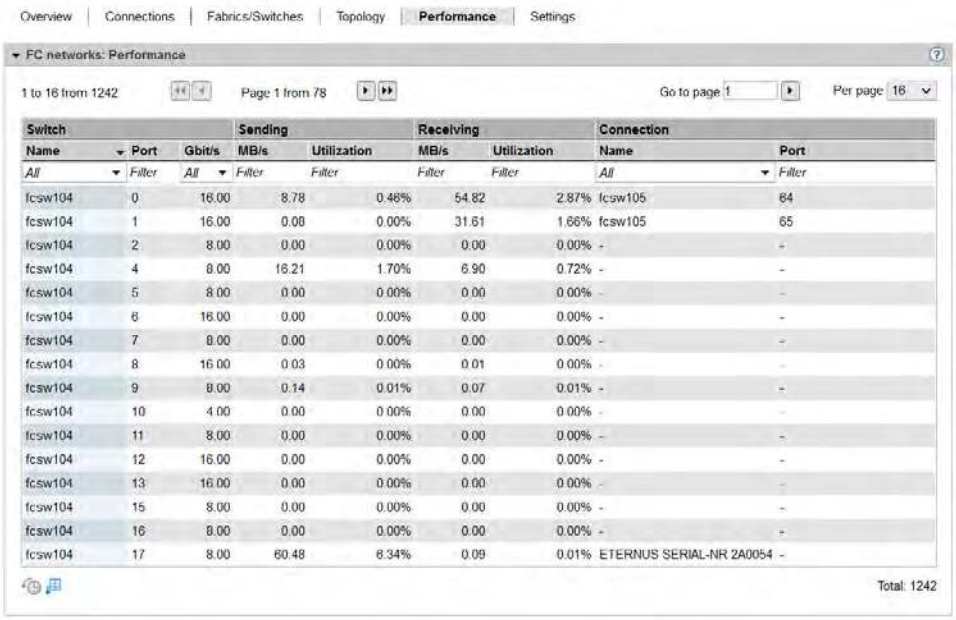
System

List of the storage systems and servers. The default is *All*, i.e. all systems are displayed. When you select a system, all switches and systems which have no connection to this system are grayed out.

10.3.4 Displaying performance

The *Performance* tab displays the performance values of the FC switches.

> Select *Hardware* -> *FC networks*, *Performance* tab.



Switch			Sending		Receiving		Connection	
Name	Port	Gbit/s	MB/s	Utilization	MB/s	Utilization	Name	Port
All	Filter	All	Filter	Filter	Filter	Filter	All	Filter
fcsw104	0	16.00	8.78	0.46%	54.82	2.87%	fcsw105	64
fcsw104	1	16.00	0.08	0.00%	31.61	1.66%	fcsw105	65
fcsw104	2	8.00	0.00	0.00%	0.00	0.00%	-	-
fcsw104	4	8.00	16.21	1.70%	6.90	0.72%	-	-
fcsw104	5	8.00	0.00	0.00%	0.00	0.00%	-	-
fcsw104	6	16.00	0.00	0.00%	0.00	0.00%	-	-
fcsw104	7	8.00	0.00	0.00%	0.00	0.00%	-	-
fcsw104	8	16.00	0.03	0.00%	0.01	0.00%	-	-
fcsw104	9	8.00	0.14	0.01%	0.07	0.01%	-	-
fcsw104	10	4.00	0.00	0.00%	0.00	0.00%	-	-
fcsw104	11	8.00	0.00	0.00%	0.00	0.00%	-	-
fcsw104	12	16.00	0.00	0.00%	0.00	0.00%	-	-
fcsw104	13	16.00	0.00	0.00%	0.00	0.00%	-	-
fcsw104	15	8.00	0.00	0.00%	0.00	0.00%	-	-
fcsw104	16	8.00	0.00	0.00%	0.00	0.00%	-	-
fcsw104	17	8.00	60.48	6.34%	0.09	0.01%	ETERNUS SERIAL-NR 2A0054	-

10.3.5 Configuring settings

In the *Settings* tab you configure the access data for the FC switches to be monitored. Prerequisite for this are the settings mentioned below.

Required settings at the FC switches

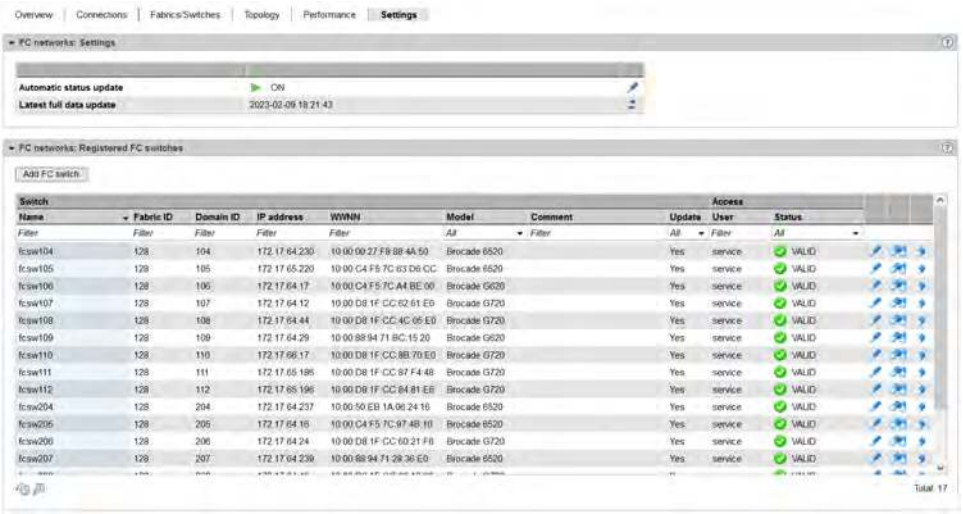
FC switches of the manufacturer Broadcom® (Brocade®) are supported. Details concerning the supported switch models and fabric OS versions are described in the support matrix (see https://bs2manuals.ts.fujitsu.com/ > Fujitsu Server BS2000 > Server Connectivity > FC-Switch).

Details of the settings can be found in the manufacturer's documentation „Brocade® Fabric OS® Administration Guide“.

- The discovery of the properties and states of switches, fabrics and ports is carried out encrypted via the Brocade REST API.
- To fulfill the requirement of access via https, SSL must be configured in the switches. In addition, the REST API must be enabled.
- To configure a switch in SEM, a user with one of the following roles is required in the switch: admin, user, switchadmin, operator, zoneadmin, fabricadmin, basicswitchadmin, securityadmin.

> Actions for changing the configuration are only available to an administrator resp. FC network administrator.

> Select *Hardware -> FC networks*, *Settings* tab.



Settings

In the *Settings* group, you can configure the data update regarding the registered switches (switch discovery) and the therefore necessary access data.

Actions:

> Activating/deactivating the automatic status update including performance data ( )

> Updating the complete FC network data including the FC network configuration ( )
This action is required after configuration changes like e.g. adding or removing a switch, configuration of disks or changes on the zoning.

Registered FC switches

In the *Registered FC switches* group, you can specify which FC switches are to be registered in SEM.

Actions:

> To add a switch to the list of registered FC switches, click *Add FC switch*. In the *Add FC switch* wizard, you can make the required entries step by step.

> To change the settings for a switch, click the *Change* ( ) icon by the desired switch, follow the instructions of the following wizard, and confirm your changes.

> To discover and add additional virtual or fabric switches for a registered FC switch, click the *Discover* ( ) icon by the desired switch.

> To remove a switch from the list of registered FC switches, click the *Remove* ( ) icon by the desired switch.

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 the management of the storage. The prerequisite for this is that the add-on pack STORMAN is installed and running.

For STORMAN versions V10.3 and higher on the local MU, the Storage Manager is directly integrated into the SE Manager. The STORMAN user interface is accessible immediately below the *Storage* menu.

For STORMAN versions older than V10.3 on the local MU the following applies:

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.

- Overview of the storage systems of the SE server configuration
- Overview over the storage systems of an MU
- Storage Manager

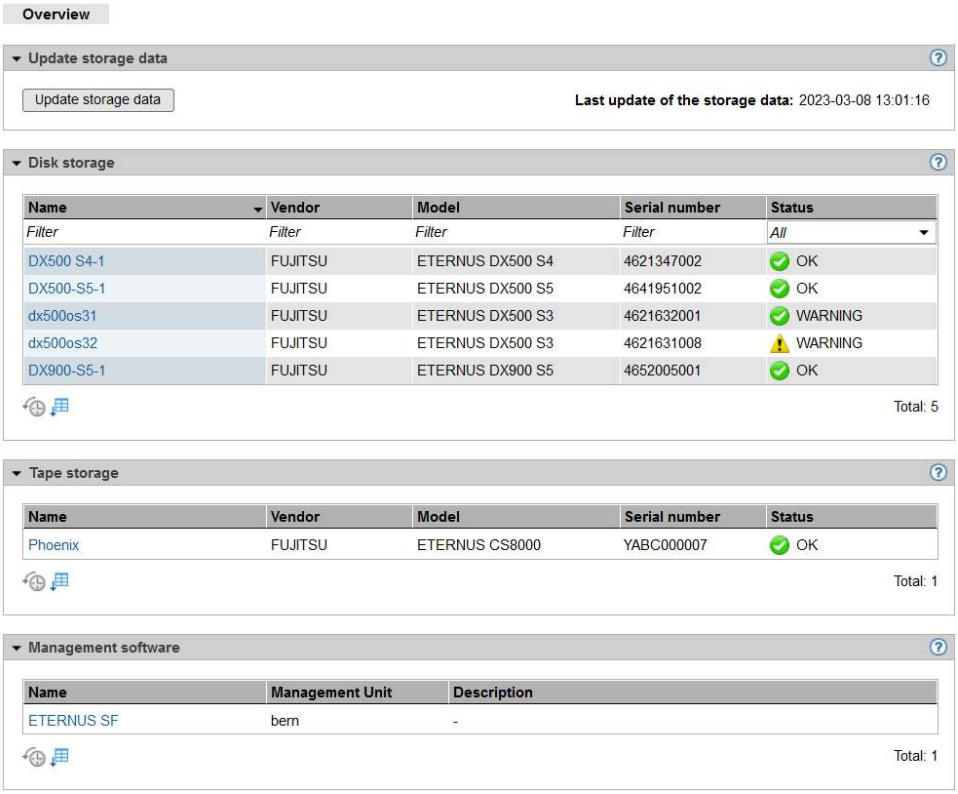
10.4.1 Overview of the storage systems of the SE server configuration

Depending on the version of the Storage Manager on the local MU, the navigation in the SE Manager differs:

For STORMAN V10.3 and higher, the Storage Manager is fully integrated in SEM. In this case, the STORMAN user interface is directly accessible in the navigation below the *Storage* menu with the *Overview* tab.

For older versions, STORMAN can be called from SEM. The *Storage Manager* tab provides access to its user interface.

> Select *Hardware* -> *Storage*, *Overview* tab.



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 the Storage Manager displays for storage systems.

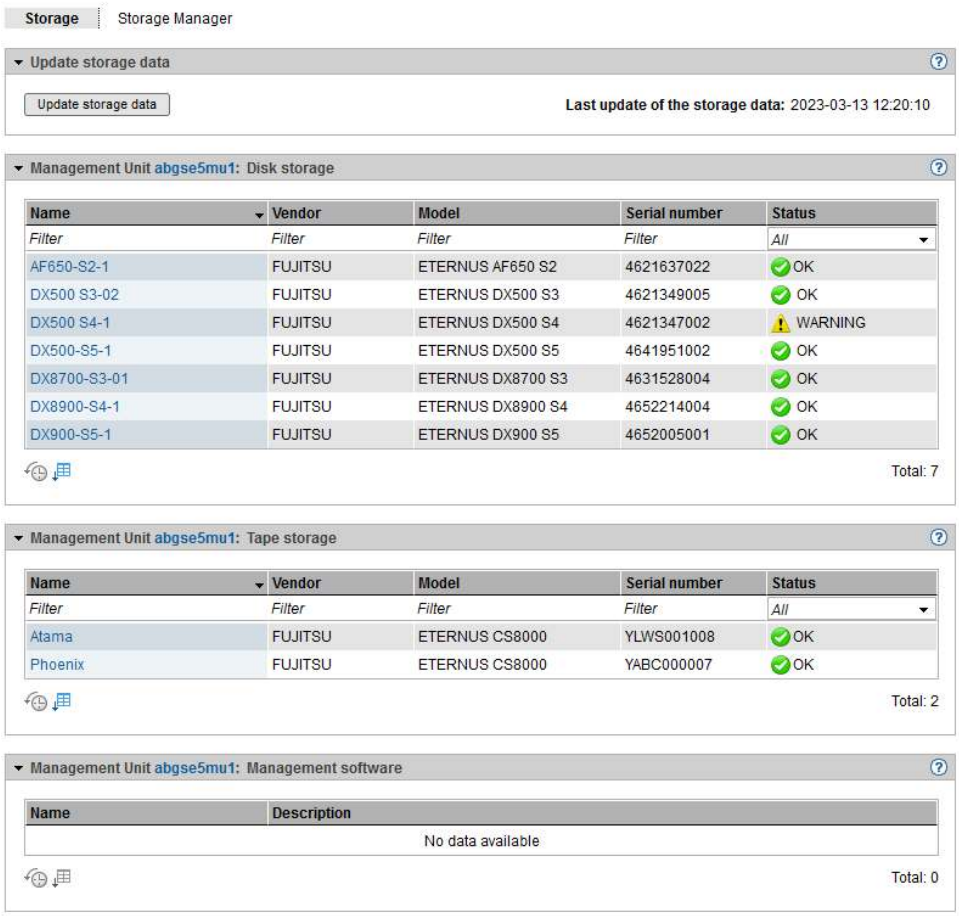
In an SE server configuration with multiple MUs, the *Overview* tab informs of the storage systems as well as the management software that the Storage Manager manages on all MUs. Storage systems which are found on more than one MU are displayed only once, namely with the worst status. A tool tip displays the status of the storage systems on the various MUs if you move the mouse over the icon in column *Status*.

10.4.2 Overview over the storage systems of an MU

This tab is only displayed, if the STORMAN version on the local MU is older than V10.3.

In this case, 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.



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

This tab is only displayed, if the STORMAN version on the local MU is older than V10.3.

In this case, you call the Storage Manager 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 the Storage Manager as authorized, the call is rejected.

In configurations with multiple MUs, switch to the GUI of the Storage Manager instance on the MU *<mu-name>*.

Further details on using the Storage Manager are provided in the online help and documentation for the Storage Manager.

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 the case of a Management Cluster, the following is added:

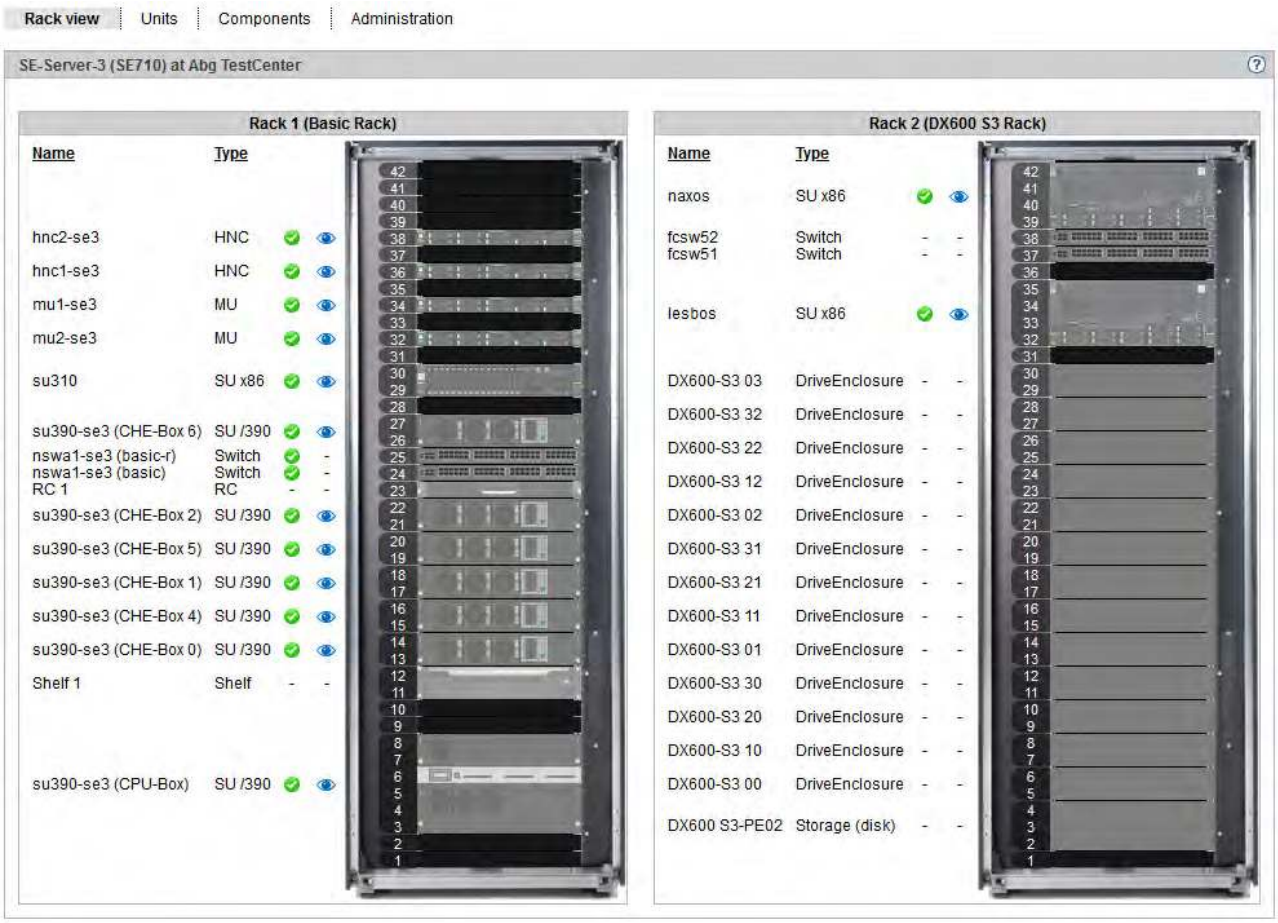
- The main window *Hardware -> HW inventory -> Units* provides an overview of all units of the entire configuration (details in the server-specific *Units* window).
- Below *Hardware -> HW inventory* a submenu *<se server> (SE<model>)* with the hardware equipment of this SE server is displayed for each 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 SE710 with two racks as an example.



The 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.

> Select *Hardware -> HW inventory* [*-> <se server> (SE<model>)*], *Units* tab.

The *Units* tab opens, here with an SE730 as an example.

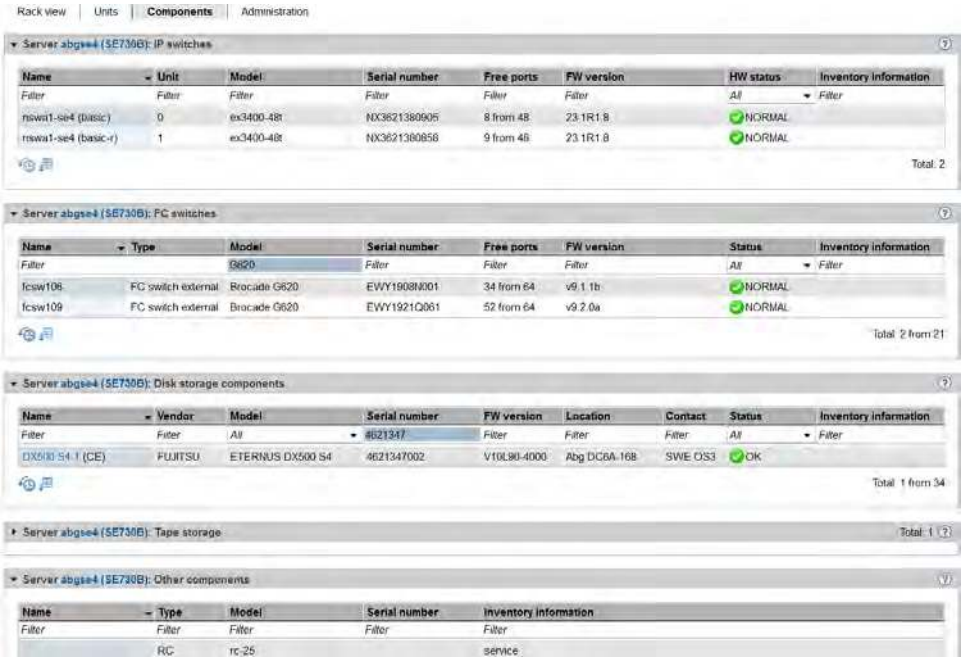
> In the case of a Management cluster, the central server-spanning main window *Hardware -> HW inventory -> Units* provides an overview of all units of the entire configuration. That main window has the same structure as the server-specific *Units* main window and contains the additional *Server* column.

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 server with an SU /390 as an example.

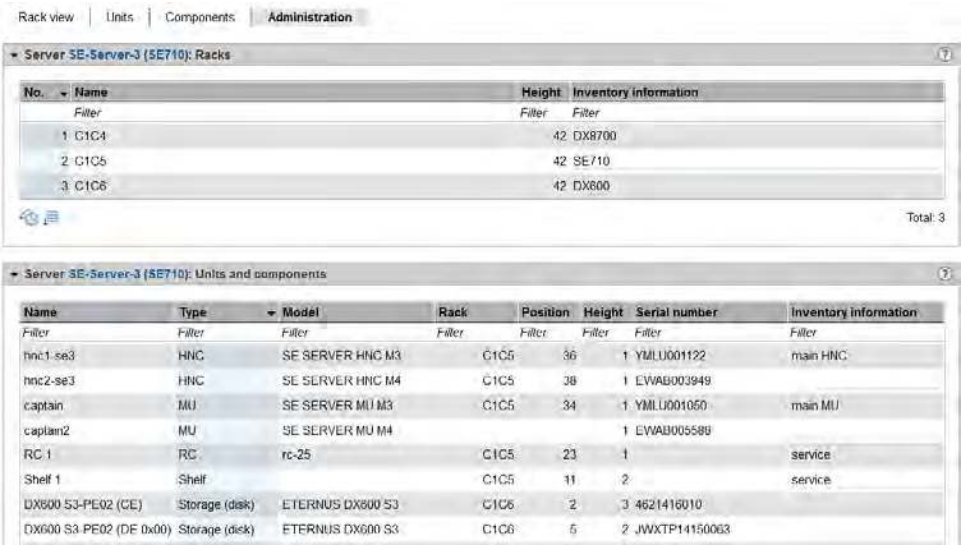


10.5.4 Administration

In the administration view all racks and hardware components are displayed in tabular form. One group is displayed for each racks and other hardware components.

> Select *Hardware -> HW inventory* [*-> <se server> (SE<model>)*], *Administration* tab.

The *Administration* tab opens, here with an SE710 as an example.



> In the *Inventory information* column you can directly enter a comment or change the existing comment.

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
- Scheduled power on/off of units of the SE server

10.6.1 Monitoring energy consumption of the units of the SE server

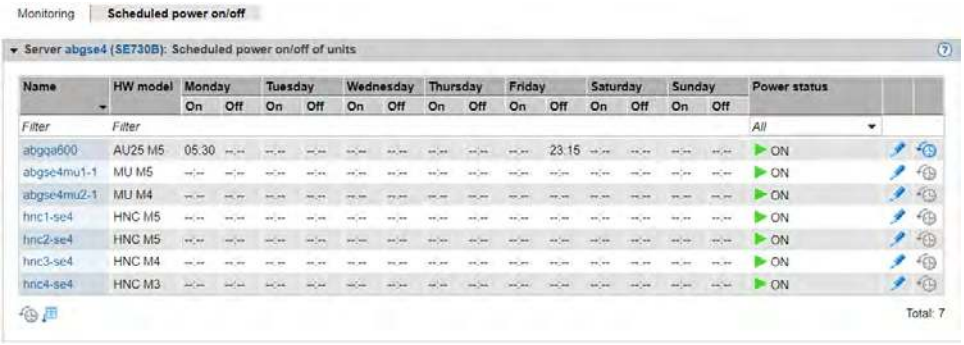
The *Monitoring* tab displays the current energy consumption, the hardware-specific maximum performance, and the power status for all units of the SE server (SU, MU, HNC, and AU).

> Select *Hardware -> Energy* [*-> <se server> (SE<model>)*], *Monitoring* tab.

Using the  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 Scheduled power on/off of units of the SE server

> Select *Hardware -> Energy* [*-> <se server> (SE<model>)*], *Scheduled power on/off* tab.



A list is displayed containing all the units of the SE server which can be powered on and off on a scheduled basis.

The power on/off times currently set and the current power status are displayed for each unit of the type MU, HNC, SU x86, and AU PY. 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

A cluster is configured by Customer Support as per the customer's request.

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 or more SE servers are always managed in a Management cluster. Depending on the configuration, there can be one or more additional SU clusters.

The *Cluster -> Overview* tab displays all clusters in the server configuration and their status.
In the *Dashboard* main menu, the *Cluster -> Overview* tile displays the status of the clusters in accumulated form, and the link branches to the *Cluster -> Overview* tab.

> In the case of a Management cluster, the displays in SEM become correspondingly more complex. Examples:
>
> - The dashboard contains another tile called *Cluster* (also in case of an SU cluster only).
> - Where necessary, tables contain a further column called *Server*, e.g. the central overviews for systems and units.
> - Where necessary, menus are split into server-specific menus, e.g. for systems and units.
>
> A detailed description of the cluster functionality is provided in the "Cluster Solutions for SE Servers" whitepaper [8].

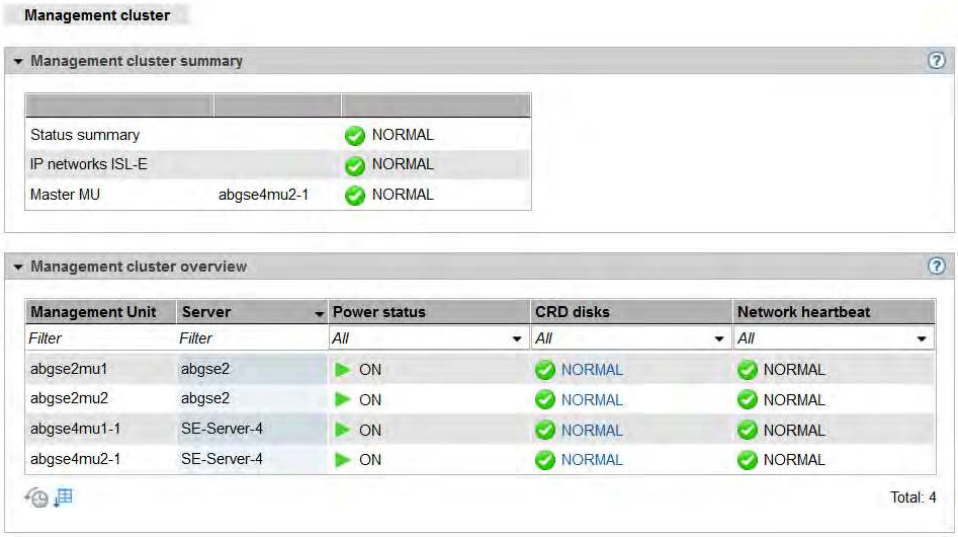
In this chapter the following further topics are briefly presented:

- Status of the Management cluster
- Managing an SU cluster

11.1 Status of the Management cluster

If an SE server configuration consists of two or more 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.



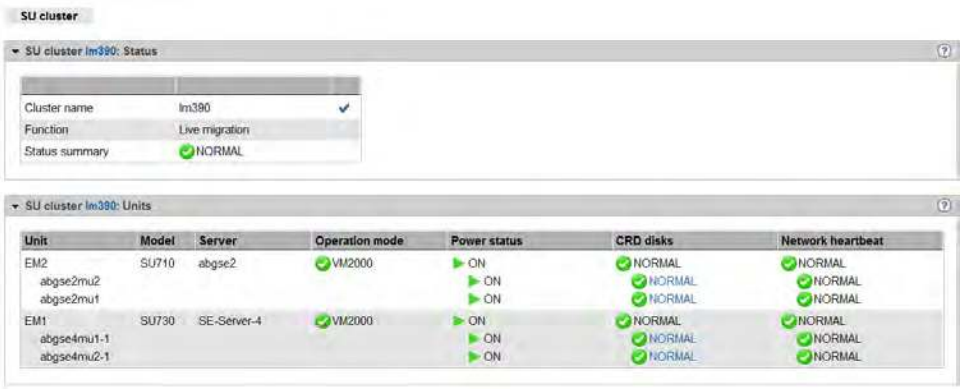
11.2 Managing an SU cluster

An SU cluster combines SUs of the same type (SU /390 or SU x86), which enable the Live Migration (LM) of 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 icon ✔ to activate or deactivate an SU cluster.

> Select *Cluster* -> <cluster-name>, *SU cluster* tab.



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

For information on managing authorizations, see the following sections:

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"). The prerequisite for this is that access to an LDAP server has been configured (see section "Access to an LDAP server").

For the administration and operation of the SE server, an administrator or security administrator can assign the following basic roles to the accounts. In addition, user-defined roles can be configured by combining basic roles (except Administrator and Service).

- Administrator
- BS2000 administrator
- BS2000 operator
- AU administrator
- Read-only administrator
- Security administrator
- Hardware administrator
- Storage administrator
- Power operator
- IP network administrator
- FC network administrator
- Shadow terminal operator
- OPENSM2 administrator and OPENSM2 information
- OPENUTM administrator, OPENUTM operator and OPENUTM information
- ROBAR administrator and ROBAR operator
- STORMAN administrator and STORMAN information
- 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".

- Managing accounts
- Managing passwords
- Managing multi-factor authentication
- Managing operator rights
- Managing sessions

12.1.1 Managing accounts

The administrator resp. security administrator manages all accounts on the SE server or the SE servers of a Management Cluster, with the exception of the service accounts. They create new accounts and change or delete 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 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 resp. security administrator you can create, modify and delete further accounts with a basic role or a user-defined role. 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".

Users who are not an administrator or security administrator are only authorized to manage their own account, i.e. they can change the access password for their local account themselves, see section "Managing passwords".

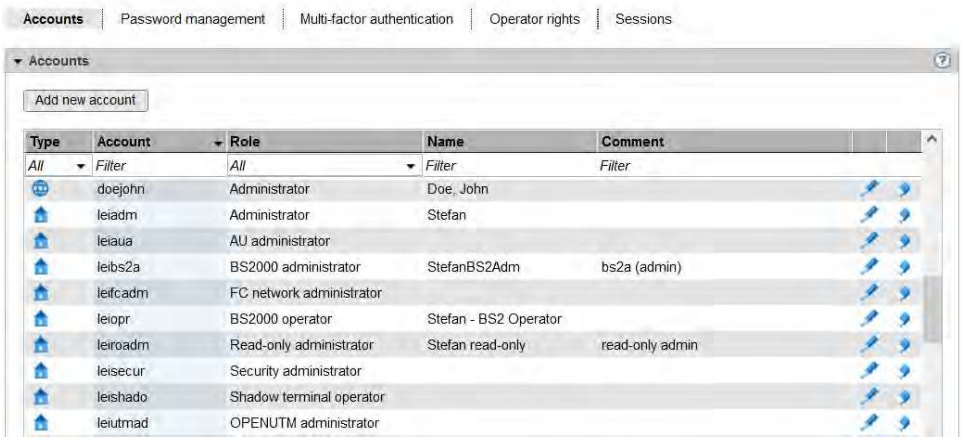
BS2000 operators obtain access to BS2000 systems and the corresponding BS2000 devices only in accordance with their individual authorizations which are assigned by the administrator resp. security administrator, see section "Managing access to the BS2000 console and dialog".

On the *Accounts* tab you can create, delete and manage accounts:

> For users who are not an administrator or security administrator, the functionality is limited to displaying their own account and changing the name and comment.

Displaying and managing accounts

> Select *Authorizations -> Users, Accounts* tab.



An administrator or security 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. Users with another role see only their 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 it.

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 on which the LDAP account is to be released, access to the LDAP server is configured and active (see section "Access to an LDAP server").
- 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 *AU administrator* role only if at least one AU exists in the SE server configuration.

Change an account

You can change the *Name* and *Comment* properties of an account.

> ¡ For users who are not an administrator or security administrator, the functionality is restricted to their own account.

> In the row of the required account click the *Change* icon and change the required account properties.

Remove an account

> ¡ Every user with the *Administrator* or *Security 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

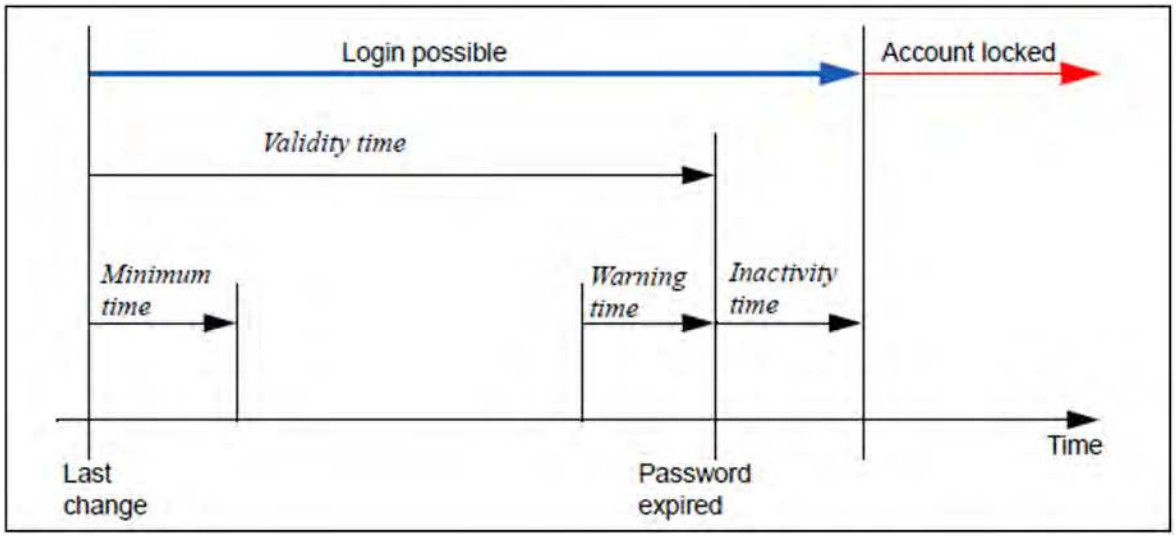
In the *Password management* tab you manage the passwords of all defined local accounts.

> 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 or security administrator, users with another role 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) administrator resp. security administrator 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

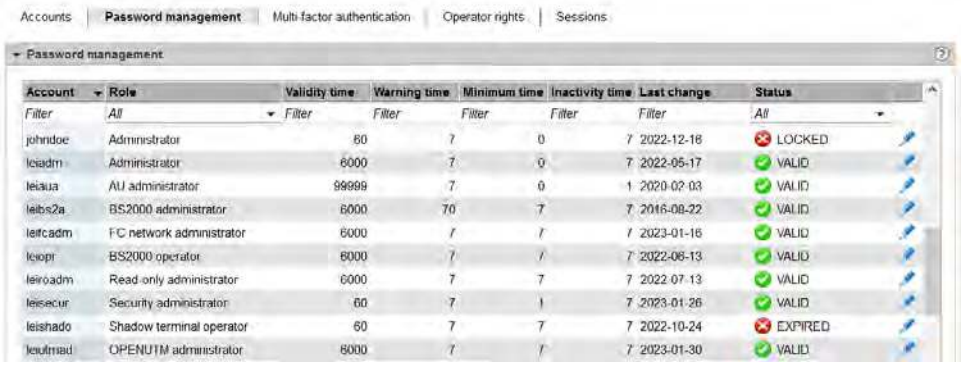
The minimum time is not relevant for an administrator resp. security administrator account and the value 0 is therefore displayed for it.

As administrator or security 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 *Password management* tab displays the defined local accounts with their password attributes.

Changing passwords or password attributes

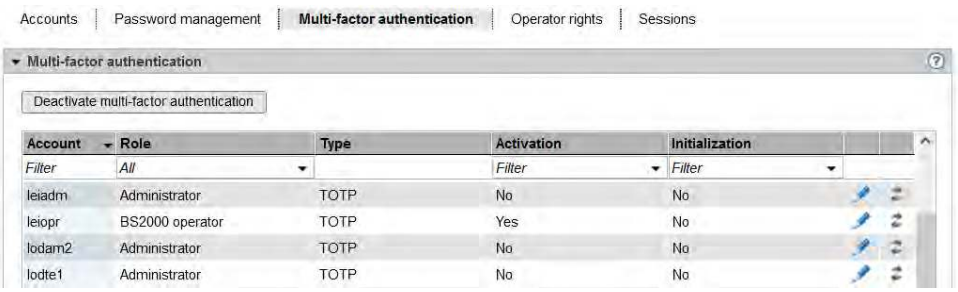
> For users who are not an administrator or security administrator, the functionality is restricted to their own account: They can change their own password if it has not yet expired and the minimum time between two changes has been reached.
> Only an administrator or security administrator can change 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 multi-factor authentication

The *Multi-factor authentication* tab shows for which accounts multi-factor authentication (MFA) is configured and allows to activate and deactivate MFA in general and for individual accounts.

> Select *Authorizations -> Users*, *Multi-factor authenticaton* tab.



The *Multi-factor authentication* tab displays - only if MFA is activated generally - all accounts with their respective MFA configuration.
For users who are not an administrator or security administrator, the functionality is restricted to their own account.

Activate/Deactivate multi-factor authentication generally

> Administrator or Security administrator only: Click the *Activate/Deactivate multi-factor authentication* button above the table and confirm the action to activate resp. deactivate MFA in general.

> After the general activation of MFA, it is initially inactive for all accounts and must then be activated for the desired accounts.

(De)activate MFA for an account

> Administrator or Security administrator only: Click the *Activate/Deactivate MFA* icon ( ) at the desired account and confirm the action in order to activate resp. deactivate MFA for the account.

Renew MFA secret

> Only for accounts with MFA initialized: Click the *Renew MFA secret* icon ( ) at the desired account and confirm the action in order to create a new MFA secret for the account.

12.1.4 Managing operator rights

The *Operator rights* tab displays all BS2000 operator accounts (local accounts and LDAP accounts with the *BS2000 operator* role) and their current individual rights.

The tab is not available to users who are not an administrator, security administrator or BS2000 operator.
For BS2000 operators the functionality is restricted to their own account. They only see their own rights. Only an administrator or security administrator can make changes.

> Select *Authorizations -> Users*, *Operator rights* tab.

The *Operator rights* tab lists all BS2000 operator accounts, including accounts whose user-defined role includes the *BS2000 operator* role, together with their individual rights.

Changing operator rights

> ¡ Only an administrator or security administrator can make changes.

> Click on the *Change operator rights* icon by the desired account. Assign the desired rights for the BS2000 operator in the following dialog.

Managing access to the BS2000 console and dialog

A BS2000 operator can access the console of a BS2000 system solely by means of individual rights.

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 resp. BS2000 administrator can always access the BS2000 consoles and the BS2000 dialog. BS2000 operators can only access BS2000 consoles and BS2000 dialogs for which they have an individual right.

12.1.5 Managing sessions

The *Sessions* tab informs the administrator resp. security 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.

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.

Delete session

> Deleting your own session is not possible.

> Click the *Delete* icon by the required session and confirm the action.

12.2 Roles

An administrator or security administrator can create and manage user-defined roles in the *Authorizations -> Roles* menu.

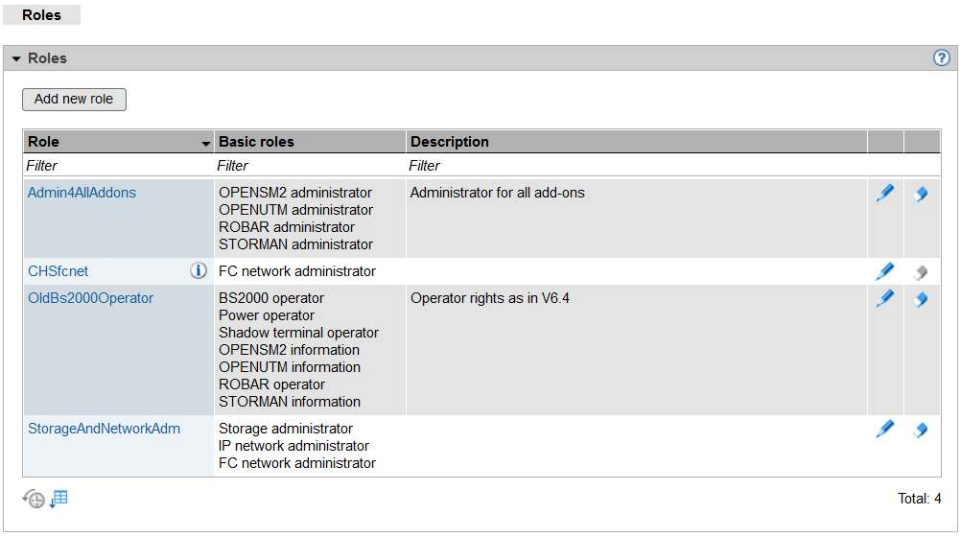
A user-defined role is a combination of predefined basic roles under a freely definable name.

The following basic roles are available for the configuration of a user-defined role:

- BS2000 administrator
- BS2000 operator
- AU administrator
- Read-only administrator
- Security administrator
- Hardware administrator
- Storage administrator
- Power operator
- IP network administrator
- FC network administrator
- Shadow terminal operator
- Add-on-specific roles
  - OPENSM2 administrator and OPENSM2 information
  - OPENUTM administrator, OPENUTM operator and OPENUTM information
  - ROBAR administrator and ROBAR operator
  - STORMAN administrator and STORMAN information

Detailed information on the various roles is provided in section "Role and user strategy".

> Select *Authorizations -> Roles, Roles* tab.



The *Roles* table displays all configured user-defined roles.

The following actions are available:

Add new role

> Select *Add new role*.

> In the following dialog, provide a name and optionally a description for the new role and select the basic roles it shall comprise.

Change a role

You can change the *Basic roles* and the *Description* of a role.

> If the role is currently assigned to an account, its basic roles cannot be changed.

> In the row of the required role click the *Change* icon ( ) and change the role's properties in the following dialog.

Remove a role

> Click the *Remove* icon ( ) by the required role and confirm the action.

12.3 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.

- Access to an LDAP server
- IP-based access restriction to the MUs

12.3.1 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.
>
> The explicitly configured port for the LDAP protocol (default 389 resp. in case of communication secured by LDAPS 636) as well as ports 88 and 750 for the Kerberos protocol must be open in the firewall to allow communication with the LDAP 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 all SE servers together (i.e. all 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 all 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.

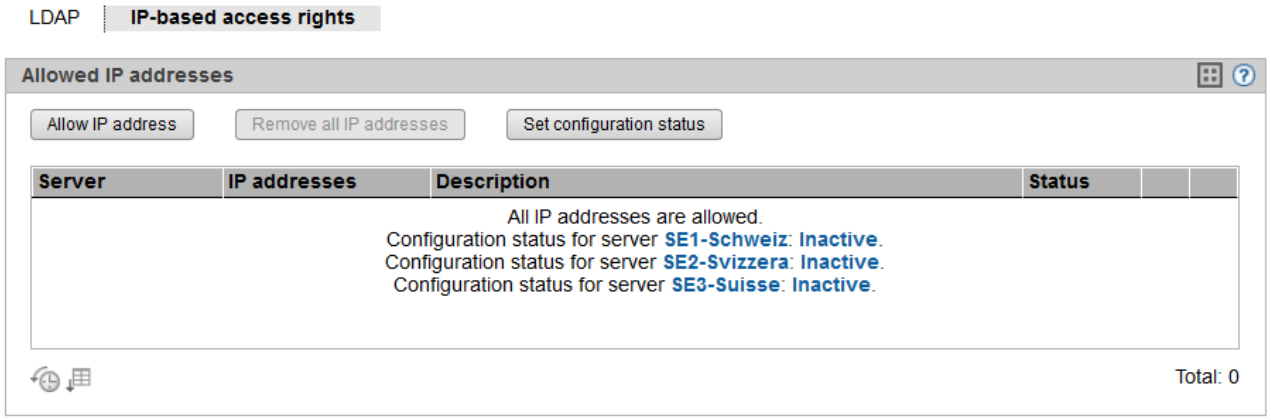
Delete LDAP configuration

> 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.

12.3.2 IP-based access restriction to the MUs

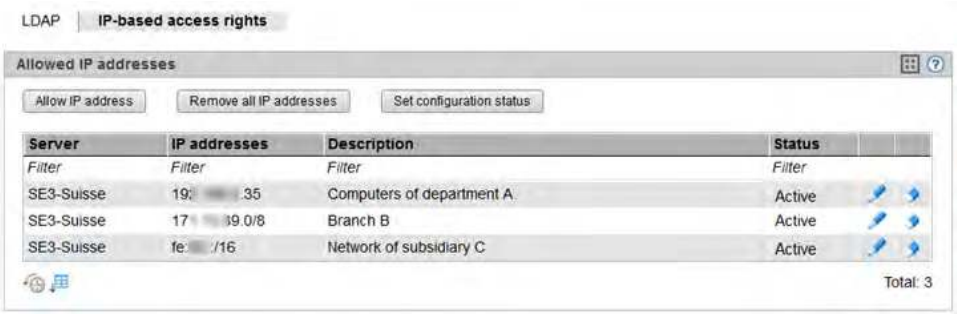
An administrator or security administrator can configure the access to the MUs (applies for access via SE Manager and CLI) of the SE server in such a manner that it is possible only for explicitly configured IP addresses or for IP addresses from an explicitly configured IP network.

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>*]

You also have the option of entering a description for the allowed access, such as usage or the contact details of the responsible administrator.
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*.

> **i** 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 all IP addresses

> Click *Remove all IP addresses* and in the subsequent dialog box select either an SE server, for which all IP addresses are to be removed, or choose *All* to remove the IP addresses for all SE servers. Thereby unrestricted access to all associated Management Units is possible.

Set configuration status

> Click *Set configuration status* and in the subsequent dialog box determine for each SE server, whether the IP-based access rights should be active or inactive. Only with active IP-based access rights, access to the associated Management Units will be restricted.

Modify the description for the allowed IP address

> By the required IP address or network, click the *Change* icon and enter a description, such as usage or the contact details of the responsible administrator.

Remove IP address or network

> By the required IP address or network, click the *Remove* icon and confirm the action.

> **i** 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.

12.4 Certificates

The handling of certificates is described in the following sections:

- SSL certificate
  - Confirming/importing a certificate in the web browser
- Managing certificates
  - Using the standard certificate
  - Creating and enabling a new self-signed SSL certificate
  - Requesting an SSL certificate
  - Uploading and activating a customer-specific certificate

12.4.1 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.

12.4.1.1 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.

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.

> ℹ You have to explicitly select "Trusted root certification authorities" as certificate memory (for details, see "Security Manual" [7]).

Alternatively or for other browsers, you can also download and install the CA certificate, see "Uploading and activating a customer-specific certificate".

12.4.2 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)*.

12.4.2.1 Using the standard certificate

A self-signed, system-specific certificate is preinstalled for each MU 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 there does not know the certificate, either.

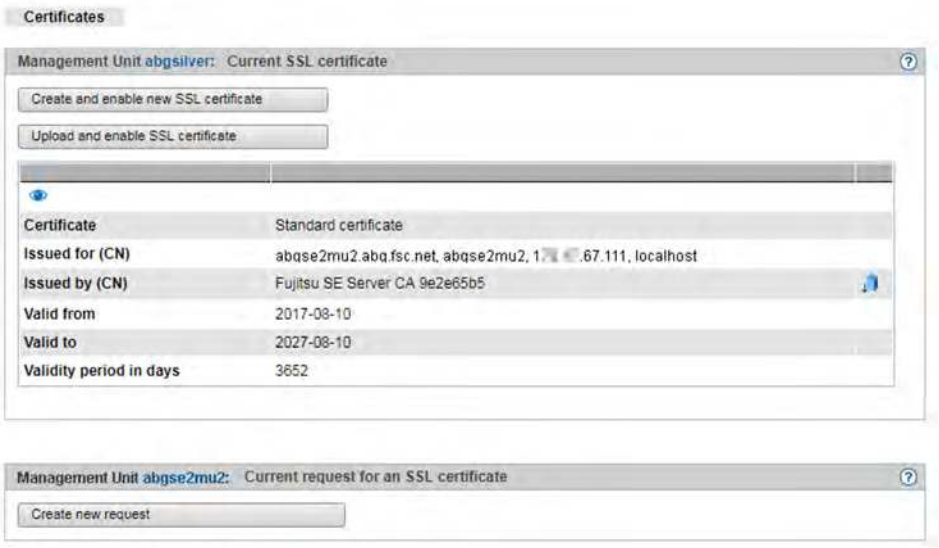
You are granted access to the SE Manager of the system only if the certificate is temporarily accepted or permanently imported.

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.



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.

12.4.2.2 Creating and enabling a new self-signed SSL certificate

The preinstalled standard certificate contains data which is of course 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").

> 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.

12.4.2.3 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".

When the signed certificate is returned to you, enter the certificate in the system: see the "Uploading and activating a customer-specific certificate" and "Using the standard certificate" sections.

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* icon.

The file with the current request for the SSL certificate is downloaded in the browser.

12.4.2.4 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") 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").

> 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: certificate and optionally key and CA certificate. 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 CA certificate currently installed on the Management Unit 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 the logging

The *Logging* menu comprises the functions for central management of the audit logging and event logging and the configuration of the alarm management of the SE server configuration.

- Displaying audit logging
- Displaying event logging
- Alarm management

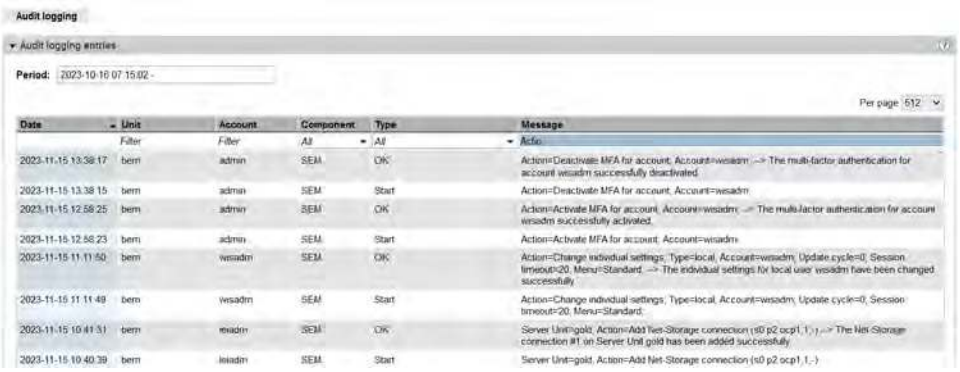
> In a multi-MU configuration, the following must be observed when displaying audit logging records and events on an MU:
>
> In normal operation, the displayed entries are the same at each MU.
>
> However, if an MU is not available during the generation of an entry (e.g. switched off), the entry cannot 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, security administrator or read-only administrator to trace at all times who performed which action and when.

> Select *Logging* -> *Audit logging*, *Audit logging* tab.



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

> ℹ 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* tabs.

> The dashboard of the SE Manager contains the *Events* tile, on which the number of currently not yet acknowledged 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.

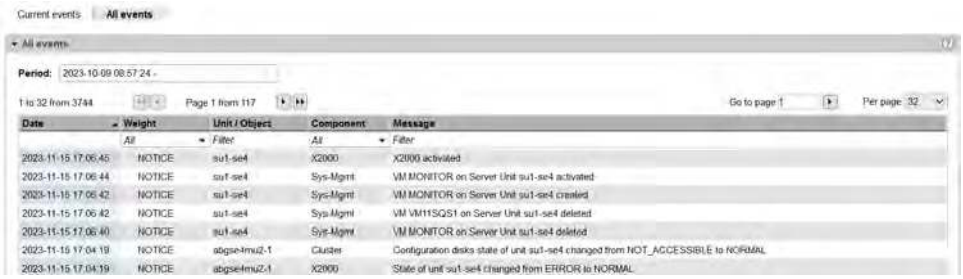
The *Current events* tab contains a list of all events that occurred since events have been acknowledged the last time. You can only acknowledge the events of the whole table:

> Click on the *Acknowledge current events* button 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.



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 date 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 dates are consistent, it is required that all units (MU, SU x86, HNC etc.) are synchronized with an NTP server.
> See also section "NTP server".

To restrict the number of displayed results, you can filter by the following criteria:

- Weight of the event (e.g. WARNING, ERROR or CRITICAL)
- Name of the unit on which the message was issued
- Component that issued the warning (e.g. M2000, HNC, X2000, ResMon, Sys-Mgmt, Cluster, RemSrv or the 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 "General information".

> Generally all events with weight >=WARNING generate a teleservice call. The following exceptions from this rule apply:
> Events of the add-on packs OPENSM2, ROBAR, SEHAMONITOR and STORMAN do not generate teleservice calls. The add-on pack OPENUTM at present doesn't create events.

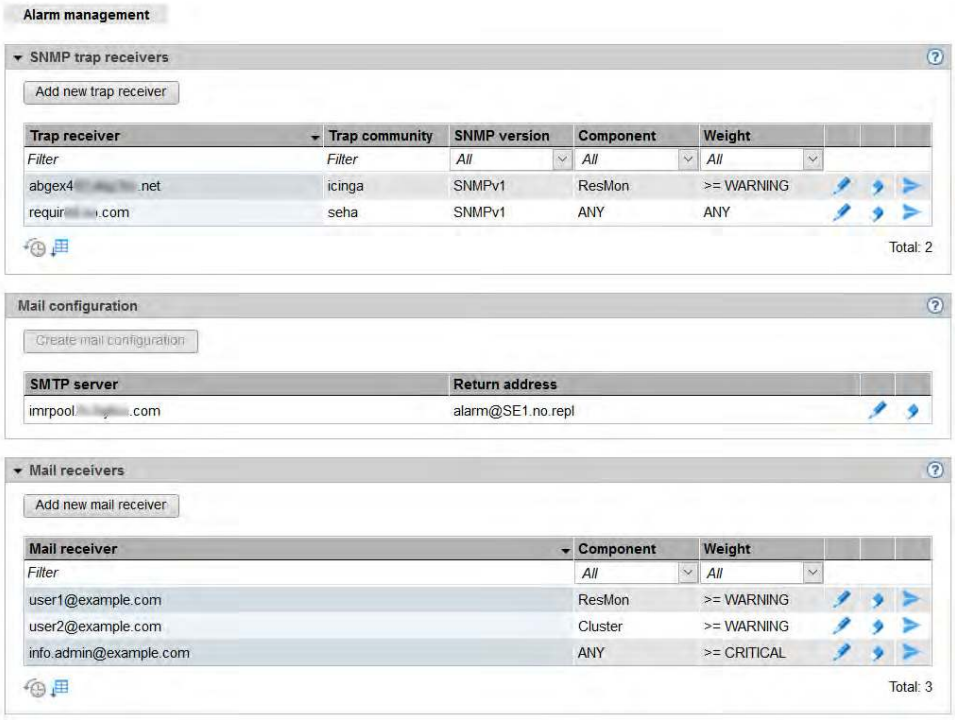
13.3 Alarm management

As administrator or security 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.



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:

- Sender: Contains the return address as configured in the *Mail configuration* group and the name of the reporting Management Unit
- 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 *General information -> List of possible 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 receivers* group, click the *Add new trap receiver* button and in the subsequent dialog, enter the required information for the trap receiver.
Define the component for which a notification is to be made and the threshold weight of the events, starting from which a notification is to be made for this component, and confirm the action.
If a receiver is to receive notifications for several components, several entries may have to be created for them.

Change the properties of an SNMP trap receiver

> In the *SNMP trap receivers* 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 receivers* 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 receivers* 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* group, click the *Change* icon. Modify the required properties and confirm the action.

Delete mail configuration

> In the *Mail configuration* group click the *Remove* icon by the entered SMTP server and confirm the action.

Add a new e-mail receiver

> In the *Mail receivers* group, click the *Add new mail receiver* button and in the subsequent dialog enter the e-mail address of the receiver.
Define the component for which a notification is to be made and the threshold weight of the events, starting from which a notification is to be made for this component, and confirm the action.
If a receiver is to receive notifications for several components, several entries may have to be created for them.

Change the properties of an e-mail receiver

> In the *Mail receivers* group click the *Change* icon by the required receiver. Modify the weight and confirm the action.

Remove an e-mail receiver from the list

> In the *Mail receivers* 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 receivers* group click the *Test* icon by the required receiver and confirm the action.

14 Managing service-related functions

The *Service* main menu comprises the menus *Information, Configuration, Remote service sessions* and *Units*.

The *Information* menu contains displays and functions that the customer needs when communicating with the Service Center for configuration changes, maintenance, or troubleshooting. Furthermore, the SE operation state can be changed and an information to be displayed in the SE Manager's header area can be configured here.

The *Configuration* menu allows to configure the remote access for service technicians on the *Remote service access* tab.

The *Remote Service Sessions* menu displays on the *Sessions and files* tab the current AIS Connect sessions and existing AIS Connect logging files and allows to delete and download logging files.

The *Units* menu provides you for each Management Unit, HNC and Server Unit x86 of the SE server configuration in a unit-specific menu with diagnostics and maintenance functions as well as functions for the administration of updates and (MU only) of the remote maintenance via AIS Connect.

14.1 Information

The *Information* tab displays data that the customer needs when communicating with the Service Center.
In addition, the SE operation state and an information to be displayed in the SE Manager's header area can be configured here.

Customer ID

The *SE Server: Customer ID* group displays the customer ID or in case of a Management cluster the customer IDs.
Using the customer ID, the customer data – configurations and contracts – can be quickly and uniquely identified in the Service Center..

SE operation state / Maintenance state

In the SE operating state group, an administrator can configure the operating state and an information that is displayed in the header area of the SE Manager of all main windows.
This way, all users are informed about current conditions or warned about special conditions.

Particularly noteworthy here is the so-called maintenance state:
This can and should be used during the execution of maintenance work to make all users aware of the current special situation:

- The maintenance state is displayed in red in the header of each main window, dialog, wizard, etc.
- In SEMVT, before the actual functionality is called, "Be aware of the SE operation state! State maintenance ..." is displayed for a few seconds.

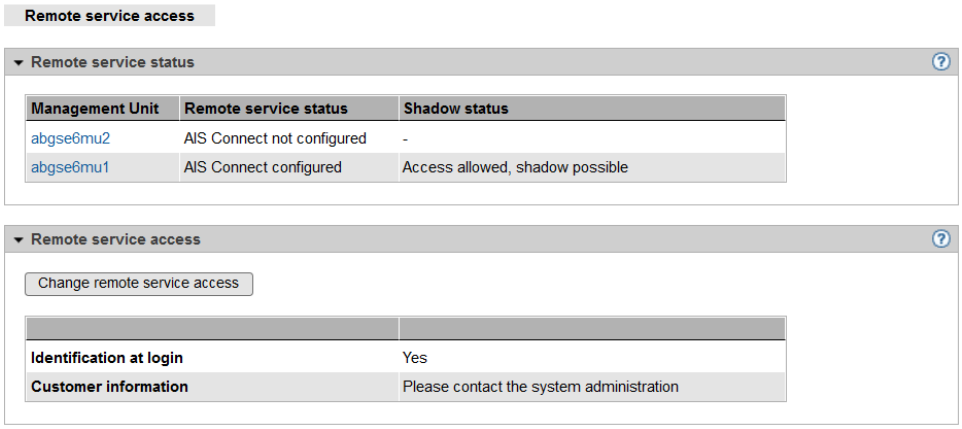
> **Service consultation**
>
> The timing of setting or leaving/resetting the maintenance state should be agreed in consultation with the Customer Service performing this work.

> **Events and teleservice calls**
>
> Each time the operating state is changed, an event is generated which can be forwarded to all registered users via alarm.
> Setting or leaving/resetting the maintenance state is also reported to the service center.

14.2 Remote service access

On the *Remote service access* tab the status of the AIS configuration is displayed and the customer can configure if service technicians have to identify themselves when establishing a remote connection, and which customer-specific information is displayed to a service technician after login.

> In the tree structure select *Service -> Configuration*.



The *Remote service access* tab opens. It contains the two groups *Remote service status* and *Remote service access*.

The *Remote service status* group displays in a table the status of the AIS configuration for each MU.

The *Remote service access* group displays the current configuration: *Identification at login* with the possible values *Yes* or *No* and the configured *Customer information*.

If identification at login is required, service technicians have to specify their name as well as a disruption number and a description when establishing a remote connection, otherwise access will be denied.

A customer information, e.g. names and telephone numbers of administrators or other persons responsible at the customer, is optional and is displayed to the service technician after login.

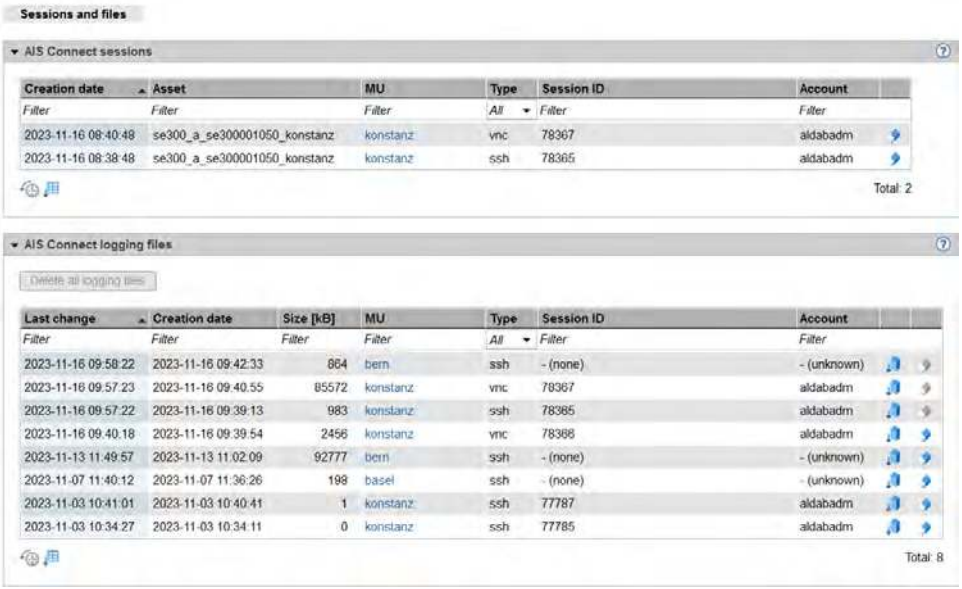
The *Change remote service access* button opens a dialog box which allows to change the configuration.

14.3 Remote service sessions

The *Sessions and files* tab in the *Remote service sessions* menu displays the currently active AIS Connect sessions and in a second table the existing AIS Connect logging files. The information displayed is cross-MU, i.e. it concerns all Management Units of the SE administration area.

The first table is displayed only if at least one direct connection to AIS Connect exists.

> In the tree structure select *Service -> Remote service sessions*.



The *Sessions and files* tab opens. The *AIS Connect sessions* table displays the currently active sessions.

As an administrator or security administrator you can delete a session by clicking the *Delete* ( ) icon for the required session.

The *AIS Connect logging files* table displays the existing logging files.

By clicking *Delete all logging files* you as an administrator can delete all logging files at once.

Clicking the *Download* ( ) icon by the required logging file downloads it to the local PC.

Clicking the *Delete* ( ) icon by the required logging file deletes it after confirmation.

Both functions are also only available to an administrator.

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: logging files with *.flv suffix

Alternatively to using the SE Manager, you can also list and delete the logging files using the `aisLog` command. You can also view the logging files of SSH sessions with `aisLog`. You may 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".

> 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 to your PC (e.g. with `scp` under an administrator account). The tool VLC media player can be used for viewing.

14.4 Units

The *Units* menu provides you for each Management Unit, HNC and Server Unit x86 of the SE server configuration in a unit-specific menu with diagnostics and maintenance functions as well as functions for the administration of updates and (MU only) of the remote maintenance via AIS Connect.

In the case of a single SE server, the menu is displayed as *Units (SE<model>)*.

When multiple SE servers are operated in a Management Cluster, a server-specific menu *<server-name> (SE<model>)*, which ranks above the unit-specific menus of the associated units, exists in the *Units* menu for each SE server.

14.4.1 Managing updates

Fundamental information on updates is provided in section "Customer Support and maintenance".

The administrator uses the *Update* tab to manage updates for the unit (MU, SU x86 or HNC).

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

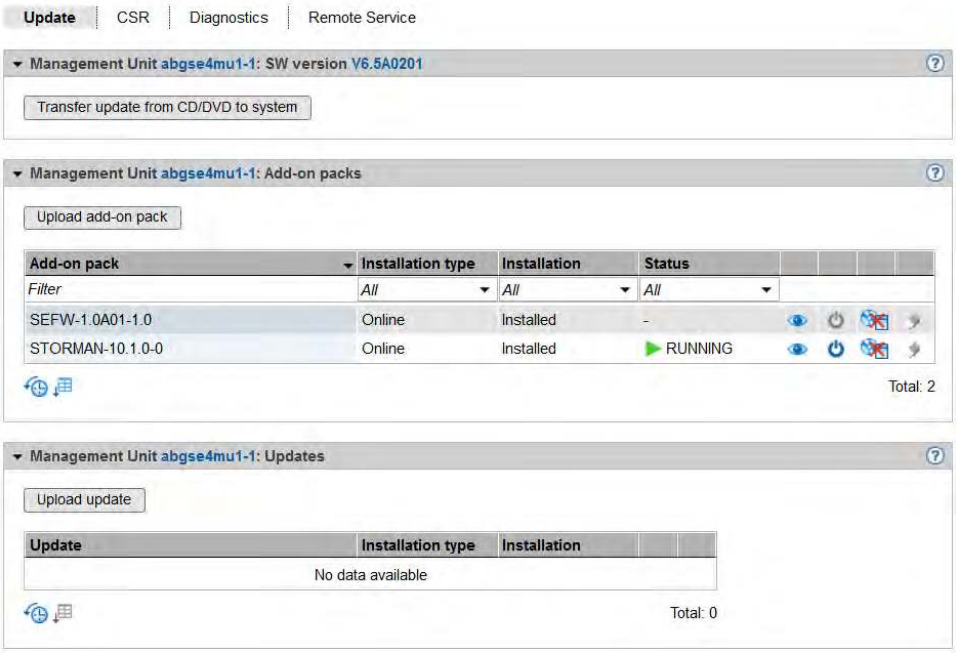
- Add-on packs enhance the basic software and are functional software components which have their own version schema. Add-on packs exist only for Management Units.
- Updates solve customer-specific problems.

Updates (for an MU also add-on packs) 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" and section "Tasks of the customer"):

- 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 installed by Customer Support.

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

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



When the group is collapsed, 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 (for Management Units only)
  Administrators 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 administrator can manually change the status of the add-on pack via the *Change add-on status* icon ( ) (e.g. Start, Stop, Restart, Reload).
- *Updates* group
  An administrator can upload updates.
  They can delete updates which have not been installed or their installation sources. Only Customer Support can install updates (see section "Tasks of Customer Support" and section "Tasks of the customer").

14.4.2 Managing configuration data (CSR) of the MU

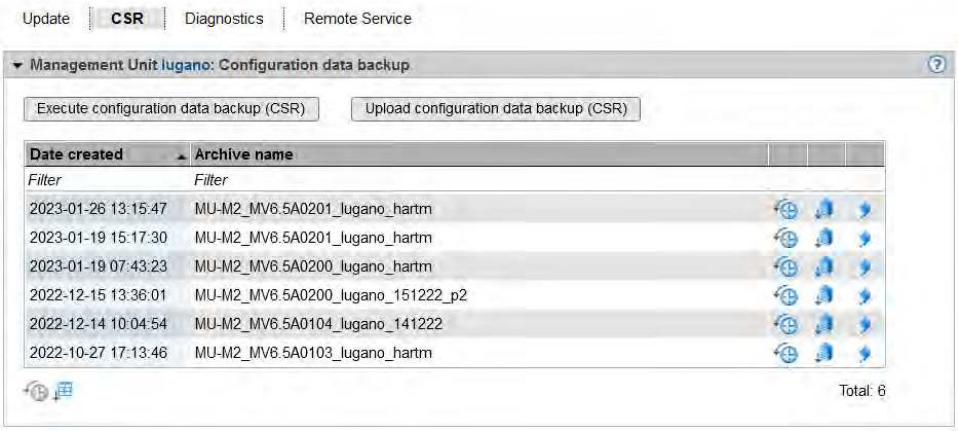
You use a CSR backup (CSR = Configuration Save and Restore) to back up the configuration data of the unit in an archive. A CSR backup allows the configuration of the unit at the time of the backup to be restored later. Each backup archive has a creation date and an archive name.

The backup archive contains the complete configuration of the basic system, e.g. the devices and for SU x86 and HNC the Net-Storage configuration, as well as for an MU all other configuration data that are managed via the SE Manager. For an MU 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, for a Management Unit there is a difference between MU-specific and MU-global data (see the **Important information** under "Restoring configuration data from a file archive").

You manage the configuration data of the unit using the associated unit menu, *CSR* tab.

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



The following options are available to you:

Executing configuration data backup for the unit

> Click *Execute configuration data backup (CSR)* and confirm the action after selecting a file archive for configuration data backup.

Uploading configuration data backup to the unit

> 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 configuration data backup for the unit

> To download the file archive, click the *Download* icon ( ) in the row with the required file archive, if necessary 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 unit

> 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 an archive file

> Click the *Restore* icon ( ) in the row with the required archive file and confirm the action. If the Customer Support staff has already prepared restoration, the action is rejected with a message to this effect.

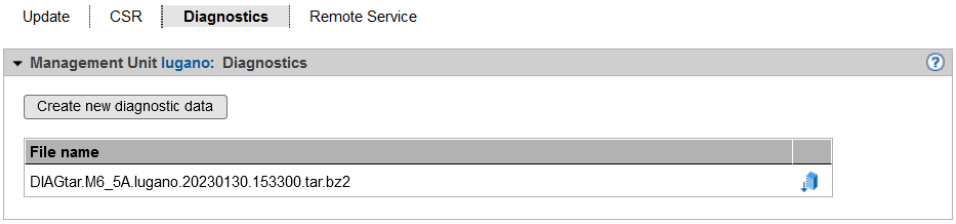
> ! Restoration leads to the unit being rebooted immediately.

> ¡ **Important information** (for Management Units)
>
> - 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 missing MU-global data available in the CSR backup 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.

14.4.3 Generating diagnostic data

To support error diagnosis by Customer Support, an administrator, BS2000 administrator or BS2000 operator can generate diagnostic data when an error situation occurs and send this to the Support Center.

> Select *Service -> Units ->* [*<se server> (SE<model>) ->*] *<unit> (<unit-type>)*, *Diagnostics* tab.



An already existing diagnostic data file 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. For an MU the name has the following format:

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

For SU x86, the name starts with the prefix `DIAGtar.X`, for HNC with `DIAGtar.H`. Otherwise, the format is the same as for MU.

As administrator, BS2000 administrator or BS2000 operator, 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.

> **Note**
>
> When communicating with the Support Center please specify the customer ID of your SE server. See for this also chapter "Tasks of the customer".

14.4.4 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 teleservice 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 for connection via a gateway.

Service accounts

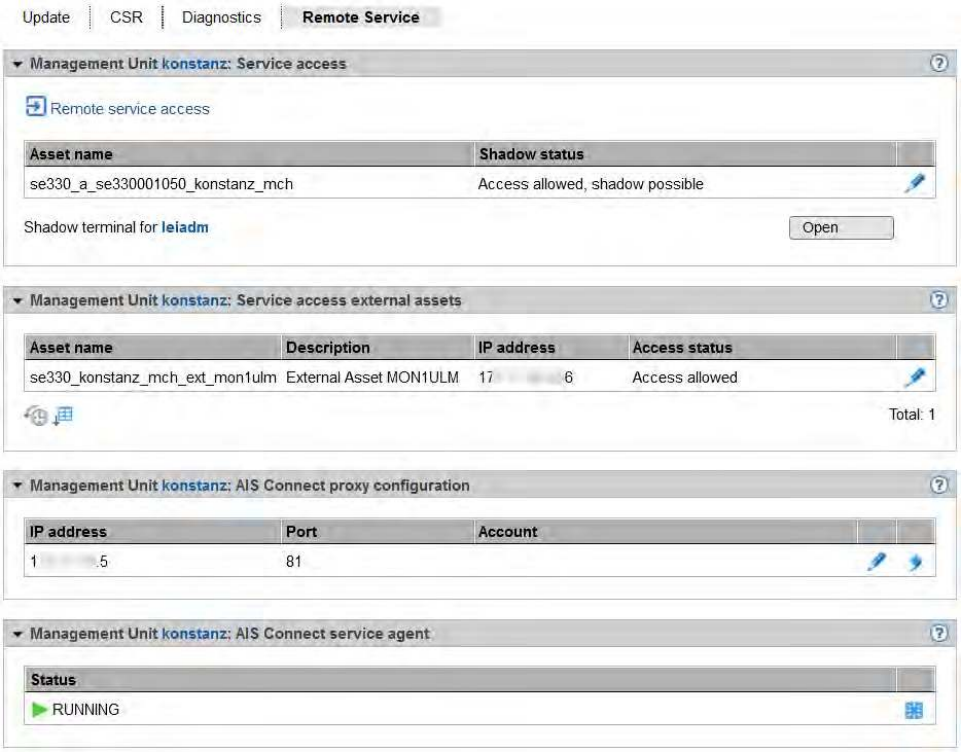
To perform its work, Customer Support logs in (remotely via Teleservice or locally) under the service account provided for this purpose. On the units the protected account *service* is available to Customer Support in the operating system.

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

The *Remote Service* tab displays the groups *Service access*, *Service access external assets* (if at least one service access to an external assets is configured), *AIS Connect proxy configuration* (only for a directly connected MU), *AIS Connect gateway* (only for connection via a gateway) and *AIS Connect service agent*.



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 Add-on administrators, the whole main window is not displayed.
- BS2000 administrators can operate the shadow terminal.
- Operators can only operate the shadow terminal if they have 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 <pid_1>.<pid_2>.<pid_3> after you have logged in on the shadow terminal.

> Enter the `screen -x <pid1>.<pid2>.<pid3>` command to establish a connection to this AIS Connect session.

> Enter `screen -ls` to display open sessions.

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.

AIS Connect gateway

The group displays - only if the AIS Connect access is carried out via a gateway - the IP address of the gateway and in case given the name of the AIS Connect box.

Rebooting a service agent

> In the *AIS Connect Service agent* group click the *Restart* icon and confirm the action.

15 Appendix

The sections below describe the alternative BS2000 operation using PuTTY.

15.1 Operating BS2000 with PuTTY

Users with the roles *Administrator*, *BS2000 administrator* or *BS2000 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 with the role *Administrator*, *BS2000 administrator* or *BS2000 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.

  > ℹ 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.

  An 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 *General information -> PDF documents*.

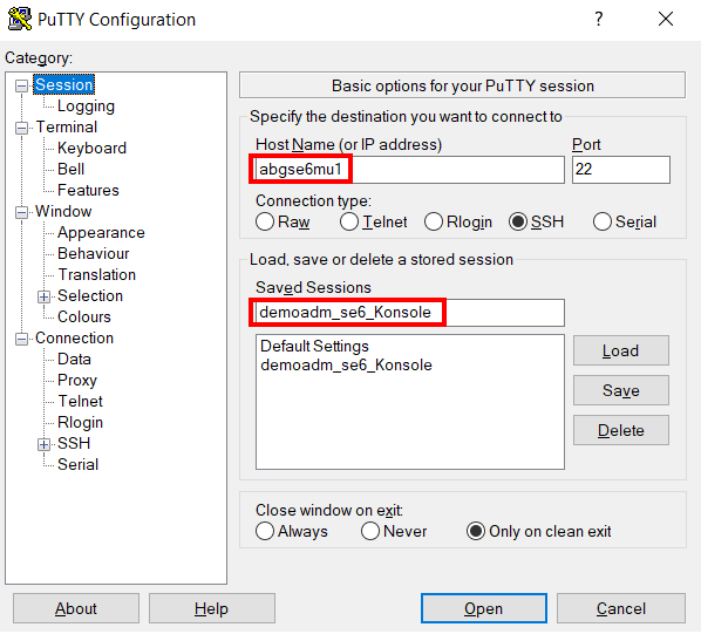
Notes on PuTTY

- 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

The following sections describe the BS2000 operation with PuTTY in more detail. Some screenshots still show M2000 version V6.2A. The described procedure, however, also applies to newer M2000 versions.

15.1.1 BS2000 console on MU or SU /390

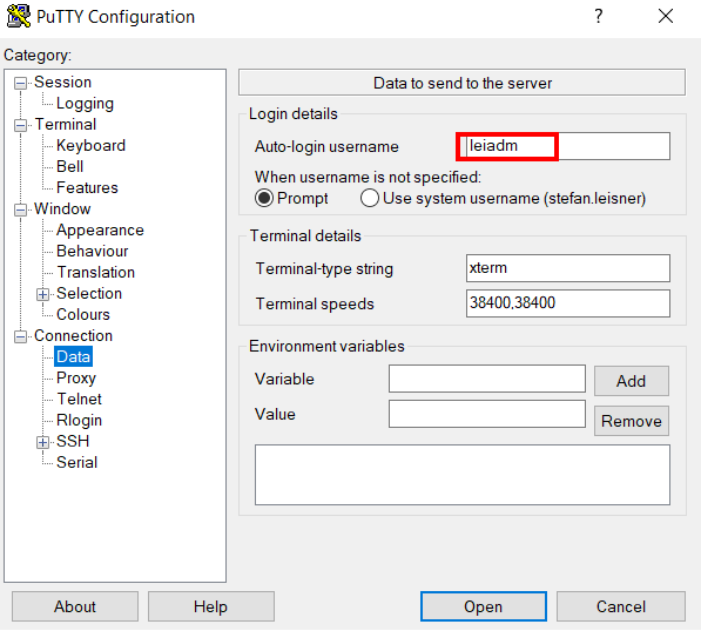
> Address the MU via hostname or IP address.



> Optional: Save the session under a meaningful name (*Session* menu).

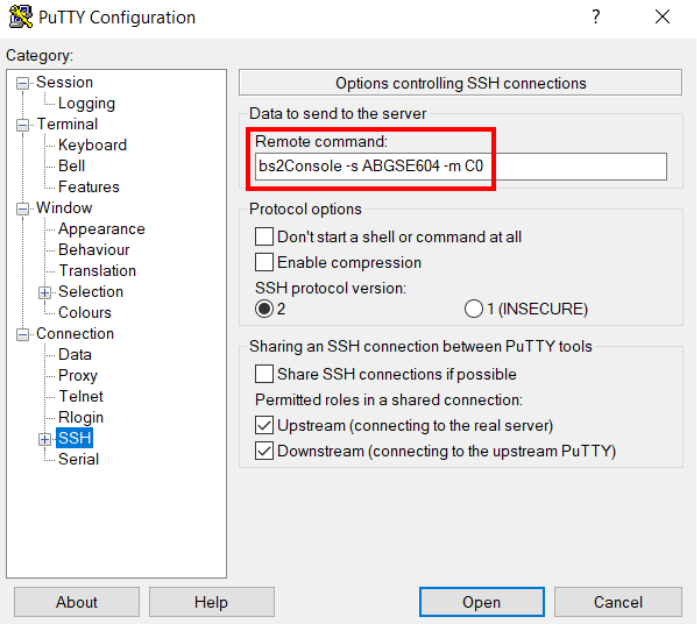
> Optional: Set a meaningful name for the title bar (*Window* -> *Behaviour* menu).

> Enter your own account (*Connection* -> *Data* menu):



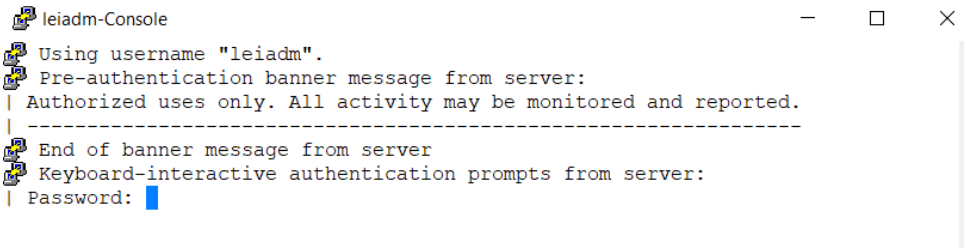
> Enter the `bs2Console` follow-up command (*Connection -> SSH* menu) with the following parameters:

- a BS2000 system of the local or explicitly addressed MU (system name, SE name or host name)
- only as administrator or BS2000 administrator: with specification of a console

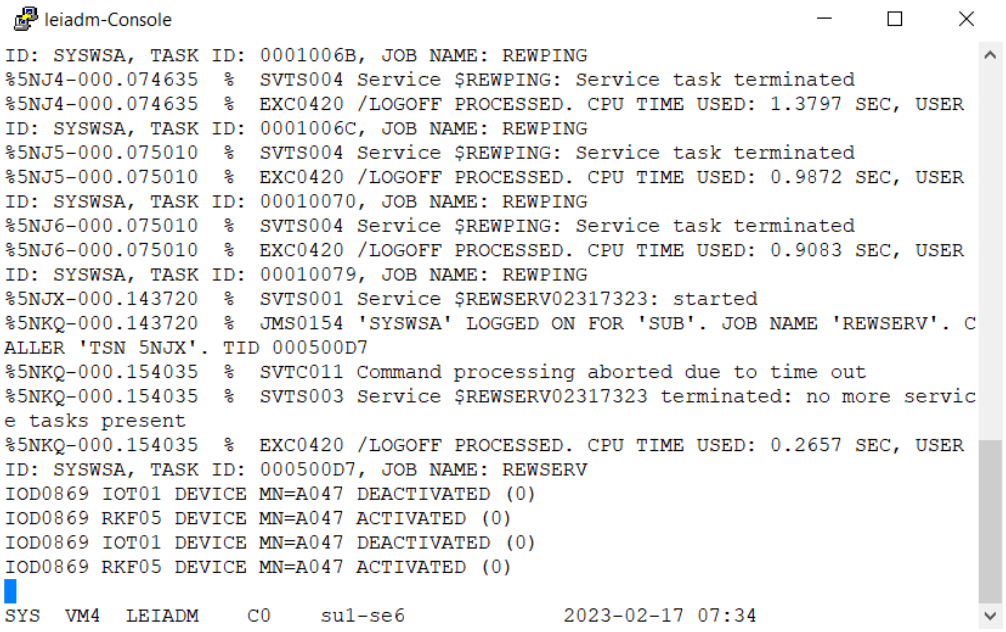


As BS2000 operator, you may not enter the console (option *-m*)! It is defined in the individual rights and will be determined.

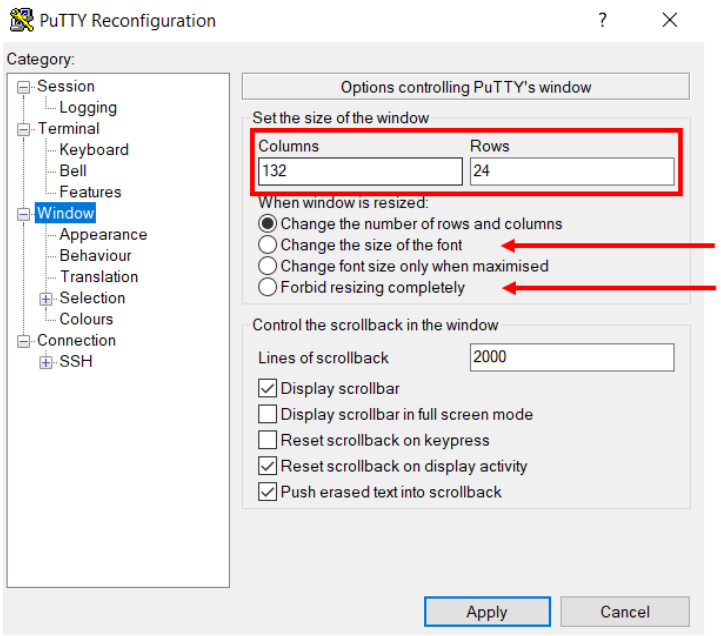
> Click *Open,* and in the console window, enter the password for the specified account:



After successful login, the connection to the console of the BS2000 system to which the specified KVP is assigned, is opened:



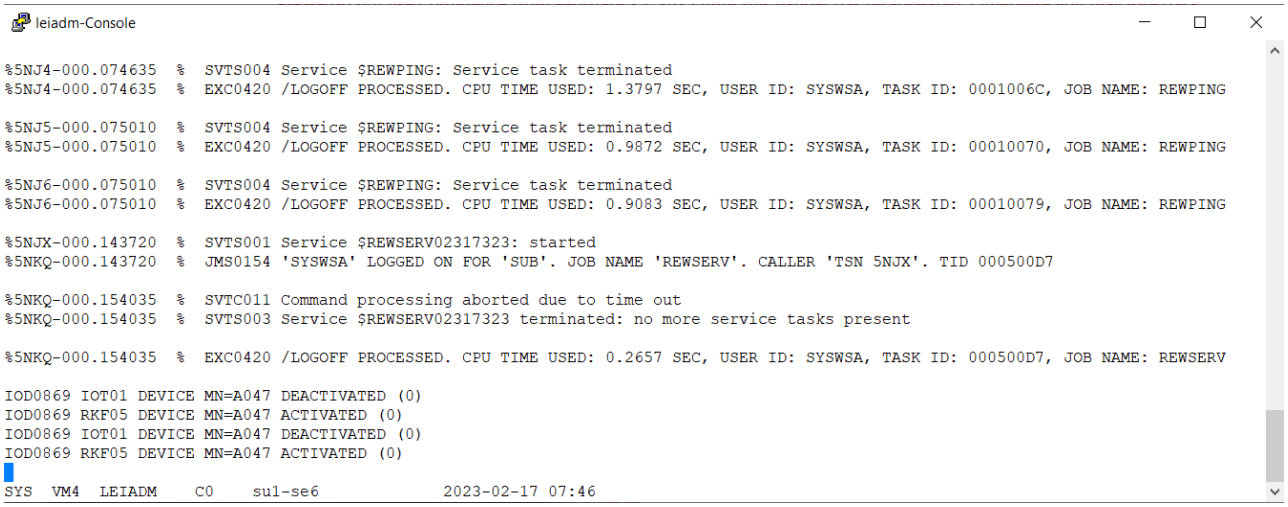
> Choose an alternative setting for the window size (the default size is 80 x 24). To avoid line breaks, we recommend using 132 columns. To do this, right-click on the header of the console window and select *Change Settings...* from the context menu:



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 the size of the font* (see above)
- Set a fixed window size: *Forbid resizing completely* (see above)

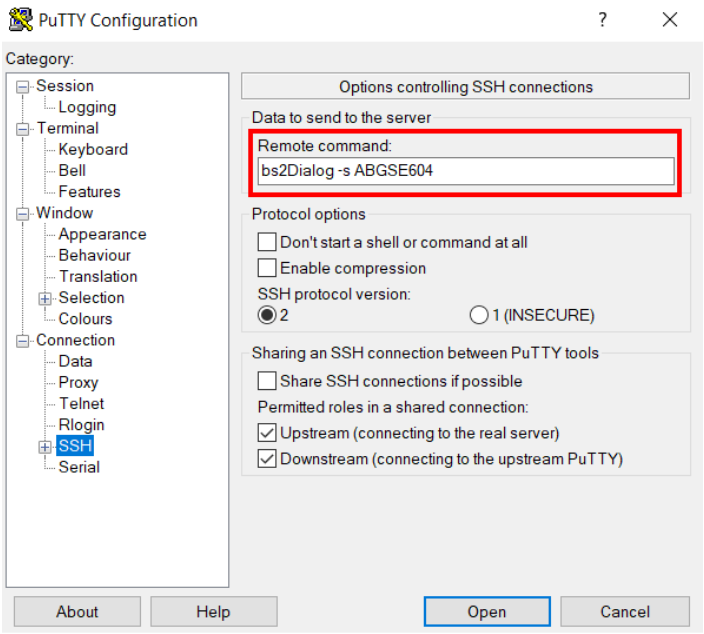
The console window with 132 columns:


leiadm-Console
%5NJ4-000.074635 % SVTS004 Service $REWPING: Service task terminated
%5NJ4-000.074635 % EXC0420 /LOGOFF PROCESSED. CPU TIME USED: 1.3797 SEC, USER ID: SYSWSA, TASK ID: 0001006C, JOB NAME: REWPING
%5NJ5-000.075010 % SVTS004 Service $REWPING: Service task terminated
%5NJ5-000.075010 % EXC0420 /LOGOFF PROCESSED. CPU TIME USED: 0.9872 SEC, USER ID: SYSWSA, TASK ID: 00010070, JOB NAME: REWPING
%5NJ6-000.075010 % SVTS004 Service $REWPING: Service task terminated
%5NJ6-000.075010 % EXC0420 /LOGOFF PROCESSED. CPU TIME USED: 0.9083 SEC, USER ID: SYSWSA, TASK ID: 00010079, JOB NAME: REWPING
%5NJX-000.143720 % SVTS001 Service $REWSERV02317323: started
%5NKQ-000.143720 % JMS0154 'SYSWSA' LOGGED ON FOR 'SUB'. JOB NAME 'REWSERV'. CALLER 'TSN 5NJX'. TID 000500D7
%5NKQ-000.154035 % SVTC011 Command processing aborted due to time out
%5NKQ-000.154035 % SVTS003 Service $REWSERV02317323 terminated: no more service tasks present
%5NKQ-000.154035 % EXC0420 /LOGOFF PROCESSED. CPU TIME USED: 0.2657 SEC, USER ID: SYSWSA, TASK ID: 000500D7, JOB NAME: REWSERV
IOD0869 IOT01 DEVICE MN=A047 DEACTIVATED (0)
IOD0869 RKF05 DEVICE MN=A047 ACTIVATED (0)
IOD0869 IOT01 DEVICE MN=A047 DEACTIVATED (0)
IOD0869 RKF05 DEVICE MN=A047 ACTIVATED (0)
SYS VM4 LEIADM C0 su1-se6 2023-02-17 07:46

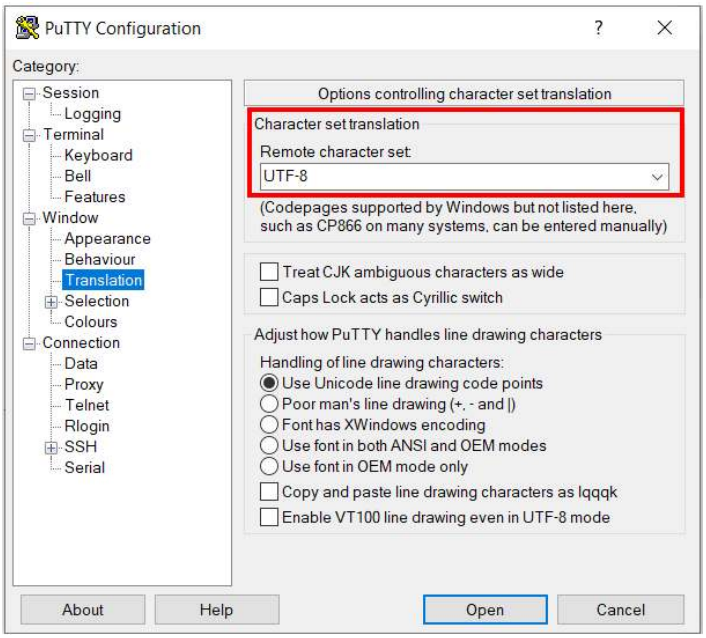
15.1.2 BS2000 dialog on MU or SU /390

> Enter the `bs2Dialog` follow-up command with the following parameters:

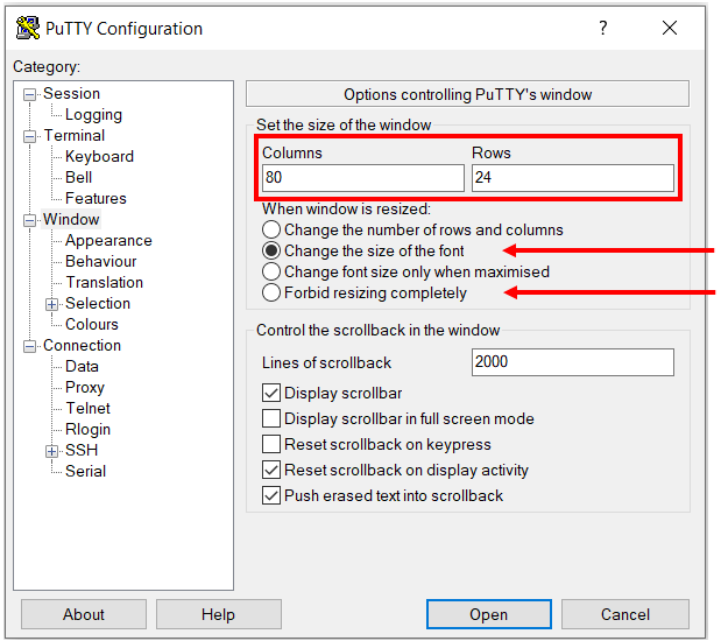
- a BS2000 system of the local or explicitly addressed MU (system name, SE name or host name)
- a LOCLAN connection (only if there is more than one LOCLAN assigned to the BS2000 system)



> Make sure to use the default character set UTF-8 that supports the display and the keyboard shortcuts required in the BS2000 dialog (*Window* -> *Translation* menu):



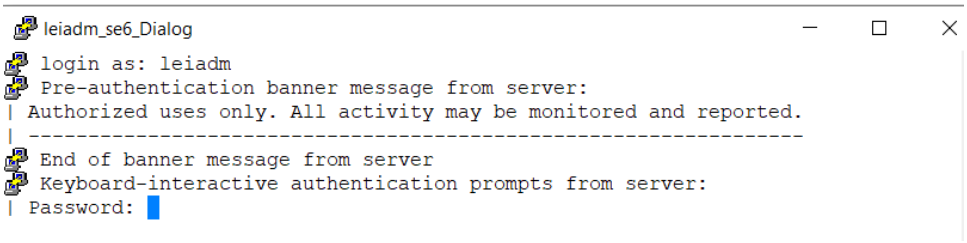
> Make sure to retain the default window size of 80 columns and 24 lines!



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:

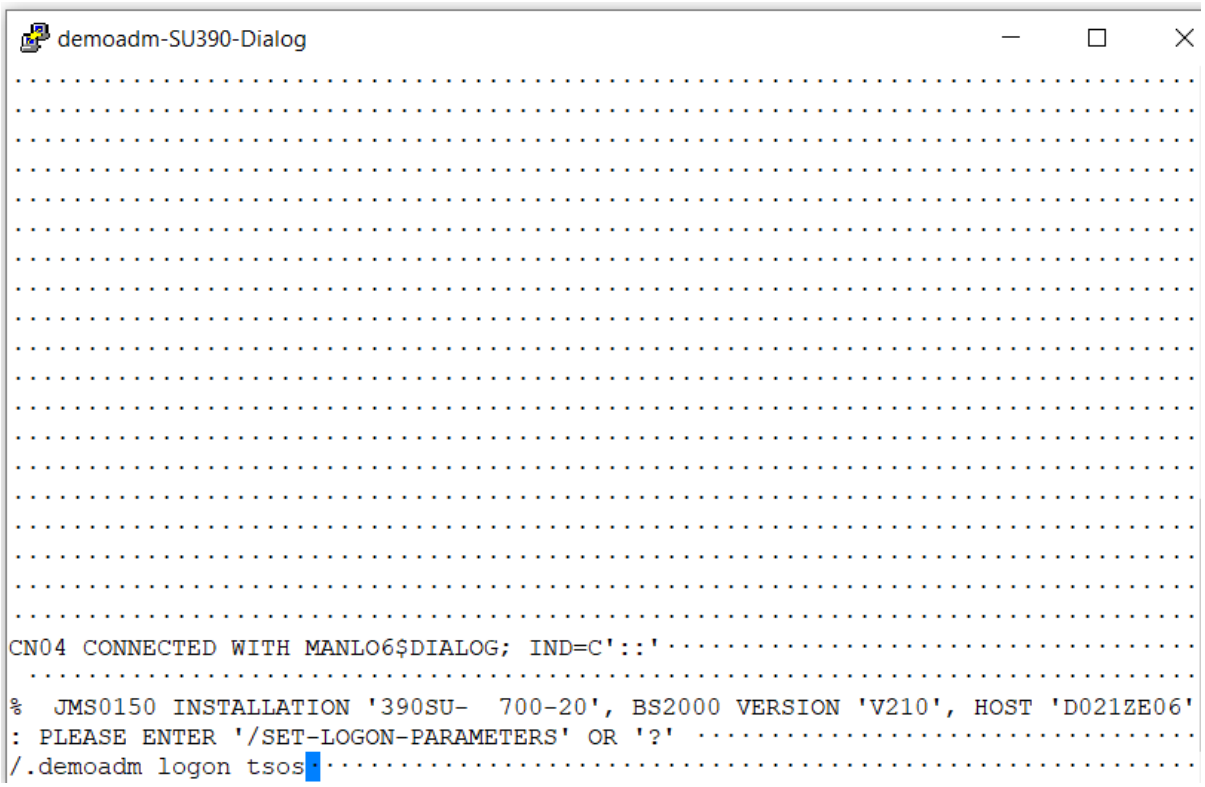
- Changing the font size together with the window size: *Change the size of the font* (see above)
- Set a fixed window size: *Forbid resizing completely* (see above)

> In the dialog window, enter the password for the specified account:



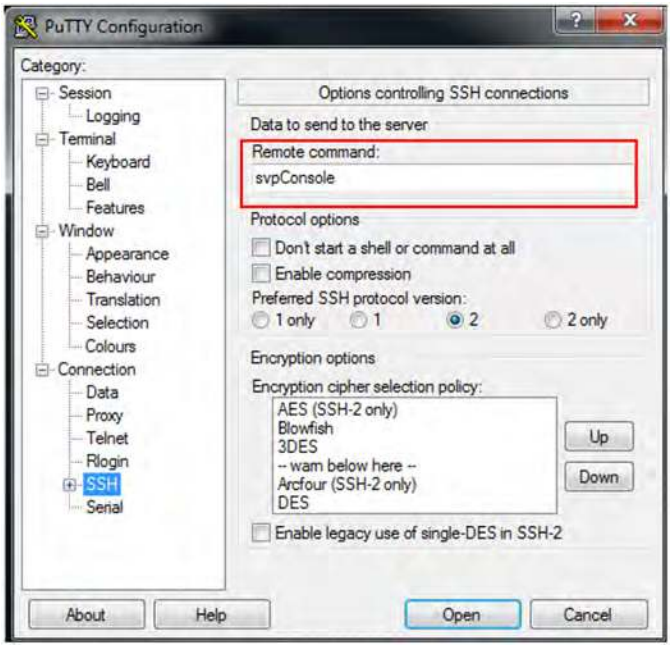
After successful login, the connection to the BS2000 dialog is opened and you can login to BS2000. Important keys:

K1	F5
K2	F6
EM	F11
DUE	F12

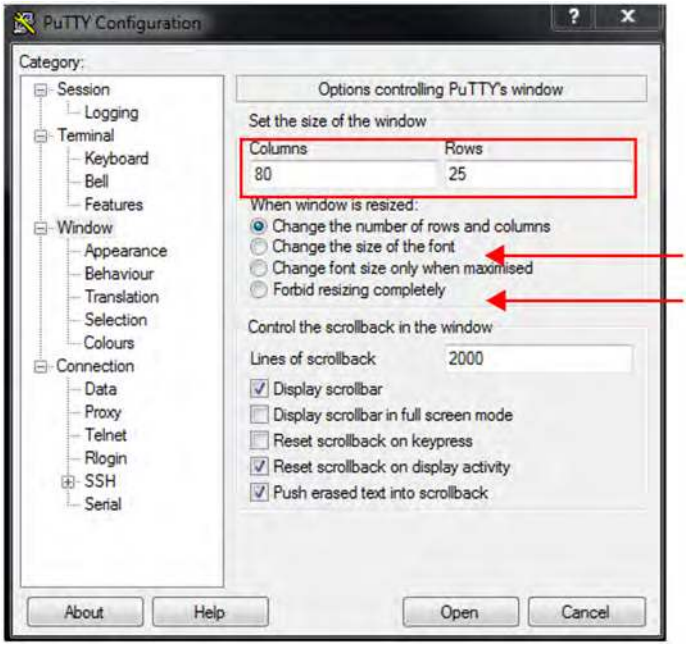

demoadm-SU390-Dialog
CN04 CONNECTED WITH MANLO6$DIALOG; IND=C'::'
% JMS0150 INSTALLATION '390SU- 700-20', BS2000 VERSION 'V210', HOST 'D021ZE06'
: PLEASE ENTER '/SET-LOGON-PARAMETERS' OR '?'
/.demoadm logon tsos

15.1.3 SVP console on MU or SU /390

> Enter the `svpConsole` follow-up command:



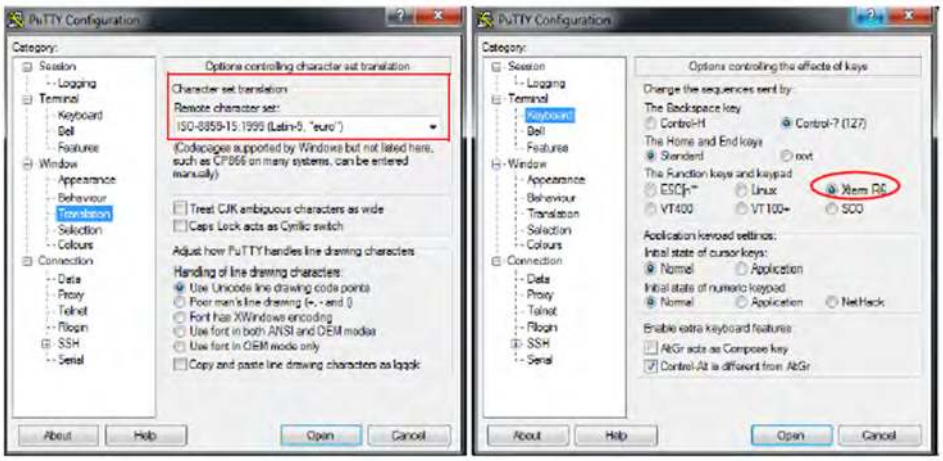
> Specify a window size of 80 columns and 25 lines. This setting must be kept at all times!



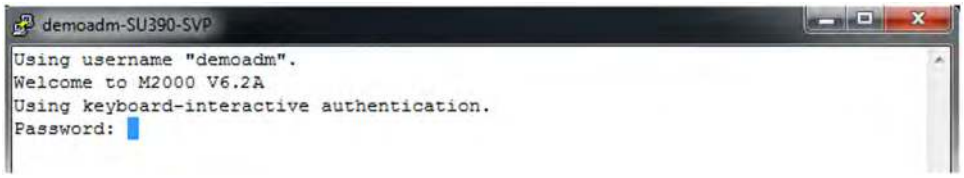
The number of columns and lines may not change when the dialog window is dragged, as this would disrupt the display. Therefore, select one of the following settings for window size:

- Changing the font size together with the window size: *Change the 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:

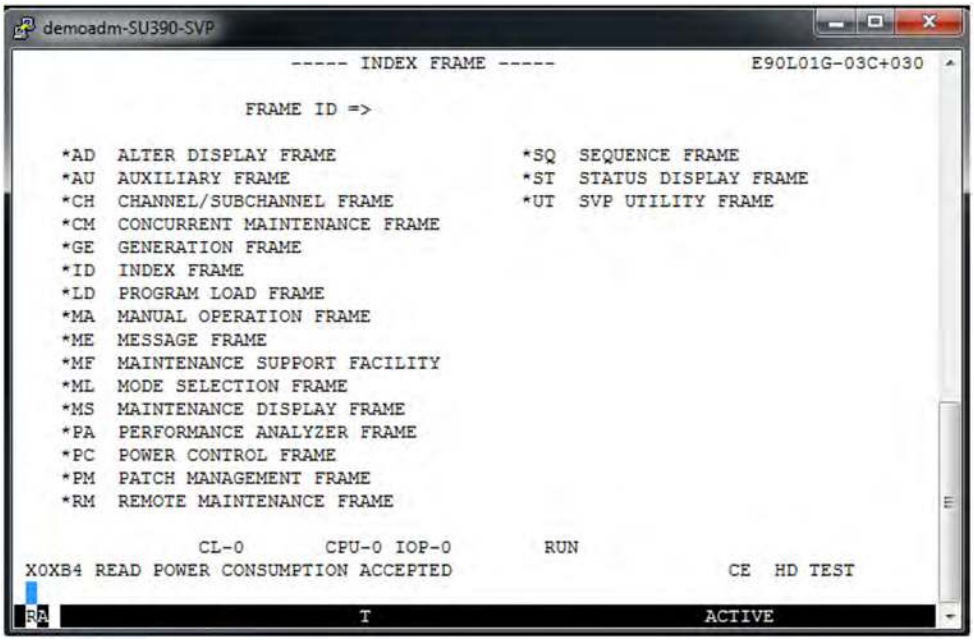


> In the console window, enter the password for the specified account:



After successful login, the connection to the SVP console is opened. Important keys:

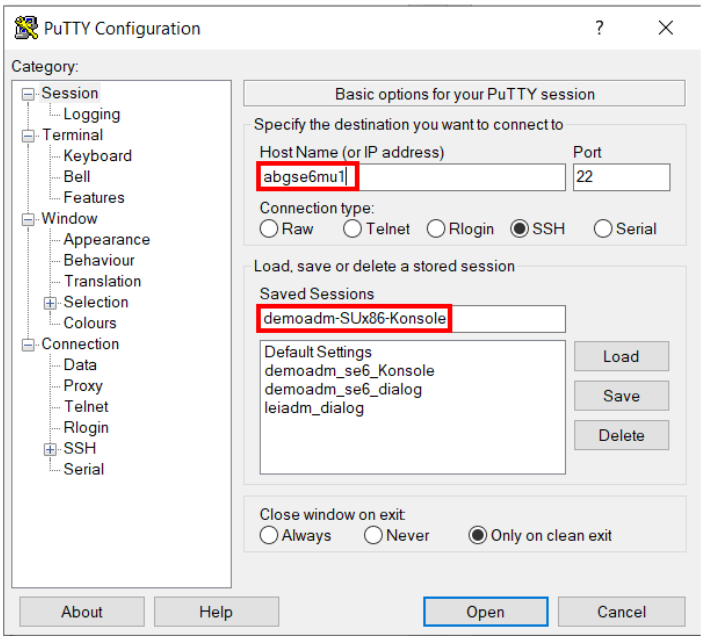
PF3	ESC + F3	(in this order)
INDEX	ESC + F2	(in this order)



15.1.4 BS2000 console on SU x86

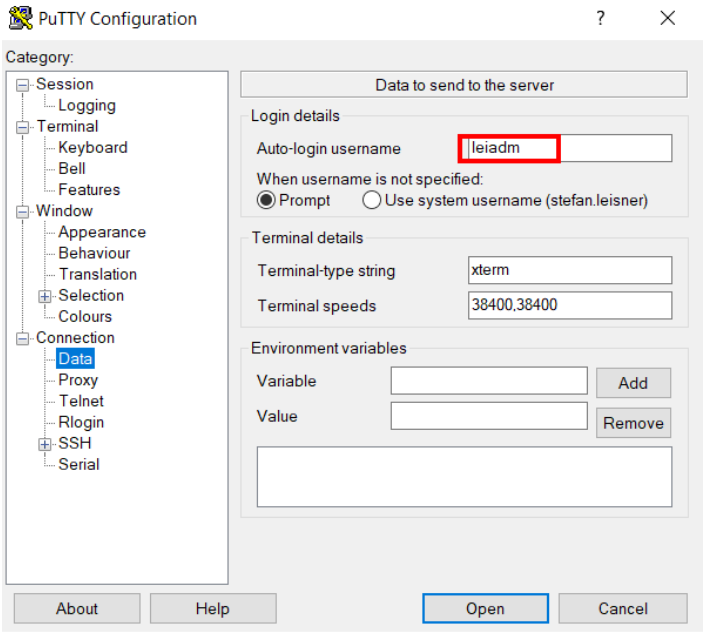
> Address the MU via hostname or IP address.

> Optional: Save the session under a meaningful name (*Session* menu).



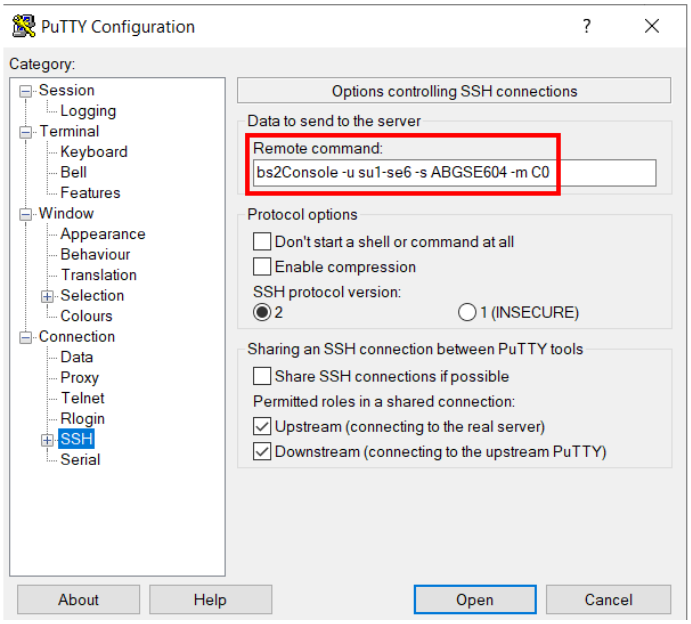
> Optional: Set a meaningful name for the title bar (*Window* -> *Behaviour* menu).

> Enter your own account (*Connection* -> *Data* menu):



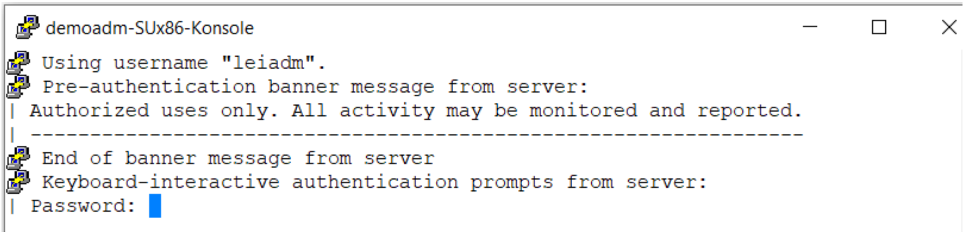
> Enter the `bs2Console` follow-up command with the following parameters:

- the unit: external or internal name of the SU x86
- the system specified by its system name or SE name or hostname
- only as administrator or BS2000 administrator: the console MN



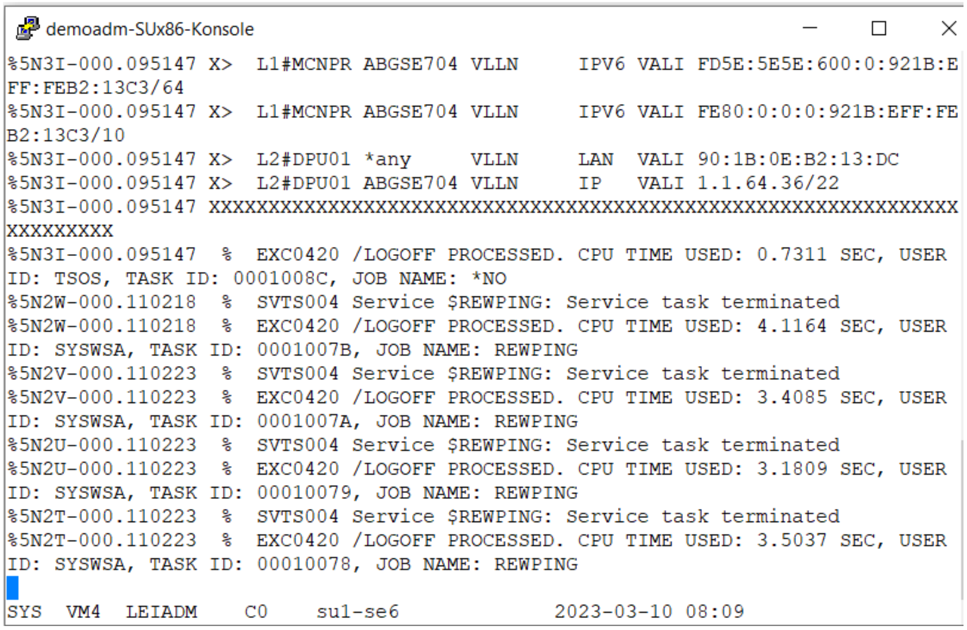
As BS2000 operator, you may not enter the console (-m C0 in the example)! It is defined and will be determined.

> In the console window, enter the password for the specified account:



```
demoadm-SUx86-Konsole
Using username "leiadm".
Pre-authentication banner message from server:
| Authorized uses only. All activity may be monitored and reported.
| ----------------------------------------------------------------
End of banner message from server
Keyboard-interactive authentication prompts from server:
| Password:
```

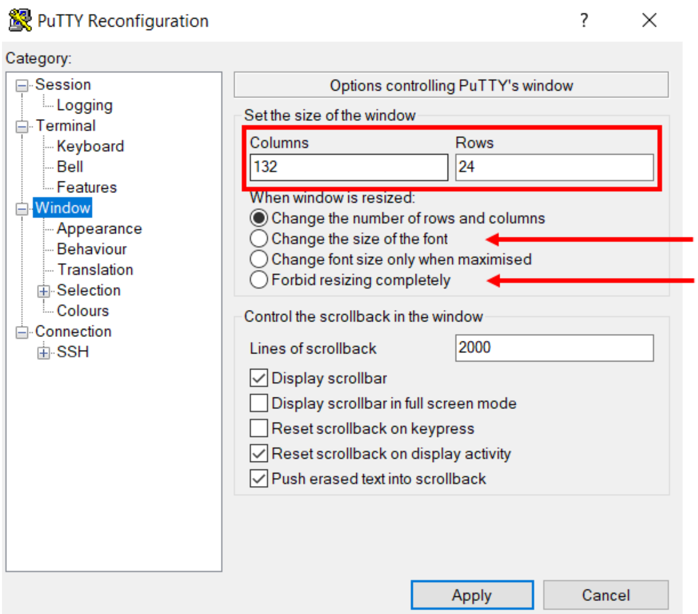
After successful login, the connection to the console of the BS2000 system is opened:



```
demoadm-SUx86-Konsole
%5N3I-000.095147 X>  L1#MCNPR ABGSE704 VLLN     IPV6 VALI FD5E:5E5E:600:0:921B:E
FF:FEB2:13C3/64
%5N3I-000.095147 X>  L1#MCNPR ABGSE704 VLLN     IPV6 VALI FE80:0:0:0:921B:EFF:FE
B2:13C3/10
%5N3I-000.095147 X>  L2#DPU01 *any     VLLN     LAN  VALI 90:1B:0E:B2:13:DC
%5N3I-000.095147 X>  L2#DPU01 ABGSE704 VLLN     IP   VALI 1.1.64.36/22
%5N3I-000.095147 XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXX
%5N3I-000.095147  %  EXC0420 /LOGOFF PROCESSED. CPU TIME USED: 0.7311 SEC, USER
ID: TSOS, TASK ID: 0001008C, JOB NAME: *NO
%5N2W-000.110218  %  SVTS004 Service $REWPING: Service task terminated
%5N2W-000.110218  %  EXC0420 /LOGOFF PROCESSED. CPU TIME USED: 4.1164 SEC, USER
ID: SYSWSA, TASK ID: 0001007B, JOB NAME: REWPING
%5N2V-000.110223  %  SVTS004 Service $REWPING: Service task terminated
%5N2V-000.110223  %  EXC0420 /LOGOFF PROCESSED. CPU TIME USED: 3.4085 SEC, USER
ID: SYSWSA, TASK ID: 0001007A, JOB NAME: REWPING
%5N2U-000.110223  %  SVTS004 Service $REWPING: Service task terminated
%5N2U-000.110223  %  EXC0420 /LOGOFF PROCESSED. CPU TIME USED: 3.1809 SEC, USER
ID: SYSWSA, TASK ID: 00010079, JOB NAME: REWPING
%5N2T-000.110223  %  SVTS004 Service $REWPING: Service task terminated
%5N2T-000.110223  %  EXC0420 /LOGOFF PROCESSED. CPU TIME USED: 3.5037 SEC, USER
ID: SYSWSA, TASK ID: 00010078, JOB NAME: REWPING

SYS  VM4  LEIADM    C0    su1-se6            2023-03-10 08:09
```

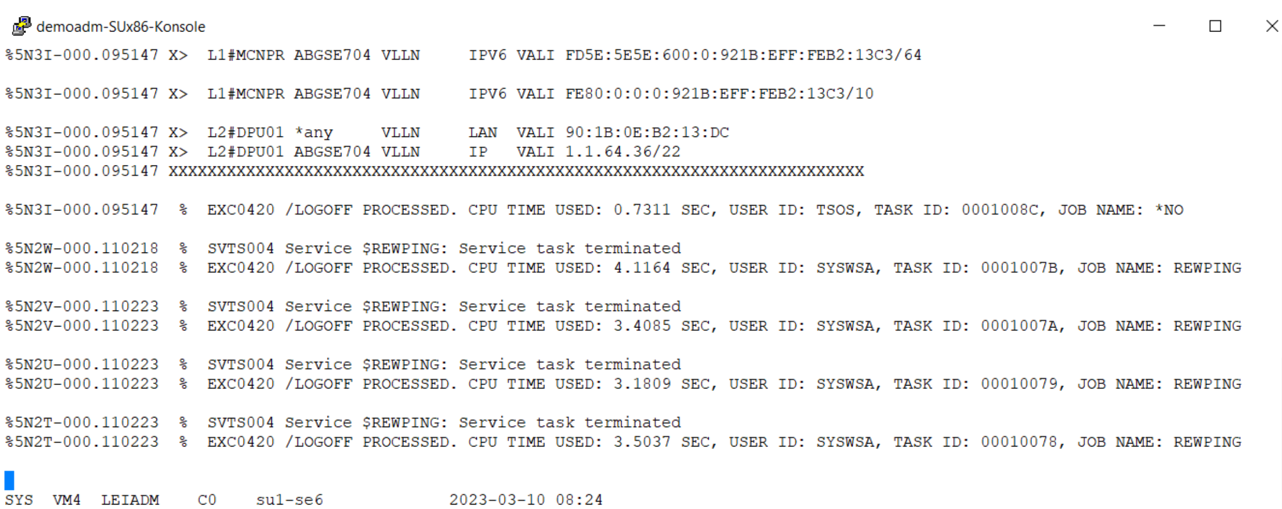
> Choose an alternative setting for the window size (the default size is 80 x 24). To avoid line breaks, we recommend using 132 columns:



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)

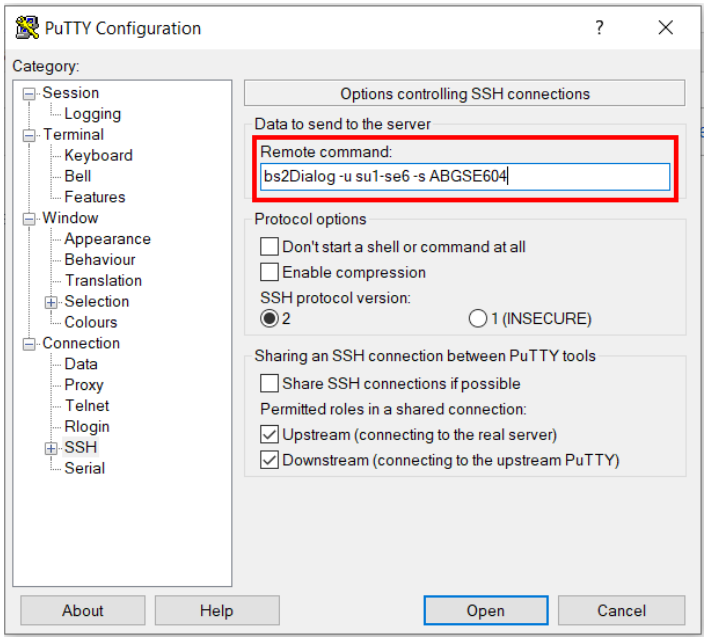
The console window with 132 columns:



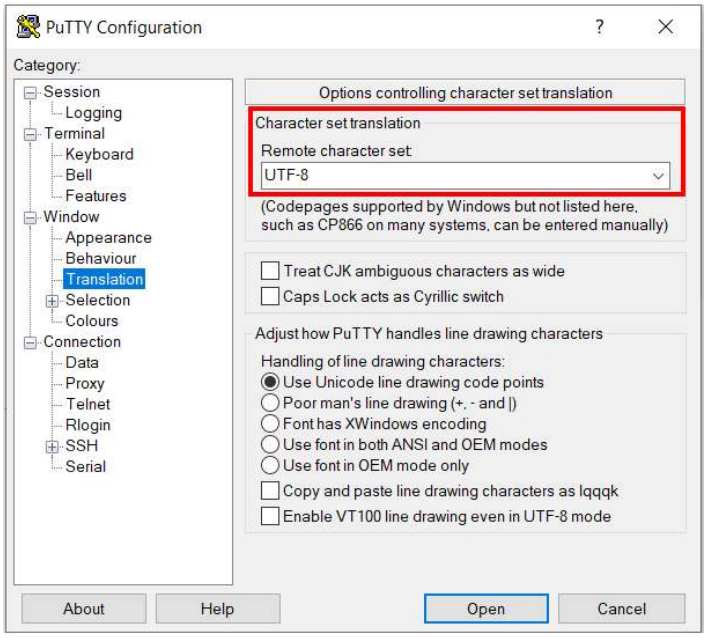
15.1.5 BS2000 dialog on SU x86

> Enter the `bs2Dialog` follow-up command with the following parameters:

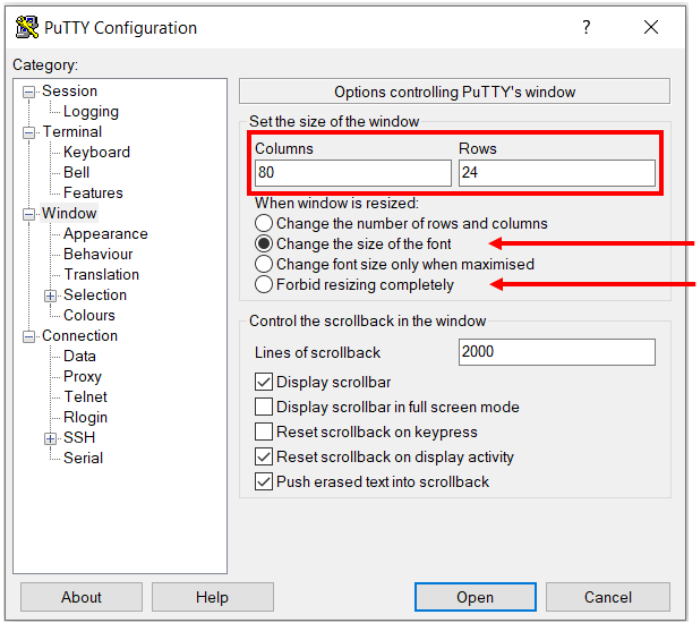
- the unit: external or internal name of the SU x86
- the system specified by its system name or SE name or hostname



> Make sure to use the default character set UTF-8 that supports the display and the keyboard shortcuts required in the BS2000 dialog (*Window* -> *Translation* menu):



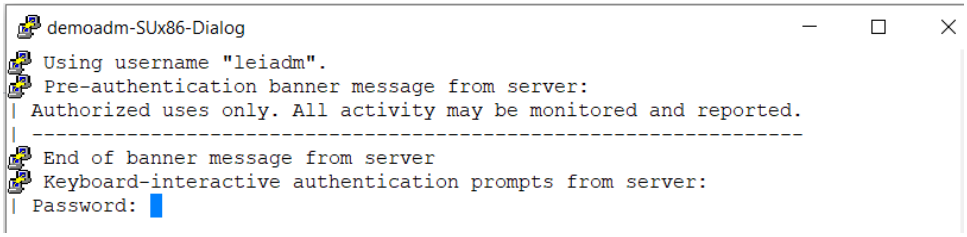
> Make sure to retain the default window size of 80 columns and 24 lines!



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:

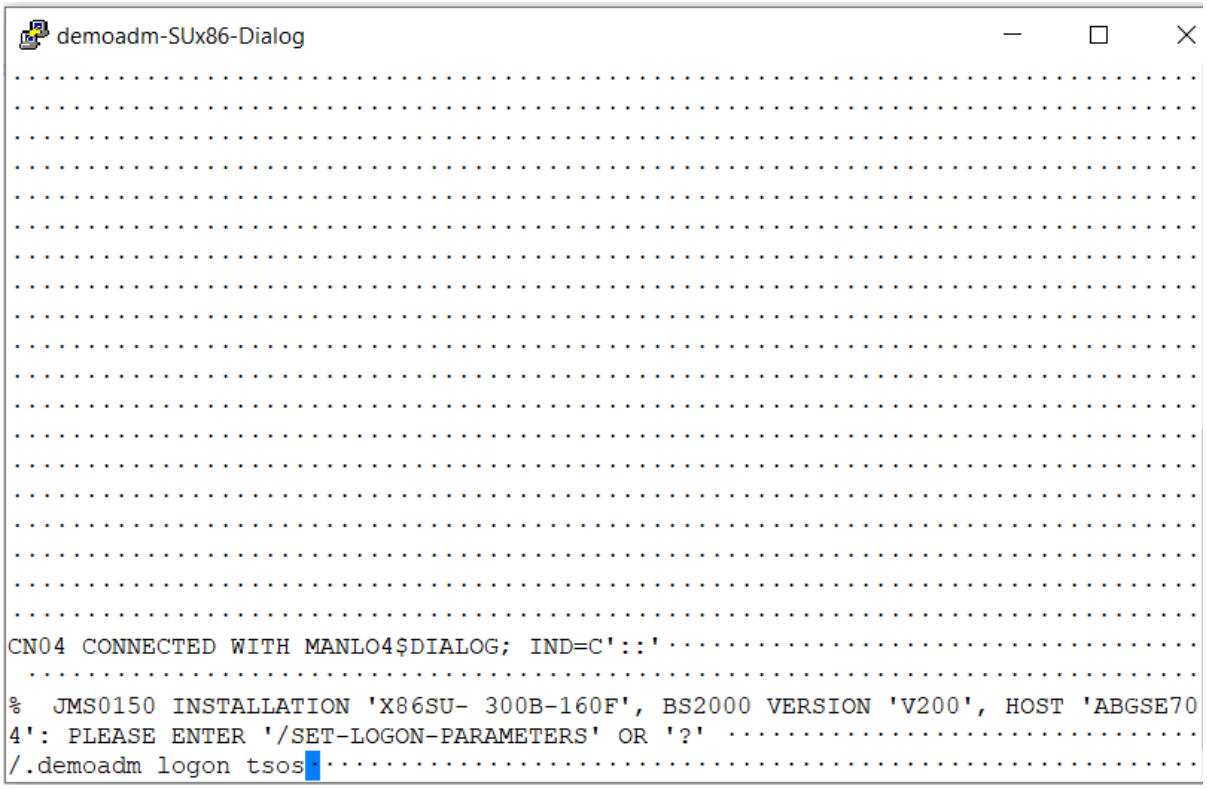
- Changing the font size together with the window size: *Change the size of the font* (see above)
- Set a fixed window size: *Forbid resizing completely* (see above

> 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


demoadm-SUx86-Dialog
CN04 CONNECTED WITH MANLO4$DIALOG; IND=C'::'
% JMS0150 INSTALLATION 'X86SU- 300B-160F', BS2000 VERSION 'V200', HOST 'ABGSE70
4': PLEASE ENTER '/SET-LOGON-PARAMETERS' OR '?'
/.demoadm logon tsos

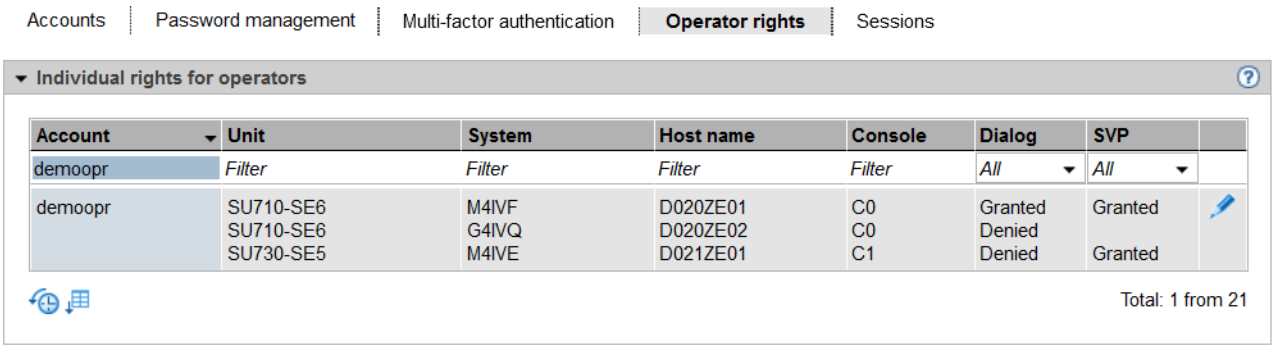
15.1.6 Information on the user strategy

For administrators and BS2000 administrators, the accesses described are unrestricted. For other roles except *BS2000 operator* none of the accesses is possible.

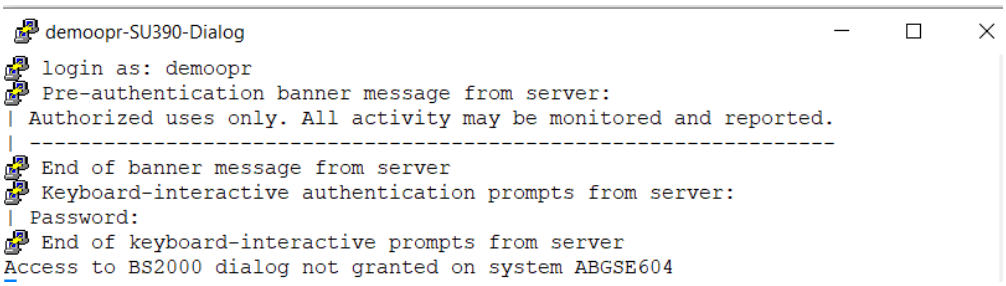
For BS2000 operators, their individual rights apply, as specified by an administrator or security administrator (also see the following example):

- BS2000 console rights:
  Access to the defined systems of the individual SUs is only possible with fixed consoles.
- BS2000 dialog rights:
  The access to the BS2000 dialog is possible for the BS2000 systems allowed by the individual rights.
- SVP console (SU /390):
  Access is possible according to the individual rights.

Example for a BS2000 operator with individual rights (*Authorizations* -> *Users* menu):



The authorizations are tested, the call is rejected:



> **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!

16 Glossary

Application Unit
AU, AU PY, AU PQ

Optional component of the SE server.
An AU permits operation of applications under Linux, Windows, VMware or other hypervisors.
Application Unit PY (AU PY) refers to all PRIMERGY based AUs (e.g. the AU20 or AU47 hardware models).
Application Unit PQ (AU PQ) refers to all PRIMEQUEST based AUs (e.g. the AUQ38E or DBU38E hardware models).

Configuration Save and Restore
CSR

Saves the configuration data of the Management Unit in an archive. The backup archive contains all configuration data that the customer manages himself using the SE Manager.

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

Customer ID

The customer ID is defined by the service and serves to uniquely identify the customer data in the Support Center. It is displayed in the SE Manager and must be specified for each communication with the Support Center.

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).

FDDRL

FDDRL (Fast Disk Dump and ReLoad) is a BS2000 software product for saving the contents of BS2000 disks and pubsets. FDDRL supports both public and private disks. The pubsets can be either single-feature (SF) or system-managed (SM).

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.

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.

High-speed Net Connect
HNC

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.

HSMS

HSMS (Hierarchical Storage Management System) is a BS2000 software product for data backup which supports data management on external storage devices in a BS2000 system.

Initial Program Load
IPL

First phase of system initialization after booting. IPL reads in the CLASS1-EXEC, system parameters, and REPs.

IO Configuration File / Input/Output Resource File
IOCF / IORSF

Contains information on the configuration of the input/output devices of an SU /390.
An IORSF contains a BS2000 device configuration, which is required to start up an SU /390.
The IOCF must be installed in the service processor SVP in order to be used.

IOGEN

BS2000 utility routine to generate an IORSF configuration (IOCF)

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 SE servers with SU /390.

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.

Multi-factor authentication
MFA

Login procedure (at the SE Manager) in which the access authorization is checked by several (here: two) independent characteristics (factors).

Net-Storage

The storage space provided by a 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-Storage server's file system.

Net-Storage client

Implements access to Net-Storage for the operating system using it.
In BS2000 the Net-Storage 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-Storage server.

Net-Storage server

File server in the worldwide computer network which provides storage space (Network Attached Storage, NAS) for use by other servers and offers corresponding file server services.

Net Unit
NU

Component of the SE server; enables an SE server to be connected to customer networks (LAN/SAN). The Net Unit incorporates High-speed Net Connect (HNC).

Net Unit Extension
NUX

The optional add-on pack NUX serves to connect the SE server to the customer networks by means of additive Cisco switches outside the SE server.
In a broader sense, NUX refers to the entirety of these Cisco switches, their configuration and integration into SEM using the NUX add-on pack.

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.

SE Manager
SEM

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. Frequently used abbreviation: SEM.

SENET
senet

A DNS server for the "senet" domain which provides name resolution for communication (especially for the internal communication within MCNPR) runs on every 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 in addition.

Server line, Server type
SE /390, SE x86

- SE /390: A server of this line resp. of this type contains one SU /390 and optional one or several SU x86.
- SE x86: A server of this line resp. of this type contains one or several SU x86 and contains no SU /390.

Server Unit
SU

Component of the SE server that supports the operation of BS2000 (Native-BS2000 or VM2000). SU types are SU /390 and SU x86 - see below. The models and the abbreviations used for them can be found, for example, in the Basic Operating Manual [1].

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).

Service and console processor
SKP

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 which has a local console, a Host Controller, and various ports for LAN connection and supporting remote service.
  On the SE server the Management Unit (MU) provides this hardware functionality for operating SU /390.
- Software functionality
  On an SKP hardware unit the SKP Manager provides the SKP functionality for operating the S server and managing the devices and remote service.
  On the SE server the SKP functionality is integrated into the SE Manager.
- Device type
  In BS2000 an SKP device type is used (e.g. SKP2).

SVP

Service processor of the SU /390.
With SU x86 there is an emulated SVP functionality in the X2000, as faras necessary.

SVP clock

Autonomous clock which supplies the TODR (Time of Day Register) 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.

Unit x86

Component of the SE server with x86 architecture: Server Unit x86, Management Unit or HNC

17 Related publications

You can find the following BS2000 manuals on the manual server with the BS2000 documentation at https://bs2manuals.ts.fujitsu.com.

Other manuals, for example descriptions of the Fujitsu PRIMERGY and PRIMEQUEST servers, can be found on the general Fujitsu support pages at https://support.ts.fujitsu.com/.

[1] **Fujitsu Server BS2000 SE Series**
Basic Operating Manual

[2] **Fujitsu Server BS2000 SE Series**
Server Unit /390
Operating Manual

[3] **Fujitsu Server BS2000 SE Series**
Server Unit x86
Operating Manual

[4] **Fujitsu Server BS2000 SE Series**
Additive Components
Operating Manual

[5] **Fujitsu Server BS2000 SE Series**
Administration and Operation
User Guide

[6] **Fujitsu Server BS2000 SE Series**
Quick Guide
User Guide

[7] **Fujitsu Server BS2000 SE Series**
Security Manual
User Guide

[8] **Fujitsu Server BS2000 SE Series**
Cluster Solutions for SE Servers
Whitepaper

[9] **BS2000 OSD DX**
System Installation
User Guide

[10] **BS2000 OSD DX**
Introduction to System Administration
User Guide

[11] **BS2000 OSD DX**
Utility Routines
User Guide

[12] **VM2000** (BS2000)
Virtual Machine System
User Guide

[13] **openNet Server**
BCAM
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 Net-Storage Guide.

[16] **ServerView Suite**
iRMC S<n>
User Guide (Documentation for the current version)

[17] **ServerView Suite**
ServerView Operations Manager
Installation for Linux / Installation for Windows (one Installation Guide for each)

[18] **ServerView Suite**
ServerView Operations 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

[21] **Fujitsu Software**
openUTM WebAdmin
User Guide

[22] **ROBAR**
Controlling MTC Archive Systems
User Guide

[23] **Storage Manager (StorMan)**
Managing virtualized storage resources
Administrator and User Guide