Deutsch

Fujitsu Server BS2000 SE Serie

Sicherheitshandbuch

Benutzerhandbuch

Stand der Beschreibung:
M2000 V6.6A SP1
X2000 V6.6A SP1
HNC V6.6A SP1

Ausgabe März 2025

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 bs2000services@fujitsu.com senden.

Zertifizierte Dokumentation nach DIN EN ISO 9001:2015

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: 2015 erfüllt.

Copyright und Handelsmarken

Inhaltsverzeichnis

Sicherheitshandbuch

1 Einleitung

Das vorliegende Benutzerhandbuch beschreibt die Sicherheitsmerkmale des SE Servers ausgehend von dessen Bedien- und Servicekonzept.
Eine allgemeine Beschreibung des SE Servers finden Sie im Benutzerhandbuch "Bedienen und Verwalten" [1].

Die Beschreibung der Sicherheitsmerkmale des SE Servers bezieht sich im Wesentlichen auf die Ebene des Basisbetriebssystems M2000 an der von außen zugänglichen Management Unit (MU). Die Units vom Typ HNC und Server Unit (SU) sind nach außen abgeschottet und werden deshalb nicht näher beschrieben. Gegebenenfalls wird auf Unterschiede, die bei Application Units (AU) zu beachten sind, eingegangen.

Die wichtigsten allgemeinen Sicherheitseigenschaften seien nachfolgend genannt. Die auf SUSE Linux Enterprise Server (SLES) 15 basierenden Basis-Systeme der Units des SE Servers (M2000, HNC und X2000) können aus folgenden Gründen als sicher und gehärtet bezeichnet werden:

- Nur für den Betrieb zwingend erforderliche signierte Softwarekomponenten werden installiert.
- Für Benutzer aller Rollen (z.B. Administrator oder BS2000-Operator) 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 vorgesehen, 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 MU, HNC und SU 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.

> ¡ 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 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 enthält das Handbuch „Einführung in die Systembetreuung“ [8] sowie die Handbücher zum Softwareprodukt SECOS [9 und 10].

Readme-Datei

Wenn für eine Produktversion eine Readme-Datei existiert, finden Sie diese online auf dem Manualserver unter https://bs2manuals.ts.fujitsu.com. Diese Datei enthält eine kurze Information über die Produktversion in deutscher oder englischer Sprache.

Ergänzende Produkt-Informationen in der Freigabemitteilung

Aktuelle Informationen, Versions-, Hardware-Abhängigkeiten und Hinweise für Installation und Einsatz einer Produktversion enthält die zugehörige Freigabemitteilung. Solche Freigabemitteilungen finden Sie ebenfalls online unter https://bs2manuals.ts.fujitsu.com.

Zielgruppen des Handbuchs

Dieses Handbuch wendet sich an Administratoren und Sicherheitsbeauftragte (z.B. mit der Rolle Security-Administrator) eines SE Servers. Kenntnisse der Betriebssysteme BS2000, Linux und ggf. Windows werden vorausgesetzt. Grundkenntnisse der Bedienung von grafischen Oberflächen sind vorteilhaft.

1.2 Änderungen gegenüber dem Vorgänger-Handbuch

Das vorliegende Handbuch beschreibt die Funktionalität des SE Managers mit Einsatz der Basis-Software M2000 /X2000/HNC V6.6A.

Funktionale Erweiterungen

Die funktionalen Erweiterungen mit der Basis-Software M2000/X2000/HNC V6.6A sind vollständig im Benutzerhandbuch „Bedienen und Verwalten“ [2] beschrieben.
Unter Sicherheitsaspekten ist insbesondere Folgendes relevant:

- Service-Kennung *service*
  - Das Passwort und dessen Verwaltung muss den heute allgemein gültigen Sicherheitsanforderungen entsprechen.
  - Dies gilt für die Länge und die Komplexität, sowie für die Gültigkeit und Warnzeit.
  - Die konkreten Werte für die Ablaufzeit und Inaktivzeit werden einvernehmlich zwischen dem Kunden und dem Service festgelegt.
  - Die Verwaltung des Passworts der Kennung *service* erfolgt gemäß der gemeinsamen Festlegung ausschließlich durch den Service.
- SNMPv3
  - Bei der Konfiguration von Trap-Empfängern – im Alarm Management und in der MU-spezifischen Weiterleitung von von der Hardware ausgelösten SNMP-Traps – wird das SNMPv3-Protokoll, welches hohen Sicherheitsanforderungen genügt, unterstützt.
  - Mit SP1: In SEM wird für jede einzelne MU ihre spezifische persistente SNMP-Engine-ID angezeigt.
- Anzeige der Teleservice-Meldungen
  - Alle Teleservice-Meldungen, welche vom SE Sever an die Service-Zentrale gesendet werden, werden in SEM als Events mit der Komponente TsCall und mit dem Gewicht NOTICE angezeigt.
- Neue Rolle
  - Eine neue Basis-Rolle *Remote-Service-Administrator* wurde eingeführt.
  - Mit SP1: Die neue Basis-Rolle *Shell-Zugang* wurde als Hilfsrolle eingeführt.
- Verwaltung der Passwörter
  - Im SE Manager erfolgt die Eingabe eines Passworts aus Sicherheitsgründen verdeckt.
    Während der Eingabe wird vor dem Eingabefeld ein Auge-Icon angezeigt, mit dem das Passwort sichtbar gemacht und wieder verborgen werden kann.
  - Mit SP1: Die Passwortregeln wurden verschärft, um die Sicherheit zu erhöhen.
  - Mit SP1: Die Passwörter der Kennungen werden überwacht. Dabei werden gegebenenfalls Events mit der Komponente PwMon erzeugt.

1.3 Darstellungsmittel

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

i	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`	Systemeingaben und -ausgaben
<abc>	Variablen, die durch Werte ersetzt werden.
Tastensymbole	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

In diesem Handbuch werden zur Bezeichnung der SE Server-Modelle und ihrer Komponenten Abkürzungen verwendet. Diese sind in der Einleitung der Basis-Betriebsanleitung [3] im Abschnitt "Modelle, Bezeichnungen, Abkürzungen" erklärt.

2 Architektur der SE Server und der Netzwerke

Die Beschreibung gliedert sich in die folgenden Abschnitte:

2.1 Hardware

Ein Server der Fujitsu Server BS2000 SE Serie (kurz: SE Server) kann aus folgenden Komponenten bestehen:

- Management Unit (MU) mit SE Manager
  Der Betrieb des SE Servers mit einer Management Unit wird als Single-MU-Konfiguration bezeichnet. Es ist möglich, die Management Unit redundant auszulegen. Eine SE Server-Konfiguration mit mehreren Management Units (MU-Redundanz am SE Server oder Management Cluster mit zwei SE Servern) wird als Multi-MU-Konfiguration bezeichnet.
  MU-Redundanz stellt sicher, dass die Komponenten des SE Servers auch bei Ausfall einer MU bedient werden können. Insbesondere steht damit die SKP-Funktionalität für die Bedienung einer SU /390 weiter zur Verfügung.
- Server Unit (SU)
  Eine SU ermöglicht den Betrieb von BS2000 (Native-BS2000 oder VM2000). Die SE Server SE710, SE730 /SE730B und SE740 sind jeweils mit einer SU /390 bestückt. Die SE Server SE310, SE320, SE330/SE330B und SE340 enthalten jeweils eine SU x86.
- Application Unit (AU)
  Am SE Server können mehrere AUs betrieben werden. Eine AU ermöglicht den Betrieb von Applikationen unter Linux, Windows oder Hypervisor-basierten Systemen.
- Net Unit (NU)
  Die Net Unit bietet höchste Performanz und Sicherheit für die interne Kommunikation in einem SE Server und für die Anbindung an Kundennetzwerke (IP-Netzwerke). Für eine SU /390 ist ein HNC zusätzlicher Bestandteil der Net Unit.
  Bei SE /390 ist die Net Unit immer redundant, bei SE x86 ist die Redundanz optional.
  Die Net Unit wird vorkonfiguriert ausgeliefert, ist bezüglich SE Server Management autark und kann einfach an das Kundennetzwerk angeschlossen werden.
- Rack-Konsole und KVM-Switch
- Peripherie (Storage)
- Optionale Hardware-Komponenten:
  Plattenspeichersysteme (für SU x86, AU), Tape Library Systeme (für SU x86), FC-Switche

2.2 Architektur der SE Server

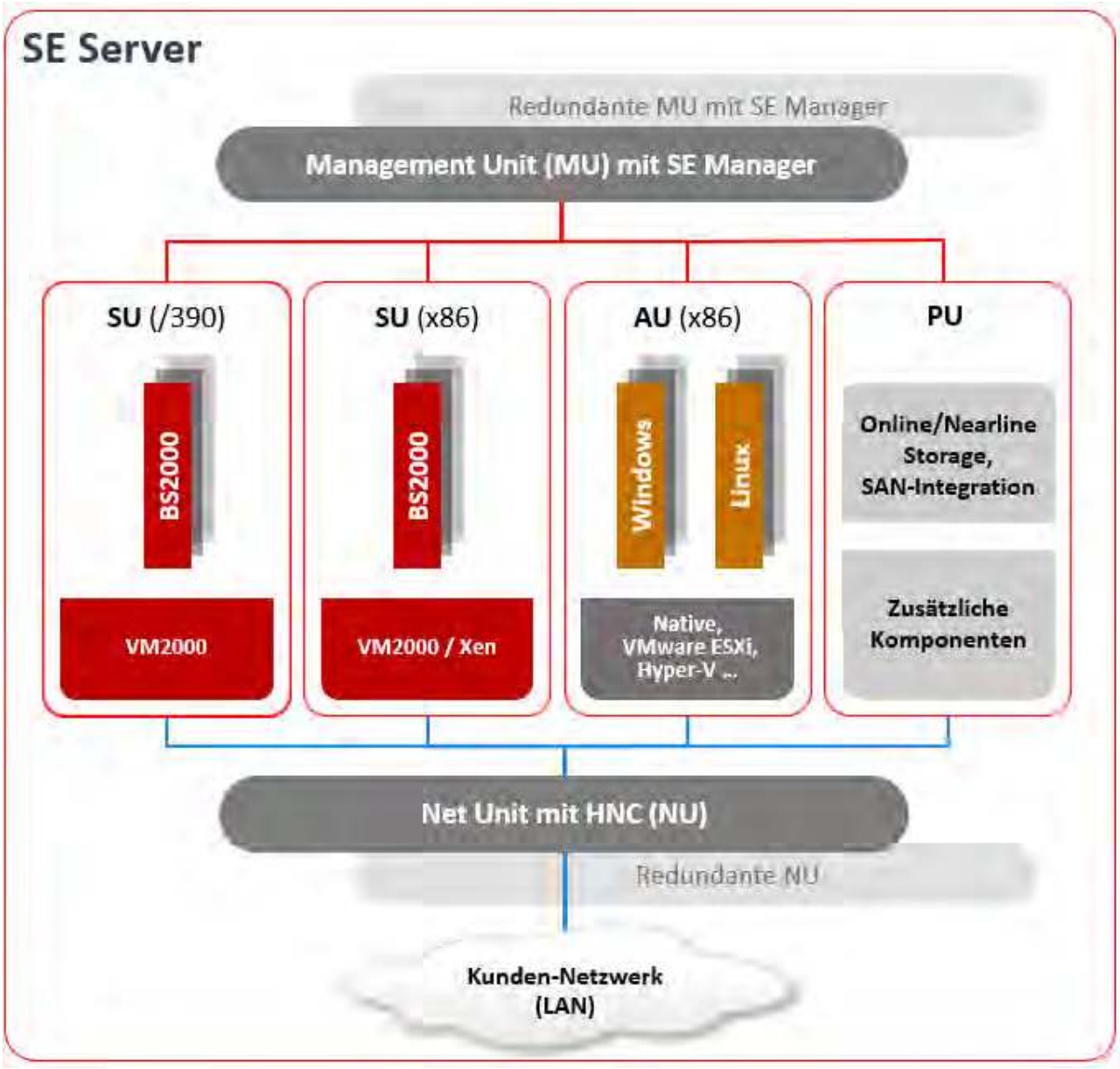


Bild 1: Architektur der SE Server

Mit dem SE Manager jeder MU können Sie alle Komponenten des SE Servers zentral bedienen und verwalten. Der SE Manager bietet dazu eine komfortable, Web-basierte Benutzeroberfläche.

Die Net Unit bietet höchste Performanz 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 nur an einer MU der SE Server-Konfiguration vorgenommen werden:

- Sie können Benutzerkennungen einrichten und für BS2000-Operator-Kennungen individuelle Berechtigungen vergeben. Siehe Abschnitt „Rollenkonzept und Benutzerkennungen".
- Sie können für Benutzerkennungen Multi-Faktor-Authentisierung (MFA) zur Anmeldung am SE Manager konfigurieren. Siehe Abschnitt „Authentisierung".
- Für die Verwendung von zentral verwalteten Kennungen (LDAP-Kennungen) müssen Sie einen LDAP-Zugang einrichten und aktivieren, siehe Abschnitt „Zugang zu einem LDAP-Server konfigurieren".

Die folgenden sicherheitsrelevanten Einstellungen und Maßnahmen müssen an jeder MU der SE Server-Konfiguration vorgenommen werden:

- Sie müssen die Konfiguration der IP-Adressen und Netzwerke für beide MUs gleich einrichten, siehe Kapitel „Netzwerksicherheit".
- Sie müssen die Sicherheitseinstellungen für den Service-Zugang an jeder MU festlegen, siehe Abschnitt „Funktion „Schattenterminal" nutzen" und Abschnitt „Zugang zu externen Assets".
- Sie müssen an jeder MU, an welcher Sie den SE Manager aufrufen, das Zertifikat dieser MU bestätigen bzw. importieren, siehe Abschnitt „Digitale Zertifikate".

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 acht 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 SE710/SE730 die SVP-Kommunikation zur SU /390.
- Öffentliche Daten-Netzwerke
  - Data Network Public (DANPU): bei Bedarf können bis zu acht Netzwerke DANPU<n> (mit <n>= 01..08) für die Anbindung von Anwendungen an das öffentliche Kundennetzwerk 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 eingerichtet werden.

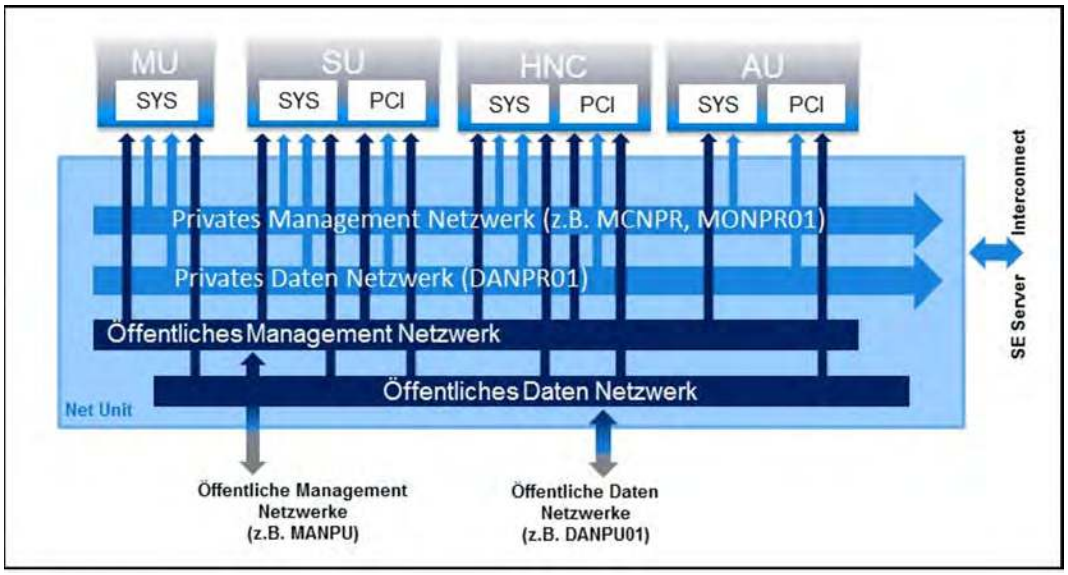


Bild 2: Net Unit Blockschaltbild

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 mittels ACL die Dienste (TCP/UDP Ports) der Netzwerke DANPU<xx>, MANPU, MONPU, DANPR<xx> und MONPR<xx> eingeschränkt werden (siehe Abschnitt „Sicherheit auf der Ebene der Net Unit").

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

> **Ausnahme**: Das gilt nicht, wenn Net-Storage mit Anschluss an MANPU oder DANPU an HNC oder SU x86 konfiguriert ist!
> Mit einer geeigneten Firewall-Einstellung an HNC oder SU x86 stellen Sie sicher, dass nur der für die Kommunikation (via NFS v3 oder v4) mit dem Net-Storage notwendige Port zugänglich ist.

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

2.4 Cluster

In einer SE Server-Konfiguration sind zwei Arten von Clustern möglich.

Management Cluster

Werden zwei oder mehrere SE Server miteinander zu einer Management-Einheit verbunden, wird von einem „Management Cluster“ (auch „SE Cluster“) gesprochen.

Ein Management Cluster wird auf Kundenwunsch vom Service konfiguriert und dient der gemeinsamen Bedienung und Verwaltung aller SE Server des Clusters.

Wesentliche Voraussetzungen für den Aufbau eines Management Clusters sind eine Net-Unit-Verbindung zwischen den beteiligten SE Servern (ISL-E) sowie eine externe CRD-Platte (oder zwei) zur Verwaltung der globalen Daten.

In Bezug auf Administration und Bedienung sind alle MUs des Management Clusters gleichwertig. Somit können Sie an jeder MU alle Objekte der gesamten SE Server-Konfiguration zentral administrieren und bedienen.

Die SE Server bleiben bedienbar, solange noch mindestens eine MU funktionsfähig ist. Für die SVP-Bedienung einer SU /390 und ihre korrekte HW-Anzeige wird jedoch eine MU des eigenen SE Servers vorausgesetzt.

SU Cluster

Zwei Server Units des gleichen Typs (SU /390 oder SU x86) können zu einer logischen Einheit, einem sogenannten „SU Cluster“ zusammengefasst werden.

Ein SU Cluster wird auf Kundenwunsch vom Service konfiguriert und stellt die Funktion Live Migration (LM) für die BS2000-Systeme der zwei Server Units zur Verfügung.

Weitere Details zu den Cluster-Arten und der Funktion Live Migration finden Sie im Handbuch „Bedienen und Verwalten“ [2]. Details zum Einsatz von Clustern beschreibt das Whitepaper „Cluster-Lösungen für SE Server“ [7].

3 Sicherer Zugang zu Management-Funktionen

Die Beschreibung gliedert sich in die folgenden Abschnitte:

3.1 Rollenkonzept und Benutzerkennungen

Kennungen und Berechtigungen sind global, d.h. MU-übergreifend. In einer Multi-MU-Konfiguration muss jede Maßnahme nur einmal an einer der MUs durchgeführt werden.

Im Falle eines Management Clusters gilt jede Rolle bzw. Kennung im gesamten Cluster.

Näheres dazu finden Sie in folgenden Abschnitten:

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 Rechte-Eskalation 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 die im Folgenden genannten Basis-Rollen definiert. Darüber hinaus können benutzerdefinierte Rollen durch Kombination von Basis-Rollen konfiguriert werden. Mit Ausnahme der Rollen Administrator und Service besitzen die übrigen Rollen eingeschränkte Rechte, die auf ihre jeweiligen Aufgabenbereiche zugeschnitten sind.
Über die unten beschriebene SEM-Funktionalität hinaus hat jede Basis-Rolle außerdem Zugang zu einigen weiteren SEM-Fenstern, wie etwa den Hauptfenstern Dashboard oder Zertifikate, kann ihr Passwort verwalten, das CA-Zertifikat der MU herunterladen und auf das Event Logging zugreifen.

- Administrator
  Die Rolle Administrator ist den anderen Rollen (mit Ausnahme der Rolle Service) übergeordnet. Sie berechtigt zu allen Funktionen des SE Managers sowie zum Shell-Zugang und zur Ausführung aller Funktionen des empfohlenen CLI. Sie kann nicht mit anderen Rollen in einer benutzerdefinierten Rolle kombiniert werden.
- BS2000-Administrator
  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. Außerdem darf ein BS2000-Administrator die Kommandos bs2Console, bs2Dialog und svpConsole mit Hilfe von PuTTY an einer entfernten Unit ausführen.
- BS2000-Operator
  Ein BS2000-Operator besitzt die Berechtigung für Funktionen des SE Managers, die für Betrieb und Operating von BS2000-Systemen notwendig sind. Zusätzlich kann ein Administrator oder Security-Administrator bestimmte Berechtigungen individuell für eine BS2000-Operator-Kennung konfigurieren. Außerdem darf ein BS2000-Operator die Kommandos bs2Console, bs2Dialog und svpConsole mit Hilfe von PuTTY an einer entfernten Unit ausführen.
- AU-Administrator
  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.
- Read-only-Administrator
  Ein Read-only-Administrator besitzt die Berechtigung alle Fenster des SE Managers anzuschauen, aber ändernde Aktionen dürfen nicht ausgeführt werden.

- Security-Administrator
  Ein Security-Administrator besitzt die vollständige Berechtigung für die Fenster und Funktionen des SE Managers unter den Kategorien Berechtigungen und Logging.
- Hardware-Administrator
  Ein Hardware-Administrator besitzt die vollständige Berechtigung für die Fenster und Funktionen des SE Managers unter den Kategorien Hardware -> Units, Hardware -> HW Inventory, Hardware -> Energy und Service -> Units.
- Storage-Administrator
  Ein Storage-Administrator besitzt die vollständige Berechtigung für die Fenster und Funktionen des SE Managers unter den Kategorien Geräte -> … -> IORSF-Dateien | Platten | Bandgeräte, Hardware -> Units -> … -> FC Anschlüsse | Multipath-Platten | CRD-Platten sowie Hardware -> Storage (ohne STORMAN!).
- Power-Operator
  Ein Power-Operator besitzt die Berechtigung für das Hauptfenster Units unter der Kategorie Hardware und die Funktionen zum Ein- und Ausschalten von Units.
- IP-Netzwerk-Administrator
  Ein IP-Netzwerk-Administrator besitzt die vollständige Berechtigung für die Fenster und Funktionen des SE Managers unter den Kategorien Hardware -> Units -> … -> IP Anschlüsse, Hardware -> Management -> … -> IP-Konfiguration | Routing & DNS sowie Hardware -> IP Netzwerke.
- FC-Netzwerk-Administrator
  Ein FC-Netzwerk-Administrator besitzt die vollständige Berechtigung für die Fenster und Funktionen des SE Managers unter den Kategorien Hardware -> FC Netzwerke und Geräte -> BS2000 Pfade.
- Schattenterminal-Operator
  Ein Schattenterminal-Operator besitzt die Berechtigung zum Zugang zum Hauptfenster Service -> Units -> <MU> -> Remote Service, auf dem ein Schattenterminal geöffnet werden kann.
- Remote-Service-Administrator
  Ein Remote-Service-Administrator besitzt die vollständige Berechtigung für die Fenster und Funktionen im Menü Service des SE Managers, welche in Bezug auf Remote Service relevant sind: Service -> Information (nur Kundenschlüssel) | Remote Service Zugang | Remote Service Sessions und Service -> Units -> ... -> Remote Service.
- Shell-Zugang
  Benutzer mit dieser Basis-Rolle besitzen die Berechtigung zum Shell-Zugang. Diese Rolle ist eine Hilfsrolle, die nur in Kombination mit einer anderen Basis-Rolle verwendet werden kann.

- Add-on-spezifische Rollen
  Die nachfolgende Beschreibung der Add-on-spezifischen Rollen bezieht sich auf den SE Manager.
  Die Rollenbeschreibung innerhalb der einzelnen Add-ons sind in den Add-on-spezifischen Handbüchern zu finden.
  - OPENSM2
    - OPENSM2-Administrator
      Ein OPENSM2-Administrator besitzt die Berechtigung zum Zugang zum Add-on OPENSM2 und zu dessen Administration auf allen Management Units.
    - OPENSM2-Information
      Ein Benutzer mit der Rolle OPENSM2-Information besitzt die Berechtigung zum Zugang zum Add-on OPENSM2. Die Administration des Add-ons ist nicht zulässig.
  - OPENUTM
    - OPENUTM-Administrator
      Ein OPENUTM-Administrator besitzt die Berechtigung zum Zugang zum Add-on OPENUTM und zu dessen Administration auf allen Management Units (Privilegien Master und Administration Write).
    - OPENUTM-Operator
      Ein OPENUTM-Operator besitzt die Berechtigung zum Zugang zum Add-on OPENUTM einschließlich Administration (Privileg Administration Write).
    - OPENUTM-Information
      Ein Benutzer mit der Rolle OPENUTM-Information besitzt die Berechtigung zum lesenden Zugang zum Add-on OPENUTM (Privileg Administration Read).
  - ROBAR
    - ROBAR-Administrator
      Ein ROBAR-Administrator besitzt die Berechtigung zum Zugang zum Add-on ROBAR und zu dessen Administration auf allen Management Units.
    - ROBAR-Operator
      Ein ROBAR-Operator besitzt die Berechtigung zum Zugang zum Add-on ROBAR. Die Administration des Add-ons ist nicht zulässig.
  - STORMAN
    - STORMAN-Administrator
      Ein STORMAN-Administrator besitzt die Berechtigung zum Zugang zum Add-on STORMAN und zu dessen Administration auf allen Management Units.
    - STORMAN-Information
      Ein Benutzer mit der Rolle STORMAN-Information besitzt die Berechtigung zum Zugang zum Add-on STORMAN. Die Administration des Add-ons ist nicht zulässig.
- Service
  Die Rolle Service ist ausschließlich dem Service vorbehalten.

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

Wenn im Folgenden spezielle Basis-Rollen genannt werden, wie z.B. BS2000-Administrator oder Security-Administrator, so sind damit auch jene benutzerdefinierten Rollen gemeint, welche diese Basis-Rollen beinhalten.

> **Sicherheitsrelevante Aktionen**
> Nutzen Sie das abgestufte Rollenkonzept und vergeben Sie den Anwendern nur jene Rechte, welche sie auch tatsächlich benötigen.

Individuelle Berechtigungen für BS2000-Operatoren

Ein Administrator oder Security-Administrator kann einer BS2000-Operator-Kennung für bestimmte Funktionen des SE Managers individuelle Berechtigungen erteilen oder entziehen.

- Konsol-Zugang zu einzelnen BS2000-Systemen
- Dialog-Zugang zu einzelnen BS2000-Systemen
- SVP-Zugang zu einzelnen SU /390

Hinweis: Konsol- und Dialog-Zugang für nicht-persistente BS2000-Systeme (VMs) verlieren beim Neustart der SU ihre Gültigkeit und müssen neu erteilt werden.

> **Sicherheitsrelevante Aktionen**
> Folgende Funktionen des SE Managers kann ein Administrator oder Security-Administrator für das Operating freigeben oder sperren (siehe Hauptmenü *Berechtigungen -> Benutzer -> Operator-Berechtigungen*):
>
> - 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

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 lokale Administratorkennung `admin`.
- Es können beliebig viele weitere Administratorkennungen angelegt werden.
  Diese Kennungen können wieder gelöscht werden.
- Vom Funktionsumfang her sind alle Administratorkennungen gleichwertig.

BS2000-Operating

- Es können beliebig viele BS2000-Operator-Kennungen angelegt werden.
  Diese Kennungen können wieder gelöscht werden.
- Vom Funktionsumfang her sind alle neu eingerichteten BS2000-Operator-Kennungen zunächst gleichwertig.
  Durch Vergabe von individuellen Berechtigungen lässt sich der Funktionsumfang individuell erweitern.

Kennungen mit sonstigen Rollen

- Es können beliebig viele Kennungen mit einer der anderen Basis-Rollen bzw. mit einer benutzerdefinierten Rolle angelegt werden.
  Diese Kennungen können wieder gelöscht werden.
- Vom Funktionsumfang her sind alle Kennungen mit derselben Rolle gleichwertig.

Service

- Es gibt die vordefinierte, nicht löschbare und nicht änderbare Kennung `service`, welche dem Service vorbehalten ist.
  Siehe auch Abschnitt „Weitere Kennungen des Basis-Systems".

3.1.2.1 Zentral verwaltete Kennungen (LDAP-Kennungen)

Neben lokalen Kennungen kann ein Administrator oder Security-Administrator auch LDAP-Kennungen für die verschiedenen Rollen zulassen. Diese Kennungen werden zentral auf einem LDAP-Server verwaltet (insbesondere auch die Passwörter).

Um LDAP-Kennungen zu nutzen, muss der Zugang zu einem LDAP-Server konfiguriert sein. Im Management Cluster kann der Zugang zum LDAP-Server SE-Server-spezifisch konfiguriert sein. Siehe Abschnitt „Zugang zu einem LDAP-Server konfigurieren".
Unter dieser Voraussetzung kann der Administrator beim Einrichten einer Kennung eine LDAP-Kennung über den Kennungstyp für die gewünschte Rolle freigeben. Die gleichzeitige Verwendung einer zentralen und einer lokalen Kennung gleichen Namens ist nicht möglich.
Beim Entfernen einer LDAP-Kennung wird der Zugang für diese Kennung wieder gesperrt.

3.1.2.2 Berechtigung zur Kennungsverwaltung

Nur unter einer Administratorkennung bzw. einer Kennung mit der Rolle Security-Administrator können andere Kennungen (unabhängig vom Typ) verwaltet werden. Im Einzelnen umfasst dies folgende Funktionen:

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

Sicherheitsrelevante Aktionen

- Für die vordefinierte Kennung `admin` ist ein initiales Passwort voreingestellt, das Sie beim Service erfragen können.

  Ändern Sie das Passwort unmittelbar nach dem ersten Anmelden.
  Ändern Sie ggf. auch die Gültigkeitsdauer und die anderen Passwortattribute.

  Zur Passwortverwaltung gelangen Sie wie folgt:

  - im SE Manager: *Berechtigungen -> Benutzer -> Passwortverwaltung*
  - im iRMC S5 bzw. S6: *Einstellungen -> Benutzerverwaltung -> Lokale Benutzerkennungen im iRMC*

- 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 mindestens 14 Zeichen lang sein und gewissen Komplexitätsanforderungen genügen muss.

3.1.2.3 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.

  > Die Service-Kennung (Kennung mit der Rolle Service) wird in der Benutzerverwaltung angezeigt, unterliegt aber nicht der Kennungsverwaltung durch den Administrator bzw. Security-Administrator. Die nachfolgenden Kennungen des Basis-Systems werden in der Benutzerverwaltung nicht angezeigt und unterliegen auch nicht der Kennungsverwaltung durch den Administrator bzw. Security-Administrator.

- `tele`
  Die Kennung `tele` dient dem Service als Zugangskennung und dem Anwender zur Bedienung des Schattenterminals. Unter dieser Kennung steht keine weitere Funktionalität zur Verfügung.
- `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 benötigte Kennungen, die jedoch für den Anwender nicht sichtbar und für die Anmeldung gesperrt sind:

- `x2kinternal` für interne Zugriffe
- `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 installiert ist
- Diverse interne Funktionskennungen wie z.B. die AIS-Kennung `aisconnect`

3.1.2.4 Kennungen für Add-on Packs

Für Add-on Packs gilt allgemein:

- Add-ons haben in der Regel ein eigenes Rollenkonzept.
- Im SE Manager werden explizite Berechtigungen für einzelne Add-ons durch Add-on-spezifische Rollen vergeben:
  - Voraussetzung für den Zugang zu einem Add-on ist eine Kennung mit einer Add-on-spezifischen Rolle. Damit hat die Kennung Zugang zu allen Instanzen des Add-ons im SE-Verwaltungsbereich.
  - Die Rolle bzw. Berechtigung innerhalb des einzelnen Add-ons ergibt sich aus der im SE Manager für die Kennung festgelegten Rolle.
- Die Abbildung der SEM-Rollen mit Zugang zu Add-ons zu den einzelnen Add-on-internen Rollen bzw. Berechtigungen wird in folgender Tabelle dargestellt („-“ bedeutet keinen Zugang; nicht angezeigte Basis-Rollen besitzen keinen Zugang zu irgendeinem Add-on):

SEM Basis-Rolle	openSM2	openUTM	ROBAR	STORMAN
Administrator	Administration	Master + Administration Write	Administrator	Administrator
Service	Administration	Master + Administration Write	Administrator	Administrator
OPENSM2-Administrator	Administration	-	-	-
OPENSM2-Information	Monitoring	-	-	-
OPENUTM-Administrator	-	Master + Administration Write	-	-
OPENUTM-Operator	-	Administration Write	-	-
OPENUTM-Information	-	Administration Read	-	-
ROBAR-Administrator	-	-	Administrator	-
ROBAR-Operator	-	-	Operator	-
STORMAN-Administrator	-	-	-	Administrator
STORMAN-Information	-	-	-	Storage info

3.1.3 Authentisierung

Der Zugang zum SE Manager einer MU ist nur mit Authentisierung über Kennung und Passwort möglich. Zur Erhöhung der Sicherheit kann für jede Kennung Multi-Faktor-Authentisierung (MFA) konfiguriert werden. In diesem Fall ist bei der Anmeldung am SE Manager nach der Eingabe von Kennung und Passwort in einem zweiten Schritt zusätzlich die Eingabe eines Einmalpassworts erforderlich. Dieses wird mit Hilfe einer Authentisierungs-App generiert.

Für lokale 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 Desktop der lokalen Konsole

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

Jede Authentisierung wird im Audit-Logging protokolliert.

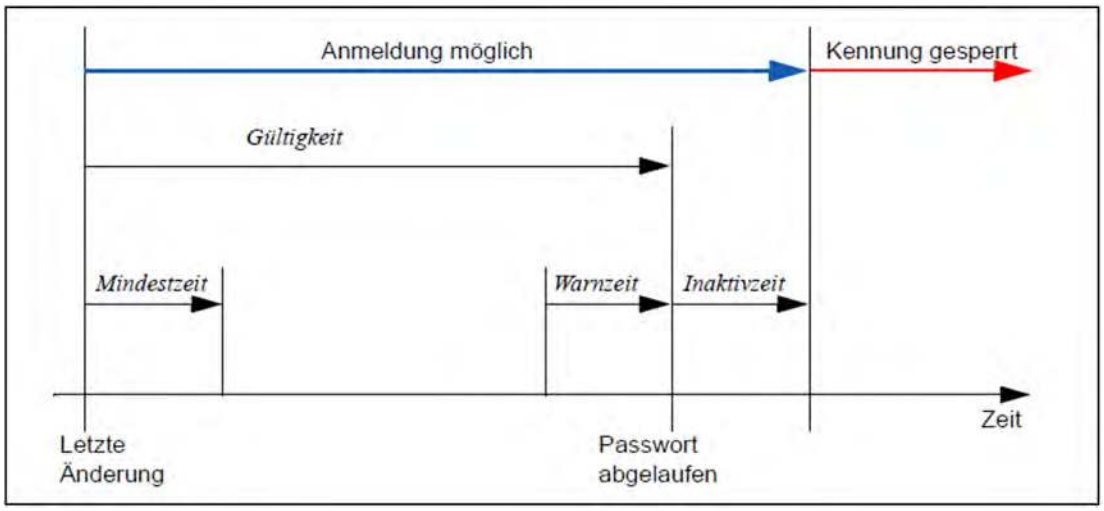
Wenn die Anmeldung am SE Manager scheitert, ist eine erneute Anmeldung erst nach einer Wartezeit von zehn Sekunden möglich. Diese Wartezeit schützt vor automatisierten Einbruchversuchen.

3.1.4 Passwortverwaltung für lokale Kennungen

Die Passwörter der lokalen 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) Administrator- bzw. Security-Administrator-Kennung 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.



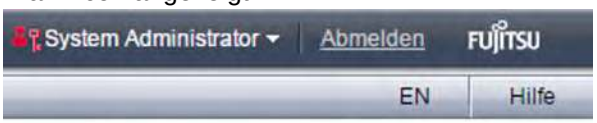
Auf der Basis der Einstellungen für die Systemhärtung werden Kundenkennungen mit folgenden Default-Werten für die Passwortverwaltung angelegt:

- Gültigkeitsdauer des Passworts: 60 Tage
- Mindestzeit bis zur nächsten Änderung des Passworts: 7 Tage
  Für eine Administratorkennung ist die Mindestzeit irrelevant und wird immer als 0 angezeigt.
- Warnzeit vor Ablauf des Passworts: 7 Tage
- Inaktivzeit nach Ablauf des Passworts: 7 Tage

Jeder Administrator und Security-Administrator kann jederzeit einzelne Einstellungen der Passwortverwaltung einer Kennung ändern.
Andere Benutzer können nur das Passwort der eigenen Kennung ändern. Dies ist aber nur möglich, wenn die Mindestzeit verstrichen ist.

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 Tooltipp dem Anwender, nach wie vielen 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.

- Wenn die Inaktivzeit verstrichen ist, ist die Kennung gesperrt und es ist keine Anmeldung mehr möglich. Ein Eingriff seitens eines (anderen) Administrators, Security-Administrators oder des Service ist dann notwendig (siehe „Sicherheitsrelevante Aktionen").

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.`

  > **Achtung!**
  > Das Kommando *passwd* darf auf Shell-Ebene nicht verwendet werden!

  In dieser Situation sollte sich der Anwender noch vor Ablauf der Warnzeit am SE Manager anmelden und das Passwort ändern.

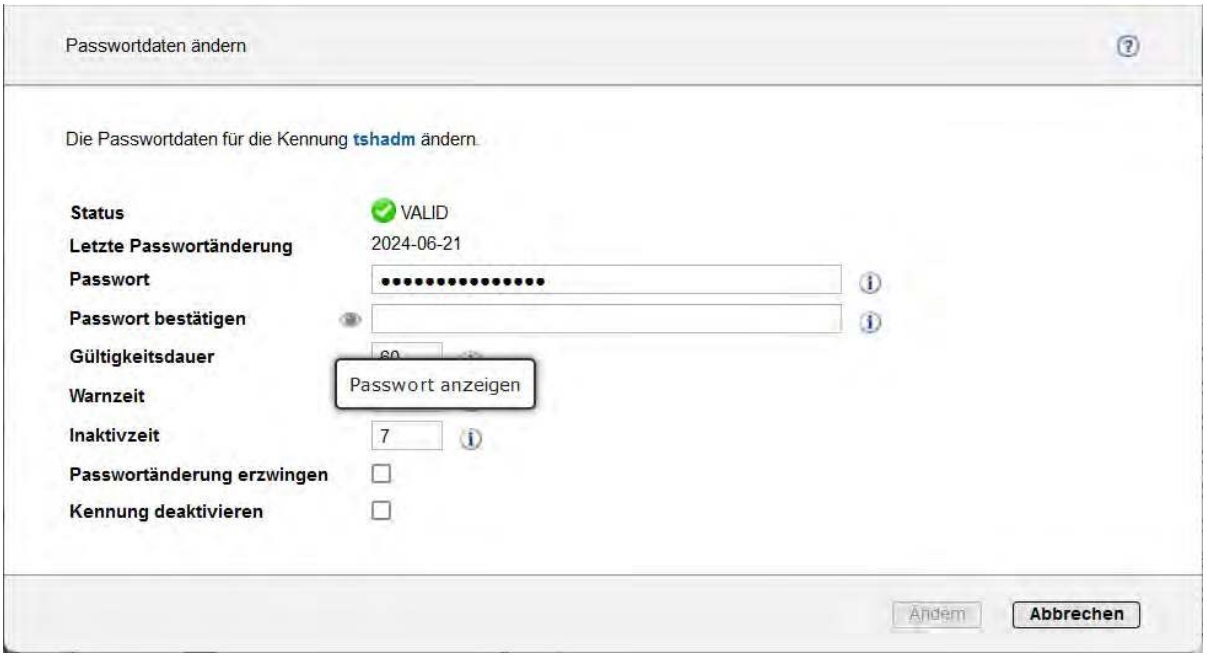
- Während der Inaktivzeit wird bei der Anmeldung die Passwortänderung erzwungen. In dieser Situation muss der Anwender wie folgt vorgehen:
  1. Die Anmeldung an der Shell abbrechen.
  2. Am SE Manager anmelden und im Anmeldefenster das Passwort ändern.
  3. Die Anmeldung an der Shell wiederholen.

- 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

- Ein Administrator oder Security-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 bzw. Security-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.

Im SE Manager erfolgt die Eingabe eines Passworts in der Regel aus Sicherheitsgründen verdeckt.
Während der Eingabe wird vor dem Eingabefeld ein Auge-Icon ( ) angezeigt, mit dem das Passwort sichtbar gemacht und durch nochmaliges Klicken auf das Icon wieder verborgen werden kann:



Service-Kennung service

Die Service-Kennung service wird bei der Installation mit einem Passwort mit der Gültigkeit von 30 Tagen initialisiert.
Anschließend verwaltet der Service das Passwort der Kennung service bezüglich Gültigkeit und Warnzeit in Absprache mit dem Kunden und gemäß den von diesem vorgegebenen Sicherheitsrichtlinien.
Mindestzeit und Inaktivzeit sind für die Kennung service grundsätzlich deaktiviert und können nicht geändert werden.
Es ist sichergestellt, dass die Kennung service nie gesperrt wird, dass also der Service nie vom SE Server ausgesperrt wird.

3.1.5 Zugang zu einem LDAP-Server konfigurieren

Mit der Registerkarte *LDAP* im Menü *Berechtigungen -> Konfiguration* können Sie den Zugang zu einem LDAP-Server konfigurieren und bearbeiten, auf dem die LDAP-Kennungen verwaltet werden, die für den SE Server freigegeben werden können.

In einem Management Cluster können Sie pro SE Server einen eigenen LDAP-Server konfigurieren. Zwei redundante MUs innerhalb eines SE Servers verwenden denselben LDAP-Server.

LDAP-Server und die MU(s) müssen ihre Zeit über denselben NTP-Server synchronisieren.

In einem Management Cluster wird die Konfiguration für jeden SE Server in einer eigenen Gruppe angezeigt. Die LDAP-Konfiguration ist SE-Server-spezifisch, im Standardfall wird sie aber für die beteiligten SE Server gemeinsam (d.h. gleich) konfiguriert. Details zur LDAP-Konfiguration im Management Cluster finden Sie im Whitepaper „Cluster-Lösungen für SE Server“ [7].

Sicherheitsrelevante Aktionen

Als Administrator oder Security-Administrator können Sie den Zugang zu einem LDAP-Server konfigurieren.
Für den Zugang benötigen Sie eine gültige Kennung auf einem LDAP-Server (Bind-DN) mit Passwort.

- Wenn Sie die Zugangsdaten eintragen oder ändern, können Sie testen, ob die LDAP-Konfiguration funktioniert. Nur wenn der Test erfolgreich war, kann mit LDAP-Kennungen gearbeitet werden.
- Sobald Sie den Zugang aktivieren und eine Verbindung zum LDAP-Server besteht, können die freigegebenen LDAP-Kennungen zur Anmeldung am SE Manager genutzt werden.
- Sobald Sie den Zugang deaktivieren, können die freigegebenen LDAP-Kennungen nicht mehr genutzt. werden.
- Wenn Sie die LDAP-Konfiguration löschen, werden die Konfigurationsdaten entfernt und LDAP-Kennungen können nicht mehr zur Anmeldung am SE Manager genutzt werden. Die gültigen Kennungen auf einem LDAP-Server sind weiterhin vorhanden.
- Die Kommunikation zwischen SE Server und LDAP-Server kann mittels TLS (Standard-Port 389) oder mittels LDAPS (Standard-Port 636) gesichert werden.
- Bei Verwendung von LDAP müssen für die Kommunikation mit dem LDAP-Server der für das LDAP-Protokoll konfigurierte Port (standardmäßig 389 bzw. 636 - siehe oben) sowie die Ports 88 und 750 für das Kerberos-Protokoll in der Firewall geöffnet sein.

3.2 Zugang zum SE Manager

Die Beschreibung gliedert sich in die folgenden Abschnitte:

- Sicherheitseinstellungen auf dem Administrations-PC
- Kommunikation mit Verschlüsselung
- Session-Management

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 1.3 (Transport Layer Security) unterstützt werden. Für die interne Kommunikation mit verwalteten AUs wird TLS 1.1 verwendet.

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 *Sessions* den Administrator über alle Sessions der Benutzer, die aktuell am SE Manager angemeldet sind. Angezeigt wird 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)
- ein Administrator oder Security-Administrator kann eine Session abbrechen

In allen 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 zur BS2000-Konsole und zum BS2000-Dialog
- 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 *Individuelle Einstellungen 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)

Zugangsfunktionen im SE Manager

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

- Zugang zur BS2000-Konsole und zum BS2000-Dialog
- Zugang zum SVP der SU /390
- Zugang zum CLI mit Ausführrechten eines eingeschränkten Satzes von CLI-Kommandos (siehe „CLI-Kommandos“ in der Online-Hilfe unter *Allgemeine Informationen*)
- Schattenterminal (in der Registerkarte *Remote Service*)

Anmeldung und Session-Einbindung

Beim Aufruf des Terminal-Fensters wird die Gültigkeit der Session des SE Managers geprüft und es ist keine weitere Anmeldung mehr nötig. Anschließend bleibt das Terminal-Fenster unabhängig von der Session geöffnet.

Verschlüsselte Kommunikation mit Secure Shell

Die Kommunikation erfolgt stets verschlüsselt über das SSH-Protokoll.
Dies gilt sowohl für die interne Kommunikation (z.B. bei den Verbindungen zu BS2000-Konsolen an SU x86) als auch für die externe Kommunikation (z.B. zwischen SSH-Client und der MU).

Keine Rechteeskalation

Eine Rechteeskalation im Basisbetriebssystem ist nicht möglich.

3.4 Alternative Zugänge mit Secure Shell

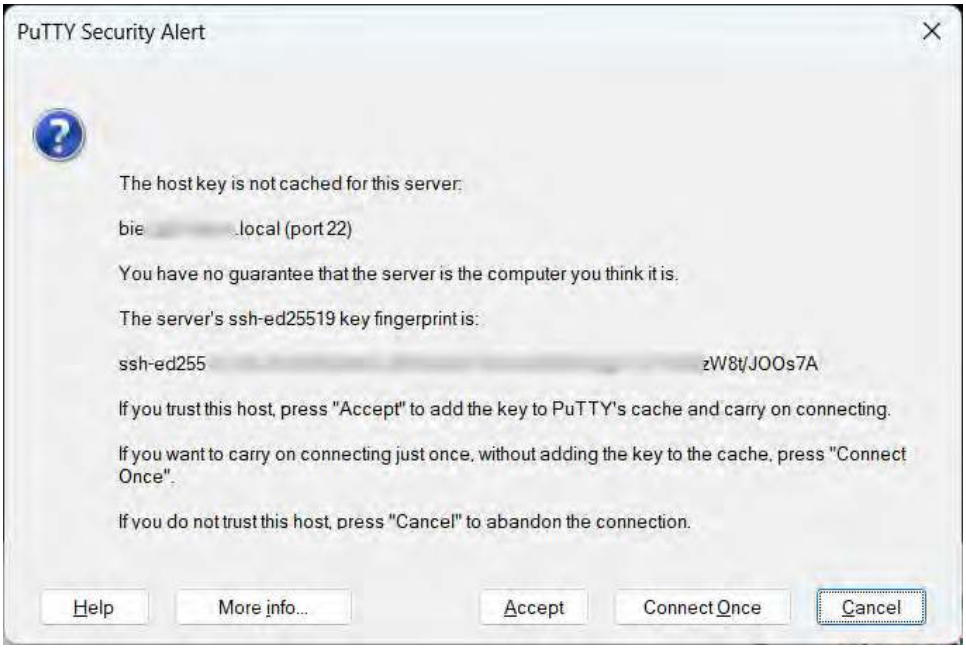
Zur Kommunikation auf Shell-Ebene können Sie alternativ zu dem im SE Manager integrierten Terminal den SSH-Client PuTTY (ab Version 0.63) benutzen. Siehe Abschnitt „Alternativer Zugang zum BS2000-Betriebssystem mit PuTTY".

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

Secure Shell Host-Schlüssel

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

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



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.

3.4.1 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 entfernten 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 entfernte 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 oder zum Prüfen einer Signatur dient, muss – im Gegensatz zum privaten Schlüssel – nicht 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" 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 Schlüsselpaares 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.

3.4.2 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 eingetippt 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_SOCK=/tmp/ssh-JGK12327/agent.12327; export SSH2_AUTH_SOCK;
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
```

3.4.3 PuTTY mit PuTTYgen und Pageant

In diesem Abschnitt wird die Erzeugung von Schlüsselpaaren und die Verteilung der öffentlichen Schlüssel mit Hilfe von PuTTY beschrieben (siehe http://www.chiark.greenend.org.uk/~sgtatham/putty). PuTTY ist eine freie Implementierung von Telnet und Secure Shell für Win32 und Unix System-basierte Plattformen und ist nützlich im Dialogmodus.

- Schlüsselgenerator PuTTYgen
- Authentifizierungs-Agent Pageant

3.4.3.1 Schlüsselgenerator PuTTYgen

Der Schlüsselgenerator PuTTYgen (siehe http://the.earth.li/~sgtatham/putty/latest/htmldoc/Chapter8.html) 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.
- 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.

3.4.3.2 Authentifizierungs-Agent Pageant

PuTTY's Authentifizierungs-Agent Pageant (siehe http://the.earth.li/~sgtatham/putty/latest/htmldoc/Chapter9.html) 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 *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.

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".

Zugang zu Management Unit mit Linux-Desktop

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

Die Anmeldung ist unter jeder Kennung möglich.

Die Funktionalität des 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 entsprechende 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 Desktop.
  Die standardmäßige Timeout-Einstellung des 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.

Der Zugang zum iRMC ist über den SE Manager möglich:
Im Menü *Hardware -> Units -> [<se-server> ->] <mu> -> Information* zeigt die Registerkarte *System* das Feld *iRMC-Adresse* mit einem Link zum iRMC an. Über diesen Link lässt sich die Web-Oberfläche des iRMC öffnen.

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

Der Administration werden die folgenden Funktionen empfohlen:

- Ein-/Ausschalten der Management Unit (über die Web-Oberfläche des iRMC Schalter rechts oben: *System-Ein-/Ausschalter*)
  Mittels *System hochfahren* kann die Management Unit aus der Ferne hochgefahren werden.
- Ändern des eigenen Passworts (nur per Kommando)

Sicherheitsrelevante Aktionen

- **Benutzerverwaltung**
  - Bei Auslieferung des SE Servers ist für die vordefinierte Kennung `admin` ein initiales Passwort eingestellt, das beim Service erfragt werden kann bzw. ab MU M5 auf der ID-Karte ersichtlich ist.
    Auf iRMC-Ebene besitzt `admin` das Privileg Operator und das zusätzliche Privileg der Konsolenumleitung. Es stehen keine weiteren Konfigurationsmöglichkeiten zur Verfügung.
    Ändern Sie das Passwort unmittelbar nach dem ersten Anmelden!
    Das ist mit dem M2000-Kommando `rmcPasswdAdmin`, welches unter jeder Administrator-Kennung ausgeführt werden kann, möglich.
  - Es ist möglich, weitere (personalisierte) Kennungen durch den Service anlegen zu lassen. Diese sollten aber nicht mit höheren Privilegien als die vordefinierte Kennung `admin` ausgestattet werden. 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 von Linux benutzte Bootloader GRUB (GRand Unified Bootloader) ist ebenfalls durch ein Passwort geschützt, das dem Service bekannt ist.

> **i** Standardmäßig ist die Rack-Konsole (lokale Konsole) der Management Unit zugeschaltet. Wenn Sie den Konsol-Switch umschalten (siehe Abschnitt „Zugang über die lokale Konsole"), 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 und zu den Systemen auf den Application Units.

4.1 Sicherer Zugang zu BS2000-Systemen

Die Beschreibung gliedert sich in die folgenden Abschnitte:

- Sicherheit im BS2000-Betriebssystem
- KVP-Logging-Dateien herunterladen
- Alternativer Zugang zum BS2000-Betriebssystem mit PuTTY

4.1.1 Sicherheit im BS2000-Betriebssystem

Das Betriebssystem BS2000 stellt Basisfunktionen für die Systemsicherheit bereit. Siehe dazu das Handbuch „Einführung in die Systembetreuung“ [8].

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 ([9] und [10]).

4.1.2 KVP-Logging-Dateien herunterladen

Die KVP-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 oder BS2000-Administrator können Sie die KVP-Logging-Dateien herunterladen und für die weitere Verwendung auf den Administrations-PC speichern.

Den Zugriff zu den KVP-Logging-Dateien erhalten Sie über das jeweilige BS2000-System:

- im Native-BS2000-Modus über die Registerkarte *KVP-Logging* unter *Systeme* -> [*<se server> (SE<model>)* ->] *<unit> (SU<model>) -> BS2000*
- im VM2000-Modus über die Registerkarte *KVP* unter *Systeme* -> [*<se server> (SE<model>)* ->] *<unit> (SU<model>) -> <bs2000-vm>*

Alternativ ist der Zugriff auch möglich über die Registerkarte *KVP* unter *Geräte* -> [*<se server> (SE<model>)* ->] *<unit> (SU<model>).*

> **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, SVP-Konsole (nur SU /390) und BS2000-Dialog über den SSH-Client PuTTY (ab Version 0.63) unter folgenden Voraussetzungen möglich:

- Die Verbindung erfolgt zur MU.
- Es wird eine gültige Administrator-, BS2000-Administrator- oder BS2000-Operator-Kennung (letztere nur remote!) angegeben. Eine Authentisierung mit Passworteingabe oder installiertem ssh-Schlüssel ist erforderlich.
- Als Folgekommando wird das CLI-Kommando `bs2Console`, `svpConsole` bzw. `bs2Dialog` mit entsprechenden Parametern angegeben.
  Ein BS2000-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.

Beispiele für die alternative BS2000-Bedienung mit PuTTY enthält der Anhang des Handbuchs „Bedienen und Verwalten“ [2]. Eine detaillierte Syntaxbeschreibung der CLI-Kommandos finden Sie in der CLI Kommando-Referenz, siehe Online-Hilfe des SE Managers unter *Allgemeine Informationen -> CLI-Kommandos*.

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 / Management Board verantwortlich (Sicherheit des Betriebssystems, Passwortverwaltung, Verbieten unsicherer Dienste, Administration des iRMC / Management Boards, Service-Fähigkeit, usw.).

> **i** 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 Unit 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" entsprechend.

4.2.2 Zugang zum iRMC / Management Board der Application Unit

Bei Application Unit PY erfolgt der Zugang über den iRMC, bei Application Unit PQ über das Management Board.

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

- Benutzerverwaltung an der Application Unit

  Sicherheitsrelevante Aktionen

  - Die Kennung `semuser` dient dem SE Manager als fest vorgegebener Zugang und darf durch den Administrator bzw. Security-Administrator nicht gelöscht werden (siehe auch Abschnitt „Einbindung der Application Unit in den SE Manager").
    Die Kennung `semuser` ist nach der Konfiguration durch den Service mit einem initialen Passwort geschützt, das Sie beim Service erfragen können.
    Ändern Sie dieses Passwort sofort bei der Inbetriebnahme.
  - Es ist möglich, weitere (personalisierte) Kennungen anzulegen. Beachten Sie dabei das auf dem iRMC / Management Board vorgegebene Privilegienkonzept.
    Nicht benutzte Kennungen sollten Sie deaktivieren.

- Ein-/Ausschalten der Application Unit
  Hierzu steht der Administration auf dem iRMC / Management Board 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.

  Sicherheitsrelevante Aktionen

  Schutzfunktionen:

  - Es ist möglich, sich per *Logout* von der Web-Oberfläche des iRMC / Management Board abzumelden.
    Dies kann beim Verlassen des Arbeitsplatzes alternativ oder zusätzlich zu den Sperrmechanismen des Administrations-PCs genutzt werden.
  - Die Web-Oberfläche des iRMC / Management Board 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 kann an folgender Stelle konfiguriert bzw. eingesehen werden:

    - iRMC S5 bzw. S6 Web Server: unter *Einstellungen -> Dienste -> Web-Zugriff -> Sitzungs-Zeitüberschreitung*
    - Bei Bedarf kann der Service diese Einstellung für Sie vornehmen.
    - Die Session-Timeout-Einstellung ist für alle Kennungen gültig.

4.2.3 Einbindung der Application Unit in den SE Manager

Zugang zum iRMC / Management Board der Application Unit

Zur Einbindung der Application Unit in den SE Manager (Statusinformationen, Ein-/Ausschalten, etc.) wird ein Zugang zum iRMC / Management Board der Application Unit benötigt.

Wenn der Service eine Application Unit konfiguriert, richtet er die fest vorgegebene Kennung `semuser` mit den Rechten „*LAN Channel Privilege Administrator*, *Serial Channel Privilege User*“ und einem initialen Passwort ein.

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

Zugang zur Application Unit

Dieser Zugang wird benötigt, wenn die Application Unit mit dem Betriebssystem VMware vSphere ESXi betrieben wird.

Der Administrator oder AU-Administrator stellt auf der AU eine Kennung bereit und konfiguriert diese und das Zugangspasswort im SE Manager:

- *Hardware -> Units ->* [*<se server> (SE<model>) ->*] *<unit> (AU<model>) -> Management -> IP Konfiguration*, Aktion *Zugangsdaten ändern* in der jeweiligen Gruppe der Zugangsdaten.

4.2.4 Zugang über die lokale Konsole

Wenn Sie den Konsol-Switch umschalten (siehe Abschnitt „Zugang über die lokale Konsole"), 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`.
- Das Umschalten des Konsol-Switch oder das Ausschalten der Konsole hat kein automatisches Abmelden zur Folge.

5 Remote-Service (via 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`. Da `tele` nur eine Zugangskennung ohne weitere Funktionalität ist, wechselt der Service-Techniker in der Regel 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.
- Der Kunde kann sich über die aktuell offenen AIS Connect Verbindungen informieren oder informieren lassen. Im Notfall kann er eingreifen und eine bestehende Verbindung abbrechen.
- 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 Funktion „Schattenterminal" nutzen).

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

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-Kennung

Auf einer Management Unit steht dem Service im Basis-System die Kennung `service` zur Verfügung. Unter dieser Kennung arbeitet der Service-Techniker sowohl 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 Konsole (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 Konsole (Konsol-Mnemonik) verwendet. Um eine Unterscheidung zu erreichen, können Sie den BS2000-Operator-Kennungen unterschiedliche Konsolen zuteilen (über individuelle Zugangsrechte). Für Administrator-Kennungen, BS2000-Administrator-Kennungen und insbesondere auch den Service kann nur eine Absprache getroffen werden, bestimmte eindeutige Konsolen zu verwenden.

Sicherheitsrelevante Aktionen

- Ändern der Konsole für BS2000-Operator-Kennungen
  Im SE Manager erhalten Sie unter *Berechtigungen -> Benutzer -> Operator-Berechtigungen* die Möglichkeit, den Konsolzugang zu einem System mit einer bestimmten Konsole einzutragen. Die Änderung wird sofort wirksam.
- Konsole im Betriebssystem BS2000 definieren
  Es muss sichergestellt sein, dass die verwendeten Konsolen im BS2000 definiert sind, damit der Konsolzugang funktionstauglich ist.
  Die Konsolen 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 Konsole finden Sie im Handbuch „Einführung in die Systembetreuung“ [8].

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].

> ℹ 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 1.2 (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 ihre 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 Schattenterminal-Operator (nicht AIS Proxy-Konfiguration) im SE Manager durch. Die Funktionen sind in der Registerkarte *Remote Service* unter *Service -> Units ->* [*<se server> (SE<model>) ->*] *<unit> (MU)* zusammengefasst.

In einer Multi-MU-Konfiguration müssen Sie an jeder MU 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 Aktuelle Nutzung des Service-Zugangs überwachen

Anzeige der Remote-Service-Sessions

Auf der SEM-Seite *Service -> Remote Service Sessions* werden AIS Connect Sessions und AIS Connect Logging-Dateien angezeigt.

Die Gruppe *AIS Connect Sessions* zeigt die Sessions an, die die Service-Zugänge zu der Management Unit und zu den externen Assets aktuell nutzen.

> ¡ Die Anzeige der Sessions ist nur möglich bei direktem Anschluss der MU, nicht aber bei Anschluss über ein Gateway.

Über das Icon *Löschen* ( ) haben Sie auch die Möglichkeit eine Session zu löschen. Damit wird die aktuelle Nutzung des Service-Zugangs abgebrochen.

> ¡ Da Sie durch diese Aktion ggf. einen wichtigen Service-Vorgang abbrechen, sollte die Aktion nur im Notfall erfolgen.

In einer SE-Server-Konfiguration mit mehreren MUs erhalten Sie den vollständigen Überblick über alle Service-Zugänge, wenn Sie sich die Sessions an jeder MU anzeigen lassen.

Benachrichtigung über Remote-Service-Sessions (nur ssh)

- Sie können sich über das Zustandekommen von Remote-Service-Sessions auf ssh-Ebene folgendermaßen zeitnah informieren lassen:
  - Bei jeder Remote-Anmeldung eines Service-Technikers wird ein Event für die Komponente RemSrv erzeugt. Diese Events sind in SEM im Menü *Logging -> Event Logging* zu sehen.
  - Sie können sich im Alarm Management für eine Benachrichtigung per Mail für diese Komponente anmelden. Dann werden Sie sofort über jede neue Remote-Service-Session informiert.
    Dies können Sie im Menü *Logging -> Alarm Management* konfigurieren.
- Zusätzliche Optionen:
  - Sie können erzwingen, dass sich der Service-Techniker bei der Anmeldung persönlich identifiziert und den aktuellen Auftrag nennt. Die Angaben des Service-Technikers werden Teil des Events und werden auch in der Alarm-Mail sichtbar.
  - Sie können dem Service-Techniker bei der Anmeldung Informationen bereitstellen, welche ihm bei einer Arbeit weiterhelfen können, z.B. Informationen bezüglich Kontaktpersonen im Rechenzentrum.
  - Die dafür nötige Konfigurationsmöglichkeit finden Sie im Menü *Service -> Konfiguration -> Remote Service Zugang*.
- In einer SE-Server-Konfiguration mit mehreren MUs sind diese Einstellungen global bzw. MU-übergreifend.

5.6 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 in der Registerkarte *Remote Service* unter *Service -> Units ->* [*<se server> (SE<model>) ->*] *<unit> (MU)* an.
Als Administrator, Security-Administrator oder Schattenterminal-Operator 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 zugelassen
    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.

  In einer SE-Server-Konfiguration mit mehreren MUs müssen Sie an jeder MU die selben Einstellungen vornehmen.

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

6 Konfigurations- und Diagnosedaten

Die Beschreibung gliedert sich in die folgenden Abschnitte:

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.
In einer Single-MU-Konfiguration lässt sich mit einer CSR-Sicherung die Konfiguration des betreffenden Basis-Systems zum Zeitpunkt der Sicherung wiederherstellen.

In einer Multi-MU-Konfiguration muss zwischen MU-spezifischen und MU-globalen Daten unterschieden werden.

- Für die MU-spezifischen Daten gilt:
  Die aktuellen MU-spezifischen Daten werden bei einer Wiederherstellung aus einem CSR-Archiv durch die alten Daten ersetzt.
- Für die MU-globalen Daten gilt:
  Die aktuellen MU-globalen Daten werden bei einer Wiederherstellung unverändert beibehalten, nur alte nicht mehr existierende MU-globale Daten werden restauriert.
  Die MU-globalen Daten sind die konfigurierten Berechtigungen (Kennungen, LDAP-Konfiguration, IP-basierte Zugangsberechtigungen), die Konfiguration des Alarm Managements, die konfigurierten Application Units, die konfigurierten Anwendungen, die Konfiguration der FC Netzwerke, die konfigurierten SU Cluster.

> **Sicherheitsrelevante Aktionen**
>
> Als Administrator, BS2000-Administrator oder AU-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).
>
> Die CSR-Sicherung enthält sicherheitsrelevante Daten des Basis-Systems. Kundendaten aus Ihren darauf oder damit betriebenen BS2000-Systemen sind jedoch nicht enthalten.

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.

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 Benutzerrollen BS2000-Administrator und BS2000-Operator ist diese Funktion ebenfalls zugänglich.

Sicherheitsrelevante Aktionen

Als Administrator, BS2000-Administrator oder BS2000-Operator 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.

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

Die Beschreibung gliedert sich in die folgenden Abschnitte:

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

Typ	Name und Port	Verwendungszweck
TCP	ssh (22)	Kommunikation auf Shell-Ebene (z.B. BS2000-Konsole/Dialog, SVP-Konsole, Schattenterminal)
TCP	domain (53)	Einbindung in den Domain Name Service (DNS)
TCP	http (80)	Die Kommunikation über diesen Port wird grundsätzlich auf https (443) umgelenkt.
TCP	kerberos (88)	Optional: Für Kerberos
TCP	snmp (161)	Für lesenden SNMP-Zugriff durch Management-Stationen
TCP	snmptrap (162)	Für Empfang von SNMP-Traps von der Hardware-Überwachung
TCP	ldap (389)	Optional: Für das Lightweight Directory Access Protocol (LDAP)
TCP	https (443)	Kommunikation zwischen Browser (z.B. auf Administrator-PC) und Web-Oberfläche des Systems (z.B. SE Manager)
TCP	ldaps (636)	Optional: LDAP protocol over TLS/SSL
TCP	rfile (750)	Optional: Für Kerberos Version IV
TCP	iascontrol-oms (1156)	PRSC/prscx (Periodical Remote System Check) sendet regelmäßig Lebend-Meldungen an die Service-Zentrale
TCP	nfs (2049)	Optional: Network File System (NFSv4) [RFC5665]
TCP	caupc-remote (2122)	Optional: AIS Gateway
TCP	storman (4178)	Optional: Für die Kommunikation mit StorMan (Add-on)
TCP	5800	Browser-Zugang zur VNC-Schattenfunktionalität des Remote Service (AIS Connect)
TCP	rfb (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	kerberos (88)	Optional: Für Kerberos

UDP	ntp (123)	Einbindung in das Network Time Protocol (NTPl) [RFC5905]
UDP	snmp (161)	Für lesenden SNMP-Zugriff durch Management-Stationen
UDP	snmptrap (162)	Für Empfang von SNMP-Traps von der Hardware-Überwachung
UDP	syslog (514)	Für die Überwachung von Komponenten (SYSLOG)
UDP	dhcpv6-client (546)	Optional: Der DHCPv6-Client-Port wird bei entsprechender Konfiguration einer LAN-Schnittstelle genutzt.
UDP	loadav/kerberos-iv (750)	Optional: Für Kerberos Version IV
UDP	multicast-ping (9903)	Für die Überwachung von Komponenten [RFC6450]
ICMP	-	Internet Control Message Protocol (ping)

Tabelle 1: Ports für eingehende Verbindungen

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.

Hinweis zu HNC und SU x86

Bei Verwendung der Net-Storage-Funktionalität über die Netzwerke MANPU und DANPU gibt es an diesen Units direkte ausgehende Verbindungen, welche aber kein Sicherheitsrisiko darstellen.

Einstellungen der externen Firewall

Die in der Tabelle 1 beschriebenen Ports müssen ggf. in der externen Firewall freigeschaltet sein. Ausnahmen sind TCP 10021-10022, welche der redundanten SKP-Funktionalität der MUs innerhalb des SE Servers dienen.

Außerdem müssen ggf. auch Ports für weitere optional genutzte Funktionen mit ausgehenden Verbindungen freigeschaltet werden.

- Bei Verwendung von LDAP der in SEM eingestellte Port LDAP-Port (je nach Portokoll standardmäßig 389 oder 636), sowie die Ports 88 und 750 für Kerberos.
- Für die SNMP-Abfragen muss in der Firewall der Port 161 geöffnet sein.
- Für Traps der Port 162.

Beispiele:

- Verbindung zu einem LDAP-Server, standardmäßig TCP-Port 389
- NFSv4-Port TCP 2049 bei Verwendung der Net-Storage-Funktionalität
- Im Falle von ROBAR müssen die für den Zugang zu den Speichersystemen nötigen Ports freigeschaltet werden.

7.2 IP-basierte Zugangsbeschränkung

Der Administrator kann den Zugang zum SE Server 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.
In einem Management Cluster ist eine serverspezifische Konfiguration möglich.

Die aktuelle Einstellung zeigt die Registerkarte *IP-basierte Zugangsberechtigungen* im Menü *Berechtigungen -> Konfiguration*.

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

Sicherheitsrelevante Aktionen

- Sie können die gesamte Konfiguration für die IP-basierte Zugangsbeschränkung wechselweise deaktivieren und aktivieren. (Status aktiv/inaktiv)
  Das Deaktivieren ist z.B. für Wartungszwecke und Tests sinnvoll, oder dann, wenn man zunächst eine vollständige Konfiguration vorbereiten und diese anschließend insgesamt aktivieren will.
- Mit dem ersten Eintrag (IP-Adresse oder IP-Netzwerk) im aktivierten Zustand aktivieren Sie die IP-basierte Zugangsbeschränkung zum SE Server. Der Zugang ist dann nur noch für IP-Adressen möglich, die entweder explizit oder über ein IP-Netzwerk eingetragen sind.
  Sie müssen deshalb Folgendes unbedingt **beachten**:
  Stellen Sie sicher, dass beim Aktivieren Ihre eigene IP-Adresse (bzw. das Subnetz) Teil der Konfiguration ist. Anderenfalls sperren Sie sich aus und verlieren den Zugang zum SE Server!
- Wenn Sie den letzten Eintrag aus der Liste für die Zugangsbeschränkungen löschen, ist der Zugang zum SE Server wieder unbeschränkt für alle IP-Adressen möglich, unabhängig vom Status der Konfiguration.
  Es ist auch das Löschen der gesamten Konfiguration in einem Schritt möglich.
- In einem Management Cluster ist eine serverspezifische Konfiguration möglich. Alle Aktionen können deshalb pro Server oder für den gesamten Management Cluster durchgeführt werden.

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.

  > ℹ 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.
- 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. bei Statusänderungen) Traps an Management-Stationen.
- Auf Application Units müssen Sie SNMP dagegen selbst konfigurieren.

Um einfach auf SE-Server-spezifische Daten lesend zuzugreifen und um die SE-Server-spezifischen 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`

An den Management Units und Server Units x86 führt ServerView RAID periodisch Prüfungen der Hardware-Komponenten durch. Diese Vorgänge werden per Trap gemeldet, und zwar auch im Gutfall mit dem Gewicht `NOTIFICATION`. Text-Beispiel eines solchen erfolgreichen Prüfvorgangs: "*Patrol Read started*" und "*Patrol Read finished*". Damit diese Traps durch die Management-Station korrekt dargestellt werden, muss die MIB /usr/share /snmp/mibs/FSC-RAID-MIB.txt an der Management-Station importiert werden.

Damit die Traps von ServerView und get-Anfragen durch die Management-Station korrekt dargestellt werden, müssen die MIBs `/usr/share/snmp/mibs/SRVMAGT-INVENT.TXT` und `/usr/share/snmp/mibs/SRVMAGT-SC2.TXT` an der Management-Station importiert werden.
Damit allgemeine Hardware-bezogene Traps und get-Anfragen durch die Management-Station korrekt dargestellt werden, muss die MIB `/usr/share/snmp/mibs/INTEL-WFM-MIB.mib` an der Management-Station importiert werden.

> Die Traps enthalten in der Regel weder das Trap-Gewicht noch den Meldungstext.
> Diese Informationen können nur aus der MIB gelesen werden.

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

SNMP-Protokolle:

- Bezüglich lesender Zugriffe werden die Protokolle SNMPv1 und SNMPv2c unterstützt.

- Bei der Konfiguration von Trap-Empfängern - im Alarm Management und in der MU-spezifischen Weiterleitung von von der Hardware ausgelösten SNMP-Traps - wird (neben SNMPv1 und SNMPv2c) auch das SNMPv3-Protokoll unterstützt.
  Mit SNMPv3, der neuesten Version des SNMP-Protokolls, stehen verbesserte Sicherheitsfunktionen zur Verfügung:
  Dadurch werden etwa Authentisierung und Verschlüsselung unterstützt, um die Integrität und Vertraulichkeit der übertragenen Daten zu gewährleisten.
  In SEM wird für jede einzelne MU ihre spezifische persistente SNMP-Engine-ID angezeigt. Diese kann an einer SNMP-Management-Station zur Identifikation der MU benutzt werden.

Sicherheitsrelevante Aktionen

- Leseberechtigungen
  Achten Sie bei der Erstellung der SNMP-Konfiguration für Leseberechtigungen darauf, dass durch entsprechende Konfiguration der Read Community mit der Beschränkung auf die Management-Station nur vertrauenswürdige Management-Stationen auf die Management Unit bzw. die Server Units des SE Servers 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).
- Traps
  Verwenden Sie SNMPv3 bei der Konfiguration von Trap-Empfängern, sofern möglich.

8 Sicherheit des Basis-Systems

Die Beschreibung gliedert sich in die folgenden Abschnitte:

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 Administrationstätigkeiten 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) 15.

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 Passworteigenschaften 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.

Die Basis-Systeme der SE Server werden von Fujitsu regelmäßig auf potentiell sicherheitsrelevante Schwachstellen untersucht. Einbezogen werden dabei insbesondere die vom Fujitsu PSIRT (Product Security Incident Response Team) publizierten Security Advisories und Notices und die Ergebnisse von Security Scans. Die potentiellen Schwachstellen werden unter Berücksichtigung der Härtung und der Einsatzszenarien der SE Appliances bewertet und unter Einbeziehung ihres Gefahrenpotentials bei Bedarf im Rahmen des Updateprozesses für die SE Systeme behoben.

Eine SE-Infrastruktur ist grundsätzlich immer entsprechend den vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegebenen Regeln IT-Grundschutz-zertifizierbar und kann deshalb auch in Umgebungen, die KRITIS-konform betrieben werden müssen (Kritische Infrastrukturen), eingefügt werden.

- Die Systemkomponenten sind bei Lieferung weitestgehend so vorkonfiguriert bzw. können im Rahmen eines tatsächlichen Aufbaus einer SE-Infrastruktur so konfiguriert werden, dass die technischen Anforderungen, die sich aus den relevanten System-Bausteinen des IT-Grundschutz-Kompendiums ergeben, erfüllt werden.
- Eine SE-Infrastruktur unterstützt mit ihren Eigenschaften damit auch grundsätzlich die Umsetzung von Anforderungen, die sich aus relevanten Prozess-Bausteinen des IT-Grundschutz-Kompendiums ergeben.
- Die interne Netzwerk-Architektur einer SE-Infrastruktur enthält allerdings selbst keine P-A-P-Struktur (Paketfilter – Application Layer Gateway – Paketfilter) und stellt kein DMZ-Konzept (Demilitarisierte Zone) bereit.
  - Eine SE-Infrastruktur stellt bewusst kein „Datacenter-in-a-Box“-Konzept dar, fügt sich jedoch nahtlos in BSI-IT-Grundschutz-konforme Rechenzentrumsnetzwerk-Architekturen ein.
  - In der Grundkonfiguration präsentiert sich eine SE-Infrastruktur dem Rechenzentrumsnetzwerk gegenüber als einfacher „Compute-Node“.
  - Optional kann eine SE-Infrastruktur aber auch mehrere virtuelle Netzwerksegmente mit Hilfe des internen Netzwerks im Rahmen des Rechenzentrumsnetzwerks realisieren. Die Net Unit repräsentiert dabei dann einen „Top-of-Rack-Switch“.

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 15 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

  Das Zertifikat muss dem X.509-Standard mit PEM-Encoding entsprechen und die Zertifikatdatei muss das Suffix . key besitzen.

  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.

Die nachfolgend prinzipiell beschriebenen Vorgehensweisen beruhen auf dem Browser Firefox und laufen abhängig vom eingesetzten Browser und der Version unterschiedlich ab. Einzelheiten zu speziellen Vorgehensweisen finden Sie in der Online-Hilfe Ihres Browsers.

CA-Zertifikat herunterladen und im Browser installieren

Um den Zertifikatfehler in Zukunft zu vermeiden, können Sie das aktuelle CA-Zertifikat der Management Unit (ggf. das kundeneigene CA-Zertifikat) herunterladen und im Browser installieren.

> **i** In einer SE-Server-Konfiguration mit mehreren MUs müssen Sie für jede MU dieselben Aktionen durchführen!

> Wählen Sie *Berechtigungen -> Zertifikate ->* [<*mu-name*> (MU)], Registerkarte *Zertifikate*. Die Tabelle zeigt das aktuelle Zertifikat der MU an.

> Klicken Sie in der Zeile *Ausgestellt durch (CN)* das Icon *CA-Zertifikat herunterladen*.

Das Kommando `sslCertCA` dient zum Anzeigen, Kopieren und Ausgeben des aktuellen CA-Zertifikats der MU.

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

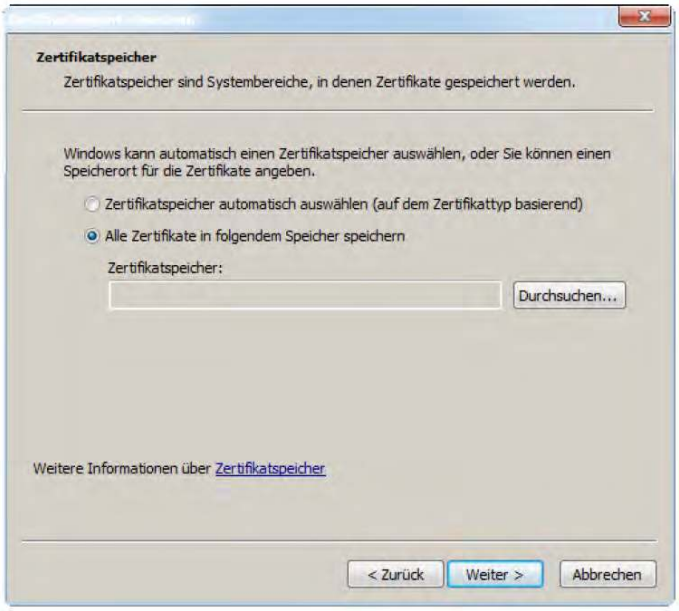
> Öffnen Sie die Zertifikatdatei (Standardname **<*mu-name*>-ca.crt**) und beantworten Sie die Sicherheitswarnung, die „*Unbekannter Herausgeber*“ anzeigt, mit *Öffnen*. Es werden die Informationen des Zertifikats angezeigt:

> Wählen Sie *Zertifikat installieren...*.

Der Zertifikatsimport-Assistent des Browsers führt Sie schrittweise durch die Installation des Zertifikats.

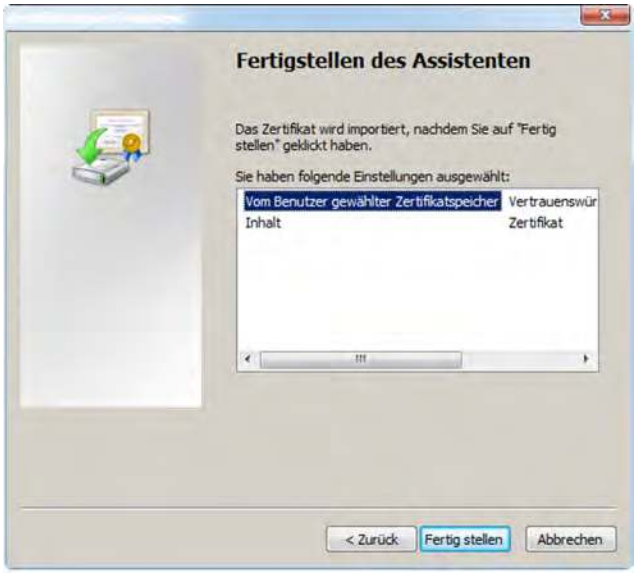
> Klicken Sie *Weiter*.

> Wählen Sie die Option *Alle Zertifikate in folgendem Speicher speichern* und klicken Sie *Durchsuchen...*:



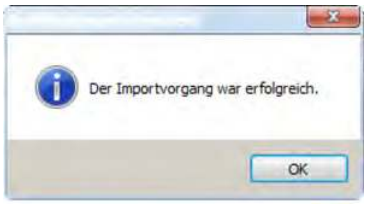
> Wählen Sie *Vertrauenswürdige Stammzertifizierungsstellen* als Zertifikatspeicher und klicken Sie *OK* und dann *Weiter*:

> Bestätigen Sie die Rückfrage, die die von Ihnen getroffene Auswahl noch einmal anzeigt, mit einem Klick auf *Fertig stellen*.



> Bestätigen Sie die anschließende Sicherheitswarnung, die den Zertifikatnamen und den „Fingerabdruck“ anzeigt, mit *Ja*. Damit wird das Zertifikat installiert.

> Beenden Sie nach erfolgreichem Import den Zertifikatsimport-Assistent mit *OK*:



Zertifikatfehler temporär akzeptieren

> 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 Domänennamen (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.

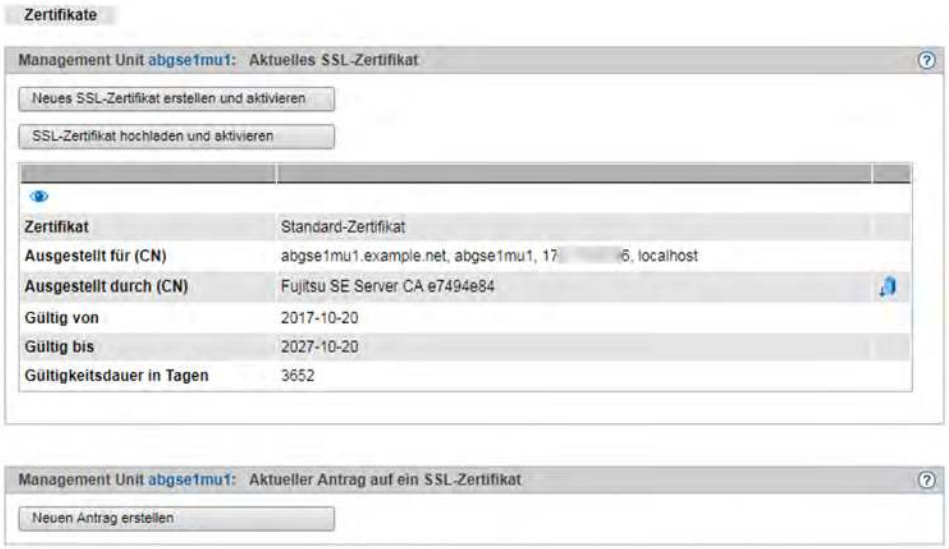
Wenn Sie den SE Manager an der lokalen Konsole aufrufen, müssen Sie das Standard-Zertifikat ebenfalls bestätigen oder importieren, da der am Desktop der lokalen Konsole eingesetzte Browser das Zertifikat ebenfalls nicht kennt.
Sie erhalten den Zugriff auf den SE Manager des jeweiligen Systems erst, wenn 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* -> *Zertifikate* -> [<*mu-name*> (MU)], Registerkarte *Zertifikate*.

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



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.

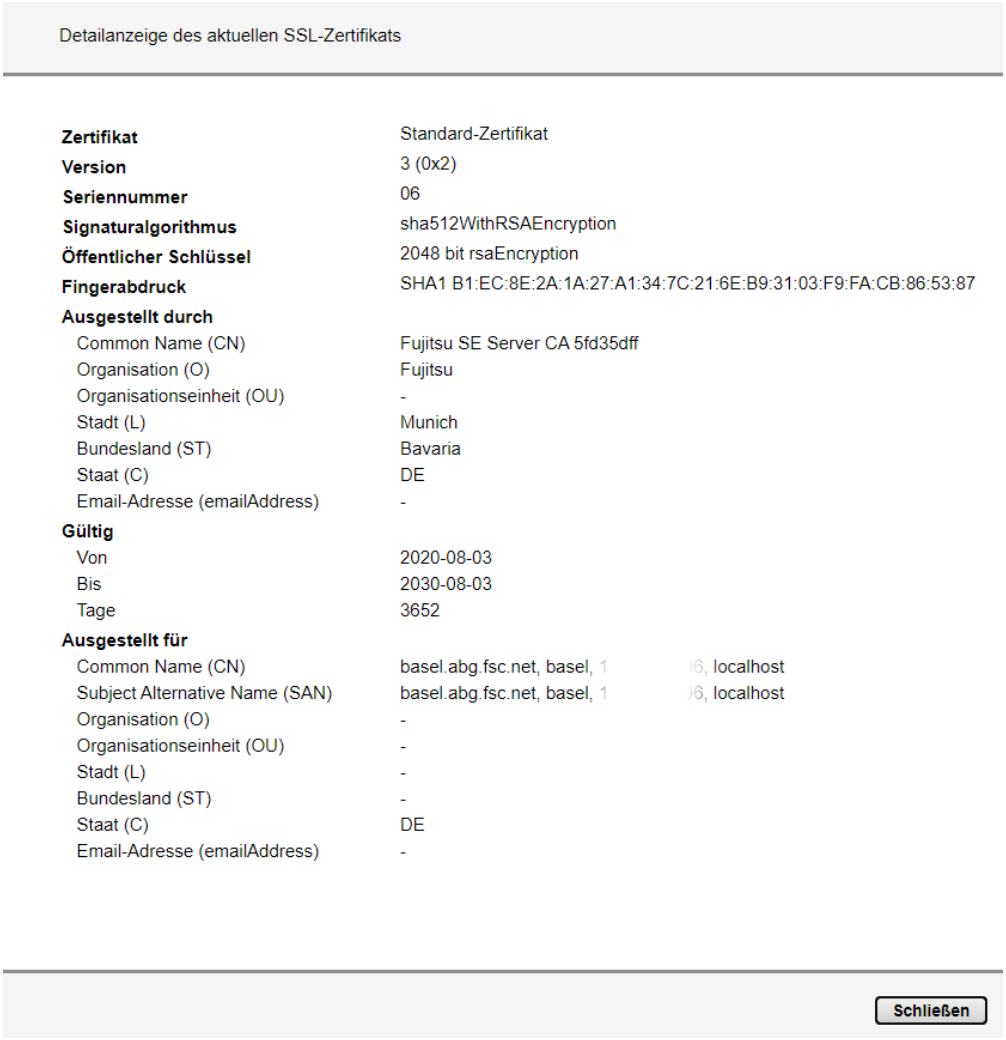
Informationen zu den Attributen *Gültig von*, *Gültig bis*, *Gültigkeitsdauer in Tagen* sowie *Email-Adresse (email Address)* finden Sie in der Online-Hilfe.

Zertifikat detailliert anzeigen

> Wählen Sie *Berechtigungen* -> *Zertifikate* -> [<*mu-name*> (MU)], Registerkarte *Zertifikate*.

> Klicken Sie das Icon *Details* ( ).

In einem Dialog werden alle Eigenschaften des Zertifikats angezeigt.


Detailanzeige des aktuellen SSL-Zertifikats
Zertifikat
Standard-Zertifikat
Version
3 (0x2)
Seriennummer
06
Signaturalgorithmus
sha512WithRSAEncryption
Öffentlicher Schlüssel
2048 bit rsaEncryption
Fingerabdruck
SHA1 B1:EC:8E:2A:1A:27:A1:34:7C:21:6E:B9:31:03:F9:FA:CB:86:53:87
Ausgestellt durch
Common Name (CN)
Fujitsu SE Server CA 5fd35dff
Organisation (O)
Fujitsu
Organisationseinheit (OU)
-
Stadt (L)
Munich
Bundesland (ST)
Bavaria
Staat (C)
DE
Email-Adresse (emailAddress)
-
Gültig
Von
2020-08-03
Bis
2030-08-03
Tage
3652
Ausgestellt für
Common Name (CN)
basel.abg.fsc.net, basel, 1 6, localhost
Subject Alternative Name (SAN)
basel.abg.fsc.net, basel, 1 6, localhost
Organisation (O)
-
Organisationseinheit (OU)
-
Stadt (L)
-
Bundesland (ST)
-
Staat (C)
DE
Email-Adresse (emailAddress)
-
Schließen

8.3.3 Neues selbstsigniertes Zertifikat erzeugen und aktivieren

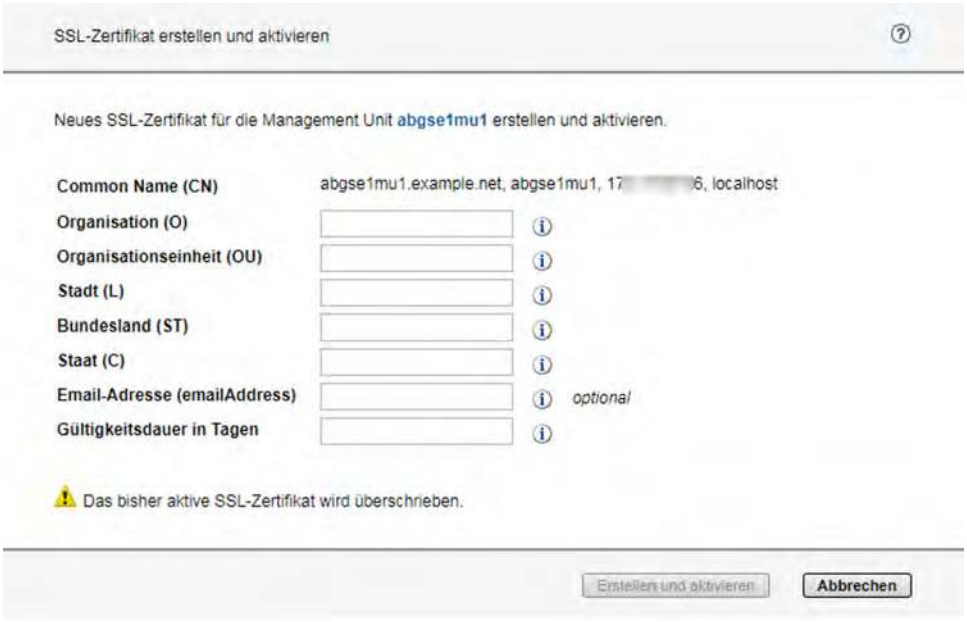
Das vorinstallierte Standardzertifikat beinhaltet Daten, die selbstverständlich nicht kundenspezifisch sind.

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 -> Zertifikate ->* [<*mu-name*> (MU)], Registerkarte *Zertifikate*.

> Klicken Sie *Neues SSL-Zertifikat erstellen und aktivieren* oberhalb der Tabelle.

Es wird ein Dialog geöffnet:



Tragen Sie die wesentlichen Daten des Zertifikats ein. Der Wert für den *Common Name (CN)* ist fest vorgegeben und beinhaltet den vollqualifizierten Domänennamen (FQDN) des Systems. Informationen zu den Attributen *Organisation (O)*, *Organisationseinheit (OU)*, *Stadt (L)*, *Bundesland (ST)*, *Staat (C)*, *Email-Adresse (emailAddress), 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").

8.3.4 Antrag auf ein SSL-Zertifikat stellen

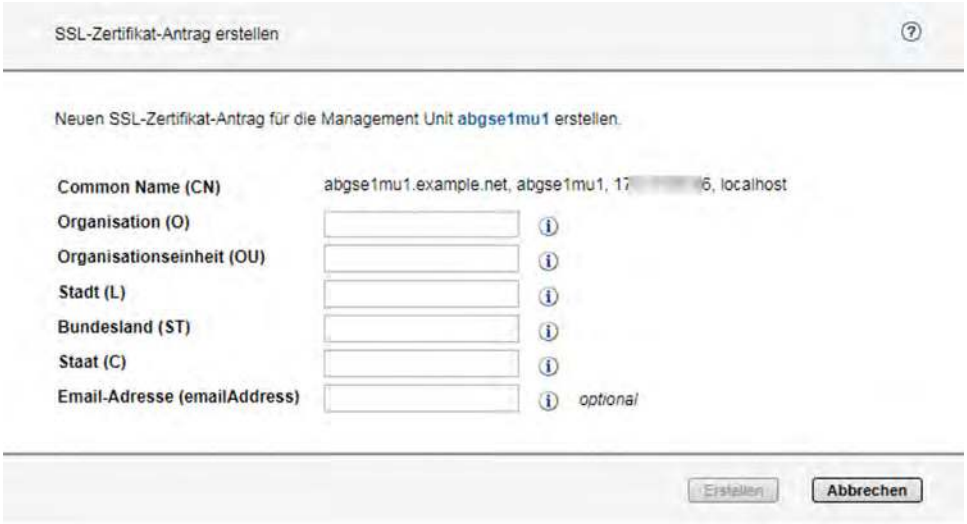
Wenn Sie ein systemspezifisches Zertifikat, das von einer CA (Certification Authority) signiert wurde, einsetzen wollen, unterstützt Sie der SE Manager beim Erstellen des Antrags:

> Wählen Sie *Berechtigungen -> Zertifikate ->* [*<mu-name>* (MU)], 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 Zertifikats ein. Der Wert für den *Common Name (CN)* ist fest vorgegeben und beinhaltet den vollqualifizierten Domänennamen (FQDN) des Systems. Informationen zu den Attributen *Organisation (O)*, *Organisationseinheit (OU)*, *Stadt (L)*, *Bundesland (ST)*, *Staat (C)*, *Email-Adresse (emailAddress)* 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 Icon *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" und Abschnitt „Standard-Zertifikat einsetzen".

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

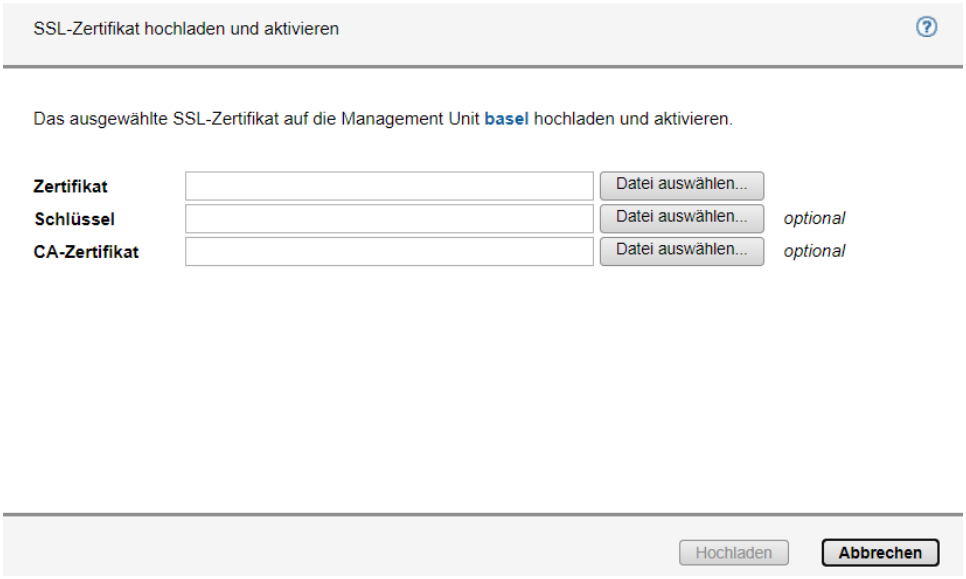
Statt eines im System erzeugten selbstsignierten Zertifikats (Standardzertifikat oder benutzerdefiniertes Zertifikat) können Sie für den Zugang zum SE Manager des Systems ein eigenes Zertifikat verwenden.

Für das Zertifikat wurde ein Certificate Signing Request im System erzeugt (siehe Abschnitt „Antrag auf ein SSL-Zertifikat stellen") 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 -> Zertifikate ->* [<*mu-name*> (MU)], Registerkarte *Zertifikate*.

> Klicken Sie *SSL-Zertifikat hochladen und aktivieren*.

Ein Dialog wird geöffnet.



Zertifikat

> Klicken Sie *Datei auswählen...* um eine Zertifikatsdatei 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 *Datei auswählen...* um eine Schlüsseldatei auf Ihrem Administrations-PC auszuwählen.

CA-Zertifikat

Wählen Sie, falls nötig, eine CA-Zertifikatsdatei aus.

> Klicken Sie *Datei auswählen...* um eine CA-Zertifikatsdatei 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.

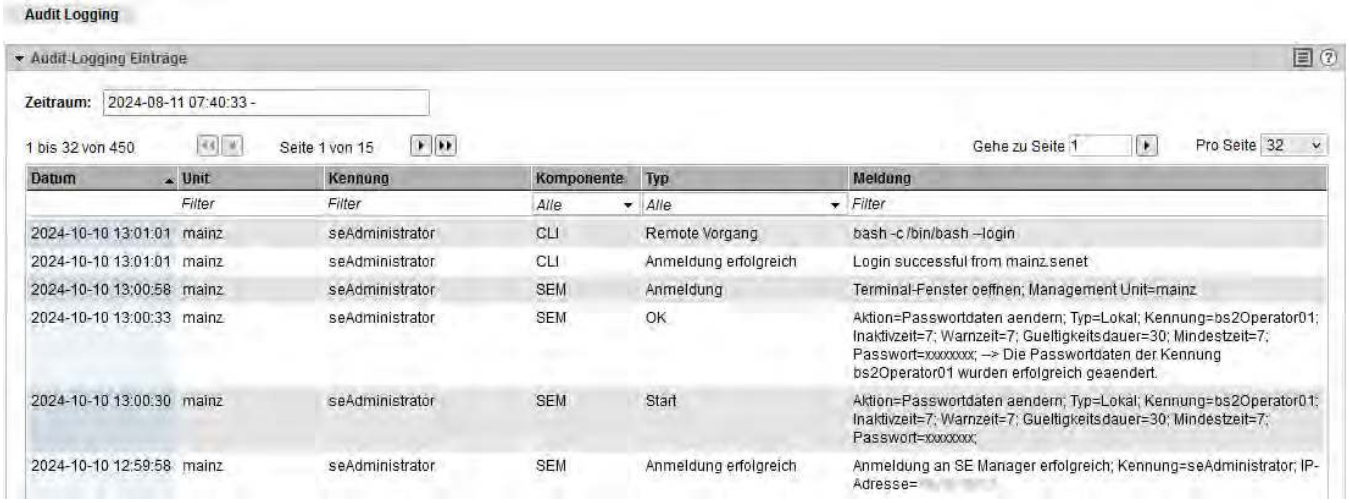
Hinweise

- 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").

9 Aktionen protokollieren (Audit Logging)

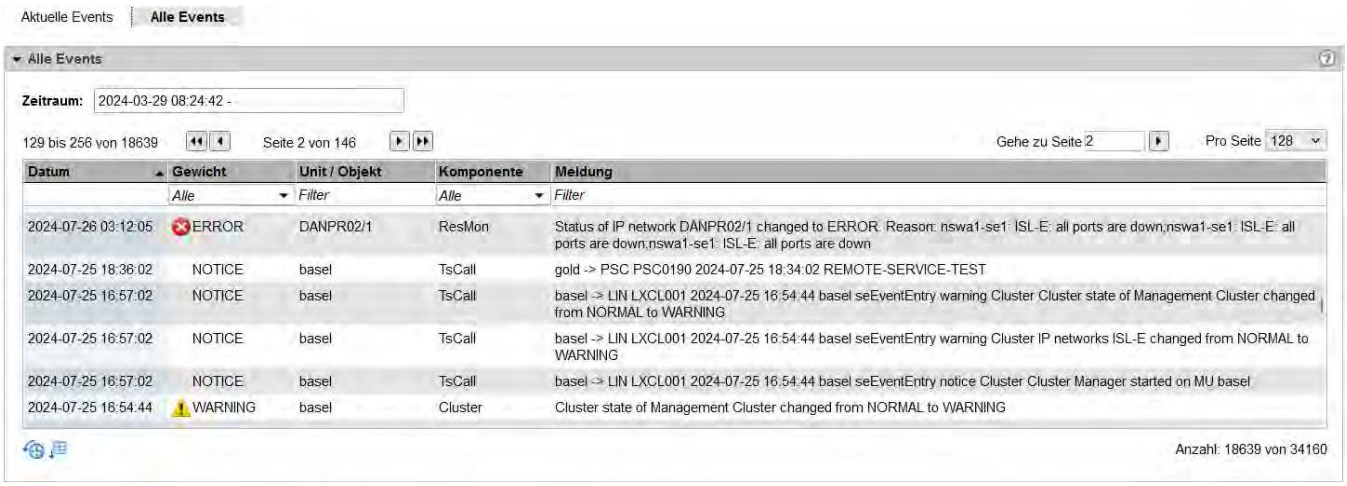
Die interne Funktion Audit Logging protokolliert alle Aktionen, die an einer Unit (MU, SU, HNC) der SE Server-Konfiguration über den SE Manager, über ein Add-on oder über ein CLI-Kommando ausgeführt werden und die eine Konfigurationsänderung oder Zustandsänderung im System bewirken. An- und Abmeldungen werden ebenfalls protokolliert. Reine Anzeigefunktionen werden nicht protokolliert.

Anhand der Protokolleinträge kann ein Administrator oder Security Administrator in der Registerkarte *Audit Logging* unter *Logging -> Audit Logging* jederzeit nachvollziehen, wer wann welche Aktion mit welchem Ergebnis durchgeführt hat. Damit sind insbesondere alle sicherheitsrelevanten Aktionen im System eindeutig einem „Verursacher“ zuordenbar.



10 Event Logging und Alarm Management

Die Funktion *Event Logging* protokolliert alle Ereignisse, die auftreten, und zeigt die protokollierten Ereignisse unter *Logging -> Event Logging* in der Registerkarte *Alle Events* an. Zur besseren Übersicht werden die aktuellen Ereignisse, die Sie noch nicht zur Kenntnis genommen haben, zusätzlich in der Registerkarte *Aktuelle Events* angezeigt. Eine Zusammenfassung dieser Registerkarte zeigt das Dashboard in der Kachel *Events* an.

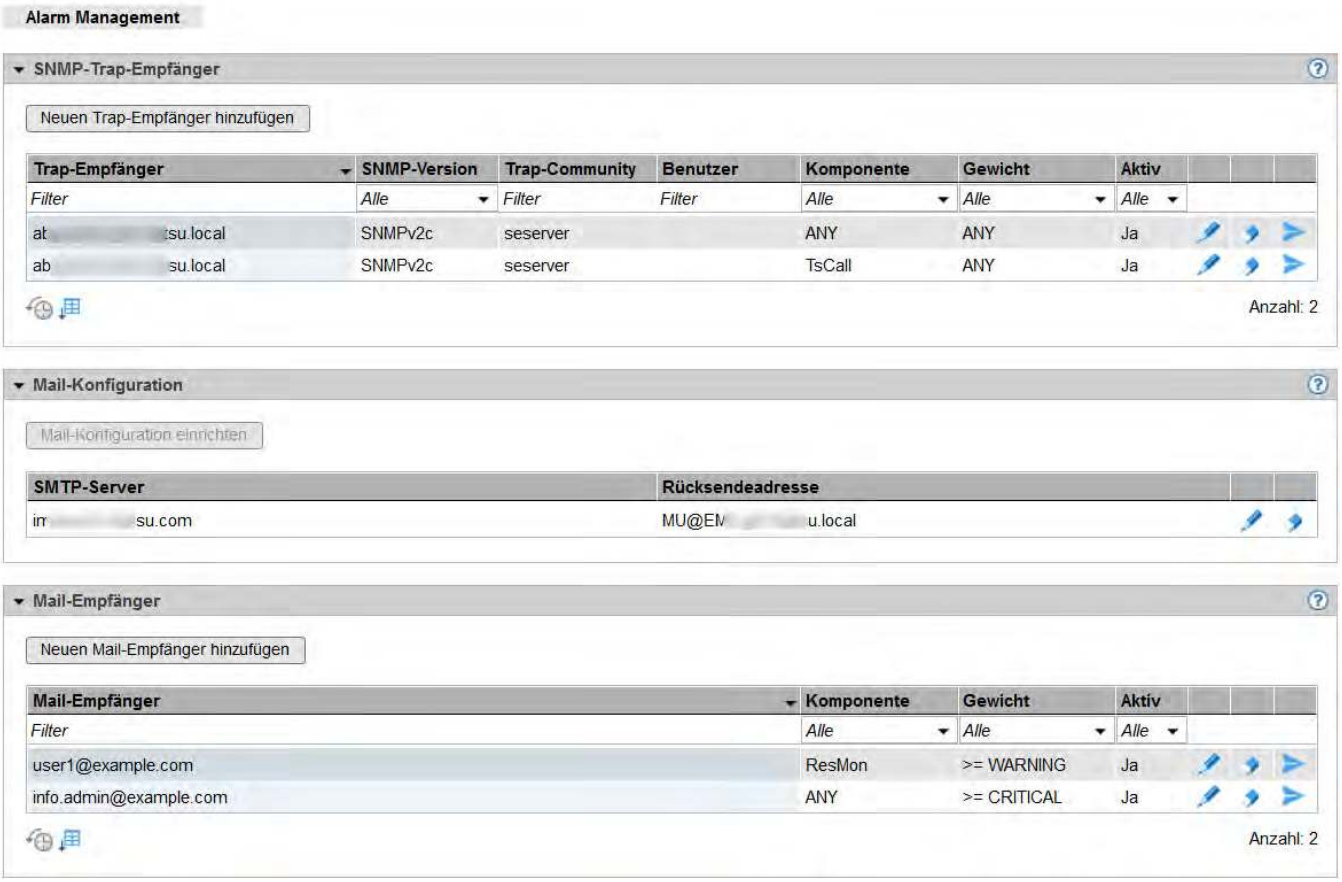


> Wenn Sie über die Schaltfläche *Aktuelle Events zur Kenntnis nehmen* die bisher angezeigten Ereignisse aus der Tabelle *Aktuelle Events* entfernen, zeigt auch die Kachel *Events* entsprechend weniger Ereignisse an. Die zur Kenntnis genommenen Ereignisse werden ausschließlich in der Registerkarte *Alle Events* angezeigt.

> Die aktuell möglichen Events mit Meldungen sind unter *Allgemeine Informationen* in der Online-Hilfe des SE Managers aufgelistet.

Damit Sie wichtige Ereignisse wie Fehlersituationen auch in großen SE Server-Konfigurationen schneller erkennen und ggf. erforderliche Maßnahmen ebenfalls schnell einleiten können, bietet das *Alarm Management* die Möglichkeit zur Konfiguration von automatischen Benachrichtigungen per SNMP Trap oder per Mail für Events mit bestimmten Meldungsgewichten und/oder von bestimmten Komponenten.

Die aktuelle Alarm Management Konfiguration zeigt der SE Manager im Menü *Logging -> Alarm Management* an.



Sicherheitsrelevante Aktionen

Da bei einer Benachrichtigung ggf. sensible Daten nach außen verschickt werden, sollten Sie bei der Konfiguration eines neuen SNMP-Trap- bzw. Mail-Empfängers die angegebene Adresse sorgfältig prüfen. Versenden Sie über die Funktion *Testen* einen Test-Trap bzw. eine Test-Mail an den neuen Empfänger, um zu prüfen, ob Benachrichtigungen bei dem gewünschten Empfänger ankommen.

11 Literatur

Die folgenden BS2000 Handbücher finden Sie im Internet auf dem Manualserver mit der BS2000 Dokumentation unter https://bs2manuals.ts.fujitsu.com.

Weitere Handbücher, beispielsweise Beschreibungen zu den PRIMERGY und PRIMEQUEST Servern von Fujitsu , sind auf den allgemeinen Fujitsu Support Seiten unter https://support.ts.fujitsu.com/ zu finden.

[1] **Fujitsu Server BS2000 SE Serie**
Kurzanleitung
Benutzerhandbuch

[2] **Fujitsu Server BS2000 SE Serie**
Bedienen und Verwalten
Benutzerhandbuch

[3] **Fujitsu Server BS2000 SE Serie**
Basis-Betriebsanleitung

[4] **Fujitsu Server BS2000 SE Serie**
Server Unit /390
Betriebsanleitung

[5] **Fujitsu Server BS2000 SE Serie**
Server Unit x86
Betriebsanleitung

[6] **Fujitsu Server BS2000 SE Serie**
Additive Komponenten
Betriebsanleitung

[7] **Fujitsu Server BS2000 SE Serie**
Cluster-Lösungen für SE Server
Whitepaper

[8] **BS2000 OSD DX**
Einführung in die Systembetreuung
Benutzerhandbuch

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

[10] **SECOS**
Security Control System - Beweissicherung
Benutzerhandbuch