

FUJITSU Server BS2000

SE700 / SE500 / SE300

Sicherheitshandbuch

Benutzerhandbuch

Stand der Beschreibung:

M2000 V6.0A / V6.1A

X2000 V6.0A / V6.1A

HNC V6.0A / V6.1A

Kritik... Anregungen... Korrekturen...

Die Redaktion ist interessiert an Ihren Kommentaren zu diesem Handbuch. Ihre Rückmeldungen helfen uns, die Dokumentation zu optimieren und auf Ihre Wünsche und Bedürfnisse abzustimmen.

Sie können uns Ihre Kommentare per E-Mail an manuals@ts.fujitsu.com senden.

Zertifizierte Dokumentation nach DIN EN ISO 9001:2008

Um eine gleichbleibend hohe Qualität und Anwenderfreundlichkeit zu gewährleisten, wurde diese Dokumentation nach den Vorgaben eines Qualitätsmanagementsystems erstellt, welches die Forderungen der DIN EN ISO 9001:2008 erfüllt.

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

Copyright und Handelsmarken

Copyright © 2015 Fujitsu Technology Solutions GmbH.

Alle Rechte vorbehalten.

Liefermöglichkeiten und technische Änderungen vorbehalten.

Alle verwendeten Hard- und Softwarenamen sind Handelsnamen und/oder Warenzeichen der jeweiligen Hersteller.

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 und SUSE sind eingetragene Marken von Novell, Inc. in den USA und anderen Ländern.

Linux ist eine eingetragene Marke von Linus Torvalds.

Windows® ist ein eingetragenes Warenzeichen der Microsoft Corporation.

Die Linux-basierte Basis-Software M2000, X2000 und HNC, die auf Management Unit, Server Unit x86 und HNC installiert ist, beinhaltet Open-Source-Software. Die Lizenzen dazu finden Sie auf der jeweiligen Installations-DVD im Verzeichnis LICENSES.

Inhalt

1	Einleitung	7
1.1	Zielsetzung und Zielgruppen des Handbuchs	10
1.2	Konzept des Handbuchs	10
1.3	Darstellungsmittel	12
1.4	Open-Source-Software	14
2	Architektur der SE Server und der Netzwerke	15
2.1	Hardware	15
2.2	Architektur der SE Server	16
2.3	Netzwerke	17
3	Sicherer Zugang zu Management-Funktionen	19
3.1	Rollenkonzept und Benutzerkennungen	19
3.1.1	Rollenkonzept und Rollenrechte	19
3.1.2	Benutzerkennungen	22
3.1.2.1	Berechtigung zur Kennungsverwaltung	23
3.1.2.2	Weitere Kennungen des Basis-Systems	24
3.1.2.3	Kennungen für Add-on Packs	24
3.1.3	Authentisierung	25
3.1.4	Passwortverwaltung für Kennungen	25
3.2	Zugang zum SE Manager	29
3.2.1	Sicherheitseinstellungen auf dem Administrations-PC	29
3.2.2	Kommunikation mit Verschlüsselung	29
3.2.3	Session-Management	30

3.3	Textbasierter Zugang (auf Shell-Ebene)	32
3.3.1	Verschlüsselte Kommunikation mit Secure Shell	32
3.3.2	Keine Rechteeskalation	32
3.3.3	Zugangsfunktionen im SE Manager	32
3.3.4	Zugang zu BS2000-Konsole im KVP-Menü sperren	32
3.4	Alternative Zugänge mit Secure Shell	33
3.4.1	Secure Shell Host-Schlüssel	33
3.4.2	Kommunikation mit Secure Shell-Schlüsseln	33
3.4.3	Generierung der Schlüssel	34
3.4.4	Benutzung von SSH-Agenten	36
3.4.5	PuTTY mit PuTTYgen und Pageant	37
3.4.5.1	Schlüsselgenerator PuTTYgen	38
3.4.5.2	Authentifizierungs-Agent Pageant	39
3.5	Zugang über die lokale Konsole	40
3.6	Zugang zum iRMC der Management Unit	42
3.7	Geschützter Zugang zum BIOS und zum Bootloader	43
4	Sicherer Zugang zu Systemen	45
4.1	Sicherer Zugang zu BS2000-Systemen	45
4.1.1	Sicherheit im BS2000-Betriebssystem	45
4.1.2	KVP-Logging-Dateien herunterladen	46
4.1.3	Alternativer Zugang zum BS2000-Betriebssystem mit PuTTY	46
4.2	Sicherer Zugang zu Systemen auf Application Units	47
4.2.1	Konfigurationsänderungen	47
4.2.2	Zugang zum iRMC der Application Unit	48
4.2.3	Zugang über die lokale Konsole	49
4.3	Sicherer Zugang zu XenVMs auf SU x86	50
4.3.1	XenVMs auf der SU x86	50
4.3.2	Alternativer Zugang über SSL-fähigen VNC-Viewer	51

5	Remote-Service (AIS Connect)	53
5.1	Service-Kennungen	54
5.2	Service-Vorgänge protokollieren	55
5.3	Verschlüsselung nutzen	55
5.4	Funktion „Schattenterminal“ nutzen	56
5.5	Zugang zu externen Assets	57
6	Konfigurations- und Diagnosedaten	59
6.1	Konfigurationsdatensicherung	59
6.2	Diagnosedaten	60
7	Netzwerksicherheit	61
7.1	Netzwerkdienste	61
7.2	IP-basierte Zugangsbeschränkung	62
7.3	Sicherheit auf der Ebene der Net Unit	63
7.4	Net-Storage	63
7.5	SNMP	64
8	Sicherheit des Basis-Systems	65
8.1	Härtung des Basis-Systems	65
8.2	Software-Signatur	66
8.3	Digitale Zertifikate	67
8.3.1	Zertifikat im Web-Browser bestätigen/importieren	68
8.3.2	Standard-Zertifikat einsetzen	69
8.3.3	Neues selbstsigniertes Zertifikat erzeugen und aktivieren	72
8.3.4	Antrag auf ein SSL-Zertifikat stellen	73
8.3.5	Kundeneigenes Zertifikat hochladen und aktivieren	74
8.4	Security Fixes	76

9 Aktionen im System protokollieren (Audit-Logging) 77

Literatur 79

Stichwörter 81

1 Einleitung

Die FUJITSU Server BS2000 der SE Serie führen die bisherigen Serverlinien S-Server und SQ-Server in der Serverlinie der SE Server zusammen.

Der SE Server enthält je nach Anforderung alle erforderlichen Systemkomponenten für den Betrieb als Gesamtanwendung:

- SU /390 für BS2000-Gastsysteme
- Server Unit x86 mit BS2000-, Linux- oder Windows-Gastsystemen
- x86-basierte Application Units für den Betrieb unter Linux, Windows oder VMware
- gemeinsam nutzbare Band- und Plattenperipherie
- eine schnelle serverinterne Infrastruktur zur Verbindung der Komponenten untereinander und mit dem IP- oder FC-Netzwerk des Kunden.

Der SE Server bietet folgende Vorteile:

- systemübergreifende Administration mit moderner browserbasierter GUI (SE Manager) als single point of operation
- gemeinsame Systemüberwachung aller Bestandteile
- einheitliches Redundanzkonzept
- gemeinsames Service-Verfahren
- alle Möglichkeiten zur Konsolidierung durch Virtualisierung
- SE Komponenten und Infrastruktur werden vorkonfiguriert an Kunden ausgeliefert "ready to use"

SE Server ermöglichen daher eine flexible und anwendungsangepasste Implementierung, die durch die Verwendung von High-End-Komponenten und ein durchgehendes Hochverfügbarkeitskonzept hohe SLAs erfüllt und trotzdem durch ihre Einheitlichkeit einen kostengünstigen Betrieb des Gesamtsystems mit wenigen Ressourcen ermöglicht.

Dabei profitieren auch Intel x86-basierten Serversysteme mit ihren VMware-, Linux- oder Windows-Systemplattformen von den beim Mainframe erprobten Konzepten für einen stabilen Systembetrieb:

- Auswahl hochwertiger Server-Bestandteile
- Redundante Hardwarekomponenten
- Vorbereitete Betriebskonzepte, die auch Hochverfügbarkeit mit einschließen
- Umfangreiche Tests vor der Freigabe
- Umfassendes Servicekonzept.

Die für alle SE Server einheitliche Managementoberfläche, der SE Manager, ermöglicht den Blick auf alle beteiligten Systemkomponenten und ermöglicht aus dieser übergeordneten Sichtweise die Optimierung der Ressourcen durch eine effiziente Verteilung der Anwendung auf die aktuell am wenigsten belasteten Systeme.

So ermöglichen SE Server einen besonders stabilen Systembetrieb, der nicht nur die schon bisher als besonders ausfallsicher bekannten Mainframe-Plattformen einschließt, sondern auch andere Server Units und die vom SE Server genutzte Infrastruktur und Peripherie umfasst. Dies kann mit geringeren Ressourcen bei der Administration und Systembedienung erfolgen als bei einem separaten Betrieb von verschiedenen IT-Systemen.

Die Basis-Systeme von Management Unit, HNC und Server Unit x86 sind Systeme, die hohen Sicherheitsansprüchen genügen. Dabei handelt es sich um die statisch implementierte Sicherheit gehärteter Systeme, die durch Administrationsmaßnahmen nicht wesentlich beeinflusst wird.

Die auf SUSE Linux Enterprise Server (SLES) 11 basierenden Basis-Systeme dieser Units (M2000, HNC und X2000) können aus folgenden Gründen als gehärtet bezeichnet werden:

- Nur für den Betrieb zwingend erforderliche signierte Softwarekomponenten werden installiert.
- Für Administration und Operatorzugang werden unprivilegierte Kennungen genutzt. Diese sind im Rahmen eines differenzierten Rollenkonzepts mit klar definierten (und beschränkten) Funktionen und Zugriffsrechten ausgestattet. Außerhalb dieses Rollenkonzepts gibt es keinen Zugang zum System. Eine Rechteeskalation ist nicht möglich, der Zugang zur Kennung `root` ist gesperrt.
- Das Rollen- und Benutzerkonzept erlaubt es, personalisierte Kennungen einzurichten sowie Passwörter und Passworteigenschaften zu verwalten.
- Der Datenverkehr zwischen Administrations-PC und Management Unit, HNC und Server Unit x86 ist verschlüsselt.
- Alle nicht benutzten Ports sind geschlossen. Dienste werden nur dann gestartet, wenn sie wirklich benutzt werden.

Die Konfiguration der Basis-Systeme orientiert sich an den Empfehlungen des Center for Internet Security (CIS, <http://www.cisecurity.org>). Abweichungen von den Empfehlungen ergeben sich nur durch die für den Betrieb erforderlichen Funktionen. Diese Abweichungen führen aber nicht zu Sicherheitslücken.

Im vorliegenden Sicherheitshandbuch werden ausgehend von den Funktionen des Bedien- und Servicekonzepts die Sicherheits- und Härtingsmerkmale auf der Ebene der Basisbetriebssysteme beschrieben. Diese Sicherheits- und Härtingsmerkmale sind an Management Unit, HNC und Server Unit x86 weitgehend identisch. Sie unterscheiden sich nur an den Stellen, wo es die Funktionalität erforderlich macht. Die Aussagen in diesem Handbuch gelten damit immer für alle drei Systeme, sofern nicht gesondert auf spezifische Unterschiede oder besondere Funktionalitäten hingewiesen wird. Gegebenenfalls wird auch auf Unterschiede, die bei Application Units zu beachten sind, eingegangen.



Für die wenigen Fälle, in denen Administrationsmaßnahmen die Sicherheit des Systems tangieren, werden unter der Überschrift **Sicherheitsrelevante Aktionen** Hinweise und Anleitungen zur korrekten Handhabung gegeben.

Sicherheitsrelevante Aspekte von BS2000 oder anderen Betriebssystemen und Anwendungen, die auf oder mittels der Systeme betrieben werden, werden nicht betrachtet.

1.1 Zielsetzung und Zielgruppen des Handbuchs

Dieses Handbuch wendet sich an Sicherheitsbeauftragte und Administratoren eines SE Servers. Kenntnisse der Betriebssysteme BS2000, Linux und ggf. Windows werden vorausgesetzt. Grundkenntnisse der Bedienung von grafischen Oberflächen sind vorteilhaft.

1.2 Konzept des Handbuchs

Das Handbuch fasst die sicherheitsrelevanten Informationen für SE Server zusammen. Dabei werden am SE-Server die Systeme Management Unit, HNC, ,Server Unit x86 und Application Units einzeln betrachtet.

Eine Sonderstellung nehmen die Application Units ein. Im Vergleich zu Management Unit, HNC und Server Unit liegt hier die Administration und Überwachung stärker in der Hand des Anwenders. Die Aussagen in diesem Handbuch gelten deshalb im Allgemeinen nur für Management Unit, HNC und Server Unit x86. Wenn Aussagen auch für Application Units gelten, so ist dies besonders erwähnt.

Bei Management Unit, HNC und Server Unit x86 handelt es sich um speziell durch FUJITSU konfigurierte und gehärtete Systeme.

Dagegen enthält das auf einer Application Unit optional vorinstallierte Betriebssystem keine besonderen Sicherheitsvorkehrungen. Für die Konfiguration eines sicheren Systems ist der Anwender hier allein verantwortlich.

Andererseits unterscheiden sich Management Unit, HNC und Server Unit x86 in ihrer Funktionalität, so dass manche Informationen in diesem Handbuch nur für einige der Systeme gültig sind. In diesem Fall sind die betroffenen Systeme zu Beginn des Abschnittes (in der Überschrift bzw. im Einleitungssatz) aufgeführt.

Die einzelnen Kapitel des Handbuches behandeln die sicherheitsrelevanten Themen.

Die Bedienung und die Verwaltung des SE Servers ist im Handbuch „Bedienen und Verwalten“ [2] und der kontextsensitiven Online-Hilfe des SE Managers detailliert beschrieben. Dort finden Sie auch weiterführende Informationen zur Bedienung der in diesem Sicherheitshandbuch angesprochenen Funktionen.

Informationen zur Sicherheit von BS2000 OSD/BC enthalten die Handbücher „Einführung in die Systembetreuung“ [7] sowie die Handbücher zum Softwareprodukt SECOS [8 und 9].

Readme-Datei

Funktionelle Änderungen der aktuellen Produktversion und Nachträge zu diesem Handbuch entnehmen Sie bitte ggf. der produktspezifischen Readme-Datei.

Readme-Dateien stehen Ihnen online bei dem jeweiligen Produkt zusätzlich zu den Produkthandbüchern unter <http://manuals.ts.fujitsu.com> zur Verfügung. Alternativ finden Sie Readme-Dateien auch auf der Softbook-DVD.

Informationen unter BS2000

Wenn für eine Produktversion eine Readme-Datei existiert, finden Sie im BS2000-System die folgende Datei:

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

Diese Datei enthält eine kurze Information zur Readme-Datei in deutscher oder englischer Sprache (<lang>=D/E). Die Information können Sie am Bildschirm mit dem Kommando `/SHOW-FILE` oder mit einem Editor ansehen.




Das Kommando `/SHOW-INSTALLATION-PATH INSTALLATION-UNIT=<product>` zeigt, unter welcher Benutzerkennung die Dateien des Produkts abgelegt sind.

Ergänzende Produkt-Informationen

Aktuelle Informationen, Versions-, Hardware-Abhängigkeiten und Hinweise für Installation und Einsatz einer Produktversion enthält die zugehörige Freigabemitteilung. Solche Freigabemitteilungen finden Sie online unter <http://manuals.ts.fujitsu.com>.

1.3 Darstellungsmittel

In diesem Handbuch werden folgende **Darstellungsmittel** verwendet:

	Dieses Symbol kennzeichnet wichtige Informationen und Tipps, die Sie beachten sollten, insbesondere den Abschnitt Sicherheitsrelevante Aktionen .
	Dieses Symbol steht mit dem Signalwort ACHTUNG! vor Warnhinweisen, die Sie im Interesse der System- und Betriebssicherheit unbedingt beachten müssen.
	Mit diesem Symbol wird ein Arbeitsschritt, den Sie ausführen müssen, dargestellt.
Kursive Schrift	Zitate aus dem SE Manager
dicktengleich	Systemein- und ausgaben
dicktengleich halbfett	Über die Tastatur einzugebende Anweisungen werden dicktengleich halbfett dargestellt.
<abc>	Variablen, die durch Werte ersetzt werden.
<u>Tastensymbole</u>	Tasten werden entsprechend ihrer Abbildung auf der Tastatur dargestellt. Wenn explizit Großbuchstaben eingegeben werden sollen, so wird die Shift-Taste angegeben, z.B. [SHIFT] - [A] für A. Müssen zwei Tasten gleichzeitig gedrückt werden, so wird dies durch einen Bindestrich zwischen den Tastensymbolen gekennzeichnet.
[zahl]	Literaturhinweise werden im Text in Kurztiteln angegeben. Der vollständige Titel jeder Druckschrift, auf die durch eine Nummer verwiesen wird, ist im Literaturverzeichnis hinter der entsprechenden Nummer aufgeführt.

Bezeichnungen und Abkürzungen

Wegen der häufigen Nennung der Bezeichnungen, werden der Einfachheit und Übersichtlichkeit halber folgende **Abkürzungen** gebraucht:

- **SE Server** für die FUJITSU Server BS2000 SE Serie (Server Units /390 und x86) mit folgenden Modellen:
 - **SE300** für FUJITSU Server BS2000 SE300 (mit SU300, optional AUs)
 - **SE500** für FUJITSU Server BS2000 SE500 (mit SU500, optional SU300 und AUs)
 - **SE700** für FUJITSU Server BS2000 SE700 (mit SU700, optional SU300 und AUs)
- **SU** für die Server Unit unabhängig vom Unit-Typ
Abhängig vom Unit-Typ werden SUs unterschieden:
 - **SU /390** für Server Unit /390 (Typ einer Server Unit mit einem oder mehreren /390 Prozessoren)
 - **SU x86** für Server Unit x86 (Typ einer Server Unit mit einem oder mehreren x86 Prozessoren)

Nach Modellen werden folgende SUs unterschieden:

- **SU300** für die Server Unit vom Unit-Typ SU x86 in SE300, optional in SE500 / SE700
- **SU500** für die Server Unit vom Unit-Typ SU /390 in SE500
- **SU700** für die Server Unit vom Unit-Typ SU /390 in SE700
- **MU** für die Management Unit. Die MU ermöglicht zentrales, komfortables und systemübergreifendes Management am SE Server.
- **AU** für die Application Unit (auf unterschiedlicher Hardware-Basis)
Die Modelle werden abhängig von der Hardware-Basis unterschieden. **AU47** ist z.B. eine Application Unit auf Basis eines PRIMERGY RX4770.
- **HNC** (High Speed Net Connect)
Der HNC verbindet die Server Unit /390 mit dem LAN und ermöglicht als Net-Client den BS2000-Systemen auf der SU /390 den Zugriff zum Net-Storage. HNC ist außerdem auch die Bezeichnung für die HNC-Software.
- **SKP** (Service Konsol Prozessor)
Die SKP-Funktionalität für eine SU /390 ist in der MU bzw. im SE Manager integriert.
- **SVP** (Service Prozessor)
Die SVP-Funktionalität für eine SU /390 ist in der MU bzw. im SE Manager integriert.

- **BS2000-Server** als Oberbegriff für SE Server, S- und SQ-Server. BS2000-Server werden mit dem entsprechenden BS2000-Betriebssystem betrieben.
- **S-Server** für die Business Server der S-Serie (/390-Architektur)
- **SQ-Server** für die Business Server der SQ-Serie (x86-Architektur)
- **BS2000** für das Betriebssystem BS2000 OSD/BC.

1.4 Open-Source-Software

Die Linux-basierte Basis-Software M2000, X2000 und HNC, die auf Management Unit, Server Unit x86 und HNC installiert ist, beinhaltet Open-Source-Software. Die Lizenzen dazu finden Sie auf der jeweiligen Installations-DVD im Verzeichnis LICENSES.

2 Architektur der SE Server und der Netzwerke

2.1 Hardware

Ein FUJITSU Server BS2000 der SE Serie (kurz: SE Server) besteht im Maximalausbau aus folgenden Komponenten:

- Management Unit (MU) mit SE Manager
Es können eine oder zwei MUs mit redundanter SKP-Funktionalität installiert werden.
- Server Units
 - Eine /390-basierte Server Unit (SU /390) ermöglicht den Betrieb von BS2000 (Native-BS2000 oder VM2000).
 - Eine x86-basierte Server Unit (SU x86) ermöglicht den Betrieb von BS2000 (Native-BS2000 oder VM2000). Optional ist zusätzlich der XenVM-Betrieb mit Linux- oder Windows-Gastsystemen möglich.
- Application Units (AU)
Am SE Server können AUs betrieben werden. Eine AU ermöglicht den Betrieb von Applikationen unter Linux, Windows, VMware oder anderen Hypervisoren.
- Net Unit (für SU /390 mit HNC)
- Rack-Konsole und KVM-Switch
- Peripherie (Storage)
- Optionale Hardware-Komponenten:
ETERNUS JX40 (für SU x86, AU), ETERNUS LT40 S2 (für SU x86), FC-Switches

2.2 Architektur der SE Server

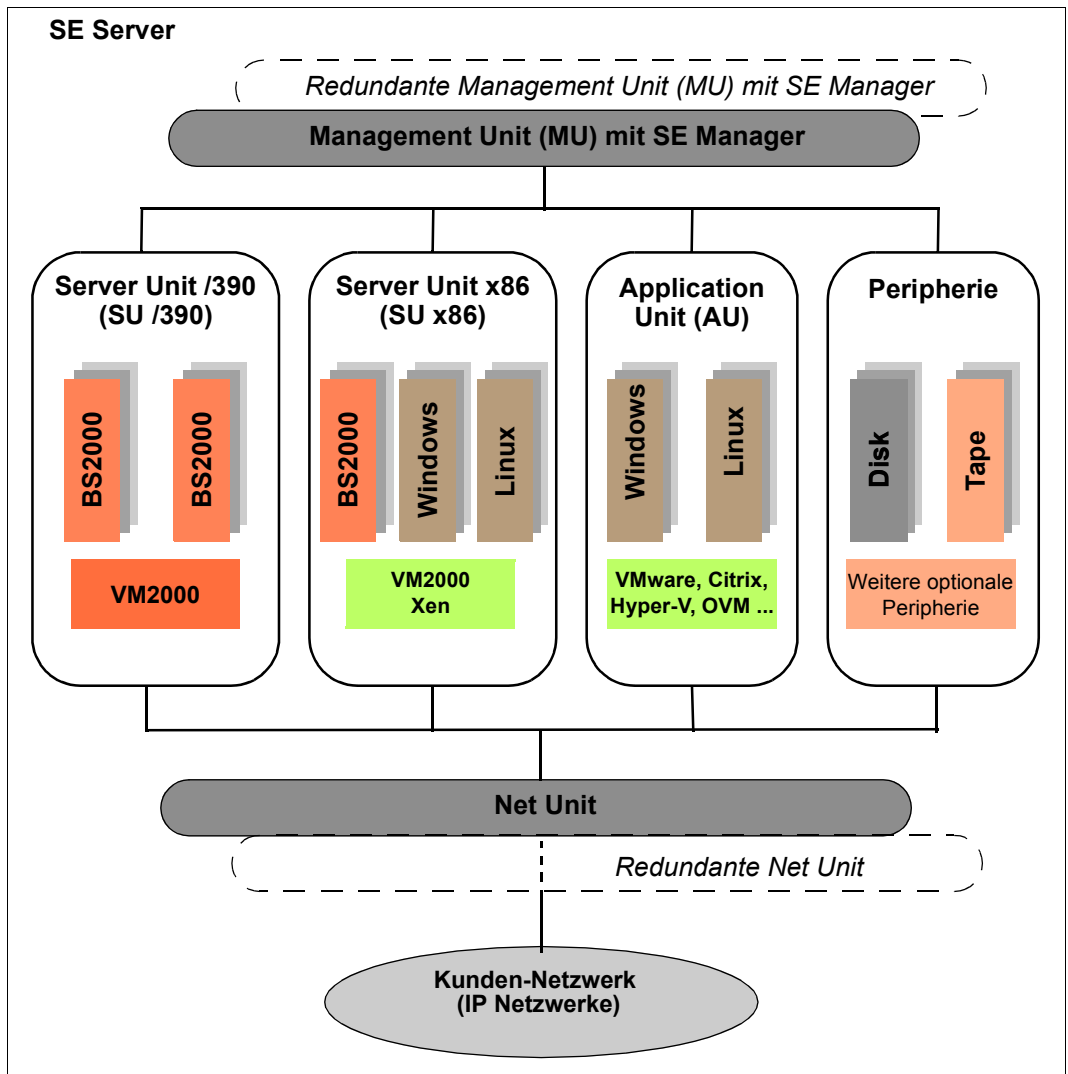


Bild 1: Architektur der SE Server

Mit dem SE Manager jeder MU können Sie alle Komponenten des SE Servers zentral bedienen und verwalten.

Wenn zwei MUs installiert sind, dann müssen Sie die Sicherheitsvorkehrungen an beiden MUs durchführen, siehe [Seite 17](#).

Die Net Unit bietet höchste Performance und Sicherheit für die interne Kommunikation in einem SE Server und für die Anbindung an Kundennetzwerke (IP Netzwerke).



Sicherheitsrelevante Aktionen

Die folgenden sicherheitsrelevanten Einstellungen und Maßnahmen müssen ggf. an beiden MUs vorgenommen werden:

- Sie müssen die Benutzerkennungen an beiden MUs gleich einrichten und für Operatorkennungen die gleichen individuellen Berechtigungen vergeben. Siehe [Abschnitt „Rollenkonzept und Benutzerkennungen“ auf Seite 19](#).
- Sie müssen die Sicherheitseinstellungen für den Service-Zugang an jeder MU festlegen, siehe [Abschnitt „Funktion „Schattenterminal“ nutzen“ auf Seite 56](#) und [Abschnitt „Zugang zu externen Assets“ auf Seite 58](#).
- Sie müssen die Konfiguration der IP-Adressen und Netzwerke für beide MUs gleich einrichten, siehe [Kapitel „Netzwerksicherheit“ auf Seite 61](#).
- Sie müssen an jeder MU ein Zertifikat bestätigen bzw. importieren, siehe [Abschnitt „Digitale Zertifikate“ auf Seite 67](#).

2.3 Netzwerke

Die Net Unit realisiert den Anschluss der Units an die Netzwerke des SE Servers und an Kunden-Netzwerke. Zusätzlich stehen private Netzwerke zur internen Kommunikation im SE Server bereit.

Die folgenden logischen Netzwerke werden unterstützt:

- Öffentliche Management-Netzwerke
 - Management Admin Network Public (MANPU)
 - Management Optional Admin Network Public (MONPU): bei Bedarf kann das additive Administrations-Netzwerk eingerichtet werden (z. B. wenn AIS Connect nicht über MANPU betrieben werden soll).
- Private Management-Netzwerke
 - Management Control Network Private (MCNPR) für die SE Server-Kommunikation
 - Management Optional Network Private (MONPR): bei Bedarf können bis zu 8 additive Netzwerke MONPR<n> (mit <n>= 01..08) für die SE Server-Kommunikation eingerichtet werden.
 - Management Control Network Local (MCNLO) für die lokale SE Server-Kommunikation

- Management SVP Network Private (MSNPR) ermöglicht an SE700/SE500 die SVP-Kommunikation zur SU /390
- Öffentliche Daten-Netzwerke
 - Data Network Public (DANPU): bei Bedarf können bis zu 8 Netzwerke DANPU<n> (mit <n>= 01..08) für die Anbindung von Anwendungen an das öffentliche Kunden-netzwerk eingerichtet werden.
- Private Daten-Netzwerke
 - Data Network Private (DANPR): bei Bedarf können bis zu 99 Netzwerke DANPR<n> (mit <n>= 01..99) für SE Server interne private Kundennetzwerke ein-gerichtet werden.

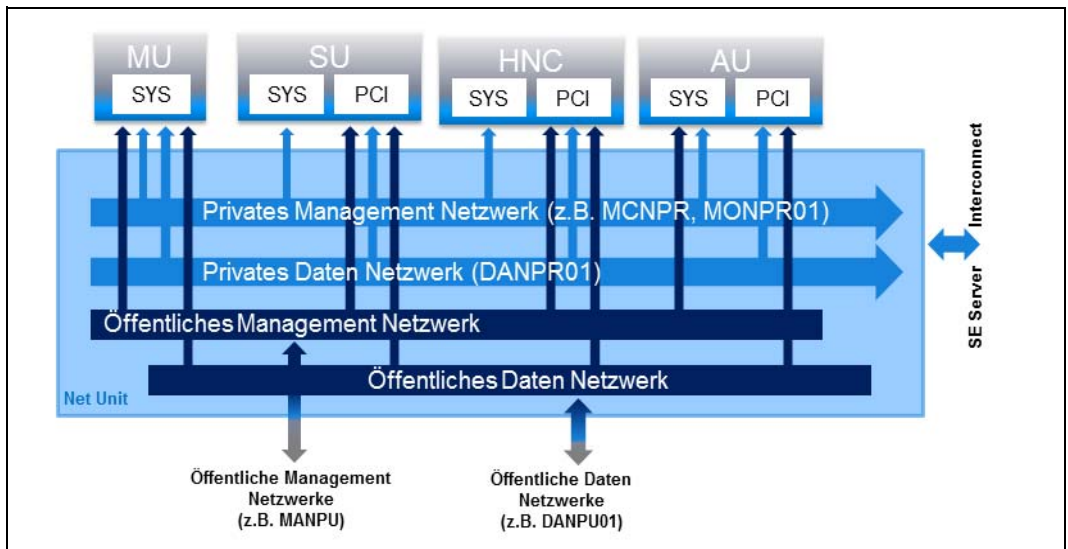


Bild 2: Net Unit Blockschaltbild

Durch die Nutzung verschiedener Netzwerke können Komponenten eines Netzwerkes das andere Netzwerk nicht beeinflussen, d.h. die Netzwerke sind abgeschottet.

Weiter können in der Net Unit Konfiguration die ACL Dienste (TCP/UDP Ports) der Netzwerke DANPU<xx>, MANPU, MONPU, DANPR<xx> und MONPR<xx> eingeschränkt werden.

Die Basisbetriebssysteme von HNC und SU x86 sind nur über die internen Netzwerke erreichbar und sind damit gegenüber den Kundennetzwerken abgeschottet.

Zusätzlich zu den Anschlüssen der Units an die Switches der Net Unit können (für die Nutzung durch die Gastssysteme) auch Direktleitungen von den Units in das Kundennetzwerk eingesetzt werden.

3 Sicherer Zugang zu Management-Funktionen

3.1 Rollenkonzept und Benutzerkennungen

Kennungen und Berechtigungen werden zentral an der Management Unit verwaltet. Wenn der SE Server über eine zweite MU verfügt, müssen Sie Kennungen und Berechtigungen an beiden MUs gleich einrichten und Änderungen an beiden MUs durchführen.

3.1.1 Rollenkonzept und Rollenrechte

Ein wesentlicher Bestandteil des Sicherheitskonzepts ist das Rollenkonzept mit folgenden Eigenschaften:

- Die Rollen sind abgestuft:
Jeder Rolle stehen nur die notwendigen Oberflächen und Funktionen zur Verfügung.
- Jede Benutzerkennung ist einer Rolle fest zugeordnet.
- Eine Rechteeskalation ist nicht möglich, d.h. der Zugang (oder Übergang) zu anderen Oberflächen und Funktionen als den vorgesehenen ist nicht möglich. Insbesondere ist der Zugang zur Kennung `root` des Basisbetriebssystems nicht möglich.
- Rollen
Für Anwender sind folgende Rollen definiert:
 - Administrator
 - BS2000-Administrator (ab M2000 V6.1A)
 - Operator
 - XenVM-Administrator (ab M2000 V6.1A)
 - AU-Administrator
 - Service

Die Rolle Administrator ist den Rollen BS2000-Administrator, Operator, XenVM-Administrator und AU-Administrator übergeordnet und ist berechtigt alle Funktionen des SE Managers und des empfohlenen CLI auszuführen.

Die Rolle Service ist ausschließlich dem Service vorbehalten.

Die Rollen BS2000-Administrator, Operator, XenVM-Administrator und AU-Administrator besitzen eingeschränkte Rechte, die auf ihre getrennten Aufgabenbereiche zugeschnitten sind:

- Ab M2000 V6.1A: Ein BS2000-Administrator besitzt die Berechtigung für Funktionen des SE Managers die für Betrieb und Operating von BS2000-Systemen notwendig sind. Zusätzlich besitzt er noch einige Administrator-Berechtigungen: Ein-/Ausschalten der Units SU, MU und HNC, Durchführung von CSR-Sicherung, Erstellung von Diagnosedaten, Zugang zum Schattenterminal, Lesezugriff zum Hardware-Inventory und Konfiguration für zeitgesteuertes Ein-/Ausschalten der Units SU, MU und HNC.
- Ein Operator besitzt nur die Berechtigung für Funktionen des SE Managers, die für Betrieb und Operating von BS2000-Systemen notwendig sind. Zusätzlich kann der Administrator bestimmte Berechtigungen individuell für eine Operatorkennung konfigurieren.
- Ein XenVM-Administrator besitzt nur die Berechtigung für Funktionen des SE Managers die für Betrieb und Operating von XenVM-Systemen notwendig sind.
- Ab M2000 V6.1A: Ein AU-Administrator besitzt die Berechtigung für Funktionen des SE Managers die für Betrieb und Operating der Systeme auf AUs notwendig sind. Zusätzlich besitzt er noch einige Administrator-Berechtigungen: Ein-/Ausschalten der AUs, Lesezugriff zum Hardware-Inventory und Konfiguration für zeitgesteuertes Ein-/Ausschalten der AUs.

Übersichten zu den rollenspezifischen Aufgaben und Funktionen finden Sie im Handbuch „Bedienen und Verwalten“ [2] bzw. in der Online-Hilfe.

- Individuelle Berechtigungen

Der Administrator kann einer Operatorkennung für bestimmte Funktionen des SE Managers Berechtigungen erteilen oder entziehen. Unterschieden werden dabei serverbezogenen und systembezogene Berechtigungen.

Die nachfolgenden Berechtigungen sind serverbezogene Berechtigungen:

- *Ein/Aus*
Zeigt an, ob der Operator die Berechtigung zum Ein-/Ausschalten von Units besitzt (*Erlaubt* oder *Blockiert*).
Wenn die Berechtigung besteht, kann der Operator alle Units, die in der Unit-Übersicht angezeigt werden, im Notfall ein- oder ausschalten.
- *Schatten*
Zeigt an, ob der Operator Zugang zum Schatten-Terminal besitzt (*Erlaubt* oder *Blockiert* dem Service-Techniker den Zugang).

- *SVP*
Nur an SE Servern mit SU /390:
Zeigt an, ob der Operator die SVP-Berechtigung besitzt (*Erlaubt* oder *Blockiert* z.B. IPL und Shutdown).

Die nachfolgenden Berechtigungen sind systembezogene Berechtigungen:

- *Unit*
Unit, für die systembezogene Rechte, genauer Konsol-Berechtigungen, vergeben sind. Die Zugangsrechte zu BS2000-Systemen einer SU /390 werden für die Management Unit eingetragen, wobei der BCAM-Name der SU /390 in Klammern dahinter angezeigt wird. Die Zugangsrechte zu BS2000-Systemen einer SU x86 werden für die jeweilige SU x86 eingetragen.
- *Konsol-Berechtigungen*
Zeigt an, zu welchen Systemen der Operator die Berechtigung zum Konsolzugang besitzt. Die erlaubten Systeme sind explizit mit KVP und Konsol-MN eingetragen.
- *Dialog*
Zeigt an, ob der Operator die Berechtigung zum BS2000-Dialogzugang besitzt (*Erlaubt* oder *Blockiert* den Zugang). Diese Berechtigung kann nur vergeben werden, wenn mindestens eine Konsol-Berechtigung eingetragen ist.



Sicherheitsrelevante Aktionen

Folgende Funktionen des SE Managers kann ein Administrator für das Operating freigeben oder sperren (siehe Hauptmenü *Berechtigungen* → *Benutzer* → *Individuelle Berechtigungen*):

- Ein-/Ausschalten von Units
- Zugang zu einem Schattenterminal
- Zugang zum SVP (nur SE Server mit SU /390)
- Zugang zu einer BS2000-Konsole an einem bestimmten BS2000-System
- Zugang zum BS2000-Dialog an einem bestimmten BS2000-System

Wenn der SE Server über eine zweite MU verfügt, müssen Sie sich an der anderen MU anmelden und dort dieselben Aktionen durchführen!

3.1.2 Benutzerkennungen

(Benutzer-)Kennungen sind den Rollen und Verwendungen eindeutig zugeordnet.

Die Kennungen haben folgende rollenspezifischen Eigenschaften:

Administration

- Es gibt die vordefinierte, nicht löschbare Administratorkennung `admin`.
- Es können beliebig viele Administratorkennungen angelegt werden. Diese Kennungen können wieder gelöscht werden.
- Vom Funktionsumfang her sind alle Administratorkennungen gleichwertig.

BS2000-Administration (ab M2000 V6.1A)

- Es können beliebig viele BS2000-Administratorkennungen angelegt werden. Diese Kennungen können wieder gelöscht werden.
- Vom Funktionsumfang her sind alle BS2000-Administratorkennungen gleichwertig.

Operating

- Es können beliebig viele Operator Kennungen angelegt werden. Diese Kennungen können wieder gelöscht werden.
- Vom Funktionsumfang her sind alle neu eingerichteten Operator Kennungen zunächst gleichwertig. Durch Vergabe von individuellen Berechtigungen lässt sich der Funktionsumfang individuell erweitern.

XenVM-Administration

- Es können beliebig viele XenVM-Administratorkennungen angelegt werden. Diese Kennungen können wieder gelöscht werden.
- Vom Funktionsumfang her sind alle XenVM-Administratorkennungen gleichwertig.

AU-Administration (ab M2000 V6.1A)

- Es können beliebig viele AU-Administratorkennungen angelegt werden. Diese Kennungen können wieder gelöscht werden.
- Vom Funktionsumfang her sind alle AU-Administratorkennungen gleichwertig.

Service

- Es gibt die vordefinierte, nicht löschbare Servicekennung `service`.
Siehe auch [Abschnitt „Weitere Kennungen des Basis-Systems“ auf Seite 24](#).

3.1.2.1 Berechtigung zur Kennungsverwaltung

Nur unter einer Administratorkennung können andere Kennungen (unabhängig vom Typ) verwaltet werden. Im Einzelnen umfasst dies folgende Funktionen:

- Kennung anlegen
- Kennung löschen
- Passwort und Passworteigenschaften für Kennungen verwalten



Sicherheitsrelevante Aktionen

- Die vordefinierte Kennung `admin` ist mit dem Standardpasswort `admin` initialisiert.
Ändern Sie bei der Inbetriebnahme das Passwort der vordefinierten Kennung sofort.
- Neue Kennungen sollten „personalisiert“ angelegt werden.
Das bedeutet, dass die Zuordnung der Kennung zu einer Person mit einem bestimmten Namen sofort erkennbar ist.
- Beim Anlegen einer Kennung vergeben Sie ein Passwort, das 6-20 Zeichen lang sein muss.

3.1.2.2 Weitere Kennungen des Basis-Systems

Folgende Kennungen sind dem Service vorbehalten:

- `service`
Die Kennung `service` dient dem Service (lokal und per Remote Service) als Zugangs- und Diagnosekennung.
Service-Kennungen (Kennungen mit der Rolle Service) werden in der Benutzerverwaltung angezeigt, unterliegen aber nicht der Kennungsverwaltung durch den Administrator.
- `tele`
Die Kennung `tele` dient dem Service als Zugangskennung und zur Bedienung des Schattenterminals.
- `root` und `vroot`
Die Kennung `root` ist gesperrt. Die Kennung `vroot` ist eine virtuelle Kennung ohne Shell und ohne home-Verzeichnis. Sie ist ausschließlich der Service-Zentrale vorbehalten, um in schwerwiegenden Fehlersituationen die Rechte der Kennung `service` weiter als vorgesehen zu eskalieren (erweitern).

Außerdem existieren noch folgende intern benötigten Kennungen, die jedoch für die Anmeldung gesperrt sind:

- `x2kinternal` sowie die AIS-Kennung `c2suxadm`.
- `storman`, wenn das Add-on Pack StorMan installiert ist.
- `opensm2`, wenn das Add-on Pack openSM2 installiert ist.
- `openutm`, wenn das Add-on Pack openUTM installiert ist.
- `robar`, wenn das Add-on Pack ROBAR-SV installiert ist.

3.1.2.3 Kennungen für Add-on Packs

Für Add-on Packs gilt allgemein:

- Add-ons haben in der Regel eine eigene Benutzer- und Rollenverwaltung. Diese Benutzer- und Rollenverwaltung wird beibehalten.
- Kennungen in Add-ons sind erst wirksam, wenn sie auch als Kennungen im SE Manager definiert sind.

Im SE Manager werden keine expliziten Berechtigungen für einzelne Add-ons vergeben. Die Aufrufberechtigungen für Add-ons ergeben sich implizit aus der Rolle der Benutzerkennung, mit der der Anwender am SE Manager angemeldet ist, und können innerhalb der Add-on Packs gemäß deren Benutzer- und Rollenkonzept verändert werden.

3.1.3 Authentisierung

Der Zugang zum SE Manager einer MU ist nur mit Authentisierung über Kennung und Passwort möglich.

Für Kennungen wird gegen das Passwort geprüft, das in der Datei `/etc/shadow` hinterlegt ist.

Für die Authentisierung wird eine geeignete fest eingestellte PAM-Konfiguration (PAM = Pluggable Authentication Modules) eingesetzt. Die PAM-Konfiguration wird in folgenden Fällen genutzt:

- SSH-Anmeldung auf Shell-Ebene
- Anmeldung an der Web-Oberfläche
- Anmeldung am Gnome-Desktop der lokalen Konsole

Die Passwordeingabe geschieht verdeckt (Darstellung des Passworts mit Punkten), Passwörter können somit nicht ausgespäht werden.

Wenn die Anmeldung am SE Manager scheitert, ist eine erneute Anmeldung erst nach einer Wartezeit von 10 Sekunden möglich. Diese Wartezeit schützt vor automatisierten Einbruchversuchen.

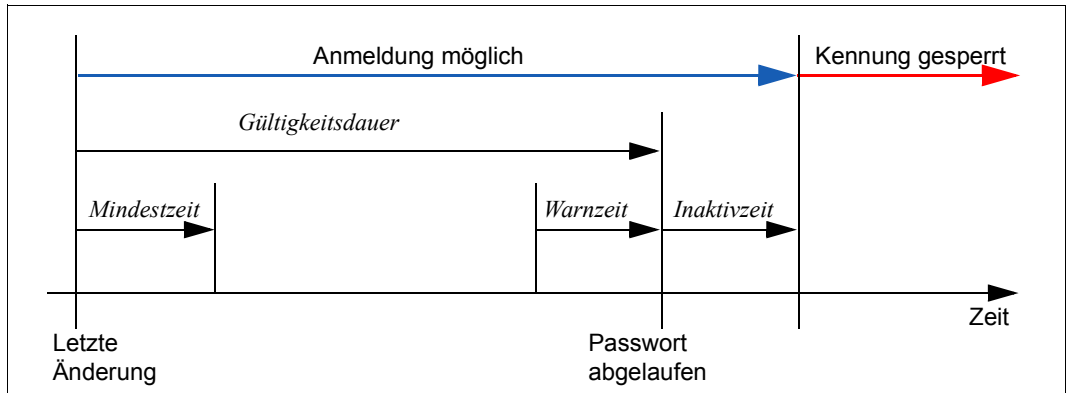
3.1.4 Passwortverwaltung für Kennungen

Die Passwörter der Kennungen haben folgende Attribute:

Gültigkeitsdauer, Warnzeit, Mindestzeit, Inaktivzeit:

- Während der Gültigkeitsdauer, die ab dem letzten Setzen des Passworts gilt, ist die Anmeldung unbeschränkt möglich.
- Während der Mindestzeit kann ein Nicht-Administrator das eigene Passwort nicht verändern.
- Während der Warnzeit wird eine Warnung ausgegeben, dass das Passwort bald ausläuft. Die Anmeldung ist aber ohne Einschränkungen möglich.
- Während der Inaktivzeit ist das Passwort zwar abgelaufen, eine Anmeldung ist aber trotzdem möglich. Direkt bei der Anmeldung wird eine Passwortänderung verlangt.
- Nach Ablauf der Inaktivzeit ist die Kennung gesperrt. Sie kann von einer (anderen) Administratorkennung aus oder notfalls durch den Service wieder geöffnet werden.
- Der Wert `-1` bei der *Inaktivzeit* führt dazu, dass die Inaktivzeit nicht abläuft.
- Der Wert `99999` für die *Gültigkeitsdauer* bedeutet in der Praxis, dass Sie das Passwort nicht ändern müssen.

Die folgende Grafik zeigt, wie sich diese Zeiten zueinander verhalten.



Auf der Basis der Einstellungen für die Systemhärtung werden Kundenkennungen mit folgenden Default-Werten für die Passwortverwaltung angelegt:

- Gültigkeitsdauer des Passworts: 60 Tage
- Mindestzeit bis zur nächsten Änderung des Passworts: 7 Tage
Für eine Administratorkennung ist die Mindestzeit irrelevant und wird auch nicht angezeigt.
- Warnzeit vor Ablauf des Passworts: 7 Tage
- Inaktivzeit nach Ablauf des Passworts: 7 Tage

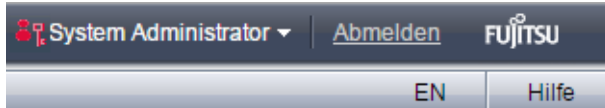
Jeder Administrator kann jederzeit einzelne Einstellungen der Passwortverwaltung einer Kennung ändern.

Ein Nicht-Administrator kann nur das Passwort der eigenen Kennung ändern. Dies ist aber nur möglich, wenn die Mindestzeit verstrichen ist.

Wenn ein Nicht-Administrator sein Passwort auf Shell-Ebene ändert, greifen die Sicherheitseinstellungen des Basisbetriebssystems: Das Passwort muss sich von den letzten 10 Passwörtern unterscheiden und es muss den üblichen Komplexitätsanforderungen genügen.

Bei der Anmeldung an der Web-Oberfläche ergeben sich bezüglich des Passwortzustands und der Passwortverwaltung je nach Rolle die folgenden Situationen:

- Wenn sich die aktuelle Kennung in der Warnzeit befindet, wird dies in der Kopfzeile des Hauptfensters durch ein Warn-Icon angezeigt:



Zusätzlich zeigt ein Tooltip dem Anwender, nach wievielen Tagen sein Passwort abläuft.

- Wenn sich eine Kennung in der Inaktivzeit befindet, ist eine Anmeldung zwar noch möglich, im Anmeldefenster wird aber eine sofortige Passwortänderung erzwungen.

Anmeldung

System: **exmp1.example.net**
Bitte melden Sie sich mit Ihrer Kennung und Ihrem Passwort an.

! Das Passwort ist abgelaufen. Ein neues Passwort muss vergeben werden!

Kennung

Altes Passwort

Neues Passwort

Neues Passwort (Wiederholung)

- Wenn die Inaktivzeit verstrichen ist, ist die Kennung gesperrt und es ist keine Anmeldung mehr möglich. Ein Eingriff seitens eines (anderen) Administrators oder des Service ist dann notwendig (siehe „[Sicherheitsrelevante Aktionen](#)“ auf Seite 28).

Auf Shell-Ebene gilt beim Anmelden das bekannte Verhalten in Linux-Systemen:

- Während der Warnzeit wird bei der Anmeldung eine Warnung ausgegeben, z.B. Your password will expire in 2 days.

- Während der Inaktivzeit wird bei der Anmeldung die Passwortänderung erzwungen, z.B.:

```
login as: test1
Authorized use only!
Using keyboard-interactive authentication.
Password: *****
Using keyboard-interactive authentication.
Your password has expired. Choose a new password.
Old Password: *****
New Password: *****
Using keyboard-interactive authentication.
Reenter New Password: *****
Password changed.
...
```



Die Passwordeingabe ist nicht sichtbar, im obigen Beispiel wurde sie mit ***** dargestellt.

- Wenn die Inaktivzeit verstrichen ist, ist die Kennung gesperrt und es ist keine Anmeldung mehr möglich. Die Anmeldung scheitert ohne Angabe eines Grunds.



Sicherheitsrelevante Aktionen

- Der Administrator kann die Einstellungen für die Passwortverwaltung den jeweiligen Sicherheitsrichtlinien im Data Center anpassen. Die Einstellungen können nur für einzelne Kennungen und nicht pauschal für alle Kennungen des Systems geändert werden.
- Jeder Anwender ist aufgefordert, sein Passwort so zu pflegen, wie es die Sicherheitsrichtlinien in seinem Data Center vorsehen.
- Es kann vorkommen, dass eine Kennung wegen Überschreitung der Inaktivzeit gesperrt ist. In diesem Fall kann ein (anderer) Administrator für diese Kennung die Sperre für genau eine Anmeldung aufheben. Dazu dient die Funktion *Passwortänderung erzwingen* (siehe die Online-Hilfe).
- Der Service ist immer in der Lage, die Sperre für eine Kennung aufzuheben.
- Falls nötig (z.B. aufgrund von Sicherheitsrichtlinien), ist der Kunde in der Lage, die Passwörter aller Kennungen selbst zu verwalten. Es wird jedoch dringend empfohlen, dies nur in Absprache mit dem Service zu tun.

3.2 Zugang zum SE Manager

3.2.1 Sicherheitseinstellungen auf dem Administrations-PC

Die Software-Voraussetzungen für den Administrations-PC finden Sie im Handbuch „Bedienen und Verwalten“ [2] bzw. in der Online-Hilfe. Von diesen Voraussetzungen sind folgende Punkte sicherheitsrelevant:

- **Die Ausführung von JavaScript ist im Web-Browser möglich und erlaubt.**
Wenn die Ausführung von JavaScript auf dem Administrations-PC nicht erlaubt ist, kann der SE Manager nicht benutzt werden.
- **Cookies werden im Web-Browser zugelassen.**
Wenn auf dem Administrations-PC keine Cookies zugelassen werden, kann der SE Manager nicht benutzt werden.

Der SE Manager erzeugt und benutzt mehrere Cookies:

- Ein Cookie dient der Verwaltung der Session.
- Ein weiteres Cookie speichert Session-übergreifend die vom Benutzer explizit im SE Manager vorgenommene Spracheinstellung.
- Darüber hinaus werden weitere temporäre Cookies verwendet für die Verwaltung aktueller Einstellungen (z.B. Klappzustand der Primärnavigation) oder für andere technische Zwecke (z.B. für variable Objektlisten der Primärnavigation).



Sicherheitsrelevante Aktionen

- Web-Browser bieten je nach Konfiguration die Funktion *Passwort speichern* an. Es wird davon abgeraten diese Funktion zu benutzen, da dann in der Regel auch eine Funktion *Passwort anzeigen* verfügbar ist, die die Passwörter im Klartext anzeigt.

3.2.2 Kommunikation mit Verschlüsselung

Die Kommunikation erfolgt grundsätzlich über HTTPS (HyperText Transfer Protocol Secure), wobei die darunter liegenden Verschlüsselungsprotokolle SSL 3.0 (Secure Sockets Layer) und TLS 1.0 (Transport Layer Security) unterstützt werden. SSL 2.0 wird nicht unterstützt.

Für HTTP-Aufrufe findet eine automatische Umlenkung nach HTTPS statt. Dies gilt sowohl für die externe Kommunikation zwischen dem Administrations-PC und einem der Systeme Server Unit, Management Unit oder HNC als auch für die interne Kommunikation dieser Systeme untereinander.

3.2.3 Session-Management

Der SE Manager ist gegen den unbefugten Zugang sowohl durch die Authentisierung als auch durch das sogenannte Session-Management geschützt.

Nach dem Login wird pro Client (Browser-Instanz des aufrufenden Web-Browsers) und System eine Sitzung (Session) aufgebaut, deren Gültigkeit permanent überwacht wird.

Im Menü *Berechtigungen* → *Benutzer* informiert die Registerkarte *Sitzungen* den Administrator über alle Sessions der Benutzer, die aktuell am SE Manager der lokalen Management Unit angemeldet sind. Angezeigt werden neben den Informationen zu Benutzer und IP-Adresse des PCs auch die aktuelle individuelle Einstellung für die Session.

Eine Session endet in folgenden Fällen:

- explizit durch *Abmelden* im Kopfbereich des Hauptfensters
- durch Session-Timeout (Voreinstellung: nach 20 Minuten Inaktivität im SE Manager)

In beiden Fällen erhalten Sie die Login-Seite für die erneute Anmeldung, beim *Abmelden* sofort und bei Session-Timeout mit der ersten Aktion, die nach Eintritt des Session-Timeout erfolgt.

Fenster, in denen Terminals geöffnet werden, unterliegen nicht dem Session-Management. Dies gewährleistet eine unterbrechungsfreie Nutzung der folgenden Zugangsfunktionen:

- Zugang zu BS2000-Konsole und BS2000-Dialog
- Zugang zur XenVM-Konsole
- Zugang zum CLI (Shell)
- Zugang zum Schattenterminal (Remote Service)
- Zugang zur SVP-Konsole der SU /390



Sicherheitsrelevante Aktionen

- Jeder Anwender kann die Einstellung für den Session-Timeout für sich persönlich ändern:
 - ▶ Klicken Sie im Kopfbereich auf die Anmeldeinformation. Es öffnet sich eine Liste mit dem Menüpunkt *Individuelle Einstellungen*.
 - ▶ Klicken Sie *Individuelle Einstellungen*. Es öffnet sich der Dialog „Aktualisierungszyklus und Session-Timeout ändern“, in dem Sie den Session-Timeout aktivieren/deaktivieren und die Ablaufzeit im Bereich von 5 bis 60 Minuten einstellen können.

Die individuelle Einstellung wird Browser-spezifisch gespeichert.

Zusätzlich zur Sperre des Administrations-PCs werden beim Verlassen des Arbeitsplatzes folgende Schutzmaßnahmen empfohlen:

- Explizites Abmelden vom SE Manager.
- Schließen aller Fenster, die ein Terminal geladen haben.
Falls die Anwendung über einen eigenen Sperrmechanismus verfügt (z.B. die Konsolbildschirme), kann das Fenster geöffnet bleiben und der verfügbare Sperrmechanismus benutzt werden.

3.3 Textbasierter Zugang (auf Shell-Ebene)

3.3.1 Verschlüsselte Kommunikation mit Secure Shell

Die Kommunikation erfolgt stets verschlüsselt über das SSH-Protokoll.

Dies gilt für die interne Kommunikation (z.B. bei den Verbindungen zu BS2000-Konsolen an SU x86) und die externe Kommunikation (z.B. zwischen SSH-Client und dem System).

3.3.2 Keine Rechteeskalation

Eine Rechteeskalation mit dem Linux-Kommando `su` im Basisbetriebssystem ist nicht möglich.

3.3.3 Zugangsfunktionen im SE Manager

Beim Aufruf folgender Funktionen wird ein im SE Manager integriertes Terminal in einem eigenen Fenster geladen:

- Zugang zu BS2000-Konsole und -Dialog
- Zugang zur XenVM-Konsole
- Zugang zum CLI
- Schattenterminal (im Registerblatt *Remote Service*)
- Zugang zum SVP der SU /390

3.3.4 Zugang zu BS2000-Konsole im KVP-Menü sperren

Details zum KVP-Menü sind im Handbuch „Bedienen und Verwalten“ [2] beschrieben.



Sicherheitsrelevante Aktionen

Das Konsolfenster können Sie beim Verlassen des Arbeitsplatzes sperren:

- ▶ Öffnen Sie im Konsolfenster mit der Taste `[F2]` das KVP-Menü.
- ▶ Sperren Sie die Konsole mit `[2]`.
- ▶ Entsperren Sie die Konsole wieder mit `[1]` und geben Sie anschließend das Passwort der Linux-Benutzererkennung ein, die der benutzten Kennung zugeordnet ist.

3.4 Alternative Zugänge mit Secure Shell

Zur Kommunikation auf Shell-Ebene können Sie alternativ zu dem im SE Manager integrierten Terminal den SSH-Client PuTTY (ab Version 0.63) benutzen. Siehe [Abschnitt „Alternativer Zugang zum BS2000-Betriebssystem mit PuTTY“ auf Seite 46](#).

Die nachfolgenden Beispiele beziehen sich auf den SSH-Client PuTTY.

3.4.1 Secure Shell Host-Schlüssel

Bei der Systeminstallation wird auf dem System ein sogenannter Hostschlüssel („host key“) erzeugt.

Bei der ersten Verbindungsaufnahme müssen Sie (je nach SSH-Client) diesen Hostschlüssel ggf. wie im nachfolgenden Beispiel mit PuTTY bestätigen.



3.4.2 Kommunikation mit Secure Shell-Schlüsseln

Die SSH-Authentisierung ist nicht nur mittels Kennung und Passwort, sondern auch mittels eines SSH-Schlüsselpaares möglich.

Insbesondere ist diese Authentisierung beim Programmieren von automatisierten Abläufen zu bevorzugen, da damit die Codierung eines Passwortes im Klartext vermieden werden kann.



Sicherheitsrelevante Aktionen

Als Administrator können Sie SSH-Schlüssel(paare) ablegen.

Die abgelegten Schlüssel können Sie zusätzlich durch sogenannte „Passphrasen“ schützen.

Das damit zusammenhängende Schlüssel-Management wird im nächsten Abschnitt detailliert beschrieben.

3.4.3 Generierung der Schlüssel

Authentifizierung und Verschlüsselung basieren in SSH auf dem asymmetrischen System der öffentlichen und privaten Schlüssel. Ver- und Entschlüsselung werden mit verschiedenen Schlüsseln durchgeführt. Dabei ist es nicht möglich, den Schlüssel für die Entschlüsselung von demjenigen für die Verschlüsselung herzuleiten. Zu diesem Zweck generiert der Benutzer ein Schlüsselpaar, das aus einem öffentlichen und einem privaten Schlüssel besteht. Der öffentliche Schlüssel ist zur Weitergabe an andere Benutzer gedacht, wohingegen der private Schlüssel vom Benutzer nicht weitergegeben wird.

Die beiden Schlüssel werden auf folgende Art benutzt:

Authentifizierung

- Bei der Anmeldung eines Benutzers an einem remote System erzeugt dieses System eine Zufallszahl, verschlüsselt sie mit dem öffentlichen Schlüssel des Benutzers und sendet sie an das lokale System zurück. Zur Entschlüsselung dieser kodierten Zufallszahl ist der passende private Schlüssel erforderlich; das entschlüsselte Datum wird nun an das remote System zurückgeschickt und dort geprüft, dadurch authentisiert sich der Besitzer dieses privaten Schlüssels.
- Mit dem privaten Schlüssel können Signaturen (z.B. für eine digitale Unterschrift) erzeugt werden. Eine mit einem privaten Schlüssel erzeugte Signatur kann von niemandem nachgemacht werden, der diesen Schlüssel nicht besitzt.

Jeder, der den dazugehörigen öffentlichen Schlüssel besitzt, kann verifizieren, dass eine Signatur echt ist.

Verschlüsselung

- Der öffentliche Schlüssel kann auch dazu benutzt werden, eine Nachricht an jemanden, der den dazugehörigen privaten Schlüssel besitzt, zu verschlüsseln.
- Nur derjenige, der den dazugehörigen privaten Schlüssel besitzt, kann eine solche Nachricht entschlüsseln.

Da der öffentliche Schlüssel nur zum Verschlüsseln einer Nachricht dient, muss – im Gegensatz zum privaten Schlüssel – nicht allzu sehr darauf geachtet werden, dass er nicht in falsche Hände gerät.

Generierung der Schlüssel

Es gibt verschiedene Algorithmen zur Erzeugung solcher Schlüsselpaare; die bekanntesten sind RSA und DSA. Unter Linux werden sie über einen Aufruf des Kommandos `ssh-keygen` (siehe <http://www.openssh.com>) erzeugt. Es kann nur mit RSA-Schlüsseln der Version 2 gearbeitet werden. Die minimale Schlüssellänge beträgt 512 Bits. Generell werden 1024 Bits als ausreichend erachtet. Die erzeugten Schlüssel werden im lokalen Dateisystem abgespeichert:

Die RSA Authentisierungs-Identität wird in der Datei `$HOME/.ssh/id_rsa` sowie der öffentliche RSA-Schlüssel in der Datei `$HOME/.ssh/id_rsa.pub` abgelegt.

Die DSA Authentisierungs-Identität wird in der Datei `$HOME/.ssh/id_dsa` sowie der öffentliche DSA-Schlüssel in der Datei `$HOME/.ssh/id_dsa.pub` abgelegt.

Die Generierung der Schlüsselpaare kann auch mittels eines GUI-gestützten Tools erfolgen. Im [Abschnitt „PuTTY mit PuTTYgen und Pageant“ auf Seite 37](#) wird hierfür der Schlüsselgenerator von PuTTY beschrieben.

Verteilung der öffentlichen Schlüssel an die Kommunikationspartner

Im nächsten Konfigurationsschritt muss der Benutzer den öffentlichen Schlüssel in die Datei `$HOME/.ssh/authorized_keys` auf allen entfernten Systemen bringen, mit denen er kommunizieren will. Dies kann man z.B. erreichen, indem die lokale Identity Datei für den öffentlichen Schlüssel zu den entfernten Systemen kopiert wird und ihr Inhalt dort an die Datei `$HOME/.ssh/authorized_keys` angehängt wird.

Passphrasen

Der private Schlüssel darf nicht in die falschen Hände geraten. Zu diesem Zweck gibt es einige Schutzmechanismen in SSH. Das Programm `ssh` bringt eine Warnung, falls die lokale Identity-Datei von jemand anderem als dem Eigentümer lesbar ist. Bei der Generierung eines Schlüssel-Paares kann eine Passphrase vereinbart werden. Diese Passphrase dient zur Ver- und Entschlüsselung des privaten Schlüssels beim Schreiben in die bzw. Lesen aus der Identity Datei.

Es wird empfohlen, den privaten Schlüssel mit einer Passphrase zu schützen.

Eine Passphrase ist eine Erweiterung des Passworts. Sie kann eine Folge von Worten, Zahlen, Leerzeichen, Interpunktionen oder sonstigen beliebigen Zeichen sein. Gute Passphrasen sind 10 bis 30 Zeichen lang und enthalten eine nicht leicht erratbare Folge von Groß- und Kleinbuchstaben, Zahlen sowie nicht-alphanumerischen Zeichen.

Eine Passphrase wird im Rahmen des Authentifizierungsverfahrens – anders als ein Passwort – nicht an den entfernten Rechner übertragen.

Es gibt keine Möglichkeit, eine verlorene Passphrase wiederzugewinnen. Wenn sie verloren gegangen ist, muss ein neues Schlüsselpaar generiert und sein öffentlicher Schlüssel an die Kommunikationspartner verteilt werden.

3.4.4 Benutzung von SSH-Agenten



Die Verwendung eines SSH-Agenten macht es überflüssig, dass bei jedem Aufruf des Programms `ssh` die (üblicherweise lange und komplexe) Passphrase eingegeben werden muss.

In einem Initialisierungsvorlauf für SSH wurden die Schlüsselpaare erzeugt, in den lokalen Dateien abgelegt und die öffentlichen Schlüssel an die Kommunikationspartner verteilt. Zu Beginn einer interaktiven Session bzw. am Anfang eines Scripts wird der SSH-Agent mittels eines Aufrufs des Kommandos `ssh-agent` (siehe <http://www.openssh.com>) gestartet. Dann werden ihm die notwendigen privaten Schlüssel mittels `ssh-add` übergeben. Der SSH-Agent führt diese privaten Schlüssel im Speicher in entschlüsselter Form. Für diesen Entschlüsselungsprozess benötigt er die Passphrasen, falls welche spezifiziert wurden.

Von nun an bis zu seiner Beendigung kontaktieren SSH-Clients den SSH-Agenten automatisch für alle Schlüssel-bezogenen Operationen. Wenn mittels eines `ssh`-Aufrufs eine remote Verbindung eingerichtet werden soll, führen der lokale SSH-Agent und der remote `sshd`-Dämon automatisch die erforderliche Authentifizierungsprozedur durch.

Wenn eine Passphrase verwendet wird, muss sie nur einmal eingegeben werden. Sie wird von `ssh-add` vom aktuellen Terminal gelesen, falls `ssh-add` vom Terminal gestartet wurde. Wenn `ssh-add` kein ihm zugeordnetes Terminal besitzt, aber die Variablen `DISPLAY` und `SSH_ASKPASS` gesetzt sind, wird das durch `SSH_ASKPASS` spezifizierte Programm ausgeführt und ein X11-Window zum Lesen der Passphrase geöffnet. Dies ist nützlich wenn `ssh-add` in einer `.Xsession` oder in einem Startup-Script aufgerufen wird.

Beispiel

```
ssh-keygen -b 1024 -t rsa -C <comment> -N "<passphrase>"
# Erzeugt einen 1024 bit RSA key in SSH Version 2 geschützt durch eine
Passphrase
ssh-agent /bin/csh # Als Argument kann der Pfad auf eine Shell oder ein
Shell Script angegeben werden
ssh-add # Lädt standardmäßig alle Schlüssel der Identity-Datei
```

Es müssen die Umgebungsvariablen, die auf den Socket des SSH-Agenten zeigen, gesetzt werden, damit der SSH-Client mit dem Agenten kommunizieren kann. Das Programm `ssh-agent` liefert hierfür bei seiner Rückkehr die notwendige Information:

Beispiel

```
# In SSH Version 2 Notation:
SSH2_AUTH_SOCKET=/tmp/ssh-JGK12327/agent.12327; export SSH2_AUTH_SOCKET;
SSH2_AGENT_PID=12328; export SSH2_AGENT_PID;
```

Diese Output-Kommandos des Programms `ssh-agent` können mittels des `eval`-Kommandos ausgeführt werden. Beachten Sie dabei die rückläufigen Anführungszeichen (```):

```
eval `ssh-agent ...`
```

Das `eval`-Kommando weist die Shell an, das Kommando `ssh-agent` ablaufen zu lassen und anschließend die von ihm generierten Kommandos auszuführen. Danach stehen die Shell Variablen `SSH_AUTH_SOCK` und `SSH_AGENT_PID` zur Verfügung. Nach Ausführung des Kommandos `eval `ssh-agent`` wird die PID des SSH-Agenten ausgegeben.

Das Kommando `eval `ssh-agent`` sollte in die Datei `~/.bash_profile` aufgenommen werden.

Shell Scripts

Wenn SSH Shell Scripts genutzt werden sollen, kann die Installation des SSH-Agenten, das Setzen der korrekten Umgebung, und die Versorgung des Agenten mit den notwendigen Schlüsseln und Passphrasen in einer Initialisierungsphase oder in einem Startup-Script gemacht werden, bevor das Script mit den `ssh`-Aufrufen gestartet wird.

Zusätzlich muss das SSH-Script instrumentiert werden, um diese Werte in den Umgebungsvariablen zu setzen. Dazu muss der Output des Programms `ssh-agent` in einer Hilfsdatei abgespeichert worden sein, die dann im Script mittels des „Punkt“-Kommandos ausgeführt wird.

Beispiel

```
ssh-agent|head -2 > <auxfile> #Speichere Umgebung in Initialisierungsphase
:
:
:
. <auxfile> # Setze Umgebung im Script
```

3.4.5 PuTTY mit PuTTYgen und Pageant

In diesem Abschnitt wird die Erzeugung von Schlüsselpaaren und die Verteilung der öffentlichen Schlüssel mit Hilfe von PuTTY¹ beschrieben. PuTTY ist eine freie Implementierung von Telnet und Secure Shell für Win32 und Unix System-basierte Plattformen und ist nützlich im Dialogmodus.

¹ siehe <http://www.chiark.greenend.org.uk/~sgtatham/putty>

3.4.5.1 Schlüsselgenerator PuTTYgen

Der Schlüsselgenerator PuTTYgen¹ erzeugt Paare von privaten und öffentlichen Schlüsseln, die mit PuTTY, PSCP, und Plink, wie auch von PuTTY's Authentifizierungsagent Pageant genutzt werden können.

Das generelle Vorgehen bei der Erzeugung eines neuen Schlüsselpaares mittels PuTTYgen ist wie folgt:

- ▶ Wählen Sie den Typ des Schlüssels (RSA für SSH Version 2, oder DSA für SSH Version 2) und geben Sie die Schlüssellänge an.
- ▶ Klicken Sie *Generate* und bewegen Sie während der Generierung den Mauszeiger im Fensterbereich.

Wenn der Schlüssel erzeugt ist, ändert das Fenster seinen Aufbau: Der Schlüssel wird insgesamt angezeigt und danach zeigt das Feld *Key fingerprint* den Fingerprint-Wert, eine Kurzbezeichnung für den erzeugten Schlüssel.

- ▶ Tragen Sie in die Felder *Key passphrase* und *Confirm passphrase* eine Passphrase ein. Wenn Sie diese Felder leer lassen, wird der private Schlüssel beim Speichern nicht verschlüsselt. Dies sollte nicht ohne triftigen Grund geschehen.
- ▶ Klicken Sie *Save private key*.

PuTTYgen öffnet eine Dialogbox, um nach dem Ablageort zu fragen.

- ▶ Wählen Sie ein Verzeichnis und einen Dateinamen aus.

Die Datei wird in dem von PuTTY verwendeten Format gespeichert (Dateiendung .ppk).

- ▶ Klicken Sie *Save public key*.

PuTTYgen öffnet eine Dialogbox, um nach dem Ablageort zu fragen.

- ▶ Wählen Sie ein Verzeichnis und einen Dateinamen aus.

Den öffentlichen Schlüssel müssen Sie nicht unbedingt lokal auf Platte speichern. Sie können ihn auch direkt auf PuTTY Sessions, die auf den jeweiligen remote Servern laufen, kopieren. Dazu gehen Sie wie folgt vor:

- ▶ Stellen Sie zu diesen Servern mittels PuTTY eine Verbindung her.
- ▶ Wechseln Sie danach in das dortige Verzeichnis `$HOME/.ssh` und öffnen Sie die Datei `authorized_keys` mit einem Editor (existiert dort noch kein öffentlicher Schlüssel, muss die Datei erst erzeugt werden).
- ▶ Wechseln Sie in das Fenster von PuTTYgen, wählen Sie den gesamten Text im Feld *Public key for pasting into authorized_keys file* aus, und kopieren Sie ihn in die Zwischenablage.

¹ siehe <http://the.earth.li/~sgtatham/putty/latest/html/doc/Chapter8.html>

- ▶ Wechseln Sie wieder in das Fenster von PuTTY und fügen Sie die Daten aus der Zwischenablage in die geöffnete Datei ein. Achten Sie darauf, dass sich dabei alle Daten in einer Zeile befinden.
- ▶ Speichern Sie die Datei ab.

3.4.5.2 Authentifizierungs-Agent Pageant

PuTTY's Authentifizierungs-Agent Pageant¹ hält die entschlüsselten privaten Schlüssel im Speicher und erzeugt bei Bedarf Signaturen bzw. handelt das Authentifizierungsverfahren ab.

Die von Pageant gehaltenen Schlüssel listen Sie wie folgt auf:

- ▶ Starten Sie das Programm Pageant.
- ▶ Klicken Sie mit der rechten Maustaste das Pageant Icon in der Taskbar.

Es öffnet sich ein Menü.

- ▶ Wählen Sie *View Keys*.

Es öffnet sich das Hauptfenster von Pageant, das eine List Box mit allen derzeit von Pageant gehaltenen privaten Schlüssel enthält.

Wenn der benötigte Schlüssel noch nicht enthalten ist, fügen Sie ihn wie folgt hinzu:

- ▶ Klicken Sie die *Add Key*.

Pageant öffnet die Dialogbox *Select Private Key File*.

- ▶ Wählen Sie die zu Ihrem privaten Schlüssel gehörige Datei aus und klicken Sie *Open*.

Pageant lädt nun den privaten Schlüssel in den Speicher. Wenn der Schlüssel durch eine Passphrase geschützt ist, fordert Pageant diese an.

Sobald der Schlüssel geladen ist, erscheint er in der List Box des Pageant Hauptfensters.

Sie können nun PuTTY starten und eine SSH Verbindung zu einem System eröffnen, das Ihren Schlüssel akzeptiert. PuTTY erkennt, dass Pageant läuft, holt den Schlüssel automatisch von Pageant, und benutzt ihn für die Authentifizierung. Sie können nun weitere PuTTY Verbindungen öffnen, ohne jedes Mal die Passphrase eintippen zu müssen.

¹ siehe <http://the.earth.li/~sgtatham/putty/latest/html/doc/Chapter9.html>

3.5 Zugang über die lokale Konsole

Der Zugang zur lokalen Konsole bzw. der physikalische Zugang zum System ist in der Regel schon dadurch geschützt, dass es beim Zugang zum Data Center diverse Sperren und Restriktionen gibt.

An der lokalen Konsole am SE Server (Rack-Konsole) können Sie per Hotkey-Taste den Konsol-Switch bedienen und zwischen den vorhandenen Units des Typs Management Unit, HNC, Server Unit x86 und Application Unit wechseln.

Für Application Units siehe [Abschnitt „Zugang über die lokale Konsole“ auf Seite 49](#).

Zugang zu Management Unit mit Linux-Desktop (Gnome-Desktop)

Beim Zugang zur Management Unit über die lokale Konsole erhalten Sie als Bedienoberfläche einen Linux-Desktop vom Typ Gnome.

Die Anmeldung ist unter jeder Kennung möglich.

Die Funktionalität des Gnome-Desktops ist für alle Kennungen gleich.

Im Menü *Computer* ist der Web-Browser Firefox verankert. Diesen können Sie nutzen, um den SE Manager (Adressierung z.B. mit *https://localhost*) aufzurufen.

Wie bei der Remote-Bedienung ist für den SE Manager eine weitere Authentisierung mit der aktuellen Kennung notwendig. Nach erfolgreicher Anmeldung bietet der SE Manager die Funktionalität für die der Kennung entsprechenden Benutzerrolle an.

Weitere Funktionen des Desktops an der lokalen Konsole sind Funktionen zum Aufruf eines Terminalfensters, zum Sperren des Bildschirms, zum Konfigurieren des Bildschirmschoners und der Maus sowie zum Abmelden.



Sicherheitsrelevante Aktionen

- Beim Verlassen des Arbeitsplatzes sollte zumindest der Bildschirm gesperrt werden.
Achtung: Die Bildschirminhalte überdauern ein Abmelden und Anmelden.
- Bei längerem Verlassen des Arbeitsplatzes wird ein Abmelden (Logout) empfohlen. Dabei gehen die Bildschirminhalte verloren.
- Bei Inaktivität sperrt der Bildschirmschoner den Gnome-Desktop.
Die standardmäßige Timeout-Einstellung des Gnome-Desktops ist 10 Minuten.
Sie können diese Einstellung Ihren Bedürfnissen anpassen.

3.6 Zugang zum iRMC der Management Unit

Die Nutzung des iRMC der Management Unit ist optional. Die Voraussetzung dafür ist seine Anbindung an das öffentliche Management-Netzwerk MANPU.

Auf dem iRMC steht der Administration die vordefinierte Kennung `admin` zur Verfügung.

Der Administration werden die folgenden Funktionen der Web-Oberfläche des iRMC empfohlen:

- Ein-/Ausschalten der Management Unit (*Power Management* → *Power On/Off*)
Mittels *Power On* kann die Management Unit aus der Ferne hochgefahren werden.
- Ändern des eigenen Passworts (*User Management* → *iRMC S2 User*)



Sicherheitsrelevante Aktionen

- **Benutzerverwaltung**

- Die Web-Oberfläche des iRMC setzt die Spezifikation von IPMI Version 2.0 um. Dadurch steht dem Administrator die Benutzerverwaltung im gesamten Umfang zur Verfügung.
Die vordefinierte Kennung `admin` ist mit dem Standardpasswort `admin` initialisiert. **Ändern Sie dieses Passwort sofort bei der Inbetriebnahme.**
- Es ist möglich, weitere (personalisierte) Kennungen anzulegen. Diese sollten aber nicht mit höheren Privilegien als die vordefinierte Kennung `admin` ausgestattet werden: Auf iRMC-Ebene besitzt `admin` das Privileg `Operator` und die zusätzlichen Privilegien der Benutzerverwaltung und der Konsolenumleitung).
Da administrative Tätigkeiten auf dem iRMC der Management Unit aber äußerst selten sind, besteht keine Notwendigkeit für weitere Kennungen.



ACHTUNG!

Es wird dringend davon abgeraten, das Passwort der Kennung `service` zu ändern oder diese Kennung zu löschen. In einem solchen Fall ist die Service-Fähigkeit des iRMC nicht gegeben und damit auch die der Management Unit beeinträchtigt.
Falls eine solche Maßnahme dennoch nötig sein sollte, ist sie unbedingt mit der Service-Zentrale abzustimmen.
Ebenso darf nichts an der Funktionskennung `x2kinternal` geändert werden, da ansonsten die Funktionalität des SE Managers beeinträchtigt wird!

- **Schutzfunktionen**

- Es ist möglich, sich per *Logout* von der Web-Oberfläche des iRMC abzumelden. Dies kann beim Verlassen des Arbeitsplatzes alternativ oder zusätzlich zu den Sperrmechanismen des Administrations-PCs genutzt werden.

3.7 Geschützter Zugang zum BIOS und zum Bootloader

Das BIOS von Management Unit, HNC und Server Unit x86 ist durch ein Passwort geschützt, das dem Service bekannt ist.

Der vom Linux benutzte Bootloader GRUB (GRand Unified Bootloader) ist ebenfalls durch ein Passwort geschützt, das dem Service bekannt ist.



Standardmäßig ist die Rack-Konsole (lokale Konsole) der Management Unit zugeschaltet. Wenn Sie den Konsol-Switch umschalten (siehe [Abschnitt „Zugang über die lokale Konsole“ auf Seite 40](#)), können Sie BIOS und GRUB von HNC oder SU x86 über die lokale Konsole erreichen.

4 Sicherer Zugang zu Systemen

Das Kapitel beschreibt den sicheren Zugang zum BS2000-Betriebssystem auf den Server Units, zu Systemen auf den Application Units und zu XenVMs auf den SU x86.

4.1 Sicherer Zugang zu BS2000-Systemen

4.1.1 Sicherheit im BS2000-Betriebssystem

BS2000 OSD/BC stellt Basisfunktionen für die Systemsicherheit bereit. Siehe dazu das Handbuch „Systembetreuung“ [7].

Weitergehende Sicherheitsfunktionen in BS2000 realisiert das Softwareprodukt SECOS mit folgenden Bestandteilen:

- SRPM (System Resources and Privileges Management),
- GUARDS (Generally Usable Access contRol aDministration System)
- GUARDDEF (GUARDs DEFault protection)
- GUARDCOO (GUARDs COOwner protection)
- SAT (Security Audit Trail)
- SECOS-KRB (Kerberos-Authentisierung)

Diese Bestandteile von SECOS stellen Verwaltungssysteme und Schnittstellen zur Verfügung, die für jeden einzelnen Benutzer die Definition eines individuellen Rahmens an Rechten und Pflichten ermöglicht.

Details finden Sie in den SECOS-Handbüchern ([8] und [9]).

4.1.2 KVP-Logging-Dateien herunterladen

Die Logging-Dateien enthalten die Historie des BS2000-Betriebssystems auf Konsol- und KVP-Ebene.

Die Historie enthält bis zu 40 KVP-Logging-Dateien pro KVP. Wenn 40 Dateien existieren, wird durch Anlegen einer neuen KVP-Logging-Datei die älteste Datei gelöscht.

Wie weit die Historie zeitlich in die Vergangenheit zurückreicht, hängt im Wesentlichen davon ab, wieviele Meldungen das jeweilige System ausgibt.

Als Administrator können Sie die KVP-Logging-Dateien herunterladen und für die weitere Verwendung auf den Administrations-PC speichern.



Sicherheitsrelevante Aktionen

- **Download von vertraulichen Daten:**

Beachten Sie beim Verwalten der KVP-Logging-Dateien auf dem Administrations-PC, dass diese Dateien eventuell vertrauliche BS2000-Daten enthalten. Sorgen Sie deshalb dafür, dass auf diese heruntergeladenen Dateien nur von vertrauenswürdigen Personen zugegriffen werden kann.

4.1.3 Alternativer Zugang zum BS2000-Betriebssystem mit PuTTY

Sofern Sie den im SE Manager integrierten Zugang zu BS2000-Konsole und -Dialog nutzen, findet die Datenübertragung zwischen dem Administrations-PC und der Server Unit bzw. Management Unit auf der Ebene des Basis-Systems statt und ist verschlüsselt und somit sicher.

Alternativ ist ein sicherer Zugang zu BS2000-Konsole und -Dialog über den SSH-Client PuTTY (ab Version 0.63) unter folgenden Voraussetzungen möglich:

- Die Verbindung erfolgt zur MU.
- Es wird eine gültige Administrator- oder Operatorkennung angegeben.
- Als Folgekommando wird das CLI-Kommando `bs2Console` bzw. `bs2Dialog` mit entsprechenden Parametern angegeben.
Ein Operator erhält nur Zugang gemäß seiner individuellen Berechtigungen.
- Für eine BS2000-Konsole sollte zur Vermeidung von Zeilenumbrüchen die Anzahl der Spalten auf 132 eingestellt werden. Für einen BS2000-Dialog ist die Einstellung eines Zeichensatzes notwendig, der die Darstellung und die Tastenkombinationen, die im BS2000-Dialog benötigt werden, unterstützt.

Die Beschreibung der CLI-Kommandos finden Sie in der Online-Hilfe.

4.2 Sicherer Zugang zu Systemen auf Application Units

Als Administrator installieren Sie auf den Application Units eigene Software (z.B. Software zur Datensicherung oder Datenbanken) und führen andere Administrations- und Konfigurationsaufgaben sowohl auf Anwendungs- als auch auf Betriebssystem-Ebene durch.

Die Administrationsmaßnahmen an der Application Unit liegen allein in der Verantwortung des Kunden. Damit sind Sie auch für die Sicherheit aller Zugänge auf die Application Unit und ihres iRMC verantwortlich (Sicherheit des Betriebssystems, Passwortverwaltung, Verboten unsicherer Dienste, Administration des iRMC, Service-Fähigkeit, usw.).



Die Sicherheit auf den Application Units hat keinen Einfluss auf die Sicherheit der anderen Systeme des SE Servers.

4.2.1 Konfigurationsänderungen

Standardmäßig sind Application Units in die Statusüberwachung und in das Remote-Service-Verfahren des SE Servers eingebunden. Dies erfordert Konfigurationsmaßnahmen in der SNMP-Konfiguration der Application Unit.

SNMP-Konfiguration

Die Management Unit startet Abfragen an den SNMP-Agenten auf der Application Unit, um Informationen zur Verwaltung der Application Units zu erhalten.

Einzelheiten zur Einbindung der Application Unit in die Statusüberwachung sind im Handbuch „Bedienen und Verwalten“ [2] und in der Online-Hilfe beschrieben.



Sicherheitsrelevante Aktionen

- Wenn Sie die für die Statusüberwachung erforderliche SNMP-Konfiguration vornehmen oder ändern, sollten Sie darauf achten, dass nur SNMP-Abfragen von der Management Unit aus erlaubt sind.
- Für die SNMP-Abfragen muss in der Firewall der Port 161 geöffnet sein.
- Falls Sie die Application Unit oder darauf laufende Anwendungen mittels SNMP durch eine oder mehrere Management-Stationen überwachen wollen, gelten die Hinweise zu den sicherheitsrelevanten Aktionen im [Abschnitt „SNMP“ auf Seite 64](#) entsprechend.

4.2.2 Zugang zum iRMC der Application Unit

Die Nutzung des iRMC einer Application Unit sieht unter anderen folgende Szenarien vor:

- Ein-/Ausschalten der Application Unit
Hierzu steht der Administration auf dem iRMC die vordefinierte Kennung `admin` zur Verfügung.
- Remote-Zugriff auf die Konsole der Application Unit über die Funktion „Video Redirection“ (Grafische Konsolenumleitung)“. Die Funktionalität ist entsprechend wie beim [Zugang über die lokale Konsole](#).
- Abfragen von Statusinformationen durch die Management Unit
Zur Nutzung der iRMC-Schnittstelle muss der Verwalter der Application Unit auf dem iRMC eine Kennung `semuser` mit den Rechten „LANchannel privilege Administrator, SerialChannel Privilege user“ bereitstellen.
Wenn der Service eine Application Unit konfiguriert, richtet er die Kennung `semuser` mit dem Standardpasswort ein.
Einzelheiten zur Einbindung der Application Unit in die Statusüberwachung sind im Handbuch „Bedienen und Verwalten“ [2] und in der Online-Hilfe beschrieben.



Sicherheitsrelevante Aktionen

- **Benutzerverwaltung**

- Die Web-Oberfläche des iRMC setzt die Spezifikation von IPMI Version 2.0 um. Dadurch steht dem Administrator die Benutzerverwaltung im gesamten Umfang zur Verfügung.
Die Kennung `semuser` ist nach der Konfiguration durch den Service mit dem Standardpasswort geschützt. **Ändern Sie dieses Passwort sofort bei der Inbetriebnahme.**
Es ist möglich, weitere (personalisierte) Kennungen anzulegen. Beachten Sie dabei das auf dem iRMC vorgegebene Privilegienkonzept.
Nicht benutzte Kennungen sollten Sie deaktivieren.

- **Schutzfunktionen**

- Es ist möglich, sich per *Logout* von der Web-Oberfläche des iRMC abzumelden.
Dies kann beim Verlassen des Arbeitsplatzes alternativ oder zusätzlich zu den Sperrmechanismen des Administrations-PCs genutzt werden.
- Die Web-Oberfläche des iRMC kann gegen unbefugten Zugang auch durch ein *Session Timeout* geschützt werden. Die Sitzung (Session) läuft ab, wenn in der Web-Oberfläche eine Zeit lang (Timeout-Zeit) keine Tätigkeit festgestellt wird.
Anschließend ist eine neue Anmeldung nötig.

Dieses Verhalten können Sie unter *Network Settings* → *Ports* auf 2 Arten konfigurieren:

- ▶ Deaktivieren Sie *Enable Auto Refresh*.
Dies hat auch zur Folge, dass die Web-Oberfläche nicht automatisch aktualisiert wird.
- ▶ Stellen Sie den Wert von *Refresh every* (Aktualisierungszyklus) größer ein als den von *Session Timeout*.
Dies hat zur Folge, dass bei normaler Timeout-Zeit von 20 Minuten die Refresh-Zeit unangemessen hoch ist, oder dass bei normaler Refresh-Zeit im Minutenbereich die Timeout-Zeit unangemessen niedrig ist.

4.2.3 Zugang über die lokale Konsole

Wenn Sie den Konsol-Switch umschalten (siehe [Abschnitt „Zugang über die lokale Konsole“ auf Seite 40](#)), erhalten Sie über die lokale Konsole Zugang zu dem Betriebssystem der Application Unit. Die Art des Zugangs (z.B. Shell oder Desktop) hängt von dem installierten Betriebssystem ab.

Die Bereitstellung und Verwaltung von Zugangskennungen liegen in Ihrer Verantwortung.

Der zur Verfügung stehende Kommando- bzw. Funktionsumfang ist abhängig von dem eingesetzten Betriebssystem.



Sicherheitsrelevante Aktionen

- Beim Verlassen des Arbeitsplatzes sollten Sie sich explizit mit der der Oberfläche entsprechenden Methode abmelden, z.B. auf Shell-Ebene mit dem Kommando `exit`.
- Beim Verlassen des Arbeitsplatzes sollten Sie sich explizit mit der der Oberfläche entsprechenden Methode abmelden, z.B. auf Shell-Ebene mit dem Kommando `exit`.
- Das Umschalten des Konsol-Switch oder das Ausschalten der Konsole hat kein automatisches Abmelden zur Folge.

4.3 Sicherer Zugang zu XenVMs auf SU x86

4.3.1 XenVMs auf der SU x86

Der Zugang zur Konsole einer XenVM sollte mit einem Passwort geschützt werden, da das Schließen des Konsolfensters keine Sperrung der Konsole bzw. des Desktops bewirkt. Die Konsole steht somit dem nächsten Anwender ungeschützt zur Verfügung. Ein Konsol-Passwort kann entweder beim Einrichten der XenVM oder durch nachträgliches Ändern der XenVM-Eigenschaften gesetzt werden.

Bezüglich des Konsol-Passwortes ist Folgendes zu beachten:

- Das Passwort ist maximal 8 Zeichen lang.
- Es sollte eine gewisse Komplexität aufweisen (wird bei der Eingabe nicht geprüft!).
- Das Passwort wird nicht benutzerspezifisch gesetzt. Es ist für alle Benutzer der jeweiligen XenVM-Konsole gleich.
- Wenn der Zugang nicht über den SE Manager erfolgt, bietet das Passwort zumindest einen einfachen Schutz für den Zugang zur XenVM-Konsole.
- Für den Schutz des Passworts gilt:
 - Die Übertragung vom Client zum Server geschieht SSL-verschlüsselt.
 - Das Passwort ist bei allen XenVM-Anzeigen ausgeblendet.
 - Die XenVM-Konfigurationsdaten sind zugriffsgeschützt (Zugriff erfordert root-Berechtigung).
 - Die Konsol-Passwörter sind in CSR-Sicherungen enthalten, aber nur Systemadministratoren und der Service besitzen Zugriff auf diese Sicherungen.



Sicherheitsrelevante Aktionen

- **Zurücksetzen des Konsol-Passwortes:**
Der Zugang zur XenVM-Konsole ist ohne Passwort möglich. Dieser Zustand sollte aus Sicherheitsgründen vermieden werden.
- **Einspielen einer CSR-Sicherung:**
Beim Einspielen einer CSR-Sicherung werden die Konsol-Passwörter auf den Stand der Sicherung gesetzt, d.h. ggf. werden auch Konsol-Passwörter zurückgesetzt. Es sollte geprüft werden, ob noch Passwortschutz besteht und ggf. ein Passwort gesetzt werden.

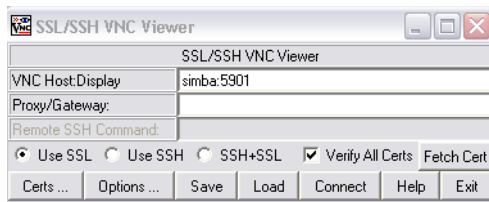
- **Download einer CSR-Sicherung auf den Administrations-PC:**
Die Datei muss vor unberechtigtem Zugriff geschützt sein, sonst können ggf. Konsol-Passwörter ausgespäht werden.

Neben dem Zugang zur Konsole einer XenVM über den SE Manager ist alternativ auch der Zugang über einen VNC-Viewer möglich. Den für den Verbindungsaufbau benötigten VNC-Port der gewünschten XenVM-Konsole zeigt Ihnen der SE Manager in der Übersicht über die XenVMs: *Systeme* → *<unit-name> (SU<x86>)* → *Virtuelle Maschinen* → *XenVM*, Registerkarte *VM-Verwaltung*.

4.3.2 Alternativer Zugang über SSL-fähigen VNC-Viewer

Auf Ihrem Administrations-PC ist ein SSL-fähiger VNC-Viewer installiert (Download von <http://www.karlrunde.com/x11vnc/ssvnc.html>).

- ▶ Starten Sie den VNC-Viewer.
- ▶ Geben Sie den Hostnamen des Server Unit und den VNC-Port der XenVM-Konsole im Format `host:port` an.



Da der VNC-Zugang nicht mit einem Passwort geschützt ist, warnt eine Meldung vor der fehlenden Authentisierung.

- ▶ Klicken Sie *OK* um die Verbindung zur XenVM-Konsole zu bestätigen.

5 Remote-Service (AIS Connect)

Der Remote-Service stellt sicher, dass bei Auftreten einer Störung ein Service-Call vom Remote-Service-Endpunkt des Kundensystems an die Service-Zentrale gesendet wird und der Service die Möglichkeit zum Remote-Zugang erhält.

Die Verbindung erfolgt über Internet. Dazu ist AIS Connect am Remote-Service-Endpunkt konfiguriert. Der Remote-Service-Endpunkt an einem SE Server ist die Management Unit.

Bei zugelassenem Zugang erfolgt die Initiative des Verbindungsaufbaus immer von der Kundenseite in Form von regelmäßigen Kontakten des Service-Agenten mit der Service-Zentrale, welche über das Internet erreichbar ist. Die Service-Zentrale nutzt bei Bedarf diese Möglichkeiten des Verbindungsaufbaus um sich beim Kunden anzumelden.

Aufträge aus der Service-Zentrale an den Service-Agenten auf der Management Unit (z.B. Filetransfer, Remote-Zugang) werden von diesem entgegengenommen. Der Service-Agent führt diese Aufträge aus, indem er z.B. beim Remote-Zugang den Tunnel dafür aufbaut.

Im Falle einer SSH-Sitzung erhält der Service-Techniker der Service-Zentrale Zugang zur Management Unit unter der Kennung `tele`. In der Regel wechselt er anschließend in die Kennung `service` um die Wartungsarbeiten durchzuführen.

Remote-Service genügt hohen Sicherheitsansprüchen:

- Die Initiative zum Verbindungsaufbau kommt immer von der Kundenseite. Damit ist sichergestellt, dass nur die konfigurierte Service-Zentrale Zugang zum Kundensystem erhält.
- Der Datentransfer erfolgt stets verschlüsselt.
- Der Kunde kann über die Funktion „Schattenterminal“ die Arbeit des Service beobachten oder sogar eingreifen. Es sind mehrere Sicherheitsstufen einstellbar.
- Die Arbeit des Service wird protokolliert. Der Kunde kann diese Protokolle lesen und jederzeit nachvollziehen, welche Aktionen der Service durchgeführt hat.
- AIS Connect unterstützt auch die Einbindung in eine Proxy-Server-Konfiguration (siehe [Seite 57](#)).

Ausgehende Verbindungen sind Service-Calls und regelmäßige Meldungen des Systemprogramms PRSC (Periodical Remote System Check), die einmal pro Woche an den Service verschickt werden. Service-Calls werden wie folgt propagiert:

- Störung an einem System am SE Server:
Hardware → SE Server (modell) → <unit-name> (MU) → Service → Remote Service

Eingehende Verbindungen sind Verbindungen, die der Service herstellt um eine Störung zu beheben oder um präventive Maßnahmen durchzuführen. Er stellt dabei die Verbindung zu dem Remote-Service-Endpunkt (Management Unit) her und wechselt dann gegebenenfalls in das zu wartende System (z.B. das BS2000-System).

Wenn es erforderlich ist, können Sie als Administrator (in geringerem Umfang auch als Operator) die Remote-Service-Konfiguration ändern oder in einen gerade laufenden Service-Vorgang eingreifen, siehe Handbuch „Bedienen und Verwalten“ [2].



Wichtig!

Sprechen Sie bitte jede Änderung der Remote-Service-Konfiguration unbedingt mit der Service-Zentrale ab, da ansonsten die Service-Fähigkeit Ihres SE Servers gefährdet ist.

5.1 Service-Kennungen

Auf einer Management Unit stehen dem Service im Basis-System die Kennungen `service` und `teile` zur Verfügung. Unter diesen Kennungen arbeitet der Service-Techniker sowohl lokal vor Ort als auch remote über den Remote-Service-Zugang an allen zur Verfügung stehenden Oberflächen (Web-Oberfläche, Linux-Desktop der lokalen Konsole, Shell-Ebene).

Die Kennung `service` besitzt auch Zugang zur BS2000-Konsole. Für die Protokollierung von Eingaben an der BS2000-Konsole ist Folgendes zu beachten:

- In den KVP-Logging-Dateien kann unterschieden werden, unter welcher Kennung (z.B. `admin` oder `user1`) eine Eingabe gemacht wurde.
- Dagegen kann im BS2000 in den CONSLOG-Dateien nur anhand der Konsol-Mnemonik (z.B. `C0`) unterschieden werden, von wem die Eingabe gemacht wurde. Damit sind Konsoleingaben verschiedener Benutzer nur eindeutig identifizierbar, wenn jeder Benutzer beim Konsolzugang eine andere Konsol-Mnemonik verwendet. Um eine Unterscheidung zu erreichen, können Sie den Operatorkennungen unterschiedliche Konsol-MNs zuteilen (über individuelle Zugangsrechte). Für Administrator-Kennungen, BS2000-Administrator-Kennungen und insbesondere auch den Service kann nur eine Absprache getroffen werden, bestimmte eindeutige Konsol-MNs zu verwenden.



Sicherheitsrelevante Aktionen

- Ändern der Konsol-Mnemonik für Operatorerkennung
Im SE Manager erhalten Sie unter *Berechtigungen* → *Benutzer* → *Individuelle Berechtigungen* die Möglichkeit den Konsolzugang zu einem System mit einer bestimmten Konsol-MN einzutragen. Die Änderung wird sofort wirksam.
- Konsol-Mnemonik in BS2000 OSD/BC definieren
Es muss sichergestellt sein, dass die verwendeten Konsol-MNs im BS2000 definiert sind, damit der Konsolzugang funktionstauglich ist.
Die Konsol-MNs definieren Sie in den BS2000-Parameterdateien (z.B. SYSPAR.BS2.nnn) im Abschnitt /BEGIN OPR mit dem Schlüsselwort DEFINE-CONSOLE. Der Parameter TELESERVICE=YES stellt dabei sicher, dass die Konsole dem Service nicht entzogen wird (d.h. die Konsole kann weder Ersatzkonsole einer anderen Konsole noch Hauptkonsole werden).
Details zur Konfiguration der Konsol-Mnemonik finden Sie im Handbuch „Einführung in die Systembetreuung“ [7].

5.2 Service-Vorgänge protokollieren

Die Sitzungen werden immer protokolliert, sowohl SSH- als auch VNC-Sitzungen. Protokolldateien von SSH-Sitzungen können Sie mit dem CLI-Kommando `aisLog` ansehen. Protokolldateien von VNC-Sitzungen können Sie auf Ihren PC laden und dort im Web-Browser ansehen.

Siehe hierzu auch das Handbuch „Bedienen und Verwalten“ [2].



Da Protokolldateien von VNC-Sitzungen sehr groß werden können, muss der Administrator sie von Zeit zu Zeit kontrollieren und bei Bedarf löschen.

5.3 Verschlüsselung nutzen

Die Kommunikation erfolgt grundsätzlich über HTTPS (HyperText Transfer Protocol Secure). Dabei werden die darunter liegenden Verschlüsselungsprotokolle SSL 3.0 (Secure Sockets Layer) und TLS 1.0 (Transport Layer Security) unterstützt.

5.4 Funktion „Schattenterminal“ nutzen

Mit der Remote-Service-Standardkonfiguration ist die Service-Zentrale zu jedem Zeitpunkt in der Lage, ohne weitere Mitwirkung oder Erlaubnis des Kunden Zugang zum System zu erhalten und seine Arbeit durchzuführen.

Sie können die Remote-Service-Konfiguration Ihren Sicherheitskriterien anpassen (z.B. Service-Zugang sperren oder öffnen).

Für die Administration des Service-Zugangs stellt Ihnen der SE Manager alle notwendigen Funktionen zur Verfügung.

Sie können jederzeit den Service-Zugang und die Nutzung des Schattenterminals verändern (sperren oder mit verschiedenen Einstellungen öffnen). Sie können die Arbeit des Service-Technikers beobachten, daran teilnehmen oder sich von ihm führen lassen.

Unabhängig von der Zugangseinstellung erhalten Sie Informationen über aktuelle Teleservice-Sitzungen (Name des Service-Technikers und Zugangsart) und den aktuellen Status des AIS-Agenten.



Sicherheitsrelevante Aktionen

- Ändern des Service-Zugangs:

Folgende Einstellungen sind für den Service-Zugang von AIS Connect möglich:

- Zugang zulassen, ohne Schatten
Der Service hat jederzeit Zugang zum System und muss Sie nicht in Kenntnis setzen. Ein Schattenterminal zur Verfolgung der Service-Tätigkeit steht nicht zur Verfügung.
- Zugang zulassen, Schatten möglich
Der Service hat jederzeit Zugang zum System und muss Sie nicht in Kenntnis setzen. Ein Schattenterminal zur Verfolgung der Service-Tätigkeit kann geöffnet werden.
- Zugang zulassen, Schatten zwingend
Der Service erhält nur Zugang zum System, wenn Sie vorher ein Schattenterminal geöffnet haben. In diesem können Sie die Service-Tätigkeit mit verfolgen.
- Zugang nicht zugelassen
Der Service erhält keinen Zugang zum System.

- Ändern der AIS Proxy-Konfiguration:

Falls die Internetverbindung über einen Proxy-Server erfolgt, sind in der AIS Proxy-Konfiguration die IP-Adresse des Proxy-Servers, die Port-Nummer und gegebenenfalls auch Kennung und Passwort für die Proxy-Authentisierung eingetragen.

Wenn sich Ihre Proxy-Server-Konfiguration ändert, müssen Sie die AIS Proxy-Konfiguration entsprechend anpassen. Auf dem Proxy-Server müssen Sie die Firewall-Einstellungen anpassen. Nur so bleibt die Service-Fähigkeit erhalten.

Die konkreten Aktionen führen Sie als Administrator oder Operator (nicht AIS Proxy-Konfiguration) im SE Manager durch. Die Funktionen sind unter *Hardware* → *Server (SE modell)* → *<unit-name>* → *Service* → *Remote Service* zusammengefasst.

Wenn der SE Server über eine zweite MU verfügt, müssen Sie sich an der anderen MU anmelden und dort dieselben Aktionen durchführen!

Eine Beschreibung zur Arbeit mit dem Schattenterminal finden Sie im Abschnitt „Service-Zugang verwalten“ im Handbuch „Bedienen und Verwalten“ [2].

5.5 Zugang zu externen Assets

AIS Connect ermöglicht das Einrichten von Service-Verbindungen via Management Unit zu ausgewählten Storage-Systemen, die in diesem Kontext **externe Assets** genannt werden.

Das Einrichten dieser Verbindungen geschieht durch den Service in Absprache mit dem Kunden.

Die konfigurierten externen Assets zeigt der SE Manager im Menü *Hardware* → *Server (SE modell)* → *<unit-name>* → *Service* → *Remote Service an*.

Als Administrator können Sie jederzeit den Service-Zugang zu einzelnen externen Assets verändern (zulassen oder nicht zulassen).



Sicherheitsrelevante Aktionen

- Ändern des Service-Zugangs zu externen Assets:

Folgende Einstellungen sind möglich:

- Zugang zulassen
Der Service hat jederzeit Zugang zum externen Asset.
- Zugang nicht zugelassen
Der Service erhält keinen Zugang zum externen Asset.

Auch im Zustand **Zugang nicht zugelassen** ist sichergestellt, dass die Teleservice-Meldungen an die Service-Zentrale durchgereicht werden.

Wenn der SE Server über eine zweite MU verfügt, müssen Sie sich an der anderen MU anmelden und dort dieselben Aktionen durchführen!

Eine Beschreibung finden Sie im Abschnitt „Service-Zugang verwalten“ im Handbuch „Bedienen und Verwalten“ [2] und in der Online-Hilfe.

6 Konfigurations- und Diagnosedaten

6.1 Konfigurationsdatensicherung

Mit einer CSR-Sicherung (CSR = Configuration Save and Restore) sichern Sie Konfigurationsdaten einer Unit (Management Unit, HNC oder Server Unit x86) in einem Archiv.

CSR-Sicherungen bleiben bei einer Neuinstallation erhalten.

Mit einer CSR-Sicherung lässt sich die Konfiguration des betreffenden Basis-Systems zum Zeitpunkt der Sicherung wiederherstellen.



Sicherheitsrelevante Aktionen

Als Administrator können Sie im SE Manager Konfigurationsdatensicherungsarchive auf den Administrations-PC herunterladen (Download) um sie für den Katastrophenfall zu sichern. Bei Bedarf können Sie als Administrator die Sicherung auch wieder hochladen (Upload).

Diese Funktionen stehen nur an der lokalen MU zur Verfügung (die MU, an der Sie angemeldet sind).

Die CSR-Sicherung enthält sicherheitsrelevante Daten des Basis-Systems. Kundendaten aus Ihren darauf oder damit betriebenen BS2000-Systemen sind jedoch nicht enthalten. Dies gilt auch für Kundendaten, die in XenVM-Systemen liegen.

Die in den Archiven gesammelten Daten können nicht ohne Weiteres benutzt werden, um in das System einzudringen oder es zu kompromittieren. Trotzdem ist Vorsicht geboten:

- Sorgen Sie bei der Verwaltung der Archive auf dem Administrations-PC dafür, dass auf diese Archive nur vertrauenswürdige Personen zugreifen können.
- Beim Hochladen achten Sie darauf, dass die Daten des Archivs nur an dem gewünschten Zielsystem und an keinem anderen System sonst aktiviert werden.

Empfehlung: Führen Sie zur Datensicherheit nach jeder Konfigurationsänderung eine CSR-Sicherung durch und sichern sie diese gemäß Ihren Sicherheitsrichtlinien.

Hinweis: Eine CSR-Sicherung enthält keine Passwörter von Kennungen. Falls nötig, können Sie den Service mit der Sicherung und der Restaurierung der Passwörter beauftragen.

6.2 Diagnosedaten

Der Administrator kann an den Units (Management Unit, HNC und Server Unit x86) Diagnosedaten erzeugen und diese dem Service zur Verfügung stellen, wenn der Service diese Unterstützung benötigt.

Für die anderen Benutzerrollen ist diese Funktion ebenfalls zugänglich.



Sicherheitsrelevante Aktionen

Als Administrator können Sie im SE Manager Diagnosedaten auf den Administrations-PC herunterladen (Download), um sie dann z.B. per E-Mail an den Service zu schicken.

Die Diagnosedaten enthalten sicherheitsrelevante Daten des Basis-Systems. Kundendaten aus Ihren darauf oder damit betriebenen BS2000-Systemen sind jedoch nicht enthalten.

Dies gilt auch für Kundendaten, die in XenVM-Systemen einer SU x86 liegen.

Die Diagnosedaten können nicht ohne Weiteres benutzt werden, um in das System einzudringen oder es zu kompromittieren. Trotzdem ist Vorsicht geboten: Achten Sie bei der Verwaltung der Diagnosedaten auf dem Administrations-PC sowie beim Verschicken an die Service-Zentrale darauf, dass auf diese Diagnosedaten nur vertrauenswürdige Personen zugreifen können.

7 Netzwerksicherheit

7.1 Netzwerkdienste

Die Tabelle beschreibt die Dienste, die im Basis-System der Management Unit freigeschaltet sind. Mittels ACL können die Dienste für einzelne Netzwerke weiter eingeschränkt werden, siehe [Abschnitt „Sicherheit auf der Ebene der Net Unit“ auf Seite 63](#).

HNC und SU x86 sind abgeschottet und werden nicht näher beschrieben.

Typ	Name und Nummer	Verwendungszweck
TCP	ssh (22)	Kommunikation auf Shell-Ebene (z.B. BS2000-Konsole/Dialog, SVP-Konsole, Schattenterminal)
TCP	http (80)	Die Kommunikation über diesen Port wird grundsätzlich auf https (443) umgelenkt.
TCP	https (443)	Kommunikation zwischen Browser (z.B. auf Administrator-PC) und Web-Oberfläche des Systems (z.B. SE Manager)
TCP	iascontrol-oms (1156)	PRSC/prscx (Periodical Remote System Check) sendet regelmäßig Lebend-Meldungen an die Service-Zentrale
TCP	4178	Optional: für die Kommunikation (http) mit StorMan
TCP	5800	Browser-Zugang zur VNC-Schattenfunktionalität des Remote Service (AIS Connect)
TCP	5900	VNC-Viewer-Zugang zur VNC-Schattenfunktionalität des Remote Service (AIS Connect)
TCP	10021-10022	im Falle eines SKP-Verbundes (redundanter SKP) für die SKP-SKP-Kommunikation
TCP	rs2_rctd (13333)	für Remote-Service-Anbindung von BS2000
UDP	domain (53)	Einbindung in den Domain Name Service (DNS)
UDP	multicast-ping (9903)	für die Überwachung von Komponenten
UDP	ntp (123)	Einbindung in das Network Time Protocol (NTPI)
UDP	snmp (161)	für lesenden SNMP-Zugriff durch Management-Stationen
UDP	snmptrap (162)	für Empfangen von SNMP-Traps von der Hardware-Überwachung

Tabelle 1: Ports für eingehende Verbindungen (Teil 1 von 2)

Typ	Name und Nummer	Verwendungszweck
UDP	syslog (514)	für die Überwachung von Komponenten
UDP	dhcpv6-client (546)	Optional: Der DHCPv6-Client-Port wird bei entsprechender Konfiguration einer LAN-Schnittstelle genutzt.
ICMP	-	Internet Control Message Protocol (ping)

Tabelle 1: Ports für eingehende Verbindungen (Teil 2 von 2)

Durch den auf den Systemen installierten Paketfilter (SuSEfirewall2) sind diese Ports für eingehende Verbindungen (incoming) freigeschaltet, alle anderen Ports sind gesperrt.

Für ausgehende Verbindungen (outgoing) sind in dem Paketfilter alle Ports freigeschaltet.

Ein im Paketfilter freigeschalteter Port für eingehende Verbindungen stellt kein Sicherheitsrisiko dar, solange der diesen Port nutzende Dienst nicht gestartet wird, weil das System jeden Verbindungsversuch blockiert.

7.2 IP-basierte Zugangsbeschränkung

Ab M2000 V6.1A kann der Administrator den Zugang zur MU und damit zum SE Manager so konfigurieren, dass der Zugang nur für explizit eingetragene IP-Adressen oder für IP-Adressen aus einem explizit eingetragenen IP-Netzwerk möglich ist.

Die aktuelle Einstellung zeigt die Registerkarte IP Netzwerke im Menü *Berechtigungen* → *Konfiguration*.

Standardmäßig ist die Liste für die Zugangsbeschränkungen leer und der Zugang ist unbeschränkt für alle IP-Adressen zugelassen.



Sicherheitsrelevante Aktionen

- Mit dem ersten Eintrag (IP-Adresse oder IP-Netzwerk) aktivieren Sie die IP-basierte Zugangsbeschränkung zur MU. Der Zugang ist dann nur noch für IP-Adressen möglich, die entweder explizit oder über ein IP-Netzwerk eingetragen sind.
- Wenn Sie den letzten Eintrag aus der Liste für die Zugangsbeschränkungen löschen, ist der Zugang zur MU wieder unbeschränkt für alle IP-Adressen möglich!

7.3 Sicherheit auf der Ebene der Net Unit

Auf der Ebene der Net Unit können die Dienste für die einzelnen Netzwerke mittels ACL weiter eingeschränkt werden.

Für die Netzwerke DANPU<xx>, MANPU, MONPU, DANPR<xx> und MONPR<xx> können Sie einzelne TCP/UDP Ports (Dienste) sperren oder freischalten:

- Entweder definiert der Administrator eine ACL-Liste vom Typ „permit“, in der alle freigeschalteten Dienste (Ports) explizit eingetragen werden.



Nach dem Einrichten der ACL vom Typ „permit“ ist die Liste zunächst leer. Damit ist der Zugang zum Netzwerk für alle Dienste (Ports) gesperrt!

- Oder der Administrator definiert eine ACL-Liste vom Typ „deny“, in der alle gesperrten Dienste (Ports) explizit eingetragen werden.

Für IPv4 und IPv6 kann jeweils eine ACL-Liste definiert werden.

7.4 Net-Storage

Die Units HNC und Server Unit x86 unterstützen als Net-Client den Zugriff des BS2000 zu einem Net-Storage. Dabei ist der HNC der Net-Client für die BS2000-Systeme, die auf der SU /390 ablaufen, und die SU x86 ist der Net-Client für die auf ihr ablaufenden BS2000-Systeme.

Für jeden Net-Client wird die Konfiguration des Zugangs zu einem Net-Storage im SE Manager verwaltet:

- Der Net-Client benötigt Zugriffsrechte für den Net-Server, der den Net-Storage bereitstellt. Eingetragen wird eine Benutzer und Gruppen ID, die auf dem Net-Server die nötigen Zugriffsrechte zu dem freigegebenen Speicher besitzt. Alternativ kann auch ein LDAP-Server NFSv4 zur Authentifizierung eingetragen werden.



Der Zugang über einen LDAP-Server ist nur möglich, wenn das Zertifikat des LDAP-Servers auf den HNC bzw. die SU x86 hochgeladen wurde.

Wenn die Konfiguration des LDAP-Servers nicht aktiv ist bzw. deaktiviert ist oder gelöscht wird, erfolgt die Authentifizierung über die eingetragene Benutzer und Gruppen ID!

- Jeder Net-Storage Anschluss muss im Netzwerk konfiguriert sein.

7.5 SNMP

Die zentrale SNMP-Einbindung des SE Servers wird über den SE Manager auf der Management Unit verwaltet. Die Vorkonfiguration ist so angelegt, dass Sie mittels SNMP auch die anderen Units an den Management-Stationen überwachen können, sofern auf der Management Unit eine Konfiguration für die SNMP-Einbindung (Leseberechtigung, Trap-Empfänger) besteht:

- Abfragen bezüglich der Server Unit /390 sind an der Management Unit möglich (siehe die privaten MIBs).
- Management-Stationen können den SNMP-Agenten an Server Unit x86 oder HNC ansprechen und Daten abfragen (der SNMP-Agent unterstützt für Abfragen die MIB-II und private MIBs).
- Der SNMP-Agent an Server Unit x86 oder HNC sendet in definierten Situationen (z.B. Statusänderungen) Traps an Management-Stationen.
- Auf Application Units müssen Sie SNMP dagegen selbst konfigurieren.

Um lesend zugreifen und um die Traps interpretieren zu können, müssen folgende private MIBs an der Management-Station importiert werden:

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

Der Zugriff auf die Management Unit ist z.B. mit scp (secure copy) unter jeder Administratorkennung möglich.



Sicherheitsrelevante Aktionen

- Achten Sie bei der Erstellung der SNMP-Konfiguration darauf, dass durch entsprechende Konfiguration der Read Community mit der Beschränkung auf die Management-Station nur vertrauenswürdige Management-Stationen auf den SNMP-Agenten der Server Unit x86 zugreifen können.
 - Verwenden Sie nach Möglichkeit nur spezifische Read-Communities (nicht *public*).
 - Erlauben Sie den Zugriff nur genau festgelegten Management-Stationen (durch Spezifizierung von deren Host-Namen).
- Achten Sie bei der Erstellung der SNMP-Konfiguration darauf, dass nur vertrauenswürdige Management-Stationen von der Server Unit x86 Traps zugestellt bekommen.
 - Verwenden Sie nach Möglichkeit eine spezifische Trap-Community (nicht *public*).
 - Tragen Sie nur die hierfür vorgesehenen Management-Stationen als Trap-Empfänger ein.

8 Sicherheit des Basis-Systems

8.1 Härtung des Basis-Systems

Die FUJITSU Server BS2000 SE Serie mit Management Unit, HNC und Server Unit x86 sind Systeme, die hohen Sicherheitsansprüchen genügen. Dabei handelt es sich um die statisch implementierte Sicherheit eines gehärteten Systems, welche durch Administrationsstätigkeiten nicht beeinflusst werden kann.

Das Basis-System von Management Unit, HNC und Server Unit x86 ist jeweils ein Linux-System, basierend auf SUSE Linux Enterprise Server (SLES) 11.

Das Basis-System dient ausschließlich der Administration der Systeme selbst. Es findet kein normaler Benutzerbetrieb mit Kundenapplikationen statt.

Folgende Eigenschaften kennzeichnen diese Systeme:

- Es sind nur für den Betrieb erforderliche, signierte Softwarekomponenten installiert.
- Die an den Systemen zum Einsatz kommende Basis-System-Software wird auf einer CD/DVD ausgeliefert, die eine Prüfsumme enthält. Anhand der Prüfsumme wird bei der Installation überprüft, ob sich alle Pakete der CD in einem unverfälschten, d.h. der Produktion entsprechenden Zustand befinden.
- Für den Benutzerzugang werden nichtprivilegierte Kennungen genutzt.
- Diese Kennungen sind im Rahmen eines differenzierten Rollenkonzepts mit klar definierten (und beschränkten) Funktionen und Zugriffsrechten ausgestattet.
- Außerhalb dieses Rollenkonzepts ist kein Zugang zum System möglich.
- Eine Rechteeskalation ist im Rahmen des Rollenkonzepts nicht möglich. Der Zugang zur Kennung `root` ist gesperrt. Notwendige Rechte für Service/Diagnose oder für Updates durch den Service von FUJITSU sind durch erweiterte Rechte der Rolle `Service` realisiert.
- Das Rollen- und Benutzerkonzept erlaubt es, personalisierte Kennungen einzurichten sowie Passwörter und Passwortheigenschaften zu verwalten.

- Aktionen, welche zu Konfigurations- oder Zustandsänderungen führen, werden protokolliert und können den sie ausführenden Personen zugeordnet werden.
- Der Datenverkehr zwischen Administrations-PCs und Basis-System erfolgt ausschließlich verschlüsselt.
- Alle nicht benutzten Netzwerk-Dienste sind deaktiviert.
- Der Netzwerkzugang ist durch die jeweilige systeminterne Firewall auf die benötigten Netzwerk-Ports eingeschränkt.

Die Konfiguration der Basis-Systeme orientiert sich an den Empfehlungen des Center for Internet Security (CIS, <http://www.cisecurity.org>).

Abweichungen von diesen Empfehlungen ergeben sich nur durch Funktionen, die für den Betrieb der Basis-Systeme erforderlich sind (z.B. ist für den SE Manager im Basisbetriebssystem immer ein Webserver aktiv, der die Benutzeroberfläche bereitstellt). Diese Abweichungen von den CIS-Empfehlungen führen nicht zu Sicherheitslücken.

8.2 Software-Signatur

Die Software, die an Management Unit, HNC und Server Unit x86 zum Einsatz kommt, wird in Paketen ausgeliefert, die mit einer Signatur versehen sind.

- Die Pakete der zugrundeliegenden Basissoftware Linux SLES 11 sind vom Hersteller signiert.
- Die für Management Unit, HNC und Server Unit x86 spezifischen Pakete sind von FUJITSU signiert.

Anhand der Signatur wird bei der Installation überprüft, ob sich ein Paket in einem unverfälschten, d.h. der Produktion entsprechenden Zustand befindet.

Wenn die Überprüfung der Signatur fehlschlägt, wird die Installation des Pakets abgelehnt.

8.3 Digitale Zertifikate

Die Nutzung von HTTPS/SSL setzt auf der Management Unit außer einem SSL-Schlüsselpaar auch ein sogenanntes (digitales) SSL-Zertifikat voraus. Dieses Server-Zertifikat hat folgende zwei Aufgaben:

- Das Zertifikat ist immer systemspezifisch (beinhaltet den FQDN) und weist dem Browser auf dem Administrations-PC die Online-Identität des jeweiligen Systems nach.
- Das Zertifikat stellt den öffentlichen Schlüssel bereit, mit dem der Browser auf dem Administrations-PC seine Nachrichten zum Server hin verschlüsselt.

Auf jeder Management Unit ist ein selbstsigniertes systemspezifisches Zertifikat, das in dem System generiert wurde, als Standard-Zertifikat vorinstalliert.

Statt des vorinstallierten selbstsignierten Zertifikats können Sie auch andere Zertifikate einsetzen. Es bestehen folgende Möglichkeiten:

- Benutzung eines selbstsignierten Zertifikats

Ein solches Zertifikat ist auf dem System als Standard-Zertifikat vorinstalliert. Es muss in jedem Browser, der mit dem SE Manager arbeitet, explizit bestätigt oder importiert werden.

- Benutzung eines kundeneigenen (von einer Kunden-CA signierten) Zertifikats

Falls die kundenspezifischen Richtlinien die Nutzung eines solchen Zertifikats vorsehen, kann dieses einfach installiert werden.

Das Zertifikat wird in der Regel von einem kundenspezifischen Stammzertifikat abgeleitet. Ein solches Zertifikat ist den beim Kunden verwendeten Browsern bekannt und wird ohne Nachfrage (d.h. ohne Bestätigung oder Import) akzeptiert.

- Benutzung eines kommerziellen (von einer root-CA signierten) Zertifikats

Ein solches Zertifikat wird von einer vertrauenswürdigen Stammzertifizierungsstelle (CA = Certification Authority) kostenpflichtig erstellt und ist damit allen Browsern bekannt. Deshalb akzeptiert jeder Browser solche Zertifikate ohne Nachfrage.

8.3.1 Zertifikat im Web-Browser bestätigen/importieren

Wenn die aufgerufene Web-Oberfläche ein selbstsigniertes Zertifikat verwendet (also z.B. das vorinstallierte Standard-Zertifikat), lehnen Web-Browser den Aufruf der Seite ab, da das Zertifikat aus ihrer Sicht nicht vertrauenswürdig ist.

Damit Seiten des SE Managers überhaupt im Browser geladen werden, müssen Sie den Zertifikatfehler entweder temporär akzeptieren oder Sie können das CA-Zertifikat der Management Unit herunterladen und dauerhaft im Browser importieren.

CA-Zertifikat herunterladen und im Browser installieren

Um den Zertifikatfehler in Zukunft zu vermeiden, können Sie das CA-Zertifikat des SE Servers herunterladen und im Browser installieren.

- ▶ Wählen Sie *Berechtigungen* → *Konfiguration*, Registerkarte *Zertifikate*. Die Tabelle zeigt das aktuelle Zertifikat an.
- ▶ Klicken Sie in der Zeile *Ausgestellt durch (CN)* das Symbol *CA-Zertifikat herunterladen*.

Nach dem Download können Sie das Zertifikat in Ihrem Browser installieren.

- ▶ Öffnen Sie die Zertifikatdatei und klicken Sie *Zertifikat installieren*.
Der Zertifikatsimport-Assistent des Browsers führt Sie schrittweise durch die Installation des Zertifikats.

Zertifikatfehler temporär akzeptieren

Die nachfolgend prinzipiell beschriebene Vorgehensweise beruht auf dem Internet-Explorer ab Version 11 und verläuft abhängig vom eingesetzten Browser und der Version unterschiedlich ab. Einzelheiten zur speziellen Vorgehensweise finden Sie in der Online-Hilfe Ihres Browsers.

- ▶ Öffnen Sie Ihren Web-Browser.

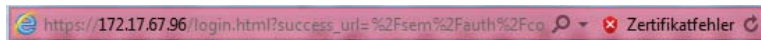
- Rufen Sie im Browser-Fenster den SE Manager des gewünschten Systems auf.



Der Web-Browser meldet einen Zertifikatfehler.

- Akzeptieren Sie das Laden der Web-Seite.

Sie erhalten die Login-Seite. Die Adresszeile des Browsers zeigt als Warnung *Zertifikatfehler* an.



Informationen über das mögliche Sicherheitsrisiko erhalten Sie, wenn Sie auf *Zertifikatfehler* klicken. Prüfen Sie das angezeigte Zertifikat. Fahren Sie nur fort, wenn keine Zweifel am Zertifikat bestehen.

Das Zertifikat ist jetzt temporär für diese Session akzeptiert und Sie können jetzt mit dem SE Manager dieses Systems arbeiten.

8.3.2 Standard-Zertifikat einsetzen

Auf der Management Unit ist jeweils ein selbstsigniertes systemspezifisches Zertifikat vorinstalliert. Dieses ist weder den Web-Browsern direkt bekannt noch ist es von einem bekannten Stammzertifikat (root-Zertifikat) abgeleitet.

Ein Standard-Zertifikat wird bei jedem Umbenennen der Management Unit (Ändern des FQDN) automatisch neu erzeugt und aktiviert. Das neue Standard-Zertifikat muss anschließend selbstverständlich in den Browsern wieder akzeptiert bzw. importiert werden.

Die wichtigsten Kennzeichen dieses Zertifikats sind:

- Der *Common Name (CN)* ist identisch mit dem vollqualifizierten Domännennamen (FQDN) des Basisbetriebssystems.
- Die Gültigkeitsdauer beträgt 10 Jahre.

- Der Fingerabdruck, der das Zertifikat eindeutig identifiziert, wird mit dem Algorithmus SHA-1 und mit RSA-Verschlüsselung erzeugt.

Da der Browser das selbstsignierte Zertifikat nicht kennt, fordert er beim Aufruf des SE Managers den Anwender dazu auf, das Zertifikat für die aktuelle Sitzung temporär zu akzeptieren oder dauerhaft zu importieren.

Wenn Sie den SE Manager an der lokalen Konsole aufrufen, müssen Sie das Standard-Zertifikat ebenfalls bestätigen oder importieren, da der am Gnome-Desktop eingesetzte Browser das Zertifikat ebenfalls nicht kennt.

Sie erhalten den Zugriff auf den SE Manager des jeweiligen Systems erst, wenn das Zertifikat temporär akzeptiert oder dauerhaft importiert ist.

Wenn Zweifel bestehen, sollten Sie das Zertifikat erst lesen und gegenprüfen, bevor Sie es temporär akzeptieren oder dauerhaft importieren.

Aktuelles Zertifikat anzeigen

- Wählen Sie *Berechtigungen > Konfiguration, Registerkarte Zertifikate*.

Der Arbeitsbereich zeigt eine Übersicht der wichtigsten Eigenschaften des aktuellen Zertifikats.

Zertifikate

Management Unit **abgse2mu1**: Aktuelles SSL-Zertifikat ?

Zertifikat	Standard-Zertifikat	
Ausgestellt für (CN)	abgse2mu1.abg.fsc.net, abgse2mu1, 172.17.67.154, localhost	
Ausgestellt durch (CN)	Fujitsu SE Server CA 76258d4c	
Gültig von	2015-06-11	
Gültig bis	2025-06-11	
Gültigkeitsdauer in Tagen	3653	

Management Unit **abgse2mu1**: Aktueller Antrag auf ein SSL-Zertifikat ?

Zertifikat

Typ des Zertifikats: *Standard-Zertifikat* oder *Benutzerdefiniert*

Ausgestellt für (CN)

FQDN des Servers, für den das Zertifikat ausgestellt wurde.

Ausgestellt durch (CN)

Herausgeber des Zertifikats (z.B. Organisation). Bei benutzerspezifischen Zertifikaten ist dies ebenfalls die FQDN des Servers, für den das Zertifikat ausgestellt wurde.

Informationen zu den Attributen *Gültig von*, *Gültig bis*, *Gültigkeitsdauer in Tagen* sowie *Email-Adresse (email Address)* finden Sie in der Online-Hilfe.

Zertifikat detailliert anzeigen

- ▶ Wählen Sie *Berechtigungen > Konfiguration, Registerkarte Zertifikate*.
- ▶ Klicken Sie das Symbol *Details*.

In einem Dialog werden alle Eigenschaften des Zertifikats angezeigt.

Detailanzeige des aktuellen SSL-Zertifikats

Version	3 (0x2)
Seriennummer	06
Signaturalgorithmus	sha512WithRSAEncryption
Öffentlicher Schlüssel	2048 bit RSA
Fingerabdruck	SHA1 36:09:91:AE:35:5E:AE:F0:9E:40:D5:09:A6:A7:B0:BE:9F:4B:4B:32
Ausgestellt durch	
Common Name (CN)	Fujitsu SE Server CA 76258d4c
Organisation (O)	Fujitsu
Organisationseinheit (OU)	-
Stadt (L)	Munich
Bundesland (ST)	Bavaria
Staat (C)	DE
Email-Adresse (emailAddress)	-
Gültig	
Von	2015-06-11
Bis	2025-06-11
Tage	3653
Ausgestellt für	
Common Name (CN)	abgse2mu1.abg.fsc.net, abgse2mu1, 172.17.67.154, localhost
Organisation (O)	Fujitsu
Organisationseinheit (OU)	Fujitsu SE Manager Server Certificate
Stadt (L)	Munich
Bundesland (ST)	Bavaria
Staat (C)	DE
Email-Adresse (emailAddress)	-

Schließen

8.3.3 Neues selbstsigniertes Zertifikat erzeugen und aktivieren

Das vorinstallierte Standardzertifikat beinhaltet Daten, die selbstverständlich nicht kundenspezifisch sind.

Wenn Sie mit einem Zertifikat mit kundenspezifischen Daten arbeiten wollen, können Sie jederzeit ein solches erzeugen und verwenden. Diese Aktion kann auch dann nötig sein, wenn Sie das Zertifikat erneuern wollen. Gehen Sie wie folgt vor:


- ▶ Wählen Sie *Berechtigungen* → *Konfiguration*, Registerkarte *Zertifikate*.
- ▶ Klicken Sie *Neues SSL-Zertifikat erstellen und aktivieren* oberhalb der Tabelle.

Es wird ein Dialog geöffnet:

SSL-Zertifikat erstellen und aktivieren ?

Neues SSL-Zertifikat für die Management Unit **abgse2mu1** erstellen und aktivieren.

Common Name (CN)	abgse2mu1.abg.fsc.net, abgse2mu1, 172.17.67.154, localhost
Organisation (O)	<input type="text"/>
Organisationseinheit (OU)	<input type="text"/>
Stadt (L)	<input type="text"/>
Bundesland (ST)	<input type="text"/>
Staat (C)	<input type="text"/>
Email-Adresse (emailAddress)	<input type="text"/> <i>optional</i>
Gültigkeitsdauer in Tagen	<input type="text"/>

 Das bisher aktive SSL-Zertifikat wird überschrieben.

Tragen Sie die wesentlichen Daten des Zertifikats ein. Der Wert für den *Common Name (CN)* ist fest vorgegeben und beinhaltet den vollqualifizierte Domännennamen (FQDN) des Systems. Informationen zu den Attributen *Organisation (O)*, *Organisationseinheit (OU)*, *Stadt (L)*, *Bundesland (ST)*, *Staat (C)*, *Email-Adresse (email Address)*, *Gültigkeitsdauer in Tagen* finden Sie in der Online-Hilfe.

- ▶ Klicken Sie *Erstellen und aktivieren*.

Das Zertifikat wird erzeugt, sofort aktiviert und als aktuelles Zertifikat angezeigt.

Hinweise:

- Das Aktivieren des Zertifikats beinhaltet einen automatischen Neustart des Web-Servers.
- Da es sich bei dem neuen Zertifikat auch um ein Zertifikat handelt, dessen Vertrauenswürdigkeit dem Web-Browser nicht bekannt ist, muss es wie das Standardzertifikat explizit akzeptiert oder importiert werden (siehe [Abschnitt „Zertifikat im Web-Browser bestätigen/importieren“ auf Seite 68](#)).

8.3.4 Antrag auf ein SSL-Zertifikat stellen

Wenn Sie ein systemspezifisches Zertifikat, das von einer CA (Certification Authority) signiert wurde, einsetzen wollen, unterstützt Sie der SE Manager beim Erstellen des Antrags:

- ▶ Wählen Sie *Berechtigungen* → *Konfiguration*, Registerkarte *Zertifikate*.

Die Gruppe *Aktueller Antrag auf ein SSL-Zertifikat* zeigt, ob bereits ein Antrag gestellt wurde: In diesem Fall werden die Attribute für das beantragte Zertifikat angezeigt.

- ▶ Klicken Sie *Neuen Antrag erstellen* in der Gruppe *Aktueller Antrag auf ein SSL-Zertifikat*.



Ein bereits erstellter Antrag wird überschrieben.

Es wird ein Dialog geöffnet: Tragen Sie die wesentlichen Daten des beantragten Zerti-

SSL-Zertifikat-Antrag erstellen ?

Neuen SSL-Zertifikat-Antrag für die Management Unit **abgse2mu1** erstellen.

Common Name (CN)	abgse2mu1.abg.fsc.net, abgse2mu1, 172.17.67.154, localhost	
Organisation (O)	<input type="text"/>	
Organisationseinheit (OU)	<input type="text"/>	
Stadt (L)	<input type="text"/>	
Bundesland (ST)	<input type="text"/>	
Staat (C)	<input type="text"/>	
Email-Adresse (emailAddress)	<input type="text"/>	<i>optional</i>

fikats ein. Der Wert für den *Common Name (CN)* ist fest vorgegeben und beinhaltet den vollqualifizierte Domännennamen (FQDN) des Systems. Informationen zu den Attributen *Organisation (O)*, *Organisationseinheit (OU)*, *Stadt (L)*, *Bundesland (ST)*, *Staat (C)*, *Email-Adresse (email Address)*, *Gültigkeitsdauer in Tagen* finden Sie in der Online-Hilfe.

- ▶ Klicken Sie *Erstellen*.

Der Antrag wird erzeugt und in der Gruppe *Aktueller Antrag auf ein SSL-Zertifikat* angezeigt. Damit Sie den Antrag per E-Mail an die Zertifizierungsstelle schicken können, laden Sie den Antrag über das Symbol *Antrag herunterladen* zuerst auf Ihren Administrations-PC herunter.

Wenn Sie das Zertifikat signiert zurück erhalten, bringen Sie das Zertifikat in das System ein: Siehe [Abschnitt „Kundeneigenes Zertifikat hochladen und aktivieren“ auf Seite 74](#) und [Abschnitt „Standard-Zertifikat einsetzen“ auf Seite 69](#).

Hinweise

- Beim Erzeugen des Certificate Signing Request wird dieser mit dem Standard-SSL-Schlüssel des Systems verknüpft. Falls dieser Schlüssel zwischen dem Erzeugen des Certificate Signing Request und dem Einbringen des signierten Zertifikats in das System geändert wird, kann das Zertifikat nicht verwendet werden.
- Der Standard-SSL-Schlüssel wird bei Neuinstallation oder beim Ändern des Hostnamens neu angelegt.

Deshalb sollte zwischen Erzeugen des Certificate Signing Request und Einbringen des signierten Zertifikats in das System keine Neuinstallation und kein Ändern des Hostnamens durchgeführt werden.

8.3.5 Kundeneigenes Zertifikat hochladen und aktivieren

Statt eines im System erzeugten selbstsignierten Zertifikats (Standardzertifikat oder benutzerdefiniertes Zertifikat) können Sie für den Zugang zum SE Manager des Systems ein eigenes Zertifikat verwenden.

Für das Zertifikat wurde ein Certificate Signing Request im System erzeugt (siehe [Abschnitt „Antrag auf ein SSL-Zertifikat stellen“ auf Seite 73](#)) und an eine Zertifizierungsstelle geschickt. Sobald Ihnen das von der CA (Certification Authority) signierte Zertifikat vorliegt, können Sie es hochladen und aktivieren:

- ▶ Wählen Sie *Berechtigungen* → *Konfiguration*, *Registerkarte Zertifikate*.
- ▶ Klicken Sie *SSL-Zertifikat hochladen und aktivieren*.

Ein Dialog wird geöffnet.

SSL-Zertifikat hochladen und aktivieren

Das ausgewählte SSL-Zertifikat auf die Management Unit **abgse2mu1** hochladen und aktivieren.

Zertifikat	<input type="text"/>	<input style="border: none; background-color: #eee; padding: 2px 5px;" type="button" value="Datei auswählen..."/>
Schlüssel	<input type="text"/>	<input style="border: none; background-color: #eee; padding: 2px 5px;" type="button" value="Datei auswählen..."/>

Zertifikat

- ▶ Klicken Sie *Durchsuchen* um eine Zertifikats-Datei auf Ihrem Administrations-PC auszuwählen.

Schlüssel

Wählen Sie, falls nötig, eine passende Schlüsseldatei aus. Eine Schlüsseldatei wird nur benötigt, wenn das Zertifikat auf einem anderen System erzeugt wurde. Ohne Angabe wird der Standardschlüssel verwendet.

- ▶ Klicken Sie *Durchsuchen* um eine Schlüsseldatei auf Ihrem Administrations-PC auszuwählen.
- ▶ Klicken Sie *Hochladen* um den Upload der Datei(en) zu starten.

Die angegebenen Dateien werden in das Zielsystem hochgeladen, sofort aktiviert und als aktuelles SSL-Zertifikat angezeigt.

Hinweise

- Das Aktivieren des Zertifikats auf dem Zielsystem beinhaltet einen Neustart des Web-Servers mit dem neuen Zertifikat. Dabei kann es zu einer kurzzeitigen Unterbrechung der Verbindung des SE Managers zum System kommen.
- Wenn das neue Zertifikat dem verwendeten Web-Browser (am Administrations-PC oder an der lokalen Konsole) als vertrauenswürdig bekannt ist oder dessen Stammzertifikat (root-Zertifikat) bekannt ist, ist keine weitere Aktion nötig.
- Ein Zertifikat, dessen Vertrauenswürdigkeit dem Web-Browser nicht bekannt ist, muss explizit bestätigt oder importiert werden (siehe [Abschnitt „Zertifikat im Web-Browser bestätigen/importieren“ auf Seite 68](#)).

8.4 Security Fixes

Security Fixes sind Sammlungen von Updates zu den Linux-basierten Basis-Systemen von Management Unit, HNC und Server Unit x86. Security Fixes verbessern den Schutz des jeweiligen Systems z.B. gegen unbefugtes Eindringen oder gegen Angriffe von außen.

Aktuelle Security Fixes müssen bei erhöhtem Sicherheitsbedarf regelmäßig installiert werden, insbesondere dann, wenn auf das jeweilige System nicht nur von einem abgeschotteten Management-Netzwerk, sondern auch von außen zugegriffen werden kann. Aktuelle Security Fixes werden im Internet auf den Support-Seiten von FUJITSU oder (bei Anforderung) auf CD/DVD bereitgestellt und grundsätzlich vor Ort durch den Administrator installiert.



Sicherheitsrelevante Aktionen

Security Fixes werden für das jeweilige System (Management Unit, HNC und Server Unit x86) bereitgestellt und auf diesem System verwaltet. Deshalb müssen Sie die nachfolgenden Tätigkeiten für jedes der eingesetzten Systeme ausführen (d.h. an einem SE Server auf Management Unit, HNC und Server Unit x86):

- Klären des Bedarfs der Installation von Security Fixes.
- Beschaffen des Security Fix vom Download-Server von FUJITSU im Internet und Herunterladen (Download) des Security Fix in ein beliebiges Verzeichnis auf dem Administrations-PC.
In Ausnahmefällen erhalten Sie den Security Fix per CD/DVD vom Service.
- Wenn sich der Security Fix auf dem Administrations-PC befindet, müssen Sie ihn in das jeweilige System bringen.
Wenn die Lieferung per CD/DVD erfolgt ist, müssen Sie den Security Fix auf die Platte des jeweiligen Systems übertragen.
- Installieren des Security Fix (falls installierbar).
- Wenn der installierte Security Fix die Installationsart *Reboot* hat, wird er erst nach einem Reboot aktiv (Status "nicht aktiv").

Für den Neustart der Server Unit benötigen Sie ein Wartungsfenster.

Bei einem Reboot der Management Unit sind BS2000-Konsolen und Dialoge sowie die SVP-Konsole nicht bedienbar. Außerdem werden eventuell genutzte LOCLAN-Verbindungen unterbrochen und EMFILES sind nicht nutzbar. Wenn eine redundante Management Unit vorhanden ist, kann das BS2000 darüber bedient werden.

Bei einem Reboot des HNC werden die ZASLAN-Verbindungen unterbrochen. Wenn ein redundanter HNC vorhanden ist, schaltet BCAM bei entsprechender Konfiguration die Verbindungen auf diesen um.

9 Aktionen im System protokollieren (Audit-Logging)

Die interne Funktion Audit-Logging protokolliert alle wichtigen Aktionen, die über den SE Manager oder das CLI ausgeführt werden und die eine Konfigurationsänderung oder Zustandsänderung im System bewirken. Anmeldungen werden ebenfalls protokolliert. Reine Anzeigefunktionen werden nicht protokolliert.

Anhand der Protokolleinträge kann der Service im Auftrag des Kunden jederzeit nachvollziehen, wer wann welche Aktion durchgeführt hat. Damit sind insbesondere alle sicherheitsrelevanten Aktionen im System eindeutig einem „Verursacher“ zuordenbar.

Literatur

Die Handbücher finden Sie im Internet unter <http://manuals.ts.fujitsu.com>. Handbücher, die mit einer Bestellnummer angezeigt werden, können Sie auch in gedruckter Form bestellen.

- [1] **FUJITSU Server BS2000
SE700 / SE500 / SE300**
Kurzanleitung
- [2] **FUJITSU Server BS2000
SE700 / SE500 / SE300**
Bedienen und Verwalten
- [3] **FUJITSU Server BS2000
SE700 / SE500 / SE300**
Basis-Betriebsanleitung
- [4] **FUJITSU Server BS2000
SE700 / SE500**
Server Unit /390
- [5] **FUJITSU Server BS2000
SE700 / SE500 / SE300**
Server Unit x86
- [6] **FUJITSU Server BS2000
SE700 / SE500 / SE300**
Additive Komponenten
- [7] **BS2000 OSD/BC**
Einführung in die Systembetreuung (SE Server)
Benutzerhandbuch

- [8] **SECOS**
Security Control System - Zugangs- und Zugriffskontrolle
Benutzerhandbuch
- [9] **SECOS**
Security Control System - Beweissicherung
Benutzerhandbuch

Stichwörter

A

Add-on Pack [24](#)
admin (Administrator-Rolle) [22](#)
Administrator (Rolle) [19](#)
Anmeldungen
 protokollieren [77](#)
Application Unit [10, 15, 47](#)
Asset, extern [57](#)
AU [13](#)
AU (Application Unit) [13](#)
AU-Administrator (Rolle) [19](#)
Audit-Logging [77](#)
Authentifizierung [34](#)
Authentisierung [25](#)

B

Basis-System, härten [65](#)
Benutzerkennung [22](#)
BIOS [43](#)
Bootloader [43](#)
BS2000
 sicherer Zugang [46](#)
BS2000 OSD/BC
 Sicherheit [45](#)
BS2000-Administrator (Rolle) [19](#)
BS2000-Konsole
 sicherer Zugang [46](#)
BS2000-Server [14](#)

C

c2suxadm [24](#)
Center for Internet Security [8](#)
Cookies [29](#)
CSR-Sicherung [50, 59](#)

D

Diagnosedaten [60](#)
DSA-Schlüssel [35](#)

G

Gnome-Desktop [40](#)
Gültigkeitsdauer [25](#)

H

HNC [10, 13](#)
HNC (High Speed Net Connect) [13](#)
hochladen
 Zertifikat [74](#)
Host-Schlüssel [33](#)

I

Inaktivzeit [25](#)
Informationen über Sessions [30](#)
IP-basierte Zugangsbeschränkung [62](#)
iRMC, Zugang [42](#)

J

JavaScript [29](#)

K

Kennung

- admin 22
- Basisbetriebssystem 24
- c2suxadm 24
- für Add-on Pack 24
- interne 24
- opensm2 24
- openutm 24
- robar 24
- root 24
- service 23, 24
- Sicherheit 22
- storman 24
- tele 24

Kennung und Rolle 19

Kennungsverwaltung

- Berechtigung 23

Kommunikation, verschlüsselt 32

Konfiguration

- Änderung protokollieren 77

Konfigurationsdaten sichern 59

Konfigurationsdatensicherung 59

Konsol-Passwort (XenVM) 50

Konsole

- lokal 40
- XenVM 50

KVP-Logging

- Sicherheit 46

KVP-Menü 32

L

Linux-Desktop 40

Lizenzen für Open-Source-Software 14

lokale Konsole, Zugang 40

M

Management Unit 10, 15

Management-Netzwerk

- öffentlich 42

Management-Station 64

MANPU 42

Mindestzeit 25

MU 13

Kennungen 22

- Zugang IP-basiert einschränken 62

MU (Management Unit) 13

N

Net Unit 15, 17

Net-Client 63

Net-Storage 63

Netzwerkdienste 61

O

Open-Source-Software, Lizenzen 14

opensm2 24

openutm 24

Operator (Rolle) 19

Operatorberechtigung 20

P

Passphrase 35

Passwortverwaltung 25

PuTTY 33, 37

R

Read Community konfigurieren 64

Readme-Datei 11

Rechteeskalation 19, 32

Registerkarte

- Zertifikate 70, 71, 72, 73

robar 24

Rollenkonzept 19

root 24

RSA-Schlüssel 35

S

Schattenterminal 56

Schlüssel generieren 35

Schlüssel-Management 33

SE Manager 16

- Zugang 29

SE Server 13, 15

SE300 13

SE500 13

SE700 13

Secure Shell (SSH) 32, 33
Secure Shell Host-Schlüssel 33
Security Fix 76
Server Unit 10, 15
service 24, 42
Service (Rolle) 19
service (Service-Rolle) 23
Session-Management 30
Sessions anzeigen 30
Sicherheit 8
Signatur 66
SNMP, Sicherheit 64
Software-Signatur 66
SSH 32
SSH-Agent 36
SSH-Agenten 36
SSH-Client 33
SSH-Schlüssel 33
Storage-System (externes Asset) 57
storman 24
SU (Server Unit) 13
SU /390 13
SU x86 13
SU300 13
SU500 13
SU700 13
SVP (Service Prozessor) 13
System, gehärtet 8

T

tele 24

V

Verschlüsselung 29, 34
VNC-Viewer 51

W

Warnzeit 25

X

XenVM
 Konsol-Passwort 50
XenVM-Administrator (Rolle) 19
XenVM-Konsole, sicherer Zugang 50

Z

Zertifikat
 anzeigen 70
 beantragen 73
 bestätigen 68
 detailliert anzeigen 71
 erzeugen 72
 hochladen und aktivieren 74
Zertifikat, digital 67

