Deutsch

FUJITSU Software BS2000

interNet Services V3.4B

Administratorhandbuch

Ausgabe Juni 2017

Kritik… Anregungen… Korrekturen…

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

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

Zertifizierte Dokumentation nach DIN EN ISO 9001:2008

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

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

Copyright und Handelsmarken

Inhalt

1 Einleitung

Das Produkt interNet Services ergänzt die TCP/IP-Funktionalität von openNet Server um folgende Standards:

- DNS Resolver und Server
- NTP Client und Server
- FTP Client und Server
- TELNET Client und Server
- OpenSSH
- Mail-Sender im BS2000
- Mail-Reader im BS2000
- Mail-Server in POSIX

1.1 Zielgruppe des Handbuchs

Das vorliegende Administratorhandbuch wendet sich an BS2000-Systembetreuer, die interNet Services auf BS2000 installieren und betreiben wollen. Kenntnisse des Betriebssystems BS2000 OSD/BC sowie der TCP/IP-Grundbegriffe werden vorausgesetzt. Neben dem hier vorliegenden Administratorhandbuch gibt es zu interNet Services ein Benutzerhandbuch, das dem Systembetreuer zusätzlich zum Administratorhandbuch zur Verfügung stehen sollte.

1.2 Wegweiser durch das Handbuch

Das vorliegende Handbuch ist folgendermaßen strukturiert:

- Kapitel 2: Internet Services ohne FTP, TELNET und Mail installieren

  Dieses Kapitel beschreibt die Installation der Services DNS, NAMED, OpenSSH und NTP als POSIX-Programmpakete mit dem POSIX-Installationsprogramm.

- Kapitel 3: FTP und TELNET installieren

  Dieses Kapitel beschreibt die Installation der Services FTP und TELNET über SDF-Kommando.

- Kapitel 4: Konfiguration und Betrieb von FTP

  In diesem Kapitel werden die TLS/SSL-Unterstützung im FTP-Server sowie die Konfiguration via Installationskommando bzw. mithilfe einer Option-Datei beschrieben. Zusätzlich sind in diesem Kapitel das Starten und Beenden sowie der Betrieb und die Server Exits des FTP-Servers beschrieben.

- Kapitel 5: Konfiguration und Betrieb von TELNET

  In diesem Kapitel werden die TLS/SSL-Unterstützung im TELNET-Server sowie die Konfiguration via Installationskommando bzw. mithilfe einer Option-Datei beschrieben. Zusätzlich sind in diesem Kapitel das Starten und Beenden sowie der Betrieb und die Server Exits des TELNET-Servers beschrieben.

- Kapitel 6: Generierung von Zufallszahlen

  Dieses Kapitel beschreibt die Generierung von Zufallszahlen im BS2000 und POSIX.

- Kapitel 7 - 11

  In diesen Kapiteln werden die einzelnen Komponenten der interNet Services ausführlich vorgestellt. Die Funktionalität der Komponenten, Konfiguration und Hinweise zum Betrieb und zu Diagnosemöglichkeiten sind die wichtigsten Themen dieser Kapitel.

- Kapitel 12: Aufbau einer Verschlüsselungsverfahren-Vorzugslisten-Spezifikation

  Dieses Kapitel beschreibt zentral den Aufbau der Chiffre-Mnemonics zur Erstellung von Vorzugslisten-Spezifikationen.

1.3 Lizenzrechtliche Bestimmungen

Im Folgenden sind die lizenzrechtlichen Bestimmungen zum OpenSSL-Paket und zum TLS-FTP-Patch von Peter 'Luna' Runestig abgedruckt.

Die deutsche Fassung des Lizenztextes dient dem Leser nur als Hilfestellung zum leichteren Verständnis. Die deutsche Übersetzung ist nicht rechtsverbindlich. In Zweifelsfällen ist ausschließlich der englische Originaltext maßgebend.

Deutsche Fassung des Lizenztextes (Übersetzung)

```
OpenSSL-Lizenz
==============

Copyright (c) 1998-2000 The OpenSSL Project. Alle Rechte vorbehalten.
Der Weitervertrieb und die Verwendung in Quell- und binären Formularen ist -
mit oder ohne Veränderungen - grundsätzlich zulässig, sofern die folgenden
Bedingungen eingehalten werden:
1. Weitervertriebene Quellcodes müssen den oben aufgeführten Copyright-
Hinweis, die hier genannten Bedingungen und die nachstehende
Ausschlussklausel enthalten.
2. Im Fall des Weitervertriebs in binärer Form müssen der oben genannte
Copyright-Hinweis, die hier aufgeführten Bedingungen und die nachstehende
Ausschlussklausel und/oder andere in der Bereitstellung enthaltene
Materialien genannt werden.
3. Alle Werbematerialien, in denen Funktionen der Software erwähnt oder
verwendet werden, müssen den folgenden Hinweis enthalten:
"Dieses Produkt enthält Software, die vom OpenSSL Project für die Verwendung
mit dem OpenSSL Toolkit entwickelt wurde (http://www.openssl.org/)."
4. Die Bezeichnungen "OpenSSL Toolkit" und "OpenSSL Project" dürfen ohne
vorherige schriftliche Genehmigung nicht zur Produktkennzeichnung oder zu
sonstigen Werbezwecken verwendet werden. Schriftliche Genehmigungen erhalten
Sie unter: openssl-core@openssl.org.
5. Auch für von dieser Software abgeleitete Produkte darf der Name "OpenSSL"
weder als Produktbezeichnung noch als Bestandteil der Produktbezeichnung ohne
vorherige schriftliche Genehmigung des OpenSSL Projects verwendet werden.
6. Der Weitervertrieb darf nur unter folgendem Hinweis erfolgen:
"Diese Produkt enthält Software, die vom OpenSSL Project für die Verwendung
mit dem OpenSSL Toolkit entwickelt wurde (http://www.openssl.org/)."


DAS OPENSSL PROJECT STELLT DIESE SOFTWARE "OHNE MÄNGELGEWÄHR" BEREIT. DIESER
GEWÄHRLEISTUNGSAUSSCHLUSS BEZIEHT SICH AUF VERTRAGLICHE ODER GESETZLICHE
GARANTIEN, EINSCHLIESSLICH VON, ABER NICHT BESCHRÄNKT AUF, GESETZLICHE
GARANTIEN BEZÜGLICH HANDELSÜBLICHER QUALITÄT UND EIGNUNG FÜR EINEN BESTIMMTEN
ZWECK. IN KEINEM FALLE KÖNNEN OPENSSL PROJECT ODER SEINE MITARBEITER FÜR
JEGLICHE DIREKTEN, INDIREKTEN, ZUFÄLLIGEN, SPEZIELLEN, EXEMPLARISCHEN SCHÄDEN
```

ODER FOLGESCHÄDEN (EINSCHLIESSLICH VON, JEDOCH NICHT BESCHRÄNKT AUF, BESCHAFFUNG VON ERSATZGÜTERN ODER -DIENSTLEISTUNGEN, NUTZUNGSAUSFÄLLEN, DATENVERLUSTEN ODER ENTGANGENEN GEWINNEN ODER BETRIEBSUNTERBRECHUNGEN) GLEICH WELCHEN URSPRUNGS HAFTBAR GEMACHT WERDEN. JEGLICHE HAFTUNGSANSPRÜCHE AUF VERTRAGSBASIS, IM HINBLICK AUF DELIKTSHAFTUNG ODER GEFÄHRDUNGSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT UND SONSTIGES), DIE AUS DER VERWENDUNG DIESER SOFTWARE ENTSTEHEN, WERDEN AUCH DANN AUSGESCHLOSSEN, WENN AUF DIE MÖGLICHKEIT DIESER SCHÄDEN HINGEWIESEN WURDE.

Das Produkt enthält kryptographische Software, die von Eric Young (eay@cryptsoft.com) entwickelt wurde. Das Produkt enthält Software, die von Tim Hudson (tjh@cryptsoft.com) entwickelt wurde.

SSLeay-Original-Lizenz
==========
Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com). Alle Rechte vorbehalten.
Bei dem vorliegenden Paket handelt es sich um eine SSL-Implementierung, die von Eric Young (eay@cryptsoft.com) entwickelt wurde. Die Implementierung wurde so erstellt, dass sie mit dem SSL von Netscape kompatibel ist.
Die Bibliothek steht zur kostenlosen gewerblichen und nichtgewerblichen Nutzung zur Verfügung, sofern die nachstehenden Bedingungen erfüllt werden. Die nachstehenden Bedingungen gelten außer für den SSL-Code für alle in der Bereitstellung enthaltenen Codes, beispielsweise RC4, RSA, lhash, DES usw. Für die in der Bereitstellung enthaltene SSL-Dokumentation gelten dieselben Copyrights, wobei als Eigentümer in diesem Fall Tim Hudson (tjh@cryptsoft.com) zu nennen ist.
Das Copyright verbleibt bei Eric Young, weshalb die Copyright-Hinweise innerhalb des Codes nicht entfernt werden dürfen.
Wenn das Paket innerhalb eines Produkts verwendet wird, ist Eric Young als Urheber der verwendeten Teile der Bibliothek zu erwähnen.
Dies kann in Form einer Textmeldung beim Programmstart oder in der dem Produktpaket beiligenden Dokumentation (online oder in Druckform) erfolgen.
Der Weitervertrieb und die Verwendung in Quell- und binären Formularen ist - mit oder ohne Veränderungen - grundsätzlich zulässig, sofern die folgenden Bedingungen eingehalten werden:
1. Weitervertriebene Quellcodes müssen den Copyright-Hinweis, die hier genannten Bedingungen und die nachstehende Ausschlussklausel enthalten.
2. Im Fall des Weitervertriebs in binärer Form müssen der oben genannte Copyright-Hinweis, die hier aufgeführten Bedingungen und die nachstehende Ausschlussklausel und/oder andere in der Bereitstellung enthaltene Materialien genannt werden.
3. Alle Werbematerialien, in denen Funktionen der Software erwähnt oder verwendet werden, müssen den folgenden Hinweis enthalten:
"Das Produkt enthält kryptographische Software, die von Eric Young (eay@cryptsoft.com) entwickelt wurde."

Das Wort "kryptographisch" muss nicht erwähnt werden, wenn die verwendeten Routinen aus der Bibliothek nicht mit kryptographischem Bezug verwendet werden.
4. Wenn Sie Windows-spezifische Codes (oder Ableitungen davon) aus dem Apps-Verzeichnis (Anwendungscode) verwenden, ist der folgende Hinweis erforderlich:
"Das Produkt enthält Software, die von Tim Hudson (tjh@cryptsoft.com) entwickelt wurde."
DIESE SOFTWARE WIRD VON ERIC YOUNG "OHNE MÄNGELGEWÄHR" BEREITGESTELLT. DIESER GEWÄHRLEISTUNGSAUSSCHLUSS BEZIEHT SICH AUF VERTRAGLICHE ODER GESETZLICHE GARANTIEN, EINSCHLIESSLICH VON, ABER NICHT BESCHRÄNKT AUF, GESETZLICHE GARANTIEN BEZÜGLICH HANDELSÜBLICHER QUALITÄT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK. IN KEINEM FALLE KÖNNEN DER AUTOR ODER MITARBEITER FÜR JEGLICHE DIREKTEN, INDIREKTEN, ZUFÄLLIGEN, SPEZIELLEN, EXEMPLARISCHEN SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH VON, JEDOCH NICHT BESCHRÄNKT AUF, BESCHAFFUNG VON ERSATZGÜTERN ODER -DIENSTLEISTUNGEN, NUTZUNGSAUSFÄLLEN, DATENVERLUSTEN ODER ENTGANGENEN GEWINNEN ODER BETRIEBSUNTERBRECHUNGEN) GLEICH WELCHEN URSPRUNGS HAFTBAR GEMACHT WERDEN. JEGLICHE HAFTUNGSANSPRÜCHE AUF VERTRAGSBASIS, IM HINBLICK AUF DELIKTSHAFTUNG ODER GEFÄHRDUNGSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT UND SONSTIGES), DIE AUS DER VERWENDUNG DIESER SOFTWARE ENTSTEHEN, WERDEN AUCH DANN AUSGESCHLOSSEN, WENN AUF DIE MÖGLICHKEIT DIESER SCHÄDEN HINGEWIESEN WURDE.

Die Lizenz und die Bedingungen für den Weitervertrieb von allen öffentlich erhältlichen Versionen oder Ableitungen dieses Codes können nicht verändert werden, d.h., der Code kann nicht einfach kopiert und in eine andere Weitervertriebslizenz integriert werden [einschließlich der GNU Public Licence.]

Englischer Lizenztext (Originaltext)

```
LICENSE ISSUES
==============

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of
the OpenSSL License and the original SSLeay license apply to the toolkit.
See below for the actual license texts. Actually both licenses are BSDstyle
Open Source licenses. In case of any license issues related to OpenSSL
please contact openssl-core@openssl.org.

OpenSSL License
---------------

/* ====================================================================
 * Copyright (c) 1998-2003 The OpenSSL Project.  All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in
 *    the documentation and/or other materials provided with the
 *    distribution.
 *
 * 3. All advertising materials mentioning features or use of this
 *    software must display the following acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
 *    endorse or promote products derived from this software without
 *    prior written permission. For written permission, please contact
 *    openssl-core@openssl.org.
 *
 * 5. Products derived from this software may not be called "OpenSSL"
 *    nor may "OpenSSL" appear in their names without prior written
 *    permission of the OpenSSL Project.
 *
 * 6. Redistributions of any form whatsoever must retain the following
 *    acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
```

```
 * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
 * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
 * PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
 * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
 * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
 * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
 * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
 * OF THE POSSIBILITY OF SUCH DAMAGE.
 * ====================================================================
 *
 * This product includes cryptographic software written by Eric Young
 * (eay@cryptsoft.com).  This product includes software written by Tim
 * Hudson (tjh@cryptsoft.com).
 *
 */

 Original SSLeay License
 -----------------------

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long as
 * the following conditions are aheared to.  The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA,
 * lhash, DES, etc., code; not just the SSL code.  The SSL documentation
 * included with this distribution is covered by the same copyright terms
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in
 * the code are not to be removed.
 * If this package is used in a product, Eric Young should be given attribution
 * as the author of the parts of the library used.
```

```
* This can be in the form of a textual message at program startup or
* in documentation (online or textual) provided with the package.
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the copyright
*    notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in the
*    documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
*    must display the following acknowledgement:
*    "This product includes cryptographic software written by
*     Eric Young (eay@cryptsoft.com)"
*    The word 'cryptographic' can be left out if the rouines from the library
*    being used are not cryptographic related :-).
* 4. If you include any Windows specific code (or a derivative thereof) from
*    the apps directory (application code) you must include an acknowledgement:
*    "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
*
* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*
* The licence and distribution terms for any publically available version or
* derivative of this code cannot be changed.  i.e. this code cannot simply be
* copied and put under another distribution licence
* [including the GNU Public Licence.]
*/
```

```
/*
 * Copyright (c) 1999 - 2002 Peter 'Luna' Runestig <peter@runestig.com>
 * All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without modifi-
 * cation, are permitted provided that the following conditions are met:
 *
 *   o  Redistributions of source code must retain the above copyright notice,
 *      this list of conditions and the following disclaimer.
 *
 *   o  Redistributions in binary form must reproduce the above copyright no-
 *      tice, this list of conditions and the following disclaimer in the do-
 *      cumentation and/or other materials provided with the distribution.
 *
 *   o  The names of the contributors may not be used to endorse or promote
 *      products derived from this software without specific prior written
 *      permission.
 *
 * THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
 * ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED
 * TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
 * PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LI-
 * ABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUEN-
 * TIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEV-
 * ER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABI-
 * LITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF
 * THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
*/
```

NTP-Lizenz
==========

```
********************************************************************************
*                                                                              *
* Copyright (c) University of Delaware 1992-2015                               *
*                                                                              *
* Permission to use, copy, modify, and distribute this software and            *
* its documentation for any purpose with or without fee is hereby              *
* granted, provided that the above copyright notice appears in all             *
* copies and that both the copyright notice and this permission                *
* notice appear in supporting documentation, and that the name                 *
* University of Delaware not be used in advertising or publicity               *
* pertaining to distribution of the software without specific,                 *
* written prior permission. The University of Delaware makes no                *
* representations about the suitability this software for any                   *
* purpose. It is provided "as is" without express or implied                   *
* warranty.                                                                    *
```

```
*                                                                      *
************************************************************************
Content starting in 2011 from Harlan Stenn, Danny Mayer, and Martin Burnicki
is:

************************************************************************
*                                                                      *
* Copyright (c) Network Time Foundation 2011-2015                      *
*                                                                      *
* All Rights Reserved                                                  *
*                                                                      *
* Redistribution and use in source and binary forms, with or without   *
* modification, are permitted provided that the following conditions   *
* are met:                                                             *
* 1. Redistributions of source code must retain the above copyright    *
*    notice, this list of conditions and the following disclaimer.     *
* 2. Redistributions in binary form must reproduce the above           *
*    copyright notice, this list of conditions and the following       *
*    disclaimer in the documentation and/or other materials provided   *
*    with the distribution.                                            *
*                                                                      *
* THIS SOFTWARE IS PROVIDED BY THE AUTHORS ``AS IS'' AND ANY EXPRESS   *
* OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED    *
* WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE   *
* ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHORS OR CONTRIBUTORS BE     *
* LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR  *
* CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT    *
* OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR   *
* BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF           *
* LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT            *
* (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE    *
* USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH     *
* DAMAGE.                                                              *
************************************************************************
```

1.4 Übersicht über die Dienste von interNet Services

interNet Services V3.4B setzt folgende Software voraus:

– BS2000/OSD ≥ V9.0A
– openNet Server ≥ V3.6

Die in interNet Services enthaltenen Komponenten belegen standardmäßig folgende Portnummern:

Port		**Protokoll**	**Erläuterung**
20	tcp	FTP	File Transfer Protocol [Default Data]
21	tcp	FTP	File Transfer Protocol [Control]
22	tcp	SSH	Secure Shell
23	tcp	TELNET	TELNET
25	tcp	SMTP	Simple Mail Transfer Protocol
53	tcp/udp	DNS	Domain Name Server
80	tcp	HTTP	World Wide Web HTTP
110	tcp	POP3	Post Office Protocol - Version 3
123	udp	NTP	Network Time Protocol
143	tcp	IMAP	Internet Message Access Protocol
443	tcp	HTTPS	HTTP over TLS (Transport Layer Security) / SSL (Secure Sockets Layer)
953	tcp/udp	DNS	rndc-Tool (NAMED)
1235	tcp/udp	DNS	Domain Name Resolver

1.5 Änderungen gegenüber der Vorgängerversion

Das folgende Änderungsprotokoll gibt einen Überblick über die Neuerungen in interNet Services V3.4B, die das vorliegende Handbuch betreffen.

Über Neuerungen, die das Handbuch „interNet Services Benutzerhandbuch“ betreffen, informiert Sie das zugehörige Änderungsprotokoll.

OpenSSH

- Die SSH Protokollversion 1 wird nicht mehr unterstützt.
- Neu unterstützt wird Elliptic Curve Cryptography (ECDSA, Ed25519).

SSL/TLS-Protokollversionen und Cipher-Suiten für FTP, TELNET, Mail-Sender und Mail-Reader

- Wegfall von SSLv2
- Erweiterung um TLSv1.1 und TLSv1.2.
- Neue Cipher-Suiten für die SSL/TLS-Cipher-Suiten

FTP

- Neue FTP-Option *-TVFS* zum (De)aktivieren von TVFS.
- Neue Kommandos in Unterereignis in *FTPCMD* durch die neuen FTP-Server-Kommandos MLSD und MLST.

Telnet

- Neuer Wert *optional* in der START-TLS-Option *-Z tls-required*.

Mail-Sender im BS2000

- Neue Optionen *maxQueueLifeTime*, *smtpReadMaxWaitTime*, *smtpRetryTimeBase* und *smtpRetryTimeMaxExp*, um die maximale Lebensdauer einer Mail und die Wartezeiten bei wiederholten Zustellversuchen zu steuern.
- Die Option *retryLimit* wird nicht mehr unterstützt. Sie wird ersetzt durch die Option *maxQueueLifeTime*.

Entfallene Funktionen

- Wegfall Krypto-Hardware
  Die Krypto-Hardware wird nicht mehr unterstützt. Dadurch entfallen die Optionen *tlsUseCryptoHardware* und *-Z UseCryptoHardware* sowie der Konfigurationsparameter *USE-CRYPTO-HARDWARE* im Kommando SET-FTP-TELNET-PARAMETERS.
- Der POSIX-*prngd*-Dämon wird nicht mehr ausgeliefert und daher nicht mehr beschrieben. Stattdessen können Zufallszahlen über den BS2000-PRNGD bezogen werden.

Geänderte Handbuchstruktur

- Der Aufbau der Chiffre-Mnemonics zur Erstellung von Vorzugslisten-Spezifikationen wird jetzt zentral im Kapitel „Spezifikation einer Vorzugsliste für Verschlüsselungsverfahren“ auf Seite 383 beschrieben.

1.6 Typographische Gestaltungsmittel

In diesem Handbuch werden folgende Mittel zur Darstellung von funktional wichtigen Textteilen verwendet:

kursive Schrift
: für Dateinamen, Programmnamen, Namen von Auftragsfenstern, Parameterbezeichnungen, Menütitel und Menüeinträge sowie Kommandos und Variablen im Fließtext.

<spitze Klammern>
: kennzeichnen Variable, wenn Sie dafür Werte einsetzen müssen.

[eckige Klammern]
: kennzeichnen optionale Eingaben.

{geschweifte Klammern}
: kennzeichnen eine Liste von Alternativen, die durch „|“ voneinander getrennt sind.

`dicktengleiche Schrift`
: kennzeichnet Eingaben für das System, Systemausgaben und Dateinamen in Beispielen.

kommando
: In der Syntaxbeschreibung für Kommandos werden diejenigen Bestandteile (Bezeichnungen von Kommandos und Parametern) fett dargestellt, die unverändert eingegeben werden müssen.


für Hinweistexte


ACHTUNG!
für Warnhinweise

Verweise

Verweise innerhalb des Handbuchs geben die betreffende Seite im Handbuch und je nach Bedarf auch den Abschnitt bzw. das Kapitel an. Verweise auf Themen, die in einem anderen Handbuch beschrieben sind, enthalten den Kurztitel des Handbuchs. Die vollständigen Titel finden Sie im Literaturverzeichnis.

Syntax der Kommandobeschreibung

Metasyntax

Kennzeichnung	Bedeutung	Beispiele
GROSSBUCHSTABEN	Großbuchstaben bezeichnen Schlüsselwörter (Kommando-, Anweisungs-, Operandennamen, Schlüsselwortwerte) und konstante Operandenwerte. Schlüsselwortwerte beginnen mit *.	**HELP-SDF** **SCREEN-STEPS** = ***NO**
GROSSBUCHSTABEN in Halbfett	Großbuchstaben in Halbfett kennzeichnen garantierte bzw. vorgeschlagene Abkürzungen der Schlüsselwörter.	**GUID**ANCE**-MODE** = ***Y**ES
=	Das Gleichheitszeichen verbindet einen Operandennamen mit den dazugehörenden Operandenwerten.	**GUID**ANCE**-MODE** = ***NO**
< >	Spitze Klammern kennzeichnen Variablen, deren Wertevorrat durch Datentypen und ihre Zusätze beschrieben wird (siehe Tabellen 2 und 3).	**SYNTAX-F**ILE = <filename 1..54>
Unterstreichung	Der Unterstrich kennzeichnet den Default-Wert eines Operanden.	**GUID**ANCE**-MODE** = ***NO**
/	Der Schrägstrich trennt alternative Operandenwerte.	**NEXT-FIELD** = ***NO** / ***Y**ES
(...)	Runde Klammern kennzeichnen Operandenwerte, die eine Struktur einleiten.	,**UNGUID**ED**-DIA**LOG = ***Y**ES (...) / ***NO**
[ ]	Eckige Klammern kennzeichnen struktureinleitende Operandenwerte, deren Angabe optional ist. Die nachfolgende Struktur kann ohne den einleitenden Operandenwert angegeben werden.	**SELECT** = [***BY-ATTR**IBUTES](...)

Tabelle 1: Metasyntax (Teil 1 von 2)

Kennzeichnung	Bedeutung	Beispiele
Einrückung	Die Einrückung kennzeichnet die Abhängigkeit zu dem jeweils übergeordneten Operanden.	,**GUID**ED-**DIA**LOG = ***Y**ES (...) ***Y**ES(...) **SCREEN-STEPS** = ***NO** / ***Y**ES
|	Der Strich kennzeichnet zusammengehörende Operanden einer Struktur. Sein Verlauf zeigt Anfang und Ende einer Struktur an. Innerhalb einer Struktur können weitere Strukturen auftreten. Die Anzahl senkrechter Striche vor einem Operanden entspricht der Strukturtiefe.	**SUP**PORT = ***TAPE**(...) ***TAPE(...)** **VOL**UME = ***ANY**(...) ***ANY**(...) ...
,	Das Komma steht vor weiteren Operanden der gleichen Strukturstufe.	**GUID**ANCE-**MODE** = ***NO** / ***Y**ES ,**SDF-COM**MANDS = ***NO** / ***Y**ES
list-poss(n):	Aus den list-poss folgenden Operandenwerten kann eine Liste gebildet werden. Ist (n) angegeben, können maximal n Elemente in der Liste vorkommen. Enthält die Liste mehr als ein Element, muss sie in runde Klammern eingeschlossen werden.	list-poss: ***SAM** / ***ISAM** list-poss(40): <structured-name 1..30> list-poss(256): ***OMF** / ***SYSLST**(...) / <filename 1..54>
Kurzname:	Der darauf folgende Name ist ein garantierter Aliasname des Kommando- bzw. Anweisungsnamens.	**HELP-SDF** Kurzname: **HPSDF**

Tabelle 1: Metasyntax (Teil 2 von 2)

Datentypen

Datentyp	Zeichenvorrat	Besonderheiten
alphanum-name	A…Z 0…9 $, #, @	
cat-id	A…Z 0…9	maximal 4 Zeichen; darf nicht mit der Zeichenfolge PUB beginnen
command-rest	beliebig	
composed-name	A…Z 0…9 $, #, @ Bindestrich Punkt Katalogkennung	alphanumerische Zeichenfolge, die in mehrere durch Punkt oder Bindestrich getrennte Teilzeichenfolgen gegliedert sein kann. Ist auch die Angabe eines Dateinamens möglich, so kann die Zeichenfolge mit einer Katalogkennung im Format :cat: beginnen (siehe Datentyp filename).
c-string	EBCDIC-Zeichen	ist in Hochkommata einzuschließen; der Buchstabe C kann vorangestellt werden; Hochkommata innerhalb des c-string müssen verdoppelt werden
date	0…9 Strukturkennzeichen: Bindestrich	Eingabeformat: jjjj-mm-tt jjjj: Jahr; wahlweise 2- oder 4-stellig mm: Monat tt: Tag
device	A…Z 0…9 Bindestrich	Zeichenfolge, die maximal 8 Zeichen lang ist und einem im System verfügbaren Gerät entspricht. In der Dialogführung zeigt SDF die zulässigen Operandenwerte an. Hinweise zu möglichen Geräten sind der jeweiligen Operandenbeschreibung zu entnehmen.
fixed	+, - 0…9 Punkt	Eingabeformat: [zeichen][ziffern].[ziffern] [zeichen]: + oder - [ziffern]: 0...9 muss mindestens eine Ziffer, darf aber außer dem Vorzeichen maximal 10 Zeichen (0…9, Punkt) enthalten

Tabelle 2: Datentypen (Teil 1 von 6)

Datentyp	Zeichenvorrat	Besonderheiten
filename	A…Z 0…9 $, #, @ Bindestrich Punkt	Eingabeformat: [:cat:][$user.] { datei | datei(nr) | gruppe | gruppe { (*abs) | (+rel) | (-rel) } } :cat: wahlfreie Angabe der Katalogkennung; Zeichenvorrat auf A…Z und 0…9 eingeschränkt; max. 4 Zeichen; ist in Doppelpunkte einzuschließen; voreingestellt ist die Katalogkennung, die der Benutzerkennung laut Eintrag im Benutzerkatalog zugeordnet ist. $user. wahlfreie Angabe der Benutzerkennung; Zeichenvorrat ist A…Z, 0…9, $, #, @; max. 8 Zeichen; darf nicht mit einer Ziffer beginnen; $ und Punkt müssen angegeben werden; voreingestellt ist die eigene Benutzerkennung. $. (Sonderfall) System-Standardkennung datei Datei- oder Jobvariablenname; kann durch Punkt in mehrere Teilnamen gegliedert sein: $name_1$[.$name_2$[...]] $name_i$ enthält keinen Punkt und darf nicht mit Bindestrich beginnen oder enden; datei ist max. 41 Zeichen lang, darf nicht mit $ beginnen und muss mindestens ein Zeichen aus A…Z enthalten.

Tabelle 2: Datentypen (Teil 2 von 6)

Datentyp	**Zeichenvorrat**	**Besonderheiten**

filename (Forts.)		#datei (Sonderfall)
		@datei (Sonderfall)
		# oder @ als erstes Zeichen kennzeichnet je nach Systemparameter temporäre Dateien und Jobvariablen.
		datei(nr)
		Banddateiname
		nr: Versionsnummer;
		Zeichenvorrat ist A…Z, 0…9, $, #, @.
		Klammern müssen angegeben werden.
		gruppe
		Name einer Dateigenerationsgruppe (Zeichenvorrat siehe unter „datei“)
		gruppe{(*abs) (+rel) (-rel)}
		(*abs)
		absolute Generationsnummer (1..9999);
		* und Klammern müssen angegeben werden.
		(+rel)
		(-rel)
		relative Generationsnummer (0..99);
		Vorzeichen und Klammern müssen angegeben werden.

integer	0…9, +, -	+ bzw. - kann nur erstes Zeichen (Vorzeichen) sein.
name	A…Z 0…9 $, #, @	darf nicht mit einer Ziffer beginnen.

Tabelle 2: Datentypen (Teil 3 von 6)

Datentyp	Zeichenvorrat	Besonderheiten
partial-filename	A…Z 0…9 $, #, @ Bindestrich Punkt	Eingabeformat: [:cat:][$user.][teilname.] :cat: siehe filename $user. siehe filename teilname wahlfreie Angabe des gemeinsamen ersten Namensteils von Dateien und Dateigenerationsgruppen in der Form: $name_1$.[$name_2$.[...]] $name_i$ siehe filename. Das letzte Zeichen von teilname muss ein Punkt sein. Es muss mindestens einer der Teile :cat:, $user. oder teilname angegeben werden.
posix-filename	A...Z 0...9 Sonderzeichen	Zeichenfolge, die maximal 255 Zeichen lang ist. Besteht entweder aus einem oder zwei Punkten, oder aus alphanumerischen Zeichen und Sonderzeichen; Sonderzeichen sind mit dem Zeichen \ zu entwerten. Nicht erlaubt ist das Zeichen /. Muss in Hochkommata eingeschlossen werden, wenn alternative Datentypen zulässig sind, Separatoren verwendet werden oder das erste Zeichen ?, ! bzw. ^ ist. Zwischen Groß- und Kleinschreibung wird unterschieden.
posix-pathname	A...Z 0...9 Sonderzeichen Strukturkennzeichen: Schrägstrich	Eingabeformat: [/]$part_1$[/.../$part_n$] wobei $part_i$ ein posix-filename ist; maximal 1023 Zeichen; muss in Hochkommata eingeschlossen werden, wenn alternative Datentypen zulässig sind, Separatoren verwendet werden oder das erste Zeichen ?, ! bzw. ^ ist.

Tabelle 2: Datentypen (Teil 4 von 6)

Datentyp	Zeichenvorrat	Besonderheiten
product-version	A…Z 0…9 Punkt Hochkomma	Eingabeformat: [[C]'][V][m]m.naso['] (naso: n = Korrekturstand, o = Freigabestand) wobei m, n, s und o jeweils eine Ziffer und a ein Buchstabe ist. Ob Freigabe- und/oder Korrekturstand angegeben werden dürfen oder ob sie angegeben werden müssen, bestimmen Zusätze zu dem Datentyp (siehe Tabelle 3, Zusätze without-corr, without-man, mandatory-man und mandatory-corr). product-version kann in Hochkommata eingeschlossen werden, wobei der Buchstabe C vorangestellt werden kann. Die Versionsangabe kann mit dem Buchstaben V beginnen.
structured-name	A…Z 0…9 $, #, @ Bindestrich	alphanumerische Zeichenfolge, die in mehrere durch Bindestrich getrennte Teilzeichenfolgen gegliedert sein kann; erstes Zeichen: A…Z oder $, #, @
text	beliebig	Das Eingabeformat ist den jeweiligen Operandenbeschreibungen zu entnehmen.
time	0…9 Strukturkennzeichen: Doppelpunkt	Angabe einer Tageszeit Eingabeformat: { hh:mm:ss | hh:mm | hh } hh: Stunden mm: Minuten ss: Sekunden führende Nullen können weggelassen werden
vsn	a) A…Z 0…9 b) A…Z 0…9 $, #, @	a) Eingabeformat: pvsid.folgenummer max. 6 Zeichen; pvsid: 2-4 Zeichen; Eingabe von PUB nicht erlaubt folgenummer: 1-3 Zeichen b) max. 6 Zeichen; PUB darf vorangestellt werden, dann dürfen jedoch nicht $, #, @ folgen.

Tabelle 2: Datentypen (Teil 5 von 6)

Datentyp	Zeichenvorrat	Besonderheiten
x-string	Sedezimal: 00…FF	ist in Hochkommata einzuschließen; der Buchstabe X muss vorangestellt werden; die Anzahl der Zeichen darf ungerade sein.
x-text	Sedezimal: 00…FF	ist nicht in Hochkommata einzuschließen; der Buchstabe X darf nicht vorangestellt werden; die Anzahl der Zeichen darf ungerade sein.

Tabelle 2: Datentypen (Teil 6 von 6)

Zusätze zu Datentypen

Zusatz	Bedeutung
x..y *unit*	beim Datentyp integer: Intervallangabe x Mindestwert, der für integer erlaubt ist. x ist eine ganze Zahl, die mit einem Vorzeichen versehen werden darf. y Maximalwert, der für integer erlaubt ist. y ist eine ganze Zahl, die mit einem Vorzeichen versehen werden darf. *unit* Dimension. Folgende Angaben werden verwendet: *days* *byte* *hours* *2Kbyte* *minutes* *4Kbyte* *seconds* *Mbyte* *milliseconds*
x..y *special*	bei den übrigen Datentypen: Längenangabe Bei den Datentypen catid, date, device, product-version, time und vsn wird die Längenangabe nicht angezeigt. x Mindestlänge für den Operandenwert; x ist eine ganze Zahl. y Maximallänge für den Operandenwert; y ist eine ganze Zahl. x=y Der Operandenwert muss genau die Länge x haben. *special* Zusatzangabe zur Beschreibung eines Sonderdatentyps, der durch die Implementierung geprüft wird. Vor *special* können weitere Zusätze stehen. Folgende Angaben werden verwendet: *arithm-expr* arithmetischer Ausdruck (SDF-P) *bool-expr* logischer Ausdruck (SDF-P) *string-expr* String-Ausdruck (SDF-P) *expr* beliebiger Ausdruck (SDF-P) *cond-expr* bedingter Ausdruck (JV) *symbol* CSECT- oder Entry-Name (BLS)

Tabelle 3: Zusätze zu Datentypen

1.7 Readme-Dateien

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

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

Informationen unter BS2000

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

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

Diese Datei enthält eine kurze Information zur Readme-Datei in deutscher oder englischer Sprache (<lang>=D/E). Die Information können Sie am Bildschirm mit dem Kommando `/SHOW-FILE` oder mit einem Editor ansehen.
Das Kommando `/SHOW-INSTALLATION-PATH INSTALLATION-UNIT=<product>` zeigt, unter welcher Benutzerkennung die Dateien des Produkts abgelegt sind.

Ergänzende Produkt-Informationen

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

2 Internet Services ohne FTP, TELNET und Mail installieren / deinstallieren

Beachten Sie bitte zusätzlich zu diesem Kapitel die mit dem Produkt ausgelieferte Freigabemitteilung.

Weitere Informationen zur Installation/Deinstallation der einzelnen interNet Services finden Sie in der jeweiligen Beschreibung.

2.1 Installation

Die einzelnen Komponenten des Software-Pakets interNet Services werden als ein POSIX-Programmpaket per Package-Installation mit dem POSIX-Installationsprogramm installiert (siehe Handbuch „POSIX Grundlagen für Anwender und Systemverwalter“).

Das Software-Paket interNet Services V3.4B muss komponentenweise installiert werden. Es stehen die Komponenten DNS, NAMED, NTP und OpenSSH zur Auswahl.

Wenn Sie interNet Services erstmalig installieren, müssen anschließend die Konfigurationsdateien der einzelnen Komponenten, wie in den entsprechenden Kapiteln beschrieben, an die individuellen Gegebenheiten angepasst werden.

Wenn interNet Services V3.4B bereits installierte Vorgängerversionen ersetzen soll, deinstallieren Sie diese bitte zuerst.

Wenn Sie eine vorhandene Installation deinstallieren und dann neu installieren, werden geänderte Konfigurationsdateien im Verzeichnis */etc/tcpipsv* gesichert. Bei der Installation werden diese Sicherungskopien in der Regel automatisch wieder in das aktive Verzeichnis */etc* gebracht, Details siehe detaillierte Beschreibung der einzelnen Komponenten.

Nach der Installation der interNet Services müssen vor dem Start der einzelnen Services die für die einzelnen Services spezifischen Konfigurationsdateien in der Regel durch Editieren an die individuellen Erfordernisse angepasst werden.

Wird das Subsystem POSIX beendet und wieder neu gestartet, werden automatisch alle nicht deaktivierten Dämonen der interNet Services gestartet.

Beispiel

```
/START-POSIX-INSTALLATION
```

Funktion: POSIX-Programmpakete installieren (IMON-Unterstützung: Y)
Produktname: TCP-IP-SV
Paketname: DNS oder NAMED oder NTP oder PRNGD oder OPENSSH

Nachfolgend ist die Bildschirmmaske des Installationsprogramms für die DNS-Installation abgebildet. Eingaben des Benutzers sind durch **Fettdruck** hervorgehoben.

```
                      BS2000 POSIX package installation


 IMON support ?     :  Y   (y)  mandatory for official package
                           (n)  private package (SINLIB...)

 name of product    :  TCP-IP-SV
 package of product :  DNS                    (optional for certain products)

 version of product :              (format Vmm.n or mmn)

 correction state     :            (format aso, optional for IMON support)

 installation userid   :           (mandatory for no IMON support)


 The definition of a installation path is optional for this product.
 Please enter the full pathname of the wanted installation directory:
 /opt/TCP-IP-SV/dns



 install: DUE       help: F1      terminate: F2
--------------------------------------------------------------------------------
```

2.2 Deinstallation

Analog zur Installation der Komponenten von interNet Services wird auch die Deinstallation mithilfe des POSIX-Installationsprogrammes unter der Kennung TSOS durchgeführt. Bei der Deinstallation wird nach aktiven Dämonen der interNet Services gesucht, diese Prozesse werden dann beendet. In der Syslog-Datei */var/adm/syslog* wird die Beendigung noch aktiver Dämonen protokolliert. Anschließend werden alle Dateien, Links und Prozeduren der interNet Services-Komponenten gelöscht.

Im Rahmen der Deinstallation werden einige Konfigurationsdateien im Verzeichnis */etc/tcpipsv* gesichert. Nähere Informationen dazu entnehmen Sie bitte der Deinstallationsbeschreibung der einzelnen interNet Services.

2.3 Inbetriebnahme

Der Anwender kann die Dämonen der Komponenten von interNet Services einzeln anstarten. Die entsprechenden Prozeduren sind im Verzeichnis */etc/init.d/* installiert.

Die Startaufrufe lauten:

- Für DNS: */etc/init.d/TCP-IP-SV.dns start* bzw. */etc/init.d/TCP-IP-SV.named start*
- Für NTP: */etc/init.d/TCP-IP-SV.ntp start*
- Für OpenSSH: */etc/init.d/TCP-IP-SV.openssh start*

Zusätzlich wird für alle Dämonen ein Restartaufruf angeboten, der erforderlich wird, wenn im laufenden Betrieb eine modifizierte Konfigurationsdatei eingelesen werden soll.

Die Restartaufrufe lauten:

- Für DNS: */etc/init.d/TCP-IP-SV.dns restart* bzw. */etc/init.d/TCP-IP-SV.named restart*
- Für NTP: */etc/init.d/TCP-IP-SV.ntp restart*
- Für OpenSSH: */etc/init.d/TCP-IP-SV.openssh restart*

Innerhalb des Restartprozedur-Ablaufs wird überprüft, ob der entsprechende Dämon gestartet ist. Wird kein aktiver Dämon gefunden, dann erfolgt ein normaler Neustart.

2.4 Außerbetriebnahme

Die Stopaufrufe lauten:

- Für DNS: */etc/init.d/TCP-IP-SV.dns stop* bzw. */etc/init.d/TCP-IP-SV.named stop*
- Für NTP: */etc/init.d/TCP-IP-SV.ntp stop*
- Für OpenSSH: */etc/init.d/TCP-IP-SV.openssh stop*

Die Außerbetriebnahme gilt nur bis zur Beendigung des Subsystemes POSIX. Soll ein automatischer Wiederanlauf beim erneuten Starten des Subsystemes POSIX verhindert werden, muss der Start der Dämonen verhindert werden, wie es bei der Installation der jeweiligen Komponente beschrieben wird. Falls erforderlich kann aber immer noch ein manueller Start mit *mstart* statt *start* durchgeführt werden.

Alle komponentenweise installierbaren Dienste (DNS, NAMED, OPENSSH, NTP) werden durch POSIX-Deinstallation permanent deaktiviert.

3 FTP und TELNET - Installation

Beachten Sie bitte zusätzlich zu diesem Kapitel die mit dem Produkt ausgelieferte Freigabemitteilung.

Nach der Installation der Produktdateien ist für FTP und TELNET noch ein weiterer Installationsschritt mit dem SDF-Kommando SET-FTP-TELNET-PARAMETERS nötig. Dabei wird gleichzeitig die Konfiguration durchgeführt.

Bei der Ausführung des Kommandos SET-FTP-TELNET-PARAMETERS (siehe Seite 42) wird für den FTP- und den TELNET-Server je eine Option-Datei erzeugt, in der die einzelnen FTP-Server-Parameter bzw. TELNET-Server-Parameter als Options abgelegt sind.

3.1 Installation von FTP und TELNET via SDF-Kommando

Das SDF-Kommando SET-FTP-TELNET-PARAMETERS bietet folgende Funktionalität:

– Parameter für FTP- und TELNET-Server festlegen und in Option-Dateien separat für FTP- und TELNET-Server ablegen (siehe Seite 70 bzw. Seite 150)

– ENTER-Dateien für FTP- und TELNET-Dämon erstellen

SET-FTP-TELNET-**PAR**AMETERS

FTP-SERVER-PROC=*NO / *CREATE(...)

***CRE**ATE(...)

JOB-NAME= *STD / <name 1..5>

, JOB-CLASS= *STD / <name 1..8>

, CPU-TIME= *STD / <integer 1..32767>

, PRIORITY**= *STD** / <integer 0..255>

, DEBUG= *STD / <integer 0..9>

, TRACE= *STD / <integer 0..9>

, MAXIMUM-**CONN**ECTIONS**= *STD** / <integer 1..900>

, STATION-**ID= *STD** / <integer 0..6>

, TRANSFER-**JOB-CLASS= *STD** / <name 1..8>

, TRANSFER-**CPU-TIME= *STD** / <integer 1..32767>

, TIMEOUT-VALUE**= *STD** / <integer 1..32767>

, SYSTEM-**EXIT-LEV**EL**= *STD**/<integer 0..3>

SET-FTP-TELNET-**PAR**AMETERS

, FTAC-SUPPORT**= *STD** / ***NO** / ***YES**(...)
***YES**(...)
LEVEL**= *STD** / <integer 1..2>
, JOB-CLASS= *STD / <name 1..8>
, ENTER-**F**ILE**= *STD** / <filename 1..54_without-generation-version>
, SERVER-INFORMATION-**F**ILE**= *STD** / <filename 1..54_without-generation-version>
,FTAC-USERID=*STD /<name 1..8>
, TLS-SUPPORT**= *STD** / ***NO** / ***YES**(...)
***YES**(...)
PROTOCOL= *STD / <text 1..80>
, CIPHER-SUITE= *STD / <text 1..80>
, RSA-CERTIFICATE-FILE= *STD / ***NONE** / <filename 1..54_without-generation-version>
, RSA-KEY-FILE= *STD / ***NONE** / <filename 1..54_without-generation-version>
, DSA-CERTIFICATE-FILE= *STD / ***NONE** / <filename 1..54_without-generation-version>
, DSA-KEY-FILE= *STD / ***NONE** / <filename 1..54_without-generation-version>
, CA-CERTIFICATE-FILE= *STD / ***NONE** / <filename 1..54_without-generation-version>
, CLIENT-CA-FILE= *STD / ***NONE** / <filename 1..54_without-generation-version>
, CERT-CHAIN-FILE= *STD / ***NONE** / <filename 1..54_without-generation-version>
, CA-REVOCATION-FILE= *STD / ***NONE** / <filename 1..54_without-generation-version>
, RANDOM-FILE= *STD / ***NONE** / <filename 1..54_without-generation-version>
, SSL-LIBRARY= *STD / ***NONE** / <filename 1..54_without-generation-version>
, VERIFY-CLIENT= *STD / ***NONE** / ***OPTIONAL** / ***REQUIRE**
, VERIFY-DEPTH= *STD / <1..32767>
, SEC-CONTROL-CONN= *STD / ***NONE** / ***OPTIONAL** / ***REQUIRE**
, SEC-DATA-CONN= *STD / ***NONE** / ***OPTIONAL** / ***REQUIRE**
, ACCOUNTING= *STD / ***NO** / ***YES**(...)
***YES**(...)
FILE= *STD / <filename 1..54_without-generation-version>
, OPTION-FILE= *STD / <filename 1..54_without-generation-version>
, SELECTOR= *STD / <text 1..511>
, INITIAL-COMMANDS= *STD / <c-string 2..256>
, PORT-NUMBER= *STD / <integer 1..32767>
, SERVER-ENTER-FILE= *STD / <filename 1..54_without-generation-version>
, LOGGING-FILE= *STD / <filename 1..54_without-generation-version>
, ALLOW-TSOS-LOGIN= *STD / ***NO** / ***YES** / ***TLS**

SET-FTP-TELNET-**PAR**AMETERS

, TELNET-**SERVER-PROC= *NO / *CRE**ATE(...)

***CRE**ATE(...)

JOB-NAME= *STD / <name 1..5>

, JOB-CLASS= *STD / <name 1..8>

, CPU-TIME= *STD / <integer 1..32767>

, PRIORITY**= *STD** / <integer 0..255>

, DEBUG= *STD / <integer 0..9>

, TRACE= *STD / <integer 0..9>

, MAXIMUM-**CONN**ECTIONS**= *STD** / <integer 1..900>

, STATION-**ID= *STD** / <integer 0..6>

, ASCII-TABLE**= *STD** / <text 1..8>

, EBCDIC-TABLE**= *STD** / <name 1..8>

, TLS-SUPPORT= *STD / ***NO** / ***PARAMETERS(...)**

***PARAMETERS (...)**

OPTION= *STD / ***START-TLS** / ***AUTHENTICATION(...)**

***AUTHENTICATION(...)**

DEBUG= *STD / ***NO** / ***YES**

, PROTOCOL= *STD / <text 1..80>

, CIPHER-SUITE = *STD / <text 1..80>

, RSA-CERTIFICATE-FILE = *STD / ***NONE** / <filename 1..54_without-generation-version>

, RSA-KEY-FILE = *STD / ***NONE** / <filename 1..54_without-generation-version>

, DSA-CERTIFICATE-FILE = *STD / ***NONE** / <filename 1..54_without-generation-version>

, DSA-KEY-FILE = *STD / ***NONE** / <filename 1..54_without-generation-version>

, CA-CERTIFICATE-FILE = *STD / ***NONE** / <filename 1..54_without-generation-version>

, CLIENT-CA-FILE = *STD / ***NONE** / <filename 1..54_without-generation-version>

, CERT-CHAIN--FILE = *STD / ***NONE** / <filename 1..54_without-generation-version>

, CA-REVOCATION-FILE = *STD / ***NONE** / <filename 1..54_without-generation-version>

, RANDOM-FILE = *STD / <filename 1..54_without-generation-version>

, SSL-LIBRARY = *STD / ***NONE** / <filename 1..54_without-generation-version>

, VERIFY-CLIENT= *STD / ***NONE** / ***OPTIONAL** / ***REQUIRE**

, VERIFY-DEPTH= *STD / <1..32767>

, ENCRYPTION= *STD **/ *NO / *YES(...)**

***YES(...)**

DEBUG= = *STD / ***NO** / ***YES**

, KEY= <x-text 1..16>

, SSL-LIBRARY = *STD / ***NONE** / <filename 1..54_without-generation-version>

SET-FTP-TELNET-**PAR**AMETERS
, OPTION-FILE= *STD / <filename 1..54_without-generation-version> **, SELECTOR= *STD /** <text 1..511> **, PORT-NUMBER= *STD** / <integer 0..32767> **, SERVER-ENTER-FILE= *STD** / <filename 1..54_without-generation-version> **, LOGGING-FILE= *STD** / <filename 1..54_without-generation-version>
, START-PROCEDURE**= *NO** / ***CRE**ATE

Gemeinsame Operanden von FTP und TELNET

Für die Beschreibung der FTP-Operanden, siehe Seite 57.
Für die Beschreibung der TELNET-Operanden, siehe Seite 140.

START-PROCEDURE=
Gibt an, ob die Datei SYSENT.TCP-IP-AP.*nnn*.START erstellt werden soll, die die Start-Enter-Datei für FTP und TELNET enthält.

START-PROCEDURE=*NO
Die Datei wird nicht erstellt.

START-PROCEDURE=*CREATE
Die Datei wird erstellt.

Returncodes des SET-FTP-TELNET-PARAMETERS-Kommandos

(SC2) SC1	Maincode	Bedeutung / garantierte Meldungen
0	TCP9000	INSTALLATION WURDE ERFOLGREICH BEENDET
1	CMD0202	SYNTAX-FEHLER IM KOMMANDO (Dieser Returncode tritt bei Syntaxfehlern auf, die schon auf der Ebene der SDF-Kommandodefinitionen festgestellt werden.)
1	TCP9002	UNGUELTIGER DATEINAME: (&00)
1	TCP9003	DAS PASSWORT (&00) IST UNGUELTIG.
1	TCP9004	DER INSTALLATIONSBEGRIFF (&00) IST UNGUELTIG.
1	TCP9005	DIE KENNUNG (&00) IST UNGUELTIG.
1	TCP9006	DIE BS2000 VERSION (&00) IST UNGUELTIG.
1	TCP9007	DER LOGON-NAME (&00) IST UNGUELTIG.
1	TCP9008	(&00) MAXIMALE VERBINDUNGEN LIEGEN IN EINEM NICHT GUELTIGEN BEREICH.
1	TCP9009	DER (&01) PARAMETER (&00) IST UNGUELTIG.
1	TCP9010	DIE JOB-KLASSE (&00) IST UNGUELTIG.
1	TCP9011	DAS CPU-LIMIT (&00) IST UNGUELTIG.
1	TCP9012	(&00) PARAMETER EINSETZEN.
1	TCP9014	DIE PRIORITAET (&00) IST UNGUELTIG.
1	TCP9015	DER DCAM-APPLICATIONSNAME (&00) IST UNGUELTIG.
1	TCP9016	DIE PORTNUMMER (&00) IST UNGUELTIG.
1	TCP9017	DER WERT (&00) FUER PORTUEBERWACHUNG IST NICHT KORREKT.
1	TCP9018	DER WERT (&00) FUER AUTORISIERUNGSDIENST IST NICHT KORREKT.
1	TCP9020	DIE ANZAHL DER STELLEN ZUR BILDUNG DES DCAM-ANWENDUNGSNAMENS (&00) IST UNGUELTIG.
1	TCP9021	DIE STANDARD-ASCII CODETABELLE (&00) IST UNGUELTIG.
1	TCP9022	DIE STANDARD-EBCDIC CODETABELLE (&00) IST UNGUELTIG.
1	TCP9023	SDF-FEHLER BEIM LESEN DER ANWEISUNG.
64	TCP9200	OEFFNEN VON (&00) NICHT MOEGLICH DVS: (&01)
64	TCP9201	SCHREIB-FEHLER AUF DER INSTALLATIONSDATEI: DVS: (&00)
64	TCP9202	INSTALLATIONSPROGRAMM UND PARAMETERDATEI HABEN EINE UNGLEICHE VERSION.
64	TCP9203	FILE-KOMMANDO KONNTE NICHT ABGESETZT WERDEN.
64	TCP9205	INSTALLATION (&00) WURDE NICHT GEFUNDEN. DVS:(&01)
64	TCP9206	(&00) ENTER-DATEI KONNTE NICHT ERSTELLT WERDEN. DVS:(&01)
64	TCP9207	SCHLIESSEN DER INST.-DATEI (&00) NICHT MOEGLICH. DVS:(&01)
64	TCP9208	MSG-GROUP TCP KONNTE NICHT INSTALLIERT WERDEN . CODE (&00)
64	TCP9209	LESE-FEHLER AUF DER INSTALLATIONSDATEI: (&00)

3.2 Installation und Deinstallation von FTP- und TELNET-Client in POSIX

FTP- und TELNET-Client werden gemeinsam mit dem SNMP-Subagenten für FTP (siehe Handbuch „SNMP-Management für openNet Server und interNet Services“) als ein POSIX-Programmpaket via Package-Installation mit dem POSIX-Installationsprogramm installiert. Eventuell vorhandene ältere Versionen des Programmpakets TCP-IP-AP müssen zuvor deinstalliert werden.

Installation

```
/START-POSIX-INSTALLATION
```

Funktion: POSIX-Programmpakete installieren (IMON-Unterstützung: Y)
Produktname: TCP-IP-AP

Nachfolgend ist die Installationsmaske mit den Angaben für die Installation dargestellt.

```
                        BS2000 POSIX package installation


  IMON support ?     :  Y   (y)  mandatory for official package
                            (n)  private package (SINLIB...)

  name of product    :  TCP-IP-AP
  package of product :                        (optional for certain products)

  version of product :              (format Vmm.n or mmn)

  correction state     :            (format aso, optional for IMON support)

  installation userid   :           (mandatory for no IMON support)









  install: DUE       help: F1      terminate: F2
--------------------------------------------------------------------------------
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
```

Deinstallation

```
/START-POSIX-INSTALLATION
```

Funktion: POSIX-Programmpakete deinstallieren
Produktname: TCP-IP-AP

3.3 Fragen und Antworten zu Installation und Betrieb von FTP und TELNET (FAQ)

- **Frage:**
  Welche Bedeutung hat die Ausgabe der folgenden Meldung nach dem Laden von FTP- oder TELNET-Client bzw. von FTP- oder TELNET-Server?

```
BLS0340 UNRESOLVED EXTERNAL REFERENCES
BLS0342 ### 'YS6GSBN ……
BLS0342 ### 'YS6SOCE …….
BLS0342 ### 'YS6CLOS …….
BLS0342 ### 'YS6SHTD …….
BLS0342 ### 'YS6ERRO …….
```

  Antwort:
  Die Programme wurden entweder mit START-PROG ... ohne PROG-MODE=*ANY gestartet oder das Socket-Subsystem SOC6 ist nicht gestartet.

- **Frage:**
  Der Verbindungsaufbau mit *open* im FTP- oder TELNET-Client dauert sehr lange. Was ist die Ursache?

  Antwort:
  Sowohl Client als auch Server benutzen beim Verbindungsaufbau DNS-Funktionen. Wenn die zugehörigen Resolver-Dateien nicht ordnungsgemäß eingestellt sind, können längere Wartezeiten die Folge sein. Dies ist beispielsweise der Fall, wenn der in den Resolverdateien spezifizierte DNS-Server nicht erreichbar ist.

  Der Name der Resolver-Datei im BS2000 lautet:

  SYSDAT.SOCKETS.*nnn*.SOC6.RESOLV bzw:
  SYSDAT.LWRESD.*nnn*.RESOLV.CONF

- **Frage:**
  Welche Bedeutung hat die folgende FTP-Client-Meldung?

```
"time limit for server response exceeded"
```

  Antwort:
  Der Client wartet auf eine Antwort des Servers, die nach einer voreingestellten Anzahl von Sekunden (30 Sekunden) nicht eingetroffen ist. Ursache hierfür kann z.B. eine zu hohe Netzbelastung sein.
  Das Problem können Sie oft dadurch lösen, dass Sie den voreingestellten Timeout-Wert von 30 Sekunden mit dem FTP-Benutzerkommando *settime* (siehe Handbuch „interNet Services Benutzerhandbuch“) erhöhen.

- **Frage:**
  Wenn ich mit FTP eine Datei transferiere und sie im Zielsystem als PAM-Datei abspeichere, wird am Ende der String „C-DATEIENDE“ angefügt. Wozu dient das, und wie kann ich es verhindern?

  Antwort:
  Der String „C-DATEIENDE“ wird normalerweise benutzt, um das genaue Ende einer PAM-Datei zu markieren. Mit dem FTP-Benutzerkommando `setfile datend off` können Sie das Anhängen des Strings „C-DATEIENDE“ unterdrücken.

- **Frage:**
  In früheren FTP-Versionen (< V4.0) wurden Tabulatorzeichen in einer Textdatei automatisch in die entsprechende Anzahl von Leerzeichen umgesetzt. Jetzt ist dies nicht mehr der Fall. Was ist die Ursache?

  Antwort:
  Im Zuge der Unterstützung der Restart-Fähigkeit im BS2000-FTP ab V4.0 wurde die Voreinstellung für den Transfer von Textdateien von `ftyp text` auf `ftyp textbin` geändert. Daher werden Tabulatorzeichen standardmäßig nicht mehr umgesetzt.

  Wenn Sie die Umsetzung der Tabulatorzeichen dennoch nutzen wollen, können Sie dies wahlweise via *ftyp*-Kommando oder via Option-Datei einstellen:

  – *ftyp*-Kommando (siehe Handbuch „interNet Services Benutzerhandbuch“). Spezifizieren Sie `ftyp text` im Client bzw. `quote site ftyp text` im Server.

  – Option-Datei des FTP-Client (Option -*initialCommand*, siehe Handbuch „interNet Services Benutzerhandbuch“) bzw. Option-Datei des FTP-Servers (Option *initialChildCmds*, siehe Seite 80)

- **Frage:**
  In früheren FTP-Versionen (< V4.0) wurden SAM-Dateien mit fester Satzlänge bei *type binary* vollständig binär übertragen und ohne Satzende-Zeichen abgespeichert. In der aktuellen FTP-Version ist die Zieldatei mit Satzende-Zeichen versehen. Wie kann ich das verhindern?

  Antwort:
  Auch für SAM-Dateien mit fester Satzlänge werden jetzt die *ftyp*-Einstellungen berücksichtigt. Wenn *ftyp* ungleich „binary“ ist, bleibt die Satzstruktur der Ursprungsdatei bei der Übertragung erhalten. Um dies zu verhindern, müssen Sie explizit *ftyp binary* einstellen.

- **Frage:**
  Im BS2000-FTP und -TELNET ist es möglich mit den Kommandos *trace* und *debug* (bei den Clients) bzw. mit den Options -*T* und -*D* (bei den Servern) Diagnoseinformation zu erzeugen. Worin besteht der Unterschied zwischen *trace* bzw. -*T* einerseits und *debug* bzw. -*D* andererseits?

  Antwort:
  debug bzw. -*D* erzeugen Diagnoseinformationen, die die Produkte FTP bzw. TELNET selbst betreffen. Der höchste sinnvolle Level ist hier 2.
  Dagegen geben *trace* bzw. -*T* Diagnoseinformationen aus, die von den Sockets erzeugt wurden. Der höchste sinnvolle Level ist hier 10.

- **Frage:**
  Ich habe einen zweiten FTP- bzw. TELNET-Server gestartet, kann zu diesem aber keine Verbindung herstellen. Was kann die Ursache sein?

  Antwort:
  Die häufigsten Ursachen des Problems sind:

  – Angabe einer bereits vergebenen Portnummer für den Server.
  – Verwendung eines schon vergebenen Applikationsnamens (Option -*A*) im Server.

- **Frage:**
  Mein FTP-Login wird vom (BS2000-) FTP-Server mit der Meldung `invalid login` abgewiesen. Ich kann aber keine Ursache für dieses Verhalten finden. Was ist zu tun ?

  Antwort:
  Schalten Sie - falls möglich - im FTP-Server den FTP-Trace mit folgendem Kommando ein:

  ```
  /INFORM-PROGRAM 'debug 2',*TSN(<tsn_des_ftpservers>)
  ```

  Wiederholen Sie das Login und speichern Sie die Traces mit dem Kommando

  ```
  /INFORM-PROGRAM 'rdProt',*TSN(<tsn_des_ftpservers>)
  ```

  in die Datei SYSOUT.TCP-IP-AP.*nnn*.FTPD.<MMDDHHMMSS> ab.

  (MMDDHHMMSS ist Datum- und Zeitangabe der Form
  Month Day Hour Minute Second.)

- **Frage:**
  Wie erreiche ich mit einem Webbrowser einen BS2000-FTP-Server?

  Antwort:
  Über die folgende URL erhalten Sie Zugang zum POSIX-Dateiverzeichnis der Kennung <userid>:

  ```
  ftp://<userid>,<accountnummer>@<rechnername>:<portnummer>/
  ```

  Damit ist zumindest die Ausgabe der Dateiverzeichnisse möglich. Ein Zugang zum BS2000-Dateiverzeichnis ist über den Webbrowser nicht möglich.

- **Frage:**
  Es gibt bei FTP die Möglichkeit, mit `quote <command>` das Kommando <command> an den Server zu schicken. Es gibt aber auch `quote site <command>` und `quote site exec <command>`. Worin besteht der Unterschied?

  Antwort:

  – Mit `quote <command>` schicken Sie standard-konforme FTP-Kommandos an den Server.

  – Mit `quote site <command>` schicken sie BS2000-spezifische („proprietäre“) Kommandos, nicht im Standard definierte Kommandos an den Server. Solche Kommandos sind u.a. *ftyp*, *cmod*, *modc*, *file*, *setc*, *sfil*.

  – Mit `quote site exec <command>` senden Sie BS2000-Kommandos zur Ausführung an den Server. Um die missbräuchliche Verwendung dieser Kommandos im Zielsystem zu verhindern, wird diese Variante beim Einsatz von FTAC (Option -*FTAClevel* > 0) oder durch die Option -*disableSiteExecCommand* deaktiviert.

- **Frage:**
  Beim Einsatz von FTP-Clients mit grafischer Benutzeroberfläche (GUI) besteht oft keine Möglichkeit, die für die Verbindung mit BS2000 erforderliche Abrechnungsnummer anzugeben. Was ist in diesem Fall zu tun?

  Antwort:
  Geben Sie in diesen Fällen die Abrechnungsnummer bereits bei der Eingabe der Kennung wie folgt ein:

  ```
  <userid>,<account>
  ```

- **Frage:**
  Beim Abholen einer Datei von einem BS2000-FTP-Server bricht mein Nicht-BS2000-FTP-Client nach einer gewissen Zeit die Ausführung ab, ohne dass mit dem eigentlichen Datentransfer begonnen wurde.

  Antwort:
  Manche FTP-Clients zeigen den Transfer-Fortschritt durch einen Fortschrittsbalken an. Zu diesem Zweck erfragen die Clients zunächst mit dem FTP-Protokollkommando *SIZE* die Größe der Datei vom Server. Der Server muss i.A. für die Bearbeitung dieses Kommandos die betreffende Datei vollständig lesen. Dies kann bei sehr großen Dateien naturgemäß recht lange dauern, so dass die Zeitüberwachung des Client die Verbindung abbricht.
  Leider kann diese Zeitüberwachung bei manchen Clients nicht auf längere Wartezeiten umkonfiguriert werden. Darüber hinaus wird in vielen Fällen auch bei Deaktivierung des Fortschrittsbalkens ein *SIZE*-Kommando an den Server abgesetzt.

  Wenn vom Hersteller des FTP-Client keine Verbesserung der Konfigurationsmöglichkeiten zu erhalten ist, besteht beim BS2000-FTP-Server die Möglichkeit, mithilfe der Option *-disableSizeCommand* das *SIZE*-Kommando zu deaktivieren (siehe Handbuch „interNet Services Benutzerhandbuch“).

  Da von einem Client die Unterstützung des *SIZE*-Kommandos durch den Server nicht vorausgesetzt werden darf, sollte der Transfer in jedem Fall funktionieren. Allerdings müssen Sie in Kauf nehmen, dass der Restart-Mechanismus nicht mehr funktioniert, da hierfür das *SIZE*-Kommando benötigt wird.

- **Frage:**

  Beim Transfer einer LMS-Datei von einem NK2- auf ein NK4-Pubset ist die Zieldatei keine gültige LMS-Datei mehr.

  Antwort:

  Transferieren Sie die Datei zunächst auf ein nicht-NK4-Pubset auf dem Zielrechner und kopieren Sie dann die LMS-Bibliothek mithilfe von LMS auf das NK4-Pubset.

  Alternativ können Sie auf dem Quellrechner die LMS-Bibliothek auf ein NK4-Pubset umsetzen und dann mit FTP auf das NK4-Pubset des Zielrechners transferieren.

4 FTP - Konfiguration und Betrieb

Die Konfiguration von FTP können Sie entweder über das SDF-Kommando oder über die Option-Datei durchführen.

Das Kapitel behandelt folgende Themen zu Konfiguration und Betrieb von FTP-Servern:

- Verwendung von TLS/SSL zur Absicherung von FTP-Server (siehe Seite 54).
- Konfiguration von FTP über SDF-Kommando (siehe Seite 57) oder via Option-Datei (siehe Seite 70).
- Starten und beenden von FTP-Servern (siehe Seite 101).
- Anmerkungen zu Installation und Nutzung der FTAC-Funktionalität (siehe Seite 106).
- Ein-/Ausschalten des Accounting und Festlegen der Abrechnungsdatei (siehe Seite 107).
- Sichern der Protokolldatei von FTP-Servern (siehe Seite 111).
- Anzeigen der aktuellen Einstellungen des FTP-Servers (siehe Seite 111).
- Angabe von Kommandos über die Konsolschnittstelle (siehe Seite 114).
- Verwendung von IPv6-Adressen in FTP (siehe Seite 118).
- Hinweise zur Verwendung des SNMP-Subagenten für FTP (siehe Seite 121).
- Exits für FTP-Client und den FTP-Server (siehe Seite 122).

4.1 TLS/SSL-Unterstützung im FTP-Server

Einen allgemeinen Überblick über SSL finden Sie im Handbuch „interNet Services Benutzerhandbuch“.

Für die TLS/SSL-Unterstützung im FTP-Server stehen folgende Instrumente zur Verfügung:

- Option-Datei bzw. Option-Dateien
- Installationskommando SET-FTP-TELNET-PARAMETERS
- FTP-Protokoll-Kommandos

4.1.1 Parametrisierung der TLS/SSL-Unterstützung im FTP-Server

Die TLS/SSL-Unterstützung bietet ein breites Spektrum an Einstellmöglichkeiten. Diese Einstellungen können Sie wahlweise wie folgt vornehmen:

- Mithilfe von Options, die in einer oder mehreren Option-Dateien hinterlegt werden, und beim Start des FTP-Servers ausgewertet werden (siehe Abschnitt „Konfiguration von FTP via Option-Datei“ auf Seite 70).
- Mithilfe von Parametern des Installationskommandos SET-FTP-TELNET-PARAMETERS (siehe Abschnitt „Konfiguration von FTP via Installationskommando SET-FTP-TELNET-PARAMETERS“ auf Seite 57).

In der folgenden Tabelle sind die Options für die TLS/SSL-Unterstützung im FTP-Server aufgelistet. Zu den einzelnen Options existieren entsprechende Parameter des SET-FTP-TELNET-PARAMETERS-Kommandos.

Option	Beschreibung	Seite
-tlsProtocol	SSL-Protokollversionen selektiv auswählen	86
-tlsCipherSuite	Verschlüsselungsverfahren-Vorzugsliste spezifizieren	87
-tlsRSAcertificateFile	Datei spezifizieren, die das RSA-basierte X.509-Server-Zertifikat im PEM-Format enthält	87
-tlsRSAkeyFile	Datei spezifizieren, die den privaten RSA-Server-Schlüssel im PEM-Format enthält	88
-tlsDSAcertificateFile	Datei spezifizieren, die das DSA-basierte X.509-Server-Zertifikat im PEM-Format enthält	89
-tlsDSAkeyFile	Datei spezifizieren, die den privaten DSA-Server-Schlüssel im PEM-Format enthält	90
-tlsCertificateChainFile	Datei spezifizieren, in der alle zur Verifikation des Server-Zertifikats benötigten Zertifikate abgelegt werden können	91
-tlsCAcertificateFile	Datei spezifizieren, die die für die Authentifizierung des FTP-Client erforderlichen Zertifikate im PEM-Format enthält	92
-tlsAcceptableClientCAFile	Datei spezifizieren, aus der die Namen der CAs hervorgehen, die der Server als Unterzeichner von Client-Zertifikaten akzeptiert	93
-tlsCArevocationFile	Datei spezifizieren, die die CRLs der CAs enthält	94
-tlsVerifyClient	Festlegen, ob der FTP-Client ein Zertifikat für den Server-Zugang vorweisen muss	94
-tlsVerifyDepth	Verifizierungstiefe festlegen	95
-tlsSecureControlConnection	Festlegen, ob die Kontroll-Verbindung vom FTP-Client zum FTP-Server mit TLS abgesichert werden soll	96
-tlsSecureDataConnection	Festlegen, ob die Daten-Verbindung vom FTP-Client zum Server-Child mit TLS abgesichert werden soll	97
-tlsRandFile	Datei spezifizieren, aus der beim Server-Start die Daten für die Initialisierung des PRNG gelesen werden	98
-tlsOpenSSLlibName	Festlegen, aus welcher LMS-Datei die OpenSSL-Bibliothek nachgeladen werden soll	98

4.1.2 FTP-Protokoll-Kommandos

Der FTP-Server unterstützt die FTP-Protokoll-Kommandos *AUTH*, *CCC*, *PBSZ* und *PROT* in der von RFC 4217 geforderten Form:

- Für das Kommando *AUTH* sind die Parameter *TLS*, *TLS-C*, *TLS-P* und *SSL* zulässig. *SSL*, *TLS* und *TLS-C* haben die gleiche Bedeutung und fordern eine TLS-Absicherung nur für die Kontroll-Verbindung an. Bei TLS-P wird zusätzlich auch eine Absicherung der Daten-Verbindung angefordert.
- Das *PBSZ*-Kommando wird nur formell mit dem Parameter 0 unterstützt, um einen Protokollablauf gemäß RFC 2228 zu gewährleisten.
- Das *PROT*-Kommando wird mit den Parametern C und P unterstützt, wobei mit C (= Clear) die Verschlüsselung der Daten-Verbindung ausgeschaltet und mit P (= Private) eingeschaltet wird.
- Falls die TLS-Unterstützung aktiviert ist, meldet das *FEAT*-Kommando [RFC 2389] dies durch zusätzliche Aufzählung von *AUTH TLS*, *PBSZ* und *PROT*.

Die Ausgabe des *STAT*-Kommandos wird um drei Zeilen ergänzt. In diesen Zeilen wird zunächst dokumentiert, ob die Kontroll- bzw. Daten-Verbindung mit TLS abgesichert ist. Weiterhin wird angegeben, mit welchen Algorithmen gegebenenfalls Kontroll- und Daten-Verbindung abgesichert werden.

Beispiele

1. ungesicherte Kontroll-Verbindung:

```
Protected control channel: Off
Private data channel: Off
Cipher: clear
```

2. mit Triple-DES abgesicherte Kontroll-Verbindung, ungesicherte Daten-Verbindung:

```
Protected control channel: On
Private data channel: Off
Cipher: DES-CBC3-SHA (168 bits)
```

3. mit Triple-DES abgesicherte Kontroll- und Daten-Verbindung:

```
Protected control channel: On
Private data channel: On
Cipher: DES-CBC3-SHA (168 bits)
```

4. mit Triple-DES abgesicherte Kontroll- und Daten-Verbindung, wobei die Kontrollverbindung nach dem *ccc*-Kommando wieder unverschlüsselt ist:

```
Protected control channel: Off (cleared)
Private data channel: On
Cipher: DES-CBC3-SHA (168 bits)
```

4.2 Konfiguration von FTP via Installationskommando SET-FTP-TELNET-PARAMETERS

Für die komplette Kommando-Syntax und die Beschreibung der Installations-Operanden, siehe Seite 42.

SET-FTP-TELNET-**PAR**AMETERS

(...)

, FTP-SERVER-PROC=*NO / *CREATE(...)

***CRE**ATE(...)

JOB-NAME= *STD / <name 1..5>

, JOB-CLASS= *STD / <name 1..8>

, CPU-TIME= *STD / <integer 1..32767>

, PRIORITY**= *STD** / <integer 0..255>

, DEBUG= *STD / <integer 0..9>

, TRACE= *STD / <integer 0..10>

, MAXIMUM-**CONN**ECTIONS**= *STD** / <integer 1..900>

, STATION-**ID= *STD** / <integer 0..6>

, TRANSFER-**JOB-CLASS= *STD** / <name 1..8>

, TRANSFER-**CPU-TIME= *STD** / <integer 1..32767>

, TIMEOUT-VALUE**= *STD** / <integer 1..32767>

, SYSTEM-**EXIT-LEV**EL**= *STD**/<integer 0..3>

, FTAC-SUPPORT**= *STD** / ***NO** / ***YES**(...)

***YES**(...)

LEVEL**= *STD** / <integer 1..2>

, JOB-CLASS= *STD / <name 1..8>

, ENTER-**F**ILE**= *STD** / <filename 1..54_without-generation-version>

, SERVER-INFORMATION-**F**ILE**= *STD** / <filename 1..54_without-generation-version>

,FTAC-USERID=*STD /<name 1..8>

, TLS-SUPPORT**= *STD** / ***NO** / ***YES**(...)

***YES**(...)

PROTOCOL= *STD / <text 1..80>

, CIPHER-SUITE= *STD / <text 1..80_with-lower-case>

, RSA-CERTIFICATE-FILE= *STD / ***NONE** / <filename 1..54_without-generation-version>

, RSA-KEY-FILE= *STD / ***NONE** / <filename 1..54_without-generation-version>

, DSA-CERTIFICATE-FILE= *STD / ***NONE** / <filename 1..54_without-generation-version>

, DSA-KEY-FILE= *STD / ***NONE** / <filename 1..54_without-generation-version>

, CA-CERTIFICATE-FILE= *STD / ***NONE** / <filename 1..54_without-generation-version>

, CLIENT-CA-FILE= *STD / ***NONE** / <filename 1..54_without-generation-version>

, CERT-CHAIN-FILE= *STD / ***NONE** / <filename 1..54_without-generation-version>

, CA-REVOCATION-FILE= *STD / ***NONE** / <filename 1..54_without-generation-version>

SET-FTP-TELNET-**PAR**AMETERS

```
        , RANDOM-FILE= *STD / *NONE / <filename 1..54_without-generation-version>
        , SSL-LIBRARY= *STD / *NONE / <filename 1..54_without-generation-version>
        , VERIFY-CLIENT= *STD / *NONE / *OPTIONAL / *REQUIRE
        , VERIFY-DEPTH= *STD / <1..32767>
        , SEC-CONTROL-CONN= *STD / *NONE / *OPTIONAL / *REQUIRE
        , SEC-DATA-CONN= *STD / *NONE / *OPTIONAL / *REQUIRE
    ,ACCOUNTING=*STD / *NO / *YES(...)
      *YES(...)
        FILE=*STD / filename_1..54_without-generation-version
    ,OPTION-FILE=*STD / filename_1..54_without-generation-version
    ,SELECTOR=*STD / text_1..511
    ,INITIAL-COMMANDS=*STD / c-string_2..256
    ,PORT-NUMBER =*STD / integer_1..32767
    ,SERVER-ENTER-FILE=*STD/ filename_1..54_without-generation-version
    ,LOGGING-FILE=*STD / filename_1..54_without-generation-version
    ,ALLOW-TSOS-LOGIN=*STD / *NO / *YES / *TLS
    ,TVFS=*STD / *NO / *YES
(...)
```

FTP-SERVER-PROC=
Parameter für FTP-Server

FTP-SERVER-PROC=*NO
Es soll keine Installation für den FTP-Server durchgeführt werden.

FTP-SERVER-PROC=*CREATE(...)
Der FTP-Server soll konfiguriert werden. Aus den eingegebenen Parametern wird die Enter-Datei zum Start des FTP-Servers erstellt.

JOB-NAME=
Dieser Name wird als Präfix verwendet. Um den Datenstationsnamen der jeweiligen Verbindung zu erhalten, wird an den Parameter JOB-NAME die laufende Nummer angehängt. Siehe auch Option *-appPrefix* auf Seite 71.

JOB-NAME=*STD
Entspricht der Angabe FTPSR bzw. dem Wert in der Installationsdatei

JOB-NAME=<name 1..5>
Job-Name

JOB-CLASS=
Jene Jobklasse, in welcher der Serverprozess laufen soll. Stellen Sie sicher, dass in dieser Jobklasse Enter-Jobs mit folgenden Parametern gestartet werden dürfen: CPU-LIMIT=*NO, RUN-PRIORITY=120 sowie START=*IMMEDIATELY.

JOB-CLASS=*STD
Entspricht der Standard-Jobklasse des Systems bzw. dem Wert in der Installationsdatei.

JOB-CLASS=<name 1..8>
Name der Job-Klasse

CPU-TIME=
CPU-Zeit, die für den Serverprozess maximal zur Verfügung steht.

CPU-TIME=*STD
Entspricht der Angabe NTL bzw. dem Wert in der Installationsdatei.

CPU-TIME=<integer 1..32767>
CPU-Zeit in Sekunden

PRIORITY=
Priorität, mit der der Serverprozess laufen soll.

PRIORITY=*STD
Entspricht der Angabe 120 bzw. dem Wert in der Installationsdatei.

PRIORITY=<integer 0..255>
Server-Priorität

DEBUG=
Trace zur Benutzerebene. Siehe auch Option *-debugLevel* auf Seite 73.

DEBUG=*STD
Entspricht der Angabe 0 bzw. dem Wert in der Installationsdatei

DEBUG=<integer 0..9>
Debug-Level

TRACE=
Trace zur TCP/IP-(Socket)-Schnittstelle. Siehe auch Option *-socketTraceLevel* auf Seite 78.

TRACE=*STD
Entspricht der Angabe 0 bzw. dem Wert in der Installationsdatei

TRACE=<integer 0..10>
Socket-Trace-Level

MAXIMUM-CONNECTIONS=
Maximale Anzahl an Verbindungen, die der Server bedienen soll. Siehe auch Option *-maxConn* auf Seite 76.

MAXIMUM-CONNECTIONS=*STD
Entspricht der Angabe 15 bzw. dem Wert in der Installationsdatei.

MAXIMUM-CONNECTIONS=<integer 1..900>
Maximale Anzahl an Verbindungen, die der Server bedienen soll.

STATION-ID=
Anzahl der Stellen, mit denen der Name des fernen Rechners bzw. der Job-Name des FTP-Servers im Datenstationsnamen berücksichtigt werden soll. Siehe auch Option *-DSSidLength* auf Seite 77.

STATION-ID=*STD
Entspricht der Angabe 0 bzw. dem Wert in der Installationsdatei.

STATION-ID=<integer 0..6>
Anzahl der Stellen, mit denen der Name des fernen Rechners bzw. der Job-Name des FTP-Servers im Datenstationsnamen berücksichtigt werden soll.

TRANSFER-CPU-TIME=
CPU-Zeit, die für den Job-Lauf des Child-Prozesses zur Verfügung steht. Siehe auch Option *-logonExtension* auf Seite 75.

TRANSFER-CPU-TIME=*STD
Entspricht der Angabe NTL bzw. dem Wert in der Installationsdatei.

TRANSFER-CPU-TIME=<integer 1..32767>
CPU-Zeit, die für den Job-Lauf des Child-Prozesses zur Verfügung steht.

TRANSFER-JOB-CLASS=
Die Jobklasse, in welche die Child-Prozess-Jobs eingereiht werden sollen. Siehe auch Option *-logonExtension* auf Seite 75.

TRANSFER-JOB-CLASS=*STD
Entspricht der Standard-Jobklasse des Systems bzw. dem Wert in der Installationsdatei.

TRANSFER-JOB-CLASS=<name 1..8>
Voreinstellung: Standard-Dialog-Jobklasse auf dem System

TIMEOUT-VALUE=
Zeit, nach der die Verbindung zwischen Client und Server abgebrochen wird, falls in dem angegebenen Zeitraum keine Aktivität zwischen Client und Server beobachtet wurde. Siehe auch Option *-timeout* auf Seite 76.

TIMEOUT-VALUE=*STD
Entspricht der Standardeinstellung von 3600 Sekunden.

TIMEOUT-VALUE=<integer 1..32767>
Timeout-Wert in Sekunden.

SYSTEM-EXIT-LEVEL=
Mit einem Wert ungleich 0 wird der FTP-System-Exit eingeschaltet. Wenn dabei auch FTAC-SUPPORT=*YES ist, wird der System-Exit nur bei den Unterereignissen FTPBYE und FTPCMDE aufgerufen, ansonsten bei allen Unterereignissen. Siehe auch Option *-systemExit* auf Seite 79.

SYSTEM-EXIT-LEVEL=*STD
Entspricht der Angabe 0 bzw. dem Wert in der Installationsdatei.

SYSTEM-EXIT-LEVEL=<integer 0..3>
System-Exit-Level

FTAC-SUPPORT=
Gibt an, ob der FTP-Server die FTAC-Funktionalität nutzen soll oder nicht.

FTAC-SUPPORT=*STD
Voreinstellung: *NO oder Wert in der angegebenen Installationsdatei INSTALLATION-FILE.

FTAC-SUPPORT=*NO(...)
Die Berechtigungsprüfung durch Nutzung der FTAC-Funktionalität wird nicht durchgeführt.

FTAC-SUPPORT=*YES(...)
Die Berechtigungsprüfung wird unter Nutzung der FTAC-Funktionalität durchgeführt.

LEVEL=
FTAC-Level: Stufe, auf der die FTAC-Berechtigungsprüfung durchgeführt wird.
Wert 1 bedeutet, dass der Zugang über eine Dialogkennung nicht von FTAC überprüft wird, aber zusätzlich ein Zugang mit einer FTAC-Transfer-Admission möglich ist.
Wert 2 bedeutet, dass auch der Zugang über eine Dialogkennung von FTAC überprüft wird (anhand des jeweiligen Berechtigungssatzes). Ab Wert 1 ist u.U. kein Zugang mit der Kennung TSOS möglich. Siehe auch Options *-allowTSOSLogin* auf Seite 82 und *-FTAClevel* auf Seite 72.

LEVEL=*STD
Dies entspricht dem Wert 1.

LEVEL=<integer 1..2>
FTAC-Level

JOB-CLASS=
Job-Klasse, in der die Child-Prozesse laufen sollen. Stellen Sie sicher, dass in dieser Job-Klasse Enter-Jobs mit dem Parameter SCHEDULING-TIME=*PARAMETERS(START=*IMMEDIATELY) gestartet werden dürfen. In dieser Jobklasse laufen nur Jobs, die im Rahmen einer Anmeldung per FTAC-Transfer-Admission angestartet werden. Siehe auch Option *-childJobClass* auf Seite 74.

JOB-CLASS=*STD
Entspricht der Standard-Batch-Job-Klasse des aktuellen Systems.

JOB-CLASS=<name 1..8>
Name der Job-Klasse

ENTER-FILE=
Name der Enter-Datei, die den Child-Prozess startet. Siehe auch Option *-childEnterJob* auf Seite 74.

ENTER-FILE=*STD
Entspricht der Datei SYSENT.TCP-IP-AP.*nnn*.FTPDC.

ENTER-FILE=<filename 1..54_without-generation-version>
Name der Enter-Datei, die den Child-Prozess startet.

SERVER-INFORMATION-FILE=
Name der Datei für den Austausch von Informationen zwischen Server und Child-Prozess. In dieser Datei wird z.B. die Portnummer hinterlegt, unter der der Server für den Child-Prozess erreichbar ist. Siehe auch Option *-serverInfoFile* auf Seite 73.

SERVER-INFORMATION-FILE=*STD
Entspricht der Datei SYSDAT.TCP-IP-AP.*nnn*.SI

SERVER-INFORMATION-FILE=<filename 1..54_without-generation-version>
Name der Datei für den Informationsaustausch zwischen Server und Child-Prozess.

FTAC-USERID=
Kennung, die anstatt $FTAC eingegeben werden kann, um beim Login anzuzeigen, dass die Zugangsberechtigungsprüfung über eine FTAC-Transfer-Admission erfolgen soll. Siehe auch Option *-FTACuserId* auf Seite 75.

FTAC-USERID=*STD
Entspricht der Voreinstellung $FTAC.

FTAC-USERID=<name 1..8>
FTAC-User id

TLS-SUPPORT=
Legt fest, ob die TLS/SSL-Absicherung für den FTP-Server aktiviert wird.

TLS-SUPPORT=*STD
Voreinstellung: *NO.

TLS-SUPPORT=*NO
Der FTP-Server führt keine Absicherung der Verbindungen mittels TLS durch.

TLS-SUPPORT=*YES(...)
Der FTP-Server führt (prinzipiell) eine Absicherung der Verbindungen mittels TLS durch.

PROTOCOL=
Siehe Option *-tlsProtocol* auf Seite 86.

PROTOCOL=*STD
Voreinstellung: ALL –SSLv2

PROTOCOL=<text 1..80>
Spezifikation des zu verwendenden TLS/SSL-Protokolls.

CIPHER-SUITE=
Siehe Option *-tlsCipherSuite* auf Seite 87.

CIPHER-SUITE=*STD
Voreinstellung: ALL:!EXP:!ADH

CIPHER-SUITE=<text 1..80_with-lower-case>
Spezifikation der zu verwendenden Verschlüsselungsalgorithmen.

RSA-CERTIFICATE-FILE=
Siehe Option *-tlsRSAcertificateFile* auf Seite 87.

RSA-CERTIFICATE-FILE=*STD
Voreinstellung: *NONE

RSA-CERTIFICATE-FILE=*NONE
Es wird keine RSA-Zertifikats-Datei angegeben.

RSA-CERTIFICATE-FILE=<filename 1..54_without-generation-version>
Name der RSA-Zertifikats-Datei.

RSA-KEY-FILE=
Siehe Option *-tlsRSAkeyFile* auf Seite 88.

RSA-KEY-FILE=*STD
Voreinstellung: *NONE

RSA-KEY-FILE=*NONE
Es wird keine RSA-Schlüssel-Datei angegeben.

RSA-KEY-FILE=<filename 1..54_without-generation-version>
Name der RSA-Schlüssel-Datei.

DSA-CERTIFICATE-FILE=
Siehe Option *-tlsDSAcertificateFile* auf Seite 89.

DSA-CERTIFICATE-FILE=*STD
Voreinstellung: *NONE

DSA-CERTIFICATE-FILE=*NONE
Es wird keine DSA-Zertifikats-Datei angegeben.

DSA-CERTIFICATE-FILE=<filename 1..54_without-generation-version>
Name der DSA-Zertifikats-Datei.

DSA-KEY-FILE=
Siehe Option *-tlsDSAkeyFile* auf Seite 90.

DSA-KEY-FILE=*STD
Voreinstellung: *NONE

DSA-KEY-FILE=*NONE
Es wird keine DSA-Schlüssel-Datei angegeben.

DSA-KEY-FILE=<filename 1..54_without-generation-version>
Name der DSA-Schlüssel-Datei.

CA-CERTIFICATE-FILE=
Siehe Option *-tlsCACertificateFile* auf Seite 92.

CA-CERTIFICATE-FILE=*STD
Voreinstellung: *NONE

CA-CERTIFICATE-FILE=*NONE
Es wird keine CA-Zertifikats-Datei angegeben.

CA-CERTIFICATE-FILE=<filename 1..54_without-generation-version>
Name der CA-Zertifikats-Datei.

CLIENT-CA-FILE=
Siehe Option *-tlsAcceptableClientCAFile* auf Seite 93.

CLIENT-CA-FILE=*STD
Voreinstellung: *NONE

CLIENT-CA-FILE=*NONE
Es wird keine Datei angegeben.

CLIENT-CA-FILE=<filename 1..54_without-generation-version>
Name der Datei mit den Zertifikaten der akzeptierten CAs.

CERT-CHAIN-FILE=
Siehe Option *-tlsCertificateChainFile* auf Seite 91.

CERT-CHAIN-FILE=*STD
Voreinstellung: *NONE

CERT-CHAIN-FILE=*NONE
Es wird keine CA-Zertifikatsketten-Datei angegeben.

CERT-CHAIN-FILE=<filename 1..54_without-generation-version>
Name der CA-Zertifikatsketten-Datei.

CA-REVOCATION-FILE=
Siehe Option *-tlsCArevocationFile* auf Seite 94.

CA-REVOCATION-FILE=*STD
Voreinstellung: *NONE

CA-REVOCATION-FILE=*NONE
Es wird keine CA-Widerruf-Datei angegeben.

CA-REVOCATION-FILE=<filename 1..54_without-generation-version>
Name der CA-Wiederruf-Datei.

RANDOM-FILE=
Siehe Option *-tlsRandFile* auf Seite 98.

RANDOM-FILE=*STD
Voreinstellung: SYSDAT.TCP-IP-AP.*nnn*.FTPD.RAND

RANDOM-FILE=<filename 1..54_without-generation-version>
Name der Zufallszahlen-Datei.

SSL-LIBRARY=
Siehe Option *-tlsOpenSSLlibName* auf Seite 98.

SSL-LIBRARY=*STD
Voreinstellung: LMS-Bibliothek, auf die die IMON Logical-ID SYSLNK verweist.

SSL-LIBRARY=*NONE
Es wird keine LMS-Bibliothek angegeben.

SSL-LIBRARY=<filename 1..54_without-generation-version>
Name der LMS-Bibliothek, die den OpenSSL-Nachlade-Modul enthält.

VERIFY-CLIENT=
Siehe Option *-tlsVerifyClient* auf Seite 94.

VERIFY-CLIENT=*STD
Voreinstellung: *NONE

VERIFY-CLIENT=*NONE
Es wird kein Zertifikat vom FTP-Client angefordert.

VERIFY-CLIENT=*OPTIONAL
Es wird ein Zertifikat vom FTP-Client angefordert. Wird aber kein oder nur ein ungültiges Zertifikat zurückgeschickt, so wird dem FTP-Client dennoch der Zugang erlaubt.

VERIFY-CLIENT=*REQUIRE
Es wird ein Zertifikat vom FTP-Client angefordert. Wird kein oder nur ein ungültiges Zertifikat zurückgeschickt, dann wird dem FTP-Client der Zugang verweigert.

VERIFY-DEPTH=
Siehe Option *-tlsVerifyDepth* auf Seite 95.

VERIFY-DEPTH=*STD
Voreinstellung: 1

VERIFY-DEPTH=<integer 1..32767>
Anzahl der Zertifikate zwischen dem Client-Zertifikat und dem Zertifikat, das dem FTP-Server bekannt ist (inklusive letzterem).

SEC-CONTROL-CONN=
Siehe Option *-tlsSecureControlConnection* auf Seite 96.

SEC-CONTROL-CONN=*STD
Voreinstellung: *OPTIONAL

SEC-CONTROL-CONN=*NONE
Die Kontrollverbindung wird nie mit TLS abgesichert. Entsprechende Anforderungen des Client werden abgewiesen.

SEC-CONTROL-CONN=*OPTIONAL
Die Kontrollverbindung wird abgesichert, wenn der Client es anfordert.

SEC-CONTROL-CONN=*REQUIRE
Es wird kein Login über eine nicht abgesicherte Control-Verbindung zugelassen.

SEC-DATA-CONN=
Siehe Option *-tlsSecureDataConnection* auf Seite 97.

SEC-DATA-CONN=*STD
Voreinstellung: *OPTIONAL

SEC-DATA-CONN=*NONE
Die Datenverbindung wird nie mit TLS abgesichert. Entsprechende Anforderungen des Client werden abgewiesen.

SEC-DATA-CONN=*OPTIONAL
Die Datenverbindung wird abgesichert, wenn der Client es anfordert.

SEC-DATA-CONN=*REQUIRE
Es wird kein Datentransfer über eine nicht abgesicherte Datenverbindung zugelassen.

ACCOUNTING=
Gibt an, ob FTP-Abrechnungssätze erfasst werden sollen. Siehe auch Options *-acctActive* und *-acctFile* auf Seite 81.

ACCOUNTING=*STD
Voreinstellung: *NO

ACCOUNTING=*NO
Eine Erfassung der Abrechnungssätze wird nicht durchgeführt.

ACCOUNTING=*YES(...)
Es werden Abrechnungssätze erfasst.

FILE=
Name der Abrechnungsdatei.

FILE=*STD
Dies entspricht der Datei SYSDAT.TCP-IP-AP.*nnn*.FTPD.ACCOUNTING

FILE=<filename 1..54_without-generation-version>
Name der Abrechnungsdatei.

OPTION-FILE=
Datei, in der die folgenden Optionen hinterlegt werden.

OPTION-FILE=*STD
Voreinstellung: SYSDAT.TCP-IP-AP.*nnn*.FTPD.OPT

OPTION-FILE=<filename 1..54_without-generation-version>
Name der Option-Datei.

SELECTOR=
Selector für FTP-Exit Routinen. Siehe auch Option *-convSelector* auf Seite 78.

SELECTOR=*STD
Voreinstellung: Keine Exits

SELECTOR=<text 1..511>
Spezifiziert den Selektor für die FTP-Exit-Routinen.

INITIAL-COMMANDS=
Siehe Option *-initialChildCmds* auf Seite 80.

INITIAL-COMMANDS=*STD
Es werden keine Kommandos zum Child-Prozess gesendet.

INITIAL-COMMANDS=<c-string 2..256>
Spezifiziert die an den Child-Prozess zu sendenden Kommandos.

PORT-NUMBER=
Portnummer, unter der der FTP-Server gestartet wird. Siehe auch Option *-portNumber* auf Seite 77.

PORT-NUMBER=*STD
Voreinstellung: 21

PORT-NUMBER=<integer 0..32767>
Spezifiziert die Portnummer, unter der der FTP-Server gestartet wird.

SERVER-ENTER-FILE=
Name der Start-Datei für den FTP-Server.

SERVER-ENTER-FILE=*STD
Voreinstellung: SYSENT.TCP-IP-AP.*nnn*.FTPD

SERVER-ENTER-FILE=<filename 1..54_without-generation-version>
Spezifiziert den Namen der Start-Datei für den FTP-Server.

LOGGING-FILE=
Name der Protokoll-Datei für den FTP-Server.

LOGGING-FILE=*STD
Voreinstellung: SYSOUT.TCP-IP-AP.*nnn*.FTPD

LOGGING-FILE=<filename 1..54_without-generation-version>
Spezifiziert den Namen der Protokoll-Datei für den FTP-Server.

ALLOW-TSOS-LOGIN=
Siehe Option *-allowTsosLogin* auf Seite 82.

ALLOW-TSOS-LOGIN=*STD
Das Verhalten wird wie in älteren Versionen von der Level-Einstellung bei der FTAC-Unterstützung bestimmt.

ALLOW-TSOS-LOGIN=*NO
Ein Login-Versuch mit der Kennung TSOS wird abgewiesen.

ALLOW-TSOS-LOGIN=*YES
Ein Login-Versuch mit der Kennung TSOS wird zugelassen.

ALLOW-TSOS-LOGIN=*TLS
Ein Login-Versuch mit der Kennung TSOS wird nur über eine TLS/SSL-gesicherte Verbindung zugelassen.

TVFS=
Aktiviert oder Deaktiviert das TVFS (Trivial Virtual File System), siehe Option *-TVFS* auf Seite 100.

TVFS=*STD
Voreinstellung: *NO

TVFS=*NO
TVFS ist nicht aktiviert.

TVFS=*YES
TVFS ist aktiviert, d.h. DVS- und POSIX-Dateien sind über ein einheitliches, POSIX ähnliches Dateisystem zugreifbar.

4.3 Konfiguration von FTP via Option-Datei

Bei der Ausführung des Kommandos SET-FTP-TELNET-PARAMETERS (siehe Seite 42) wird eine Option-Datei erzeugt, in der die einzelnen FTP-Server-Parameter als Options abgelegt sind. Der Standarddateiname der Option-Datei lautet:

SYSDAT.TCP-IP-AP.*nnn*.FTPD.OPT

Unter $TSOS, der Ablaufkennung.

Wenn eine Datei mit diesem Namen in der Ablaufkennung des FTP-Servers existiert, wird sie beim Start des FTP-Servers über die Start-Datei des FTP-Servers (Standard-Dateiname: SYSENT.TCP-IP-AP.*nnn*.FTPD) ausgewertet, und der FTP-Server wird entsprechend konfiguriert.

Somit können Sie Änderungen der FTP-Server-Parameter via Option-Datei vornehmen, ohne erneut die Installation mithilfe des SET-FTP-TELNET-PARAMETERS-Kommandos starten zu müssen.

Wollen Sie eine Datei mit einem anderen Namen als Option-Datei verwenden, so geben Sie in der Start-Datei die folgende Option an:

-M *option-datei-name*

Option-Datei und Parameterzeilen-Options

Auch die bereits in früheren Versionen unterstützten Parameterzeilen-Options können Sie in der Option-Datei spezifizieren. Dabei können Sie wählen zwischen dem bekannten, aus einem Zeichen bestehenden Option-Namen und dem zugeordneten neuen, einprägsameren Namen, der aus mehreren Zeichen besteht.

Eine gemischte Anwendung von Option-Datei und Options in der Parameterzeile ist ebenfalls möglich. Dabei sind in der Parameterzeile auch weiterhin nur Option-Namen zulässig, die aus einem Zeichen bestehen. Wenn eine bestimmte Option sowohl in der Parameterzeile als auch in der Option-Datei angegeben ist, hat die in der Parameterzeile spezifizierte Option Vorrang.

Notation der Options in der Option-Datei

Die einzelnen Options müssen gemäß den folgenden Regeln in die Option-Datei eingetragen sein:

- Jede Option muss in einer eigenen Zeile stehen.
- Erstrecken sich die Argumente einer Option über mehrere Zeilen, dann muss jede fortzusetzende Zeile mit dem Fortsetzungszeichen „\“ abgeschlossen werden.
- Eine Zeile, die mit dem Zeichen „#“ in Spalte 1 beginnt, wird beim Einlesen ignoriert.
- Bei den Option-Namen wird Klein-/Groß-Schreibung nicht unterschieden.

Beschreibung der Options

Nachfolgend sind die einzelnen Options beschrieben:

- Bei den Options, die den bisher schon unterstützten Parameterzeilen-Options entsprechen, ist der aus einem Zeichen bestehende Name als Alias-Name angegeben.
- Die Options, die die TLS/SSL-Unterstützung im FTP-Server regeln, sind durch das Präfix „tls“ im Option-Namen gekennzeichnet.

-appPrefix | -A

Mit der Option *-appPrefix* wird ein Namens-Präfix spezifiziert. Dieser Namens-Präfix wird verwendet, um den Datenstationsnamen durch Anhängen einer laufenden Nummer zu bilden. Der vom Server für jeden Client gestartete Job erhält als Job-Namen diesen Namens-Präfix.

-appPrefix **-A**
<Job-Namens-Präfix>

<Job-Namens-Präfix>
Namens-Präfix
Voreinstellung: FTPSR

-FTAClevel | -B

Mit der Option *-FTAClevel* wird der FTAC-Level spezifiziert. Der FTAC-Level gibt die Stufe an, auf der die FTAC-Berechtigungsprüfung durchgeführt wird.

-FTAClevel **-B**
0 | **1** | **2**

0
FTAC wird nicht verwendet.
0 ist Voreinstellung

1
Der Zugang über eine Dialogkennung wird nicht von FTAC überprüft. Es ist aber zusätzlich ein Zugang mit einer FTAC-Transfer-Admission möglich.

2
Auch der Zugang über eine Dialogkennung wird von FTAC anhand des jeweiligen Berechtigungssatzes überprüft.

Wenn der FTAC-Level > 0 ist, dann ist u.U. kein Zugang mit der Kennung TSOS möglich (siehe Option *-allowTsosLogin* auf Seite 82).

-childName | -C

Mit der Option *-childName* wird der Pfad für den Aufruf des Child-Programms spezifiziert.

-childName **-C**
<Pfad-für-Child-Aufruf>

<Pfad-für-Child-Aufruf>
Pfad für den Aufruf des Child-Programms.
Voreinstellung: FTPDC

-debugLevel | -D

Mit der Option *-debugLevel* wird der Debug-Level spezifiziert. Der Debug-Level legt fest, ob bzw. welche Diagnose-Informationen zum FTP-Server-Ablauf in die Protokolldatei geschrieben werden.

-debugLevel **-D**
<integer 0..9>

<integer 0..9>
Debug-Level.
Mit „0“ wird die Protokollierung ausgeschaltet. Je größer der Wert ist, um so mehr Informationen werden in der Protokolldatei hinterlegt.
Voreinstellung: 0

-serverInfoFile | -E

Mit der Option *-serverInfoFile* wird eine Datei für den Austausch von Informationen zwischen Server- und Child-Prozess spezifiziert. In dieser Datei wird z.B. die Portnummer hinterlegt, unter der der Server für den Child-Prozess erreichbar ist. Dies gilt nur für Child-Prozesse, die im Rahmen eines Login über eine FTAC-Transfer-Admission gestartet werden.

-serverInfoFile **-E**
<Dateiname 1..54>

<Dateiname 1..54>
Name der Datei für den Informationsaustausch zwischen Server- und Child-Prozess.
Voreinstellung: SYSDAT.TCP-IP-AP.*nnn*.SI

-childEnterJob | -F

Mit der Option *-childEnterJob* wird der Name einer Enter-Datei spezifiziert, die den Child-Prozess startet, falls der Login über eine FTAC-Transfer-Admission erfolgt.

-childEnterJob **-F**
<Dateiname 1..54>

<Dateiname 1..54>
Name der Enter-Datei.
Voreinstellung: SYSENT.TCP-IP-AP.*nnn*.FTPDC

-childJobClass | -J

Mit der Option *-childJobClass* wird eine Job-Klasse spezifiziert, in der die Child-Prozesse ablaufen, die beim Login über eine FTAC-Transfer-Admission gestartet werden.

Stellen Sie sicher, dass in dieser Job-Klasse Enter-Jobs mit dem Parameter SCHEDULING-TIME=*PARAMETERS(START=*IMMEDIATELY) gestartet werden dürfen.

-childJobClass **-J**
<Job-Klasse 1..8>

<Job-Klasse 1..8>
Job-Klasse, in der die Child-Prozesse ablaufen.
Die Voreinstellung ist systemabhängig.

-FTACuserId | -K

Mit der Option *-FTACuserId* wird eine Pseudo-Kennung spezifiziert, mit der beim Login angezeigt wird, dass der Login nicht mit einer echten BS2000-Benutzerkennung erfolgen soll, sondern mit einer FTAC-Transfer-Admission.

-FTACuserId **-K**
<userId 1..8>

<userId 1..8>
Pseudokennung
Voreinstellung: $FTAC

-logonExtension | -L

Mit der Option *-logonExtension* können Zusatzangaben für das Logon-Kommando zum Starten des FTP-Childs spezifiziert werden. Insbesondere sind dies die Job-Klasse und das CPU-Limit des Dialog-Jobs.

-logonExtension **-L**
<logonExt 1..511>

<logonExt 1..511>
Zusatzangaben für das Logon-Kommando zum Starten des FTP-Childs.
Die Voreinstellung ist systemabhängig.

-maxConn | -N

Mit der Option *-maxConn* wird die maximale Anzahl an Verbindungen spezifiziert, die der FTP-Server gleichzeitig bedienen soll.

-maxConn **-N**
<integer 1..900>

<integer 1..900>
Maximale Anzahl an Verbindungen, die der FTP-Server gleichzeitig bedienen soll.
Voreinstellung: 15

-timeout | -O

Mit der Option *-timeout* wird das Timeout-Intervall eingestellt für die Verbindung zwischen FTP-Server und FTP-Client. Wenn in der angegebenen Zeit zwischen Server und Client keine Aktivität festgestellt wird, wird die Verbindung abgebrochen.

-timeout **-O**
<Anzahl Sekunden>

<Anzahl Sekunden>
Timeout-Intervall in Sekunden.
Voreinstellung: 3600

-portNumber | -P

Mit der Option *-portNumber* wird die Portnummer spezifiziert, unter der der FTP-Server erreichbar ist.

-portNumber **-P**
<integer 1..65535>

<integer 1..65535>
Portnummer, unter der der FTP-Server erreichbar ist.
Voreinstellung: 21

-DSSidLength | -S

Mit der Option *-DSSidLength* wird die Anzahl Stellen festgelegt, mit denen der Name des fernen Rechners bzw. der Job-Name des FTP-Servers im Datenstationsnamen berücksichtigt werden soll.

-DSSidLength **-S**
<integer 0..6>

<integer 0..6>
Anzahl der zu berücksichtigenden Stellen.
Voreinstellung: 0

-socketTraceLevel | -T

Mit der Option *-socketTraceLevel* wird der Socket-Trace-Level spezifiziert. Der Socket-Trace-Level gibt an, ob bzw. welche Diagnose-Informationen des TCP/IP-(Socket)-Systems in die Protokolldatei geschrieben werden.

-socketTraceLevel **-T**
<integer 0..10>

<integer 0..10>
Socket-Trace-Level
Mit „0“ wird die Protokollierung ausgeschaltet. Je größer der Wert ist, desto mehr Informationen werden in der Protokolldatei hinterlegt.
Voreinstellung: 0

-convSelector | -U

Mit der Option *-convSelector* können benutzerdefinierte Exit-Routinen des FTP-Servers aktiviert bzw. deaktiviert werden. Näheres zur Selektor-Definition finden Sie im Abschnitt „Exit-Mechanismen für FTP-Server und FTP-Client“ auf Seite 131.

-convSelector **-U**
<selektor-definition 1..511>

<Selektor-Definition 1..511>
Selektor-Definition
Voreinstellung: <leerer String>, d.h. keine benutzerdefinierten Exit-Routinen.

-verbose | -V

Die Option *-verbose* ist die Kurzform für *-debugLevel 1* und *-socketTraceLevel 1*.

-verbose **-V**

-systemExit | -X

Mit der Option *-systemExit* wird der System-Exit aktiviert bzw. deaktiviert.

-systemExit **-X**
0 | **1**

0
System-Exit wird deaktiviert.
0 ist Voreinstellung.

1
System-Exit wird aktiviert.

-initialChildCmds | -Z

Mit der Option *-initialChildCmds* können Sie Kommandos spezifizieren, die direkt nach dem Start des Child-Programms zu diesem geschickt werden. Hierfür eignen sich vor allem Kommandos, die dauerhafte Einstellungen vornehmen, wie die RFC 959-Kommandos *type*, *stru* und *mode* sowie die BS2000-proprietären Kommandos *ftyp*, *setc*, *modc*, *sfil* und *cmod*. In speziellen Fällen kann auch die Verwendung der RFC 959-Kommandos *dele* und *cwd* sowie des BS2000-proprietären Kommandos *file* sinnvoll sein. Die BS2000-proprietären Kommandos sind im Handbuch „interNet Services Benutzerhandbuch“ beschrieben. Beachten Sie: Im Gegensatz zur dort beschriebenen Verwendungsweise darf im Option-Argument den proprietären Kommandos kein „site“ vorangestellt werden. Die einzelnen Kommandos im Kommando-String sind jeweils durch `\n` bzw. `\N` abzuschließen.

Die Option *-initialChildCmds* können Sie z.B. verwenden, um Voreinstellungen zu verändern. So können Sie mit `-initialChildCmds FTYP text\nSFIL pademptyrec on\n` die FTYP-Voreinstellung auf `text` (dies ist die Voreinstellung älterer FTP-Versionen) setzen und das Auffüllen von leeren SAM-Sätzen mit einem Leerzeichen aktivieren.

-initialChildCmds **-Z**
<string 2..511>

<string 2..511>
String, der die Kommandos enthält.
Voreinstellung: <leerer String>, d.h. kein Kommando.

-acctActive

Mit der Option *-acctActive* wird die Erfassung der FTP-Abrechnungsdaten (FTP-Accounting) ein- bzw. ausgeschaltet.

-acctActive
ON | **OFF**

ON
Das FTP-Accounting wird eingeschaltet.

OFF
Das FTP-Accounting wird ausgeschaltet.
OFF ist Voreinstellung.

-acctFile

Mit der Option *-acctFile* wird der Name der Abrechnungsdatei für das FTP-Accounting spezifiziert, in der die Abrechnungssätze hinterlegt werden. Die Abrechnungsdatei ist eine SAM-Datei mit variabler Satzlänge.

Wenn bereits eine Abrechnungsdatei dieses Namens für das FTP-Accounting existiert, wird diese beim Start des FTP-Servers fortgeschrieben.

-acctFile
<Name der Abrechnungsdatei 1..54>

<Name der Abrechnungsdatei 1..54>
Name der Abrechnungsdatei für das FTP-Accounting.
Voreinstellung: SYSDAT.TCP-IP-AP.*nnn*.FTPD.ACCOUNTING

-allowTsosLogin

Mit der Option *-allowTsosLogin* wird spezifiziert, ob bzw. unter welchen Bedingungen ein Login unter der Benutzerkennung TSOS möglich ist.

Bisher wurde der Login über die Benutzerkennung TSOS abgewiesen, wenn die FTAC-Unterstützung aktiviert wurde (`-FTAClevel > 0`, siehe Seite 72).

Mit der Option *-allowTsosLogin* können Sie nun unabhängig von der Option *-FTAClevel* spezifizieren, ob ein TSOS-Login möglich ist:

- Wenn Sie die Option *-allowTsosLogin* nicht verwenden, hängt es wie bei interNet Services V2.0 von der Option *-FTACLevel* ab, ob ein TSOS-Login möglich ist.
- Wenn Sie die Option *-allowTsosLogin* verwenden, gelten unabhängig von einer FTAC-Aktivierung die nachfolgend beschriebenen argumentabhängigen Bedingungen.

-allowTsosLogin
NO | TLS | YES

NO
Ein Login-Versuch unter TSOS wird in jedem Fall abgewiesen.

TLS
Bei der Angabe „`TLS`“ ist ein Login nur über eine TLS/SSL-gesicherte Verbindung möglich.

YES
Es gibt keine Restriktionen für den TSOS-Login.

Aus Sicherheitsgründen sollten nur die Werte „NO“ oder „TLS“ verwendet werden. Dabei ist „NO“ zu bevorzugen.

-defaultFTACsecurityLevel

Mit der Option *-defaultFTACsecurityLevel* wird eine FTAC-Sicherheitsstufe definiert, die den FTP-Partnern zugeordnet werden soll. Ist in einem Berechtigungssatz ein kleinerer Wert angegeben, dann steht die jeweils zugehörige Grundfunktion FTP-Partnern nicht zur Verfügung.

Wird also beispielsweise dem Gros der FT-Partner die Sicherheitsstufe 80 zugeordnet und sollen FTP-Partner Zugriff auf die gleichen Grundfunktionen wie diese FT-Partner bekommen, dann sollte *-defaultFTACsecurityLevel 80* verwendet werden.

-defaultFTACsecurityLevel
<integer 1..100>

<integer 1.100>
Sicherheitsstufe, die FTP-Partnern zugeordnet werden soll.
Voreinstellung: 100

-disableSiteExecCommand

Mit der Option *-disableSiteExecCommand* wird spezifiziert, ob der Server das proprietäre FTP-Protokoll-Kommando *SITE EXEC* unterstützt. Dieses Kommando ermöglicht es dem FTP-Client-Benutzer, BS2000-Kommandos auf dem Server auszuführen und birgt dadurch ein recht hohes Missbrauchspotential. Daher wurde dieses Kommando bereits bisher bei der Aktivierung der FTAC-Unterstützung (`-FTAClevel > 0`, siehe Seite 72) deaktiviert, während es in den restlichen Fällen noch unterstützt wurde.

Mit der Option *-disableSiteExecCommand* können Sie nun das Kommando *SITE EXEC* unabhängig von der Option *-FTAClevel* aktivieren bzw. deaktivieren:

- Wenn Sie die Option *-disableSiteExecCommand* nicht verwenden, dann hängt die Verwendbarkeit des Kommandos wie in interNet Services < V3.0A von der Option *-FTAClevel* ab.
- Wenn Sie die Option *-disableSiteExecCommand* mit dem Argument „YES“ verwenden, ist das Kommando in keinem Fall verfügbar.
- Wenn Sie die Option *-disableSiteExecCommand* mit dem Argument „NO“ verwenden, ist das Kommando in jedem Fall verfügbar.

-disableSiteExecCommand
NO | **YES**

NO
Die Unterstützung des *SITE EXEC*-Kommandos wird nicht deaktiviert.

YES
Die Unterstützung des *SITE EXEC*-Kommandos wird deaktiviert.

-disableSizeCommand

Mit der Option *-disableSizeCommand* wird festgelegt, ob der Server das Kommando *SIZE* unterstützt. Das *SIZE*-Kommando ist im Handbuch „interNet Services Benutzerhandbuch“ beschrieben.

Ein Problem im Zusammenhang mit dem *SIZE*-Kommando besteht darin, dass das *SIZE*-Kommando die zu untersuchende Datei i.A. komplett lesen muss, bevor es eine korrekte Meldung über die Dateigröße senden kann. Somit ist die Ausführung des *SIZE*-Kommandos ressourcen- und zeitintensiv, insbesondere bei sehr großen Dateien.

Daraus resultieren

- eine Schwäche in Bezug auf „Denial of Service“-Angriffe,
- Probleme mit manchen FTP-Clients.

Diese Clients führen zu Beginn eines Transfers das *SIZE*-Kommando aus, um einen Fortschrittsbalken mit dem relativen Transferfortschritt anzeigen zu können. Abgesehen von der Frage, ob dieser Fortschrittsbalken ein zweifaches Lesen der betreffenden Datei durch den Server rechtfertigt, entsteht zumindest bei einem der Clients das Problem, dass dieser nach Ablauf einer festen, vom Anwender nicht veränderbaren Zeit, ohne Rückmeldung vom Server die Verbindung abbricht. Somit ist dieser Client für den Transfer sehr großer Dateien nicht geeignet. Dabei ist zu beachten, dass der Client das *SIZE*-Kommando selbst dann absetzt, wenn der Fortschrittsbalken deaktiviert ist.

Wenn die Notwendigkeit besteht, solche Clients zu unterstützen, empfiehlt es sich, das *SIZE*-Kommando mit der Option *-disableSizeCommand* zu deaktivieren. Dabei ist zu beachten, dass die Client-Kommandos *reget* und *reput* mit dem betreffenden Server u.U. nicht mehr ausgeführt werden können.

-disableSizeCommand
NO | **YES**

NO
Die Unterstützung des *SIZE*-Kommandos wird nicht deaktiviert.
NO ist Voreinstellung.

YES
Die Unterstützung des *SIZE*-Kommandos wird deaktiviert.

-tlsProtocol

OpenSSL unterstützt das SSL-Protokoll der Version 3 sowie das TLS-Protokoll in den Versionen 1, 1.1 und 1.2. Mit der Option *-tlsProtocol* können einige dieser Protokolle selektiv aktiviert werden.

-tlsProtocol
[**+** | **-**] {**SSLv3** | **TLSv1** | **TLSv1**.1 | **TLSv1**.2 | **All** } ...

+
Das nachfolgend spezifizierte Protokoll ist zugelassen.

-
Das nachfolgend spezifizierte Protokoll ist nicht zugelassen.

Wenn weder „+“ noch „-“ angegeben werden, hat dies dieselbe Wirkung wie die Angabe von „+“.

SSLv3
SSL-Protokoll der Version 3

Das SSL-Protokoll in der Version 3 weist einige sicherheitstechnische Mängel auf und sollte nach Möglichkeit nicht verwendet werden.

TLSv1
TLS-Protokoll der Version 1

TLSv1.1
TLS-Protokoll der Version 1.1

TLSv1.2
TLS-Protokoll der Version 1.2

ALL
Alle Protokolle sollen aktiviert werden.

All -SSLv3 ist Voreinstellung.

Beispiel

Die Angaben `-tlsProtocol TLSv1 TLSv1.1 TLSv1.2` und `-tlsProtocol All -SSLv3` haben dieselbe Wirkung, solange keine Unterstützung für die zukünftige TLS-Protokollversion 1.3 zum FTP hinzugefügt wird.

-tlsCipherSuite

Mit der Option *-tlsCipherSuite* wird eine Verschlüsselungsverfahren-Vorzugsliste spezifiziert. Falls diese Option nicht angegeben wird, wird eine voreingestellte Vorzugsliste verwendet.

-tlsCipherSuite
<Spezifikation>

<Spezifikation>
Spezifikation in einer Verschlüsselungsverfahren-Vorzugsliste, siehe Kapitel „Spezifikation einer Vorzugsliste für Verschlüsselungsverfahren“ auf Seite 383.
ALL: !EXP: !ADH:!RC4 ist Voreinstellung.

-tlsRSAcertificateFile

Mit der Option *-tlsRSAcertificateFile* wird eine Datei spezifiziert, die das RSA-basierte X.509-Server-Zertifikat im PEM-Format enthält. Diese Datei kann auch den privaten RSA-Server-Schlüssel enthalten. In der Regel werden aber Zertifikat und Schlüssel in getrennten Dateien abgelegt. In diesem Fall wird die Schlüsseldatei mithilfe der Option *-tlsRSAkeyFile* (siehe Seite 88) spezifiziert.

-tlsRSAcertificateFile
<dateiname 1 .. 54> | ***NONE**

<dateiname 1 .. 54>
Name der Datei, die das RSA-basierte X.509-Server-Zertifikat im PEM-Format enthält.

***NONE**
Es wird keine Datei mit RSA-Zertifikaten verwendet.
*NONE ist Voreinstellung.

-tlsRSAkeyFile

Mit der Option *-tlsRSAkeyFile* wird eine Datei spezifiziert, die den privaten RSA-Server-Schlüssel im PEM-Format enthält.

Wenn sowohl X.509-Zertifikat als auch privater Server-Schlüssel innerhalb derselben Datei enthalten sind (siehe Option *-tlsRSAcertificateFile* auf Seite 87), braucht die Option *-tlsRSAkeyFile* nicht angegeben zu werden.

Da es möglich sein soll, den FTP-Server im unbedienten Betrieb automatisch hochzufahren, kann beim Server-Start keine Pass-Phrase für den privaten Server-Schlüssel eingegeben werden. Deshalb müssen Sie eine eventuell vorhandene Verschlüsselung des privaten Schlüssels mit Pass-Phrase entfernen. Verhindern Sie in diesem Fall unbedingt, dass unbefugte Personen auf diesen Schlüssel zugreifen können.

-tlsRSAkeyFile
<dateiname 1 .. 54> | ***NONE**

<dateiname 1 .. 54>
Name der Datei, die den privaten RSA-Server-Schlüssel enthält.

***NONE**
Es wird keine eigene Datei für den RSA-Server-Schlüssel verwendet.
*NONE ist Voreinstellung.

-tlsDSAcertificateFile

Mit der Option *-tlsDSAcertificateFile* wird eine Datei spezifiziert, die das DSA-basierte X.509-Server-Zertifikat im PEM-Format enthält. Diese Datei kann auch den privaten DSA-Server-Schlüssel enthalten. In der Regel werden aber Zertifikat und Schlüssel in getrennten Dateien abgelegt. In diesem Fall wird die Schlüsseldatei mithilfe der Option *-tlsDSAkeyFile* (siehe Seite 90) spezifiziert.

-tlsDSAcertificateFile
<dateiname 1 .. 54> | ***NONE**

<dateiname 1 .. 54>
Name der Datei, die das DSA-basierte X.509-Server-Zertifikat im PEM-Format enthält.

***NONE**
Es wird keine Datei mit DSA-Server-Zertifikaten verwendet.
*NONE ist Voreinstellung.

-tlsDSAkeyFile

Mit der Option *-tlsDSAkeyFile* wird eine Datei spezifiziert, die den privaten DSA-Server-Schlüssel im PEM-Format enthält.

Wenn sowohl X.509-Zertifikat als auch privater Server-Schlüssel innerhalb derselben Datei enthalten sind (siehe Option *-tlsDSAcertificateFile* auf Seite 89), braucht die Option *-tlsDSAkeyFile* nicht angegeben zu werden.

Da es möglich sein soll, den FTP-Server im unbedienten Betrieb automatisch hochzufahren, kann beim Server-Start keine Pass-Phrase für den privaten Server-Schlüssel eingegeben werden. Deshalb müssen Sie eine eventuell vorhandene Verschlüsselung des privaten Schlüssels mit Pass-Phrase entfernen. Verhindern Sie in diesem Fall unbedingt, dass unbefugte Personen auf diesen Schlüssel zugreifen können.

-tlsDSAkeyFile
<dateiname 1 .. 54> | ***NONE**

<dateiname 1 .. 54>
Name der Datei, die den privaten DSA-Server-Schlüssel enthält.

***NONE**
Es wird keine eigene Datei für den DSA-Server-Schlüssel verwendet.
*NONE ist Voreinstellung.

-tlsCertificateChainFile

Mit der Option *-tlsCertificateChainFile* wird eine Datei spezifiziert, in der alle Zertifikate abgelegt werden können, die für die Verifikation des Server-Zertifikats benötigt werden. Das erste Zertifikat in dieser Datei ist das Server-Zertifikat. Die restlichen Zertifikate müssen eine lückenlose Kette bilden, ausgehend vom Zertifikat der CA, die das Server-Zertifikat ausgestellt hat, bis hin zum Root-Zertifikat einer CA, das vom FTP-Client direkt verifiziert werden kann. Die Zertifikate der Kette müssen so sortiert sein, dass das Root-Zertifikat an letzter Stelle steht.

Die spezifizierte Datei wird nur benötigt, wenn das Server-Zertifikat von einer CA ausgestellt ist, die den FTP-Clients nicht bekannt ist und somit ohne Zusendung der Zertifikats-Kette von den FTP-Clients nicht verifiziert werden kann. Dieser Mechanismus setzt voraus, dass nicht gleichzeitig RSA- und DSA-Zertifikate für den Server genutzt werden, da die Datei für beide Varianten verwendet wird.

-tlsCertificateChainFile
<dateiname 1 .. 54> | ***NONE**

<dateiname 1 .. 54>
: Name der Datei, in der alle Zertifikate abgelegt sind, die für die Verifikation des Server-Zertifikats benötigt werden.

***NONE**
: Es wird keine Datei spezifiziert.
*NONE ist Voreinstellung.

-tlsCAcertificateFile

Mit der Option *-tlsCAcertificateFile* wird eine Datei spezifiziert, die die für die Authentifizierung des FTP-Clients erforderlichen CA-Zertifikate im PEM-Format enthält. Die einzelnen PEM-Zertifikate sind sequenziell in der Datei angeordnet.

Zum Hinzufügen oder Löschen von Zertifikaten können Sie die Datei mit einem beliebigen Text-Editor bearbeiten. Die einzelnen Zertifikate sind wie folgt in der Datei notiert:

```
-----BEGIN CERTIFICATE-----
< CA-Zertifikat in Base64-Codierung >
-----END CERTIFICATE-----
```

Text außerhalb dieser Sequenzen wird vom FTP-Server ignoriert und kann deshalb zum Kennzeichnen der Zertifikate verwendet werden, die wegen der ASN.1/Base64-Codierung in nicht lesbarer Form vorliegen.

-tlsCAcertificateFile
<dateiname 1 .. 54> | ***NONE**

<dateiname 1 .. 54>
: Name der Datei, die die für die Authentifizierung des FTP-Clients erforderlichen Zertifikate im PEM-Format enthält.

***NONE**
: Es wird keine Datei spezifiziert.
*NONE ist Voreinstellung.

-tlsAcceptableClientCAFile

Bei aktivierter Client-Authentifizierung teilt der Server beim TLS/SSL-Verbindungsaufbau dem Client die Namen derjenigen CAs mit, die er als Unterzeichner von Client-Zertifikaten akzeptiert. Diese CA-Namen werden den Zertifikaten entnommen, die in der durch die Option *-tlsAcceptableClientCAFile* spezifizierten Datei stehen. Die einzelnen Zertifikate im PEM-Format stehen dabei der Reihe nach in dieser Datei.

Zum Hinzufügen oder Löschen von Zertifikaten können Sie die Datei mit einem beliebigen Text-Editor bearbeiten. Die einzelnen Zertifikate sind wie folgt in der Datei notiert:

```
-----BEGIN CERTIFICATE-----
< CA-Zertifikat in Base64-Codierung >
-----END CERTIFICATE-----
```

Text außerhalb dieser Sequenzen wird vom FTP-Server ignoriert und kann deshalb zum Kennzeichnen der Zertifikate verwendet werden, die wegen der ASN.1/Base64-Codierung in nicht lesbarer Form vorliegen.

-tlsAcceptableClientCAFile
<dateiname 1 .. 54> | ***NONE**

<dateiname 1 .. 54>
Name der Datei.

***NONE**
Es wird keine Datei spezifiziert.
*NONE ist Voreinstellung.

-tlsCArevocationFile

Mit der Option *-tlsCArevocationFile* wird eine Datei spezifiziert, die die CRLs (Certificate Revocation List) der Zertifizierungsinstanzen (Certificate Authorithy, CA) enthält. Zertifikate, die von einer Zertifizierungsinstanz herausgegeben wurden, können durch Veröffentlichung einer so genannten Certificate Revocation List (CRL) für ungültig erklärt werden.

-tlsCArevocationFile
<dateiname 1 .. 54> | ***NONE**

<dateiname 1 .. 54>
Name der Datei, die die CRLs der Zertifizierungsinstanzen enthält.

***NONE**
Es wird keine Datei mit CRLs spezifiziert.
*NONE ist Voreinstellung.

-tlsVerifyClient

Mit der Option *-tlsVerifyClient* wird festgelegt, ob ein FTP-Client ein Zertifikat für den Server-Zugang vorweisen muss.

-tlsVerifyClient
NONE | **OPTIONAL | REQUIRE**

NONE
Der FTP-Server fordert kein Zertifikat vom FTP-Client an.
NONE ist Voreinstellung.

OPTIONAL
Der FTP-Server fordert den FTP-Client auf, sein Zertifikat zu senden. Wenn der Client dies aber verweigert oder ein ungültiges Zertifikat liefert, wird ihm dennoch der Zugang gewährt.

REQUIRE
Der FTP-Client muss ein gültiges Zertifikat übermitteln, da ihm andernfalls der Zugang verwehrt wird.

-tlsVerifyDepth

Mit der Option *-tlsVerifyDepth* wird die so genannte Verifizierungstiefe festgelegt, d.h. die Anzahl der maximal zulässigen Zertifikate zwischen dem FTP-Client-Zertifikat und dem Zertifikat, das dem FTP-Server bekannt ist.

Im Einzelnen ist zu beachten:

- Wird für die maximale Tiefe der Wert 1 spezifiziert (Default), dann muss das Client-Zertifikat direkt von einer dem FTP-Server bekannten Certificate Authority (CA) signiert worden sein, damit es akzeptiert wird.
- Wird die maximale Tiefe überschritten, dann wird die Verbindung abgebrochen, sofern nicht aufgrund von *-tlsVerifyClient NONE* (siehe Seite 94) oder *-tlsVerifyClient OPTIONAL* die zwingende Verifizierung des FTP-Client-Zertifikats ausgeschaltet ist.
- Die Spezifikation der Tiefe 0 ist nicht sinnvoll. In diesem Fall wären nur selbstsignierte Zertifikate zulässig.

-tlsVerifyDepth
<tiefe>

<tiefe>
Anzahl der maximal zulässigen Zertifikate zwischen dem FTP-Client-Zertifikat und dem Zertifikat, das dem FTP-Server bekannt ist.
Voreinstellung: 1

-tlsSecureControlConnection

Mit der Option *-tlsSecureControlConnection* wird festgelegt, ob die Kontrollverbindung vom FTP-Client zum FTP-Server mit TLS abgesichert werden soll.

-tlsSecureControlConnection
NONE | **OPTIONAL | REQUIRE**

NONE
Die Kontrollverbindung wird nie abgesichert, d.h. ein entsprechendes *AUTH*-Kommando (siehe Seite 56) wird mit einem negativen Returncode abgewiesen.
NONE ist Voreinstellung.

OPTIONAL
Die Kontrollverbindung wird auf Anforderung des Client abgesichert.

REQUIRE
Ein Login ist nur bei vorheriger Absicherung der Kontrollverbindung erlaubt.

-tlsSecureDataConnection

Mit der Option *-tlsSecureDataConnection* wird festgelegt, ob die Datenverbindung vom FTP-Client zum Server-Child mit TLS abgesichert werden soll.

Da eine Absicherung der Datenverbindung nur bei abgesicherter Kontrollverbindung möglich ist, macht es keinen Sinn, für *-tlsSecureControlConnection* (siehe Seite 96) eine schwächere Einstellung als für *-tlsSecureDataConnection* zu wählen. Deshalb wird gegebenenfalls *-tlsSecureControlConnection* automatisch auf den gleichen Wert angehoben wie *-tlsSecureDataConnection*.

-tlsSecureDataConnectionr
NONE | **OPTIONAL | REQUIRE**

NONE
Die Kontrollverbindung wird nie abgesichert, d.h. ein entsprechendes *PROT*-Kommando (siehe Seite 56) wird mit einem negativen Returncode abgewiesen.
NONE ist Voreinstellung.

Die Einstellung „NONE“ ist z.B. dann sinnvoll, wenn Sie nur die Möglichkeit anbieten wollen, das Passwort verschlüsselt zu übertragen, aber nicht bereit oder von der Serverleistung her in der Lage sind, eine Verschlüsselung der übertragenen Dateien anzubieten. Allerdings ist hierbei zu beachten, dass viele Windows-FTP-Clients nicht die Möglichkeit bieten, nur die Kontrollverbindung abzusichern.

OPTIONAL
Die Datenverbindung wird auf Anforderung des Client abgesichert.

REQUIRE
Ein Datentransfer ist nur bei vorheriger Absicherung der Datenverbindung erlaubt.

-tlsRandFile

Mit der Option *-tlsRandFile* wird eine Datei spezifiziert, aus der beim Server-Start Daten für die Initialisierung des Pseudo-Zufallszahlengenerators (PRNG) gelesen werden. Beim Beenden des Servers werden entsprechende Daten des PRNG in diese Datei geschrieben, um sie beim nächsten Server-Start zu verwenden.

Werden mehrere FTP-Server parallel betrieben, so muss für jeden Server jeweils eine eigene Datei definiert werden. Wenn das BS2000-Subsystem PRNGD aktiv ist, wird keine Datei für die Initialisierung des PRNG benötigt.

ACHTUNG!

Diese Datei darf für Unbefugte nicht zugreifbar sein.

-tlsRandFile
<dateiname 1 .. 54>

<dateiname 1 .. 54>
Name der Datei, die Daten für die Initialisierung des PRNG enthält.
Voreinstellung: SYSDAT.TCP-IP-AP.*nnn*.FTPD.RAND

-tlsOpenSSLlibName

Mit der Option *-tlsOpenSSLlibName* wird der Name der LMS-Datei spezifiziert, aus der die OpenSSL-Bibliothek nachgeladen wird. Eine vom Standardnamen abweichende Angabe kann z.B. erforderlich sein, wenn die OpenSSL-Bibliothek auch von anderen Produkten verwendet wird.

Das Nachladen der OpenSSL-Bibliothek lässt sich nämlich durch Cache-Speichern mithilfe von DAB beschleunigen. Bei Verwendung einer gemeinsamen OpenSSL-Bibliothek durch mehrere Produkte wird die Größe des verwendeten DAB-Puffers verringert.

-tlsOpenSSLlibName
<openssl-libname>

<openssl-libname>
Name der LMS-Datei, aus der die OpenSSL-Bibliothek nachgeladen werden soll.
Voreinstellung: LMS-Datei, auf die die IMON Logical-ID SYSLNK verweist.

-sizeCmdTimeLimit

Mit der Option *-sizeCmdTimeLimit* kann die Ausführungszeit des SIZE-Kommandos begrenzt werden. Die Motivation hierfür ist die gleiche wie bei der Option *-disableSizeCommand* (siehe Seite 85), nur dass hier das SIZE-Kommando nicht komplett deaktiviert wird, sondern die Ausführung des Kommandos abgebrochen wird, wenn der Resourcenverbrauch unverhältnismäßig groß wird.

-sizeCmdTimeLimit
<Anzahl Sekunden>

<Anzahl Sekunden>
Zeitlimit in Sekunden.
Voreinstellung: 60

-cmdBufSize

Mit der Option *-cmdBufSize* kann die Größe eines Puffers verändert werden, der für die Auflistung von Dateinamen verwendet wird. Bei Kennungen mit sehr vielen Dateien kann die Voreinstellung zu klein sein, sodass z.B. die Client-Kommandos *ls* oder *dir* mit Fehler abgebrochen werden. Als Anhaltspunkt gilt: der Puffer muss so groß sein wie die Ausgabe des entsprechenden FSTAT-Kommandos.

-cmdBufSize
<Anzahl Bytes>

<Anzahl Bytes>
Größe des Puffers.
Voreinstellung: 524 288

-TVFS

Mit der Option *-TVFS* können Sie das TVFS (Trivial Virtual File System) aktivieren oder deaktivieren.

-TVFS
ON | **OFF**

ON

TVFS ist aktiviert, d.h. DVS- und POSIX-Dateien sind über ein einheitliches, POSIX-ähnliches Dateisystem zugreifbar. Für weitere Informationen zum TVFS siehe Abschnitt „FTP-Client im BS2000“ im Benutzerhandbuch.
Wenn vor allem FTP-Clients mit graphischer Oberfläche genutzt werden, sollte man ON wählen. Wenn der jeweilige FTP-Client die Möglichkeit bietet, zu Sitzungsbeginn zusätzliche (proprietäre) Kommandos an den Server zu senden, dann kann das TVFS auch je nach Erfordernis für die jeweilige FTP-Sitzung mit dem BS2000-spezifischen FTP-Serverkommando *svfs* aktiviert bzw. deaktiviert werden. Details zu *svfs* siehe Abschnitt „FTP-SERVER im BS2000“ im „InterNet Services Benutzerhandbuch“.

OFF

TVFS ist nicht aktiviert.
OFF ist Voreinstellung, da hier bei DVS-Dateien die Möglichkeit besteht, Dateiteilqualifizierungsstufen als Pseudo-Unterverzeichnisse zu nutzen, was menschlichen Anwendern entgegenkommt.

4.4 FTP-Server starten und beenden

Mit den nachfolgend beschriebenen Kommandos können Sie den FTP-Server starten und beenden.

Diese Kommandos können auch via Operator-Konsole eingegeben werden.

4.4.1 FTP-Server starten

Folgende Voraussetzungen müssen erfüllt sein:

- Die /START-Kommandos sind nur unter Kennungen erlaubt, die das Privileg NET-ADMIN besitzen.
- Das Subsystem TCPIPAP muss vor /START-FTP-DEMON bzw. /START-TCP-IP-DEMON gestartet sein.
- Der FTP-Server muss unter der Kennung $TSOS gestartet werden.
- Für die Inbetriebnahme eines per FTAC gesicherten FTP-Servers ist zu beachten, dass beim Start des FTP-Servers FTAC betriebsbereit ist, also insbesondere die Subsysteme FTAC und FT aktiviert worden sind.

Die */START*-Kommandos für die Enter-Jobs lauten:

/START-TCP-IP-DEMON	Enter-Job für TCP-IP-AP
/START-FTP-DEMON	Enter-Job für den FTP-Server

Wenn Sie FTP und TELNET gleichzeitig starten wollen, verwenden Sie das Kommando START-TCP-IP-DEMON.

4.4.2 FTP-Server beenden

Die nachfolgend beschriebenen Kommandos zum Beenden von FTP-Server sind nur wirksam für Server ab interNet Services V3.0A.

Den FTP-Server beenden Sie mit dem Kommando STOP-FTP-DEMON.

STOP-FTP-DEMON
PORT-NUMBER=*STD-PORT/*ANY/<integer 0..32767>

PORT-NUMBER=
Angabe der Portnummer des zu beendenden FTP-Servers.
Voreinstellung: Es wird der FTP-Server mit der Standardportnummer 21 beendet.

PORT-NUMBER=*STD-PORT
Bewirkt dasselbe wie keine Angabe von Parametern.

PORT-NUMBER=*ANY
Es werden alle aktiven FTP-Server beendet.

PORT-NUMBER=<integer 0..32767>
Ein FTP-Server der angebenen Portnummer soll beendet werden.

4.4.3 Weitere FTP-Server-Tasks einrichten

In bestimmten Fällen kann es erwünscht sein, weitere FTP-Server zu betreiben, z.B. als Testversion. Zu diesem Zweck wird jeweils eine Kopie der Standard-Enter-Jobs SYSENT.TCP-IP-AP.*nnn*.FTPD und SYSENT.TCP-IP-AP.*nnn*.FTPDC erstellt.

Bei Konfiguration über eine Option-Datei muss eine zweite Option-Datei mit entsprechend geänderten Server-Options angelegt werden. Der Name dieser zweiten Option-Datei muss mit der Option *-M* in der Kopie von SYSENT.TCP-IP-AP.*nnn*.FTPD angegeben werden.

Die folgende Tabelle beschreibt die zwingend erforderlichen Änderungen, die für Server 2 durchzuführen sind. Die Änderungen sind durch **fette** Schrift hervorgehoben.

Server 1	**Server 2**
SYSENT.TCP-IP-AP.nnn.FTPD: /.FTPSR LOGON ... /SYSFILE SYSLST=$TSOS.SYSOUT.TCP-IP-AP.nnn.FTPD ... -B 0 \ -F $TSOS.SYSENT.TCP-IP-AP.nnn.FTPDC\ -E $TSOS.SYSDAT.TCP-IP-AP.nnn.SI\ -K $FTAC \ -J cccccccc\ -X 0\ -O 03600\ -A FTPSR\ -N 0015\ - D 0\ - T 0\ - S 0\ -C *MOD($TSOS.SYSLNK.TCP-IP-AP.nnn,FTPDC,RUN=ADV,PROG=ANY)	*SYSENT.TCP-IP-AP.nnn.FTPD2*: /.FTPS**2** LOGON ... /SYSFILE SYSLST=$TSOS.SYSOUT.TCP-IP-AP.nnn.FTPD**2** ... -B 0 \ -F $TSOS.SYSENT.TCP-IP-AP.nnn.FTPDC**2**\ -E $TSOS.SYSDAT.TCP-IP-AP.nnn.SI**2**\ -K $FTAC \ -J cccccccc\ -X 0\ -O 03600\ -A FTPS**2**\ -N 0015\ - D 0\ - T 0\ - S 0\ -C *MOD($TSOS.SYSLNK.TCP-IP-AP.nnn,FTPDC,RUN=ADV,PROG=ANY) \ **-P *nnn*** (***nnn*** ist Portnummer)
SYSENT.TCP-IP-AP.nnn.FTPDC: /.FTPSR LOGON ... -N\ -E $TSOS.SYSDAT.TCP-IP-AP.nnn.SI\ -D 0\ -T 0	*SYSENT.TCP-IP-AP.nnn.FTPDC**2***: /.FTPS2 LOGON ... -N\ -E $TSOS.SYSDAT.TCP-IP-AP.nnn.SI**2**\ -D 0\ -T 0
Start der Server-Task: /START-FTP-DEMON	Start der 2. Server-Task: /ENTER-JOB SYSENT.TCP-IP-AP.nnn.FTPD2
Verbindungsaufbau: /FTP open <rechner>	Verbindungsaufbau: /FTP open <rechner> ***nnn*** (*nnn* ist Portnummer)

Weitere Änderungen an den Server-Parametern sind möglich. Der Backslash „\“ hinter den Server-Anweisungen wird als Fortsetzungszeichen interpretiert. Hinter „\“ dürfen keine weiteren Zeichen stehen.

4.4.4 Shutdown

Weiterhin ist das Beenden der Server auch durch das Kommando */INFORM-PROGRAM 'shutdown',*TSN(<tsn>)* möglich. <*tsn*> bezeichnet die TSN der jeweiligen Server-Task.

4.4.5 Hinweise und Einschränkungen zum Starten und Beenden von FTP-Servern

Beim Starten und Beenden von Servern sind folgende Punkte zu beachten:

- Das Kommando START-FTP-DEMON ist nur wirksam, wenn die Start-Prozedur SYSENT.TCP-IP-AP.*nnn*.FTPD existiert.

  Wenn das Kommando an der Konsole eingegeben wird, muss sie zusätzlich shareable sein. Dies hat keine negativen Folgen für die Sicherheit, da ab TCP-IP-AP V5.0 alle Server-Options in einer eigenen Option-Datei hinterlegt werden können, die nicht shareable sein muss (siehe Abschnitt „Konfiguration von FTP via Option-Datei“ auf Seite 70).

- Mit dem Parameter VERSION für die START-Kommandos lassen sich auch die Server mit TCP-IP-AP-Versionen < 5.0 starten. Da sich aber die Server erst ab V5.0 bei jedem Start beim Subsystem TCPIPAP anmelden, können nur solche Server wieder durch STOP-Kommandos beendet werden.

- Es dürfen sich maximal 20 Teilnehmer an das Subsystem TCPIPAP anbinden. Mehr Teilnehmer sind aufgrund der Größe interner Tabellen nicht zulässig. Der Maximalwert von 20 Teilnehmern wird jedoch für die Praxis ausreichen. Bei Überschreitung der Maximalzahl beendet sich der Server beim Start mit folgender Meldung:

  „error: too many connections to Subsystem TCPIPAP“

- Wenn der Server nicht unter TSOS gestartet wurde, beendet er sich mit folgender Meldung:

  „error: no privilege to connect to Subsystem TCPIPAP“

  Dies kann nur beim Versuch vorkommen, den Server via explizitem Aufruf der Start-Prozedur anstatt mithilfe des START-...-DEMON-Kommandos zu starten, denn dies würde unter einer Kennung ungleich TSOS abgewiesen.

4.4.6 Meldungen und Returncodes

Meldungen

```
TCP2000   (&00)-KOMMANDO FUER (&01)-SERVER ERFOLGREICH AUSGEFUEHRT.
          &00  =  START oder STOP
          &01  =  FTP oder TELNET oder TCP-IP
```

Bedeutung
Das START/STOP-Kommando fuer FTP/TELNET-Server war erfolgreich.

Maßnahme
<keine>

```
TCP2001   STOP-KOMMANDO FUER (&00)-SERVER HAT KEINE WIRKUNG.
          &00  =  FTP oder TELNET
```

Bedeutung
Keine Server vorhanden.

Maßnahme
<keine>

```
TCP2003   GEWUENSCHTE PORTNUMMER FUER (&00)-SERVER EXISTIERT NICHT.
          &00  =  FTP oder TELNET
```

Bedeutung
Angegebener Server nicht vorhanden.

Maßnahme
<keine>

```
TCP2004   FEHLER BEIM STARTEN DER PROZEDUR FUER (&00): (&01).
          &00  =  FTP oder TELNET oder TCP-IP
          &01  =  <Startprozedur>
```

Bedeutung
(&00)-Server konnte mit Prozedur (&01) nicht gestartet werden.

Maßnahme
<keine>

Kommando-Returncodes

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	siehe Meldung TCP2000
	0	CMD0001	siehe Meldung TCP2001
	1	TCP2003	siehe Meldung TCP2003
	32	TCP2004	siehe Meldung TCP2004
	32	CMD0220	beim /CANCEL-JOB-Kommando passierte ein Fehler

4.5 Anmerkungen zur Installation der FTAC-Funktionalität

Zusätzlich zur Beschreibung des FTAC-SUPPORT-Operanden im Kommando SET-FTP-TELNET-PARAMETERS (siehe Seite 42/Seite 57) liefert dieser Abschnitt weitere Informationen, die bei der Nutzung der FTAC-Funktionalität zu beachten sind:

- Die Nutzung der FTAC-Funktionalität setzt den Einsatz von openFT (BS2000) voraus.
- Bei aktivierter FTAC-Funktionalität ist kein FTP-Zugang zur TSOS-Kennung via Dialogkennung möglich, da in diesem Fall eine alternative Zugangsmöglichkeit per FTAC-Transfer-Admission vorhanden ist (siehe aber Option *-allowTsosLogin* auf Seite 82).
- Um auch bei abgeschalteter FTAC-Funktionalität das Risiko des Ausspionierens des TSOS-Passworts zu minimieren, führt die Angabe eines ungültigen LOGON-Passworts für die Kennung TSOS zu einer Zeitstrafe, die sich bei jedem weiteren Fehlversuch verlängert. Nach jeder ungültigen Passworteingabe wird nach ca. fünf Sekunden der Verbindungsaufbau-Wunsch abgelehnt. Erst nach Ablauf der Zeitstrafe - unabhängig davon, ob inzwischen das richtige Passwort angegeben wurde - kann ein erfolgreicher LOGON-Versuch unternommen werden. Die Dauer der Zeitstrafe bleibt für den potenziellen „Einbrecher“ unsichtbar.
- Wenn die FTAC-Überprüfung aktiviert wird, müssen auch vom FTAC-Verwalter und von den Inhabern der in einen FTP-Transfer involvierten Benutzerkennungen Aktionen, wie z.B. Anpassen der Berechtigungssätze, durchgeführt werden, da andernfalls der FTP-Zugang zu vielen bzw. allen Benutzerkennungen gesperrt sein kann.

  Um dies zu verhindern, muss deshalb rechtzeitig eine geeignete Migrationsstrategie festgelegt werden:

  – Eine Möglichkeit besteht darin, für die FTAC-Überprüfung den Level 1 zu wählen. Dies bedeutet, dass der Zugang über die Dialogkennung - wie bisher - nicht via FTAC überprüft wird. Es ist jedoch zusätzlich ein Zugang über FTAC-Transfer-Admissions möglich.

  – Eine andere bzw. zusätzliche Möglichkeit besteht darin, beispielsweise während einer Übergangsphase zwei Server parallel zu installieren (siehe Abschnitt „Weitere FTP-Server-Tasks einrichten“ auf Seite 102): Ein Server hat die Standard-Portnummer 21, der andere Server hat eine andere Portnummer. Nur *ein* Server führt dabei die volle FTAC-Prüfung (Level 2) durch.

4.6 Accounting im FTP

Mithilfe des FTP-Accountings können FTP-Abrechnungssätze erfasst und in eine Datei ausgegeben werden (Voreinstellung: SYSDAT.TCP-IP-AP.*nnn*.FTPD.ACCOUNTING).

4.6.1 Accounting ein-/ausschalten und Abrechnungsdatei festlegen

Für das Ein-/Ausschalten des FTP-Accountings und das Festlegen der Abrechnungsdatei stehen Ihnen wahlweise folgende Möglichkeiten zur Verfügung:

- Installationskommando SET-FTP-TELNET-PARAMETERS (siehe Seite 42/Seite 57)
- Options *-acctActive* und *-acctFile* (siehe Seite 81)

Diese Einstellungen können Sie mithilfe des Kommandos */INFORM-PROGRAM* auch im laufenden Betrieb modifizieren, um das Erfassen der Abrechnungssätze ein-/auszuschalten oder die Abrechnungsdatei zu wechseln:

`/INFORM-PROGRAM 'acctActive: ',*TSN(<tsn>)`	FTP-Accounting ein-/ausschalten (siehe Seite 116)
`/INFORM-PROGRAM 'acctFile: ',*TSN(<tsn>)`	neue Abrechnungsdatei spezifizieren (siehe Seite 116)

4.6.2 Struktur der Abrechnungssätze

Die Struktur des FTP-Abrechnungssatzes in der Abrechnungsdatei ist an die Struktur des FT-Abrechnungssatzes angelehnt. Die einzelnen Bestandteile des Abrechnungssatzes sind so aneinandergefügt und mit Längen- und Offset-Informationen versehen, dass die Kompatibilität zu älteren Auswertungsprogrammen auch bei folgenden Modifikationen erhalten bleibt:

- einzelne Bestandteile vergrößern
- Zahl der variablen Satzerweiterungen erhöhen

Der FTP-Abrechnungssatz gliedert sich in folgende vier Bestandteile:

1. Satzbeschreibung
2. Kennzeichnungsteil
3. Grundinformation
4. variable Information

Beschreibung der Bestandteile des FTP-Abrechnungssatzes

Die Beschreibungen der einzelnen Satzteile enthalten die folgenden Kennzeichen:

- Feldnummer: laufende Nummer des Datenfeldes innerhalb des beschriebenen Satzteils
- Distanz: relativer Abstand des Datenfeldes zum Anfang des beschriebenen Satzteils
- Länge: Länge des Datenfeldes (in Byte)
- Format: Format des Datenfeldes

In der nachfolgenden Beschreibung der Bestandteile des FTP-Abrechnungssatzes werden folgende Abkürzungen verwendet::

A = alphanumerisch (einschließlich $, # und @)
B = Binärzahl
C = abdruckbare Zeichen
F = Dateiname für BS2000
Z = Zeitangabe im Format YYYYMMDDHHMMSS
\- = undefiniert

Satzbeschreibungsteil

Feld-Nr.	Distanz	Länge	Format	Bedeutung
1	0x00	4	A	Satzkennung „FTP0“
2	0x04	8	-/B	Zeitstempel der Tageszeituhr
3	0x0C	2	B	Länge des Kennzeichnungsteils
4	0x0E	2	B	Länge der Grundinformation
5	0x10	4	-	reserviert

Kennzeichnungsteil

Feld-Nr.	Distanz	Länge	Format	Bedeutung
1	0x00	8	A	Benutzerkennung
2	0x08	8	A	Abrechnungsnummer
3	0x10	4	Z	TSN des FTP-childs

Grundinformation

Feld-Nr.	Distanz	Länge	Format	Bedeutung
1	0x00	14	Z	Zeit des Kommandoempfangs
2	0x0E	14	Z	Zeit des Übertragungsende
3	0x1C	1	C	Ergebnis der Übertragung: +: erfolgreiche Durchführung -: fehlerhafte Durchführung 0: unbestimmt
4	0x1D	3	-	reserviert
5	0x20	8	B	Anzahl der Bytes von/zu Platte
6	0x28	8	B	Anzahl der Bytes in/aus Netz
7	0x30	4	B	Anzahl der Plattenzugriffe
8	0x34	4	B	verbrauchte Rechenzeit in Millisekunden

Erläuterung zu Feld-Nr. 3

Der FTP-Server kann teilweise nicht erkennen, ob eine Übertragung fehlgeschlagen ist. Ursache: In vielen Fällen wird das Ende des Dateitransfers durch Beenden der Datenverbindung signalisiert. Dieses Beenden der Verbindung kann jedoch auch durch einen Fehler verursacht worden sein. In solchen Fällen wird also das „Ergebnis der Übertragung“ mit „0“ (= unbestimmt) gekennzeichnet.

Erläuterung zu Feld-Nr. 8

Gemessen wird jeweils der Rechenzeitverbrauch vom Ende eines vorangegangenen Transfers (bzw. vom Start des Childs) bis zum Ende des Transfers der jeweiligen Datei. Eingeschlossen sind Aktionen wie Setzen von Optionen, Wechseln und Auflisten von Verzeichnissen. Manche Aktionen können einem nachfolgenden Dateitransfer nicht mehr zugeordnet werden, weil zwischenzeitlich die Verbindung beendet wurde. Diese Aktionen werden in einem speziellen Abrechnungssatz berücksichtigt, der am Ende einer Verbindung geschrieben wird. In diesem Satz ist als Ergebnis der Übertragung der Wert X’00’ eingetragen, das Feld „Dateiname“ erhält keinen Eintrag (siehe Tabelle „Satzerweiterung für den Dateinamen“ auf Seite 110).

Variable Information

Feld-Nr.	Distanz	Länge	Format	Bedeutung
1	0x00	2	B	Anzahl der Erweiterungen = 1
2	0x02	2	B	Distanz zwischen der Satzerweiterung für die Partneridentifizierung und dem Satzanfang
3	0x04	2	B	Distanz zwischen der Satzerweiterung für den Dateinamen und dem Satzanfang
Wenn eine Distanz auf 0 gesetzt ist, ist die entsprechende Satzerweiterung nicht angegeben.				

Kopf des variablen Teils

Feld-Nr.	Distanz	Länge	Format	Bedeutung
1	0x00	2	A	Erweiterungsidentifikation = „PI“
2	0x02	1	B	Erweiterungs-Typ = 0x00
3	0x03	1	-	reserviert
4	0x04	2	B	Länge der Erweiterung (ohne Identifikation, Typ und Längenfeld)
5	0x06	1	B	Adresstyp: 1: IPv4 2: IPv6
6	0x07	16	B	IP-Adresse (linksbündig)
7	0x17	1	-	reserviert
8	0x18	2	B	Länge des Partnernamens
9	0x1A	siehe Feld 8	F	Partnername

Satzerweiterung für die Partneridentifizierung

Feld-Nr.	Distanz	Länge	Format	Bedeutung
1	0x00	2	A	Erweiterungsidentifikation = „FN“
2	0x02	1	B	Erweiterungs-Typ = 0x00
3	0x03	1	-	reserviert
4	0x04	2	B	Länge des Dateinamens
5	0x06	siehe Feld 4	F	Dateiname

Satzerweiterung für den Dateinamen

4.7 Protokolldatei von FTP-Servern

FTP-Server protokollieren ihre Ausgaben in einer Protokolldatei mit dem Standard-Dateinamen SYSOUT.TCP-IP-AP.*nnn*.FTPD. Die Protokolldatei enthält immer die Differenzeinträge zur aktuellen Sicherung mit dem */INFORM-PROGRAM*-Kommando rdProt
(siehe Abschnitt „rdProt - Protokolldatei von FTP-Servern sichern“ auf Seite 117).

4.8 Anzeige der aktuellen Einstellungen von FTP-Servern

Mithilfe des BS2000-Kommandos SHOW-FTP-TELNET-STATUS können Sie sich über die aktuellen Einstellungen von BS2000-FTP-Servern informieren.

Ausgegeben werden die folgenden Informationen:

- Einstellungen, die bei der Generierung der Server vorgenommen wurden
- aktuelle Informationen über die TSN der Servertasks und Anzahl aktiver Verbindungen

Die Server hinterlegen die Daten in Hilfsdateien mit folgenden Namen:

- SYSDAT.TCP-IP-AP.*nnn*.FTPD.CONF.<port>

<port> spezifiziert die Portnummer des Servers.

Diese Datei wird beim Beenden des jeweiligen FTP-Servers wieder gelöscht.

SHOW-FTP-TELNET-STATUS
SERVER= *FTP(...)/ ***TELNET**(...) ***FTP**(...) **PORT-NUMBER= *STD-PORT** / ***ANY** / <integer 0..32767> ***TELNET**(...) **PORT-NUMBER=*STD-PORT** / ***ANY** / <integer 0..32767> **, INFORM= *STD /*ALL** **, OUTPUT=*SYSOUT/*SYSLST**

SERVER=
Name des Servers, dessen Daten ausgegeben werden sollen (FTP oder TELNET).

SERVER=*FTP(...)
Ausgabe der Konfigurationsdaten eines FTP-Servers. Dies ist die Voreinstellung.

PORT-NUMBER=
Portnummer des FTP-Servers, dessen Konfigurationsdaten ausgegeben werden sollen.

PORT-NUMBER=*STD-PORT
Portnummer 21. Dies ist die Voreinstellung.

PORT-NUMBER=*ANY
Es werden Informationen über alle zurzeit aktiven FTP-Server ausgegeben.

PORT-NUMBER=<integer 0..32767>
Portnummer des FTP-Servers, dessen Konfigurationsdaten ausgegeben werden sollen.

INFORMATION=
Art und Umfang der ausgegebenen Informationen.

INFORMATION= *STD
Ausgabe einer Liste der durch PORT-NUMBER spezifizierten Server. Dies ist die Voreinstellung.

INFORMATION= *ALL
Ausgabe aller Informationen aller durch PORT-NUMBER spezifizierten Server.

OUTPUT=
Ausgabemedium, in das die Informationen geschrieben werden sollen.

OUTPUT=*SYSOUT
Ausgabe erfolgt nach SYSOUT. Dies ist die Voreinstellung.

OUTPUT=*SYSLST
Ausgabe erfolgt nach SYSLST.

Meldungen und Returncodes

Meldungen

TCP9240 KOMMANDO SHOW-FTP-TELNET-STATUS ERFOLGREICH BEENDET.

Bedeutung
SHOW-FTP-TELNET-STATUS erfolgreich beendet.

Maßnahme
<keine>

TCP9241 FSTAT-FEHLER DMS(&00).

Bedeutung
Fehler bei FSTAT auf Konfigurationsdateien.

Maßnahme
Nachprüfen ob überhaupt irgendein Server aktiv ist.

TCP9242 KONFIGURATIONSDATEI (&00) KONNTE NICHT GEOEFFNET WERDEN.

Bedeutung
Konfigurationsdatei (&00) konnte nicht geöffnet werden.

Maßnahme
Nachprüfen, ob der gewünschte Server aktiv ist.

TCP9243 KONFIGURATIONSDATEI (&00) KONNTE NICHT GELESEN WERDEN.

Bedeutung
Konfigurationsdatei (&00) konnte nicht gelesen werden.

Maßnahme
Datei überprüfen.

Kommando-Returncodes

(SC2)	SC1	Maincode	Bedeutung
	0	TCP9240	Kommmando erfolgreich beendet
	64	TCP9241	siehe Meldung TCP9241
	64	TCP9242	siehe Meldung TCP9242
	64	TCP9243	siehe Meldung TCP9243

4.9 Konsolschnittstelle

Einige Kommandos können vom Systembediener auch über die Konsolschnittstelle, eingeleitet mit dem Kommando */INFORM-PROGRAM*, angegeben werden. Die mit */INFORM-PROGRAM* abgesetzten Kommandos dienen zum

– Steuern der Server-Traces,
– Beenden der verschiedenen Server-Tasks,
– Steuern des FTP-Accounting,
– Sichern der Protokolldateien.

Folgende Server-Kommandos sind über die Konsolschnittstelle möglich:

Operation	**Kurzbeschreibung**
debug	Trace zur Benutzerebene ein/ausschalten
trace	Trace zur TCP/IP-Schnittstelle ein/ausschalten
shutdown	Service beenden
acctActive	FTP-Accounting ein-/ausschalten
acctFile	beim FTP-Accounting auf neue Abrechnungsdatei wechseln
rdProt	Protokolldatei des FTP-Servers sichern

Die Kommandos für Inbetriebnahme und Außerbetriebnahme der FTP-Server (siehe Seite 101) können auch an der Konsole eingegeben werden.

debug - Trace zur Benutzerebene ein-/ausschalten

/INFORM-PROGRAM
'debug <debug-wert>**'**,***TSN**(<tsn>)

<tsn>
TSN der Server-Task, für den der Trace zur Benutzerebene eingeschaltet werden soll.

debug <debug-wert>
Zulässig sind Werte von 0 bis 9. Je größer der Wert, desto mehr Informationen werden ausgegeben. Wert 0 bedeutet, dass der Trace ausgeschaltet ist. Dieses Kommando dient dem Systemkundendienst zur Fehlerdiagnose. Ein Debug-Wert > 2 ist nicht sinnvoll.

trace - Trace zur TCP/IP-Schnittstelle ein-/ausschalten

/INFORM-PROGRAM
'trace <trace-wert>**',*TSN**(<tsn>)

<tsn>
TSN der Server-Task, für den der Trace zur TCP/IP- Schnittstelle eingeschaltet werden soll.

trace <trace-wert>
Zulässig sind Werte von 0 bis 10. Je größer der Wert, desto mehr Informationen werden ausgegeben. Wert 0 bedeutet, dass der Trace ausgeschaltet ist. Dieses Kommando dient dem Systemkundendienst zur Fehlerdiagnose.

shutdown - Service beenden

/INFORM-PROGRAM
'shutdown',***TSN**(<tsn>)

<tsn>
TSN der zu beendenden Server-Task.

acctActive - FTP-Accounting ein-/ausschalten

/INFORM-PROGRAM
'**acctActive** {**ON** | **OFF**}',***TSN**(<tsn>)

<tsn>
TSN der Server-Task.

ON
FTP-Accounting wird eingeschaltet.
(Standard-Abrechnungsdatei: SYSDAT.TCP-IP-AP.*nnn*.FTPD.ACCOUNTING)

OFF
FTP-Accounting wird ausgeschaltet.

acctFile - Abrechnungsdatei des FTP-Accounting wechseln

/INFORM-PROGRAM
'acctFile <Name der Abrechnungsdatei>',***TSN**(<tsn>)

<tsn>
TSN des FTP-Servers.

<Name der Abrechnungsdatei>
Name der neuen Abrechnungsdatei.

Die bisherige Abrechnungsdatei wird geschlossen und kann ausgewertet werden.

rdProt - Protokolldatei von FTP-Servern sichern

Mit dem Kommando *rdProt* wird die Protokolldatei eines FTP-Servers abgespeichert unter dem Namen der ursprünglichen Protokolldatei (Standarddateiname: SYSOUT.TCP-IP-AP.*nnn*.FTPD), erweitert um einen Suffix, der Datum und Uhrzeit (UTC) in der Form <MMDD><HHMMSS> spezifiziert. Diese Datei enthält immer die Differenzeinträge zur vorausgegangenen Sicherung. Beachten Sie, dass Sie keinen zu langen Namen für die Protokolldatei wählen: Das *rdProt* schlägt fehl, wenn der Name nach dem Anhängen des Suffix die zulässige Länge von 38 Zeichen überschreitet.

/INFORM-PROGRAM
'rdProt ',*TSN(<tsn>)

<tsn>
TSN der Server-Task.

4.10 IPv6-Adressen in FTP

Dieser Abschnitt behandelt im Zusammenhang mit der Verwendung von IPv6-Adressen in FTP die folgenden Themen:

- Aufbau der Kontrollverbindung
- Aufbau der Datenverbindung mit Aktiv- und Passivmodus
- Proxy-Mechanismus
- Einsatzhinweise in heterogenen Netzen

4.10.1 Aufbau der Kontrollverbindung

Beim Aufbau der Kontrollverbindung mit dem Client-Kommando *open* kann als Adresse auch eine IPv6-Adresse verwendet werden, die in sedezimaler Darstellung mit Doppelpunkt (:) angegeben wird (siehe Handbuch „interNet Services Benutzerhandbuch“).

4.10.2 Aufbau der Datenverbindung

Für den Aufbau der Datenverbindung mit IPv6-Adressen stehen die folgenden beiden FTP-Protokoll-Kommandos zur Verfügung:

- EPRT: PORT-Kommando erweitert um die IPv6-Fähigkeit
- EPSV: PASV-Kommando erweitert um die IPv6-Fähigkeit

Folgende zwei Modi werden beim Aufbau der Datenverbindung unterschieden:

- Aktivmodus
- Passivmodus

Aktivmodus

Der Verbindungsaufbau erfolgt mit aktivem Child und passivem Client. Dem Child wird der eigene Verbindungsendpunkt mithilfe der folgenden Kommandos mitgeteilt:

- PORT-Kommando, wenn die eigene Adresse eine IPv4-Adresse (IPv4-MAPPED-Adresse) ist.
- EPRT-Kommando, wenn die eigene Adresse eine IPv6-Adresse ist.

PORT a1, a2, a3, a4, p1, p2	ai, i = 1,..,4: IPv4-Adresse; pi, i = 1, 2: Portnummer
EPRT |2|a|p|	2: IPv6-Protokoll, a: IPv6-Adresse in Doppelpunktnotation, p: Portnummer

Passivmodus

Der Passivmodus wird mit dem Client-Kommando *passive* eingestellt (siehe Handbuch „interNet Services Benutzerhandbuch“).

Die Datenverbindung wird aufgebaut mit passivem Child und aktivem Client. Der Child schickt seine IPv4-Adresse inklusive Portnummer (PASV) oder nur seine Portnummer (EPSV), die der Client dann mit der von der Kontrollverbindung bekannten IPv6-Adresse des Servers kombiniert.

Angestoßen wird der genannte Vorgang durch eines der beiden folgenden vom Client gesendeten Kommandos:

- PASV-Kommando, wenn die IP-Adresse des Servers bei der Kontrollverbindung eine IPv4-MAPPED-Adresse ist.
- EPSV-Kommando, wenn die IP-Adresse des Servers bei der Kontrollverbindung eine IPv6-Adresse ist.

227 Entering Passive Mode (a1, a2, a3, a4, p1, p2)	ai, i = 1,..,4: IPv4-Adresse; pi, i = 1, 2: Portnummer (Antwort auf PASV)
229 Entering Extended Passive Mode EPRT (|||p|)	p: Portnummer (Antwort auf EPSV)

Der Passivmodus ist mittlerweile Standardeinstellung in vielen Client-Implementierungen und dient dazu, aus einem lokalen Netz über eine Firewall ins Internet zu gelangen. Solche Firewalls unterbinden häufig den aktiven Verbindungsaufbau in das eigene lokale Netz hinein.

4.10.3 Proxy-Mechanismus

Beim Datentransfer zwischen zwei FTP-Servern (im Folgenden erster Server und Proxy-Server genannt) schickt der FTP-Client ein PASV- bzw. EPSV-Kommando an den Proxy-Server, je nachdem ob der Proxy-Server bei der Kontrollverbindung unter einer IPv4- bzw. IPv6-Adresse erreichbar ist. Die in der Rückantwort enthaltene Adressinformation schickt der Client mit einem PORT- bzw. EPRT-Kommando an den ersten Server.

Folgendes Problem kann dabei auftreten:

- Der Proxy-Server besitzt eine IPv6-Adresse.
- Der erste Server dagegen ist ein reiner IPv4-Server, der über IPv6-Adressen nicht erreichbar ist, und entsprechend noch mit dem IPv4-FTP arbeitet.

Um dieses Problem zu lösen, muss der Proxy-Server zusätzlich zu den IPv6-Adressen mindestens eine IPv4-Adresse besitzen. Diese IPv4-Adresse müssen Sie beim Aufbau der Kontrollverbindung als IPv4-MAPPED-Adresse angeben. Das PASV-Kommando liefert dann eine IPv4-Adresse, unter der der Proxy-Server erreichbar ist, und die auch der erste Server verarbeiten kann.

4.10.4 Einsatzhinweise für heterogene Netze

Wichtigste Voraussetzung für den Einsatz eines IPv6-FTP im BS2000 ist die Existenz von IPv6-fähigen Sockets. Im BS2000 wurde hierfür das Subsystem SOC6 entwickelt, welches ab SOCKETS(BS2000) Version 2.0A realisiert ist.

Hierbei ist zu beachten:

- Wenn ein Rechner nur IPv4-Adressen besitzt, können Sie einen IPv6-fähigen FTP-Server einsetzen, sofern IPv6-fähige Sockets vorhanden sind. Es darf aber kein weiterer IPv4-Server parallel dazu laufen.
- Wenn ein Rechner sowohl IPv4- als auch IPv6-Adressen besitzt, sollten Sie nur den IPv6-fähigen FTP einsetzen. Andernfalls könnte ein IPv6-fähiger Client von einem anderen Rechner aus versuchen, eine IPv6-Verbindung aufzubauen, die dann misslingt.
- Wenn ein Rechner nur IPv6-Adressen besitzt, müssen Sie den IPv6-fähigen FTP einsetzen.

4.11 SNMP-Subagent für FTP

Für den FTP-Server gibt es einen eigenen Subagenten (FTP-Subagent), der über eine Management-Anwendung, den BCAM-Manager, bedient wird.

Im Handbuch „SNMP-Management für openNet Server und interNet Services“ finden Sie Informationen zu folgenden Themen:

- Handhabung des BCAM-Managers
- Software-Voraussetzungen
- Installation und Deinstallation
- In- und Außerbetriebnahme des FTP-Subagenten

Interaktion zwischen FTP-Subagent und FTP-Server

Der FTP-Server erreicht den FTP-Subagenten unter der festen Portnummer 3237. Unmittelbar nach dem Start meldet sich der FTP-Server beim FTP-Subagenten, sofern dieser gestartet ist, und liefert ihm folgende Informationen:

- Portnummer, unter der der FTP-Subagent den FTP-Server erreichen kann
- Server-Portnummer für die Kontrollverbindung zu den FTP-Clients

Sofern nicht bereits ein Server-Entry mit dieser Server-Portnummer existiert, legt der FTP-Server einen entsprechenden Server-Entry an.

Jeder FTP-Server schreibt beim Start seine beiden Portnummern in die Datei SYSDAT.TCP-IP-AP.*nnn*.SNMP. Falls der FTP-Subagent erst nachträglich gestartet wird, kann er sich in SYSDAT.TCP-IP-AP.*nnn*.SNMP über die momentan aktiven FTP-Server informieren und die entsprechenden Datenstrukturen anlegen.

Wenn der FTP-Server beendet wird, löscht er seinen Eintrag aus der Datei SYSDAT.TCP-IP-AP.*nnn*.SNMP.

4.12 FTP-Exit

Für den FTP-Client und den FTP-Server gibt es folgende Exits:

- FTP-System-Exit
- Exit-Mechanismen für FTP-Server und FTP-Client

4.12.1 FTP-System-Exit

Der FTP-System-Exit bietet dem Betreiber eines BS2000-FTP-Servers die Möglichkeit, FTP-Server-Funktionen zu erweitern bzw. zu ändern und eigene Funktionen hinzuzufügen. Solche Funktionen sind z.B.:

- über den Dialog-Login hinausgehende Sicherheitsüberprüfung des FTP-Server-Zugangs und der danach empfangenen FTP-Kommandos,
- Protokollierung der überprüften FTP-Kommandos,
- Modifizierung von FTP-Kommandos.

Wenn der System-Exit vom FTP-Server aufgerufen werden soll, muss, je nach gewählter Installationsart (Kapitel „FTP und TELNET - Installation“, siehe Seite 41)

- im SDF-Kommando SET-FTP-TELNET-PARAMETERS ein von 0 verschiedener System-Exit Level eingestellt werden (siehe Seite 61) oder
- in der Option-Datei die Option `-systemExit 1` (siehe Seite 79) spezifiziert werden oder
- im zugehörigen Enter-Job die Option *-x 1* angegeben werden.

Wenn gleichzeitig FTAC genutzt wird, wird der System-Exit bei den Unterereignissen FTPLOG und FTPCMD nicht angesprungen.

Zum Schutz des BS2000-FTP-Servers führt bei abgeschalteter FTAC-Funktionalität die Angabe eines falschen LOGON-Passworts für die Kennung TSOS zu einer Zeitstrafe, die sich bei jedem weiteren Fehlversuch verlängert. Nach jeder falschen Passwortangabe wird nach etwa fünf Sekunden der Verbindungsaufbauwunsch abgelehnt. Erst nach Ablauf der Zeitstrafe - unabhängig davon, ob inzwischen das richtige Passwort angegeben wurde - kann ein erfolgreicher LOGON-Versuch unternommen werden. Die Dauer der Zeitstrafe bleibt für den potentiellen „Einbrecher“ unsichtbar.

4.12.1.1 FTP-System-Exit-Ereignisse

Der FTP-System-Exit wird bei den im Folgenden erläuterten Ereignissen aufgerufen. Jedes Ereignis wird eindeutig gekennzeichnet durch den Hauptereignis-Namen und den Unterereignis-Namen. Zur Zeit existiert nur ein Hauptereignis *FTP* für die FTP-System-Exit-Routine mit den Unterereignissen *FTPLOG, FTPBYE, FTPCMD* und *FTPCMDE*.

Bei der Programmierung der Exit-Routinen sollten Sie berücksichtigen, dass es in zukünftigen Versionen des Exits weitere Haupt- und Unterereignisse geben kann.

Bei jedem Aufruf des Exits wird die Portnummer des FTP-Servers und eine „Connection-Id“ mitgegeben. Falls mehrere FTP-Server (mit unterschiedlichen Portnummern) gestartet werden, kann mithilfe der Portnummer für jeden Server eine eigene Verhaltensweise der Exit-Routine realisiert werden. Die „Connection-Id“ erlaubt es, alle zu einer bestimmten FTP-Sitzung gehörenden Unterereignisse *FTPCMD*, *FTPCMDE*, *FTPBYE* zu identifizieren, mit anderen Worten, alle Ereignisse mit einer bestimmten „Connection-Id“ gehören zum jeweils letzten vorangegangenen FTPLOG-Ereignis mit der gleichen „Connection-Id“. Damit kann die Exit-Routine Informationen zwischenspeichern und wiederfinden, die bei späteren Aufrufen durch die gleiche FTP-Sitzung benötigt werden.

Unterereignis FTPLOG

Das Unterereignis *FTPLOG* wird bei jedem FTP-Login-Versuch aufgerufen. Die Exit-Routine kann anhand der mitgegebenen Parameter (User id, Account, Password, Partnersystem) entscheiden, ob dieser Login-Versuch zugelassen werden soll. Die Exit-Routine kann darüber hinaus alle Zugangsversuche protokollieren und manche Parameter (User id, Account, Password) verändert zurückgeben, indem sie den Returncode „Aufruf modifizieren“ verwendet. Dies kann zum Beispiel dazu benutzt werden, die Herausgabe von Dialogzugangsberechtigungen unnötig zu machen, indem die Exit-Routine spezielle FTP-Login-Kennungen, die keinen Dialogzugang ermöglichen, auf echte Dialog-Kennungen abbildet.

Unterereignis FTPBYE

Das Unterereignis *FTPBYE* wird beim Beenden einer FTP-Sitzung aufgerufen. Die Exit-Routine kann dann z.B. eine abschließende Protokollierung der FTP-Sitzung erstellen und gegebenenfalls zwischengespeicherte Daten löschen. Zusätzlich zu den immer mitgelieferten Daten werden bei diesem Aufruf User id, Account, Password, Partnersystem und ’ftp login’ als Aktionsklasse mitgeliefert.

Unterereignis FTPCMD

Das Unterereignis *FTPCMD* wird beim Empfang von bestimmten FTP-Kommandos aufgerufen. Dabei wird nicht nur der Name des FTP-(Protokoll-)Kommandos, sondern auch eine zugeordnete Aktionsklasse (siehe nachfolgende Tabelle) mitgegeben. Es wird empfohlen, die Erlaubnisentscheidung anhand der Aktionsklasse und nicht des Kommando-Namen zu treffen, um unnötige Änderungen bei einer evtl. Änderung der Menge der überprüften FTP-Kommandos in zukünftigen FTP-Versionen zu vermeiden.

Außerdem wird der Kommando-Parameter (Datei- oder Verzeichnisname) mitgeliefert.

Kommando	**Aktionsklasse**
RETR	YAPXREAD
STOR	YAPXWRT
STOU	YAPXWRT
APPE	YAPXWRT
RNFR	YAPXMODA
DELE	YAPXDEL
FILE	YAPXCREA
PWD	YAPXSHDR
XPWD	YAPXSHDR
CWD	YAPXSHDR
XCWD	YAPXSHDR
LIST	YAPXSHDR
NLST	YAPXSHDR
CDUP	YAPXSHDR
XDUP	YAPXSHDR
MKD	YAPXCRDR
XMKD	YAPXCRDR
RMD	YAPXDLDR
XRMD	YAPXDLDR
SIZE	YAPXSHDR
MDTM	YAPXSHDR
MLSD	YAPXSHDR
MLST	YAPXSHDR

Bei allen anderen FTP-Kommandos wird der System-Exit nicht aufgerufen.

Wenn der Exit durch ein Kommando verursacht wird, das aus Sicht des FTP-Servers zu einem schreibenden Zugriff führt, wird in einem Parameter angegeben, ob dieser Zugriff eine Datei erweitern, ersetzen oder neu schreiben soll. Außerdem wird der Datei- bzw. Verzeichnisname, auf den das Kommando wirkt, mitgegeben. Dieser kann gegebenenfalls (z.B. durch Voransetzen eines Präfix) modifiziert wieder zurückgegeben werden. Der FTP-Server verwendet dann nachfolgend nur diesen veränderten Namen. Hierfür ist der Returncode „Aufruf modifizieren“ zu verwenden.

Unterereignis FTPCMDE

Das Unterereignis *FTPCMDE* wird nach Abarbeitung eines Kommandos mit den gleichen Parametern wie *FTPCMD* aufgerufen. Zusätzlich wird mitgeteilt, ob das Kommando fehlerfrei abgeschlossen wurde (Feld YAPXCMDR mit den Werten YAPXOK oder YAPXERR).

Registerversorgung

Beim Ansprung der Exit-Routine sind die Register 4 bis 11 undefiniert, die übrigen Register enthalten folgende Werte:

R0 = Exitnummer '023'

R1 = A(YAPXPARL) = FTP-System-Exit-Parameterliste s.u.

R2 = A(Task Control Block)

R3 = A(Executive Vector Table)

R12 = A(TPR Program Manager)

R13 = A(Sicherungsbereich der rufenden Komponente)

R14 = A(Indirekter Rücksprung)

R15 = A(Exit-Routine)

Die Register 12, 13 und 14 dürfen von der Exit-Routine nicht zerstört werden.

Rückkehrinformation

Die Exit-Routine gibt in Register 15 Rückkehrinformation an die rufende FTP-Komponente in folgendem Format zurück:

R15 = X'BB0000RR'

BB = Rückkehrinformation des Basismechanismus

00	kein Fehler
04	Exit-Routine nicht aktiviert
08	fehlerhafter Aufruf

RR = Rückkehrinformation der Exit-Routine an die rufende FTP-Komponente.

Folgende Werte sind möglich:

00	Aufruf ablehnen
04	Aufruf annehmen
08	Aufruf modifizieren

Mit dem Makro YAPSEPA kann eine DSECT für die FTP-System-Exit-Parameterliste erstellt werden.

Layout der Operandenliste

(Makro-Auflösung mit MF=D und Standardwerten für PREFIX und MACID)

```
[label]    YAPSEPA   MF=D [,PREFIX=Y | <prefix>]
                              _
                          [,MACID=APX | <mac-id>]
                                  ___
```

Beispiel

```
           YAPSEPA MF=D
 1         MFTST MF=D,PREFIX=Y,MACID=APX,ALIGN=F,                          C
 1               DMACID=APX,SUPPORT=(D,C,M,L),DNAME=APXPARL
 2 YAPXPARL DSECT ,
 2               *,##### PREFIX=Y, MACID=APX #####
 1 *   Parameter area
 1 *
 1 YAPXHDR  DS    0XL16                    Header
 1 YAPXVERS DS    F                        Interface version
 1 *   VERSION
 1 YAPXVER1 EQU   1                        Internet Services V1.0
 1 YAPXVER2 EQU   2                        Internet Services V2.0
 1 *
 1 YAPXMCAS DS    F                        Exit main case
 1 *   Exit main case
 1 YAPXFTP  EQU   1                        FTP
 1 *
 1 YAPXSCAS DS    F                        Exit sub case
 1 *   Exit sub case
 1 YAPXFLOG EQU   1                        FTP login
 1 YAPXFCMD EQU   2                        FTP command
 1 YAPXFCDE EQU   3                        FTP command end
 1 YAPXFBYE EQU   4                        FTP logout
 1 *
 1 YAPXRSLT DS    F                        Internally used
 1 *
 1 *
 1 YAPXIND  DS    0XL856                   Input parameters
 1 YAPXPORT DS    F                        FTP server port number
 1 YAPXCNID DS    F                        Connection id
 1 YAPXACT  DS    F                        FTP action class
 1 *   Action class
 1 YAPXWRT  EQU   1                        write
 1 YAPXREAD EQU   2                        read
 1 YAPXSHAT EQU   4                        show attributes
 1 YAPXDEL  EQU   8                        delete
 1 YAPXCREA EQU   16                       create
 1 YAPXMODA EQU   32                       modify attributes
 1 YAPXSHDR EQU   64                       show directory
 1 YAPXMOVE EQU   128                      move
 1 YAPXCRDR EQU   256                      create directory
 1 YAPXDLDR EQU   512                      delete directory
 1 YAPXMDDR EQU   1024                     modify directory
 1 YAPXLOG  EQU   2048                     ftp login
 1 *
 1 YAPXWRMD DS    F                        Write mode
```

```
 1 *   Write mode
 1 YAPXNEW  EQU   1                        New
 1 YAPXREPL EQU   2                        Replace
 1 YAPXEXT  EQU   4                        Extend
 1 *
 1 YAPXPRTN DS    CL256                    Partner system
 1 YAPXUSER DS    CL9                      User id
 1 YAPXACCT DS    CL9                      Account
 1 YAPXPASS DS    CL35                     Password
 1 YAPXFILE DS    CL500                    File name
 1 YAPXCMD  DS    CL5                      FTP command
 1 YAPXRSV1 DS    XL2                      Reserved
 1 YAPXCMDR DS    F                        FTP command rc
 1 *   Command rc
 1 YAPXOK   EQU   0                        Ok
 1 YAPXERR  EQU   1                        Error
 1 *
 1 YAPXRSV2 DS    XL20                     Reserved
 1 *
 1 *
 1 YAPXOUTD DS    0XL576                   Output parameters
 1 YAPXUSRO DS    CL9                      User id
 1 YAPXACCO DS    CL9                      Account
 1 YAPXPASO DS    CL35                     Password
 1 YAPXFILO DS    CL500                    File name
 1 YAPXRSV3 DS    XL23                     Reserved
 1 *
 1 YAPX#    EQU   *-YAPXVERS
```

Alternativ gibt es auch einen entsprechenden C-Include YAPSEPA.H:

```
#ifndef _YAPSEPA_H
#define _YAPSEPA_H

#if 0
/*****************************************************************
 BEGIN-INTERFACE   YAPSEPA

 TITLE             (/ TCP-IP-AP System exit parameter list /)
 NAME              YAPSEPA.H
 DOMAIN            TCP-IP-AP
 LANGUAGE          C
 COPYRIGHT         (C) Fujitsu Technology Solutions GmbH 2010
                       ALL RIGHTS RESERVED
 COMPILATION-SCOPE USER
 INTERFACE-TYPE    CALL
 RUN-CONTEXT       TU
```

```
 PURPOSE           (/ YAPSEPA describes the parameter list for
                      the FTP system exit.
                   /)

 END-INTERFACE     YAPSEPA.
*********************************************************************/
#endif

/* Version                                                           */
/* ENUM version_s                                                    */
#define YAPSEPAvers1 1                 /* Internet Services V1.0     */
#define YAPSEPAvers2 2                 /* Internet Services V2.0     */

/* Exit main case                                                    */
/* ENUM mainCase_s                                                   */
#define YAPSEPAFTP 1                   /* FTP                        */

/* Exit sub case                                                     */
/* ENUM subCase_s                                                    */
#define YAPSEPAFTPLOG 1                /* FTP login                  */
#define YAPSEPAFTPCMD 2                /* FTP command                */
#define YAPSEPAFTPCMDE 3               /* FTP command end            */
#define YAPSEPAFTPBYE 4                /* FTP logout                 */

/* Action class                                                      */
/* ENUM action_s                                                     */
#define YAPSEPAwrite 1                 /* write                      */
#define YAPSEPAread 2                  /* read                       */
#define YAPSEPAshow_attr 4             /* show attributes            */
#define YAPSEPAdelete 8                /* delete                     */
#define YAPSEPAcreate 16               /* create                     */
#define YAPSEPAmod_attr 32             /* modify attributes          */
#define YAPSEPAshow_dir 64             /* show directory             */
#define YAPSEPAmove 128                /* move                       */
#define YAPSEPAcre_dir 256             /* create directory           */
#define YAPSEPAdel_dir 512             /* delete directory           */
#define YAPSEPAmod_dir 1024            /* modify directory           */
#define YAPSEPAlogin 2048              /* ftp login                  */

/* Write mode                                                        */
/* ENUM writeMode_s                                                  */
#define YAPSEPAnew 1                   /* New                        */
#define YAPSEPAreplace 2               /* Replace                    */
#define YAPSEPAextend 4                /* Extend                     */

/* Command rc                                                        */
/* ENUM commandRc_s                                                  */
#define YAPSEPAok 0                    /* Ok                         */
```

```
#define YAPSEPAerror 1                  /* Error                        */
/* Parameter area                                                       */
struct YAPSEPA_pl_mdl {

        /* Header                                                       */
        struct {
                unsigned long version;  /* Interface version            */
                unsigned long mainCase; /* Exit main case               */
                unsigned long subCase;  /* Exit sub case                */
                unsigned long result;   /* Internally used              */
        } header;

        /* Input parameters                                             */
        struct {
                unsigned long portNum;  /* FTP server port number       */
                unsigned long connId;   /* Connection id                */
                unsigned long action;   /* FTP action class             */
                unsigned long writeMode;
                                        /* Write mode                   */
                char partner[256];      /* Partner system               */
                char userId[9];         /* User id                      */
                char account[9];        /* Account                      */
                char password[35];      /* Password                     */
                char fileName[500];     /* File name                    */
                char command[5];        /* FTP command                  */
                char reserved_1[2];     /* Reserved                     */
                unsigned long commandRc;
                                        /* FTP command rc               */
                char reserved_2[20];    /* Reserved                     */
        } in_data;
/* Output parameters                                                    */
        struct {
                char userId[9];         /* User id                      */
                char account[9];        /* Account                      */
                char password[35];      /* Password                     */
                char fileName[500];     /* File name                    */
                char reserved_3[23];    /* Reserved                     */
        } out_data;
};

#endif           /* _YAPSEPA */
```

4.12.2 Exit-Mechanismen für FTP-Server und FTP-Client

Wenn Sie für die transferierten Daten Code-Umwandlungen durchführen möchten, bei denen die Anzahl der Bytes nicht erhalten bleibt, können Sie hierfür XHCS nicht verwenden. Über eine spezielle Schnittstelle bei FTP-Server und FTP-Client können Sie jedoch eigene Code-Umwandlungsroutinen oder auch andere Exit-Routinen definieren, wie z.B. Routinen für Datenkomprimierung „on the fly“. Eine solche anwenderdefinierte Exit-Routine wird, sofern sie aktiviert ist, vor dem Versenden und nach dem Empfangen von Daten aufgerufen. Beachten Sie bitte, dass beim Übertragungstyp ASCII die Exit-Routine in jedem Fall nach ASCII konvertierte Daten benötigt.

4.12.2.1 Dummy-Routine

Die Exit-Routine wird beim Starten des FTP-Client-Programms bzw. der verbindungsspezifischen Server-Task automatisch aus der Modul-Bibliothek SYSLNK.TCP-IP-AP.*nnn* bzw. SKMLNK.TCP-IP-AP.*nnn* (bei x86-Rechnern) nachgeladen. Damit es hierbei nicht zu „UNRESOLVED EXTERNAL REFERENCES“-Fehlern kommt, muss in den genannten Bibliotheken immer ein Modul mit dem Entry YAPFEXIT vorhanden sein.

Die genannten Modul-Bibliotheken werden deshalb mit einer Dummy-Routine ausgeliefert, die in dem LMS-Element EXITFTP enthalten ist. Diese Routine führt keine Umwandlung durch, sondern protokolliert die übergebenen Daten auf der Standardausgabe und liefert sie ansonsten unverändert zurück. Den Quelltext für diese Routine, der sich im S-Element EXITFTP.C in der Bibliothek SYSSRC.TCP-IP-AP.*nnn* befindet, können Sie als Ausgangspunkt für eigene Routinen verwenden. Die hierfür notwendige Header-Datei finden Sie in der Bibliothek SYSLIB.TCP-IP-AP.*nnn*. Falls Sie die Routine in Assembler erstellen wollen, verwenden Sie hierfür den Makro YAPFX. Hierbei ist zu beachten, dass die Routine nach C-Konventionen aufgerufen wird.

Bei Verwendung einer eigenen Routine beachten Sie bitte, dass sich in der Modul-Bibliothek jeweils nur ein einziger Modul mit dem Einsprungspunkt YAPFEXIT befinden darf, da andernfalls evtl. der falsche Modul nachgeladen wird. Sie müssen also insbesondere das mitgelieferte Modul-Element EXITFTP entfernen.

Da der Einsprungspunkt YAPFEXIT standardmäßig nicht angesprungen wird, müssen Sie ihn per FTP-Server-Option bzw. per Kommando aktivieren.

4.12.2.2 Benutzerdefinierte Exit-Routinen

Für die Behandlung der verschiedenen Exits übergeben die Aufrufer der Exit-Routine (FTP-Client oder FTP-Server) an den Einsprungspunkt *YAPFEXIT* die Adresse einer Parameterliste. Die Struktur *YAPFX_pl_mdl* dieser Parameterleiste wird in der Header-Datei *YAPFX.H* der Bibliothek SYSLIB.TCP-IP-AP.*nnn* ausgeliefert. Die Signatur von *YAPFEXIT* lautet wie folgt:

```
void YAPFEXIT (struct YAPFX_pl_mdl*)
```

Struktur YAPFX_pl_mdl

Die Struktur *YAPFX_pl_mdl* ist wie folgt definiert:

```
/* Return codes                                          */
/* ENUM rc_s                                             */
#define YAPFXok 0                    /* Ok               */
#define YAPFXbufTooShort 1           /* Buffer too short */
#define YAPFXother 255               /* Other error      */

/* Caller                                                */
/* ENUM caller_s                                         */
#define YAPFXclient 1                /* Client           */
#define YAPFXserver 2                /* Server           */


/* Action                                                */
/* ENUM action_s                                         */
#define YAPFXrecv 1                  /* Receive          */
#define YAPFXsend 2                  /* Send             */

/* Action modifier                                       */
/* ENUM actionm_s                                        */
#define YAPFXnone 0                  /* None             */
#define YAPFXfirst 1                 /* First            */
#define YAPFXlast 2                  /* Last             */

/* Parameter area */
struct YAPFX_pl_mdl {

/* Input parameters                                         */
  struct {
    unsigned long caller;          /* Calling instance     */
    unsigned short action;         /* Action               */
    unsigned short actionm;        /* Action modifier      */
    void *selector;                /* Selector             */
    char hostname[33];             /* Host name            */
    char reserved1[7];             /* Reserved             */
    unsigned long portNo;          /* Port number                  */
    unsigned long connId;          /* Connection Id (only server)  */
    void *inBuf;                   /* Address of input buffer      */
    unsigned long inBufLen;        /* Length of data in input buffer */
    void *outBuf;                  /* Address of output buffer *   */
    unsigned long outBufLen;       /* Length of output buffer      */
  } in_data;

/* Output parameters                                        */
  struct {
```

```
    unsigned long outDataLen;         /* Lengh of data in output buffer  */
    unsigned long rc;                 /* Return code */
  } out_data;
};
```

Beschreibung der Parameter

caller
zeigt an, ob die Routine vom FTP-Client oder vom FTP-Server aufgerufen wurde.

action
zeigt an, ob der Aufruf vor dem Senden (*YAPFXsend*) oder nach dem Empfangen (*YAPFXrecv*) von Daten erfolgt ist.

actionm
zeigt an, ob der Aufruf der erste oder der letzte ist, der zu dem aktuellen Datentransfer gehört (siehe auch Parameter *connId*). Bei sehr kleinen Dateien können auch beide Flags gleichzeitig gesetzt sein.

selector
Mit *selector* können Sie unter mehreren zur Verfügung stehenden Aktionen die gewünschte Aktion auswählen. Zu diesem Zweck kann der Umwandlungsroutine ein String mitgegeben werden, auf den *selector* verweist. Dabei können Sie frei entscheiden, welche Strings mit welchen Bedeutungen verwendet werden. Lediglich den Strings „*“ und „*NONE“ ist eine feste Bedeutung zugeordnet.

hostName
liefert den Namen des jeweiligen Client-Hosts (mit Null-Byte terminiert).

portNo

wird im Fall *caller* = *YAPFXserver* versorgt und spezifiziert die Portnummer, unter der der aufrufende Server seine Dienste anbietet. Auf diese Weise können mehrere gleichzeitig gestartete Server unterschieden werden.

connId

ermöglicht es bei mehreren aktiven Verbindungen, die einzelnen Verbindungen durch das Paar (*portNo*, *connId*) zu identifizieren. Erforderlich ist dies z.B., wenn verbindungsspezifische Status-Informationen über die Dauer eines Aufrufs hinaus gespeichert und wiedergewonnen werden müssen. Wird beispielsweise bei einem Aufruf als letztes Byte nur das erste Byte einer aus zwei Zeichen bestehenden Zeichenfolge mitgeliefert, so muss dieses Byte so lange zwischengespeichert werden, bis es beim nächsten Aufruf berücksichtigt werden kann.

Wie mit solchen zwischengespeicherten Informationen verfahren werden soll, wird über die Flags in *actionm* gesteuert:

– Bei *YAPFXfirst* müssen Sie Statusinformationen löschen, die von früheren Aufrufen stammen.

– Bei *YAPFXlast* müssen Sie alle zwischengespeicherten Daten zurückliefern.

inBuf

enthält die Adresse des Puffers, in dem die umzuwandelnden Daten stehen (Eingabepuffer).

inBufLen

spezifiziert die Länge (Anzahl der gültigen Bytes) des Eingabepuffers.

outBuf

enthält die Adresse des Ausgabepuffers.

outBuflen

spezifiziert die Länge des Ausgabepuffers.

outDataLen

Vor dem Rücksprung zum Aufrufer muss die Routine in *outDataLen* hinterlegen, wieviele Bytes im Ausgabepuffer gültig sind und somit übertragen werden müssen.

rc

In *rc* zeigt die Umwandlungsroutine an, ob die Umwandlung erfolgreich beendet wurde.

Benutzerdefinierte FTP-Exits unter POSIX schreiben

Da der POSIX-FTP aus dem Zusammenbinden der LLMs FTP und FTPEXIT entsteht, können Sie auch unter POSIX mit den FTP-Exits arbeiten. Der Lieferumfang von interNet Services enthält den Dummy-Modul FTPEXIT, der nur einen Rücksprung ausführt.

Eigene FTP-Exits schreiben Sie wie folgt:

- Erstellen Sie Ihre gewünschte Version des FTPEXIT.
- Binden Sie diese Version mit FTP aus der SYSLNK.TCP-IP-AP.*nnn* zusammen.
- Schreiben Sie das resultierende LLM unter dem Namen FTP in die Bibliothek SINLIB.TCP-IP-AP.*nnn*.
- Installieren Sie anschließend POSIX-FTP (siehe Abschnitt „Installation und Deinstallation von FTP- und TELNET-Client in POSIX“ auf Seite 47).

Ergebnisse und Returncodes der Exit-Routinen

Falls der Ausgabepuffer für die vollständige Umwandlung zu klein ist, muss die Exit-Routine den Returncode YAPFXbufTooShort zurückliefern. In diesem Fall wird die Exit-Routine mit den gleichen Daten, aber größerem Ausgabepuffer erneut aufgerufen. Dies kann u.U. mehrfach erfolgen, bis der Ausgabepuffer groß genug ist oder ein internes Limit des Aufrufers überschritten wird.

Bei allen anderen Fehlern muss die Exit-Routine den Returncode YAPFXother zurückzuliefern. Der Aufrufer wird dann die Übertragung abbrechen und eine entsprechende Fehlerbehandlung einleiten.

4.12.2.3 Benutzerdefinierte Exit-Routinen aktivieren / deaktivieren

Da benutzerdefinierte Umwandlungsroutinen standardmäßig nicht angesprungen werden, müssen sie vor der Benutzung aktiviert werden.

Benutzerdefinierte Exit-Routinen des FTP-Servers aktivieren und deaktivieren

Benutzerdefinierte Exit-Routinen des FTP-Servers können Sie wahlweise im FTP-Server oder im FTP-Client aktivieren.

Benutzerdefinierte Exit-Routine des FTP-Servers im FTP-Server aktivieren

Um die Umwandlungsroutine im FTP-Server zu aktivieren, erweitern Sie in der Enter-Datei des FTP-Servers (SYSENT. TCP-IP-AP.*nnn*.FTPD) die /START-PROGRAM-Anweisung um die Option „-U“ und starten anschließend den FTP-Server:

```
-U [receive: [<recv-selector>]!][send: [<send-selector>]]
```

Der String <recv-selector> bzw. <send-selector> wird beim entsprechenden Aufruf der Umwandlungsroutine im Parameter *selector* übergeben und darf maximal 32 Zeichen lang sein.

Benutzerdefinierte Exit-Routine des FTP-Servers im FTP-Client aktivieren

Vom FTP-Client aus aktivieren Sie Umwandlungsroutinen des FTP-Servers, indem Sie dem Server vom Client aus ein *site exit*-Kommando mit einem Operanden analog zur Server-Option *-U* senden. In diesem Fall wird die Umwandlungsroutine mit diesen Parametern nur für Transfers auf dieser Verbindung aufgerufen. Wenn der FTP-Client aus interNet Services ≥ V2.0 verwendet wird, kann anstatt *quote site exit* ... auch *rexit* ... angegeben werden.

Dabei ist zu beachten:

- Das *site exit*-Kommando hat Vorrang vor der Option *-U*. D.h. auch wenn der FTP-Server mit der Option *-U* gestartet wurde, gelten die Angaben eines vom Client an den Server gesandten *site exit*-Kommandos.
- Durch Senden eines *site exit*-Kommandos mit dem Selektor-String „*“ wird wieder die allgemeine Servereinstellung gemäß Option *-U* gültig gesetzt.

Benutzerdefinierte Exit-Routine des FTP-Servers deaktivieren

Durch Senden eines *site exit*-Kommandos mit dem Selektor-String „*NONE“ wird die Exit-Routine des Servers für die aktuelle Verbindung deaktiviert.

Benutzerdefinierte Exit-Routinen des FTP-Clients aktivieren / deaktivieren

Beim FTP-Client werden benutzerdefinierte Umwandlungsroutinen mit dem *exit*-Kommando aktiviert und deaktiviert.

Benutzerdefinierte Exit-Routine aktivieren

```
exit [receive:[<recv-selector>]!] [send:[<send-selector>]]
```

Für <recv-selector> und <send-selector> müssen Sie jeweils einen konkreten Selektor angeben, der maximal 32 Zeichen lang sein darf.

Benutzerdefinierte Exit-Routine deaktivieren

```
exit receive:*NONE oder send:*NONE oder receive:*NONE!send:*NONE
```

Für <recv-selector> und <send-selector> müssen Sie jeweils `*NONE` angeben.

5 TELNET - Konfiguration und Betrieb

TELNET können Sie entweder über das SDF-Kommando oder über die Option-Datei konfigurieren.

Das Kapitel behandelt folgende Themen zu Konfiguration und Betrieb von TELNET-Servern:

- Verwendung von TLS/SSL zur Absicherung von TELNET-Server (siehe Seite 138).
- Konfiguration von TELNET über SDF-Kommando (siehe Seite 140) oder via Option-Datei (siehe Seite 150).
- Starten und beenden von TELNET-Servern (siehe Seite 176).
- Sichern der Protokolldatei von TELNET-Servern (siehe Seite 180).
- Anzeigen der aktuellen Einstellungen des TELNET-Servers (siehe Seite 181).
- Angabe von Kommandos über die Konsolschnittstelle (siehe Seite 184).
- Verwendung von IPv6-Adressen in TELNET (siehe Seite 186).
- Exits für TELNET-Client und den TELNET-Server (siehe Seite 187).

5.1 TLS/SSL-Unterstützung im TELNET-Server

Die TLS/SSL-Unterstützung im TELNET-Server bietet ein breites Spektrum an Einstellmöglichkeiten. Die Einstellungen können Sie wahlweise wie folgt vornehmen:

- Mithilfe von Options, die in einer oder mehreren Option-Dateien hinterlegt werden, und beim Start des TELNET-Servers ausgewertet werden (siehe Abschnitt „Konfiguration von TELNET via Option-Datei“ auf Seite 150).
- Mithilfe von Parametern des Installationskommandos SET-FTP-TELNET-PARAMETERS (siehe Abschnitt „Konfiguration von TELNET via Installationskommando SET-FTP-TELNET-PARAMETERS“ auf Seite 140).

Parametrisierung der TLS/SSL-Unterstützung im TELNET-Server

Im Folgenden finden Sie einen Überblick über die Einstellmöglichkeiten zur TLS/SSL-Unterstützung im TELNET-Server mithilfe der Options. Den einzelnen Options entsprechen korrespondierende Parameter des SET-FTP-TELNET-PARAMETERS-Kommandos.

Zur Parametrisierung der TLS/SSL-Unterstützung im TELNET-Server stehen die folgenden Options zur Verfügung:

- START-TLS-Option (*-Z tls-required*, siehe Seite 159)

  Mit dieser Option steuern Sie die TLS-Unterstützung im TELNET-Server. Hierfür stehen eine Reihe zusätzlicher Options (*-Z*-Options) zur Verfügung (siehe Tabelle auf Seite 139). Das Aushandeln der Authentifizierungsmodalitäten übernimmt SSL, so dass TELNET nicht davon belastet wird.

- AUTHENTICATION-Option (*-B*, siehe Seite 174)

  Diese Option verwenden Sie, um die Authentifizierungsmodalitäten auszuhandeln. Im BS2000 ist die AUTHENTICATION-Option derzeit nur für TLS/SSL realisiert.

  Mit der für TLS/SSL realisierten AUTHENTICATION-Option können Sie die TLS-Unterstützung im TELNET-Server steuern. Hierfür verwenden Sie die gleichen *-Z*-Options wie bei der START-TLS-Option (siehe Tabelle auf Seite 139).

- ENCRYPTION-Option (*-H*, Seite 175)

  Diese Option verwenden Sie, um das Verschlüsselungsverfahren sowie den verwendeten Schlüssel auszuhandeln. Derzeit wird in TELNET nur DES64 in den Varianten DES_CFB64 und DES_OFB64 unterstützt.

START-TLS-Option und AUTHENTICATION-Option dürfen nicht gleichzeitig aktiviert sein. In der folgenden Tabelle sind die Options aufgelistet, mit denen Sie in Verbindung mit der START-TLS- bzw. AUTHENTICATION-Option die TLS/SSL-Unterstützung im TELNET-Server steuern können.

Option	Beschreibung	Seite
-Z Protocol	SSL-Protokollversionen selektiv auswählen	169
-Z CipherSuite	Verschlüsselungsverfahren-Vorzugsliste spezifizieren	166
-Z RSAcertificateFile	Datei spezifizieren, die das RSA-basierte X.509-Server-Zertifikat im PEM-Format enthält	160
-Z RSAkeyFile	Datei spezifizieren, die den privaten RSA-Server-Schlüssel im PEM-Format enthält	161
-Z DSACertificateFile	Datei spezifizieren, die das DSA-basierte X.509-Server-Zertifikat im PEM-Format enthält	162
-Z DSAkeyFile	Datei spezifizieren, die den privaten DSA-Server-Schlüssel im PEM-Format enthält	163
-Z CertificateChainFile	Datei spezifizieren, in der alle Zertifikate abgelegt werden können, die für die Verifikation des Server-Zertifikats benötigt werden	168
-Z CACertificateFile	Datei spezifizieren, die die für die Authentifizierung des TELNET-Clients erforderlichen Zertifikate im PEM-Format enthält	164
-Z AcceptableClientCAFile	Datei spezifizieren, aus denen die Namen der CAs hervorgehen, die der Server als Unterzeichner von Client-Zertifikaten akzeptiert	170
-Z CARevocationFile	Datei spezifizieren, die die CRLs der CAs enthält	165
-Z VerifyClient	Festlegen, ob der TELNET-Client ein Zertifikat für den Server-Zugang vorweisen muss	172
-Z VerifyDepth	Verifizierungstiefe festlegen	171
-Z RandFile	Datei spezifizieren, aus der beim Server-Start die Daten für die Initialisierung des PRNG gelesen werden	167
-Z OpenSSLlibName	Festlegen, aus welcher LMS-Datei die OpenSSL-Bibliothek nachgeladen werden soll	173

5.2 Konfiguration von TELNET via Installationskommando SET-FTP-TELNET-PARAMETERS

Für die komplette Kommando-Syntax und die Beschreibung der Installations-Operanden, siehe Seite 42.

SET-FTP-TELNET-**PAR**AMETERS

(...)

, TELNET-**SERVER-PROC= *NO / *CRE**ATE(...)

***CRE**ATE(...)

JOB-NAME= *STD / <name 1..5>

, JOB-CLASS= *STD / <name 1..8>

, CPU-TIME= *STD / <integer 1..32767>

, PRIORITY**= *STD** / <integer 0..255>

, DEBUG= *STD / <integer 0..9>

, TRACE= *STD / <integer 0..10>

, MAXIMUM-**CONN**ECTIONS**= *STD** / <integer 1..900>

, STATION-**ID= *STD** / <integer 0..6>

, ASCII-TABLE**= *STD** / <text 1..8>

, EBCDIC-TABLE**= *STD** / <name 1..8>

, TLS-SUPPORT= *STD / ***NO** / ***PARAMETERS(...)**

***PARAMETERS (...)**

OPTION= *STD / ***START-TLS** / ***AUTHENTICATION(...)**

***AUTHENTICATION(...)**

DEBUG= *STD / ***NO** / ***YES**

, PROTOCOL= *STD / <text 1..80>

, CIPHER-SUITE = *STD / <text 1..80_with-lower-case>

, RSA-CERTIFICATE-FILE = *STD / ***NONE** / <filename 1..54_without-generation-version>

, RSA-KEY-FILE = *STD / ***NONE** / <filename 1..54_without-generation-version>

, DSA-CERTIFICATE-FILE = *STD / ***NONE** / <filename 1..54_without-generation-version>

, DSA-KEY-FILE = *STD / ***NONE** / <filename 1..54_without-generation-version>

, CA-CERTIFICATE-FILE = *STD / ***NONE** / <filename 1..54_without-generation-version>

, CLIENT-CA-FILE = *STD / ***NONE** / <filename 1..54_without-generation-version>

, CERT-CHAIN--FILE = *STD / ***NONE** / <filename 1..54_without-generation-version>

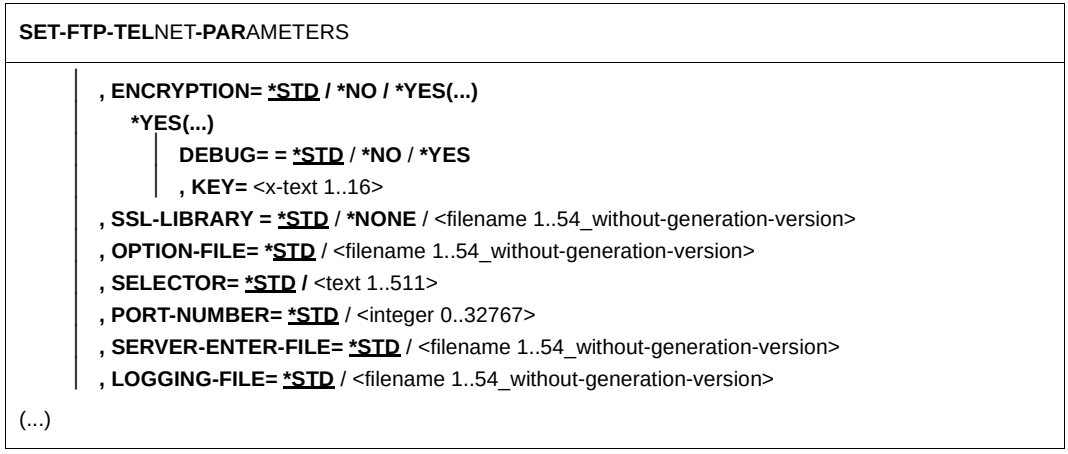
, CA-REVOCATION-FILE = *STD / ***NONE** / <filename 1..54_without-generation-version>

, RANDOM-FILE = *STD / <filename 1..54_without-generation-version>

, SSL-LIBRARY = *STD / ***NONE** / <filename 1..54_without-generation-version>

, VERIFY-CLIENT= *STD / ***NONE** / ***OPTIONAL** / ***REQUIRE**

, VERIFY-DEPTH= *STD / <1..32767>



TELNET-SERVER-PROC=
Parameter für TELNET-Server

TELNET-SERVER-PROC=*NO
Es soll keine Installation für den TELNET-Server durchgeführt werden.

TELNET-SERVER-PROC=*CREATE(...)
Der TELNET-Server soll konfiguriert werden. Aus den eingegebenen Parametern wird die Enter-Datei zum Start des TELNET-Servers erstellt.

JOB-NAME=
Dieser Name wird als Präfix verwendet. Um den Datenstationsnamen der jeweiligen Verbindung zu erhalten, wird an den JOB-NAME die laufende Nummer angehängt. Siehe auch Option *-A* auf Seite 152.

JOB-NAME=*STD
Entspricht der Angabe TELSR bzw. dem Wert in der Installationsdatei.

JOB-NAME=<name 1..5>
Job-Name, der als Prefix verwendet wird.

JOB-CLASS=
Jene Jobklasse, in welcher der Serverprozess laufen soll. Stellen Sie sicher, dass in dieser Jobklasse Enter-Jobs mit folgenden Parametern gestartet werden dürfen: CPU-LIMIT=*NO, RUN-PRIORITY=120 sowie START=*IMMEDIATELY.

JOB-CLASS=*STD
Entspricht der Standard-Jobklasse des Systems bzw. dem Wert in der Installationsdatei.

JOB-CLASS=<name 1..8>
Name der Job-Klasse.

CPU-TIME=
CPU-Zeit, die für den Serverprozess maximal zur Verfügung steht.

CPU-TIME=*STD
Entspricht der Angabe NTL bzw. dem Wert in der Installationsdatei.

CPU-TIME=<integer 1..32767>
CPU-Zeit, die für den Serverprozess maximal zur Verfügung steht.

PRIORITY=
Priorität, mit der der Serverprozess laufen soll.

PRIORITY=*STD
Entspricht der Angabe 120 bzw. dem Wert in der Installationsdatei.

PRIORITY=<integer 0..255>
Priorität, mit der der Serverprozess laufen soll.

DEBUG=
Trace zur Benutzerebene. Siehe auch Option *-D* auf Seite 152.

DEBUG=*STD
Entspricht der Angabe 0 bzw. dem Wert in der Installationsdatei.

DEBUG=<integer 0..9>
Debug-Level

TRACE=
Trace zur TCP/IP-(Socket)-Schnittstelle. Siehe auch Option *-T* auf Seite 155.

TRACE=*STD
Entspricht der Angabe 0 bzw. dem Wert in der Installationsdatei.

TRACE=<integer 0..10>
Socket-Trace-Level

MAXIMUM-CONNECTIONS=
Maximale Anzahl von Verbindungen, die der Server bedienen soll. Siehe auch Option *-N* auf Seite 153.

MAXIMUM-CONNECTIONS=*STD
Entspricht der Angabe 15 bzw. dem Wert in der Installationsdatei.

MAXIMUM-CONNECTIONS=<integer 1..900>
Maximale Anzahl von Verbindungen, die der Server bedienen soll.

STATION-ID=
Anzahl der Stellen, mit denen der Name des fernen Rechners bzw. der Job-Name des TELNET-Servers im Datenstationsnamen berücksichtigt werden soll. Siehe auch Option *-S* auf Seite 154.

STATION-ID=*STD
Entspricht der Angabe 0 bzw. dem Wert in der Installationsdatei.

STATION-ID=<integer 0..6>
Anzahl der Stellen, mit denen der Name des fernen Rechners bzw. der Job-Name des TELNET-Servers im Datenstationsnamen berücksichtigt werden soll.

ASCII-TABLE=
Standard-ASCII-Codetabelle (ISO 88591). Siehe auch Option *-X* auf Seite 156.

ASCII-TABLE=*STD
Entspricht der Angabe von 8 Blanks bzw. dem Wert in der Installationsdatei.

ASCII-TABLE=<text 1..8>
Standard-ASCII-Codetabelle.
Ein nicht-leerer Wert für ASCII-TABLE (als Kommandoparameter angegeben oder - falls ASCII-TABLE=*STD - als Wert in der evtl. angegebenen Installationsdatei), ist nur dann wirksam, wenn auch EBCDIC-TABLE (als Kommandoparameter angegeben oder - falls EBCDIC-TABLE=*STD - als Wert in der evtl. angegebenen Installationsdatei) nicht einen leeren Wert besitzt.

EBCDIC-TABLE=
Standard-EBCDIC-Code-Tabelle (EDF041). Siehe auch Option *-X* auf Seite 156.

EBCDIC-TABLE=*STD
Entspricht der Angabe von 8 Blanks bzw. dem Wert in der Installationsdatei.

EBCDIC-TABLE=<name 1..8>
Standard-EBCDIC-Code-Tabelle.
Ein nicht-leerer Wert für EBCDIC-TABLE (als Kommandoparameter angegeben oder, falls EBCDIC-TABLE=*STD gesetzt ist, als Wert in der evtl. angegebenen Installationsdatei), ist nur dann wirksam, wenn auch ASCII-TABLE (als Kommandoparameter angegeben oder - falls ASCII-TABLE=*STD - als Wert in der evtl. angegebenen Installationsdatei) nicht einen leeren Wert besitzt.

TLS-SUPPORT=
Festlegung, ob die Verbindung mit TLS/SSL abgesichert werden soll.

TLS-SUPPORT=*STD
Voreinstellung: *NO.

TLS-SUPPORT=*NO
Der TELNET-Server führt keine Absicherung der Verbindungen mithilfe der TELNET-Option START-TLS durch.

TLS-SUPPORT=*PARAMETERS(...)
Der TELNET-Server führt eine Absicherung der Verbindungen via TLS/SSL durch.

OPTION=
TELNET-Option zur Durchführung von TLS/SSL. Siehe auch Option *-Z tls-required* auf Seite 159.

OPTION=*STD
Voreinstellung: START-TLS

OPTION=*START-TLS
TLS/SSL wird über die TELNET-Option START-TLS durchgeführt.

OPTION=*AUTHENTICATION(...)
TLS/SSL wird über die TELNET-Option AUTHENTICATION durchgeführt. Siehe auch Option *-B* auf Seite 174.

DEBUG=
Schalter für den Authentication-Trace.

DEBUG=*STD
Voreinstellung: *NO

DEBUG=*NO
Authentication-Trace nicht einschalten.

DEBUG=*YES
Authentication-Trace einschalten.

PROTOCOL=
Siehe Option *-Z Protocol* Seite 169.

PROTOCOL=*STD
Voreinstellung: ALL-SSLv2

PROTOCOL=<text 1..80>
Spezifikation des zu verwendenden TLS/SSL-Protokolls.

CIPHER-SUITE=
Siehe Option *-Z CipherSuite* auf Seite 166.

CIPHER-SUITE=*STD
Voreinstellung: ALL:!EXP:!ADH

CIPHER-SUITE=<text 1..80_with-lower-case>
Spezifikation der zu verwendenden Verschlüsselungs-Algorithmen.

RSA-CERTIFICATE-FILE=
Siehe Option *-Z RSAcertificateFile* auf Seite 160.

RSA-CERTIFICATE-FILE=*STD
Voreinstellung: *NONE

RSA-CERTIFICATE-FILE=*NONE
Es wird keine RSA-Zertifikats-Datei angegeben.

RSA-CERTIFICATE-FILE=<filename 1..54_without-generation-version>
Name der RSA-Zertifikats-Datei.

RSA-KEY-FILE=
Siehe Option *-Z RSAkeyFile* auf Seite 161.

RSA-KEY-FILE=*STD
Voreinstellung: *NONE

RSA-KEY-FILE=*NONE
Es wird keine RSA-Schlüssel-Datei angegeben.

RSA-KEY-FILE=<filename 1..54_without-generation-version>
Name der RSA-Schlüssel-Datei.

DSA-CERTIFICATE-FILE=
Siehe Option *-Z DSAcertificateFile* auf Seite 162.

DSA-CERTIFICATE-FILE=*STD
Voreinstellung: *NONE

DSA-CERTIFICATE-FILE=*NONE
Es wird keine DSA-Zertifikats-Datei angegeben.

DSA-CERTIFICATE-FILE=<filename 1..54_without-generation-version>
Name der DSA-Zertifikats-Datei.

DSA-KEY-FILE=
Siehe Option *-Z DSAkeyFile* auf Seite 163.

DSA-KEY-FILE=*STD
Voreinstellung: *NONE

DSA-KEY-FILE=*NONE
Es wird keine DSA-Schlüssel-Datei angegeben.

DSA-KEY-FILE=<filename 1..54_without-generation-version>
Name der DSA-Schlüssel-Datei.

CA-CERTIFICATE-FILE=
Siehe Option *-Z CACertificateFile* auf Seite 164.

CA-CERTIFICATE-FILE=*STD
Voreinstellung: *NONE

CA-CERTIFICATE-FILE=*NONE
Es wird keine CA-Zertifikats-Datei angegeben.

CA-CERTIFICATE-FILE=<filename 1..54_without-generation-version>
Name der CA-Zertifikats-Datei.

CLIENT-CA-FILE=
Siehe Option *-Z AcceptableClientCAFile* auf Seite 170.

CLIENT-CA-FILE=*STD
Voreinstellung: *NONE

CLIENT-CA-FILE=*NONE
Es wird keine Datei angegeben.

CLIENT-CA-FILE=<filename 1..54_without-generation-version>
Name der Datei mit den Zertifikaten der akzeptierten CAs.

CERT-CHAIN-FILE=
Siehe Option *-Z CertificateChainFile* auf Seite 168.

CERT-CHAIN-FILE=*STD
Voreinstellung: *NONE

CERT-CHAIN-FILE=*NONE
Es wird keine CA-Zertifikatsketten-Datei angegeben.

CERT-CHAIN-FILE=<filename 1..54_without-generation-version>
Name der CA-Zertifikatsketten-Datei.

CA-REVOCATION-FILE=
Siehe Option *-Z CARevocationFile* auf Seite 165.

CA-REVOCATION-FILE=*STD
Voreinstellung: *NONE

CA-REVOCATION-FILE=*NONE
Es wird keine CA-Wiederruf-Datei angegeben.

CA-REVOCATION-FILE=<filename 1..54_without-generation-version>
Name der CA-Wiederruf-Datei (CRL).

RANDOM-FILE=
Siehe Option *-Z RandFile* auf Seite 167.

RANDOM-FILE=*STD
Voreinstellung: SYSDAT.TCP-IP-AP.*nnn*.TELNETD.RAND

RANDOM-FILE=<filename 1..54_without-generation-version>
Name der Datei, die die Daten für die Initialisierung des PRNG enthält.

SSL-LIBRARY=
Siehe Option *-Z OpenSSLlibName* auf Seite 173.

SSL-LIBRARY=*STD
Voreinstellung: LMS-Bibliothek, auf die die IMON Logical-ID SYSLNK verweist.

SSL-LIBRARY=*NONE
Es wird keine LMS-Bibliothek angegeben.

SSL-LIBRARY=<filename 1..54_without-generation-version>
Name der LMS-Bibliothek, die den OpenSSL-Nachlade-Modul enthält.

VERIFY-CLIENT=
Siehe Option *-Z VerifyClient* auf Seite 172.

VERIFY-CLIENT=*STD
Voreinstellung: *NONE

VERIFY-CLIENT=*NONE
Es wird kein Zertifikat vom TELNET-Client angefordert.

VERIFY-CLIENT=*OPTIONAL
Es wird ein Zertifikat vom TELNET-Client angefordert. Wird aber kein oder nur ein ungültiges Zertifikat zurückgeschickt, so wird dem TELNET-Client dennoch der Zugang erlaubt.

VERIFY-CLIENT=*REQUIRE
Es wird ein Zertifikat vom TELNET-Client angefordert. Wird kein oder nur ein ungültiges Zertifikat zurückgeschickt, dann wird dem TELNET-Client der Zugang verweigert.

VERIFY-DEPTH=
Siehe Option *-Z VerifyDepth* auf Seite 171.

VERIFY-DEPTH=*STD
Voreinstellung: 1

VERIFY-DEPTH=<integer 0..32767>
Anzahl der Zertifikate zwischen dem Client-Zertifikat und dem Zertifikat, das dem TELNET-Server bekannt ist (inklusive letzterem).

ENCRYPTION=*STD / *NO / *YES(...)
Legt fest, ob der TELNET-Server die Encryption der Verbindung mithilfe der ENCRYPTION-Option durchführt. Siehe auch Option *-H* auf Seite 175.

ENCRYPTION=*STD
Voreinstellung: *NO.

ENCRYPTION=*NO
Der TELNET-Server führt keine Encryption der Verbindungen mittels der ENCRYPTION-Option durch.

ENCRYPTION=*YES(...)
Der TELNET-Server führt (prinzipiell) eine Encryption der Verbindungen mittels der ENCRYPTION-Option durch.

ENCRYPTION=*YES(...) darf nur dann angegeben werden, wenn nicht gleichzeitig TLS-SUPPORT=*PAR(...) spezifiziert ist.

DEBUG=
Schalter für den Encryption-Trace.

DEBUG=*STD
Voreinstellung: *NO

DEBUG=*NO
Encryption-Trace nicht einschalten.

DEBUG=*YES
Encryption-Trace einschalten.

KEY=<x-text 1..16>
Für die DES 64-Encryption zu verwendender Schlüssel.
Der Schlüssel muss ohne Hochkommata angegeben werden und wird als Sedezimal-String interpretiert.
Beispiel:
Der Schlüssel „TELNET“ lautet in sedezimaler Darstellung E3C5D3D5C5E3 und muss wie folgt spezifiziert werden:
... ENCRYPTION=*YES(KEY=E3C5D3D5C5E3)

SSL-LIBRARY=
Siehe Option *-Z OpenSSLlibName* auf Seite 173.

SSL-LIBRARY=*STD
Voreinstellung: LMS-Bibliothek, auf die die IMON Logical-ID SYSLNK verweist.

SSL-LIBRARY=*NONE
Es wird keine LMS-Bibliothek angegeben.

SSL-LIBRARY=<filename 1..54_without-generation-version>
Name der LMS-Bibliothek, die den OpenSSL-Nachlade-Modul enthält.

OPTION-FILE=
Datei, in der die Optionen hinterlegt werden.

OPTION-FILE=*STD
Voreinstellung: SYSDAT.TCP-IP-AP.*nnn*.TELNETD.OPT

OPTION-FILE=<filename 1..54_without-generation-version>
Name der Option-Datei.

SELECTOR=
Selector für TELNET-Exit-Routinen. Siehe auch Option *−E* auf Seite 153.

SELECTOR=*STD
Voreinstellung: Keine Exits

SELECTOR=<text 1..511>
Spezifiziert den Selektor für die TELNET-Exit-Routinen.

PORT-NUMBER=
Portnummer unter der der TELNET-Server gestartet wird. Siehe auch Option *-P* auf Seite 154.

PORT-NUMBER=*STD
Voreinstellung: 23

PORT-NUMBER=<integer 0..32767>
Spezifiziert die Portnummer, unter der der TELNET-Server gestartet wird.

SERVER-ENTER-FILE=
Name der Start-Datei für den TELNET-Server.

SERVER-ENTER-FILE=*STD
Voreinstellung: SYSENT.TCP-IP-AP.*nnn*.TELNETD

SERVER-ENTER-FILE=<filename 1..54_without-generation-version>
Spezifiziert den Namen der Start-Datei für den TELNET-Server.

LOGGING-FILE=
Name der Protokoll-Datei für den TELNET-Server.

LOGGING-FILE=*STD
Voreinstellung: SYSOUT.TCP-IP-AP.*nnn*.TELNETD

LOGGING-FILE=<filename 1..54_without-generation-version>
Spezifiziert den Namen der Protokoll-Datei für den TELNET-Server.

5.3 Konfiguration von TELNET via Option-Datei

Bei der Ausführung des Kommandos SET-FTP-TELNET-PARAMETERS (siehe Seite 42/Seite 140) wird eine Option-Datei erzeugt, in der die einzelnen TELNET-Server-Parameter als Options abgelegt sind. Der Standarddateiname der Option-Datei lautet:

SYSDAT.TCP-IP-AP.*nnn*.TELNETD.OPT

Wenn eine Datei dieses Namens in der Ablaufkennung des TELNET-Servers existiert, wird sie beim Start des TELNET-Servers über die Start-Datei des TELNET-Servers (Standard-Dateiname: SYSENT.TCP-IP-AP.*nnn*.TELNETD) ausgewertet, und der TELNET-Server wird entsprechend konfiguriert.

Somit können Sie Änderungen der TELNET-Server-Parameter via Option-Datei vornehmen, ohne erneut die Installation mithilfe des SET-FTP-TELNET-PARAMETERS-Kommandos starten zu müssen.

Wollen Sie eine Datei anderen Namens als Option-Datei verwenden, so geben Sie in der Start-Datei die folgende Option an:

-M *option-datei-name*

Diese Datei wird dann anstatt einer eventuell vorhandenen Datei SYSDAT.TCP-IP-AP.*nnn*.TELNETD.OPT ausgewertet.

Für die Priorität der Options gilt die Reihenfolge:

1. Options, die in der Startprozedur angegeben sind
2. Options, die
   - in der via *-M*-Option spezifizierten Option-Datei angegeben sind oder,
   - falls keine *-M*-Option angegeben wurde, in der Standard-Option-Datei SYSDAT.TCP-IP-AP.*nnn*.TELNETD.OPT angegeben sind.

Option-Datei und Parameterzeilen-Options

Auch die bereits in früheren Versionen unterstützten Parameterzeilen-Options können Sie in der Option-Datei spezifizieren. Eine gemischte Anwendung von Option-Datei und Options in der Parameterzeile ist ebenfalls möglich. Wenn eine bestimmte Option sowohl in der Parameterzeile als auch in der Option-Datei angegeben ist, hat die in der Parameterzeile spezifizierte Option Vorrang.

Notation der Options in der Option-Datei

Die einzelnen Options müssen gemäß den folgenden Regeln in die Option-Datei eingetragen sein:

- Es können beliebig viele Options in einer Zeile stehen.
- Erstrecken sich die Options über mehrere Zeilen, dann muss jede fortzusetzende Zeile mit dem Fortsetzungszeichen „\“ abgeschlossen werden.
- Eine Zeile, die mit dem Zeichen „#“ in Spalte 1 beginnt, wird beim Einlesen ignoriert.
- Bei den Option-Namen wird Klein-/Groß-Schreibung nicht unterschieden.

5.3.1 Options für die allgemeine Konfiguration des TELNET-Servers

-A - Namens-Präfix spezifizieren

Mit der Option *-A* wird ein Namens-Präfix spezifiziert. Dieser Präfix wird zur Bildung eines Datenstationsnamens verwendet, indem eine laufende Nummer angehängt wird. Der vom Server für jeden Client gestartete Job erhält als Job-Namen diesen Präfix.

-A
<text 1..8>

<job-namen-präfix>
Namens-Präfix
Voreinstellung: TELSR

-D - Debug-Level

Mit der Option *-D* wird ein Debug-Level spezifiziert, der angibt, ob bzw. welche Diagnose-Informationen bezüglich des TELNET-Server-Ablaufs in die Protokolldatei geschrieben werden sollen.

-D
<integer 0..2>

<integer 0..2>
Debug-Level.
Mit dem Wert 0 wird die Protokollierung ausgeschaltet. Je höher der angegebene Wert ist, umso mehr Informationen werden in der Protokolldatei hinterlegt.
Voreinstellung: 0

-E - Exit-Routinen spezifizieren

Mit der Option -*E* können benutzer-definierte Exit-Routinen des TELNET-Servers aktiviert bzw. deaktiviert werden. Der Aufbau der Selektor-Routinen ist beschrieben im Abschnitt „Exit-Routinen“ auf Seite 188.

-E
<Selektor-Definition 1..511>

<Selektor-Definition>
Selektor-Definition

-N - Anzahl der Verbindungen spezifizieren

Mit der Option -*N* wird die Anzahl der Verbindungen festgelegt, die der TELNET-Server gleichzeitig bedienen soll.

-N
<integer 1..900>

<integer 1..900>
Anzahl der Verbindungen, die der Server gleichzeitig bedienen soll.
Voreinstellung: 15

-P - Portnummer spezifizieren

Mit der Option *-P* wird die Portnummer spezifiziert, unter der der Server erreichbar ist.

-P
<integer 1..1023>

<integer 1..1023>
Portnummer
Voreinstellung: 23

-S - Datenstationsnamen festlegen

Mit der Option *-S* wird die Anzahl der Stellen spezifiziert, mit denen der Name des fernen Rechners bzw. der Namens-Präfix (siehe Option *-A*) des TELNET-Servers im Datenstationsnamen berücksichtigt werden soll.

-S
<integer 0..6>

<integer 0..6>
Anzahl der Stellen.
Voreinstellung: 0

-T - Socket-Trace-Level spezifizieren

Mit der Option -*T* wird der Socket-Trace-Level spezifiziert. Der Socket-Trace-Level gibt an, ob bzw. welche Diagnose-Information des TCP-IP-(Socket-)Systems in die Protokolldatei geschrieben werden sollen.

-T
<integer 0..10>

<integer 0..10>
Socket-Trace-Level.
Mit dem Wert 0 wird die Protokollierung ausgeschaltet. Je höher der spezifizierte Wert ist, um so mehr Informationen werden in der Protokolldatei hinterlegt.
Voreinstellung: 0

-V - Verbose ein-/ausschalten

Die Option -*V* ist eine Kurzform für `-D 1` und `-T 1`.

-V

-X - Code-Tabellen einstellen

Mit der Option *-X* werden die gültigen EBCDIC- und ISO-Code-Tabellen eingestellt. Die Angaben der Option *-X* sind nur dann gültig, wenn in der Datei SYSDAT.TCP-IP-AP.*nnn*.CLIENTS keine abweichenden Einstellungen vorgenommen wurden. Dabei ist zu beachten, dass der TELNET-Server nur 7-Bit-Terminals unterstützt und die Angabe einer 8-Bit-Iso-Tabelle somit nicht sinnvoll ist.

-X
<ebcdic-code-tabelle>:<iso-code-tabelle>

<ebcdic-code-tabelle>:<iso-code-tabelle>
Gültige EBCDIC-Code-Tabelle und gültige ISO-Code-Tabelle.
Voreinstellung: EDF041: ISO88591

5.3.2 Options für den sicheren Einsatz von TELNET mithilfe von Authentifizierung und Verschlüsselung

Es gibt drei Verfahren, um den sicheren Einsatz von TELNET mithilfe Authentifizierung und Verschlüsselung zu gewährleisten:

- START-TLS-Option

  Die START-TLS-Option wurde ausschließlich für TLS/SSL implementiert. Im BS2000 wird sie durch die Server-Option *-Z tls-required* unterstützt.

- „Telnet Authentication Option“ (RFC 2941) für das Aushandeln eines Authentifizierungsverfahrens.

  Im BS2000 /OSD wird derzeit nur TLS/SSL unterstützt. Eingestellt wird die „Telnet Authentication Option“ durch die Server-Option *-B*. Die „Telnet Authentication Option“ wird in Zukunft möglicherweise an Bedeutung gewinnen, weil mit ihr die verschiedensten Authentifizierungsverfahren unterstützt werden können, u.a. auch Kerberos. Im Folgenden wird die „Telnet Authentication Option“ als AUTHENTICATION-Option bezeichnet.

- „Telnet Data Encryption Option“ (RFC 2946) für aus Aushandeln eines symmetrischen Verschlüsselungsverfahrens und des zugehörigen Schlüssels.

  Im BS2000 wird derzeit nur DES 64 (RFC 2952, RFC 2953) unterstützt. Eingestellt wird die „Telnet Data Encryption Option“ durch die Server-Option *-H*. Die „Telnet Data Encryption Option“ wird im Folgenden als ENCRYPTION-Option bezeichnet.

START-TLS-Option (siehe Seite 158), AUTHENTICATION-Option (siehe Seite 174) und ENCRYPTION-Option (siehe Seite 175) sind in den nachfolgenden Abschnitten ausführlich beschrieben.

Bei den nachfolgenden Optionen gilt, dass das Gleichheitszeichen ohne Leerzeichen direkt auf den Optionsnamen folgen muss und der Optionswert ebenfalls ohne Leerzeichen direkt auf das Gleichheitszeichen folgt.

5.3.3 Option -Z - Unterstützung der START-TLS-Option

Mit dieser Option können Sie die TLS-Unterstützung im TELNET-Server steuern. Das Aushandeln der Authentifizierungsmodalitäten übernimmt in diesem Fall SSL, so dass TELNET nicht davon belastet wird.

Die Options für die Nutzung der TLS-Unterstützung geben Sie wie folgt an:

```
-Z <option>
```

Zeitpunkt, zu dem Options bzw. Option-Änderungen wirksam werden

Die Option *-Z OpenSSLlibName* wird während einer TELNET-Sitzung nur einmal ausgewertet, und zwar zum Zeitpunkt des Ladens der OpenSSL-Bibliothek. Alle anderen Options werden wirksam, nachdem die Verbindung zum TELNET-Client aufgebaut ist.

Beschreibung der -Z-Options

Nachfolgend sind die -Z-Options beschrieben.

Dabei ist zu beachten:

- Mit Ausnahme der Option *-Z tls-required* können alle *-Z*-Options auch für die AUTHENTICATION-Option (siehe Seite 174) verwendet werden, da diese mit TLS/SSL-Unterstützung arbeitet.
- Die Option *-Z OpenSSLlibName* ist auch für die ENCRYPTION-Option relevant, da ausschließlich Encryption-Routinen aus der OpenSSL-Bibliothek verwendet werden.
- Die gleichzeitige Angabe der ENCRYPTION-Option (*-H*, siehe Seite 175) und einer der Options START-TLS-Option (*-tls-required*, siehe Seite 158) oder AUTHENTICATION-Option (*-B*, siehe Seite 174) führt beim Start des TELNET-Servers zu einem Fehler.
- Die gleichzeitige Angabe von START-TLS-Option (*-Z tls-required*) und AUTHENTICATION-Option (*-B*) führt beim Start des TELNET-Servers zu einem Fehler.

-Z tls-required

Mit der Option *-Z tls-required* wird die TLS-Absicherung über die START-TLS-Option im TELNET-Server ein- oder ausgeschaltet.

-Z tls-required
[={ **yes** | **no** | optional }]

yes
START-TLS-Unterstützung wird eingeschaltet. Kann keine TLS-Absicherung der Verbindung aufgebaut werden, dann wird die Verbindung wieder beendet.

optional
START-TLS-Unterstützung wird eingeschaltet. Kann keine TLS-Absicherung der Verbindung aufgebaut werden, dann wird die Verbindung ohne eine solche Absicherung verwendet.

no
START-TLS-Unterstützung wird ausgeschaltet.

-Z tls-required ohne Operanden spezifiziert
Es gilt *-Z tls-required = yes* (START-TLS-Unterstützung wird eingeschaltet).

-Z tls-required nicht angegeben
START-TLS-Unterstützung nicht eingeschaltet (Voreinstellung).

-Z RSACertificateFile

Mit der Option *-Z RSACertificateFile* wird eine Datei spezifiziert, die das RSA-basierte X.509-Server-Zertifikat im PEM-Format enthält. Diese Datei kann auch den privaten RSA-Server-Schlüssel enthalten. In der Regel werden aber Zertifikat und Schlüssel in getrennten Dateien abgelegt. In diesem Fall wird die Schlüsseldatei mithilfe der Option *-Z RSAKeyFile* (siehe Seite 161) spezifiziert.

-Z RSACertificateFile
={<dateiname 1 .. 54> | ***NONE**}

<dateiname 1 .. 54>
Name der Datei, die das RSA-basierte X.509-Server-Zertifikat im PEM-Format enthält.

***NONE**
Es wird keine Datei spezifiziert.
*NONE ist Voreinstellung.

-Z RSAKeyFile

Mit der Option *-Z RSAKeyFile* wird eine Datei spezifiziert, die den privaten RSA-Server-Schlüssel im PEM-Format enthält.

Wenn sowohl X.509-Client-Zertifikat als auch privater Server-Schlüssel innerhalb derselben Datei enthalten sind (siehe Option *-Z RSACertificateFile* auf Seite 160), braucht die Option *-Z RSAKeyFile* nicht angegeben zu werden.

Da es möglich sein soll, den TELNET-Server im unbedienten Betrieb automatisch hochzufahren, kann beim Server-Start keine Pass-Phrase für den privaten Server-Schlüssel eingegeben werden. Deshalb müssen Sie eine eventuell vorhandene Verschlüsselung des privaten Schlüssels mit Pass-Phrase entfernen. Verhindern Sie in diesem Fall unbedingt, dass unbefugte Personen auf diesen Schlüssel zugreifen können.

-Z RSAKeyFile
={<dateiname 1 .. 54> | ***NONE**}

<dateiname 1 .. 54>
Name der Datei, die den privaten RSA-Server-Schlüssel enthält.

***NONE**
Es wird keine eigene Datei für den RSA-Server-Schlüssel verwendet.
*NONE ist Voreinstellung.

-Z DSACertificateFile

Mit der Option *-Z DSACertificateFile* wird eine Datei spezifiziert, die das DSA-basierte X.509-Server-Zertifikat im PEM-Format enthält. Diese Datei kann auch den privaten DSA-Server-Schlüssel enthalten. In der Regel werden aber Zertifikat und Schlüssel in getrennten Dateien abgelegt. In diesem Fall wird die Schlüsseldatei mithilfe der Option *-Z DSAKeyFile* (siehe Seite 163) spezifiziert.

-Z DSACertificateFile
={<dateiname 1 .. 54> | ***NONE**}

<dateiname 1 .. 54>
Name der Datei, die das X.509-Client-Zertifikat im PEM-Format enthält.

***NONE**
Es wird keine Datei spezifiziert.
*NONE ist Voreinstellung.

-Z DSAKeyFile

Mit der Option *-Z DSAKeyFile* wird eine Datei spezifiziert, die den privaten DSA-Server-Schlüssel im PEM-Format enthält.

Wenn sowohl X.509-Client-Zertifikat als auch privater Server-Schlüssel innerhalb derselben Datei enthalten sind (siehe Option *-Z DSACertificateFile* auf Seite 162), braucht die Option *-Z DSAKeyFile* nicht angegeben zu werden.

Da es möglich sein soll, den TELNET-Server im unbedienten Betrieb automatisch hochzufahren, kann beim Server-Start keine Pass-Phrase für den privaten Server-Schlüssel eingegeben werden. Deshalb müssen Sie eine eventuell vorhandene Verschlüsselung des privaten Schlüssels mit Pass-Phrase entfernen. Verhindern Sie in diesem Fall unbedingt, dass unbefugte Personen auf diesen Schlüssel zugreifen können.

-Z DSAKeyFile
={<dateiname 1 .. 54> | ***NONE**}

<dateiname 1 .. 54>
Name der Datei, die den privaten Client-Schlüssel enthält.

***NONE**
Es wird keine eigene Datei für den DSA-Server-Schlüssel verwendet.
*NONE ist Voreinstellung

-Z CACertificateFile

Mit der Option *-Z CACertificateFile* wird eine Datei spezifiziert, die die für die Authentifizierung des TELNET-Servers erforderlichen CA-Zertifikate im PEM-Format enthält. Die einzelnen PEM-Zertifikate sind sequenziell in der Datei angeordnet.

Zum Hinzufügen oder Löschen von Zertifikaten können Sie die Datei mit einem beliebigen Text-Editor bearbeiten. Die einzelnen Zertifikate sind wie folgt in der Datei notiert:

```
-----BEGIN CERTIFICATE-----
< CA-Zertifikat in Base64-Codierung >
-----END CERTIFICATE-----
```

Text außerhalb dieser Sequenzen wird vom TELNET-Client ignoriert und kann deshalb zum Kennzeichnen der Zertifikate verwendet werden, die wegen der Base64-Codierung in nicht lesbarer Form vorliegen.

-Z CACertificateFile
={<dateiname 1 .. 54> | ***NONE**}

<dateiname 1 .. 54>
: Name der Datei, die die für die Authentifizierung des TELNET-Servers erforderlichen Zertifikate im PEM-Format enthält.

***NONE**
: Es wird keine Datei mit CA-Zertifikaten angegeben.
*NONE ist Voreinstellung.

-Z CARevocationFile

Mit der Option *-Z CARevocationFile* wird eine Datei spezifiziert, die die CRLs (Certificate Revocation List) der Zertifizierungsinstanzen enthält. (Zertifikate, die von einer Zertifizierungsinstanz herausgegeben wurden, können durch Veröffentlichung einer so genannten Certificate Revocation List (CRL) für ungültig erklärt werden.)

-Z CARevocationFile
={<dateiname 1 .. 54> | ***NONE**}

<dateiname 1 .. 54>
Name der Datei, die die CRLs der Zertifizierungsinstanzen enthält.

***NONE**
Es wird keine Datei mit CRLs angegeben.
*NONE ist Voreinstellung.

-Z CipherSuite

Mit der Option *-Z CipherSuite* wird eine Verschlüsselungsverfahren-Vorzugsliste spezifiziert. Falls diese Option nicht angegeben wird, wird eine voreingestellte Vorzugsliste verwendet.

-Z CipherSuite
=<Spezifikation>

<Spezifikation>
Spezifikation einer Verschlüsselungsverfahren-Vorzugsliste. Näheres siehe Kapitel „Spezifikation einer Vorzugsliste für Verschlüsselungsverfahren“ auf Seite 383.
ALL: !EXP: !ADH:!RC4 ist Voreinstellung.

-Z RandFile

Mit der Option *-Z RandFile* wird eine Datei spezifiziert, aus der beim Server-Start Daten für die Initialisierung des Pseudo-Zufallszahlengenerators (PRNG) gelesen werden. Beim Beenden des Servers werden entsprechende Daten des PRNG in diese Datei geschrieben, um sie beim nächsten Server-Start zu verwenden.

Werden mehrere TELNET-Server parallel betrieben, so muss für jeden Server jeweils eine eigene Datei definiert werden.

ACHTUNG!

Diese Datei darf für Unbefugte nicht zugreifbar sein.

-Z RandFile
=<dateiname 1 .. 54>

<dateiname 1 .. 54>
Name der Datei, die Daten für die Initialisierung des PRNG enthält.
Voreinstellung: SYSDAT.TCP-IP-AP.*nnn*.TELNETD.RAND

-Z CertificateChainFile

Mit der Option *-Z CertificateChainFile* wird eine Datei spezifiziert, in der alle Zertifikate abgelegt werden können, die für die Verifikation des Server-Zertifikats benötigt werden. Das erste Zertifikat in dieser Datei ist das Server-Zertifikat. Die restlichen Zertifikate müssen eine lückenlose Kette bilden, ausgehend vom Zertifikat der CA, die das Server-Zertifikat ausgestellt hat, bis hin zum Root-Zertifikat einer CA, das vom FTP-Client direkt verifiziert werden kann. Die Zertifikate der Kette müssen so sortiert sein, dass das Root-Zertifikat an letzter Stelle steht.

Die spezifizierte Datei wird nur benötigt, wenn das Server-Zertifikat von einer CA ausgestellt ist, die den TELNET-Clients nicht bekannt ist und somit ohne Zusendung der Zertifikats-Kette von den TELNET-Clients nicht verifiziert werden kann. Dieser Mechanismus setzt voraus, dass nicht gleichzeitig RSA- und DSA-Zertifikate für den Server genutzt werden, da die Datei für beide Varianten verwendet wird.

-Z CertificateChainFile
={<dateiname 1 .. 54> | ***NONE**}

<dateiname 1 .. 54>
Name der Datei, in der alle Zertifikate abgelegt sind, die für die Verifikation des Server-Zertifikats benötigt werden.

***NONE**
Es wird keine Datei spezifiziert.
*NONE ist Voreinstellung.

-Z Protocol

OpenSSL unterstützt das SSL-Protokoll der Version 3 sowie das TLS-Protokoll in den Versionen 1, 1.1 und 1.2. Mit der Option *-Z Protocol* können einige dieser Protokolle selektiv aktiviert werden.

-Z Protocol
=[**+** | **-**] {**SSLv3** | **TLSv1** | **TLSv1**.1 | **TLSv1**.2 | **All** } ...

+
Das nachfolgend spezifizierte Protokoll ist zugelassen.

-
Das nachfolgend spezifizierte Protokoll ist nicht zugelassen.

SSLv3
SSL-Protokoll der Version 3

Das SSL-Protokoll in der Version 3 weist einige sicherheitstechnische Mängel auf und sollte nach Möglichkeit nicht verwendet werden.

TLSv1
TLS-Protokoll der Version 1

TLSv1.1
TLS-Protokoll der Version 1.1

TLSv1.2
TLS-Protokoll der Version 1.2

ALL
Alle Protokolle sollen aktiviert werden.

All -SSLv3 ist Voreinstellung.

Beispiel

Die Angaben `-Z Protocol=TLSv1 TLSv1.1 TLSv1.2` und `-Z Protocol=All -SSLv3` haben dieselbe Wirkung, solange keine Unterstützung für die zukünftige TLS-Protokollversion 1.3 zum TELNET hinzugefügt wird.

-Z AcceptableClientCAFile

Bei aktivierter Client-Authentifizierung teilt der Server beim TLS-Verbindungsaufbau dem Client die Namen derjenigen CAs mit, die er als Unterzeichner von Client-Zertifikaten akzeptiert. Diese CA-Namen werden den Zertifikaten entnommen, die in der durch die Option-*Z AcceptableClientCAFile* spezifizierten Datei stehen. Die einzelnen Zertifikate im PEM-Format stehen dabei der Reihe nach in dieser Datei.

Zum Hinzufügen oder Löschen von Zertifikaten können Sie die Datei mit einem beliebigen Text-Editor bearbeiten. Die einzelnen Zertifikate sind wie folgt in der Datei notiert:

```
-----BEGIN CERTIFICATE-----
< CA-Zertifikat in Base64-Codierung >
-----END CERTIFICATE-----
```

Text außerhalb dieser Sequenzen wird vom TELNET-Server ignoriert und kann deshalb zum Kennzeichnen der Zertifikate verwendet werden, die wegen der ASN.1/Base64-Codierung in nicht lesbarer Form vorliegen.

-Z AcceptableClientCAFile
={<dateiname 1 .. 54> | ***NONE**}

<dateiname 1 .. 54>
Name der Datei.

***NONE**
Es wird keine Datei spezifiziert.
*NONE ist Voreinstellung.

-Z VerifyDepth

Mit der Option *-Z VerifyDepth* wird die so genannte Verifizierungstiefe festgelegt, d.h. die Anzahl der maximal zulässigen Zertifikate zwischen dem TELNET-Client-Zertifikat und dem Zertifikat, das dem TELNET-Server bekannt ist.

Im Einzelnen ist zu beachten:

- Wird für die maximale Tiefe der Wert 1 spezifiziert (Default), dann muss das Server-Zertifikat direkt von einer dem TELNET-Server bekannten CA (Certificate Authority) signiert worden sein, damit es akzeptiert wird.
- Wird die maximale Tiefe überschritten, dann wird die Verbindung abgebrochen, sofern nicht aufgrund von `-Z VerifyClient=NONE` (siehe Seite 172) oder `-Z VerifyClient=OPTIONAL` die Verifizierung des TELNET-Server-Zertifikats ausgeschaltet ist.
- Die Spezifikation der Tiefe 0 ist nicht sinnvoll. In diesem Fall wären nur selbstsignierte Zertifikate zulässig.

-Z VerifyDepth
=<integer 0..32767>

<integer 0..32767>
: Anzahl der maximal zulässigen Zertifikate zwischen dem TELNET-Client-Zertifikat und dem Zertifikat, das dem TELNET-Server bekannt ist.
Voreinstellung: 1

-Z VerifyClient

Mit der Option *-Z VerifyClient* wird festgelegt, ob ein TELNET-Client ein Zertifikat für den Server-Zugang vorweisen muss.

-Z VerifyClient
={**NONE** | **OPTIONAL** | **REQUIRE**}

NONE
Der TELNET-Server fordert kein Zertifikat vom TELNET-Client an.
NONE ist Voreinstellung.

OPTIONAL
Der TELNET-Server fordert den TELNET-Client auf, sein Zertifikat zu senden. Wenn der Client dies aber verweigert oder ein ungültiges Zertifkat liefert, wird ihm dennoch der Zugang gewährt.

REQUIRE
Der TELNET-Client muss ein gültiges Zertifikat übermitteln, da ihm andernfalls der Zugang verwehrt wird.

-Z OpenSSLlibName

Mit der Option *-Z OpenSSLlibName* wird festgelegt, aus welcher LMS-Datei die OpenSSL-Bibliothek nachgeladen werden soll. Die OpenSSL-Bibliothek wird nur nachgeladen, falls mindestens eine der Options `-Z tls-required`, `-B on` oder `-H on` spezifiziert wurde.

Eine vom Standardnamen abweichende Angabe kann z.B. erforderlich sein, wenn die OpenSSL-Bibliothek auch von anderen Produkten verwendet wird.

Das Nachladen der OpenSSL-Bibliothek lässt sich nämlich durch Cache-Speichern mithilfe von DAB beschleunigen. Bei Verwendung einer gemeinsamen OpenSSL-Bibliothek durch mehrere Produkte wird die Größe des verwendeten DAB-Puffers verringert.

--Z OpenSSLlibName
=<openssl-libname>

<openssl-libname>
: Name der LMS-Datei, aus der die OpenSSL-Bibliothek nachgeladen werden soll.
Voreinstellung: LMS-Datei, auf die die IMON Logical-ID SYSLNK verweist.

5.3.4 Option -B - AUTHENTICATION-Option aktivieren / deaktivieren

Mit der Option *-B* aktivieren bzw. deaktivieren Sie die Unterstützung der AUTHENTICATION-Option, mit der ein Authentifizierungsverfahren ausgehandelt werden kann. Im BS2000 ist die AUTHENTICATION-Option derzeit nur für TLS/SSL realisiert.

Die für den SSL-Betrieb erforderlichen Einstellungen im TELNET-Server können Sie mithilfe der bei der START-TLS-Option beschriebenen *-Z*-Options vornehmen (siehe Abschnitt „Option -Z - Unterstützung der START-TLS-Option“ auf Seite 158).

Die Options *-Z tls required* (START-TLS-Option, siehe Seite 159) und *-B* (AUTHENTICATION-Option) dürfen Sie nicht gleichzeitig angeben. Andernfalls wird folgende Fehlermeldung ausgegeben:

```
Both START-TLS and AUTHENTICATION-Option not allowed
```

-B
{**on** | **off** | **debug**}

on
Die AUTHENTICATION-Option wird unterstützt.

off
Die AUTHENTICATION-Option wird nicht unterstützt.

debug
Der Authentication-Trace wird eingeschaltet.

5.3.5 Option -H - ENCRYPTION-Option aktivieren / deaktivieren

Mit der Option *-H* aktivieren bzw. deaktivieren Sie die ENCRYPTION-Option, mit der das Verschlüsselungsverfahren sowie der verwendete Schlüssel ausgehandelt werden kann. Derzeit wird in TELNET nur DES64 in den Varianten DES_CFB64 und DES_OFB64 unterstützt. Die Option *-H* darf nicht gleichzeitig mit den Options `-Z tls-required` (siehe Seite 159) oder `-B on` (siehe Seite 174) angegeben werden. Andernfalls wird folgende Fehlermeldung ausgegeben:

```
error: SSL and encryption opton
```

Es werden ausschließlich Encryption-Routinen aus der OpenSSL-Bibliothek verwendet. Wenn eine OpenSSL-Bibliothek mit einem anderen Namen als dem Standard-Dateinamen (SYSLNK.TCP-IP-AP.*nnn*) verwendet werden soll, können Sie dies mithilfe der Option *-Z OpenSSLlibName* (siehe Seite 173) festlegen.

-H
{**on** | **off** | **debug** | **key=**{<c-string 1..8> | <x-string 1..16>}

on
Die ENCRYPTION-Option wird unterstützt.

off
Die ENCRYPTION-Option wird nicht unterstützt.

debug
Der Encryption-Trace wird eingeschaltet.

key={<c-string 1..8> | <x-string 1..16>}
Encryption-Key für DES

- Beachten Sie, dass nicht zwischen dem Schlüssel für die Verschlüsselung und dem Schlüssel für die Entschlüsselung unterschieden wird. TELNET-Client und TELNET-Server verwenden denselben Schlüssel. Im Falle des TELNET-Servers bedeutet dies, dass dieser Schlüssel für alle TELNET-Clients gilt.
- Die Angabe `-H on` benötigt auch immer die Angabe `-H key=...` . Andernfalls wird folgende Fehlermeldung ausgegeben:

  ```
  Error: Encryption on and no Encryption Key!
  ```

5.4 TELNET-Server starten und beenden

Mit den nachfolgend beschriebenen Kommandos können Sie den TELNET-Server starten und beenden.

Diese Kommandos können auch via Operator-Konsole eingegeben werden.

5.4.1 TELNET-Server starten

Die */START*-Kommandos für die Enter-Jobs lauten:

/START-TCP-IP-DEMON	Enter-Job für TCP-IP-AP
/START-TELNET-DEMON	Enter-Job für den TELNET-Server

– Die /START-Kommandos sind nur unter Kennungen erlaubt, die das Privileg NET-ADMIN besitzen.

– Wenn Sie FTP und TELNET gleichzeitig starten wollen, verwenden Sie das Kommando START-TCP-IP-DEMON.

5.4.2 TELNET-Server beenden

Die nachfolgend beschriebenen Kommandos zum Beenden des TELNET-Servers sind nur wirksam für Server ab interNet Services V3.0A.

5.4.2.1 TELNET-Server mit STOP-TELNET-DEMON beenden

Den TELNET-Server beenden Sie mit dem Kommando STOP-TELNET-DEMON.

STOP-TELNET-DEMON
PORT-NUMBER=*STD-PORT/*ANY/<integer 0..32767>

PORT-NUMBER=
Angabe der Portnummer des zu beendenden TELNET-Servers.
Voreinstellung: Es wird der TELNET-Server mit der Standardportnummer 23 beendet.

PORT-NUMBER=*STD-PORT
Bewirkt dasselbe wie keine Angabe von Parametern.

PORT-NUMBER=*ANY
Es werden alle aktiven TELNET-Server beendet.

PORT-NUMBER=<integer 0..32767>
Ein TELNET-Server der angegebenen Portnummer soll beendet werden.

5.4.2.2 TELNET-Server mit Shutdown beenden

Weiterhin ist das Beenden der Server auch durch das Kommando */INFORM-PROGRAM 'shutdown',*TSN(<tsn>)* möglich. <*tsn*> bezeichnet die TSN der jeweiligen Server-Task.

5.4.3 Hinweise und Einschränkungen zum Starten und Beenden von Servern

Beim Starten und Beenden von Servern sind folgende Punkte zu beachten:

- Das Kommando START-TELNET-DEMON ist nur wirksam, wenn die Start-Prozedur SYSENT.TCP-IP-AP.*nnn*.TELNETD existiert.

  Wenn das Kommando an der Konsole eingegeben wird, muss es zusätzlich shareable sein. Dies hat keine negativen Folgen für die Sicherheit, da ab TCP-IP-AP V5.0 alle Server-Options in einer eigenen Option-Datei hinterlegt werden können, die nicht shareable sein muss (siehe Abschnitt „Konfiguration von TELNET via Option-Datei“ auf Seite 150).

- Mit dem Parameter VERSION für die START-Kommandos lassen sich auch die Server mit TCP-IP-AP-Versionen < 5.0 starten. Da sich aber die Server erst ab V5.0 bei jedem Start beim Subsystem TCPIPAP anmelden, können nur solche Server wieder durch STOP-Kommandos beendet werden.

- Es dürfen sich maximal 20 Teilnehmer an das Subsystem TCPIPAP anbinden. Mehr Teilnehmer sind aufgrund der Größe interner Tabellen nicht zulässig. Der Maximalwert von 20 Teilnehmern wird jedoch für die Praxis ausreichen. Bei Überschreitung der Maximalzahl beendet sich der Server beim Start mit folgender Meldung:

  „`error: too many connections to Subsystem TCPIPAP`“

- Wenn der Server nicht unter TSOS gestartet wurde, beendet er sich mit folgender Meldung:

  „`error: no privilege to connect to Subsystem TCPIPAP`“

  Dies kann nur beim Versuch vorkommen, den Server via explizitem Aufruf der Start-Prozedur anstatt mithilfe des START-...-DEMON-Kommandos zu starten, denn dies würde unter einer Kennung ungleich TSOS abgewiesen.

5.4.4 Meldungen und Returncodes

Meldungen

```
TCP2000   (&00)-KOMMANDO FUER (&01)-SERVER ERFOLGREICH AUSGEFUEHRT.
          &00  =  START oder STOP
          &01  =  FTP oder TELNET oder TCP-IP
```

Bedeutung
Das START/STOP-Kommando fuer FTP/TELNET-Server war erfolgreich.

Maßnahme
<keine>

```
TCP2001   STOP-KOMMANDO FUER (&00)-SERVER HAT KEINE WIRKUNG.
          &00  =  FTP oder TELNET
```

Bedeutung
Keine Server vorhanden.

Maßnahme
<keine>

```
TCP2003   GEWUENSCHTE PORTNUMMER FUER (&00)-SERVER EXISTIERT NICHT.
          &00  =  FTP oder TELNET
```

Bedeutung
Angegebener Server nicht vorhanden.

Maßnahme
<keine>

```
TCP2004    FEHLER BEIM STARTEN DER PROZEDUR FUER (&00): (&01).
           &00  =  FTP oder TELNET oder TCP-IP
           &01  =  <Startprozedur>
```

Bedeutung
(&00)-Server konnte mit Prozedur (&01) nicht gestartet werden.

Maßnahme
<keine>

Kommando-Returncodes

(SC2)	SC1	Maincode	Bedeutung
	0	CMD0001	siehe Meldung TCP2000
	0	CMD0001	siehe Meldung TCP2001
	1	TCP2003	siehe Meldung TCP2003
	32	TCP2004	siehe Meldung TCP2004
	32	CMD0220	beim /CANCEL-JOB-Kommando passierte ein Fehler

5.5 Protokolldatei von TELNET-Servern

TELNET-Server protokollieren ihre Ausgaben in einer Protokolldatei mit dem Standard-Dateinamen SYSOUT.TCP-IP-AP.*nnn*.TELNETD. Die Protokolldatei enthält immer die Differenzeinträge zur aktuellen Sicherung mit dem */INFORM-PROGRAM*-Kommando rdProt (siehe Abschnitt „rdProt- Protokolldatei von TELNET-Servern sichern“ auf Seite 186).

5.6 Anzeige der aktuellen Einstellungen von TELNET-Servern

Mithilfe des BS2000-Kommandos SHOW-FTP-TELNET-STATUS können Sie sich über die aktuellen Einstellungen von BS2000-TELNET-Servern informieren.

Ausgegeben werden die folgenden Informationen:

- Einstellungen, die bei der Generierung der Server vorgenommen wurden
- aktuelle Informationen über die TSN der Servertask und Anzahl aktiver Verbindungen

Die Server hinterlegen die Daten in Hilfsdateien mit folgenden Namen:

- SYSDAT.TCP-IP-AP.*nnn*.TELNETD.CONF.<port>

  <port> spezifiziert die Portnummer des jeweiligen Servers.

Diese Dateien werden beim Beenden des jeweiligen Servers wieder gelöscht.

SHOW-FTP-TELNET-STATUS

SERVER= *FTP(...)/ ***TELNET**(...)

***FTP**(...)
│ **PORT-NUMBER= *STD-PORT** / ***ANY** / <integer 0..32767>

***TELNET**(...)
│ **PORT-NUMBER=*STD-PORT** / ***ANY** / <integer 0..32767>

, INFORMATION= *STD /*ALL

, OUTPUT=*SYSOUT/*SYSLST

SERVER=
Name des Servers, dessen Daten ausgegeben werden sollen (FTP oder TELNET).

SERVER=*TELNET(...)
Ausgabe der Konfigurationsdaten eines TELNET-Servers.

PORT-NUMBER=
Portnummer des TELNET-Servers, dessen Konfigurationsdaten ausgegeben werden sollen.

PORT-NUMBER=*STD-PORT
Portnummer 23. Dies ist die Voreinstellung.

PORT-NUMBER=*ANY
Es werden Informationen über alle zurzeit aktiven TELNET-Server ausgegeben.

PORT-NUMBER=<integer 0..32767>
Portnummer des TELNET-Servers, dessen Konfigurationsdaten ausgegeben werden sollen.

INFORMATION=
Art und Umfang der ausgegebenen Informationen.

INFORMATION=*STD
Ausgabe einer Liste der durch PORT-NUMBER spezifizierten Server. Dies ist die Voreinstellung.

INFORMATION=*ALL
Ausgabe aller Informationen aller durch PORT-NUMBER spezifizierten Server.

OUTPUT=
Ausgabemedium, in das die Informationen geschrieben werden sollen.

OUTPUT=*SYSOUT
Ausgabe erfolgt nach SYSOUT. Dies ist die Voreinstellung.

OUTPUT=*SYSLST
Ausgabe erfolgt nach SYSLST.

Meldungen

TCP9240 KOMMANDO SHOW-FTP-TELNET-STATUS ERFOLGREICH BEENDET.

Bedeutung
SHOW-FTP-TELNET-STATUS erfolgreich beendet.

Maßnahme
<keine>

TCP9241 FSTAT-FEHLER DMS(&00).

Bedeutung
Fehler bei FSTAT auf Konfigurationsdateien.

Maßnahme
Nachprüfen ob überhaupt irgendein Server aktiv ist.

TCP9242 KONFIGURATIONSDATEI (&00) KONNTE NICHT GEOEFFNET WERDEN.

Bedeutung
Konfigurationsdatei (&00) konnte nicht geöffnet werden.

Maßnahme
Nachprüfen, ob der gewünschte Server aktiv ist.

TCP9243 KONFIGURATIONSDATEI (&00) KONNTE NICHT GELESEN WERDEN.

Bedeutung
Konfigurationsdatei (&00) konnte nicht gelesen werden.

Maßnahme
Datei überprüfen.

Kommando-Returncodes

(SC2)	SC1	Maincode	Bedeutung
	0	TCP9240	Kommando erfolgreich beendet
	64	TCP9241	siehe Meldung TCP9241
	64	TCP9242	siehe Meldung TCP9242
	64	TCP9243	siehe Meldung TCP9243

5.7 Konsolschnittstelle

Einige Kommandos können vom Systembediener auch über die Konsolschnittstelle, eingeleitet mit dem Kommando */INFORM-PROGRAM*, angegeben werden. Die mit */INFORM-PROGRAM* abgesetzten Kommandos dienen zum

– Steuern der Server-Traces,
– Beenden der verschiedenen Server-Tasks,
– Sichern der Protokolldateien.

Folgende Server-Kommandos sind über die Konsolschnittstelle möglich:

Operation	**Kurzbeschreibung**
debug	Trace zur Benutzerebene ein/ausschalten
trace	Trace zur TCP/IP-Schnittstelle ein/ausschalten
shutdown	Service beenden
rdProt	Protokolldatei des TELNET-Servers sichern

Die Kommandos für Inbetriebnahme und Außerbetriebnahme der TELNET-Server (siehe Seite 176) können auch an der Konsole eingegeben werden.

debug - Trace zur Benutzerebene ein-/ausschalten

/INFORM-PROGRAM
'debug <debug-wert>**'**,***TSN**(<tsn>)

<tsn>
TSN der Server-Task, für den der Trace zur Benutzerebene eingeschaltet werden soll.

debug <debug-wert>
Zulässig sind Werte von 0 bis 9. Je größer der Wert, desto mehr Informationen werden ausgegeben. Wert 0 bedeutet, dass der Trace ausgeschaltet ist. Dieses Kommando dient dem Systemkundendienst zur Fehlerdiagnose. Ein Debug-Wert > 2 ist nicht sinnvoll.

trace - Trace zur TCP/IP-Schnittstelle ein-/ausschalten

/INFORM-PROGRAM
'trace <trace-wert>**'**,***TSN**(<tsn>)

<tsn>
TSN der Server-Task, für den der Trace zur TCP/IP- Schnittstelle eingeschaltet werden soll.

trace <trace-wert>
Zulässig sind Werte von 0 bis 10. Je größer der Wert, desto mehr Informationen werden ausgegeben. Wert 0 bedeutet, dass der Trace ausgeschaltet ist. Dieses Kommando dient dem Systemkundendienst zur Fehlerdiagnose.

shutdown - Service beenden

/INFORM-PROGRAM
'shutdown',***TSN**(<tsn>)

<tsn>
TSN der zu beendenden Server-Task.

rdProt- Protokolldatei von TELNET-Servern sichern

Mit dem Kommando rdProt wird die Protokolldatei eines TELNET-Servers abgespeichert unter dem Namen der ursprünglichen Protokolldatei (Standarddateiname: SYSOUT.TCP-IP-AP.*nnn*.TELNETD), erweitert um einen Suffix, der Datum und Uhrzeit (UTC) in der Form <MMDD><HHMMSS> spezifiziert. Diese Datei enthält immer die Differenzeinträge zur vorausgegangenen Sicherung. Beachten Sie, dass Sie keinen zu lange Namen für die Protokolldatei wählen: Das rdProt schlägt fehl, wenn der Name nach dem Anhängen des Suffix die zulässige Länge überschreitet.

/INFORM-PROGRAM
'rdProt ',*TSN(<tsn>**)**

<tsn>
TSN der Server-Task.

5.8 IPv6-Adressen in TELNET

Beim Aufbau der Kontrollverbindung mit dem Client-Kommando *open* kann als Adresse auch eine IPv6-Adresse verwendet werden, die in sedezimaler Darstellung mit Doppelpunkt (:) anzugeben ist (siehe Handbuch „interNet Services Benutzerhandbuch“).

5.9 TELNET-Exits

Für den TELNET-Client und den TELNET-Server gibt es folgende Exits:

- Exit vor dem Start der Dialog-Anwendung (Open-Exit)
- Exit vor dem Beenden der Dialog-Anwendung (Close-Exit)
- Exit vor dem Senden von Daten
- Exit nach dem Empfangen von Daten

Die Exits für das Starten und Beenden der Dialog-Anwendung können nur im TELNET-Server eingestellt werden.

5.9.1 DUMMY-Modul

TELNET-Exits werden in dem nachgeladenen Modul EXITTEL.C behandelt. EXITTEL.C wird als Gerüst ausgeliefert und hat als einzigen Entry den Einsprungspunkt *YAPTEXIT*. Einzige Aktion von EXITTEL.C ist der Rücksprung mit Return-Wert '0xff'. Dies zeigt an, dass noch keine benutzerdefinierten Exit-Routinen definiert sind.

Um eigene Exits zu definieren, erstellen Sie einen Modul, der den Einsprungspunkt YAPTEXIT enthält, und ersetzen in der Bibliothek SYSLNK.TCP-IP-AP.*nnn* (SRMLNK.TCP-IP-AP.*nnn*) den Modul EXITTEL durch diesen von Ihnen erstellten Modul.

5.9.2 Exit-Routinen

Für die Behandlung der verschiedenen Exits übergeben die Aufrufer der Exit-Routine (TELNET-Client oder TELNET-Server) an den Einsprungspunkt YAPTEXIT die Adresse einer Parameterliste. Die Struktur *yaptx* dieser Parameterleiste wird unter dem Namen *yaptx.h* in SYSLIB.TCP-IP-AP.*nnn* ausgeliefert.

Struktur yaptx

Die Struktur *yaptx* ist wie folgt definiert:

```
struct yaptx {
        int     caller;         /* Aufrufer: S=Server, C=Client          */
#define client  0x01            /* X'01' Client                         */
#define server  0x02            /* X'02' Server                         */
        int     action          /* main action code                     */
#define telrecv 0x01            /* action = receive                     */
#define telsend 0x02            /* action = send                        */
#define telopen 0x03            /* action = open connection             */
#define telclos 0x04            /* action = close connection            */
        char   *selector;       /* Selector                             */
        int     portno;         /* Port-Nummer (Server-Port)            */
        char    hname[128+1];   /* Hostname von Server / Client          */
        char    reserved[3];    /* Reserved                             */
        int     connid;         /* identifies uniquely client-server    */
                                /* connection. Only for Server          */
        char   *inbuf;          /* Address of input buffer              */
        int     inbuflen;       /* Length of input buffer               */
        char   *outbuf;         /* Address of output buffer             */
        int     outbuflen;      /* Length of output buffer              */
        int     outDatalen;     /* Length of output data                */
```

Beschreibung der Parameter

Folgende Parameter werden übergeben:

- Aufrufer der Exit-Routine (*caller*)
- Typ des Entries (*action*)
- abdruckbare Zeichenkette zur Identifizierung der Exit-Routine (*selector*)
- Connection Identifier (*connid*)
- Rechnername (*hname*)
  - des adressierten TELNET-Servers (bei TELNET-Clients)
  - des aufrufenden TELNET-Servers (bei TELNET-Servern)

- Portnummer (*portno*)
  - des adressierten TELNET-Servers (bei TELNET-Clients)
  - des adressierten TELNET-Clients (bei TELNET-Servern)
- bei Send-/Receive-Exits: *inbuf*, *inbuflen*, *outbuf*, *outbufLen*, *outDataLen*
  outDataLen muss vom Exit selbst versorgt werden.

caller
spezifiziert, ob die Exit-Routine vom TELNET-Client oder vom TELNET-Server aufgerufen wurde.

action
spezifiziert den Typ des Entries (*receive*, *send*, *open connection*, *close connection*)

selector
Abdruckbare Zeichenkette (String) zur Auswahl der gewünschten Exit-Routine. Die Zeichenkette wird durch '\0' abgeschlossen.

portno
Port-Nummer von Server bzw. Client:

- Bei TELNET-Clients spezifiziert *portno* die Port-Nummer des adressierten TELNET-Servers.
- Bei TELNET-Servern spezifiziert *portno die Port*-Nummer des adressierten TELNET-Clients.

hname[128+1]
Hostname von Server bzw. Client:

- Bei TELNET-Clients spezifiziert *hname* den Rechnernamen des adressierten TELNET-Servers.
- Bei TELNET-Servern spezifiziert *hname* den Rechnernamen des adressierten TELNET-Clients.

inBuf
enthält die Adresse des Puffers, in dem die umzuwandelnden Daten stehen (Eingabepuffer). Nur bei Send-/Receive-Exits von Bedeutung.

inBufLen
spezifiziert die Länge (Anzahl der gültigen Bytes) des Eingabepuffers. Nur bei Send-/Receive-Exits von Bedeutung.

outBuf
enthält die Adresse des Ausgabepuffers.Nur bei Send-/Receive-Exits von Bedeutung.

outBuflen
spezifiziert die Länge des Ausgabepuffers.Nur bei Send-/Receive-Exits von Bedeutung.

outDataLen

Vor dem Rücksprung zum Aufrufer muss die Routine in *outDataLen* hinterlegen, wieviele Bytes im Ausgabepuffer gültig sind und somit übertragen werden müssen. Nur bei Send-/Receive-Exits von Bedeutung.

connid

Connection-Identifier. Der Connection Identifier identifiziert die Client-Server-Verbindung bei festem TELNET-Server eindeutig. Wenn mehrere Server aktiv sind, identifiziert das Paar (*portno*, *connid*) die Verbindung zwischen Client und Server und somit den TELNET-Client eindeutig (siehe auch Parameter *connid*). Von Bedeutung ist dies z.B. bei der Code-Umsetzung, wenn zwei Bytes auf ein Byte abgebildet werden. In diesem Fall muss die Exit-Routine für die Umsetzung das erste Byte zwischenspeichern, um bei Eintreffen des zweiten Bytes die Umsetzung durchzuführen. Dabei gewährleistet *connid* die eindeutige Zuordnung des Zwischenspeichers zur jeweiligen Verbindung.

Ergebnisse und Return-Werte der Exit-Routinen

Exit-Routinen müssen in jedem Fall einen Return-Wert liefern. Jeder Exit, für den keine anwender-definierte Exit-Routine existiert, muss den Wert '0xff' als Return-Wert liefern.

Ergebnisse und Return-Werte bei send und receive

Nach ordnungsgemäßer Ausführung enthält *outbuf* den umgesetzten Code und *outDataLen* die Länge des umgesetzten Codes. Return-Wert: 0.

Wenn ein Exit feststellt, dass zuwenig Speicher für eine Code-Umsetzung vorhanden ist, muss der Return-Wert -2 zurückgeliefert werden.

Bei *inbuf* = 0 wird lediglich abgefragt, ob ein entsprechender Exit definiert wurde oder nicht:

- Falls ein entsprechender Exit definiert ist, muss der Return-Wert gleich 0 sein.
- Falls kein entsprechender Exit definiert ist, muss der Return-Wert gleich '0xff' sein.

Ergebnisse und Return-Werte bei open und close

open

Erlaubt der Exit den Zugang zum Server, so ist der Return-Wert gleich 0, andernfalls muss er gleich -1 sein.

close

close liefert stets den Return-Wert 0.

5.9.3 Benutzerdefinierte Exits

Für die Exit-Behandlung mit eigenen Prozeduren ergänzen Sie den Modul EXITTEL.C um den entsprechenden Code.

Wenn Sie einen Exit für *send* oder *receive* definieren, sind Sie auch für die Behandlung aller Sonderzeichen zuständig. Insbesondere müssen Sie dafür sorgen, dass

- ein Zeichen ’0xff’ beim Senden verdoppelt wird,
- zwei aufeinanderfolgende Zeichen ’0xff’ beim Empfangen in ein einzelnes ’0xff’ verwandelt werden.

Benutzerdefinierte Server-Exits im TELNET-Server aktivieren

Den so erstellten Code aktivieren Sie im TELNET-Server mit der Option -e:

```
-e
[open:<selector1>!][close:<selector2>!][receive:<selector3>!][send:<selector4
>]
```

Bei Angabe von * für <selector> wird grundsätzlich der Exit-Mechanismus ohne die genauer spezifizierende Angabe von <selector> gestartet.

Benutzerdefinierte Server-Exits im TELNET-Client aktivieren

Im TELNET-Client können Sie Server-Exits für *send* und *receive* mit dem Kommando *rexit* (remote exit) aktivieren. Dabei beschränkt sich die Wirkung von *rexit* jedoch auf die Verbindung dieses speziellen Clients zum Server.

Das *rexit*-Kommando hat folgende Syntax:

```
rexit [receive:<selector1>][<send:<selector2>]
```

Folgende Fälle sind zu unterscheiden:

- Server-Options sind angegeben:

  Wenn für eine Verbindung zwischen Client und Server kein *rexit*-Kommando angegeben wurde, gilt die Einstellung der Server-Option -e.

  Gibt es für eine Exit-Routine Angaben sowohl im *rexit*-Kommando als auch in der Server-Option -e, so gelten die Angaben des *rexit*-Kommandos. Eine spätere Angabe von * für <selector1> bzw. <selector2> im *rexit*-Kommando bewirkt ein Rücksetzen auf die Angabe in der Server-Option. Durch eine leere Angabe für <selector1> bzw. <selector2> wird der Exit ausgeschaltet.

- Es sind keine Server-Options angegeben:

  Die Angabe von * für <selector> im *rexit*-Kommando aktiviert die Exit-Routine. Eine genauere Unterscheidung der Behandlungsart, wie sie durch die Angabe von <selector> ermöglicht wird, ist in diesem Fall nicht vorgesehen. Durch eine leere Angabe für <selector1> bzw. <selector2> wird der Exit ausgeschaltet.

Benutzerdefinierte Client-Exits im TELNET-Client aktivieren

Benutzerdefinierte Exit-Routinen für den Client stellen Sie mit dem Kommando *exit* im Client ein:

```
exit [receive:<selector1>][<send:<selector2>]
```

Bei Angabe von * für <selector1> bzw. <selector2> wird zwar der Entry YAPTEXIT angesprungen, jedoch ohne die genauer spezifzierende Angabe von *selector*. Fehlt die Angabe für <selector>, so wird keine Exit-Routine angesprungen. Durch eine leere Angabe für <selector1> bzw. <selector2> wird der Exit ausgeschaltet.

Beispiele

1. Clients vom Rechner *Rechner* sollen keinen Zugang zum TELNET-Server erhalten. Dies lässt sich mit folgendem benutzerdefinierten Modul mit Entry YAPTEXIT erreichen:

```
YAPTEXIT (struct yaptx *exparam)
{
   switch (exparam->action) {
      case telopen:
         if (strcmp(exparam->hname,"Rechner") == 0)
            return(-1);
         break;
      default;
         break;
  }
}
```

   Dieser Modul muss in der Bibliothek SYSLNK.TCP-IP-AP.*nnn* den EXITTEL-Modul ersetzen und mit Option `-e open:*` aktiviert werden. Zur Ablaufzeit wird der Externverweis YAPTEXIT aus dem benutzerdefinierten Modul befriedigt.

2. Für einen TELNET-Server sind zwei verschiedene benutzerdefinierte Open-Exits definiert:

   – Meldet sich ein Client von *Rechner1*, so soll *exit1* angesprungen werden.
   – Meldet sich ein Client von *Rechner2*, so soll *exit2* angesprungen werden.

```
YAPTEXIT (struct yaptx *exparam)
{
   if ((exparam->action) == telopen)
      if (strcmp(exparam.hname,"Rechner1")==0)
         exit1(exparam)
      else
         if ((strcmp(exparam.hname,"Rechner2")==0)
            exit2(exparam);
}
```

   Die entsprechende Option lautet: `-e open;*`

3. Es sollen zwei verschiedene Code-Umsetzungen für die Daten definiert werden, die vom Client zum Server gesendet werden. So soll z.B. x'0102' nach x'0a' bzw. x'0a0b' umgesetzt werden. Im nachfolgend dargestellten Beispiel heissen die Code-Umsetzungsroutinen *proc1* bzw. *proc2*. Die Erkennungsstrings sind "proc1" bzw. "proc2".

```
YAPTEXIT (struct yaptx *exparam)
{
   if ((exparam->caller) == client) && (exparam->action == telsend))
      if (strcmp(exparam->selector,"proc1")==0)
         proc1(exparam);
      else
         if ((strcmp(exparam->selector,"proc2")==0)
            proc2(exparam);
}
```

   Die entsprechenden Kommandos zu Einschalten dieser Exits lauten:

   `exit send:proc1` bzw. `exit send:proc2`

Benutzerdefinierte TELNET-Exits unter POSIX

Der POSIX-TELNET entsteht aus dem Zusammenbinden der LLMs TELPOSIX und EXITTEL. Somit können Sie auch unter POSIX mit den TELNET-Exits arbeiten.

Der Lieferumfang von interNet Services beinhaltet den Dummy-Modul EXITTEL, der nur einen Rücksprung ausführt.

Eigene TELNET-Exits schreiben Sie wie folgt:

- Erstellen Sie Ihre gewünschte Version des EXITTEL.
- Binden Sie diese Version mit TELPOSIX aus der SYSLNK.TCP-IP-AP.*nnn* zusammen.
- Schreiben Sie das resultierende LLM unter dem Namen TELNET in die SINLIB.TCP-IP-AP.*nnn*.
- Installieren Sie POSIX-TELNET (siehe Abschnitt „Installation und Deinstallation von FTP- und TELNET-Client in POSIX“ auf Seite 47).

6 Generierung von Zufallszahlen

Dieses Kapitel beschreibt:

- Zufallszahlen-Generierung im BS2000 mit PRNGD
- Zufallszahlen-Generierung in POSIX

6.1 Zufallszahlen-Generierung im BS2000 mit PRNGD

Beinahe alle kryptographischen Verfahren benötigen starke Zufallszahlen. Wenn nämlich ein Angreifer hinreichend einschränkend vorhersagen kann, welche Zahlen der Zufallszahlen-Generator liefert, kann er relativ einfach auf die verwendeten Schlüssel schließen.

Damit nicht jede einzelne kryptographische Anwendung Verfahren für die Gewinnung solcher Zufallszahlen implementieren muss, stellt BS2000 zentral einen Zufallszahlen-Generator zur Verfügung. Der BS2000-Zufallszahlen-Generator PRNGD (**P**seudo **R**andom **N**umber **G**enerator **D**emon) ist als Pseudozufallszahlen-Generator realisiert. Dies verhindert ein Blockieren und bietet daher keine Angriffspunkte für „Denial of Services (DoS)“-Angriffe.

Der BS2000-PRNGD ist wegen der besseren Zugriffsmöglichkeiten auf Daten des Betriebssystemkerns als TPR-Subsystem implementiert. Dies ist ein wesentlicher Vorteil gegenüber anwendungsspezifischen, nicht in TPR ablaufenden Zufallszahlen-Generatoren. Außerdem ist der PRNGD dadurch besser gegen Zugriffe durch potenzielle Angreifer geschützt. Die Benutzerschnittstelle ist über einen SVC realisiert.

Nachfolgend sind Entropie-Quelle, Konfiguration und Benutzerschnittstelle des BS2000-PRNGD beschrieben.

6.1.1 Entropie-Quellen des BS2000-PRNGD

Als Entropie-Quellen verwendet der BS2000-PRNGD u.a.:

- Zugriffszeiten auf bestimmte, häufig genutzte Dateien
- Ausgaben von Kommandos, die sich auf Daten beziehen, die sich dynamisch ändern, wie z.B. SHOW-USER-STATUS mit verschiedenen Parametern oder Ausgaben des Kommandos SHOW-DAB-CACHING, falls auf dem System DAB im Automatic-Betrieb ausgeführt wird

Die zu verwendenden Dateien und Kommandos können Sie in einer Konfigurationsdatei festgelegen. Hierfür spezifizieren Sie bei den Kommandos, welchen relativen Entropie-Gehalt die jeweilige Ausgabe hat, um z.B. Kommandos mit wenig erläuterndem (d.h. unveränderlichem) Text und stark veränderlichen Ausgaben entsprechend stärker berücksichtigen zu können. Dadurch sind auch Anpassungen an die jeweiligen örtlichen Gegebenheiten möglich. Demgegenüber gehen Zugriffszeiten der Dateien nicht in die Entropie-Buchhaltung ein.

Ferner können Sie angeben, in welchen Zeitabständen die Zeitstempel der Dateien abgefragt und die Kommandos ausgeführt werden sollen. Von der Initialisierungsphase abgesehen, wird dabei zyklisch jeweils nur eine der Dateien abgefragt und eines der Kommandos ausgeführt.

Eine weitere wichtige Entropie-Quelle ist der Netzverkehr. Hierzu greift der BS2000-PRNGD auf die von BCAM gesammelten Daten des Netzverkehrs zu (Anzahl der auf einer Verbindung gesendeten und empfangenen Bytes und Pakete etc.). Eine Konfiguration ist hierfür aber weder notwendig noch möglich.

6.1.2 Konfiguration des BS2000-PRNGD

Den BS2000-PRNGD konfigurieren Sie mithilfe von Options in einer Konfigurationsdatei (Standard-Name ist SYSSSI.PRNGD.*nnn*, dieser ist änderbar mit der IMON Logical-Id SYSSSI), die beim Start des Subsystems ausgewertet wird. Die einzelnen Options müssen gemäß den folgenden Regeln in die Option-Datei eingetragen sein:

- Jede Option muss in einer eigenen Zeile stehen.
- Erstrecken sich die Argumente einer Option über mehrere Zeilen, dann muss jede fortzusetzende Zeile mit dem Fortsetzungszeichen „\“ abgeschlossen werden.
- Eine Zeile, die mit dem Zeichen „#“ in Spalte 1 beginnt, wird beim Einlesen ignoriert.
- Bei den Option-Namen wird Klein-/Groß-Schreibung nicht unterschieden.

Nachfolgend sind die einzelnen Options beschrieben.

poolSize

Mit der Option *poolSize* wird die Größe des zu verwendenden Entropie-Pools (in Byte) spezifiziert.

poolSize
<Größe>

<Größe>
Größe des zu verwendenden Entropie-Pools (in Byte).
Voreinstellung: 4096

In der Regel ist der Default-Wert ausreichend. Lediglich bei (temporär) hohem Bedarf an Zufallszahlen kann es aus Sicherheitsgründen sinnvoll sein, größere Werte zu verwenden. Wenn kleinere Werte als 1024 spezifiziert werden, wird 1024 verwendet.

minimalEntropy

Mit der Option *minimalEntropy* wird spezifiziert, wie hoch (in Byte) der Entropie-Gehalt des Entropie-Pools sein muss, bevor der Zugriff auf den Zufallszahlen-Generator erlaubt wird.

minimalEntropy
<Wert>

<Wert>
Betrag des Entropie-Gehalts des Entropie-Pools (in Byte), ab dem der Zugriff auf den Zufallszahlen-Generator erlaubt wird.
Voreinstellung: 256

Wenn dieser Wert einmal überschritten ist, werden immer Zufallszahlen geliefert, auch wenn dieser Minimalwert wieder unterschritten wird. In der Regel ist der Default-Wert ausreichend. Wenn kleinere Werte als 256 spezifiziert werden, wird 256 verwendet.

entropyThreshold

Mit der Option *entropyThreshold* wird ein Schwellenwert (in Byte) für das Auffüllen des Entropie-Pools spezifiziert: Wenn der Entropie-Gehalt des Pools den Schwellenwert unterschreitet, wird in kurzen Zeitintervallen solange Entropie durch Erfassen von Kommandoausgaben und der BCAM-internen Daten gesammelt, bis der Schwellenwert wieder überschritten ist. Während dieser Zeit werden die Options *cmdInterval* und *bcamInterval* ignoriert.

entropyThreshold
<Wert>

<Wert>
Schwellenwert für das Auffüllen des Entropie-Pools (in Byte).
Voreinstellung: 1024

seedFile

Mit der Option *seedFile* wird spezifiziert, aus welcher Datei beim Subsystem-Start die Initialisierungswerte für den Entropie-Pool des PRNGD gelesen werden.

Nach dem erfolgreichen Einlesen wird der Entropie-Pool durchmischt. Aus dem Pool entnommene Zufallszahlen werden wieder zurückgeschrieben. Damit ist gewährleistet, dass beim nächsten Start nicht mit genau den gleichen Anfangswerten gestartet wird, falls das Subsystem nicht ordnungsgemäß beendet werden konnte. Wird das Subsystem ordnungsgemäß beendet, dann werden ebenfalls vorher Daten in die Datei zurückgeschrieben.

In allen Fällen wird hierbei nicht der Entropie-Pool direkt in die Datei geschrieben. Vielmehr werden dem PRNGD so viele Zufallsbytes entnommen und in die Datei geschrieben, wie es der Größe des Entropie-Pools entspricht. Damit wird der Schaden begrenzt, falls Unbefugte auf diese Datei zugreifen.

seedFile
<Dateiname>

<Dateiname>
Name der Datei, aus der die Initialisierungswerte gelesen werden.
Voreinstellung: SYSDAT.PRNGD.*nnn*.SEED

file

Mit der Option *file* werden Dateien spezifiziert, deren Zugriffszeiten PRNGD als Entropie-Quelle verwendet. Diese Option können Sie beliebig oft angeben. Die dabei spezifizierten Dateien werden in eine Liste eingetragen, die zyklisch im Zeitintervall abgearbeitet wird, das durch die Option *fileInterval* vorgegeben ist. Sie können dieselbe Datei auch mehrfach angeben. Dies kann z.B. sinnvoll sein bei Dateien, auf die wesentlich häufiger zugegriffen wird, als auf die anderen spezifizierten Dateien.

Die durch diesen Mechanismus gesammelte Entropie wird nicht in der Entropie-Buchhaltung berücksichtigt.

file
<Dateiname>

<Dateiname>
Name der Datei, deren Zugriffszeiten als Entropie-Quelle verwendet werden.

fileInterval

Mit der Option *fileInterval* wird spezifiziert, in welchen (minimalen) Zeitintervallen eine Datei aus der mit der Option *file* definierten Liste entnommen und ihre letzte Zugriffszeit zum Entropie-Pool hinzugefügt wird.

fileInterval
<Zeitintervall>

<Zeitintervall>
Zeitintervall in Sekunden.

cmd

Mit der Option *cmd* wird ein SDF-Kommando spezifiziert, dessen SYSOUT-Ausgaben als Entropie-Quelle verwendet werden sollen. Diese Option können Sie beliebig oft angeben. Die dabei spezifizierten Kommandos werden in eine Liste eingetragen, die im durch die Option *cmdInterval* spezifizierten Zeitabstand zyklisch abgearbeitet wird.

Sie können dasselbe Kommando auch mehrfach angeben. Dies kann z.B. sinnvoll sein bei Kommandos, deren SYSOUT-Ausgabe sich wesentlich häufiger bzw. stärker ändert als bei den anderen spezifizierten Kommandos.

cmd
<SDF-Kommando-Name> <Entropie-Rate>

<SDF-Kommando-Name>
: Name des SDF-Kommandos, dessen SYSOUT-Ausgaben als Entropie-Quelle verwendet werden sollen.

<Entropie-Rate>
: geschätzter relativer Entropie-Gehalt der SYSOUT-Ausgabe des unter <SDF-Kommando-Name> spezifizierten Kommandos.

Beispiel

In diesem Beispiel wird angenommen, dass eine Zeile einer SYSOUT-Ausgabe des SDF-Kommandos SHOW-USER-STATUS INFORMATION=*PROGRAM 40 Bytes lang ist und dass es von jeder dieser Ausgabezeilen 16 verschiedene, gleichwahrscheinliche Varianten gibt. Letzteres bedeutet, dass eine Task mit gleicher Wahrscheinlichkeit eines von 16 gegebenen Programmen ausführt.

In diesem Fall enthält jede dieser Zeilen ein halbes Byte Entropie und die Entropie-Rate ist entsprechend 0,5/40 = 0,0125. In der Praxis ist es wesentlich schwieriger zu bestimmen, wieviel verschiedene Ausgaben auftreten können. Darüber hinaus sind diese Ausgaben selten gleich wahrscheinlich. Dennoch kann man versuchen, mit gewissen plausiblen Annahmen hinsichtlich der Anzahl und Wahrscheinlichkeit verschiedener Varianten einer Ausgabezeile (siehe oben) eine Abschätzung für die Entropie-Rate zu erstellen und diese dann evtl. um einen Sicherheitsfaktor zu reduzieren.

cmdInterval

Mit der Option *cmdInterval* wird spezifiziert, in welchen (minimalen) Zeitintervallen ein Kommando aus der mit der Option *cmd* definierten Liste entnommen und seine SYSOUT-Ausgabe zum Entropie-Pool hinzugefügt wird.

cmdInterval
<Zeitintervall>

<Zeitintervall>
Zeitintervall in Sekunden.
Voreinstellung: 49

bcamInterval

Mit der Option *bcamInterval* wird spezifiziert, in welchen (minimalen) Zeitintervallen die BCAM-internen Daten zum Entropie-Pool hinzugefügt werden.

bcamInterval
<Zeitintervall>

<Zeitintervall>
Zeitintervall in Sekunden.
Voreinstellung: 49

6.1.3 Programmschnittstelle GPRBYTE des BS2000-PRNGD

Die Programmschnittstelle GPRBYTE des BS2000-PRNGD steht für die Sprachen C/C++ und ASSEMBLER zur Verfügung.

GPRBYTE ist die Schnittstelle der Routine NLKRES96 im Modul GPRBYTE des DSSM-Subsystems PRNGD. Die Routine NLKRES96 liefert dem Aufrufer Pseudo-Zufallszahlen.

Kompatibilität

Die Programmschnittstelle PRNGD ist source- und objekt-kompatibel ab PRNGD Version 1.0.

Entry-Name(n) und SVC-Nummer(n)

SVC 16 (dezimal)

Makro-Typ

Die folgenden MF-Werte für die Makrogenerierung werden unterstützt (siehe Handbuch „Makroaufrufe an den Ablaufteil“):

ASSEMBLER MF = { C | D | E | L | M }

Der Assembler-Makro und die C/C++-Include-Datei finden sich in der LMS-Bibliothek SYSLIB.PRNGD.*nnn*.

Makro-Syntax

	Operation	**Operanden**
<Marke>	GPRBYTE	DATAADR = <datenpufferadresse> ,NUM_BYT = <integer 1..255> / <anzahlbytes> [,MODE = *NON_BLOCKING]

Die Operanden MF und PARAM werden gemäß Konvention unterstützt.

Beschreibung der Operanden

DATAADR = <datenpufferadresse>
Zeiger (char*) auf den Speicherbereich, in den die Zufallszahlen geschrieben werden sollen.

NUM_BYT = { <integer 1..255> | <anzahlbytes> }
Anzahl der Zufalls-Bytes, die in den Speicherbereich geschrieben werden sollen.
Die Anzahl der Zufalls-Bytes kann wie folgt spezifiziert werden:

<integer 1..255>
Ganzzahl zwischen 1 und 255

<anzahlbytes>
Variable vom Datentyp Integer

MODE = *NON_BLOCKING
Betriebsmodus des Zufallszahlen-Generators.
Derzeit wird nur der nicht-blockierende Modus unterstützt, d.h. die Zufallszahlen sollen von einem Generator geliefert werden, der nicht wegen Entropie-Mangels blockiert.

Sprachbesonderheiten

Sprache	**sprachspezifischer Operand**
ASSEMBLER	[PREFIX = { G | <name> }] [,MACID = { PRB | <name>}] [,EQUATES = { YES | NO }]
C	SVC-#: 16, UNIT = 430, FUNCTION = 1, VERSION = 1

Return-Codes

Returncode			Identifier		Bedeutung
SC2	SC1	Maincode			
0	00	0000	successfull,	ASS: GPRBSUCC	kein Fehler festgestellt
0	20	0001	int_error,	ASS: GPRBINTE	interner Fehler
0	01	0002	parameter_error,	ASS: GPRBPARE	Parameterfehler
0	40	0003	buffer_invalid,	ASS: GPRBBUFE	Puffer zu klein oder nicht allokiert
0	40	0004	too_many_bytes,	ASS: GPRBTOOM	mehr als 255 Bytes angefordert
0	80	0005	prngd_not_ready,	ASS: GPRBNRDY	Zufallszahlen-Generator hat nicht genügend Entropie
0	80	0006	timeout,	ASS: GPRBTOUT	Zufallszahlen-Generator zeitweilig nicht aufrufbar

C-Beispielprogramm

```
#include <stdio.h>
#include "FHDR.H"
#include "GPRBYTE.H"

main(int argc, char *argv[])
{
  char randomBytes[128];
  struct GPRBYTE_pl_mdl param;
  enum {UNIT = 430, FUNCTION = 1, VERSION = 1, dataLen = 32};

  FHDR_SET_RC_NIL(param.hdr);
  FHDR_MOD_IFID(param.hdr, UNIT, FUNCTION, VERSION);
  param.in_data.mode = GPRBYTEnon_blocking;
  param.in_data.buffer = &randomBytes;
  param.in_data.num_bytes = dataLen;
  GPRBYTEC(param);
  if (param.hdr.FHDR_RC_MAINCODE == GPRBYTEsuccessful) {
    int i;
    printf("GPRBYTEC called successfully\nData: ");
    for (i = 0; i < dataLen; i++)
      printf("%02X", randomBytes[i]);
    printf("\n");
  }
  else
    printf("Error in call of GPRBYTEC: %08X\n", param.hdr.FHDR_RC_NBR);
}
```

6.1.4 Meldungen

Die Meldungen von PRNGD haben den Meldungsschlüssel `GPRnnnn`.

Ausgabe von Meldungen mit /HELP-MSG-INFORMATION

Mit dem BS2000-Kommando `/HELP-MSG-INFORMATION MSG-ID=GPRnnnn` können Sie die Bedeutungs- und Maßnahmetexte zu einer Meldung im laufenden Betrieb ausgeben.

Ausgabe von Meldungen im Internet

Die Meldungen finden Sie über eine HTML-Anwendung auf dem Manual-Server (*http://manuals.ts.fujitsu.com)* und auf der DVD „BS2000 SoftBooks“.

6.2 Zufallszahlen-Generierung in POSIX

Wie angekündigt wird der POSIX-*prngd*-Dämon nicht mehr ausgeliefert. POSIX-Programme können den BS2000-PRNGD entweder direkt über die GPRBYTE-Schnittstelle ansprechen oder aber die Geräte-Datei */dev/urandom* nutzen, die die Zufallszahlen ebenfalls vom BS2000-PRNGD bezieht.

/dev/urandom bietet sich insbesondere für Skripte an, die darauf z.B. mit dem *dd*-Kommando zugreifen können.

7 DNS

Das folgende Kapitel basiert auf dem „BIND9 Administrator Reference Manual“ des Internet Software Consortium. Das Copyright für das Administratorhandbuch hält das Internet Software Consortium. Die hier vorliegende Beschreibung ist auf die BS2000-relevanten Teile gekürzt. An entsprechenden Stellen des Handbuchs, wie z.B. Syntaxbeschreibungen, wird auf das „BIND9 Administrator Reference Manual“ des Internet Software Consortium verwiesen, da nur dort die aktuellsten Versionen beschrieben sind. Sie finden das BIND9 Administrator Reference Manual des Internet Software Consortium auf Ihrem Server im Verzeichnis */opt/TCP-IP-SV/dns-named/readme* oder unter *http://www.isc.org/files/arm97.pdf* im Internet.

DNS (**D**omain **N**ame **S**ervice) ist ein TCP/IP-Protokoll der Anwendungsebene, das es TCP/IP-Anwenderprogrammen ermöglicht, die dort üblicherweise verwendeten symbolischen Rechnernamen in die zugehörigen IP-Adressen umzuwandeln. Die netzweite Zuordnung von Rechnernamen zu IP-Adressen realisiert der DNS mithilfe einer verteilten Datenbank, deren Informationen allen Interessenten im Netz zur Verfügung stehen. TCP/IP-Anwenderprogramme nutzen die DNS-Funktionalität über Socket-Funktionen wie z.B. *gethostbyname()* und *gethostbyaddr()* (siehe Handbücher „SOCKETS(BS2000)“ und „SOCKETS/XTI für POSIX“).

Die derzeit gültige Definition des DNS basiert auf den RFCs (Request for Comments). Diese Standards werden durch die Internet Engineering Task Force (IETF) und die Internet Engineering Steering Group (IESG) definiert. Umfassende Informationen zu den RFCs sind auf der Homepage der IETF: *http://www.ietf.org/rfc/*

Bei Drucklegung des Handbuchs waren folgende RFCs zugrunde gelegt:

- Standards:
  RFC974, RFC1034, RFC1035
- vorgeschlagene Standards:
  RFC2181, RFC2308, RFC1995, RFC1996, RFC2136, RFC2845, RFC2671, RFC2672, RFC2930, RFC2931, RFC3007, RFC3645
- vorgeschlagene Standards für DNS-Sicherheit:
  RFC3225, RFC3833, RFC4033, RFC4034, RFC4035
- vorgeschlagene Standards, die noch in Entwicklung sind:
  RFC1886, RFC2065, RFC2137
- weitere wichtige RFCs für die DNS-Implementierung:
  RFC1535, RFC1536, RFC1982, RFC4074
- Resource Record Typen:
  RFC1183, RFC1706, RFC2168, RFC1876, RFC2052, RFC2163, RFC2230, RFC2536, RFC2537, RFC2538, RFC2539, RFC2540, RFC2782, RFC2915, RFC3110, RFC3123, RFC3596, RFC3597
- DNS und das Internet:
  RFC1101, RFC1123, RFC1591, RFC2317, RFC2826, RFC2929
- DNS-Operationen:
  RFC1033, RFC1537, RFC1912, RFC2010, RFC2219
- weitere DNS-bezogene RFCs:
  RFC1464, RFC1713, RFC1794, RFC2240, RFC2345, RFC2352, RFC3071, RFC3258, RFC3901
- Obsolete und nicht implementierte Experimental RRs:
  RFC1712, RFC2673, RFC2874

7.1 Konzept des DNS

Der Domain Name Service ist eine verteilte, replizierte Datenbank mit Servern (DNS-Server) und Clients (Resolver). Dabei werden die Daten von verschiedenen DNS-Servern verwaltet. Die Resolver hingegen haben keine lokale Datenbasis und wenden sich bei jeder DNS-Anfrage an einen oder mehrere DNS-Server, um die benötigten Informationen zu erhalten.

7.1.1 Entwicklung des DNS

Anwendungen nutzen IP-Adressen für den Verbindungsaufbau (TCP) und den Datagrammverkehr (UDP) zum Partnerrechner. IP-Adressen sind jedoch nicht besonders anwenderfreundlich. Deshalb wurde bereits in der Anfangszeit des Internet ein Namenssystem entwickelt, mit dessen Hilfe wichtige Rechner anhand ihres Namens identifiziert werden können. Jedem Rechner im TCP/IP-Netz können ein oder mehrere frei wählbare Namen zugeordnet werden. Namen sind unabhängig von der IP-Adresse bzw. den IP-Adressen des Rechners, können aber durch Funktionen des Application Programming Interface (API) auf die IP-Adresse abgebildet werden.

Die Zuordnung zwischen Rechnernamen und IP-Adressen der Rechner, mit denen eine Kommunikation gewünscht wird, erfolgt über eine Host-Datei:

- auf Unix-Systemen: */etc/hosts*
- auf BS2000-Systemen: BCAM-Host-Datei

In der Host-Datei steht in jeder Zeile ein Rechnername mit der zugehörigen IP-Adresse.

In der Anfangszeit des Internet wurde vom Network Information Center (NIC) eine zentrale Host-Datei manuell gepflegt und in regelmäßigen Abständen per FTP an alle Rechner im Internet kopiert. Neu hinzukommende Rechner wurden vom Netzadministrator des NIC in die zentrale Host-Datei eingetragen und waren erst nach einer erneuten Verteilung dieser Datei den anderen Rechnern bekannt.

Bedingt durch das schnelle Anwachsen des Internet, wurde das geschilderte Verfahren bald unpraktikabel, da die Aktualisierung und somit Übertragung der ständig größer werdenden Host-Dateien immer häufiger notwendig wurde. Als Problemlösung bot sich die Nutzung der Datenbank-Technologie an.

7.1.2 DNS-Namensraum

Der DNS-Namensraum ist baumartig organisiert und in verschiedene Domänenebenen gegliedert. Es gibt eine Wurzel, die Root-Domäne, die der Anker für alle Suchvorgänge innerhalb des DNS-Namensraums ist. Teilbäume des DNS-Namensraums können als sogenannte Zonen eigenständige Verwaltungseinheiten bilden.

Aufbau des DNS-Namensraums

Bild 1 veranschaulicht die Domänenstruktur des DNS-Namensraums.

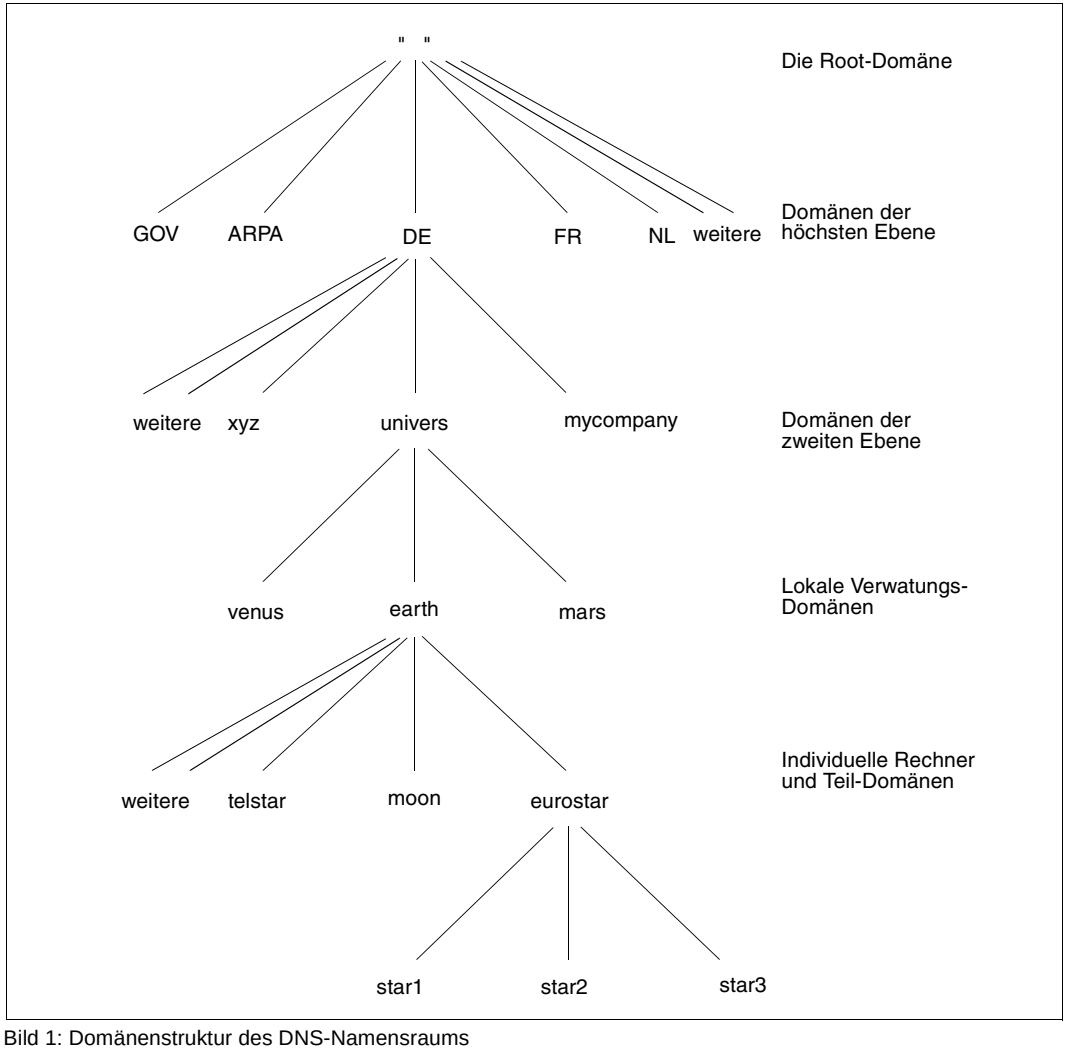


Bild 1: Domänenstruktur des DNS-Namensraums

Auf jeder Ebene des DNS-Namensraums gibt es DNS-Server. Ein DNS-Server ist ein Rechner mit folgenden Aufgaben:

- Verwaltung der Informationen über Server der jeweils untergeordneten Namensebene
- Abbildung von symbolischen Namen auf Adressen für diejenigen Namen, für die kein untergeordneter DNS-Server vorhanden ist

Die Domänen des DNS-Namensraums haben folgende Eigenschaften:

- Root-Domäne

  Die Root-Domäne steht in der DNS-Hierarchie an oberster Stelle und wird von ICANN verwaltet. Innerhalb der Root-Domäne unterhält ICANN DNS-Server der Root-Domäne, die Informationen über die DNS-Server der darunterliegenden Ebene verwalten.

- Domänen der höchsten Ebene (Top Level Domains)

  Unterhalb der Root-Domäne befinden sich die Domänen der höchsten Ebene.

  Innerhalb der USA existieren die folgenden Top Level Domains:

aero	luftfahrttechnische Einrichtungen
biz	geschäftliche Organisationen (Business)
com	kommerzielle Organisationen
coop	Kooperativen
edu	schulische Einrichtungen
gov	Einrichtungen der amerikanischen Regierung
info	freier Gebrauch
int	internationale Organisationen
mil	Einrichtungen des amerikanischen Militärs
museum	Museumseinrichtungen
name	individuelle Personen
net	Netzwerkorganisationen
org	nicht-kommerzielle Organisationen
pro	Rechtsanwälte, Ärzte und andere Berufsgruppen

  Außerhalb der USA gibt es länderspezifische Top Level Domains. Als Namen werden die ISO-Ländercodes der betreffenden Länder verwendet, z.B. DE für Deutschland, FR für Frankreich usw. Das NIC ordnet das Netz bei der Anmeldung der passenden Domäne zu.

- Domänen der zweiten Ebene

  Jede Domäne der höchsten Ebene verzweigt in mehrere Domänen der zweiten Ebene. Die auf dieser Ebene angesiedelten Organisationen ernennen Domänenverwalter, die für die Name Server ihrer Netze verantwortlich sind. Für die domänenübergreifende Verwaltungskoordination ernennt das NIC außerdem eine technische Anlaufstelle.

- Lokale Verwaltungsdomänen

  Die lokalen Verwaltungsdomänen liegen in der DNS-Hierarchie unterhalb der Domänen der zweiten Ebene. Diese Domänen werden von den Netzbetreibern eigenverantwortlich verwaltet. Hinsichtlich der Größe gibt es erhebliche Unterschiede. So gibt es lokale Verwaltungsdomänen, die aus nur einem Rechner bestehen, und solche, die aus vielen Rechnern und zusätzlichen DNS-Servern bestehen. Einer lokalen Domäne können auch weitere Verwaltungsdomänen, sogenannte Teildomänen, untergeordnet sein.

Eine spezielle Domäne, die Domäne *in-addr.arpa*, wird benötigt für die Umsetzung von IP-Adressen in DNS-Namen. IP-Adressen werden, in „decimal dotted“-Schreibweise invertiert, in die Domäne *in-addr.arpa* eingetragen.

Das Konzept des DNS macht keine Einschränkungen hinsichtlich der Umsetzung von DNS-Namen auf IP-Adressen und umgekehrt. Deshalb können einer IP-Adresse mehrere DNS-Namen zugeordnet werden. Ebenso lassen sich einem DNS-Namen mehrere IP-Adressen zuordnen.

Zonen

Eine Zone definiert einen Teil eines DNS-Namensraums, der von einem Masterserver (primärer Name Server) verwaltet wird. Eine Zone ist nicht auf eine Domäne beschränkt, sondern kann auch einige oder alle darunter liegenden Domänen umfassen.

Zonendatendateien sind Dateien, aus denen der Name Server die Zonendaten lädt.

7.1.3 Informationsablage im DNS

Alle Informationen des DNS sind nur innerhalb der DNS-Server gespeichert. Dort ist die Information in Resource Records (RR) abgelegt. Resource Records sind in ASCII codiert und enthalten folgende Informationen:

– Inhaber der Information
– RR-Typ
– Klasse (z.B. IN für Internet)
– Gültigkeitsdauer der Daten
– Daten

Das Format eines Resource Record ist auf Seite 217 näher beschrieben.

Zu den wichtigsten RR-Typen gehören:

SOA (Start of Authority)

Der SOA-RR spezifiziert den Anfang einer Zone, die von dem DNS Name Server betreut wird, auf dem der SOA-RR gespeichert ist. Eine Systemdatei darf nur einen SOA-RR pro Zone enthalten. Die Zone endet mit Beginn der nächsten Zone, d.h. wenn ein neuer SOA-Resource Record angegeben ist.

NS (Name Server)

Der NS-RR legt den Namen des Name Servers fest, der für eine bestimmte DNS-Domäne verantwortlich ist.

A (Address)

Der Adressen-RR definiert die IP-Adresse, die einem DNS-Namen zugeordnet ist. Für jede IP-Adresse eines Rechners sollte ein eigener Adressen-RR vorhanden sein.

AAAA (quad A)

Der AAAA-RR definiert die IPv6-Adresse, die einem DNS-Namen zugeordnet ist. Für jede IPv6-Adresse eines Rechners sollte ein eigener AAAA-RR vorhanden sein.

PTR (Domain Name Pointer)

Der PTR-RR definiert spezielle Namen als Zeiger auf andere Namen in der Domäne. PTR-RRs werden hauptsächlich in *in-addr.arpa*-Datensätzen zur Abbildung von Adressen (den speziellen Namen) auf Rechnernamen verwendet. PTR-Namen sollten innerhalb einer Zone eindeutig sein.

MX (Mail Exchanger)

Der MX-RR definiert die IP-Adresse, die einem DNS-Namen zugeordnet ist.

CNAME (Canonical Name)

Mit dem CNAME-RR kann einem Standard-Hostnamen ein Alternativname zugeordnet werden. Der Alternativname darf nicht im Namensfeld anderer Resource Records angegeben sein. Für Anwenderprogramme, die den Alternativnamen verwenden, ist eine Änderung des Standard-Hostnamens transparent, d.h. die Anwenderprogramme müssen bei Änderung des Standard-Hostnamens nicht angepasst werden.

Informationen über weitere Resource Record-Typen finden Sie z.B. im RFC1035. Umfassende Informationen zu den RFCs sind auf der Homepage der Internet Engineering Task Force (IETF) zu finden: *http://www.ietf.org*

7.1.4 Format einer DNS-Nachricht

Für Anfragen und Antworten wird im DNS dasselbe Format verwendet (siehe Bild 2).

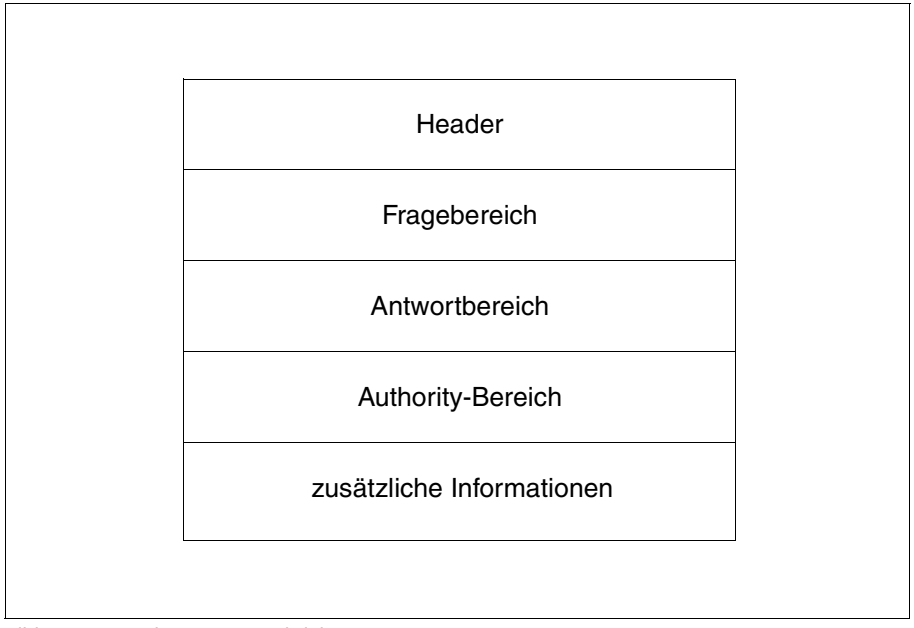


Bild 2: Format einer DNS Nachricht

Die einzelnen Bereiche einer DNS-Nachricht haben folgende Bedeutung:

- Der Header hat eine feste Länge und enthält Meta-Informationen zur DNS-Nachricht, u.A. Identifikation, Art der Nachricht (Frage oder Antwort) und Länge der nachfolgenden variablen Bereiche.
- Im Fragebereich wird die gesuchte Information spezifiziert.
- Der Antwortbereich enthält die gesuchte Information in Form einer variablen Anzahl von Resource Records.
- Der Authority-Bereich enthält in Form von RRs die Namen weiterer Name Server für den Fall, dass der zuvor kontaktierte Name Server keine Anwort liefern konnte.
- Der unterste Bereich enthält ggf. weitere Informationen in Form von RRs.

7.1.5 DNS Resolver (Überblick)

Der DNS Resolver erledigt die Anfragen zur Auflösung von DNS Domain-Namen in IP-Adressen, die Anwenderprogramme an den DNS Name Server richten.

Zugang zum DNS Resolver

Zugang zum Resolver erhalten die Anwenderprogramme über die zur Anwendung hinzugebundenen Socket-Funktionen, wie die für IPv4 verwendeten Funktionen *gethostbyname()* und *gethostbyaddr()* bzw. die für IPv4 und IPv6 verwendbaren Funktionen *getaddrinfo()*, *getnameinfo()*, *getipnodebyaddr()* und *getipnodebyname()*:

gethostbyname()	liefert zu einem Rechnernamen die zugehörige IPv4-Adresse.
gethostbyaddr()	liefert zu einer IPv4-Adresse den zugehörigen Rechnernamen.
getaddrinfo()	liefert protokollunabhängig Informationen über Rechnernamen, Rechneradressen und Services.
getnameinfo()	liefert protokollunabhängig den Namen des Kommunikationspartners.
getipnodebyaddr()	liefert protokollunabhängig Informationen über Rechnernamen.
getipnodebyname()	liefert protokollunabhängig Informationen über Rechneradressen.

Im Normalfall werden die Resolver-Funktionen in einer Bibliothek bereitgestellt, die mit den Produkten „SOCKETS(BS2000)“ bzw. „SOCKETS/XTI für POSIX“ ausgeliefert wird. Die dort verwendeten Resolver-Funktionen sind in den Handbüchern „SOCKETS(BS2000)“ bzw. „SOCKETS/XTI für POSIX“ beschrieben.

In POSIX ist es alternativ möglich, die Resolver-Funktionalität über die Bibliothek komplett in die Anwendung einzubinden. In diesem Fall sind die Resolver-Funktionen in der Online-Dokumentation zu DNS beschrieben. Zum Zugriff auf die Online-Dokumentation sind die DNS-Entwicklungsteile zu installieren (siehe Seite 227).

Auflösung der an den DNS Resolver gerichteten Anfragen

Die Auflösung der an den DNS Resolver gerichteten Anfragen kann auf verschiedene Arten erfolgen:

- Über den mit SOCKETS(BS2000) bereitgestellten Resolver unter Nutzung der Konfigurationsdatei im BS2000-Dateisystem. Diese Konfigurationsdatei hat den Namen $TSOS.SYSDAT.SOCKETS.*nnn*.SOC6.RESOLV (bis openNet Server V3.0) bzw. SYSDAT.LWRESD.*nnn*.RESOLV.CONF. *nnn* spezifiziert die Version.

  Voraussetzung für die Nutzung der DNS Resolver-Funktionalität via SOCKETS(BS2000) sind Installation und Start des Subsystems. Weitere Informationen hierzu finden Sie im Handbuch „SOCKETS(BS2000)“.

- Über den via interNet Services DNS bereitgestellten Resolver-Dämon unter Nutzung der Konfigurationsdatei */etc/resolv.conf* im POSIX-Dateisystem.

  Voraussetzung für die Nutzung der DNS Resolver-Funktionalität über interNet Services DNS sind Installation und Start des DNS Resolver-Dämons. Weitere Informationen hierzu finden Sie im Abschnitt „DNS Resolver installieren und deinstallieren“ auf Seite 225.

- Durch Einbinden der Resolver-Bibliothek unter Nutzung der Konfigurationsdatei */etc/resolv.conf* im POSIX-Dateisystem (nur in POSIX möglich).

  Hierfür müssen Sie weder das Subsystem von SOCKETS(BS2000) noch den DNS Resolver-Dämon starten. Die Konfigurationsdatei */etc/resolv.conf* im POSIX-Dateisystem muss jedoch korrekt eingerichtet sein.

- Durch Abfrage der BCAM-Tabellen.

Reihenfolge der Abfragen bei der Auflösung der Resolver-Anfragen

Wie bzw. in welcher Reihenfolge die Abfragen erfolgen, wird durch die Ablaufplattform (BS2000 oder POSIX) sowie durch das Binden der Anwendung festgelegt:

- Sockets-Anwendung im BS2000:

  Die Resolver-Funktionen verwenden zunächst den Sockets-internen Resolver bzw. ab Sockets 2.2 den im BS2000 nativ ablaufenden LWRESD. Nur wenn diese kein Ergebnis liefern, wird eine Namens- bzw. Adressumsetzung mit den Einträgen aus den BCAM-Tabellen versucht. Der DNS-Resolver-Dämon von interNet Services wird in keinem Fall angesprochen.

- Sockets-Anwendung in POSIX (Standardfall):
  - Bei Nutzung der reinen IPv4-Funktionen *gethostbyname()* und *gethostbyaddr()* in einer Sockets-Anwendung in POSIX wird zuerst eine Namens- bzw. Adressumsetzung mit den Einträgen aus den BCAM-Tabellen versucht.

    Wenn ein Name bzw. eine Adresse nicht durch eine BCAM-Anfrage ermittelt werden kann, wird der DNS Resolver-Dämon von interNet Services DNS aufgerufen.

    Wenn der Dämon kein Ergebnis liefert, dann wird die Resolver-Funktionalität der BS2000-Sockets aufgerufen, d.h. ab Sockets 2.2 wird LWRESD aufgerufen.

    Erst wenn auch dieser Umsetzungsversuch scheitert, liefern die Funktionen *gethostbyname()* bzw. *gethostbyaddr()* einen Fehler zurück.

  - Bei Nutzung der DNS Resolver-Funktionen *getaddrinfo()*, *getnameinfo()*, *getipnodebyaddr()*, *getipnodebyname()* wird zuerst die Resolverfunktionalität der BS2000-Sockets verwendet.

Wenn ein Name bzw. eine Adresse hierdurch nicht ermittelt werden kann, wird eine Namens- bzw. Adressumsetzung mit den Einträgen aus den BCAM-Tabellen versucht.

Erst wenn auch dieser Umsetzungsversuch scheitert, liefern die Funktionen *getaddrinfo()*, *getnameinfo()*, *getipnodebyaddr()*, *getipnodebyname()* einen Fehler zurück.

- Sockets-Anwendung in POSIX mit hinzugebundener Resolver-Bibliothek von interNet Services DNS:

  Durch das Einbinden der Resolver-Bibliothek von interNet Services DNS wird beim Ablauf der Anwendung für alle Aufrufe (IPv4 und IPv6) ausschließlich auf die Datei */etc/resolv.conf* im POSIX-Dateisystem zugegriffen.

  Voraussetzung für die Produktion der Anwendung ist die Installation der DNS-Entwicklungsteile (siehe Seite 227).

  Beachten Sie beim Binden der Anwendung die folgende Binde-Reihenfolge für die Bibliotheken:

  1. Resolver-Bibliothek von interNet Services DNS: */usr/lib/libbind.a*
  2. SOCKETS/XTI-Bibliothek: */usr/lib/libsocket.a*

7.1.6 DNS Name Server NAMED (Überblick)

NAMED ist der DNS Name Server im BS2000. Er ermöglicht rekursive und iterative Queries sowie Caching und kann wahlweise konfiguriert werden als

– Masterserver,
– Slaveserver,
– Caching-only Server,
– weiterleitender Server.

Rekursive und iterative Queries

Eine Anfrage (Query) eines anderen Name Servers oder des Resolvers versucht NAMED zunächst aufgrund der Informationen seiner eigenen Datenbasis zu beantworten.

Falls dies nicht gelingt, verfährt NAMED je nach Konfiguration unterschiedlich:

- **rekursive** Queries (Standardfall)

  Bei einer rekursiven Query übernimmt der Name Server alle zur Beantwortung dieser Query erforderlichen Aktivitäten. Rekursiv bedeutet hier, dass der Name Server den gleichen grundlegenden Vorgang (Queries an einen entfernten Name Server senden und Verweisen folgen) so lange wiederholt, bis er die gesuchte Antwort erhält.

  Der Resolver sendet eine rekursive Query an einen Name Server, um Informationen über einen bestimmten Domain-Namen zu ermitteln. Der Name Server sollte dann die angeforderten Daten liefern oder eine Fehlermeldung zurückliefern, die besagt, dass

  – die Daten des gewünschten Typs nicht vorhanden sind oder
  – der angegebene Domain-Name nicht existiert.

  Bei einer rekursiven Query kann der Name Server den Resolver nicht einfach an einen anderen Name Server verweisen, sondern muss selbst den nächsten ihm bekannten Name Server kontaktieren.

- **iterative** Queries

  Der Name Server weist eine Query zurück, wenn sie nicht lokal, d.h. mit den Informationen seiner eigenen Datenbasis, beantwortet werden kann. Der Urheber der Query muss sich dann zur Beantwortung der Query an einen anderen Name Server wenden.

Caching

Alle während des iterativen Prozesses eingehenden Informationen speichert NAMED in einem lokalen Cache-Puffer, der die Datenbasis des NAMED erweitert und die Antwortzeit reduziert. Wenn viele Anfragen erforderlich sind, kann der Cache sehr groß werden.

Masterserver und Slaveserver

DNS Name Server verwalten Zonen, für die sie autorisiert sind. In der Regel wird eine Zone nicht auf einem einzelnen Server, sondern auf einer Gruppe von Servern implementiert. Neben dem Masterserver (primärer Server) sollte aus Gründen der Ausfallsicherheit mindestens ein weiterer Server als Slaveserver (sekundärer Server), eingerichtet sein, der eine Kopie der Masterserver-Daten verwaltet. NAMED kann sowohl als Masterserver als auch als Slaveserver konfiguriert werden.

Änderungen der Zonendaten werden stets auf dem Masterserver vorgenommen. Der Masterserver erhält die Zonendaten aus einer Datei auf seinem Host, der Zonendaten-Datei. Der Slaveserver, der seine Daten ausschließlich vom Masterserver erhält, fragt den Masterserver in regemäßigen Intervallen ab, ob seine eigene Kopie der Masterserver-Daten aktualisiert werden muss. Die Übernahme der Masterserver-Daten durch den Slaveserver wird als Zonentransfer bezeichnet.

Wahlweise kann der Masterserver auch so konfiguriert werden, dass er bei Änderung der Zonendaten aktiv alle Slaveserver informiert. Diese können daraufhin den Zonentransfer veranlassen. Ein Slaveserver, der nur NS-Resource Records vom Masterserver übernimmt, wird als Stubserver bezeichnet.

Beim Zonentransfer können die Slaveserver die übernommenen Daten in Backup-Dateien sichern. Liegen die Backup-Daten beim Hochfahren eines Slaveservers nicht vor, dann fordert der Slaveserver die aktuellen Daten vom Masterserver an.

Zonendaten sollten regelmäßig transferiert werden, auch wenn sie nicht geändert wurden. Somit kann auf sie auch zugegriffen werden, wenn der Masterserver nicht verfügbar ist.

Ein NAMED-Server kann in verschiedenen Zonen als Master- und/oder Slaveserver eingesetzt werden.

Weiterleitender Server und Forwarder

Wenn NAMED als weiterleitender Server konfiguriert ist, leitet er Anfragen, die er nicht mit den Informationen seiner eigenen Datenbasis beantworten kann, zur rekursiven Bearbeitung an spezielle Name Server, sogenannte Forwarder, weiter. Diese Forwarder versuchen dann in einem iterativen Prozess die gewünschten Antworten zu erhalten. Wenn die Forwarder keine endgültigen Informationen liefern können, versucht der weiterleitende Server je nach Konfiguration die Bearbeitung der Anfrage noch einmal selbst oder bricht die Bearbeitung ab.

Forwarding-only Betriebsart

Bei dieser Betriebsart fragt ein Name Server, der Forwarder benutzt, nicht bei weiteren Name Servern nach, wenn der Forwarder kein Ergebnis liefert.

Caching-only Server

NAMED kann auch als Caching-only Server konfiguriert werden. Ein Caching-only Server verfügt über keine verbindliche Datenbasis. Informationen fordert der Caching-only-Server von anderen, autorisierten Name Servern an. Diese Informationen werden im Cache-Puffer des Caching-only Servers gespeichert.

Views

Mit der *view*-Anweisung kann ein NAMED-Server so konfiguriert werden, dass er Anfragen, abhängig von der Absenderadresse, unterschiedlich behandelt.

7.1.7 DNS Sicherheitskonzepte

TSIG (Transaction SIGnatures) ist ein schlüsselbasierter Sicherheitsmechanismus. Er eignet sich zur Sicherung der Kommunikation zwischen zwei Servern. Als zusätzliche Sicherheitsmaßnahme verwendet TSIG gemeinsame Geheimnisse (shared secret). TSIG ist z.B. auch für den dynamischen Update nützlich.

Die DNSSEC (DNS SECurity)-Erweiterungen sind ebenfalls schlüsselbasiert. Sie verwenden die Verschlüsselung mit öffentlichem Schlüssel.

7.1.8 Zusammenspiel der Sicherheitsmechanismen von BCAM mit DNS

Bei Konflikten zwischen den etablierten Sicherheitsmechanismen und den durch DNS sich neu ergebenden Möglichkeiten der Namens- bzw. Adressumsetzung haben grundsätzlich die systemeigenen Sicherheitsmechanismen Vorrang.

BCAM bietet zwei Möglichkeiten, Kommunikationsbeziehungen zu Partnern zuzulassen:

- Kommunikationsbeziehungen sind zu beliebigen Partnern möglich, auch wenn diese dem Transportsystem BCAM noch nicht bekannt sind.

  In diesem Fall kann es bei der Verwendung der von DNS ermittelten Adressen zu keinerlei Konflikten mit den Sicherheitsmechanismen des Transportsystems BCAM kommen, da diese explizit ausgeschaltet sind.

- Kommunikationsbeziehungen sind nur zu Partnern möglich, die dem Transportsystem BCAM bereits bekannt sind.

  Hier kann folgende Situation eintreten:

  Eine Anwendung erhält von DNS zwar die Adresse eines Partnersystems, kann zu diesem Partnersystem aber keine Verbindung aufbauen, da das Partnersystem dem Transportsystem BCAM nicht bekannt ist. Eine Kommunikation ist somit aus Sicherheitsgründen ausgeschlossen.

  Abhilfe schafft in dieser Situation, falls gewünscht, die mit openNet Server V3.1 eingeführte Transportsystem-Erweiterung BCAM-DNS-ACCESS.

7.2 DNS Resolver

Dieser Abschnitt informiert über folgende Themen:

- DNS Resolver installieren und deinstallieren
- DNS Resolver konfigurieren
- Administration und Betrieb des DNS Resolvers
- Diagnose und Wartung des DNS Resolvers

7.2.1 DNS Resolver installieren und deinstallieren

Beachten Sie bitte zusätzlich zu diesem Abschnitt die mit dem Produkt interNet Services ausgelieferte Freigabemitteilung.

Die einzelnen Komponenten des Software-Pakets interNet Services werden als ein POSIX-Programmpaket per Package-Installation mit dem POSIX-Installationsprogramm installiert (siehe Handbuch „POSIX Grundlagen für Anwender und Systemverwalter“). Nähere Informationen zur Installation der Komponenten finden Sie auch im Abschnitt „Installation“ auf Seite 37.

Zur Installation und zum Betrieb der TCP-IP-SV-Komponente muss die PLAM-Bibliothek SINLIB.TCP-IP-SV.*nnn*.DNS shareable zur Verfügung stehen. Bei der Installation von DNS kann zusätzlich der Installationspfad im POSIX-Dateisystem definiert werden. Der DNS Resolver wird standardmäßig im Verzeichnis */opt/TCP-IP-SV/dns* installiert.

DNS Resolver installieren

Nach der erfolgreichen Installation der DNS-Komponenten befinden sich die relevanten Kommandos und Dateien in den Verzeichnissen */usr/bin*, */usr/sbin* und */etc* sowie im Installationsverzeichnis */opt/TCP-IP-SV/dns*. In der Tabelle Seite 225 steht <instdir> für das Installationsverzeichnis */opt/TCP-IP-SV/dns*.

Verzeichnis	Datei/Link	Beschreibung
/etc/default	TCP-IP-SV.dns	Parameterdatei für Start/Stopp-Prozedur
	TCP-IP-SV.dns.default	Default für TCP-IP-SV.dns
/etc/init.d/	TCP-IP-SV.dns	Start/Stopp-Prozedur
/etc/rc0.d/	K66TCP-IP-SV.dns	symbolischer Link auf */etc/init.d/TCP-IP-SV.dns* (zum Beenden beim POSIX-Shutdown)

[1] Nur verfügbar, wenn die DNS-Entwicklungsteile installiert sind (siehe Seite 227).

Verzeichnis	Datei/Link	Beschreibung
/etc/rc2.d/	S70TCP-IP-SV.dns	symbolischer Link auf */etc/init.d/TCP-IP-SV.dns* (zum Starten beim POSIX-Start)
/usr/bin/	dig	symbolischer Link auf *<instdir>/bin/dig*, Diagnose-Tool für DNS
	host	symbolischer Link auf *<instdir>/bin/host*, Hostnames DNS Lookup Tool
	nslookup	symbolischer Link auf *<instdir>/bin/nslookup*, Lookup Tool für DNS
/usr/lib/	libbind.a	symbolischer Link auf *<instdir>/lib/libbind.a*[1)]
/usr/sbin/	in.dnsd	symbolischer Link auf *<instdir>/sbin/dnsd*
<instdir>/bin/	dig	Diagnose-Tool für DNS
	host	Hostnames DNS Lookup Tool
	nslookup	Lookup Tool für DNS
<instdir>/etc/	install.TCP-IP-SV-DEV.*nnn*.DNS	Installationsskript für die DNS-Entwicklungsteile
	remove.TCP-IP-SV-DEV.*nnn*.DNS	Deinstallationsskript für die DNS-Entwicklungsteile
	rc.d/dnsd	Start-/Stopp-Skript für dnsd
<instdir>/lib/	libbind.a	Resolver-Bibliothek[1)]
<instdir>/readme/	*	man-pages zu den DNS-Tools sowie zur Resolver-Bibliothek[1)] im HTML- und Textformat
<instdir>/sbin/	dnsd	DNS-Resolver-Dämon

[1)] Nur verfügbar, wenn die DNS-Entwicklungsteile installiert sind (siehe Seite 227).

Nach erfolgreicher Installation werden die weiteren erforderlichen Aktivitäten unter der POSIX-Shell in einer Kennung mit POSIX-Root-Berechtigung ausgeführt. Dazu wird mit dem BS2000-Kommando START-POSIX-SHELL die POSIX-Shell gestartet.

Nach der Installation der interNet-Services müssen vor der Inbetriebnahme die für die DNS-Komponenten spezifischen Konfigurationsdateien an die individuellen Erfordernisse angepasst werden.

DNS Resolver deinstallieren

Analog zur Installation der Komponenten von interNet Services wird auch die Deinstallation mithilfe des POSIX-Installationsprogrammes unter der Kennung TSOS durchgeführt. Bei der Deinstallation wird nach dem aktiven DNS Resolver-Dämon gesucht und dieser beendet. In der Syslog-Datei */var/adm/syslog* wird die Beendigung noch aktiver Dämonen protokolliert. Anschließend werden alle Dateien, Links und Prozeduren des DNS Resolvers gelöscht.

Im Rahmen der Deinstallation wird die Konfigurationsdatei */etc/default/TCP-IP-SV.dns* im Verzeichnis */etc/tcpipsv* gesichert, sofern sie gegenüber der Defaultdatei */etc/default/TCP-IP-SV.dns.default* verändert wurde. Existiert schon eine gleichnamige Sicherungsdatei, so wird diese zuerst umbenannt, indem das Tagesdatum angehängt wird. Die Sicherungskopie kann im Fall einer erneuten Installation als Vorlage für die Generierung der neuen Konfigurationsdatei verwendet werden. Achten Sie in diesem Zusammenhang bitte darauf, dass die Sicherungskopie dem gewünschten Stand entspricht.

DNS-Entwicklungsteile installieren/deinstallieren

Mit den DNS-Entwicklungsteilen werden zusätzliche Dateien bereitgestellt, die nicht für den Betrieb des DNS-Resolver-Dämons benötigt werden. Sie umfassen die Resolver-Bibliothek mit den zugehörigen man-pages, die benötigt werden, wenn eine Sockets-Anwendung in POSIX mit hinzugebundener Resolver-Bibliothek produziert werden soll (siehe Tabelle auf Seite 225).

Die DNS-Entwicklungsteile werden mit folgendem Shell-Skript im POSIX-Dateisystem bereitgestellt:

/opt/TCP-IP-SV/dns/etc/install.TCP-IP-SV-DEV.nnn.DNS

Wenn die DNS-Entwicklungsteile nicht mehr benötigt werden, können sie mit dem folgenden Shell-Skript aus dem POSIX-Dateisystem entfernt werden:

/opt/TCP-IP-SV/dns/etc/remove.TCP-IP-SV-DEV.nnn.DNS

7.2.2 DNS Resolver konfigurieren

Die Start-Prozedur */etc/init.d/dnsd* wird durch die Konfigurationsdatei */etc/default/TCP-IP-SV.dns* parametrisiert. Eingestellt werden können Job-Name, Account und Job-Klasse, unter denen der Dämon laufen soll. Außerdem kann festgelegt werden, ob der Dämon automatisch beim POSIX-Start gestartet wird.

Der Betrieb des DNS Resolver-Dämons wird durch die Konfigurationsdatei */etc/resolv.conf* gesteuert. Die Konfigurationsdatei kann mehrere Einträge enthalten, die die für den DNS Resolver relevanten Informationen spezifizieren.

Folgende Typen von Einträgen werden unterschieden:

- *nameserver*-Eintrag
- *domain*-Eintrag
- *search*-Eintrag
- *options*-Eintrag

Jeder Eintrag steht in einer eigenen Zeile der Konfigurationsdatei und beginnt mit dem Schlüsselwort (nameserver, domain etc.) in Spalte 1. Nach dem jeweiligen Schlüsselwort stehen durch Leerzeichen (blank) getrennt die Parameter des jeweiligen Eintrages. Nach dem letzten Parameter darf kein weiteres Leerzeichen (blank) stehen. Die Schlüsselwörter der */etc/resolv.conf*-Einträge werden in Kleinschreibung erwartet.

Zeilen in */etc/resolv.conf*, die mit einem Semikolon (;) beginnen, werden als Kommentarzeilen interprtetiert.

nameserver-Eintrag

```
nameserver ip_adresse
```

Mit einem *nameserver*-Eintrag wird dem DNS Resolver-Dämon die IP-Adresse eines DNS-Servers bekanntgegeben. Maximal dürfen drei *nameserver*-Einträge in der Konfigurationsdatei */etc/resolv.conf* spezifiziert werden.

Bei der Bearbeitung einer DNS-Anfrage durch den DNS Resolver-Dämon wird zuerst der mit dem ersten *nameserver*-Eintrag definierte DNS-Server abgefragt. Antwortet der erste DNS-Server nicht, dann wird, sofern vorhanden, der mit dem zweiten *nameserver*-Eintrag definierte DNS-Server abgefragt. Wenn auch der zweite Server nicht antwortet, wird das Verfahren mit dem dritten Name Server wiederholt. Antwortet auch der durch den dritten *nameserver*-Eintrag definierte DNS-Server nicht, dann sollten Sie die DNS-Anfrage mit allen DNS-Servern solange wiederholen, bis die maximal zulässige Anzahl an Wiederholversuchen (siehe *options*-Eintrag auf Seite 234, Parameter *attempts*) erreicht ist.

domain-Eintrag

domain domain

Durch den *domain*-Eintrag wird eine Default-Domäne für die Anfragen des DNS Resolver-Dämons an den bzw. die DNS Name Server definiert.

Dabei ist zu beachten:

- Es kann maximal ein *domain*-Eintrag in der Konfigurationsdatei */etc/resolv.conf* gültig sein. Enthält die Konfigurationsdatei mehrere *domain*-, aber keine *search*-Einträge, so gilt der letzte *domain*-Eintrag.
- *domain*- und *search*-Einträge entwerten sich gegenseitig, so dass bei mehreren *domain*- und *search*-Einträgen in der Konfigurationsdatei derjenige *domain*- bzw. *search*-Eintrag gilt, auf den kein weiterer *domain*- oder *search*-Eintrag mehr folgt.

Die Wirkungsweise des *domain*-Eintrages ist abhängig davon, ob der in einer DNS-Anfrage angegebene DNS-Name einen Punkt (.) enthält oder nicht.

Die folgende Beschreibung gilt für die Standardeinstellung des *ndots*-Parameters des *options*-Eintrags (siehe Seite 234).

- Wirkungsweise des *domain*-Eintrages, in dem der angegebene DNS-Name einen Punkt enthält:

  Wenn der DNS-Server eine DNS-Anfrage nach einem Namen *name* nicht erfolgreich beantworten kann, wird vom DNS Resolver-Dämon eine erneute DNS-Anfrage mit *name.domain* an den DNS-Server gestellt. Schlägt auch diese DNS-Anfrage fehl, dann stellt der DNS Resolver-Dämon eine weitere DNS-Anfrage mit der übergeordneten Domäne an den DNS-Server. Dieses Verfahren wird ggf. fortgesetzt bis zu einer DNS-Anfrage, bei der die angefügte Domäne eine Ebene unterhalb der Top Level Domäne liegt.

Beispiel

Das folgende Beispiel zeigt die vom DNS Resolver-Dämon erzeugten Anfragen an einen DNS-Server.

Eintrag in der Konfigurationsdatei */etc/resolv.conf*:

```
domain mch.fj.example
```

Vom Anwender angegebener Name:

```
my.host
```

Vom DNS Resolver-Dämon erzeugte Namen für die Anfragen an einen DNS-Server:

1. `my.host`
2. `my.host.mch`.fj.example
3. `my.host`.fj.example

- Wirkungsweise des *domain*-Eintrages, in dem der angegebene DNS-Name keinen Punkt enthält:

  Wenn der DNS-Server eine Anfrage für einen Namen *name.domain* nicht erfolgreich beantworten kann, wird vom DNS Resolver-Dämon eine erneute DNS-Anfrage mit *name* an den Server gestellt.

  Beispiel

  Das folgende Beispiel zeigt die vom DNS Resolver-Dämon erzeugten Anfragen an einen DNS-Server.

  Eintrag in der Konfigurationsdatei */etc/resolv.conf*:

  ```
  domain mch.fj.example
  ```

  Vom Anwender angegebener Name:

  ```
  myhost
  ```

  Vom DNS Resolver-Dämon erzeugter Name für Anfragen an einen DNS-Server:

  1. `myhost.mch`.fj.example
  2. `myhost`.fj.example
  3. `myhost`

search-Eintrag

```
search domain1[ domain2[ .... [ domain6]]]
```

Durch den *search*-Eintrag werden dem DNS Resolver-Dämon mehrere Domänennamen für die Anfragen an den bzw. die DNS Name Server definiert.

Dabei ist zu beachten:

- Es kann maximal ein *search*-Eintrag in der Konfigurationsdatei */etc/resolv.conf* gültig sein. Enthält die Konfigurationsdatei mehrere *search*-, aber keine *domain*-Einträge, so gilt der letzte *search*-Eintrag.
- *domain*- und *search*-Einträge entwerten sich gegenseitig, so dass bei mehreren *domain*- und *search*-Einträgen in der Konfigurationsdatei derjenige *domain*- bzw. *search*-Eintrag gilt, auf den kein weiterer *domain*- oder *search*-Eintrag mehr folgt.

Die Wirkungsweise des *search*-Eintrages hängt davon ab, ob der in einer Anfrage angegebene DNS-Name einen Punkt (.) enthält oder nicht.

- Wirkungsweise des *search*-Eintrages, falls der angegebene DNS-Name einen Punkt enthält:

  Wenn der DNS-Server eine DNS-Anfrage für einen Namen *name* nicht erfolgreich beantworten kann, stellt der DNS Resolver-Dämon eine erneute DNS-Anfrage mit *name.domain1* an den DNS-Server.

  Falls diese DNS-Anfrage vom DNS-Server ebenfalls nicht erfolgreich beantwortet werden kann, wiederholt der DNS Resolver-Dämon die DNS-Anfrage mit dem nächsten im *search*-Eintrag definierten Domänennamen *domainx* (x = 2 - 6). Dies wird solange fortgesetzt, bis entweder die DNS-Anfrage vom DNS-Server erfolgreich beantwortet werden kann oder bis kein weiterer Domänenname im *search*-Eintrag definiert ist.

Beispiel

Das folgende Beispiel zeigt die vom DNS Resolver-Dämon erzeugten Anfragen an einen DNS-Server:

Eintrag in der Konfigurationsdatei */etc/resolv.conf*:

```
search mch.fj.example fj.example
```

Vom Anwender angegebener Name: `my.host`

Vom DNS Resolver-Dämon erzeugte Namen für die Anfragen an einen DNS-Server:

1. `my.host`
2. `my.host.mch`.fj.example
3. `my.host`.fj.example

- Wirkungsweise des *search*-Eintrages, falls der angegebene DNS-Name keinen Punkt enthält:

  Zuerst wird eine DNS-Anfrage mit *name.domain1* an den DNS-Server gestellt. Wird diese DNS-Anfrage vom DNS-Server nicht erfolgreich beantwortet, dann wird vom DNS Resolver-Dämon die DNS-Anfrage mit dem nächsten im *search*-Eintrag definierten Domänennamen *domainx* (*x* = 2 bis 6) wiederholt. Dies wird solange fortgesetzt, bis entweder die DNS-Anfrage vom DNS-Server erfolgreich beantwortet werden konnte oder bis kein weiterer Domänenname im *search*-Eintrag definiert ist.

  Falls nach der Abarbeitung der in der *search*-Anweisung definierten Domänennamen noch kein DNS-Anfrage vom DNS-Server erfolgreich beantwortet wurde, wird eine DNS-Anfrage mit *name* gestellt.

  Beispiel

  Das folgende Beispiel zeigt die vom DNS Resolver-Dämon erzeugten Anfragen an einen DNS-Server.

  Eintrag in der Konfigurationsdatei */etc/resolv.conf*:

  ```
  search mch.fj.example fj.example
  ```

  Vom Anwender angegebener Name: myhost

  Vom DNS Resolver-Dämon erzeugte Namen für die Anfragen an einen DNS-Server:

  1. `myhost.mch`.fj.example
  2. `myhost`.fj.example
  3. `myhost`

options-Eintrag

```
options option [option] ...
```

Durch den *options*-Eintrag wird mithilfe der einzelnen, für *option* spezifizierten Werte das Verhalten einer Reihe von Resolver-Routinen festgelegt.

Für *option* können Sie die folgenden Werte spezifizieren:

debug
: Damit wird der Diagnose-Mechanismus des DNS Resolver-Dämons eingeschaltet, und es werden Diagnosemeldungen in die Datei */var/adm/syslog* geschrieben.

ndots:*n*
: Spezifiziert den unteren Schwellenwert für die Anzahl an Punkten („.“), die ein bei einer DNS-Anfrage übergebener Name enthalten muss, damit eine erste absolute („as-is“) Anfrage an den DNS Name Server ausgeführt wird.
Voreinstellung ist `ndots:1`. Wenn also in einer Anfrage an den DNS Name Server ein Name mindestens einen Punkt enthält, wird dieser Name bei einer Anfrage zunächst als absoluter Name behandelt, bevor er um Domänen-Namen ergänzt wird (siehe auch *domain*-Eintrag auf Seite 230).

attempts:*n*
: Spezifiziert die maximale Anzahl an Verbindungsversuchen, die pro DNS-Anfrage zu jedem DNS Name Server unternommen werden. Die Angabe `attempts:0` entspricht in ihrer Wirkung der Angabe `attempts:1`.
Voreinstellung ist `attempts:4`

timeout:*n*
: Spezifiziert den Start-Timeout-Wert für einen erneuten Übertragungsversuch (Retransmission) in Sekunden. Bei jedem folgenden Versuch wird der vorausgegangene Timeout-Wert verdoppelt, bis die maximale Anzahl an Verbindungsversuchen (siehe Parameter *attempts*) erreicht ist. Die Angabe `timeout:0` entspricht der Angabe `timeout:1`.
Voreinstellung ist `timeout:5`.
Bei Verwendung der voreingestellten Werte für *attempts* und *timeout* ergibt sich als Gesamt-Timeout-Wert für jeden DNS-Server folgender Wert:
5+10+20+40=75 Sekunden.

rotate
: Die Anfragen werden im Zeitscheibenverfahren an die mithilfe des *nameserver*-Eintrags generierten DNS Name Server gerichtet. Anstatt also alle Clients ihre erste Anfrage jeweils an den ersten aufgelisteten DNS-Server richten zu lassen, wird so das Anfrage-Aufkommen gleichmäßig auf alle aufgelisteten DNS Name Server verteilt.

no_tld_query
: Veranlasst den DNS Resolver, nicht nach dem Namen der Top Level Domäne zu suchen, d.h. nach einem Namen, der keine Punkte („.“) enthält. Die Verwendung dieser Option verhindert nicht, dass der DNS Resolver die Regeln gemäß eines *domain*- oder *search*-Eintrags anwendet.

7.2.3 DNS Resolver - Administration und Betrieb

Dieser Abschnitt informiert über folgende Themen:

- DNS Resolver starten und beenden
- Konfiguration des DNS Resolvers ändern

7.2.3.1 DNS Resolver starten und beenden

DNS Resolver wird automatisch beim Start des Subsystems POSIX gestartet und beim POSIX-Shutdown beendet, falls es per AUTOSTART='yes' in */etc/default/TCP-IP-SV.dns* aktiviert ist.

Start-Aufruf für den DNS Resolver

Für den DNS Resolver-Dämon lautet der Start-Aufruf:

```
/etc/init.d/TCP-IP-SV.dns start
```

Es wird zunächst geprüft, ob AUTOSTART auf 'yes' gesetzt ist. Wenn nicht, dann wird keine weitere Aktion durchgeführt. Andernfalls wird geprüft, ob bereits ein Dämon gestartet ist. Falls ja, dann wird nur eine entsprechende Meldung ausgegeben, ansonsten wird der Dämon gestartet.

Wenn der Dämon unabhängig von AUTOSTART in jedem Fall gestartet werden soll, dann muss die Option *mstart* anstatt *start* verwendet werden.

Mit der Option *dstart* kann man den Dämon zu Debug-Zwecken im Vordergrund laufen lassen, ggf. müssen die Debug-Optionen im Skript *TCP-IP-SV.dns* angepasst werden.

Restart-Aufruf für den DNS Resolver

Für den DNS Resolver-Dämon wird ein Restart-Aufruf angeboten. Dieser ist erforderlich, wenn im laufenden Betrieb eine modifizierte Konfigurationsdatei eingelesen werden soll.

Der Restart-Aufruf für den DNS Resolver lautet:

```
/etc/init.d/TCP-IP-SV.dns restart
```

Innerhalb des Restartprozedur-Ablaufs wird überprüft, ob der entsprechende Dämon gestartet ist. Wenn kein aktiver Dämon gefunden wird, erfolgt ein normaler Neustart.

DNS Resolver beenden

Für die Außerbetriebnahme des DNS Resolver-Dämons steht der folgende Aufruf zur Verfügung:

```
/etc/init.d/TCP-IP-SV.dns stop
```

Die Außerbetriebnahme gilt nur bis zur Beendigung des Subsystems POSIX. Soll ein automatischer Wiederanlauf beim erneuten Starten des Subsystems POSIX verhindert werden, dann muss in */etc/default/TCP-IP-SV.dns* die Variable AUTOSTART auf 'no' oder 'never' gesetzt werden.

7.2.3.2 Konfiguration des DNS Resolvers ändern

Die Konfigurationsdatei */etc/resolv.conf* des DNS Resolver-Dämons kann in der POSIX-Shell unter $TSOS bzw. $SYSROOT geändert werden. Die Konfigurationsdatei kann mit dem EDT bearbeitet werden. Beim Editieren der Konfigurationsdatei muss die Syntax der Einträge genau beachtet werden, da es sonst zu unerwünschten Ergebnissen bei DNS-Anfragen kommen kann.

Änderungen in der Konfigurationsdatei werden durch einen Neustart bzw. Restart des DNS Resolver-Dämons aktiv (siehe Seite 236).

7.2.4 DNS Resolver - Diagnose und Wartung

In diesem Abschnitt sind Logging-Funktionalität und Diagnose-Möglichkeiten für DNS beschrieben.

7.2.4.1 DNS Resolver - Logging

Der DNS Resolver legt seine Logging-Informationen in der Datei */var/adm/syslog* ab. Diese Einträge haben das folgende Grundformat:

```
Jan 22 15:44:58 LOG_NOTICE dnsd[nnn] <meldungtext>
```

Nach der Ausgabe von Datum und Systemzeit folgt ein Schlüsselwort für die Klassifizierung der Meldung. Der DNS Resolver-Dämon verwendet für seine Loggingmeldungen nur das Schlüsselwort LOG_NOTICE.

Nach dieser Klassifizierung kommt die Kennzeichnung als Systemmeldung mit der Information über die zugehörige Prozessnummer PID [pid]. Ist zur Meldungsausgabe keine gültige PID verfügbar (z.B. bei Meldungsausgabe durch die Start-Prozedur des Dämons), dann wird ein leerer Klammerausdruck ausgegeben. Nach der PID wird, in Doppelpunkten eingerahmt, der Name des Dämons (hier: *dnsdamon*) ausgegeben. Daran anschließend folgt der eigentliche, spezifische Meldungstext.

Nach Eingabe des Kommandos *stopdns*, d.h. wenn der DNS Resolver-Dämon sich beendet hat bzw. nicht mehr läuft, werden keine Logging-Meldungen ausgegeben.

7.2.4.2 DNS Resolver - Diagnosemöglichkeiten

Mithilfe des *options*-Eintrags (`options debug`, siehe Seite 234) in der Konfigurationsdatei */etc/resolv.conf* schalten Sie den Diagnose-Mechanismus des DNS ein. Die Diagnosemeldungen des DNS Resolver-Dämons werden dann in der Datei */var/adm/syslog* protokolliert.

7.3 DNS Name Server NAMED

Dieser Abschnitt informiert über folgende Themen:

- NAMED installieren und deinstallieren
- NAMED konfigurieren
- Administration und Betrieb von NAMED
- Diagnose und Wartung von NAMED

7.3.1 NAMED installieren und deinstallieren

Beachten Sie bitte zusätzlich die mit dem Produkt interNet Services ausgelieferte Freigabemitteilung.

Die einzelnen Komponenten des Software-Pakets interNet Services werden als ein POSIX-Programmpaket per Package-Installation mit dem POSIX-Installationsprogramm installiert (siehe Handbuch „POSIX Grundlagen für Anwender und Systemverwalter“).
Nähere Informationen zur Installation der Komponenten finden Sie auch im Abschnitt „Installation“ auf Seite 37.

Zur Installation und zum Betrieb der TCP-IP-SV-Komponente muss die PLAM-Bibliothek SINLIB.TCP-IP-SV.*nnn*.NAMED shareable zur Verfügung stehen. Bei der Installation von NAMED kann zusätzlich der Installationspfad im POSIX-Dateisystem definiert werden. Standardmäßig wird in das Verzeichnis /opt/TCP-IP-SV/*dns-named* installiert.

NAMED installieren

Nach erfolgreicher Installation der NAMED-Komponente befinden sich die relevanten Kommandos und Dateien in den Verzeichnissen */usr/sbin*, */usr/bin* und */etc* sowie im Installationsverzeichnis */opt/TCP-IP-SV/dns-named*. In der Tabelle auf Seite 239 steht <instdir> für das Installationsverzeichnis */opt/TCP-IP-SV/dns-named*.

Verzeichnis	Datei	Beschreibung
/etc/	named.conf	DNS-Konfigurationsdatei des Name Servers
/etc/default	TCP-IP-SV.named	Parameterdatei für Start/Stopp-Prozedur
	TCP-IP-SV.named.default	Default für TCP-IP-SV.named
/etc/init.d/	TCP-IP-SV.named	Start/Stopp-Prozedur

[1)] Nur verfügbar, wenn die NAMED-Entwicklungsteile installiert sind (siehe Seite 242).

Verzeichnis	Datei	Beschreibung
/etc/rc0.d/	K64TCP-IP-SV.named	symbolischer Link auf */etc/init.d/TCP-IP-SV.named* zum Beenden beim POSIX-Shutdown
/etc/rc2.d/	S72TCP-IP-SV.named	symbolischer Link auf */etc/init.d/TCP-IP-SV.named* zum Starten beim POSIX-Start
/usr/bin/	nsupdate	symbolischer Link auf *<instdir>/bin/nsupdate*
/usr/lib/	liblwres.a libisccfg.a libisccc.a libisc.a libdns.a	zusätzliche DNS-Bibliotheken, die für den Ablauf von NAMED nicht benötigt werden[1)]
/usr/sbin/	in.named	symbolischer Link auf *<instdir>/sbin/named*
	named-checkconf	symbolischer Link auf *<instdir>/sbin/named-checkconf*
	named-checkzone	symbolischer Link auf *<instdir>/sbin/named-checkzone*
	rndc	symbolischer Link auf *<instdir>/sbin/rndc*
	rndc-confgen	symbolischer Link auf *<instdir>/sbin/rndc-confgen*
	dnssec-keygen	symbolischer Link auf *<instdir>/sbin/dnssec-keygen*
	dnssec-signzone	symbolischer Link auf *<instdir>/sbin/dnssec-signzone*
<instdir>/etc/	install.TCP-IP-SV-DEV.*nnn*.NAMED	Installationsskript für die Entwicklungsteile
	remove.TCP-IP-SV-DEV.*nnn*.NAMED	Deinstallationsskript für die Entwicklungsteile
<instdir>/include/	*	Include-Dateien[1)]
<instdir>/readme/	bind9arm.pdf	Bind9 Administrator Reference Manual
	*	man-pages im HTML- und Text-Format

[1)] Nur verfügbar, wenn die NAMED-Entwicklungsteile installiert sind (siehe Seite 242).

Verzeichnis	Datei	Beschreibung
<instdir>/sbin/	named	DNS Name Server-Dämon
	named-checkconf	Syntaxprüfung einer *named.conf*-Datei
	named-checkzone	Syntaxprüfung einer Zonendaten-Datei
	rndc	Remote-Steuerungs-Programm für Name Server-Dämon
	rndc-confgen	Generierungsprogramm für *rndc*-Konfigurationsdatei
	dnssec-dsfromkey	Generierung des "Delegation Signer" Resource-Record.
	dnssec-keygen	Schlüsselgenerierung
	dnssec-revoke	Widerruf eines Schlüsselpaars
	dnssec-settime	Programm zum Setzen und Anzeigen von schlüsselspezifischen Zeitangaben
	dnssec-signzone	Zone zuweisen

[1)] Nur verfügbar, wenn die NAMED-Entwicklungsteile installiert sind (siehe Seite 242).

Nach erfolgreicher Installation werden die weiteren erforderlichen Aktivitäten unter der POSIX-Shell in einer Kennung mit POSIX-Root-Berechtigung ausgeführt. Dazu wird mit dem BS2000-Kommando START-POSIX-SHELL die POSIX-Shell gestartet.

Nach Installation der interNet-Services müssen vor der Inbetriebnahme die für die DNS-Komponenten spezifischen Konfigurations- und Systemdateien an die individuellen Erfordernisse angepasst werden.

NAMED deinstallieren

Analog zur Installation der Komponenten von interNet Services wird auch die Deinstallation mithilfe des POSIX-Installationsprogrammes unter der Kennung TSOS durchgeführt.

Bevor Sie mit dem POSIX-INSTALLER die NAMED-Komponenten entfernen, sollten Sie mit dem Skript *<instdir>/etc/remove.TCP-IP-SV-DEV.nnn.NAMED* die Entwicklerteile entfernen, falls Sie diese installiert hatten.

Bei der Deinstallation wird nach dem aktiven DNS NAMED-Dämon gesucht und dieser beendet. In der Syslog-Datei */var/adm/syslog* wird die Beendigung noch aktiver Dämonen protokolliert. Anschließend werden alle Dateien, Links und Prozeduren des DNS NAMED gelöscht.

Im Rahmen der Deinstallation werden die Konfigurationsdateien */etc/named.conf* und */etc/default/TCP-IP-SV.named* gesichert. Existiert schon eine gleichnamige Datei mit unterschiedlichem Inhalt, dann wird diese durch Anhängen des Tagesdatums umbenannt. Die Siche-

rungskopie wird im Fall einer erneuten Installation wieder in das jeweilige Verzeichnis kopiert. Achten Sie in diesem Zusammenhang bitte darauf, dass die Sicherungskopie dem gewünschten Stand entspricht.

NAMED-Entwicklungsteile installieren/deinstallieren

Mit den NAMED-Entwicklungsteilen werden zusätzliche Dateien bereitgestellt, die nicht für den Betrieb des NAMED benötigt werden. Sie umfassen intern genutzte Bind9-Bibliotheken sowie die zugehörigen Include-Dateien, die standardmäßig mit Bind9 bereitgestellt werden, aber nur dann benötigt werden, wenn Anwendungsentwicklung auf Basis dieser Bind9-Bibliotheken erfolgen soll (siehe Tabelle auf Seite 239).

Die NAMED-Entwicklungsteile werden mit dem folgenden Shell-Skript im POSIX-Dateisystem bereitgestellt:

/opt/TCP-IP-SV/dns-named/etc/install.TCP-IP-SV-DEV.nnn.NAMED

Wenn die NAMED-Entwicklungsteile nicht mehr benötigt werden, können Sie diese mit dem folgenden Shell-Skript aus dem POSIX-Dateisystem entfernen:

/opt/TCP-IP-SV/dns-named/etc/remove.TCP-IP-SV-DEV.nnn.NAMED

7.3.2 NAMED konfigurieren

Dieser Abschnitt informiert über folgende Themen:

– NAMED Konfigurationsdatei *named.conf*
– NAMED und Sicherheit
– NAMED Prozessmodelle

7.3.2.1 NAMED Konfigurationsdatei named.conf

Der Betrieb des DNS Name Server-Dämons wird durch die Konfigurationsdatei */etc/named.conf* gesteuert. Die Syntax der Konfigurationsdatei *named.conf* ist im Handbuch „BIND9 Administrator Reference Manual“ des Internet Software Consortium beschrieben.

Beispiel: Aufbau einer named.conf-Datei

```
options {
   directory "/var/named";
};

logging {
   channel my_security_channel {file "my_security_file"; severity info; };
   category security { my_security_channel; default syslog; };
   category cname { null; };
};

zone "test1.mch.fj.example" IN {
   type master;
   file "masterzone";
};

zone "test2.mch.fj.example" IN {
   type slave;
   file "slavezone";
   masters { 155.90.80.1; };
};

zone "." in {
   type hint;
   file "named.cache";
};

zone "60.155.in-addr.arpa" IN {
   type master;
   file "arpafile";
};
```

```
zone "0.0.127.in-addr.arpa" in {
   type master;
   file "loopback";
};
```

7.3.2.2 NAMED Zonendaten-Dateien

Neben allgemeinen Konfigurationseinstellungen enthält die Datei */etc/named.conf* auch Informationen über die einzurichtenden Zonen. Die eigentlichen Zonendaten werden in lokalen Systemdateien als Resource Records abgelegt und beim Starten des Server-Dämons aus diesen Systemdateien gelesen.

Die Syntax der lokalen Zonendaten-Dateien sind im Handbuch „BIND9 Administrator Reference Manual“ des Internet Software Consortium beschrieben.

Alle Zonendaten-Dateien müssen im SRR (Standard Resource Record)-Format erstellt werden, wobei jede Zeile der Datei einen Resource Record (RR) enthält.

Beispiel: Aufbau der Datei masterzone

```
test1.mch.fj.example.  IN  SOA  host1.test1.mch.fj.example.postmaster (
                       1 ; serial
                       10800 ;    Refresh nach 3 Stunden
                       3600 ;     Retry nach einer Stunde
                       604800 ;   Expire nach einer Woche
                       86400) ;   Minimale TTL von einem Tag
;
;  Nameserver
;
test1.mch.fj.example.  IN    NS     host1.test1.mch.fj.example.
                       IN    NS     host2.test1.mch.fj.example.
;
;  Adressen
;
host1             IN     A        155.60.70.1
host2             IN     A        155.60.70.2
host3             IN     A        155.60.70.3
loopback          IN     A        127.0.0.1
;  Aliases
;
alias1            IN    CNAME        host1.test1.mch.fj.example.
;
;   Mail Exchanger
;
test1.mch.fj.example.    IN    MX    0      host1.test1.mch.fj.example.
test1.mch.fj.example.    IN    MX    10     host3.test1.mch.fj.example.
```

Beispiel: Aufbau der Datei arpafile

```
60.155.in_addr.arpa.    IN   SOA   host1.test1.mch.fj.example.postmaster (
                        1       ; serial
                        10800   ; Refresh nach 3 Stunden
                        3600    ; Retry nach einer Stunde
                        604800  ;  Expire nach einer Woche
                        86400)  ;  Minimale TTL von einem Tag
;
;  Nameserver
;
60.155.in_addr.arpa.     IN  NS     host1.test1.mch.fj.example.
                         IN  NS     host2.test1.mch.fj.example.
;
;  Adressen
;
1.70            IN         PTR     host1.test1.mch.fj.example.
2.70            IN         PTR     host2.test1.mch.fj.example.
3.70            IN         PTR     host3.test1.mch.fj.example.
```

Beispiel: Aufbau der Datei loopback

```
0.0.127.in_addr.arpa.  IN  SOA  host1.test1.mch.fj.example.postmaster (
                       1       ; serial
                       10800   ; Refresh nach 3 Stunden
                       3600    ; Retry nach einer Stunde
                       604800  ; Expire nach einer Woche
                       86400)  ; Minimale TTL von einem Tag
;
;  Nameserver
;
0.0.127.in_addr.arpa.  IN  NS     host1.test1.mch.fj.example.
;
;  Adressen
;
1.0.0.127.in_addr.arpa.  IN  PTR    localhost.
```

7.3.2.3 NAMED und Sicherheit

Bei der Konfiguration von NAMED können durch folgende Optionen Sicherheitsaspekte beim Zugriff auf die Daten berücksichtigt werden:

- Mit der Option *allow-query* der *options*-Anweisung kann die Berechtigung, Anfragen an den Name Server zu richten, auf einzelne Hosts eingeschränkt werden.
- Mit der Option *allow-transfer* der *options*-Anweisung kann die Berechtigung, Zonentransfers vom Name Server zu erhalten, auf einzelne Hosts eingeschränkt werden.
- Zonenspezifisch kann mit der Option *allow-update* der *zone*-Anweisung die Möglichkeit des dynamischen Updates der Daten auf einzelne Hosts eingeschränkt werden.

TSIG

Ein weiterer Sicherheitsmechanismus sind die Transaction SIGnatures (TSIG). Sie unterstützen die Server-zu-Server-Kommunikation, einschließlich Zonentransfer, Notify und rekursiven Queries.

TSIG ist schlüssel-basiert und wird auf die Kommunikation zwischen zwei DNS Name Servern angewendet. TSIG erzeugt zunächst einen Schlüssel (automatisch oder manuell), den sich die beiden Server teilen. Durch Einträge in den Konfigurationsdateien der Server werden Übergabe und Verwendung der Schüssel gesteuert.

Eine ausführliche Beschreibung über die Arbeitsweise von TSIG finden Sie im Handbuch „BIND9 Administrator Reference Manual“ des Internet Software Consortium.

DNSSEC

DNS Security (DNSSEC)-Erweiterungen erlauben die kryptographische Authentifizierung der DNS Information. Sie sind in RFC 2535 definiert.

DNSSEC verwendet öffentliche Schlüssel für die Verschlüsselung. Dadurch können Zonen-Administratoren die Zonendaten digital signieren und sich authentifizieren. Zwischen den Administratoren der Parent-Zone und/oder Child-Zone muss eine Kommunikation bestehen, um Schlüssel und Signaturen zu übertragen.

DNSSEC stellt u.a. folgende Tools zur Verfügung:

- *dnssec-keygen* für die Schlüsselgenerierung
- *dnssec-signzone* für die Signierung einer Zone

Eine ausführliche Beschreibung über die Arbeitsweise von DNSSEC finden Sie im Handbuch „BIND9 Administrator Reference Manual“ des Internet Software Consortium.

NAMED ohne Root-Berechtigung ablaufen lassen

Standardmäßig wird NAMED mit Root-Berechtigung ausgeführt. Um zu verhindern, dass bei eventuellen Sicherheitsproblemen der Software ein Eindringling vollen Zugriff auf das Dateisystem erhalten bzw. Kommandos unter Root-Berechtigung ausführen kann, ist es möglich, NAMED auch ohne Root-Berechtigung ablaufen zu lassen. Mithilfe des */etc/default/TCP-IP-SV.named*-Parameters *USERID* können Sie NAMED unter einer beliebigen Benutzerkennung ablaufen lassen. Es empfiehlt sich, für *USERID* die niedrigst-privilegierte Benutzerkennung zu spezifizieren.

Für die Arbeitsdateien, die in der Konfigurationsdatei *named.conf* für die Einträge *directory* und *pidfile* vereinbart wurden, muss die in *USERID* definierte Benutzerkennung Schreib- und Leseberechtigung erhalten.

7.3.3 NAMED - Administration und Betrieb

Administration und Betrieb von NAMED umfassen folgende Aufgaben:

- NAMED starten und beenden
- NAMED Zonendaten ändern

7.3.3.1 NAMED starten und beenden

NAMED wird automatisch beim Start des Subsystems POSIX gestartet und beim POSIX-Shutdown beendet, falls es per AUTOSTART='yes' in */etc/default/TCP-IP-SV.named* aktiviert ist.

Start-Aufruf für NAMED

Für den NAMED-Dämon lautet der Start-Aufruf:

```
/etc/init.d/TCP-IP-SV.named start
```

Es wird zunächst geprüft, ob AUTOSTART auf 'yes' gesetzt ist. Wenn nicht, dann wird keine weitere Aktion durchgeführt. Andernfalls wird geprüft, ob bereits ein Dämon gestartet ist. Falls ja, dann wird nur eine entsprechende Meldung ausgegeben, ansonsten wird der Dämon gestartet.

Wenn der Dämon unabhängig von AUTOSTART in jedem Fall gestartet werden soll, dann muss die Option *mstart* anstatt *start* verwendet werden.

Mit der Option *dstart* kann man den Dämon zu Debug-Zwecken im Vordergrund laufen lassen, ggf. müssen die Debug-Optionen im Skript *TCP-IP-SV.named* angepasst werden.

Mithilfe des Parameters *USERID* in der Datei */etc/default/TCP-IP-SV.named* legen Sie fest, ob NAMED ohne Root-Berechtigung ablaufen soll (siehe Seite 247).

Restart-Aufruf für NAMED

Für den NAMED wird ein Restart-Aufruf angeboten. Dieser ist erforderlich, wenn im laufenden Betrieb eine modifizierte Konfigurationsdatei eingelesen werden soll.

Der Restart-Aufruf für den NAMED lautet:

```
/etc/init.d/TCP-IP-SV.named restart
```

Beim Ablauf der Restartprozedur wird überprüft, ob der entsprechende Dämon gestartet ist. Wenn kein aktiver Dämon gefunden wird, erfolgt ein normaler Neustart.

NAMED beenden

Für die Außerbetriebnahme des NAMED-Dämons steht folgender Aufruf zur Verfügung:

```
/etc/init.d/TCP-IP-SV.named stop
```

ACHTUNG!

Die Außerbetriebnahme gilt nur bis zur Beendigung des Subsystemes POSIX. Soll ein automatischer Wiederanlauf beim erneuten Starten des Subsystemes POSIX verhindert werden, dann muss in */etc/default/TCP-IP-SV.named* die Variable AUTOSTART auf 'no' oder 'never' gesetzt werden.

7.3.3.2 NAMED Zonendaten ändern

Änderungen der Zonendaten-Dateien des NAMED werden erst durch einen Neustart des NAMED wirksam.

Darüber hinaus ist es möglich, die Zonendaten-Datei über sog. dynamische Updates anzupassen. In diesem Fall lassen sich Resource Records dynamisch im laufenden Server-Betrieb hinzufügen, löschen oder ändern. Insbesondere in Verbindung mit DHCP wird diese Eigenschaft künftig eine wichtige Rolle spielen.

Dynamischer Update

Mithilfe des dynamischen Updates können Sie (ggf. abhängig von Vorbedingungen) Records oder RRsets in den Masterzonen-Dateien hinzufügen, ändern oder löschen. Der dynamische Update ist vollständig in RFC 2136 beschrieben.

Der dynamische Update ist verfügbar auf einer zone-by-zone Basis, gesteuert durch die Parameter *allow-update* oder *update-policy clause* in der *zone*-Anweisung.

Das Update von „secure zones“ (Zonen, die DNSSEC benutzen) erfolgt gemäß RFC 3007 und Nachfolgende: SIG und NXT Records, die von den Updates betroffen sind, werden automatisch durch den Server, der einen online Zonenschlüssel benutzt, wiederhergestellt. Die Update Autorisierung basiert auf Transaktions-Signaturen und einer expliziten Server-Policy.

Die Journaldatei

Alle Änderungen, die in einer Zone mit dem dynamischen Update gemacht wurden, werden in der Journaldatei der Zone gespeichert. Diese Datei wird automatisch vom Server angelegt, wenn der erste dynamische Update stattfindet. Der Name der Journaldatei wird gebildet, indem die Endung *.jnl* an den Namen der entsprechenden Zonendatei angehängt wird. Die Journaldatei liegt im Binärformat vor und sollte nicht manuell editiert werden.

Der Server schreibt gelegentlich den ganzen Inhalt der aktualisierten Zone in die Zonendatei („dump“). Dies wird nicht sofort nach jedem dynamischen Update veranlasst, weil dies den Server verlangsamen würde, wenn eine große Zone öfters aktualisiert wird. Stattdessen wird die Datenübernahme um 15 Minuten verzögert, damit auch zusätzliche Updates stattfinden können.

Nach einem Neustart des Servers wegen vorangegangenem Shutdown oder Crash wird die Journaldatei wieder eingespielt. Damit sind alle Updates, die seit dem letzten Zonendump durchgeführt wurden, in der Zone wieder verfügbar.

Änderungen, die durch hereinkommende Zonentransfers hervorgerufen werden, werden in gleicher Weise aufgezeichnet.

Zonendateien von dynamischen Zonen sollten in der Regel nicht manuell editiert werden, da sie nicht die letzten dynamischen Änderungen enthalten - diese sind nur in der Journaldatei. Die einzige Möglichkeit, sicherzustellen, dass die Zonendatei einer dynamischen Zone auf dem aktuellen Stand ist, besteht im Beenden des Servers mit *rndc stop*.

Um manuelle Änderungen in der dynamischen Zone durchzuführen, verfahren Sie wie folgt:

- Fahren Sie den Server mit *rndc stop* herunter.

  Es genügt nicht, ein Signal zu senden oder *rndc halt* einzugeben.

- Warten Sie, bis der Server beendet ist.
- Entfernen Sie die Journaldatei (*remove).*
- Editieren Sie die Zonendaten-Datei.
- Starten Sie den Server neu.

ACHTUNG!

Sie müssen die Journaldatei entfernen, da die manuellen Änderungen nicht im Journal nachvollziehbar sind und somit Inkonsistenzen zum Inhalt der Zonendatei entstehen.

7.3.4 NAMED - Diagnose und Wartung

In diesem Abschnitt sind die Logging- und Diagnosemöglichkeiten für NAMED beschrieben.

7.3.4.1 NAMED - Logging

Der DNS Name Server NAMED legt seine Logging-Informationen in der Datei */var/adm/syslog* ab. In der Konfigurationsdatei */etc/named.conf* kann mit der *logging*-Funktion festgelegt werden, für welche Bereiche (categories) das Logging durchgeführt werden soll und wohin, d.h. auf welche Kanäle (channels), die Logging-Informationen ausgegeben werden sollen.

Im Standardfall werden alle Meldungen mit Severity „Info“ bis „Critical“ über SYSLOG in der Datei */var/adm/syslog* abgelegt. Ausnahmen sind die Meldungen der Kategorien „Packet“ und „Eventlib“. Diese Meldungen, sowie alle Debug-Meldungen, werden in der Datei *named.run* im Startverzeichnis des NAMED-Dämons abgelegt.

Die Einträge des NAMED-Dämons in der Logging Datei *var/adm/syslog* enthalten folgende Informationen:

– Datum und Systemzeit
– Schlüsselwort für die Klassifizierung, das der Meldungspriorität (severity) entspricht
– Name des NAMED-Dämons und Prozessnummer (PID)
– Logging-Bereich (Category)
– eigentliche Meldung

Beispiel

```
Nov 03 11:14:12.574 load: info: master zone "test.mch.fj.example" (IN)
loaded(serial 36)
```

Die Einträge des NAMED-Dämons in der Datei *named.run* enthalten folgende Informationen:

– Datum und Systemzeit
– Logging-Bereich (Category)
– eigentliche Meldung

Beispiel

```
30-Jan-2010 11:14:12.574 load: info: master zone "test.mch.fj.example" (IN)
loaded (serial 36)
```

Weitere Informationen zum Logging finden Sie im Abschnitt „NAMED konfigurieren“ auf Seite 243.

7.3.4.2 NAMED - Diagnosemöglichkeiten

Alle Aktionen des NAMED werden im Debug-Modus mitprotokolliert. Diesen Modus können Sie durch Setzen der Umgebungsvariablen *DEBUGNAMED* oder über das *rndc*-Tool einschalten. Die Menge an Diagnose-Informationen hängt vom Debug-Level ab. Je höher dieser Level ist, umso detaillierter sind die Meldungen. Den Level können Sie direkt in der Umgebungsvariablen *DEBUGNAMED* übergeben oder mit dem *rndc*-Tool setzen. Ausschalten können Sie den Debug-Modus ebenfalls über das *rndc*-Tool.

Eine weitere Diagnosemöglichkeit ist der Datenbank-Dump. Mithilfe des *rndc*-Tools können Sie die Ausgabe der im Cache liegenden Daten sowie der Root-Daten in eine Datei auslösen. Außerdem können Sie mithilfe des *rndc*-Tools ein Abfrage-Logging aktivieren.

Das *rndc*-Tool ist im BIND9 Administrator Reference Manual des Internet Software Consortium beschrieben.

7.4 DNS Tools

Für Diagnose, Administration und Monitoring des NAMED stehen eine Reihe von Tools zur Verfügung. Nachfolgend finden Sie eine Auflistung dieser Tools. Eine Beschreibung dieser Tools finden Sie auf Ihrem Server unter */opt/TCP-IP-SV/dns/readme* bzw. unter */opt/TCP-IP-SV/dns-named/readme*.

Diagnose-Tools

- **dig** (domain information groper)

  Kommandozeilen-Tool für die Informationsbeschaffung zu den Domain Name Servern

- **host**

  Kommandozeilen-Tool zur Abfrage von Internet-Hostnamen

- **nslookup**

  Kommandozeilen-Tool zur Abfrage von Domain Name Servern im Internet. *nslookup* wird nicht mehr weiterentwickelt. Stattdessen soll künftig das Tool *dig* verwendet werden.

Administrations-Tools

- **rndc** (remote name daemon control)

  Tool zur Überwachung des Name Server-Betriebs

- **rndc-confgen**

  Utility zur Generierung der Datei *rndc.conf*

Eine ausführliche Beschreibung dieser Tools finden Sie im Handbuch „BIND9 Administrator Reference Manual“ des Internet Software Consortium.

7.4.1 Diagnose-Tool dig - Beispiele

Nachfolgend finden Sie eine Reihe von Beispielen für das Arbeiten mit dem Diagnose-Tool dig.

Abfrage der Adresse zu einem Namen (Serveradresse aus resolv.conf)

```
# dig ts.fujitsu.com

; <<>> DiG 9.7.1 <<>> ts.fujitsu.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27805
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;ts.fujitsu.com.                        IN      A

;; ANSWER SECTION:
ts.fujitsu.com.         86400   IN      A       217.115.66.11

;; Query time: 2 msec
;; SERVER: 123.123.123.123#53(123.123.123.123)
;; WHEN: Wed Nov 24 15:52:42 2010
;; MSG SIZE  rcvd: 48
```

Abfrage des Namens zu einer Adresse (Serveradresse aus resolv.conf)

```
# dig -x 217.115.66.11

; <<>> DiG 9.7.1 <<>> -x 217.115.66.11
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47949
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;11.66.115.217.in-addr.arpa.    IN      PTR

;; ANSWER SECTION:
11.66.115.217.in-addr.arpa. 202 IN      PTR     ts.fujitsu.com.

;; Query time: 7 msec
;; SERVER: 123.123.123.123#53(123.123.123.123)
;; WHEN: Wed Nov 24 15:56:31 2010
;; MSG SIZE  rcvd: 72
```

Abfrage der Name Server einer DNS-Domaine (Serveradresse aus resolv.conf)

```
# dig ts.fujitsu.com ns

; <<>> DiG 9.7.1 <<>> ts.fujitsu.com ns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46920
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 5

;; QUESTION SECTION:
;ts.fujitsu.com.                        IN      NS

;; ANSWER SECTION:
ts.fujitsu.com.         86400   IN      NS      ns2.klute-thiemann.de.
ts.fujitsu.com.         86400   IN      NS      ns3.klute-thiemann.de.
ts.fujitsu.com.         86400   IN      NS      ns4.klute-thiemann.de.
ts.fujitsu.com.         86400   IN      NS      ns1.ts.fujitsu.com.
ts.fujitsu.com.         86400   IN      NS      ns1.klute-thiemann.de.

;; ADDITIONAL SECTION:
ns2.klute-thiemann.de.  77674   IN      A       82.139.223.161
ns3.klute-thiemann.de.  78837   IN      A       81.92.4.138
ns4.klute-thiemann.de.  78837   IN      A       217.160.130.182
ns1.ts.fujitsu.com.     86400   IN      A       80.70.172.154
ns1.klute-thiemann.de.  77674   IN      A       217.194.235.1

;; Query time: 10 msec
;; SERVER: 123.123.123.123#53(123.123.123.123)
;; WHEN: Wed Nov 24 15:57:20 2010
;; MSG SIZE  rcvd: 219
```

Abfrage aller Einträge zu einem Namen (Serveradresse aus resolv.conf)

```
# dig ts.fujitsu.com any

; <<>> DiG 9.7.1 <<>> ts.fujitsu.com any
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49007
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 11, AUTHORITY: 0, ADDITIONAL: 6

;; QUESTION SECTION:
;ts.fujitsu.com.                        IN      ANY

;; ANSWER SECTION:
ts.fujitsu.com.         86400   IN      A       217.115.66.11
ts.fujitsu.com.         86400   IN      NS      ns3.klute-thiemann.de.
ts.fujitsu.com.         86400   IN      NS      ns4.klute-thiemann.de.
ts.fujitsu.com.         86400   IN      NS      ns1.ts.fujitsu.com.
ts.fujitsu.com.         86400   IN      NS      ns1.klute-thiemann.de.
ts.fujitsu.com.         86400   IN      NS      ns2.klute-thiemann.de.
ts.fujitsu.com.         900     IN      SOA     ns1.ts.fujitsu.com.
dns.ts.fujitsu.com. 2373 86400 3600 777600 86400
ts.fujitsu.com.         86400   IN      MX      50 dgate30.ts.fujitsu.com.
ts.fujitsu.com.         86400   IN      MX      10 dgate10.ts.fujitsu.com.
ts.fujitsu.com.         86400   IN      MX      10 dgate20.ts.fujitsu.com.
ts.fujitsu.com.         86400   IN      TXT     "v=spf1 +mx
include:spf.ts.fujitsu.com include:spf2.ts.fujitsu.com
include:spf3.ts.fujitsu.com include:_spf.muc.ec-messenger.com ~all"

;; ADDITIONAL SECTION:
ns3.klute-thiemann.de.  78792   IN      A       81.92.4.138
ns4.klute-thiemann.de.  78792   IN      A       217.160.130.182
ns1.ts.fujitsu.com.     86400   IN      A       80.70.172.154
ns1.klute-thiemann.de.  77629   IN      A       217.194.235.1
ns2.klute-thiemann.de.  77629   IN      A       82.139.223.161
dgate30.ts.fujitsu.com. 86400   IN      A       195.127.188.205

;; Query time: 10 msec
;; SERVER: 123.123.123.123#53(123.123.123.123)
;; WHEN: Wed Nov 24 15:58:04 2010
;; MSG SIZE  rcvd: 508
```

Beispiel für einen Zonentransfer (mit Angabe einer expliziten Serveradresse)

```
# dig @123.123.123.123 mydom.de axfr

; <<>> DiG 9.7.1 <<>> @123.123.129.15 dom1.sq axfr
; (1 server found)
;; global options: +cmd
mydom.de.               604800  IN      SOA    mydom-ns.mydom.de.
root.mydom.de. 42 172800 1
4400 3628800 604800
mydom.de.               604800  IN      MX 0   mx-host0.mydom.de.
mydom.de.               604800  IN      MX 1   mx-host1.mydom.de.
mydom.de.               604800  IN      MX 2   mx-host2.mydom.de.
mydom.de.               604800  IN      NS     mydom-ns.mydom.de.
mydom-ns.mydom.de.      604800  IN      A      123.123.123.101
mydom1.mydom.de.        604800  IN      NS     mydom1-ns.mydom1.mydom.de.
mydom1-ns.mydom1.mydom.de. 604800 IN    A      123.123.123.102
mydom2.mydom.de.        604800  IN      NS     mydom2-ns.mydom2.mydom.de.
mydom2-ns.mydom2.mydom.de. 604800 IN    A      123.123.123.103
myhost.mydom.de.        604800  IN      A      123.123.123.201
myhost.mydom.de.        604800  IN      A      123.123.123.202
myhost.mydom.de.        604800  IN      A      123.123.226.203
myhost.mydom.de.        604800  IN      AAAA
3ffe:1:1000:2000:abc:abcd:abcd:abc1
myhost.mydom.de.        604800  IN      AAAA
3ffe:1:1000:2000:abc:abcd:abcd:abc2
myhost.mydom.de.        604800  IN      AAAA
3ffe:1:1001:3000:bcd:bcde:bcde:bcd2
myhost-alias.mydom.de.  604800  IN      CNAME  myhost.mydom.de.
myhost1.mydom.de.       604800  IN      A      123.123.123.201
myhost1-aaaa.mydom.de.  604800  IN      AAAA
3ffe:1:1000:2000:abc:abcd:abcd:abc1
...
...
3628800 604800
;; Query time: 9 msec
;; SERVER: 123.123.129.15#53(123.123.129.15)
;; WHEN: Wed Nov 24 15:59:31 2010
;; XFR size: 69 records (messages 1, bytes 2056)
```

8 NTP

Das **N**etwork **T**ime **P**rotocol Version 4 ist in den RFCs 5905-5908 dokumentiert.

8.1 Konzept von NTP

Das Network Time Protocol basiert auf dem Client-/Server-Konzept. Mithilfe hochentwickelter Verfahren liefert NTP den Systemen im LAN- und/oder WAN die Uhrzeit mit einer Genauigkeit im Millisekundenbereich.

8.1.1 Funktionalität von NTP

NTP bietet folgende Funktionalität:

- Verteilung einer Referenz-Uhrzeit (Universal Time Coordinated, UTC) innerhalb eines Netzwerks
- Koordination der Uhren innerhalb beliebig großer Netzwerke

Für die Einspeisung der UTC-Zeit ins Netzwerk sollte der Netzwerk-Rechner, auf dem NTP installiert ist, mit einer funkgesteuerten Hardware-Uhr ausgestattet sein, die ein von einer Atomuhr generiertes Zeitsignal empfängt. Die Physikalisch-Technische Bundesanstalt Braunschweig stellt mit ihrem DCF77-Zeitsignal die für unsere geografischen Verhältnisse maßgebende Zeitquelle zur Verfügung.

Ein entsprechend ausgerüsteter Netzwerk-Rechner synchronisiert seine eigene Systemuhr mit der externen Hardware-Uhr und wird so zum primären Time Server in diesem Netzwerk. Die Genauigkeit eines solchen Time Servers wird von der Auflösung der eigenen Systemuhr bestimmt.

Time Server stehen in hierarchischer Beziehung zueinander. Ein sekundärer Time Server erhält seine Zeit über das Netzwerk von einem primären Time Server. Die Stellung eines Time Servers in dieser Hierarchie wird durch eine Zahl, das sog. Stratum, gekennzeichnet. Ein primärer Time Server hat ein Stratum von 1, ein sekundärer Time Server hat ein Stratum von 2 usw. Je höher das Stratum, desto weiter ist der Time Server von der primären Zeitquelle entfernt und desto höher ist die Wahrscheinlichkeit, dass es sich um einen ungenauen Time Server handelt.

Vereinfacht betrachtet, läuft die Zeitsynchronisation zwischen Client und Server wie folgt ab:

1. Der Client schickt eine NTP-Message als Datagramm an den Server.
2. Der Server nimmt das eintreffende Datagramm entgegen und tauscht die IP-Adressen und einige Felder in der Message aus.
3. Der Server schickt das modifizierte Datagramm wieder zurück an den Client.

Resultat dieses Prozesses sind vier Zeitstempel, aus denen sich die beiden folgenden Größen bestimmen lassen:

- Zeitspanne, die die NTP-Message im Netz unterwegs war (Delay)
- Zeitspanne, um welche die Uhren der Rechner differieren (Offset)

Beide Größen werden näherungsweise bestimmt. Das Offset resultiert aus einer Mittelung des Delay, d.h. NTP geht davon aus, dass Hin- und Rückweg der NTP-Pakete gleich lang sind. Abweichungen von dieser Annahme gehen als Fehler in die Berechnung des Offsets ein. Bei LANs macht das Round-Trip Delay nur einen Bruchteil des Offsets aus, weshalb sich das Offset bei LANs sehr genau bestimmen lässt. Im WAN-Bereich trifft dies jedoch nicht zu.

Um den verfälschenden Einfluss von Laufzeitschwankungen zu minimieren, werden die ermittelten Offset- und Delay-Werte zusätzlich gefiltert. Aus den letzten acht empfangenen NTP-Messages eines Time Servers bestimmt die Message mit dem geringsten Delay den aktuellen Offset-Wert. Zusätzlich wird aus denselben Messages eine weitere Größe berechnet, die Dispersion. Bei der Dispersion handelt es sich um den gewichteten Mittelwert der Offset-Abweichungen vom aktuellen Offset-Wert bei den letzten acht NTP-Messages. Dabei haben die Offset-Werte mit geringem Delay-Wert ein größeres Gewicht als Offset-Werte mit großem Delay-Wert. Die Dispersion eines Time Servers ist der Maßstab zur Bewertung der Güte dieses Time Servers.

Eine Client-/Server-Konfiguration steht und fällt mit der Verfügbarkeit ihrer Komponenten. Bei NTP werden im Wesentlichen zwei Techniken angewandt, um Störungen zu vermeiden:

- Redundanz:

  Jeder Time Server bzw. jeder Client sollte mit mindestens drei weiteren Time Servern in Verbindung stehen, die ein höheres oder zumindest gleiches Stratum haben. Fällt für einen Rechner seine aktuelle Synchronisationsquelle aus, so übernimmt diese Rolle automatisch ein anderer Time Server.

- Selektion:

  Es wird ein Selektionsmechanismus angewendet, der aus der Liste der zur Verfügung stehenden Time Server den besten als aktuelle Synchronisationsquelle auswählt.

  Auswahlkriterien sind:

  – Stratum (je kleiner, desto besser)
  – Delay (je kleiner, desto besser)
  – Dispersion (je kleiner, desto besser)

Die Unterscheidung zwischen (Time) Server und Client resultiert aus der Frage, wer von wem die korrekte Zeit bekommt. Der Client fordert vom Server eine NTP-Message mit den schon beschriebenen Zeitstempeln an und synchronisiert danach seine eigene Uhr, falls der Server sich als der beste verfügbare erweist. Im NTP-Protokoll wird von Assoziationen zwischen Time Servern gesprochen, die sich mit den fünf verschiedenen Betriebszuständen beschreiben lassen, in denen ein Time Server operiert.

Assoziation	**Host1**	**Host2**
Peer to Peer	symmetrisch aktiv	symmetrisch passiv
Client to Server	Client	Server
	Server	Client
Broadcast	Client	Broadcast Server
	Broadcast Server	Client

Symmetrische Assoziationen (Peer to Peer) zwischen Time Servern nutzen den gesamten Funktionsumfang des NTP-Protokolls. Insbesondere erhält ein Peer-Host Status-Informationen über den Gegenüber-Peer und ist ggf. bereit, ihn als Synchronisationsquelle heranzuziehen. Bei der Client-/Server-Assoziation hingegen sind die Rollen fest verteilt. Der Server liefert dem Client zwar die genaue Zeit, ist aber in keinem Fall bereit, sich mit ihm zu synchronisieren. Symmetrische Assoziationen sind üblich zwischen Time Servern mit kleinen Stratum-Werten, während Client-/Server-Assoziationen eher zwischen Time Servern mit hohen Stratum-Werten vorkommen. Broadcast-Assoziationen sind in LANs anwendbar, in denen ein Server mehrere Clients mit NTP-Messages im Broadcast-Verfahren bedient.

Nicht jeder Client, der den Time Service benötigt, sollte sich mit dem/den Stratum-1-Server(n) direkt synchronisieren. Der Server wäre bald überlastet und könnte keine exakte Zeit mehr liefern. Sinnvoller ist es, die Zeit über eine Anzahl von ausgewählten Stratum-2-Servern zu verteilen.

8.1.2 Implementierung von NTP im BS2000

BS2000 kann die NTP-Funktionalität sowohl als Client als auch als Server nutzen.

Die als POSIX-Schnittstelle sowie als privilegierte TPR-Schnittstelle angebotene Funktion *adjtime* verändert im BS2000 die Systemzeit um einen bestimmten Wert.

Die Systemzeit steht dem Anwender über folgende Schnittstellen zur Verfügung:

- GTIME (sowohl in TU als auch in TPR)
- GDATE
- Laufzeitroutinen von Hochsprachen

Das Time-of-Day-Register (TODR) wird im Rahmen einer solchen Synchronisation nicht angepasst.

Die eigentliche Anpassung der Systemzeit erfolgt in kleinen Schritten asynchron zum *adjtime*-Aufruf. Hierzu wird die Systemuhr für eine gewisse Zeit scheinbar beschleunigt oder verzögert, je nachdem, ob der Korrekturwert positiv oder negativ ist. Dabei ist garantiert, dass zwei aufeinander folgende Aufrufe zur Abfrage der aktuellen Zeit monoton aufsteigende Zeitwerte und keine Zeitsprünge liefern.

Der Vorgang zur Anpassung der Systemzeit um einen absoluten Wert von *n* Sekunden dauert 4**n* Sekunden. Die Synchronisation durch NTP erfolgt im BS2000 frühestens nach 64 Sekunden mit dem aktuellen Offset-Wert.

Der Zeitpunkt des *adjtime*-Aufrufs wird durch folgende Faktoren bestimmt:

- Aktuelle Abweichung der am eigenen System angezeigten Zeit gegenüber der maßgeblichen NTP-Server-Zeit. Bei geringer Abweichung wird das Polling-Intervall erhöht und somit die Synchronisationsfrequenz herabgesetzt.
- Eingestellter *minpoll*-Wert, der das minimale Polling-Intervall spezifiziert. Hierbei ist der Speicherbedarf des *adjtime*-Aufrufs zu beachten.
- Pro *adjtime*-Aufruf werden 8 KB CLASS4-Speicher sowie 8 KB CLASS3-Speicher benötigt. Die betreffenden Speicherbereiche werden jeweils 15 Minuten belegt.

  Damit ergibt sich folgender Bedarf an CLASS4-Speicher:

  Bedarf = (900 / *sync_intervall*) * 8 KB

  Dabei spezifiziert *sync_intervall* den Abstand (in Sekunden) zwischen zwei von NTP angestoßenen Synchronisationsvorgängen.

Ein *adjtime*-Aufruf löst einen vorhergehenden *adjtime*-Aufruf in seiner Bearbeitung ab. Die Funktionalität von *adjtime* kann im BS2000 von mehreren privilegierten Nutzern beansprucht werden. Eine interne Vorrangbeziehung legt fest, wessen Aufträge zur Synchronisation ausgeführt werden und welche nicht. Der Vorrang gilt vom Zeitpunkt der Anmeldung einer höherprioren Instanz bis zu deren Abmeldung.

Der NTP-Server meldet sich mit seinem ersten *adjtime*-Aufruf an und wird implizit durch die Beendigung seiner Ablauftask abgemeldet.

Details der Vorrangregeln finden Sie im Handbuch "BS2000 OSD-BC - Einführung in die Systembetreuung", Kapitel "Systemzeit-Verwaltung"

Der höchstpriore Time Server wird von BS2000 bevorzugt, alle anderen Time Server kommen dann nicht zum Zug. Da dies von BS2000 nicht überprüft wird, muss der Systemverwalter eine organisatorische Regelung treffen.

Standardmäßig wird in die Dateien */var/adm/ntp.log* und */var/adm/syslog* protokolliert.

Während einer Sommer-/Winterzeit-Umstellung kann NTP im Einsatz bleiben.

NTP-Programme

Die folgende Tabelle gibt einen Überblick über die Programme für den Start des NTP-Dämons und zur Steuerung der NTP-Funktionalität.

Programm	Funktion	Seite
ntpd	NTP-Dämon	267
ntpq	NTP-Status abfragen	286
ntpdate	Setzen von Datum und Uhrzeit	284
ntptrace	NTP-Server erfragen	296
ntpdc	NTP-Status abfragen (speziell)	
sntp	Client für vereinfachtes (SNTP) Protokoll	
ntp-keygen	Generierung öffentlicher und privater Schlüssel	285

8.2 Installation und Deinstallation von NTP

Beachten Sie bitte zusätzlich zu diesem Kapitel die mit dem Produkt ausgelieferte Freigabemitteilung.

8.2.1 Installation

Die einzelnen Komponenten des Software-Pakets interNet Services werden als ein POSIX-Programmpaket per Package-Installation mit dem POSIX-Installationsprogramm installiert (siehe Handbuch „POSIX Grundlagen für Anwender und Systemverwalter“).
Nähere Informationen zur Installation der Komponenten finden Sie auch im Abschnitt „Installation“ auf Seite 37.

Zur Installation und zum Betrieb der TCP-IP-SV-Komponente NTP muss die PLAM-Bibliothek SINLIB.TCP-IP-SV.*nnn*.NTP shareable zur Verfügung stehen.

- Installieren Sie NTP unter der TSOS-Kennung mit dem POSIX-Installationskommando, da auch privilegierte Aktionen durchgeführt werden müssen:

  ```
  /START-POSIX-INSTALLATION
  ```

- Wählen Sie dabei für die Installation Folgendes aus / geben Sie Folgendes an:

Funktion[1]:	Install packages on POSIX
IMON support ?	Y
name of product	TCP-IP-SV
package of product	NTP

  …

  [1] *version of product* wird durch die höchste Version in IMON bestimmt.

- Den Installationspfad, der im weiteren Verlauf angezeigt wird, können Sie ändern. Es empfiehlt sich aber, die Voreinstellung */opt/TCP-IP-SV/ntp* beizubehalten, da alle Pfadangaben in diesem Dokument auf dieser Standard-Einstellung beruhen.

  Anschließend prüft das POSIX-Installationsprogramm das /opt-Dateisystem auf ausreichenden Speicherplatz und fragt nach, ob der NTP-Dämon später automatisch bei jedem POSIX-Start mitgestartet werden soll.

- Wenn Sie die Voreinstellung "no" in "yes" ändern, können Sie diese Entscheidung später durch Editieren der Datei */etc/default/TCP-IP-SV.ntp* (Variable AUTOSTART) rückgängig machen.

  Nach Beantworten der Frage werden die Dateien aus der PLAM-Bibliothek ins POSIX-Dateisystem eingespielt.

Nach erfolgreicher Installation werden die weiteren erforderlichen Aktivitäten unter der POSIX-Shell in einer Kennung mit POSIX-Root-Berechtigung ausgeführt. Dazu wird mit dem BS2000-Kommando START-POSIX-SHELL die POSIX-Shell gestartet. Die relevanten Kommandos und Dateien befinden sich in den Verzeichnissen */etc* und */var* sowie dem Installationsverzeichnis */opt/TCP-IP-SV/ntp*. In der nachfolgenden Tabelle steht *<instdir>* für das Installationsverzeichnis */opt/TCP-IP-SV/ntp*.

Verzeichnis	**Datei**	**Beschreibung**
<instdir>/etc/rc.d	ntpd	Start/-Stopp-Skript
<instdir>/readme	<diverse>	Original-NTP-Dokumentation in verschiedenen Dateiformaten
<instdir>/sbin	ntpd	NTP-Dämon
	ntpdate	NTP-Programm
	ntpdc	NTP-Programm
	ntp-keygen	NTP-Programm
	ntp-wait	Skript für die Synchronisierung mit *ntpd*
	ntptrace	Skript zur Anzeige der NTP-Server-Kette
	ntpq	NTP-Programm
	sntp	NTP-Programm
	start-ntp-daemon	Hilfsprogramm für ntpd-Start, nicht direkt aufrufbar
/etc	ntp.conf	NTP-Konfigurationsdatei
	ntp.conf.default	Default-NTP-Konfigurationsdatei
	ntp.drift	Drift-Datei
/etc/default	TCP-IP-SV.ntp	Parameterdatei für Start-/Stopp-Skript
	TCP-IP-SV.ntp. default	Default-Parameterdatei für Start-/Stopp-Skript
/etc/init.d	TCP-IP-SV.ntp	Start-/Stopp-Skript für ntpd
/etc/rc0.d	K17TCP-IP-SV.ntp	Symbolischer Link auf Start-/Stopp-Skript
/etc/rc2.d	S97TCP-IP-SV.ntp	Symbolischer Link auf Start-/Stopp-Skript
/var/run	ntp.pid	Datei mit Pid des ntpd
/var/adm	ntpd_startup.log	Startmeldungen des ntpd
	ntp.log	Logfile des ntpd

Nach Installation des interNet Services NTP müssen Sie vor dem dem Starten des NTP-Dämons die NTP-Konfigurationsdatei an die individuellen Erfordernisse anpassen (siehe Seite 269). Dies ist jedoch nur nötig, wenn keine Sicherung der NTP-Konfigurationsdatei aus einer vorherigen Installation restauriert werden konnte.

Wenn das Subsystem POSIX beendet und wieder neu gestartet wird, werden automatisch auch die nach der Installation aktivierten Dämonen von interNet Services gestartet.

8.2.2 Deinstallation

Analog zur Installation der Komponenten von interNet Services wird auch die Deinstallation mithilfe des POSIX-Installationsprogrammes unter der Kennung TSOS durchgeführt. Bei der Deinstallation wird nach dem aktiven NTP-Dämon gesucht und dieser beendet. In der Syslog-Datei */var/adm/syslog* wird die Beendigung noch aktiver Dämonen protokolliert. Anschließend werden alle Dateien, Links und Prozeduren des NTP gelöscht.

Im Rahmen der Deinstallation werden die Konfigurationsdatei */etc/ntp.conf* und die Parameterdatei */etc/default/TCP-IP-SV.ntp* für das Start-Stopp-Skript im Verzeichnis */etc/tcpipsv/ntp* gesichert. Die Sicherungskopien werden im Fall einer erneuten Installation wieder in das aktive Verzeichnis */etc* bzw. */etc/default* kopiert. Achten Sie in diesem Zusammenhang bitte darauf, dass die Sicherungskopie dem aktuellen Stand entspricht.

8.3 Inbetriebnahme und Außerbetriebnahme von NTP

Dieser Abschnitt liefert Informationen zu folgenden Themen:

- NTP starten und beenden
- Zeitabgleich von NTP (Datum und Uhrzeit setzen)
- Konfigurationsdatei des NTP-Dämons erstellen

8.3.1 NTP starten und beenden

Wenn Sie NTP manuell starten oder beenden wollen, verwenden Sie unter SYSROOT oder TSOS folgende Skript-Aufrufe

```
/etc/init.d/TCP-IP-SV.ntp start
```

bzw.

```
/etc/init.d/TCP-IP-SV.ntp stop
```

Ein Start ist auf diese Weise nur möglich, wenn in */etc/default/TCP-IP-SV.ntp* die Variable AUTOSTART auf 'yes' gesetzt ist. Wenn Sie umgekehrt den NTP über eine Beendigung des Subsystems POSIX hinaus außer Betrieb nehmen wollen, setzen Sie die Variable AUTOSTART auf 'no' bzw. 'never'.

Wenn der Dämon unabhängig von AUTOSTART in jedem Fall gestartet werden soll, dann muss die Option *mstart* anstatt *start* verwendet werden.

Mit der Option *dstart* kann man den Dämon zu Debug-Zwecken im Vordergrund laufen lassen, ggf. müssen die Debug-Optionen im Skript *TCP-IP-SV.ntp* angepasst werden.

Um einen laufenden NTP-Dämon zu stoppen und erneut zu starten, verwenden Sie folgenden Skript-Aufruf:

```
/etc/init.d/TCP-IP-SV.ntp restart
```

8.3.2 Zeitabgleich von NTP

Der NTP-Zeitabgleich kann im BS2000 entweder kontinuierlich über den NTP-Dämon *ntpd* oder einmalig über das Programm *ntpdate* genutzt werden. (Langfristig soll das Programm *ntpdate* durch den Aufruf von *ntpd* mit der Option *-q* abgelöst werden. Es empfiehlt sich daher, *ntpd* zu verwenden.) Wie Sie Datum und Uhrzeit mit dem Programm *ntpdate* setzen, ist beschrieben im Abschnitt „Datum und Uhrzeit über NTP setzen mit dem Programm ntpdate“ auf Seite 284.

ntpd und *ntpdate* benutzen beide Port# 123. Es kann daher nur eine der beiden Anwendungen ablaufen.

Adressierung von Zeitgebern

In BS2000-POSIX kann nur die Systemuhr des lokalen Rechners als Referenz-Uhr konfiguriert werden. Allerdings sollte man nach Möglichkeit nicht die Systemuhr als Zeitgeber verwenden, selbst wenn sie über den SKP oder das Trägersystem mit externen Zeitgebern synchronisiert wird. Dies liegt u.a. daran, dass hierbei nur eine Synchronisierung mit Sekundenauflösung stattfindet. Stattdessen sollte man nach Möglichkeit per NTP die gleichen externen Zeitgeber bzw. Partnerrechner verwenden, wie sie von SKP bzw. vom Trägersystem verwendet werden.

Wenn das BS2000 an einem XCS-Verbund teilnimmt (siehe Handbuch "HIPLEX MSCF"), sollte man die Systemuhr dennoch als zusätzlichen Zeitgeber mit der *server*-Konfigurationsanweisung konfigurieren. Die Systemuhr bekommt dabei standardmäßig das stratum 5 zugewiesen, das mit der *fudge*-Anweisung noch erhöht werden kann. Wenn nun z.B. die konfigurierten NTP-Server nicht mehr erreichbar sind, dann würde ohne die Konfiguration der Systemuhr der lokale NTP-Server auf dem zuletzt erreichten stratum-Wert verharren. Mit einer als Zeitgeber auf stratum 5 konfigurierten Systemuhr fällt der lokale NTP-Server auf stratum 6, was dazu führt, dass andere Zeitsynchronisationsmechanismen zum Einsatz kommen können (insbesondere die des XCS-Verbunds).

Weitere Informationen finden Sie im Kapitel "Systemzeit-Verwaltung" im Handbuch "BS2000 OSD/BC - Einführung in die Systembetreuung".

Zeitgeber werden analog zu Partnerrechnern adressiert. Hierfür werden Pseudo-IP-Adressen verwendet, die als normale IP-Adressen ungültig sind. Zeitgeber werden über die im nachfolgenden Abschnitt beschriebenen Konfigurationsanweisungen *server* und *fudge* konfiguriert.

8.3.3 Konfigurationsdatei für den NTP-Dämon ntpd erstellen

Der Standardname für die Konfigurationsdatei des NTP-Dämons *ntpd* lautet */etc/ntp.conf*. Das Format der Konfigurationsdatei ähnelt dem Format anderer OSD/POSIX-Konfigurationsdateien. Kommentare werden durch das Zeichen „#“ eingeleitet und gelten bis zum Zeilenende. Leerzeilen werden ignoriert.

Konfigurationsanweisungen bestehen aus einem Schlüsselwort, gefolgt von einer Liste von Argumenten, die durch Zwischenraumzeichen voneinander getrennt sind. Zwischen Groß- und Kleinschreibung bei den Schlüsselwörtern der Kommandos wird nicht unterschieden. Eine Anweisung darf sich nicht über mehrere Zeilen erstrecken. Nachfolgend sind die wichtigsten Konfigurationsanweisungen beschrieben.

Eine vollständige Beschreibung finden Sie z.B. in den HTML-Dateien unter */opt/TCP-IP-SV/ntp/readme/TCP-IP-SV.ntp/html*.

Wenn *ntpd* als Broadcast-Client verwendet wird, sind keine Konfigurationsanweisungen erforderlich.

server-Anweisung

Die *server*-Anweisung setzt den lokalen *ntpd*-Dämon in den „Client“-Modus gegenüber dem angegebenen Server. In diesem Modus wird der lokale *ntpd* durch den fernen NTP-Server synchronisiert, aber nicht umgekehrt.

```
server host_addr [ autokey | key][ version #][ prefer][ minpoll minpoll][
maxpoll maxpoll]
```

---

host_addr
: Rechneradresse in Punktschreibweise, die den Server spezifiziert, gegenüber dem der lokale *ntpd*-Dämon in den Client-Modus gesetzt wird.

  Zeitgeber werden analog zu Partnerrechnern adressiert. Hierfür werden Pseudo-IP-Adressen der Form `127.127.`*t*`.`*u* verwendet, die als normale IP-Adressen ungültig sind. Dabei bezeichnet *t* den Typ des Zeitgebers, *u* ist typspezifisch. Die lokale Systemuhr wird mit der Pseudo-IP-Adresse `127.127.1.0` angegeben und ist im BS2000 der einzig mögliche Zeitgeber.

autokey
: NTP-Pakete werden gemäß dem Autokey-Schema authentifiziert gesendet und empfangen. Diese Option schließt sich mit der *key*-Option gegenseitig aus.

key
NTP-Pakete werden mit einem auf symmetrischen Schlüsseln basierendem Schema authentifiziert gesendet und empfangen. *key* gibt den Schlüssel-Identifier an, wobei der Wertebereich von 1 bis 65534 geht. Diese Option schließt sich mit der *autokey*-Option gegenseitig aus.

version *#*
Versionsnummer für abgehende NTP-Pakete. Mögliche Werte für # sind 1 bis 4.
Default: `version 4`

prefer
Der durch *host_addr* spezifizierte Rechner wird als „bevorzugt" markiert und somit unter ansonsten gleichwertigen Kandidaten für die Synchronisierung ausgewählt.

minpoll
ganze Zahl, die das minimale Polling-Intervall für NTP-Nachrichten als $2^{minpoll}$ Sekunden spezifiziert.
Default: 6 (64 sec)
Im BS2000 zulässig: ≥ 6 (64 sec)

maxpoll
ganze Zahl, die das maximale Polling-Intervall für NTP-Nachrichten als $2^{maxpoll}$ Sekunden spezifiziert.
Default: 10 (1024 sec)
Im BS2000 zulässig: bis 14 (ca. 4h 30min)

Beispiel (Client-Betrieb)

```
# ntp.conf
#
#
server 127.127.1.0              #own clock
server 172.24.4.121 prefer      #time server
server 172.25.113.36            #unix machine
server 172.25.109.118           #linux pc
```

restrict-Anweisung

Die *restrict*-Anweisung regelt die Zugangskontrolle.

```
restrict address [mask numeric_mask] [flag]
```

---

address
: Wird *address* in „decimal-dotted“ Schreibweise angegeben, dann spezifiziert die IP-Adresse eines Netzwerks, eines Subnetzwerks oder eines einzelnen Hosts. Falls die *mask*-Klausel nicht angegeben ist, spezifiziert *address* die IP-Adresse eines einzelnen Host. Alternativ kann *address* einen gültigen DNS-Namen eines Hosts spezifizieren.

numeric_mask
: *numeric_mask* ist in „decimal-dotted“ Schreibweise anzugeben und spezifiziert eine Subnetz-Maske.
Default: 255.255.255.255

flag
: Die Spezifikation von *flag* bedeutet stets eine Einschränkung der Zugriffsberechtigung. Eine *restrict*-Anweisung ohne *flag*-Angabe zeigt somit uneingeschränkte Zugriffsberechtigung an.

  Für *flag* können folgende Werte angegeben werden (eine vollständige Auflistung finden Sie z.B. in der mitgelieferten HTML-Dokumentation):

  ignore
  : Pakete, die von den durch die *restrict*-Anweisung spezifizierten Hosts kommen, werden ignoriert. Es werden weder *ntpq*/*ntpdc*-Queries noch Time Server-Polls beantwortet.

  noserve
  : Alle NTP-Pakete mit einem Modus ungleich 6 oder 7 werden ignoriert. Time Service wird verweigert, *ntpq*/*ntpdc*-Queries sind jedoch zulässig.

  notrust
  : Der lokale *ntpd*-Dämon führt keine Synchronisation auf Grund von NTP-Paketen durch, die von den durch die *restrict*-Anweisung spezifizierten Rechnern stammen.

Beispiel

```
# ntp.conf
#
#
server   127.127.1.0               #own clock
server   172.24.4.121 prefer       #time server
server   172.25.24.12              #VM2
server   172.25.109.118            #linux pc
#
# access control:
# by default, ignore all packets
#
restrict default ignore
#
# don't trust servers on local net
#
restrict 172.25.0.0 mask 255.255.0.0 notrust
#
# the above defined servers are unrestricted
#
restrict 127.127.1.0               #own clock
restrict 172.24.4.121              #time server
restrict 172.25.24.12              #VM2
restrict 172.25.109.118            #linux pc
```

fudge-Anweisung

Zeitgeber können über die *server*-Anweisung (siehe Seite 269) konfiguriert werden. Eine weitergehende Anweisung für die Konfiguration eines Zeitgebers ist die *fudge*-Anweisung. Die *fudge*-Anweisung muss unmittelbar auf die *server*-Anweisung folgen, die den Zeitgeber adressiert.

```
fudge 127.127.t.u[ stratum stratum]
```

---

t
bezeichnet den Typ des Zeitgebers.

u
ist typspezifisch. Die lokale Systemuhr wird mit der Pseudo-IP-Adresse `127.127.1.0` angegeben und ist im BS2000 der einzig mögliche Zeitgeber.

stratum
Ganze Zahl, die angibt, über wie viele Stationen der lokale *ntpd-Dämon* einen Zeitstempel höchster Genauigkeit von einem externen Zeitgeber erfragen kann. *stratum* kann für die Konfiguration der lokalen Systemuhr von Bedeutung sein. Server mit dem Stratum 1 haben direkten Zugang zu externen Zeitsignalen. Server, die ihre Zeitstempel von Stratum-1-Servern erhalten, sind Stratum-2-Server usw.

Der Wert von *stratum* ist das Hauptkriterium, nach dem *ntpd* als Client einen Server unter mehreren möglichen Servern auswählt. Auch die lokale Systemuhr ist aus der Sicht von *ntpd* ein „Server“. Der Standardwert für das Stratum der Systemuhr ist 5. Durch Angabe eines niedrigeren oder höheren Wertes für das Systemuhr-Stratum in der *fudge*-Anweisung kann die Systemuhr gegenüber anderen Servern bevorzugt bzw. zurückgestellt werden.

Beispiel (Server-Betrieb mit eigener Uhr als Zeitgeber)

```
# ntp.conf
#
#
server 127.127.1.0           #own clock
fudge  127.127.1.0 stratum 1
```

peer-Anweisung

Die *peer*-Anweisung versetzt den lokalen *ntpd* gegenüber dem fernen Server in den Betriebsmodus „symmetrisch aktiv“. In diesem Modus kann

- der lokale Server durch den fernen Server synchronisiert werden und
- der ferne Server kann durch den lokalen synchronisiert werden.

Diese Einstellung ist sinnvoll in einem Netz von Servern, in dem z.B. je nach Auslastung entweder der lokale oder der ferne Server über die bessere Zeitquelle verfügt.

```
peer host_addr [ autokey | key][ version #][ prefer][ minpoll minpoll]
     [ maxpoll maxpoll]
```

---

host_addr
: Rechneradresse in Punktschreibweise, die den Server spezifiziert, gegenüber dem der lokale *ntpd*-Dämon in den Modus „symmetrisch aktiv“ wechselt. Alternativ kann auch der DNS-Name des Hosts verwendet werden.

autokey
: NTP-Pakete werden gemäß dem Autokey-Schema authentifiziert gesendet und empfangen. Diese Option schließt sich mit der *key*-Option gegenseitig aus.

key
: NTP-Pakete werden mit einem auf symmetrischen Schlüsseln basierendem Schema authentifiziert gesendet und empfangen. *key* gibt den Schlüssel-Identifier an, wobei der Wertebereich von 1 bis 65534 geht. Diese Option schließt sich mit der *autokey*-Option gegenseitig aus.

version *#*
: Versionsnummer für abgehende NTP-Pakete. Mögliche Werte für *#* sind 1 bis 4.
Default: `version 4`

prefer
: Der durch *host_addr* spezifizierte Rechner wird als „bevorzugt" markiert und somit unter ansonsten gleichwertigen Kandidaten für die Synchronisierung ausgewählt.

minpoll
: ganze Zahl, die das minimale Polling-Intervall für NTP-Nachrichten als $2^{minpoll}$ Sekunden spezifiziert.
Default: 6 (64 sec)
Im BS2000 zulässig: ≥ 6 (64 sec)

maxpoll

ganze Zahl, die das maximale Polling-Intervall für NTP-Nachrichten als $2^{maxpoll}$ Sekunden spezifiziert.
Default: 10 (1024 sec)
Im BS2000 zulässig: bis 14 (ca. 4h 30min)

broadcast-Anweisung

Die *broadcast*-Anweisung setzt den lokalen Server *ntpd* in den „Broadcast“-Modus. Im „Broadcast“-Modus sendet der lokale Server periodisch Broadcast-Nachrichten an Clients mit einer bestimmten Adresse.

```
broadcast host_addr [ autokey | key] [ version #][ minpoll minpoll]
          [ maxpoll maxpoll]
```

---

host_addr
: Rechneradresse in Punktschreibweise, die die Clients spezifiziert, an die der lokale *ntpd*-Dämon periodisch Broadcast-Nachrichten sendet. Die Rechneradresse kann dabei die IP-Broadcast-Adresse eines lokalen Interfaces oder eine Multicast-Adresse sein. Wenn die Rechneradresse eine Multicast-Adresse ist, werden die Nachrichten an alle lokalen Interfaces geschickt. Die IANA hat die Multicast-Gruppen-Adresse IPv4 224.0.1.1 und IPv6 ff05::101 (site local) exklusiv an NTP zugewiesen. Sie können aber auch andere konfliktfreie Adressen verwenden.

autokey
: NTP-Pakete werden gemäß dem Autokey-Schema authentifiziert gesendet und empfangen. Diese Option schließt sich mit der *key*-Option gegenseitig aus.

key
: NTP-Pakete werden mit einem auf symmetrischen Schlüsseln basierendem Schema authentifiziert gesendet und empfangen. *key* gibt den Schlüssel-Identifier an, wobei der Wertebereich von 1 bis 65534 geht. Diese Option schließt sich mit der *autokey*-Option gegenseitig aus.

version *#*
: Versionsnummer für abgehende NTP-Pakete. Mögliche Werte für *#* sind 1 bis 4. Default: `version 4`

minpoll

ganze Zahl, die das minimale Polling-Intervall für NTP-Nachrichten als $2^{minpoll}$ Sekunden spezifiziert.
Default: 6 (64 sec)
Im BS2000 zulässig: ≥ 6 (64 sec)

maxpoll

ganze Zahl, die das maximale Polling-Intervall für NTP-Nachrichten als $2^{maxpoll}$ Sekunden spezifiziert.
Default: 10 (1024 sec)
Im BS2000 zulässig: bis 14 (ca. 4h 30min)

broadcastclient-Anweisung

Die *broadcastclient*-Anweisung veranlasst den lokalen *ntpd*-Dämon, die lokale Systemzeit anhand von eingehenden NTP-Broadcasts zu synchronisieren. Für die Berechnung der lokalen Systemzeit wird die Nachrichtenlaufzeit gegenüber dem Server benötigt. Um diese zu messen, wird bei Empfang der ersten Broadcast-Nachricht ein kurzer Datenaustausch mit dem Broadcast-Server initiiert, es sei denn, die *broadcastdelay*-Anweisung wurde verwendet, um eine Nachrichtenlaufzeit zu spezifizieren.

```
broadcastclient
```

---

broadcastdelay-Anweisung

Normalerweise gleicht der *ntpd*-Dämon Nachrichtenlaufzeiten zwischen einem Broadcast-Server und dem Client automatisch aus durch ein eigens dafür vorgesehenes Nachrichtenprotokoll. Mit der Anweisung *broadcastdelay* können Sie die Ausführung dieses Protokolls unterbinden und stattdessen explizit einen Wert vereinbaren.

```
broadcastdelay delaytime
```

---

delaytime
: spezifiziert den Wert (in Sekunden) für den Ausgleich der Nachrichtenlaufzeit zwischen Broadcast-Server und Client.
Für Ethernet sind Werte zwischen 0.003 und 0.007 Sekunden angemessen.

driftfile-Anweisung

Die *driftfile*-Anweisung spezifiziert die Datei, die Angaben zur Genauigkeitsabweichung des lokalen Oszillators enthält. Aus diesen Angaben kann der lokale Dämon *ntpd* einen Ausgleich zu lokalen Frequenzschwankungen errechnen.

```
driftfile filename
```

---

filename

spezifiziert die Datei, die Angaben zur Genauigkeitsabweichung des lokalen Oszillators enthält. Die Datei wird aktualisiert, indem der aktuelle Drift-Wert in eine temporäre Datei geschrieben wird, die dann umbenannt wird, um die alte Datei zu ersetzen. Daher benötigt der *ntpd* für das Verzeichnis, in dem die Datei liegt, Schreibberechtigung, und Sie sollten Dateilinks vermeiden.

Wenn die Datei *filename* nicht existiert oder die *driftfile*-Anweisung fehlt, wird zunächst eine Abweichung von 0 angenommen. Der lokale NTP-Dämon *ntpd* errechnet die Abweichung und speichert sie als Gleitpunktzahl in Vielfachen von 10^{-6} (parts-per-million, ppm). Bei einem Restart verwendet *ntpd* diesen abgespeicherten Wert.

controlkey-Anweisung

Die *controlkey*-Anweisung spezifiziert eine Schlüssel-Id für die Verwendung mit dem *ntpq*-Programm, welches das in RFC 1305 definierte Standardprotokoll verwendet.

```
controlkey key
```

---

key

ist eine Schlüssel-Id im Bereich von 1 bis 65534. Diesem Schlüssel muss per *trustedkey*-Anweisung vertraut werden.

requestkey-Anweisung

Die *requestkey*-Anweisung spezifiziert eine Schlüssel-Id für die Verwendung mit dem *ntpdc*-Programm, welches ein proprietäres Protokoll verwendet.

```
requestkey key
```

---

key
ist eine Schlüssel-Id im Bereich von 1 bis 65534. Diesem Schlüssel muss per *trustedkey*-Anweisung vertraut werden.

trustedkey-Anweisung

Die *trustedkey*-Anweisung spezifiziert die Schlüssel-Ids, denen für den Zweck der Authentifizierung von NTP-Peers per symmetrischer Kryptographie oder für die Verwendung durch *ntpq* und *ntpdc* vertraut werden soll. Die Authentifizierungsmechanismen erfordern, dass der lokale und die entfernten Server den gleichen Schlüssel und die gleiche Schlüssel-Id für diesen Zweck verwenden. Allerdings können verschiedene Schlüssel mit verschiedenen Servern verwendet werden.

```
trustedkey key [...]
```

---

key
ist eine Schlüssel-Id im Bereich von 1 bis 65534.

keys-Anweisung

Die *keys*-Anweisung spezifiziert den vollständigen Pfad der MD5-Schlüssel-Datei. Diese Datei enthält die Schlüssel und Schlüssel-Ids, die von *ntpd*, *ntpq* und *ntpdc* verwendet werden, wenn sie mit symmetrischen Schlüsseln arbeiten.

```
keys keyfile
```

---

keyfile
Vollständiger Pfadname der Schlüsseldatei.

keysdir-Anweisung

Die *keysdir*-Anweisung spezifiziert den Default-Pfadnamen für Autokey-Schlüssel, -Parameter und Zertifikate.

---

keysdir path

---

path

Pfadname des Verzeichnisses, in dem die Autokey-Dateien mit kryptographischen Schlüsseln, Parametern und Zertifikaten enthalten sind.

8.3.4 Startoptionen des NTP-Dämons ntpd

ntpd ist der NTP-Dämonprozess, der die lokale Uhrzeit eines OSD/POSIX Systems verwaltet, eventuell in Zusammenarbeit mit Internet-Standardservern.

ntpd
[-bdgq] [-c <conffile>] [-D <level>] [-f <driftfile>] [-k <keyfile>] [-l <logfile>] [-p <pidfile>] [-r <broadcastdelay>]

Sie sollten den NTP-Dämon *ntpd* normalerweise mit dem Skript */etc/init.d/TCP-IP-SV.ntp* bzw. mit dem auf dieses Skript weisenden Link */etc/rc2.d/S97TCP-IP-SV.ntp* starten. Das Skript inkludiert die Datei */etc/default/TCP-IP-SV.ntp*, um Vorbelegungen für bestimmte Shell-Variablen durchzuführen (die u.a. Job-Klasse, Job-Name, Account, *conffile*, *driftfile*, *logfile* und *pidfile* festlegen) und ruft das Programm */opt/TCP-IP-SV/ntp/sbin/start-ntp-daemon* auf.

Dieses generiert und startet einen ENTER-Job, der das Skript */opt/TCP-IP-SV/ntp/etc/rc.d/ntpd* aufruft, welches dann den *ntpd* aufruft. Veränderungen der Optionen sollten daher in */etc/default/TCP-IP-SV.ntp* vorgenommen werden.

Konfigurationsparameter für *ntpd* werden beim Start aus einer Konfigurationsdatei (Default: */etc/ntp.conf*) gelesen. Wenn *ntpd* nur als Broadcast-Client verwendet wird, kommt man auch ohne Konfigurationsdatei aus, sofern der NTP-Dämon über das Kommando *ntpd -b* und nicht mit dem Skript */etc/init.d/TCP-IP-SV.ntp* gestartet wird. Interne Variablen und/oder Konfigurationsparameter von *ntpd* können mit dem Programm *ntpq* angezeigt werden.

Der lokale *ntpd* kann gegenüber fernen Rechnern in einem der folgenden Modi konfiguriert werden:

– symmetrisch aktiv/passiv
– Client
– Broadcast-Client

Ein Broadcast-Client erkennt automatisch ferne Server und berechnet Zeitkorrekturen auf Grund von Nachrichtenlaufzeiten zwischen Server und Client. Broadcast-Clients lassen sich vollständig über Parameter in der Kommandozeile konfigurieren.

Optionen

Weitere Informationen zu den nachfolgend beschriebenen und den nicht aufgeführten Optionen finden Sie z.B. in der HTML-Dokumentation.

-b

ntpd ist Broadcast-Client, d.h. er empfängt NTP-Broadcasts und synchronisiert die lokale Uhrzeit entsprechend.

-d

ntpd wird im Testmodus (Debugging Mode) gestartet. Diese Option kann mehrfach angegeben werden, was zu umfangreicheren Testmeldungen führt. Falls die *-l-* Option (siehe unten) nicht gesetzt ist, werden die Testmeldungen in die Datei */var/adm/syslog* geschrieben.

-g

ntpd korrigiert die lokale Systemzeit auf Grund eines empfangenen Zeitstempels in jedem Fall. Ohne diese Option wird die lokale Systemzeit nur dann korrigiert, wenn sie gegenüber dem empfangenen Zeitstempel um nicht mehr als 1000 Sekunden abweicht. Diese Option können Sie mit den Optionen *-q* und *-x* verwenden.

-q

Nach dem ersten Setzen der Systemuhr wird *ntpd* beendet. Dieses Verhalten emuliert das *ntpdate*-Programm, das in der Zukunft abgeschafft werden wird. Diese Option können Sie mit den Optionen *-g* und *-x* verwenden.

-c <conffile>

verweist auf den Namen der Konfigurationsdatei
Default: */etc/ntp.conf*

-D <level>

Setzt den Testmodus-Level direkt.

-f <driftfile>

spezifiziert den Namen der Drift-Datei (siehe Seite 279). Dies bewirkt das Gleiche wie die *driftfile*-Anweisung.

-k <keyfile>

spezifiziert die Datei mit den symmetrischen Schlüsseln. Dies bewirkt das Gleiche wie die *keys*-Anweisung.

-l <logfile>

spezifiziert den Namen der Protokolldatei für *syslog*-Meldungen.

-p <pidfile>

spezifiziert die Datei, in der *ntpd* seine Prozessnummer hinterlegt.

-r <broadcastdelay>

Normalerweise gleicht *ntpd* Nachrichtenlaufzeiten zwischen einem Broadcast-Server und dem Client automatisch aus. Wenn dies nicht möglich ist, können Sie mit dieser Option eine geschätzte Nachrichtenlaufzeit vorgeben.

8.3.5 Datum und Uhrzeit über NTP setzen mit dem Programm ntpdate

Das Programm *ntpdate* setzt das lokale Datum und die Uhrzeit. Das korrekte Datum und die korrekte Uhrzeit ermittelt *ntpdate* durch Pollen des NTP-Servers auf dem angegebenen Server bzw. den angegebenen Servern.

ntpdate
[-ds] [-o <version#>] [-p <zeitstempel_anzahl>] [-t <timeout>] [-a key] <server >

ntpdate muss vom POSIX-Verwalter auf dem lokalen Rechner ausgeführt werden. Von jedem der angegebenen Server werden mehrere Zeitstempel empfangen, aus denen der am besten geeignete mithilfe der NTP-Algorithmen zur Auswahl eines NTP-Zeitgebers ausgesucht wird.

ntpdate kann in ein Startskript aufgenommen werden, um die Uhr beim POSIX-START anzugleichen, und/oder regelmäßig über *cron* ausgeführt werden. Mit mindestens drei bis vier Servern werden bessere Ergebnisse erzielt als mit einem einzigen Server. Außerdem wird die Anfälligkeit gegenüber Funktionsausfällen von Servern reduziert.

ntpdate kann nur ausgeführt werden, wenn nicht der Dämon *ntpd* auf demselben Rechner abläuft.

Das Programm *ntpdate* soll in Zukunft eingestellt werden. Daher sollten Sie sich überlegen, ob Sie nicht frühzeitig auf die Verwendung von *ntpd* mit der *-q* Option umsteigen.

Optionen

Weitere Informationen zu den nachfolgend beschriebenen und den nicht aufgeführten Optionen finden Sie z.B. in der HTML-Dokumentation.

-d

Diese Option kann verwendet werden, um eine Aktion von *ntpdate* zu simulieren, d. h., ohne diese Aktion tatsächlich auszuführen. Ferner werden Informationen für die Testhilfe ausgegeben.

-s

Diese Option weist *ntpdate* an, die Aktionen über die Funktion *syslog* (Ausgabe in */var/adm/syslog*) anstatt in der Standard-Ausgabe aufzuzeichnen. Die Option *-s* bietet sich an, wenn *ntpdate* von *cron* ausgeführt wird.

-o <version#>
Mit dieser Option kann festgelegt werden, dass in den gesendeten NTP-Paketen eine andere Versionsnummer als der Standardwert 4 verwendet wird.
Mögliche Werte sind 1, 2, 3 oder 4.

-p <zeitstempel_anzahl>
Über diese Option kann die Anzahl der Zeitstempel, die *ntpdate* erhält, auf Werte von 1 bis 8 eingestellt werden. Default: 4

-t <timeout>
Über diese Option kann angegeben werden, wie lange auf eine Antwort gewartet werden soll. Die Antwort-Wartezeit wird auf ein Vielfaches von 0,2 Sekunden gerundet. Default: 1 sec

-a <key>
aktiviert die Authentifizierungsfunktion und spezifiziert den Schlüsselindikator, der für die Authentifizierung verwendet werden soll. Die Schlüssel und die Schlüsselindikatoren müssen in Client- und Server-Schlüsseldateien übereinstimmen.

<server>
spezifiziert einen oder mehrere Rechner, von dem bzw. von denen Zeitstempel angefordert werden.

8.3.6 Kryptographische Dateien für NTPv4-Authentifizierung generieren mit dem Programm ntp-keygen

Das Programm *ntp-keygen* generiert Dateien mit kryptographischem Material, die für die NTPv4-Authentifizierungsmechanismen verwendet werden. Es kann Message Digest-Schlüssel generieren, die bei der symmetrischen Verschlüsselung verwendet werden. Außerdem generiert es Host-Schlüssel, Signierungsschlüssel, Zertifikate und Identitätsschlüssel, die bei der "Autokey"-Kryptographie mit öffentlichen Schlüsseln verwendet werden.

Eine Beschreibung der Aufrufparameter finden Sie z.B. in der HTML-Dokumentation.

8.4 Administration und Betrieb

Administration und Betrieb von NTP bestehen im Wesentlichen in der Abfrage des NTP-Status mit dem NTP-Programm *ntpq*.

Mit dem NTP-Programm *ntpq* lässt sich der aktuelle Status von NTP-Servern durch Steuernachrichten abfragen. Dabei kann *ntpq* entweder über Kommandozeilen-Optionen gesteuert oder im interaktiven Modus ausgeführt werden. Bei der interaktiven Ausführung mit Kommandos ist zu unterscheiden zwischen *ntpq*-internen Kommandos und Kommandos für Steuernachrichten.

8.4.1 NTP-Status über Kommandozeilen-Optionen abfragen

ntpq
[-inp][-d][-c <kommando>] [<server>] [...]

Wenn eine oder mehrere Anweisungen in der Kommandozeile angegeben sind, wird jede dieser Anweisungen an die NTP-Server gesendet, die auf den einzelnen in den Kommandozeilen-Optionen angegebenen Rechnern oder standardmäßig auf dem lokalen Rechner (*localhost*) ablaufen. Wenn keine Anweisungen angegeben sind, versucht *ntpq* Kommandos von der Standard-Eingabe zu lesen und diese auf dem NTP-Server auszuführen, der auf dem ersten in der Kommandozeile angegebenen Rechner oder standardmäßig (wenn kein anderer Rechner angegeben ist) auf dem lokalen Rechner läuft.

ntpq verwendet spezielle Pakete für die Kommunikation mit dem NTP-Server und kann daher auch zur Abfrage beliebiger kompatibler NTP-Server im Netz verwendet werden.

Nachfolgend werden die Kommandozeilen-Optionen beschrieben. Wenn eine andere Kommandozeilen-Option als -i oder -n angegeben wird, werden die jeweiligen Abfragen direkt an die genannten Rechner gesendet. Andernfalls versucht *ntpq* interaktiv, Kommandos von der Standard-Eingabe zu lesen.

Optionen

-i
setzt *ntpq* in den interaktiven Betriebsmodus. Kommandos werden von der Standard-Eingabe gelesen.

-n
gibt alle Rechneradressen in der Punktschreibweise aus, anstatt sie in Rechnernamen umzusetzen.

-p
druckt eine Liste der dem Server bekannten Partner (NTP-Partner-Rechner und -Zeitgeber) sowie eine Übersicht über deren Status aus. Dies entspricht dem interaktiven Kommando *peers*.

-d
schaltet die Ausgabe von Testhilfedaten ein.

-c <kommando>[<rechner>] ...
Das auf *-c* folgende Argument wird als Kommando interpretiert und zur Liste der auf den angegebenen Hosts auszuführenden Kommandos hinzugefügt. Die Option *-c* kann mehrmals angegeben werden.

<server>
Spezifiziert den NTP-Server, für den der aktuelle Status ermittelt werden soll.

8.4.2 NTP-Status interaktiv abfragen mit Kommandos

Die Kommandos zur interaktiven Abfrage des NTP-Status bestehen aus einem Schlüsselwort, gefolgt von 0 bis 4 Argumenten. Es müssen nur so viele Zeichen des Schlüsselwortes eingegeben werden, wie zur eindeutigen Identifizierung des Kommandos erforderlich sind. Die von einem Kommando erzeugte Ausgabe wird normalerweise in die Standard-Ausgabe geschrieben. Optional kann die Ausgabe einzelner Kommandos jedoch auch durch Anhängen von >*dateiname* in die Datei *dateiname* gestellt werden.

Bei den Kommandos ist zu unterscheiden zwischen

- Kommandos, die intern vom Programm *ntpq* selbst ausgeführt werden (*ntpq*-interne Kommandos).
- Kommandos, die veranlassen, dass NTP-Anforderungen an einen NTP-Server gesendet werden.

8.4.2.1 NTP-Status mit ntpq-internen Kommandos abfragen

Die nachfolgend beschriebenen Kommandos werden vom Programm *ntpq* selbst beantwortet.

Informationen zu Kommando-Schlüsselwörter ausgeben

?[schlüsselwort]

Ein allein stehendes „?“ gibt eine Liste aller Kommando-Schlüsselwörter aus, die *ntpq* kennt. Ein „?“, gefolgt von einem Kommandoschlüsselwort, gibt Informationen zur Funktion und Syntax dieses Kommandos aus.

Zeitlimit für Antworten auf Serveranfragen angeben

---

timeout millisekunden

Das *timeout*-Kommando gibt ein Zeitlimit für Antworten auf Server-Abfragen an (in Millisekunden). Da *ntpq* jede Abfrage nach einer Zeitlimitüberschreitung wiederholt, ist die Gesamtwartezeit doppelt so lang wie der angegebene Zeitlimitwert.
Default: 5000 Millisekunden

Rechnernamen für nachfolgende Abfragen angeben

---

host rechnername

Das *host*-Kommando spezifiziert den Rechner, an den nachfolgende Abfragen gesendet werden. Als *rechnername* kann entweder ein Rechnername oder eine numerische Adresse angegeben werden.

Rechnernamen bei ntpq-Ausgaben anzeigen

`hostnames yes | hostnames no`

Wenn *hostname yes* angegeben ist, werden Rechnernamen in den Ausgaben von *ntpq* angezeigt. Bei *hostname no* werden an Stelle der Rechnernamen numerische Adressen ausgegeben.

Default: *hostname yes* (Sofern der Defaultwert nicht über den Schalter *-n* in der Kommandozeile geändert wird.)

Antworten des fernen Servers unverändert anzeigen

`raw`

Die Antworten des fernen Servers auf Abfragekommandos werden so angezeigt, wie sie empfangen wurden. Die einzige an den Daten vorgenommene Formatierung/Interpretation ist die Umwandlung von Nicht-ASCII-Daten in ein abdruckbares Format.

Antworten auf Abfragekommandos aufbereiten

`cooked`

Die Antworten auf Abfragekommandos werden aufbereitet. Die Werte der vom Server erkannten Variablen werden neu, d.h. benutzerfreundlich, formatiert. Variablen, die *ntpq* nicht interpretieren kann, werden mit einem nachfolgenden „?“ gekennzeichnet.

Versionsnummer setzen

```
ntpversion 1 | ntpversion 2 | ntpversion 3 | ntpversion 4
```

Die Versionsnummer, die *ntpq* in NTP-Paketen verwendet, wird gesetzt. Zu beachten ist, dass Modus-6-Steuernachrichten (und auch der entsprechende Modus) erst ab der NTP-Version 2 existieren.
Default: `ntpversion 2`

Testhilfefunktion einschalten

```
debug more | debug less | debug off
```

Die interne Testhilfefunktion des Abfragekommandos wird ein- bzw. ausgeschaltet.

debug more
: Der Debug-Level wird um 1 erhöht, d.h. es werden mehr Diagnose-Informationen geliefert.

debug less
: Der Debug-Level wird um 1 reduziert, d.h. es werden weniger Diagnose-Informationen geliefert.

debug off
: Die Testhilfefunktion wird ausgeschaltet.

ntpq beenden

```
quit
```

Das Programm *ntpq* wird beendet.

8.4.2.2 NTP-Status mit Kommandos für Steuernachrichten abfragen

Jeder Partner, der einem Server bekannt ist, verfügt über eine 16 bit lange, ganzzahlige Zuordnungs-ID (association identifier). NTP-Steuernachrichten mit Partnervariablen müssen anhand der Zuordnungs-ID den Partner identifizieren, zu dem die Werte gehören.

Durch Kommandos für Steuernachrichten werden eine oder mehrere NTP-Nachrichten an den Server gesendet, und die zurückgegebenen Daten werden teilweise formatiert ausgegeben. Die meisten Kommandos geben eine einzelne Nachricht aus und erwarten auch eine einzelne Antwort. Ausnahme ist das Kommando *peers*, über das eine vorprogrammierte Reihe von Nachrichten gesendet wird.

Zuordnungs-IDs und Partner-Status anfordern und ausgeben

```
associations
```

Das *associations*-Kommando fordert eine Liste der Zuordnungs-IDs und Partner-Status für die Partner des abgefragten Servers an und gibt diese Liste in Spalten aus. Die erste Spalte enthält eine Nummerierung der Zuordnungen (beginnend bei 1), die zweite Spalte enthält die eigentlichen vom Server zurückgegebenen Zuordnungs-IDs, und die dritte Spalte enthält das Statuswort für den Partner. Dann folgen mehrere Spalten mit Daten, die aus dem Statuswort decodiert wurden. Die vom Kommando *associations* zurückgegebenen Daten werden *ntpq*-intern zwischengespeichert.

Anforderung zum Lesen eines Status senden

```
pstatus assocID
```

Das *pstatus*-Kommando sendet eine Anforderung zum Lesen des Status für die durch *assocID* spezifizierte Zuordnungs-ID (*assocID*) an den Server. Die zurückgelieferten Namen und Werte der Partnervariablen werden ausgegeben.

Liste der Zeitgebervariablen des Servers anfordern

```
clockvar[ assocID] [name[,name...]]
-------------------------------------------------------------------
cv[ assocID] [name[,name...]]
```

Das *clockvar*-Kommando bzw. seine Kurzform *cv* fordert eine Liste der Zeitgebervariablen des Servers an. Server, auf denen ein Zeitgeber konfiguriert ist, reagieren auf diese Anforderung positiv. *assocID* spezifiziert die Zuordnungs-ID. Wenn die Zuordnungs-ID nicht oder als „0“ angegeben wird, gilt die Anforderung für die Variablen der internen NTP-Systemuhr des Servers. Ansonsten wird die Zuordnungs-ID als Partner-Zuordnungs-ID eines Zeitgebers aufgefasst, und die zugehörigen Variablen werden angezeigt. Ohne die Angabe einer Variablenliste gibt der Server eine Standardliste von Variablen und Werten zurück.

Liste von Partnern des Servers inklusive Zusatzinformationen anfordern

```
peers
```

Das *peers*-Kommando fordert eine Liste von Partnern des Servers inklusive einer Übersicht zum Status der einzelnen Partner an. Zu den Übersichtsinformationen gehören

- die Adresse des fernen Partners,
- die Referenz-ID (0.0.0.0 bei unbekannter Referenz-ID),
- das Stratum des fernen Partners,
- der Typ des Partners (*local*, *unicast* oder *broadcast*),
- die Angabe, wann das letzte Paket eingegangen ist,
- das Polling-Intervall (in Sekunden),
- das Erreichbarkeitsregister (als Oktalzahl),
- die aktuelle Nachrichtenlaufzeit,
- Abweichung und Streuung des Partners (jeweils in Millisekunden).

Das Zeichen am linken Rand zeigt die Bedeutung dieses Partners im Zeitgeberauswahlprozess an.

Im einzelnen bedeuten die Codes:

sp
gelöscht auf Grund hohen Stratums und/oder negativer Plausibilitätsprüfungen

x
Uhrzeit wird wegen zu hoher Abweichung als ungültig angesehen

.
aus dem Ende der Kandidatenliste ausgewählt

-
von den Cluster-Algorithmen gelöscht

+
in die Endauswahlgruppe aufgenommen

#
zur Synchronisation ausgewählt. Der Synchronisationsabstand überschreitet jedoch das Maximum.

*****
zur Synchronisation ausgewählt

o
zur Synchronisation ausgewählt, externer Zeitgeber

Im Rechnerfeld kann entweder ein Rechnername, eine IP-Adresse oder der Name eines Zeitgebers angegeben sein. Bei *hostnames no* (siehe Seite 289) werden nur IP-Adressen angezeigt.

Schlüssel-Id spezifizieren für die Authentifizierung von Konfigurationsrequests

---

keyid ***keyid***

Das *keyid*-Kommando spezifiziert eine Schlüssel-Id für die Authentifizierung von Konfigurationsrequests. Die angegebene Schlüsselnummer muss zu einer Schlüsselnummer passen, die beim Server für diesen Zweck konfiguriert wurde.

Passwort erfragen lassen für die Authentifizierung von Konfigurationsrequests

passwd

Das *passwd*-Kommando erfragt ein Passwort, das einem Schlüssel entsprechen muss, der beim Server für diesen Zweck konfiguriert wurde.

8.5 Diagnose und Wartung von NTP

Die folgenden Abschnitte informieren Sie über Logging-Funktion und Trace-Funktionalität von NTP.

8.5.1 Logging-Funktion

Die Komponente NTP legt ihre Logging-Informationen in der Datei */var/adm/syslog* ab.

Die ntp-Einträge dieser Logging-Datei haben das folgende Grundformat:

```
<datum> <zeit> Schlüsselwort ntpd[pid]: <meldungstext>
```

Nach Datum und Systemzeit folgt ein Schlüsselwort für die Klassifizierung der Meldung.

Der NTP verwendet die Schlüsselwörter LOG_INFO, LOG_NOTICE, LOG_DEBUG und LOG_ERR.

Nach dieser Klassifizierung kommt der Prozessname (hier *ntpd*) mit der Information über das dazugehörige Prozesskennzeichen PID. Falls zur Meldungsausgabe keine gültige PID verfügbar ist (beispielsweise bei einer Meldungsausgabe während der Start-Phase des Dämons), wird ein leerer Klammerausdruck ausgegeben. Daran anschließend folgt der eigentliche Meldungstext.

Zusätzlich werden standardmäßig Logging-Einträge in die Datei */var/adm/ntp.log* geschrieben.

8.5.2 Trace-Funktionalität von NTP

Die Trace-Funktionalität von NTP wird durch das Perl-Skript *ntptrace* abgedeckt. Für die Verwendung muss Perl installiert sein.

8.5.2.1 ntptrace - Kette von NTP-Servern zurückverfolgen zum maßgeblichen Zeitgeber

ntptrace
-n -m <maxhosts> [<server>]

ntptrace stellt fest, woher ein bestimmter NTP-Server seine Uhrzeitangabe bezieht und verfolgt die Kette der NTP-Server zurück bis zum maßgeblichen Zeitgeber. Werden keine Argumente angegeben, beginnt das Kommando mit *localhost*.

Beispiel einer Ausgabe von *ntptrace*:

```
% ntptrace
localhost: stratum 4, offset 0.0019529, synch distance 0.144135
server2.bozo.com: stratum 2, offset 0.0124263, synch distance 0.115784
usndh.edu: stratum 1, offset 0.0019298, synch distance 0.020993, refid 'WWVB'
```

Die Felder (von links nach rechts) in jeder Zeile sind: der Rechnername, das Rechner-Stratum, die Zeitabweichung zwischen diesem und dem lokalen Rechner (wie von *ntptrace* ermittelt; daher ist dieser Wert für *localhost* nicht immer 0), der Synchronisationsabstand (Synchronization distance) des Rechners und (nur für Server des Stratums 1) die ID des externen Zeitgebers. Alle Zeiten sind in Sekunden angegeben. (Der Synchronisationsabstand ist ein Maß für die Nachrichtenlaufzeit zum Partner.)

Optionen

-n
Statt der Rechnernamen werden die IP-Adressen angegeben. Dies kann erforderlich sein, wenn kein Name Server läuft.

-m <maxhosts>
gibt eine maximale Länge für die Verfolgung der Kette der NTP-Server vor.
Default: 99

<server>
spezifiziert den Rechner, von dem aus die Kette zum maßgeblichen Zeitgeber zurückverfolgt werden soll.
Default: *localhost*

9 OpenSSH

Dieses Kapitel basiert auf den Manual Pages (Man Pages) von OpenSSH und beschreibt den OpenSSH Server. Der OpenSSH Client ist im Handbuch „interNet Services Benutzerhandbuch“ beschrieben.

Die hier vorliegende Beschreibung ist auf die BS2000-relevanten Teile gekürzt. An entsprechenden Stellen des Kapitels, wie z.B. bei der Beschreibung von Options, wird auf die Man Pages von OpenSSH verwiesen, da nur dort die aktuellsten Versionen beschrieben sind. Sie finden die Man Pages von OpenSSH im Internet unter *http://www.openssh.org/manual.html* oder nach der Installation der Komponente OpenSSH auf Ihrem Server

- unter *<installationspfad>/readme/TCP-IP-SV.openssh/html/* als HTML-Datei,
- unter *<installationspfad>/readme/TCP-IP-SV.openssh/pdf/* als PDF-Datei,
- unter *<installationspfad>/readme/TCP-IP-SV.openssh/text/* als Text-Datei.

Der Standard-Installationspfad lautet: */opt/TCP-IP-SV/openssh/*

Wenn im weiteren Verlauf dieses Kapitel wiederholt auf die „Man Pages von OpenSSH“ verwiesen wird, sind im Einzelnen diese Quellen gemeint. Dabei sind die mit dem Produkt ausgelieferten Man Pages zu bevorzugen, da diese Man Pages die BS2000-spezifischen Anpassungen enthalten (geänderte Pfadnamen, erweiterte Funktionalität etc.).

SSH (**S**ecure **Sh**ell) ist ein kryptographisches Protokoll für die Durchführung der folgenden Aufgaben:

- Login auf einen fernen Rechner
- interaktive / nicht interaktive Kommandoausführung auf einem fernen Rechner
- File Transfer zwischen verschiedenen Rechnern eines Netzes

SSH bezeichnet nicht nur das Protokoll selbst, sondern auch die konkreten Implementierungen.

Programme wie *telnet*, *rlogin*, *rsh* und *rcp* decken die genannten Aufgabenbereiche zwar ebenfalls ab, enthalten jedoch erhebliche Sicherheitslücken. So wird beispielsweise die gesamte Kommunikation inklusive der Passwörter in der Regel unverschlüsselt übertragen.

SSH gewährleistet eine kryptographisch gesicherte Kommunikation über unsichere Netze und bietet umfassende Sicherheit durch

- zuverlässige gegenseitige Authentifizierung der Kommunikationspartner,
- Integrität und Vertraulichkeit der ausgetauschten Daten.

Intention bei der Entwicklung von SSH war es u.a., die r-Utilities *rlogin*, *rsh* und *rcp* zu ersetzen. SSH ist in den Protokollversionen SSH 1 und SSH 2 verfügbar.

OpenSSH ist eine freie, d.h. nicht lizenzkostenpflichtige Version von SSH. Basis der OpenSSH-Portierung nach POSIX ist zum Zeitpunkt der Drucklegung des Handbuchs OpenSSH V7.3. Da diese OpenSSH-Version die SSH-Protokollversionen 1.3 und 1.5 nur noch teilweise unterstützt und diese Teilunterstützung in absehbarer Zeit komplett wegfallen wird, bezieht sich die nachfolgende Beschreibung nur noch auf Umstände, die bei der Nutzung der SSH-Version 2 gültig sind.

9.1 Konzept von OpenSSH

OpenSSH ist die sichere Alternative zu den r-Utilities *rlogin*, *rcp*, *rsh* und den Programmen *telnet* und *ftp*. Im Gegensatz zu den genannten Programmen verschlüsselt OpenSSH den gesamten Netzverkehr (inklusive Passwörtern) und verhindert so Eavesdropping, Connection Hijacking und andere Attacken auf Netzebene. Darüber hinaus unterstützt OpenSSH eine Vielzahl von Tunnelling-Varianten sowie eine große Bandbreite an Authentifizierungsmethoden.

9.1.1 Bestandteile der OpenSSH Protokoll-Suite

Die OpenSSH Protokoll-Suite umfasst folgende Programme bzw. Kommandos:

- Auf der Server-Seite: Server-Programm *sshd* (siehe Seite 307)
- Auf der Client-Seite (siehe Handbuch „interNet Services Benutzerhandbuch“):
  - Client-Programm *ssh* bzw. *slogin*: ersetzt *rsh* und *telnet*.
  - *scp*: ersetzt *rcp*.
  - *sftp*: ersetzt *ftp*.
- Administrations-Utilities (siehe Handbuch „interNet Services Benutzerhandbuch“):
  - *ssh-agent*
  - *ssh-add*
  - *ssh-keygen*
  - *ssh-keyscan*

Für die sichere Kommunikation via SSH von Windows-Systemen mit BS2000-Systemen stellt Ihnen z.B. die Open Source-Software *PuTTY* die Funktionalität der Client-Seite von OpenSSH zur Verfügung.

9.1.2 Netzsicherheit mit OpenSSH

OpenSSH schützt vor folgenden Bedrohungen der Netzsicherheit:

- IP Spoofing

  Beim IP Spoofing sendet ein ferner Rechner Pakete mit einer gefälschten Absenderadresse. OpenSSH schützt sogar vor einem Spoofer im lokalen Netz, der sich als Ihr Router für ausgehende Nachrichten ausgibt.

- DNS Spoofing

  Beim DNS Spoofing fälscht ein Angreifer die Resource Records (RR) im DNS Name Server.

- Connection Hijacking („Entführen von Verbindungen“)

- Eavesdropping

  Unbefugtes Mithören von unverschlüsselten Passwörtern und anderen Klartext-Nachrichten.

- Datenverfälschung

Schutz vor unbefugtem Lesen und Datenverfälschung realisiert OpenSSH durch Verschlüsselung des Netzverkehrs. IP Spoofing und DNS Spoofing verhindert OpenSSH durch gegenseitige Authentifizierung der Kommunikationspartner.

Somit kann ein Angreifer, der Kontrolle über das Netz erlangt hat, lediglich den Verbindungsabbruch von OpenSSH erzwingen. Der Angreifer kann jedoch

- keine Nachrichten entschlüsseln,
- keine Nachrichten abfangen und wieder einspielen,
- kein Connection Hijacking betreiben.

9.1.3 Merkmale von OpenSSH

OpenSSH zeichnet sich durch folgende Merkmale aus:

- starke Verschlüsselung
- automatische und transparente Verschlüsselung
- starke Authentifizierung
- Interoperabilität
- Übertragung von Binärdaten und Datenkompression
- Agent Forwarding
- TCP Forwarding

Starke Verschlüsselung

OpenSSH unterstützt die Verschlüsselungsalgorithmen AES, ChaCha20 und 3DES; die Unterstützung für Blowfish, Cast128 und Arcfour wird voraussichtlich bald entfallen.

- AES ist ein schneller Block-Chiffrierer. AES erfüllt den US Federal Information Processing Standard (FIPS) Advanced Encryption Standard und wurde als Ersatz für DES entwickelt.
- 3DES ist ein bewährter Verschlüsselungsalgorithmus für starke Verschlüsselung. 3DES zeigt aber mittlerweile wegen seiner kurzen Blocklänge von 64 Bit Schwächen und wird daher mittelfristig wohl nicht mehr von OpenSSH unterstützt werden.
- ChaCha20 ist ein schneller Stream-Chiffrierer, der das sicherheitstechnisch in Verruf geratene Arcfour ablöst.

Automatische und transparente Verschlüsselung

Standardmäßig wird die Verschlüsselung der gesamten Kommunikation zwischen OpenSSH Client und OpenSSH Server automatisch und transparent durchgeführt. Verwendet wird hierfür ein symmetrisches Verschlüsselungsverfahren, wie z.B. AES oder ChaCha20.

Starke Authentifizierung

Die Authentifizierung des OpenSSH Servers durch den OpenSSH Client basiert auf den asymmetrischen Verschlüsselungsalgorithmen RSA, DSA, ECDSA und Ed25519. Für die Authentifizierung des OpenSSH Clients durch den OpenSSH Server stehen mehrere Verfahren zur Auswahl (siehe Seite 311).

Übertragung von Binärdaten und Datenkompression

Es wird die Übertragung von Binärdaten über das Netz unterstützt. Optionale Datenkompression vor der Verschlüsselung verbessert die Performance bei der Übertragung über langsame Netzverbindungen.

Agent Forwarding

Beim Agent Forwarding verwaltet der Authentifizierungsagent (siehe Handbuch „interNet Services Benutzerhandbuch“), der auf dem lokalen Rechner des OpenSSH Clients abläuft, die Authentifizierungsschlüssel (RSA/DSA/ECDSA/Ed25519) des OpenSSH-Clients. OpenSSH kann die Verbindung automatisch an den Authentifizierungsagenten über jede Netzverbindung weiterleiten. Die Authentifizierungsschlüssel müssen dann lediglich auf Ihrem lokalen Rechner, jedoch auf keinem weiteren Rechner im Netz, bereit gehalten werden.

Port Forwarding (TCP Forwarding)

Port-Forwarding macht unsichere TCP/IP-Verbindungen sicher durch Weiterleiten („Tunnelling“) von TCP/IP-Verbindungen zu einem fernen Rechner über ein verschlüsseltes Protokoll. Port Forwarding realisiert das Mapping eines lokalen Port am Client-Rechner auf einen Port am fernen Rechner.

9.2 OpenSSH installieren und deinstallieren

Beachten Sie bitte zusätzlich zu diesem Kapitel die mit dem Produkt interNet Services ausgelieferte Freigabemitteilung.

9.2.1 OpenSSH installieren

Die einzelnen Komponenten des Software-Pakets interNet Services werden als ein POSIX-Programmpaket per Package-Installation mit dem POSIX-Installationsprogramm installiert (siehe Handbuch „POSIX Grundlagen für Anwender und Systemverwalter“).

Zur Installation und zum Betrieb der OpenSSH-Suite muss die PLAM-Bibliothek SINLIB.TCP-IP-SV.*nnn*.OPENSSH shareable zur Verfügung stehen.

```
/START-POSIX-INSTALLATION
```

Funktion: POSIX-Programmpakete installieren (IMON-Unterstützung: Y)
Produktname: TCP-IP-SV
Paketname: OPENSSH

Wenn Sie OpenSSH mit dem POSIX-Installationsprogramm installieren, werden Sie zunächst nach dem Installationspfad <*installationspfad*> gefragt. Es empfiehlt sich, die Voreinstellung */opt/TCP-IP-SV/openssh* zu verwenden. Wenn Sie einen anderen Pfadnamen angeben, wird bei der Durchführung des Post-Installation-Skripts (siehe unten) der Pfad */opt/TCP-IP-SV/openssh* als symbolischer Link auf den von Ihnen spezifizierten Pfadnamen angelegt.

Anschließend prüft das POSIX-Installationsprogramm das */opt*-Dateisystem auf ausreichenden Speicherplatz und spielt alle Dateien aus der PLAM-Bibliothek ins POSIX-Dateisystem ein.

Ablauf des Post-Installation-Skripts

Nachdem alle Dateien eingespielt sind, wird automatisch ein Post-Installation-Skript gestartet, das die rechner-spezifische Einrichtung der OpenSSH-Komponenten abwickelt.

Im Einzelnen führt das Post-Installation-Skript die folgenden Schritte durch und protokolliert die Ausführung dieser Schritte auf der Konsole:

1. Die Verzeichnisse */etc/tcpipsv/openssh*, */opt/SMAWPlus/etc* und */usr/local/etc* werden nach SSH-Host-Key-Dateien einer früheren Installation von TCP-IP-SV:openssh durchsucht. Die jeweils erste Host-Key-Datei (sofern vorhanden) jedes Verzeichnisses wird in das Verzeichnis */etc/ssh/* übernommen.

   Gesucht wird nach den folgenden Paaren von Host-Key-Dateien (privater/öffentlicher Schlüssel):

   - *ssh_host_rsa_key* und *ssh_host_rsa_key.pub* (RSA)
   - *ssh_host_dsa_key* und *ssh_host_dsa_key.pub* (DSA)
   - *ssh_host_ecdsa_key* und *ssh_host_ecdsa_key.pub* (ECDSA)
   - *ssh_host_ed25519_key* und *ssh_host_ed25519_key.pub* (Ed25519)

2. Das Verzeichnis */etc/tcpipsv/openssh* wird nach den *ssh*- und *sshd*-Konfigurationsdateien (*ssh_config*, *sshd_config*) einer früheren Installation von TCP-IP-SV:openssh durchsucht. Kann keine Konfigurationsdatei gefunden werden, so wird die mit dem Produkt ausgelieferte Konfigurationsdatei kopiert.

3. Das Verzeichnis */var/run* wird, sofern es noch nicht existiert, generiert, da es für die Prozess-ID-Datei des OpenSSH Servers *sshd* benötigt wird.

4. Falls Sie bei der Installation einen vom Standard-Installationspfad */opt/TCP-IP-SV/openssh* abweichenden Installationspfad angegeben haben, wird in den Startup-Skripts der Standard-Installationspfad in den von Ihnen spezifizierten Installationspfad geändert, und */opt/TCP-IP-SV/openssh* wird als symbolischer Link auf diesen Installationspfad eingerichtet.

5. Wenn in Schritt 1) nicht alle Host-Key-Dateien gefunden wurden, werden diese nun erzeugt. Zu diesem Zweck wird das Utility *ssh-keygen* (siehe Handbuch „interNet Services Benutzerhandbuch“) bis zu vier Mal aufgerufen (für RSA, DSA, ECDSA und Ed25519), um einen nicht wiederholbaren zufälligen Host-Key zu erzeugen.

6. Wenn keine POSIX-Gruppe mit der Group-Id 22 existiert, wird diese nun erzeugt und mit dem Gruppennamen „sshd“ in die Datei */etc/group* eingetragen.

7. Wenn noch keine Benutzerkennung SYSSSHD existiert, legt das Post-Installations-Skript diese nun an. Außerdem wird ein Address-Space-Limit von 32 MB vereinbart sowie eine POSIX User-Id 22 und eine POSIX Group-Id 22 zugewiesen. Zu diesem Zweck setzt das Post-Installations-Skript die folgenden Kommandos ab:

```
/ADD-USER USER-ID=SYSSSHD,ADDR-SP-LIM=32,-
/         ACC-ATT=*P(ACC=SYSACC,CPU-LIM=*MAX,POSIX=*YES),-
/         MAIL-ADDR='Privilege Separation user id for OpenSSH',-
/         LOGON-PASSWORD=${PASSWORD}
/SET-JOB-STEP
/MOD-USER USER-ID=SYSSSHD,ADDR-SP-LIM=32,-
/         ACC-ATT=*M(ACC=SYSACC,CPU-LIM=*MAX,POSIX=*YES),-
/         LOGON-PASSWORD=${PASSWORD}
/MOD-POS-USER-ATTR USER-ID=SYSSSHD,USER-N=22,GROUP-N=22,-
/         DIRECTORY='/var/empty',-
/         PROGRAM='/bin/false',-
/         COMM='Privilege Separation user id for OpenSSH'
```

8. In der Startup-Datei */etc/profile* der POSIX-Shell wird die PATH-Angabe erweitert auf das Verzeichnis *<installationspfad>/bin* (sowie *<installationspfad>/sbin* für den Benutzer mit der User-Id 0 (SYSROOT bzw. TSOS)). Falls eine C-Shell (*csh* oder *tcsh*) installiert ist, wird mit der *csh*-Startup-Datei (*/etc/.login* bzw. */etc/csh.login*) analog verfahren.
9. Im Falle von ADDRESS-SPACE-LIMIT < 32 MB für SYSROOT wird eine Warnung auf Konsole ausgegeben.
10. Falls kein POSIX-RLOGIN-DEFAULT für SYSROOT gesetzt ist, wird eine entsprechende Fehlermeldung auf Konsole ausgegeben.
11. Falls für die Installationsbibliothek (z.B. *SINLIB.TCP-IP-SV.nnn.OPENSSH*) keine allgemeine Leseberechtigung besteht, wird eine entsprechende Fehlermeldung auf Konsole ausgegeben.

12. Falls keine schwerwiegenden Fehler entdeckt wurden, wird abhängig von der Beantwortung der Installationsabfrage AutoStartOpenSSH das allgemeine POSIX-Start-Skript für OpenSSH aufgerufen, das den *sshd*-Dämon unter SYROOT startet. (Aufruf des POSIX-Start-Skripts: `/etc/init.d/TCP-IP-SV.openssh start`)

    Das Skript `/etc/init.d/TCP-IP-SV.openssh start` bestimmt automatisch die für SYSROOT maximal zulässigen Werte für JOB-CLASS, ACCOUNT, START und CPU LIMIT. Mit diesen Werten startet das Skript einen ENTER-Job mit dem Job-Namen SSHLOGIN.

    Der *sshd*-Dämon protokolliert wichtige Meldungen per syslog-Mechanismus in die Datei */var/adm/syslog*. Zusätzlich werden Probleme, die beim Start des ENTER-Jobs auftreten, in die Datei */var/adm/opensshd_startup.log* geschrieben.

Der *sshd*-Dämon benötigt keine individuelle Konfiguration und kann somit automatisch gestartet werden.

9.2.2 OpenSSH deinstallieren

Zu Beginn der Deinstallation von OpenSSH wird ein Pre-Remove-Skript ausgeführt, das die veränderten Konfigurationsdaten (Host-Key-Dateien, *veränderte* Konfigurationsdateien) in das Verzeichnis */etc/tcpipsv/openssh/* sichert. Unveränderte Konfigurationsdateien werden nicht gesichert. Von dort werden die genannten Dateien bei einer erneuten Installation wieder in das Konfigurationsverzeichnis */etc/ssh/* kopiert.

Wenn Sie bei einer zukünftigen Neu-Installation von OpenSSH nicht auf die Konfigurationsdaten der alten Installation aufsetzen wollen, müssen Sie den Inhalt des Verzeichnisses */etc/tcpipsv/openssh/* komplett entfernen:

```
# rm -fr /etc/tcpipsv/openssh
```

9.3 OpenSSH Server-Dämon sshd

sshd (OpenSSH Daemon) ist das Dämon-Programm für OpenSSH.

9.3.1 OpenSSH Server Dämon sshd konfigurieren

Den OpenSSH Server-Dämon *sshd* können Sie wahlweise konfigurieren:

- mithilfe von Kommandozeilen-Argumenten, die Sie beim Aufruf von *sshd* angeben (siehe Seite 308),
- mithilfe einer Konfigurationsdatei.

Die als Kommandozeilen-Argumente spezifizierten Werte haben Vorrang vor den korrespondierenden Werten in der Konfigurationsdatei.

Konfigurationsdatei von sshd

Standardmäßig liest *sshd* seine Konfigurationsdaten aus der Datei */etc/ssh/sshd_config*. Wenn Sie eine andere Konfigurationsdatei verwenden wollen, spezifizieren Sie diese beim Start von *sshd* in der Kommandozeile mit dem Parameter `-f`.

Bei Empfang eines Hangup-Signals SIGHUP liest *sshd* die Konfigurationsdatei erneut und startet sich neu. *sshd* wird dabei unter dem gleichen Namen ausgeführt, unter dem er auch gestartet wurde, z.B. */opt/TCP-IP-SV/openssh/sbin/sshd*.

In POSIX ist ein Restart nur dann erfolgreich, wenn aktuell keine *sshd*-Session aktiv ist. (Eine aktive *sshd*-Session belegt den TCP/IP-Port und verhindert den Restart.)

Syntax der Konfigurationsdatei

Die Konfigurationsdatei von *sshd* muss gemäß der folgenden Syntax aufgebaut sein:

- Die Datei enthält pro Zeile ein Paar bestehend aus Schlüsselwort und zugehörigem Argument bzw. zugehöriger Argumentenliste:
  - Bei Schlüsselwörtern wird nicht zwischen Groß- und Kleinschreibung unterschieden.
  - Bei Argumenten muss Groß-/Kleinschreibung beachtet werden.
- Leere Zeilen sowie Zeilen, die mit „#“ beginnen, werden als Kommentar interpretiert.

Die ausführliche Beschreibung der Konfigurations-Optionen finden Sie auf den Man Pages von OpenSSH.

9.3.2 sshd starten und stoppen

sshd wird in POSIX standardmäßig wie folgt gestartet und gestoppt:

```
/etc/init.d/TCP-IP-SV.openssh start
```

```
/etc/init.d/TCP-IP-SV.openssh stop
```

In diesem Start-Skript wird der *sshd*-Aufruf nur mit dem Parameter `-f <config_file>` abgesetzt, der die Konfigurationsdatei spezifiziert, aus der die *sshd*-Konfigurationsdaten gelesen werden. Nach dem Start wartet *sshd* an Port 22 auf Verbindungsanforderungen der OpenSSH Clients.

Alternativ können Sie *sshd* unter SYSROOT mit dem folgenden Kommando starten:

```
sshd [-46DdeiqTt] [-b bits] [-C connection_spec] [-c host_cert_file]
     [-E log_file] [-f config_file] [-g login_grace_time]
     [-h host_key_file] [-k key_gen_time] [-o option] [-p port]
     [-u len]
```

Die ausführliche Beschreibung der Operanden finden Sie in den Man Pages von OpenSSH.

Für jede eingehende Verbindungsanforderung erzeugt *sshd* einen neuen Child-Prozess. Diese Child-Prozesse von *sshd* erledigen Schlüsselaustausch (Key Exchange), Verschlüsselung, Authentifizierung, Kommando-Ausführung und Datenaustausch.

9.3.3 Interner Ablauf beim Verbindungsaufbau zwischen OpenSSH Server und Client

Damit *sshd* Verbindungsanforderungen von *ssh* entgegen nehmen kann, muss für *sshd* folgende Voraussetzung erfüllt sein:

- Auf dem Rechner, auf dem *sshd* abläuft (Server-Rechner), existiert ein Host-Key (RSA, DSA, ECDSA oder Ed25519). Der Host-Key ist ein Schlüsselpaar bestehend aus einem privaten und einem öffentlichen Schlüssel und identifiziert den Server-Rechner. Diese Voraussetzung ist durch die Installation in POSIX bereits erfüllt.

Bei jeder Verbindungsanforderung von *ssh* werden die folgenden Schritte ausgeführt:

1. *sshd* sendet den öffentlichen Teil seines Host-Key sowie eine Liste der von ihm unterstützten Verschlüsselungsalgorithmen an *ssh*. Als Verschlüsselungsverfahren kommen derzeit AES, ChaCha20 oder 3DES infrage.
2. *ssh* prüft, ob er *sshd* kennt, indem er nachschaut, ob zum jeweiligen System in der Datei *$HOME/.ssh/known_hosts* des Users bzw. in der vom Systemadministrator zentral bereitgestellten Datei */etc/ssh/ssh_known_hosts* ein öffentlicher Schlüssel hinterlegt ist, und wenn ja, ob dieser mit dem vom *sshd* gesendeten Host-Key gleichen Typs (RSA/DSA/ECDSA/Ed25519) übereinstimmt:
   - Falls zum jeweiligen System ein öffentlicher Schlüssel hinterlegt ist und dieser identisch zu dem vom *sshd* gesendeten öffentlichen Host-Key ist, dann wird mit Schritt 3) fortgesetzt.
   - Falls ein Schlüssel hinterlegt ist, dieser aber nicht mit dem vom *sshd* gesendeten Host-Key identisch ist, dann kann das zwei Ursachen haben:
     a) Der Host-Key des *sshd* ist neu generiert worden (harmlose Variante).
     b) Es versucht gerade jemand einen aktiven „Man-in-the-Middle“-Angriff (MITM-Angriff) auf die SSH-Verbindung.

     Daher wird vom *ssh* in dieser Situation eine entsprechende Warnung ausgegeben und man sollte diese nur abweisen, wenn man sich hinreichend sicher ist, dass die Variante a) zutrifft.

     Wenn die Warnung abgewiesen wird, dann verfährt *ssh* wie bei nicht hinterlegtem Schlüssel.
   - Falls der Host-Key in diesen Dateien nicht enthalten ist, dann berechnet *ssh* aus dem vom *sshd* gesendeten öffentlichen Host-Key einen Fingerprint. Wenn *ssh* entsprechend konfiguriert ist (*VerifyHostKeyDNS Yes*), dann holt sich *ssh* den Host-Key-Fingerprint von DNS (falls dort gespeichert) und vergleicht ihn mit dem berechneten Fingerprint. Andernfalls zeigt *ssh* den berechneten Fingerprint an und fragt den Nutzer, ob dieser ok ist.

- Stimmen die beiden Fingerprints nicht überein bzw. beantwortet der Nutzer die Frage mit "no", dann bricht *ssh* die Verbindung ab.
- Bei Antwort "yes" trägt *ssh* den Host-Key in die Datei *$HOME/.ssh/known_hosts* ein, sodass er nachfolgend bekannt ist und ein Wechsel des Host-Keys, der ein Anzeichen für einen potentiellen MITM-Angriff sein kann, bemerkt wird. Dies gilt allerdings nur, wenn die Option *StrictHostKeyChecking* in der Konfigurationsdatei *ssh_config* nicht auf *yes* gesetzt wurde. Andernfalls muss man die Datei *$HOME/.ssh/known_hosts* manuell mit den korrekten Inhalten füllen. Eine ausführliche Beschreibung der Option *StrictHostKeyChecking* finden Sie auf den Man Pages von OpenSSH).

3. *ssh* und *sshd* tauschen diverse Daten aus. Mit diesen Dateien wird zum einen ein Diffie-Hellman-Schlüsselaustausch realisiert, um einen gemeinsamen Session Key zu erhalten. Zum anderen sendet *sshd* auch Daten, die er mit seinem privaten Host-Key signiert hat. Anhand dieser Signatur kann *ssh* feststellen, dass der *sshd* wirklich im Besitz des zum übermittelten öffentlichen Host-Key gehörenden privaten Host-Key ist.
4. Beide Seiten verwenden den Session Key für die Verschlüsselung der gesamten Kommunikation innerhalb der aktuellen Session. Der Rest der Session wird mithilfe eines symmetrischen Verschlüsselungsverfahrens verschlüsselt. Derzeit kommen im Wesentlichen AES, ChaCha20 oder 3DES infrage. *ssh* wählt den Verschlüsselungsalgorithmus aus der Liste aus, die ihm *sshd* zusammen mit dem Host-Key (siehe Schritt 1) mitgeliefert hat.

   Außerdem wird der Session Key für die Sicherstellung der Datenintegrität mittels eines MAC-Verfahrens (Message Authentication Code) verwendet, welches *ssh* ebenfalls aus einer in Schritt 1 vom *sshd* gelieferten Liste auswählt. Zu solchen Verfahren gehören *HMAC-SHA2*, *HMAC-SHA1* oder *UMAC* in verschiedenen Ausprägungen.
5. Client und *sshd* führen nun einen Authentifizierungsdialog, in dem der Client gegenüber *sshd* seine Identität und Berechtigung nachweist.

   Näheres zur Client-Authentisierung finden Sie im Abschnitt „Authentifizierung zwischen OpenSSH Client und OpenSSH Server“ auf Seite 311.

   sshd authentisiert sich gegenüber dem Client implizit, da er nur mit Kenntnis seiner privaten RSA-Schlüssel den vom Client erzeugten und verschlüsselten Session Key ermitteln kann.

9.3.4 Authentifizierung zwischen OpenSSH Client und OpenSSH Server

Bei Verwendung des Default-Wertes für die Option *PreferredAuthentication* in der Client-Konfigurationsdatei *ssh_config* (siehe „InterNet Services Benutzerhandbuch“) führt der OpenSSH Client der Reihe nach folgende Authentifizierungsmethoden durch:

1. hostbased-Authentifizierung
2. Public Key-Authentifizierung
3. Passwort-Authentifizierung

Die Verfahren werden der Reihe nach angewendet, bis ein Verfahren erfolgreich authentifiziert hat bzw. bis alle Verfahren gescheitert sind.

Die Public Key-Authentifizierung gestattet die Verwendung von RSA-, DSA-, ECDSA- und Ed25519-Algorithmen. Der OpenSSH Client signiert die Session-Id (zusammen mit anderen Daten) mit seinem privaten Schlüssel (*$HOME/.ssh/id_rsa*, *$HOME/.ssh/id_dsa*, *$HOME/.ssh/id_ecdsa* oder *$HOME/.ssh/id_ed25519*) und sendet das Ergebnis an den OpenSSH Server. Der Server prüft, ob in der Datei *<user home>/.ssh/authorized_keys* ein passender öffentliche Schlüssel enthalten ist. Dabei ist *<user home>* das Home-Verzeichnis desjenigen Users ist, mit dessen Kennung sich der *ssh*-Aufrufer anmelden will). Wenn ja, dann nimmt der Server die Verbindung an.

Der OpenSSH-Client *ssh* authentifiziert den Server, indem er nachschaut, ob zum jeweiligen System in der Datei *$HOME/.ssh/known_hosts* des Users bzw. in der vom Systemadministrator zentral bereitgestellten Datei */etc/ssh/ssh_known_hosts* ein öffentlicher Schlüssel hinterlegt ist, und wenn ja, ob dieser mit dem vom *sshd* gesendeten Host-Key gleichen Typs (RSA/DSA/ECDSA/Ed25519) übereinstimmt.

Die Option *StrictHostKeyChecking* in der Konfigurationsdatei *ssh_config* steuert das Verhalten des Clients für den Fall, dass in den *known_hosts*-Dateien kein passender Eintrag gefunden wird:

– Bei *no* wird der bislang unbekannte Host-Key ohne Nachfrage in *$HOME/.ssh/known_hosts* eingetragen.

– Bei *ask* wird der Benutzer gefragt, ob der Host-Key eingetragen werden soll.

– Bei *yes* wird der Host-Key nie vom Client eingetragen, sondern muss vom Anwender bzw. vom Systemadministrator in die jeweilige *known_hosts*-Datei eingetragen werden.

Eine ausführliche Beschreibung der Option *StrictHostKeyChecking* finden Sie auf den Man Pages von OpenSSH.

9.3.5 Login-Prozess

Nach erfolgreichem Einloggen eines Benutzers führt *sshd* die folgenden Schritte durch:

1. Je nachdem, ob sich der Benutzer an einem Benutzerterminal (tty) eingeloggt hat, verfährt *sshd* wie folgt:
   - Wenn sich der Benutzer an einem tty eingeloggt und kein Kommando eingegeben hat, gibt *sshd* den Zeitpunkt des letzten Login sowie den Inhalt der Datei */etc/motd* aus. Dies setzt jedoch voraus, dass die Ausgabe nicht per Option in der *sshd*-Konfigurationsdatei oder mittels `$HOME/.hushlogin` unterdrückt wurde.
   - Wenn sich der Benutzer an einem tty eingeloggt hat, protokolliert *sshd* den Zeitpunkt des Login.
2. *sshd* prüft, ob die Datei */etc/nologin* existiert. Existiert die Datei, dann druckt *sshd* ihren Inhalt aus. Falls der sich einloggende Benutzer keine Root-Berechtigung besitzt, beendet sich *sshd*.
3. *sshd* wechselt in den Ausführungsmodus mit normalen Benutzerprivilegien.
4. *sshd* richtet eine Basis-Ablaufumgebung ein.
5. *sshd* liest die Datei *$HOME/.ssh/environment*, sofern diese existiert und Benutzer ihre Umgebungsvariablen setzen dürfen. Siehe hierzu die Option `PermitUserEnvironment` in der *sshd*-Konfigurationsdatei.
6. *sshd* wechselt in das Home-Verzeichnis des Benutzers.
7. Falls der Client innerhalb einer X11-Umgebung arbeitet und eine gültige *$DISPLAY*-Variable übermittelt,
   - wird das benutzerspezifische Kommando *$HOME/.ssh/rc* aufgerufen, wobei die X11-Authentifizierungs-Parameter über *stdin* übergeben werden, oder
   - es wird das systemweite *xauth*-Programm aufgerufen. Mangels Verfügbarkeit einer X11-Umgebung für POSIX schlägt dieser Aufruf fehl.
8. *sshd* führt die Shell des Benutzers oder das Benutzer-Kommando aus.

9.3.6 Dateien des OpenSSH Server-Dämons sshd

Neben der Konfigurationsdatei *sshd_config* (siehe Seite 307) verwendet der OpenSSH Dämon *sshd* weitere Dateien, von denen einige nachfolgend beschrieben sind. Eine vollständige Übersicht über alle von *sshd* verwendeten Dateien finden sie auf den Man Pages von OpenSSH.

$HOME/.ssh/authorized_keys

Diese Datei enthält eine Auflistung der Benutzer-Public Keys, die für Public Key-Authentifizierung (siehe Seite 311) zugelassen sind. Die Datei muss für einen Benutzer mit Root-Berechtigung lesbar und sollte nicht für andere Benutzer zugänglich sein.

Mithilfe der Option *AuthorizedKeyFile* in der Datei *sshd_config* (siehe Seite 307) können Sie eine andere Datei spezifizieren, die diese Funktion übernimmt.

Die ausführliche Beschreibung von Syntax und Options der Datei *$HOME/.ssh/authorized_keys* finden Sie auf den Man Pages von OpenSSH.

/etc/ssh/ssh_host_rsa_key
/etc/ssh/ssh_host_dsa_key
/etc/ssh/ssh_host_ecdsa_key
/etc/ssh/ssh_host_ed25519_key

Diese Dateien enthalten die privaten Bestandteile der Host-Keys und dürfen ausschließlich im Besitz von Benutzern mit Root-Berechtigung sein. Nur Benutzer mit Root-Berechtigung dürfen diese Dateien lesen. Die Dateien dürfen für niemanden sonst zugänglich sein. Beachten Sie, dass *sshd* nicht gestartet werden kann, wenn diese Dateien für die Gruppe oder für alle zugänglich sind.

/etc/ssh/ssh_host_rsa_key.pub,
/etc/ssh/ssh_host_dsa_key.pub
/etc/ssh/ssh_host_ecdsa_key.pub
/etc/ssh/ssh_host_ed25519_key.pub

Diese Dateien enthalten die öffentlichen Bestandteile der Host-Keys und sollten für alle Benutzer lesbar, aber nur für Besitzer mit Root-Berechtigung überschreibbar sein. Die in den Dateien abgespeicherten öffentlichen Bestandteile der Host-Keys sollten zu den entsprechenden privaten Bestandteilen der Host-Keys in den Dateien */etc/ssh/ssh_host_rsa_key, /etc/ssh/ssh_host_dsa_key, /etc/ssh/ssh_host_ecdsa_key* und */etc/ssh/ssh_host_ed25519_key* passen.

Die Dateien erfüllen keine wesentlichen Funktionen. Sie vereinfachen lediglich die Anwendung für den Benutzer, indem er ihren Inhalt direkt in *ssh_known_hosts*-Dateien kopieren kann.

Die Dateien werden automatisch während der Installation mithilfe von *ssh-keygen* (siehe Handbuch „interNet Services Benutzerhandbuch“) angelegt.

/etc/ssh/moduli

Diese Datei enthält Diffie-Hellman-Gruppen, die für den „Diffie-Hellman Group Exchange“ verwendet werden. Das Dateiformat ist in moduli (5) auf den Man Pages von OpenSSH beschrieben.

/var/empty

chroot-Verzeichnis, das von *sshd* während Privilege Separation in der Prä-Authentifizierungsphase verwendet wird. Das Verzeichnis sollte keine Dateien enthalten und muss im Besitz eines Benutzers mit Root-Berechtigung sein. Das Verzeichnis darf nicht im Besitz einer Gruppe oder eines Anwenders ohne Root-Berechtigung sein.

/var/run/sshd.pid

Diese Datei enthält die Prozess-ID desjenigen *sshd*, der den Port nach Verbindungsanforderungen abhorcht. Wenn mehrere *sshd*-Dämonen gleichzeitig an verschiedenen Ports horchen, enthält die Datei die ID des zuletzt gestarteten Dämons. Der Inhalt dieser Datei ist nicht vertraulich und darf allgemein lesbar sein.

/etc/nologin

Wenn diese Datei existiert, erlaubt *sshd* das Login ausschließlich Benutzern mit Root-Berechtigung. Der Inhalt der Datei wird jedem angezeigt, der versucht, sich einzuloggen, wobei Login-Versuche von Benutzern ohne Root-Berechtigung abgewiesen werden. Die Datei sollte allgemein lesbar sein.

/etc/hosts.allow, /etc/hosts.deny

In dieser Datei sind Zugriffskontrollen definiert, die von TCP-Wrappern durchgeführt werden. Weitere Informationen finden Sie unter hosts_access (5) auf den Man Pages von OpenSSH.

9.4 BS2000-spezifische Einschränkungen

Beim Arbeiten mit OpenSSH im BS2000-Umfeld sind die nachfolgend beschriebenen Besonderheiten zu beachten.

Verwendung einer eigenen Resolver-Bibliothek anstelle vom BCAM-Hostnamen

Zur Auflösung von Hostnamen verwendet OpenSSH(BS2000) weder die BCAM-Host-Tabellen, noch den Resolver auf BS2000-Seite, der in der Datei *$TSOS.SYSDAT.SOCKETS.nnn.SOC6.RESOLV* bzw *$TSOS.SYSDAT.LWRESD.nnn.RESOLV.CONF* konfiguriert wird, sondern die DNS-Resolver-Bibliothek von TCP-IP-SV:DNS(BS2000) (siehe Kapitel „DNS“ auf Seite 209). Dadurch ist der *sshd*-Dämon unabhängig von der eingesetzten BCAM-Version und verhält sich konform zu Anwendungen wie TCP-IP-SV:DNS(BS2000) und APACHE(BS2000). Voraussetzung ist, dass die Datei */etc/resolv.conf* existiert und die Adresse mindestens eines gültigen DNS Name Servers enthält.

Bei der Installation von TCP-IP-SV:OPENSSH wird überprüft, ob die Datei */etc/resolv.conf* vorhanden ist. Außerdem besteht die Möglichkeit, eine evtl. vorhandene Konfiguration aus *$TSOS.SYSDAT.LWRESD.nnn.RESOLV.CONF* oder *$TSOS.SYSDAT.SOCKETS.nnn.SOC6.RESOLV* in eine neu erstellte */etc/resolv.conf* zu übernehmen.

Auch in der *lastlog*-Datei wird der vollständige DNS-Name bzw. die vollständige IPv4- oder IPv6-Adresse eingetragen, um feststellen zu können, von wo aus ein Remote Login durchgeführt wurde. Der Hostname wird dabei in der Schreibweise verwendet, in der er vom Name Server geliefert wurde, also meistens in Kleinbuchstaben. Dieses Verhalten ist kompatibel zu anderen Unix-Plattformen, unterscheidet sich jedoch vom Verhalten des POSIX-*rlogin*. Der POSIX-*rlogin* verwendet BCAM-Namen statt DNS-Namen, und schreibt diese immer in Großbuchstaben.

Bei von POSIX ausgehenden *ssh*-Verbindungen oder *ssh-keyscan*-Aufrufen bewirkt das geschilderte Verhalten außerdem, dass Hostnamen, die nicht in der DNS-Resolver-Bibliothek von TCP-IP-SV:DNS(BS2000), aber in der BCAM-Host-Tabelle eingetragen sind, für *ssh* und *ssh-keyscan* unsichtbar und deshalb ungültig sind.

Deshalb müssen Sie in diesem Fall

- die zugehörigen IP-Adressen angeben oder
- einen in der DNS-Resolver-Bibliothek von TCP-IP-SV:DNS(BS2000) eingetragenen Namen verwenden oder
- die BCAM-Namen „von Hand“ in die Datei */etc/hosts* eintragen.

Eingabe-Aufforderung bei leerem Passwort

Gewöhnliche Unix-Systeme verlangen kein Passwort, wenn Sie sich per *login* oder *slogin* an einer Kennung ohne Passwort anmelden. Der POSIX *rlogin* verlangt jedoch auch bei einer Kennung ohne Passwort eine Passwort-Eingabe. Dieses Verhalten führt jedoch nicht zu einer höheren Sicherheit, da es gleichzeitig möglich ist, für dieselbe Kennung ein *rsh*-Kommando ohne Passwort abzusetzen.

OpenSSH verhält sich hier wie die anderen Unix-Systeme und fragt nicht nach einem leeren Passwort. Da in OpenSSH jedoch standardmäßig ein Login zu Kennungen ohne Passwort gesperrt ist, müssen Sie in diesem Fall in der Konfigurationsdatei */etc/ssh/sshd_config* die Direktive *PermitEmptyPasswords* auf „yes“ setzen.

Groß-/Kleinschreibung des Benutzernamens

Im BS2000 und BS2000 POSIX wird, anders als in Unix-Betriebssystemen, beim Benutzernamen nicht zwischen Groß- und Kleinschreibung unterschieden. Somit kann sich der Benutzer „Benutzername“ im BS2000 und POSIX als „benutzername“, „BENUTZERNAME“ oder auch „beNuTzErNaMe“ anmelden. Der Name des angemeldeten Benutzers wird in der Datei */var/adm/utmp* registriert. Mit dem `who`-Kommando können Sie sich den Benutzernamen anzeigen lassen.

Während rlogin den Benutzernamen in Großbuchstaben einträgt, verwendet OpenSSH den Benutzernamen in Kleinbuchstaben (wie auf Unix-Betriebssystemen üblich).

10 Mail-Server in POSIX

Das Versenden und Empfangen von elektronischer Post (Mail) gehört zu den wichtigsten Diensten im Internet. Die Rolle der Postämter übernehmen dabei die Mail-Server, auch Mail Transfer Agenten (MTA) genannt. Mail-Server erledigen den Transfer der Mails über das Netz und besorgen deren Zustellung in Postfächer (Mailboxen).

Mail-Benutzeragenten, auch Mail User Agenten (MUA) genannt, bieten benutzerfreundliche Schnittstellen für die Erledigung der folgenden Aufgaben:

- Verfassen und Senden von Mails
- Zugriff auf die Mailboxen
- Darstellung und Weiterverarbeitung der empfangenen elektronischen Post

Man Pages

Das vorliegende Kapitel basiert teilweise auf den Manual Pages (Man Pages) von Postfix und IMAP/POP3. An den entsprechenden Stellen des Kapitels, wie z.B. bei der Beschreibung von Programmen und Parametern/Options wird auf die Man Pages verwiesen, die weitergehende Informationen liefern. Sie finden die jeweils aktuellsten Man Pages im Internet unter:

- *www.postfix.org/* (Postfix)
- *www.washington.edu/imap/* (IMAP/POP3)

Außerdem finden Sie die Man Pages von Postfix und IMAP/POP3 nach Installation dieser Komponenten auf Ihrem Server.

Die Man Pages von Postfix finden Sie auf Ihrem Server

- unter *<installationspfad>/readme/ MAIL.postfix/html/* als HTML-Dateien,
- unter *<installationspfad>/readme/ MAIL.postfix/pdf/* als PDF-Dateien,
- unter *<installationspfad>/readme/ MAIL.postfix/text/* als Text-Dateien.

(Standard-Installationspfad für Postfix: */opt/MAIL/postfix/*)

Die Man Pages von IMAP/POP3 finden Sie auf Ihrem Server

- unter *<installationspfad>/readme/ MAIL.imap/html/* als HTML-Dateien,
- unter *<installationspfad>/readme/ MAIL.imap/text/* als Text-Dateien.

(Standard-Installationspfad für IMAP/POP3: */opt/MAIL/imap/*)

Wenn im weiteren Verlauf dieses Kapitel wiederholt auf die Man Pages von Postfix bzw. IMAP/POP3 verwiesen wird, sind im Einzelnen diese Quellen gemeint. Dabei sind die mit dem Produkt ausgelieferten Man Pages zu bevorzugen, da sich diese Man Pages auf die im Produkt enthaltene Software-Version beziehen.

10.1 Überblick

Der elektronische Postdienst im Internet basiert auf dem Simple Mail Transfer Protocol (SMTP), das in RFC 5321 definiert ist. Während ursprünglich nur reine Textnachrichten übermittelt werden konnten, kann heute über den MIME-Mechanismus (Multipurpose Internet Mail Extensions, RFC 2045 bis 2049) ein breites Spektrum von Formaten, z.B. Bilder, übermittelt werden. Mail-Server, die den elektronischen Postdienst auf der Basis des SMTP-Protokolls abwickeln, werden auch als SMTP-Server bezeichnet.

Die interNet Services im BS2000 verwenden als SMTP-Server das in das BS2000 portierte Produkt Postfix in der Version 3.1.2. Diese Version gilt für den Erstellungszeitpunkt dieses Handbuchs, im Rahmen von Korrekturpaketen kann eine Rebasierung auf eine neuere Version stattfinden. Dieser von Wietse Venema erstellte Open Source SMTP-Server zeichnet sich insbesondere durch hohe Performance, einfache Administrierbarkeit und ein hohes Maß an Sicherheit aus. Darüber hinaus gewährleistet die partielle Kompatibilität von Postfix zu dem in der interNet Value Edition enthaltenen Programm Sendmail™ den unkomplizierten Umstieg von Sendmail auf Postfix. Näheres hierzu finden Sie im Abschnitt „Umstieg von Sendmail auf Postfix“ auf Seite 351.

Für den Zugriff auf Mailboxen, die auf einem fernen Server liegen, werden von den Mail User Agenten die folgenden Protokolle verwendet:

- Internet Mail Access Protocol (IMAP, RFC 2060 u.a.)
- Post Office Protocol Version 3 (POP3, RFC 1939)

Die mit interNet Services ausgelieferten IMAP- und POP3-Server unterstützen die Protokolle IPv6 und TLS (siehe Seite 333).

Für das Versenden von Mails aus BS2000 enthält die Liefereinheit interNet Services einen einfachen Benutzer-Agenten, den Mail-Sender (siehe Handbuch „interNet Services Benutzerhandbuch“). Für die automatisierte Verarbeitung von empfangenen Mails gibt es in interNet Services einen Mail-Reader auf IMAP/POP3-Basis. Falls POSIX-SH installiert ist, steht in POSIX außerdem ein einfacher lokaler Benutzeragent (Mailx) für das Versenden und die Verarbeitung von Textnachrichten im BS2000 zur Verfügung.

10.2 Funktionalität

Ein SMTP-Server bzw. Mail Transfer Agent (MTA) ist ein Mail-Server für die Übertragung von Mails im Internet auf Basis des Simple Mail Transfer Protocol (SMTP). Dabei kann der SMTP-Server als Mail-Relay oder als Mail-Endsystem fungieren. Als weitere wesentliche Funktion ermöglicht der SMTP-Server das Einrichten von Verteilerlisten und Nachsendeaufträgen mithilfe von Aliasnamen. Aliasnamen gestatten die Ersetzung des Benutzeranteils einer lokalen Empfängeradresse durch eine oder mehrere Empfängeradressen.

Für die Wahl einer geeigneten Route zu einem Endsystem nutzt der SMTP-Server den Domain Name Service (DNS).

Der SMTP-Server erhält Nachrichten entweder von einem anderen SMTP-Server oder von einem Mail User Agenten (MUA). Aufgrund der Empfängeradresse(n) der Nachricht wird diese über eine TCP/SMTP-Verbindung an einen anderen SMTP-Server und/oder einen lokalen Mail-Zustellagenten (Mail Delivery Agent, MDA) übergeben.

Besondere Bedeutung hat dabei der lokale MDA, der die Nachrichten in speziellen Dateien (Mailboxen) abspeichert. Mithilfe des MUA lassen sich die in den lokalen Mailboxen befindlichen Nachrichten weiterverarbeiten (lesen, weiterleiten, sortieren, sichern, beantworten, löschen). Darüber hinaus ermöglicht es der MUA, Nachrichten zu erstellen und an den lokalen SMTP-Server zur Zustellung zu übergeben. Einige MUAs können auch über eine TCP/SMTP-Verbindung Nachrichten an einen fernen SMTP-Server übergeben.

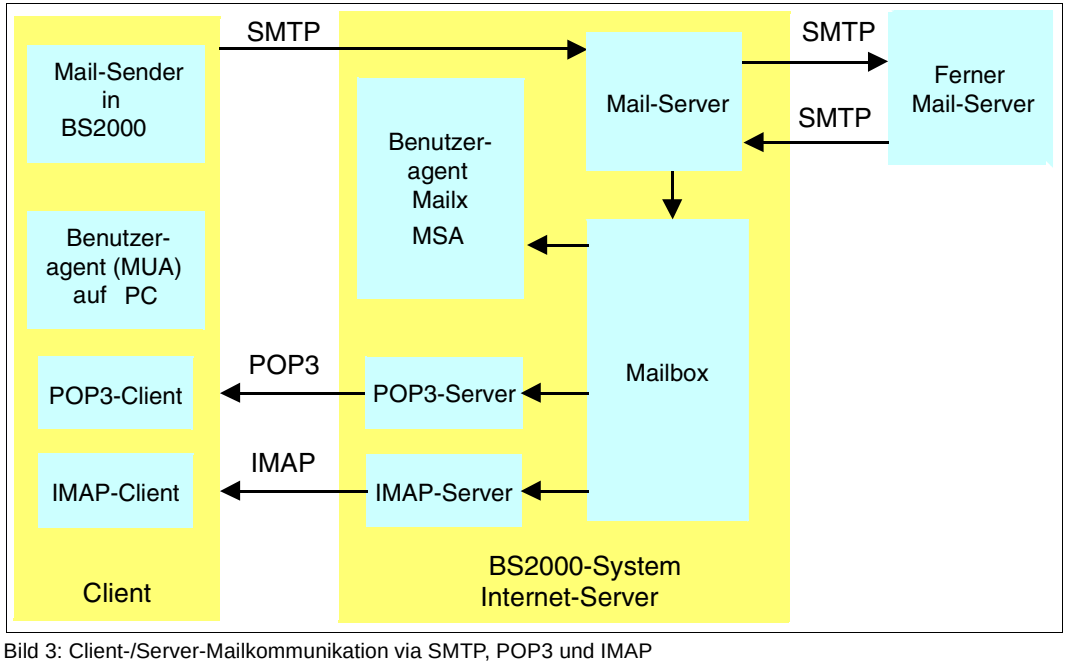


Bild 3: Client-/Server-Mailkommunikation via SMTP, POP3 und IMAP

Der IMAP- und POP3- Mechanismus erlaubt einem Client-System, insbesondere wenn dieses nicht mit einem SMTP-Server (MTA) ausgestattet ist, den Zugriff auf die Mailboxen des SMTP-Server-Systems. Hierzu werden auf dem SMTP-Server-System ein IMAP- und ein POP3-Server installiert. Beispielsweise können dann Clients (z.B. Outlook oder Mozilla/Thunderbird), die auf einem fernen System ablaufen, Nachrichten in den Mail-Boxen des Server-Systems lesen und löschen.

Bei fernen Benutzeragenten ist darauf zu achten, dass für die USER eine Abrechnungsnummer zur Abrechnung einer POSIX-Remote-Login-Session existiert (BS2000-Kommando /ADD-USER bzw. /MODIFY-USER-ATTRIBUTES POSIX-RLOGIN-DEFAULT=*YES).

IMAP und POP3 unterscheiden sich wie folgt:

- Bei IMAP verbleiben die Mails auf dem Server-Rechner, wo auch das Backup der Mails stattfindet.
- Bei POP3 werden die Mails standardmäßig auf den Client-Rechner heruntergeladen und dort gespeichert.

Aufbau der Nachrichten

Der Aufbau der Nachrichten ist in RFC 822 festgelegt. Nachrichten bestehen aus dem Nachrichtenkopf (Header) und dem Nachrichtentext. Kopf und Text werden durch genau eine Leerzeile getrennt.

Sowohl Nachrichtenkopf als auch Nachrichtentext bestehen aus lesbaren Zeichen im ASCII-Format. Der Nachrichtenkopf besteht aus mehreren Deklarationen, die im Prinzip jeweils in einer Zeile stehen, zur besseren Lesbarkeit aber auf mehrere Zeilen verteilt werden können. Die Deklarationen bestehen aus einem Namen und aus einem Textteil, dessen Format durch den Namen festgelegt ist. Abhängig vom Namen, aber auch von anderen Deklarationen, kann eine bestimmte Art von Deklarationen genau einmal, gar nicht, höchstens einmal oder beliebig oft in einem Nachrichtenkopf vorkommen.

Die meisten Namen sind in RFC 5322 festgelegt. RFC 1522 definiert einige Erweiterungen. Für private Erweiterungen sind Namen, die mit „X-“ beginnen, vorgesehen.

Mithilfe des MIME-Mechanismus können in den Nachrichtentext neben reinem Text auch Binär-Daten aufgenommen werden. Der MIME-Mechanismus definiert zusätzliche Nachrichtenkopf-Deklarationen und ist in den RFCs 2045 bis 2049 beschrieben.

10.3 Mail-Server installieren und deinstallieren

Dieser Abschnitt beschreibt Installation und Deinstallation des SMTP-Servers (Postfix-Servers) sowie des IMAP- und des POP3-Servers.

Die Mail-Server belegen standardmäßig die folgenden Portnummern:

Port		Protokoll	Erläuterung
25	tcp/udp	SMTP	Simple Mail Transfer Protocol
110	tcp/udp	POP3	Post Office Protocol - Version 3
143	tcp/udp	IMAP	Internet Message Access Protocol
993	tcp/udp	IMAPS	IMAP über TLS/SSL
995	tcp/udp	POP3S	POP3 über TLS/SSL

10.3.1 Postfix-Server (SMTP-Server) installieren und deinstallieren

Den Postfix-Server installieren Sie als ein POSIX-Programmpaket per Package-Installation mit dem POSIX-Installationsprogramm (siehe Handbuch „POSIX Grundlagen für Anwender und Systemverwalter“).

Installationsvoraussetzungen

Für Installation und Betrieb des Postfix-Servers muss die PLAM-Bibliothek SINLIB.MAIL.*nnn*.POSTFIX shareable zur Verfügung stehen. Das Subsystem POSIX muss gestartet sein.

Für einen störungsfreien Betrieb ist der Postfix-Server auf eine korrekt funktionierende DNS-Funktionalität angewiesen. Da der Server nach Abschluss der Installation automatisch gestartet werden kann, sollten Sie bereits vor Installationsbeginn eine korrekt funktionierende DNS-Funktionalität sicherstellen. Dies erreichen Sie über die korrekte Konfiguration der Datei */etc/resolv.conf* und der dort referenzierten DNS-Server (siehe Abschnitt „DNS Resolver konfigurieren“ auf Seite 228).

Bei der Installation von MAIL:POSTFIX überprüft, ob die Datei */etc/resolv.conf* vorhanden ist. Außerdem besteht die Möglichkeit, eine evtl. vorhandene Konfiguration aus *$TSOS.SYSDAT.LWRESD.nnn.RESOLV.CONF* oder *$TSOS.SYSDAT.SOCKETS.nnn.SOC6.RESOLV* in eine neu erstellte */etc/resolv.conf* zu übernehmen.

Bei nicht korrekt funktionierender DNS-Funktionalität kann sich wegen DNS-Timeout die Installation des Postfix-Servers verzögern und ein fehlerhaftes Verhalten des Postfix-Servers resultieren.

Installation starten

Der Postfix-Server muss privilegiert ablaufen. Installieren Sie deshalb den Postfix-Server mit dem POSIX-Installationskommando unter der Kennung SYSROOT bzw. TSOS (UID=0, GID=0):

- Starten Sie die Installation: `/START-POSIX-INSTALLATION`
- Wählen Sie die folgende Funktion aus: `Install packages on POSIX`
- Spezifizieren Sie in der daraufhin angezeigten Bildschirmausgabe die folgenden Werte:

IMON support?:	`Y`
name of product:	`MAIL`
package of product:	`POSTFIX`

Den im weiteren Verlauf der Installation angezeigten Installationspfad können Sie modifizieren. Es empfiehlt sich jedoch, die Voreinstellung */opt/MAIL/postfix* beizubehalten.

Sofern noch eine Version der Liefereinheit interNet Value Edition installiert ist, gibt das POSIX-Installationsprogramm eine entsprechende Fehlermeldung aus.

Eine Postfix-Installation ist grundsätzlich auch bei einer installierten interNet Value Edition möglich. In diesem Fall müssen Sie jedoch sicherstellen, dass kein *sendmail*-Dämon aktiv ist, der bei der Portnummern-Belegung mit dem Postfix-Server konkurriert. In der Regel betrifft dies die Portnummer 25.

- Brechen Sie die Postfix-Installation durch Drücken der K2-Taste ab, wenn Sie interNet Value Edition vor der Postfix-Installation deinstallieren wollen.
- Setzen Sie die Postfix-Installation durch Drücken der DUE-Taste fort, wenn Sie interNet Value Edition nicht zuvor deinstallieren wollen.

Anschließend prüft das POSIX-Installationsprogramm das */opt*-Dateisystem auf ausreichenden Speicherplatz und spielt alle Dateien aus der PLAM-Bibliothek ins POSIX-Dateisystem ein bzw. erzeugt Verweise auf PLAM-Bibliothekselemente. Nach Einspielung aller Dateien startet das POSIX-Installationsprogramm automatisch ein Post-Installations-Skript, das die rechner-spezifische Einrichtung des Postfix-Servers abwickelt.

Ablauf des Post-Installations-Skripts

Im Einzelnen führt das Post-Installations-Skript die folgenden Schritte durch.

1. Zunächst prüft das Post-Installations-Skript, ob bereits eine Benutzerkennung POSTFIX existiert.

   Wenn dies der Fall ist und zusätzlich die beiden folgenden Bedingungen erfüllt sind, wird eine Fehlermeldung ausgegeben und die Ausführung des Post-Installations-Skripts abgebrochen:

   – POSTFIX User Number ≤ Default POSIX User Number

   – POSTFIX Group Number ≤ Default POSIX Group Number

2. Falls die Benutzerkennung POSTFIX noch nicht existiert, richtet das Post-Installations-Skript diese Benutzerkennung mit den folgenden Attributen ein:

   – zufälliges Passwort
   – BS2000-Account: SYSACC
   – Address-Space-Limit: 32 MB

   Unter POSIX erhält diese Kennung das Home-Verzeichnis */var/empty* und die Login-Shell */bin/false*, da für die Kennung POSTFIX eine Login-Möglichkeit weder erforderlich noch wünschenswert ist.

3. Das Post-Installations-Skript richtet eine POSIX-Gruppe MAILDROP ein.

4. Falls die Benutzerkennung NOBODY noch nicht existiert, richtet das Post-Installations-Skript diese Benutzerkennung mit den folgenden Attributen ein:

   – zufälliges Passwort
   – BS2000-Account: SYSACC
   – Address-Space-Limit: 32 MB

   Unter POSIX erhält diese Kennung das Home-Verzeichnis */var/empty* und die Login-Shell */bin/false*, da für die Kennung NOBODY eine Login-Möglichkeit weder erforderlich noch wünschenswert ist.

5. In der Startup-Datei */etc/profile* der POSIX-Shell wird die PATH-Angabe für den Benutzer mit der User-Nummer 0 (SYSROOT bzw. TSOS) um die Verzeichnisse <*installationspfad*>*/bin* und <*installationspfad*>*/sbin* erweitert. Falls eine C-Shell (*csh* oder *tcsh*) installiert ist, verfährt das Post-Installations-Skript mit der *csh*-Startup-Datei (*/etc/.login* bzw. */etc/csh.login*) analog.

6. Falls die Default-Job-Klasse für Batch-Jobs der SYSROOT-Kennung ein JOB-CLASS-LIMIT < 20 hat, wird eine Warnung ausgegeben.

7. Falls ADDRESS-SPACE-LIMIT < 32 MB für SYSROOT beträgt, wird eine Warnung ausgegeben.

8. Falls ADDRESS-SPACE-LIMIT < 32 MB für POSTFIX beträgt, wird eine Warnung ausgegeben.
9. Falls für POSTFIX kein POSIX-RLOGIN-DEFAULT gesetzt ist, wird eine entsprechende Fehlermeldung ausgegeben.
10. Falls SYSROOT keine Leseberechtigung für die Installationsbibliothek (z.B. *SINLIB.MAIL.nnn.POSTFIX*) besitzt, wird eine entsprechende Fehlermeldung ausgegeben.
11. Durch Inspektion der DNS-Resolver-Konfigurationsdateien */etc/resolv.conf* und *$TSOS.SYSDAT.SOCKETS.nnn.SOC6.RESOLV* bzw. *$TSOS.SYSDAT.LWRESD.nnn.RESOLV.CONF* versucht das Post-Installations-Skript den Domänen-Namen des Systems zu bestimmen.
12. Durch Aufruf von *postconf -e* setzt das Post-Installations-Skript in der Postfix-Konfigurationsdatei */etc/postfix/main.cf* die folgenden Parameter: *mailq_path*, *newaliases_path*, *daemon_directory*, *readme_directory*, *html_directory*, *command_directory*, *sendmail_path*, *manpage_directory*, *mail_owner*, *setgid_group*, *config_directory* und *queue_directory*. Wurde in Schritt 11 eine Domäne gefunden, dann wird außerdem der Parameter *mydomain* gesetzt.
13. Das Post-Installations-Skript ruft das Postfix-eigene Postinstall-Skript */etc/postfix/post-install* auf.
14. Handelt es sich um eine Postfix-Erst-Installation, d.h. es existiert kein Konfigurations-Sicherungsverzeichnis */etc/postfix.sav* einer vorangegangenen Postfix-Installation, dann prüft das Post-Installations-Skript, ob eine Datei */etc/mail/aliases* oder */etc/aliases* existiert. Existiert eine dieser Dateien, dann kopiert das Post-Installations-Skript die zuerst gefundene Datei nach */etc/postfix/aliases* und trägt in die Datei */etc/postfix/main.cf* die folgenden Parameter-Definitionen ein:

    ```
    alias_maps = hash:/etc/postfix/aliases
    alias_database = hash:/etc/postfix/aliases
    ```

15. Sofern keine schwerwiegenden Fehler entdeckt wurden, ruft das Post-Installations-Skript mit */etc/init.d/MAIL.postfix start* (abhängig von der Beantwortung der Installationsabfrage AutoStartPostfix) das allgemeine POSIX-Start-Skript für Postfix auf, das den Postfix-Server unter SYSROOT startet.

    Das Skript */etc/init.d/MAIL.postfix* bestimmt automatisch die für SYSROOT maximal zulässigen Werte für JOB-CLASS, ACCOUNT, START und MAXIMUM CPU LIMIT. Mit diesen Werten startet das Skript einen Enter-Job mit dem Job-Namen POSTFIX.

    Der Postfix-Server protokolliert wichtige Meldungen per *syslog*-Mechanismus in der Datei */var/adm/syslog*. Zusätzlich notiert der Postfix-Server Probleme, die beim Start des Enter-Jobs auftreten, in der Datei *var/adm/postfix_startup.log*.

Installation abschließen

Nach erfolgreicher Installation führen Sie die weiteren, eventuell erforderlichen Aktivitäten in der POSIX-Shell unter der Kennung TSOS aus. Zu diesem Zweck starten Sie die POSIX-Shell unter der Kennung TSOS mit dem BS2000-Kommando `/START-POSIX-SHELL`.

Vom Postfix-Server verwendete Dateien und Verzeichnisse

Nachfolgend finden Sie eine Auflistung der wichtigsten vom Postfix-Server verwendeten Dateien und Verzeichnisse. Falls Sie einen vom Standard-Postfix-Installationspfad abweichenden Installationspfad verwenden, sind die in der Tabelle angegebenen Pfadnamen entsprechend anzupassen.

Name	Typ	Erläuterung
/opt/MAIL	Verzeichnis	
/opt/MAIL/postfix	Verzeichnis	Standard-Postfix-Installationsverzeichnis
/opt/MAIL/postfix/bin	Verzeichnis	Links auf Sendmail-Kompatibilitätsprogramm
/opt/MAIL/postfix/bin/mailq	Link	Ausgeben der Mail-Queue
/opt/MAIL/postfix/bin/newaliases	Link	Aktualisieren der Alias-Index-Datei
/opt/MAIL/postfix/libexec/postfix	Verzeichnis	Dämon-Programme
/opt/MAIL/postfix/libexex/postfix/local	Programm	Lokaler Zustell-Agent
/opt/MAIL/postfix/libexec/postfix/master	Programm	Zentrales Verwaltungsprogramm
/opt/MAIL/postfix/libexec/postfix/pickup	Programm	Verarbeitung lokal eingestellter Mail
/opt/MAIL/postfix/libexec/postfix/qmgr	Programm	Warteschlangen-Verwaltung
/opt/MAIL/postfix/libexec/postfix/smtpd	Programm	Entgegennahme von Mails mithilfe von SMTP
/opt/MAIL/postfix/libexec/postfix/smtp	Programm	Weitergabe von Mails per SMTP
/opt/MAIL/postfix/readme	Verzeichnis	Online-Dokumentation
/opt/MAIL/postfix/sbin	Verzeichnis	Verwaltungsprogramme
/opt/MAIL/postfix/sbin/postalias	Programm	Erzeugen/Abfragen der Alias-Index-Datei
/opt/MAIL/postfix/sbin/postcat	Programm	Ausgabe von Dateien in Warteschlangen
/opt/MAIL/postfix/sbin/postconf	Programm	Anzeige/Änderung von Postfix-Parametern
/opt/MAIL/postfix/sbin/postdrop	Programm	Schreiben von Mails in maildrop-Verzeichnis für Auslieferung durch Postfix
/opt/MAIL/postfix/sbin/postfix	Programm	Starten/Stoppen des Postfix-Systems
/opt/MAIL/postfix/sbin/postmap	Programm	Erzeugen/Abfragen von Index-Dateien

Name	Typ	Erläuterung
/opt/MAIL/postfix/sbin/postqueue	Programm	Warteschlangen-Verwaltung durch den Systemverwalter
/opt/MAIL/postfix/sbin/postsuper	Programm	Erteilt dem Systemverwalter super-user-Zugriff auf Warteschlangen
/opt/MAIL/postfix/sbin/sendmail	Programm	Sendmail-Kompatibilitätsprogramm
/opt/MAIL/postfix/share	Verzeichnis	Online-Dokumentation in Form von Man Pages
/etc/postfix	Verzeichnis	Verzeichnis für Postfix-Konfigurationsdateien
/etc/postfix/master.cf	Textdatei	Konfiguration für Master Dämon
/etc/postfix/main.cf	Textdatei	zentrale Postfix-Konfigurationsdatei
/var/spool/postfix	Verzeichnis	Verzeichnis für Warteschlangen und Lock-Dateien
/var/mail	Verzeichnis	Verzeichnis für Mailboxen
/var/mail/USER	Mailbox-Datei	Mailbox für den Benutzer USER
/etc/rc0.d/K17MAIL.postfix	Link	Link auf Start/Stop-Skript
/etc/rc2.d/S97MAIL.postfix	Link	Link auf Start/Stop-Skript
/etc/init.d/MAIL.postfix	Skript	Start/Stop-Skript

Postfix-Server (SMTP-Server) deinstallieren

Deinstallieren Sie den Postfix-Server mit dem POSIX-Installationskommando unter der Kennung SYSROOT bzw. TSOS (UID=0, GID=0):

- Starten Sie die Deinstallation: `/START-POSIX-INSTALLATION`
- Wählen Sie die folgende Funktion aus: `Delete packages from POSIX`
- Markieren Sie in der daraufhin angezeigten Bildschirmausgabe die Zeile, die die folgenden Werte enthält, und aktivieren Sie Ihre Auswahl durch Drücken der DUE-Taste:

```
Product             Version Package
...                 ...     ...
MAIL                nnn     POSTFIX
```

- Folgen Sie den weiteren Anweisungen des Tools.

Falls Postfix-Konfigurationsdateien gegenüber ihrem Stand zum Zeitpunkt der Installation verändert wurden, werden diese Dateien im Verzeichnis */etc/postfix.sav* gesichert. Bei einer erneuten Installation von POSTFIX zu einem späteren Zeitpunkt werden dann anstelle der mitgelieferten Standard-Konfigurationsdateien die Dateien aus dem Sicherungsverzeichnis */etc/postfix.sav* verwendet.

10.3.2 IMAP- und POP3-Server installieren und deinstallieren

IMAP- und POP3-Server installieren Sie als ein POSIX-Programmpaket per Package-Installation mit dem POSIX-Installationsprogramm (siehe Handbuch „POSIX Grundlagen für Anwender und Systemverwalter“).

Installationsvoraussetzungen

Für Installation und Betrieb von IMAP- und POP3-Server muss die PLAM-Bibliothek SINLIB.MAIL.*nnn*.IMAP shareable und read-only zur Verfügung stehen. Das Subsystem POSIX muss gestartet sein.

Installation starten

IMAP- und POP3-Server müssen in POSIX privilegiert ablaufen. Installieren Sie deshalb IMAP- und POP3-Server mit dem POSIX-Installationskommando unter der Kennung SYSROOT bzw. TSOS (UID=0, GID=0):

- Starten Sie die Installation: `/START-POSIX-INSTALLATION`
- Wählen Sie die folgende Funktion aus: `Install packages on POSIX`
- Spezifizieren Sie in der daraufhin angezeigten Bildschirmausgabe die folgenden Werte:

IMON support?:	`Y`
name of product:	`MAIL`
package of product:	`IMAP`

Den im weiteren Verlauf der Installation angezeigten Installationspfad können Sie modifizieren. Es empfiehlt sich jedoch, die Voreinstellung */opt/MAIL/imap* beizubehalten.

Sofern noch eine Version der Liefereinheit interNet Value Edition installiert ist, gibt das POSIX-Installationsprogramm eine entsprechende Fehlermeldung aus.

Eine IMAP- und POP3-Installation ist grundsätzlich auch bei einer installierten interNet Value Edition möglich. Die IMAP- und POP3-Dämon-Programme werden dann durch die aktuellen Versionen ersetzt.

- Brechen Sie die IMAP/POP3-Installation durch Drücken der K2-Taste ab, wenn Sie interNet Value Edition vor der IMAP/POP3-Installation deinstallieren wollen.
- Setzen Sie die IMAP/POP3-Installation durch Drücken der DUE-Taste fort, wenn Sie interNet Value Edition nicht zuvor deinstallieren wollen.

Anschließend prüft das POSIX-Installationsprogramm das */opt*-Dateisystem auf ausreichenden Speicherplatz und spielt alle Dateien aus der PLAM-Bibliothek ins POSIX-Dateisystem ein bzw. erzeugt Verweise auf PLAM-Bibliothekselemente.

Vom IMAP- und POP3-Server verwendete Dateien und Verzeichnisse

Nachfolgend finden Sie eine Auflistung der wichtigsten vom IMAP- und POP3-Server verwendeten Dateien und Verzeichnisse. Falls Sie einen vom Standard-Postfix-Installationspfad abweichenden Installationspfad verwenden, sind die in der Tabelle angegebenen Pfadnamen entsprechend anzupassen.

Name	Typ	Erläuterung
/opt/MAIL	Verzeichnis	
/opt/MAIL/imap	Verzeichnis	Standard-IMAP-Installationsverzeichnis
/opt/MAIL/imap/readme	Verzeichnis	Online-Dokumentation
/opt/MAIL/imap/sbin	Verzeichnis	Dämon-Programme
/opt/MAIL/imap/sbin/imapd	Programm	IMAP-Dämon
/opt/MAIL/imap/sbin/ipop3d	Programm	POP3-Dämon
/opt/MAIL/imap/share	Verzeichnis	Online-Dokumentation in Form von Man Pages
/usr/sbin/in.imapd	Link	Link auf IMAP-Dämon
/usr/sbin/in.ipop3d	Link	Link auf POP3-Dämon
/etc/imap	Verzeichnis	Verzeichnis für IMAP/POP3-Dateien (X.509-Zertifikate, private Schlüssel)
/etc/imap/MAKE.CERT.sh	Skript	Skript zur Erzeugung von X.509-Zertifikatsanträgen und X.509-Testzertifikaten
/etc/imap/certs	Verzeichnis	Verzeichnis für X.509-Zertifikate
/etc/imap/private	Verzeichnis	Verzeichnis für private Schlüssel
/etc/inet	Verzeichnis	Verzeichnis für Konfigurationsdateien (insbesondere *inetd*)
/etc/inet/services	Textdatei	Zuordnung von Service-Namen zu Portnummern
/etc/inet/inetd.conf	Textdatei	Konfigurationsdatei für *inetd*
/var/mail	Verzeichnis	Verzeichnis für Mailboxen
/var/mail/USER	Mailbox-Datei	Mailbox für den Benutzer USER

IMAP-Server und POP3-Server deinstallieren

Deinstallieren Sie den IMAP- und POP3-Server mit dem POSIX-Installationskommando unter der Kennung SYSROOT bzw. TSOS (UID=0, GID=0):

- Starten Sie die Deinstallation: `/START-POSIX-INSTALLATION`
- Wählen Sie die folgende Funktion aus: `Delete packages from POSIX`
- Markieren Sie in der daraufhin angezeigten Bildschirmausgabe die Zeile, die die folgenden Werte enthält, und bestätigen Sie Ihre Auswahl durch Drücken der DUE-Taste:

```
Product              Version Package=IMAP
...                  ...     ...
MAIL                  nnn     IMAP
```

- Folgen Sie den weiteren Anweisungen des Tools.

10.4 Mail-Server in Betrieb nehmen

Dieser Abschnitt behandelt die folgenden Themen:

- Inbetriebnahme des Postfix-Servers (SMTP-Servers)
- Inbetriebnahme des IMAP- und des POP3-Servers
- Nutzung TLS/SSL-gesicherter Verbindungen durch Postfix-, IMAP- und POP3-Server

10.4.1 Postfix-Server (SMTP-Server) in Betrieb nehmen

Nach der Installation des Postfix-Servers können Sie die Konfigurationsdateien */etc/postfix/master.cf* und */etc/postfix/main.cf* anpassen.

In der Regel ist der Postfix-Server auch ohne Änderung der Konfigurationsdateien einsatzbereit, da das Installationsprogramm versucht, anlagen-spezifische Parameter, wie z.B. den Domänennamen des Systems, automatisch über Systemaufrufe sowie durch Inspektion der Konfigurationsdatei */etc/resolv.conf* des DNS-Resolvers zu ermitteln und in der Konfigurationsdatei *main.cf* zu speichern. Deshalb sollten Sie bereits vor der Installation den Domänennamen des Systems (z.B. *systemx.mycompany.com*) sowie eventuelle DNS-Alias-Namen beim zuständigen DNS-Server hinterlegen. Zu diesem Zweck müssen Sie die Datei */etc/resolv.conf* entsprechend konfigurieren (siehe Abschnitt „DNS Resolver konfigurieren“ auf Seite 228).

Wenn die automatische Postfix-Konfiguration erfolgreich durchgeführt werden konnte, wird der Postfix-Server nach Abschluss der Installation abhängig von der Beantwortung der Installationsabfrage AutoStartPostfix gestartet.

In der Standard-Konfiguration arbeitet der Postfix-Server lediglich als Mail-Endsystem, nicht jedoch als Mail-Relay. Soll der Postfix-Server auch als Mail-Relay eingesetzt werden, so müssen Sie die Postfix-Konfigurationsdatei */etc/mail/postfix/main.cf* entsprechend anpassen. Nähere Informationen hierzu sowie zu anderen Abweichungen von der Standard-Konfiguration finden Sie in den Man Pages zum Postfix-Server sowie in der Literatur zum Thema Postfix, auf die im Literaturverzeichnis verwiesen wird.

ACHTUNG!
Verfahren Sie bei der Konfiguration des Postfix-Servers als Mail-Relay besonders sorgfältig, da ein aus dem Internet erreichbares offenes Mail-Relay innerhalb kurzer Zeit Mail-Spammer anzieht. Dies kann u.a. zu einer Sperrung des Internet-Zugangs durch den Internet Service Provider führen.

10.4.2 IMAP- und POP3-Server in Betrieb nehmen

Im Gegensatz zum Postfix-Server laufen IMAP- und POP3-Server nicht permanent als unabhängige Dämonen ab, sondern werden bei einem Verbindungsaufbau für die zugehörige Verbindung vom *inetd*-Dämon gestartet. Somit gibt es pro IMAP- und POP3-Verbindung jeweils einen eigenen IMAP- bzw. POP3-Dämon. Dies kann bei hoher paralleler Nutzung zu erheblichem Ressourcen-Bedarf führen.

Damit der *inetd*-Dämon die einzelnen IMAP- bzw. POP3-Dämonen starten kann, muss der *inetd*-Dämon entsprechend konfiguriert sein. Im Standardfall erfolgt die Konfiguration des *inetd*-Dämons automatisch bei der IMAP-Installation.

Falls beim Betrieb von IMAP- oder POP3-Server Probleme auftreten, sollten Sie anhand der folgenden Beschreibung prüfen, ob der *inetd*-Dämon korrekt konfiguriert wurde:

- Prüfen Sie in der Datei */etc/inet/services* die Einträge, die den Portnummern der IMAP- und POP3-Dienste die Service-Namen zuordnen.

  Es werden die folgenden Einträge benötigt:

```
pop-3           110/tcp             # Post Office V3
pop-3s          995/tcp             # SSL secured Post Office V3
imap            143/tcp             # IMAP
imaps           993/tcp             # SSL secured IMAP
```

- Stellen Sie sicher, dass ein symbolischer Link von `/etc/services` auf `/etc/inet/services` existiert.

- Prüfen Sie in der *inetd*-Konfigurationsdatei */etc/inet/inetd.conf* die Einträge für die einzelnen Service-Namen.

  Es werden die folgenden Einträge benötigt:

```
pop-3    stream tcp  nowait SYSROOT /usr/sbin/in.ipop3d in.ipop3d
pop-3s   stream tcp  nowait SYSROOT /usr/sbin/in.ipop3d in.ipop3d
imap     stream tcp  nowait SYSROOT /usr/sbin/in.imapd in.imapd
imaps    stream tcp  nowait SYSROOT /usr/sbin/in.imapd in.imapd
```

- Wenn Sie die *inetd*-Konfigurationsdatei */etc/inet/inetd.conf* „von Hand“ modifiziert haben, müssen Sie den *inetd*-Dämon mit dem folgenden Kommando über die Änderung in der Konfigurationsdatei informieren:

```
kill -HUP <process id des inetd-Dämons>
```

IMAP- und POP3-Server verfügen über keine eigene Konfigurationsdatei. Außerdem unterstützen IMAP- und POP3-Server nur das Standard-Mbox-Format für die Benutzer-Mail-Boxen, nicht jedoch das vom Postfix-Server alternativ unterstützte Maildir-Format.

10.4.3 TLS/SSL-Absicherung von IMAP-/POP3- und SMTP-Verbindungen

Sowohl beim IMAP- und POP3-Server als auch beim Postfix-Server (SMTP-Server) können die Verbindungen mithilfe von TLS/SSL abgesichert werden. Dies ist insbesondere bei IMAP- und POP3-Verbindungen wichtig, da andernfalls Passwörter unverschlüsselt übertragen werden.

Im Zusammenhang mit SSL werden X.509-Zertifikate verwendet. Ein X.509-Zertifikat enthält alle für die Identifikation des Servers oder des Clients benötigten Informationen sowie den Public Key des Zertifikat-Eigners. Zertifikate werden von einer zentralen Stelle, der so genannten Certificate Authority (CA), ausgestellt, nachdem die Identität der im Zertifikat genannten Organisation und einer vertretungsberechtigten Person überprüft wurde. Für die Beantragung eines X.509-Zertifikats bei einer CA benötigen Sie einen so genannten Certificate Signing Request (CSR), den Sie mit dem Skript */etc/imap/MAKE.CERT.sh* erzeugen können. Außerdem erzeugt dieses Skript ein Test-Zertifikat, mit dem Sie schon vorab Tests der TLS/SSL-Funktionalität durchführen können. Da dieses Test-Zertifikat mithilfe eines öffentlich bekannten CA-Schlüssels erzeugt wird und somit keinen wirksamen Schutz bietet, darf es nicht für den Produktiv-Einsatz verwendet werden.

Ausführliche Informationen zum Thema TLS/SSL finden Sie im Handbuch „interNet Services Benutzerhandbuch“.

TLS/SSL-Absicherung von IMAP- und POP3-Verbindungen

Das Test-Zertifikat und den privaten Schlüssel speichern Sie an den für den IMAP-Server passenden Positionen im Verzeichnisbaum (*/etc/imap/certs/in.imapd.pem* bzw. */etc/imap/private/in.imapd.pem*). Das Zertifikat der Test-CA legen Sie unter */etc/imap/certs/cacert.pem* ab. Explizite Konfigurationseinstellungen sind beim IMAP- und POP3-Server nicht möglich. Der CSR befindet sich unter */etc/imap/imapd-csr.pem*.

Beachten Sie, dass der private Schlüssel später auch zusammen mit dem offiziellen Zertifikat im Produktiveinsatz verwendet wird. Stellen Sie daher sicher, dass der private Schlüssel in jedem Fall gegen unbefugten Zugriff geschützt ist. Während der Installation werden deshalb die Zugriffsrechte für das Verzeichnis */etc/imap/private* auf den Super-User (SYSROOT, TSOS) beschränkt.

Für den POP3-Server werden bei der Installation automatisch passende Links angelegt, die auf das oben genannte Zertifikat und den privaten Schlüssel für den IMAP-Server verweisen. Somit können der geheime Schlüssel (Private Key) und das Zertifikat sowohl vom IMAP- als auch vom POP3-Server genutzt werden.

Sobald Sie das Zertifikat von einer offiziellen CA erhalten haben, müssen Sie dieses unter */etc/imap/certs/in.imapd.pem* ablegen und damit das nicht mehr benötigte Test-Zertifikat überschreiben.

Nachfolgend ist der Mitschnitt eines */etc/imap/MAKE.CERT.sh*-Laufs abgedruckt. Benutzereingaben sind durch **Fettdruck** hervorgehoben.

```
# /etc/imap/MAKE.CERT.sh

1. Country Name              (2 letter code) [DE]:◂

2. State or Province Name    (full name)     [Bavaria]: Bayern◂

3. Locality Name             (eg, city)      [Munich]: Muenchen◂

4. Organization Name         (eg, company)   [Manufacturer, Ltd]:
   Fujitsu Technology Solutions GmbH◂

5. Organizational Unit Name (eg, section)    [Marketing]: Internet Services◂

6. Common Name               (eg, FQDN)      [www.manufacturer.com]:
   www.ts.fujitsu.com◂

7. Email Address             (eg, name@FQDN) [info@manufacturer.com]:
   info@ts.fujitsu.com◂

8. Certificate Validity      (days)          [365]: 730◂

   Certificate Version (1 or 3)                [3]:◂

9. subjectAltName:dNSName    (eg, FQDN)      [www.ts.fujitsu.com]:◂

   Generating certificate, please wait...

   Done


Subject: C=DE, ST=Bayern, L=Muenchen, O=Fujitsu Technology Solutions GmbH,
OU=Internet Services, CN=www.ts.fujitsu.com/emailAddress=info@ts.fujitsu.com

The private key for IMAP has been created as /etc/imap/private/in.imapd.pem.
The certifcate for IMAP has been created as /etc/imap/certs/in.imapd.pem.
The used CA certificate has been saved as /etc/imap/certs/cacert.pem.

For using certificate  and  key also
 for POP3 we make appropriate links to the created files:
Creating  link  /etc/imap/private/in.ipop3d.pem  to  file
/etc/imap/private/in.imapd.pem.
Creating  link  /etc/imap/certs/in.ipop3d.pem  to  file
/etc/imap/certs/in.imapd.pem.
WARNING: Use this certificate only for testing, not for production!
#
```

TLS/SSL-Absicherung von SMTP-Verbindungen (Postfix)

SMTP-Verbindungen können jeweils nur zwischen zwei auf dem Übertragungsweg benachbarten Mail-Servern (Mail Transfer Agent, MTA) abgesichert werden. Eine End-to-End-Sicherheit kann mit TLS/SSL nicht garantiert werden. Insbesondere werden die Mails unverschlüsselt auf den MTAs zwischengespeichert. TLS/SSL kann jedoch für die Implementierung teil-offener Mail-Relays genutzt werden. Hierbei lässt sich der Nutzerkreis eines Mail-Relays via TLS/SSL-Authentifizierung auf die berechtigten Personen eingrenzen. Analog kann in Fällen, in denen die Mail direkt an den Empfänger gesendet wird, mit TLS/SSL eine für Mail-Sender und -Empfänger transparente Mail-Verschlüsselung realisiert werden.

Außerdem schützt TLS/SSL im Gegensatz zur Mail-Verschlüsselung (S/MIME, PGP) auf dem jeweiligen Übertragungsweg nicht nur den Mail-Inhalt, sondern auch die Meta-Daten. Daher sollte die TLS/SSL-Absicherung des SMTP-Verkehrs nach Möglichkeit immer verwendet werden.

Wenn Sie TLS/SSL in Verbindung mit Postfix nutzen, müssen Sie die entsprechenden Parameter in der Postfix-Konfigurationsdatei */etc/postfix/main.cf* setzen. Dabei ist zu unterscheiden zwischen der TLS/SSL-Nutzung bei eingehenden und ausgehenden Verbindungen:

- Bei eingehenden Verbindungen beginnen die Parameternamen mit dem Präfix „smtpd_“.
- Bei ausgehenden Verbindungen beginnen die Parameternamen mit dem Präfix „smtp_“.

Weitere Informationen zu den verfügbaren TLS/SSL-Parametern finden Sie in der Datei */etc/postfix/sample-tls.cf*.

Minimal-Konfiguration zur TLS/SSL-Absicherung bei eingehenden SMTP-Verbindungen

Nachfolgend sind die zusätzlichen Parameter für eine Minimalkonfiguration zur TLS/SSL-Absicherung einer eingehenden SMTP-Verbindung abgedruckt. Die TLS/SSL-Konfiguration nutzt das IMAP/POP3-Zertifikat auch als Postfix-Server-Zertifikat.

```
smtpd_tls_cert_file = /etc/imap/certs/in.imapd.pem
smtpd_tls_key_file = /etc/imap/private/in.imapd.pem
smtpd_use_tls = yes
```

Minimal-Konfiguration zur TLS/SSL-Absicherung bei ausgehenden SMTP-Verbindungen

Nachfolgend sind die zusätzlichen Parameter für eine Minimalkonfiguration zur TLS/SSL-Absicherung einer ausgehenden SMTP-Verbindung abgedruckt. Die TLS/SSL-Konfiguration nutzt das IMAP/POP3-Zertifikat auch als Postfix-Client-Zertifikat.

```
smtp_tls_cert_file = /etc/imap/certs/in.imapd.pem
smtp_tls_key_file = /etc/imap/private/in.imapd.pem
smtp_tls_CAfile = /etc/imap/certs/trusted-certs.pem
smtp_use_tls = yes
```

Die Datei */etc/imap/certs/trusted-certs.pem* (Name ist frei wählbar) muss Zertifikate aller CAs enthalten, denen vertraut werden soll. Im Testbetrieb mit Verbindungen zu einem Server, dessen Server-Zertifikat mithilfe des Skripts *MAKE.CERT.sh* erzeugt wurde, müssen Sie in die Datei */etc/imap/certs/trusted-certs.pem* den Inhalt der Datei */etc/imap/certs/cacert.pem* einbringen. Nach dem Umstieg auf Produktivbetrieb müssen Sie dieses Test-CA-Zertifikat durch das CA-Zertifikat derjenigen CA ersetzen, die das Produktiv-Server-Zertifikat ausgestellt hat.

10.5 Betrieb des Postfix-Servers

Dieser Abschnitt behandelt die folgenden Themen:

- Postfix-Lookup-Tabellen
- wichtige Programme zum Betrieb des Postfix Mail-Servers

10.5.1 Postfix-Lookup-Tabellen (Index-Dateien)

Postfix verwendet eine Reihe von Lookup-Tabellen für die effiziente Suche nach Informationen zu Adressen-Ersetzung, Zugriffskontrolle u.a.. Bei einer Lookup-Tabelle für die Adressen-Ersetzung beispielsweise stellt die alte Adresse den Suchbegriff dar, während die neue Adresse dem Suchbegriff als Suchergebnis zugeordnet ist. In einer Lookup-Tabelle zur Zugriffskontrolle können z.B. alle lokalen Mail-Empfänger verzeichnet sein, die Postfix akzeptiert. Hier ist es für Postfix lediglich wichtig zu wissen, ob der Suchbegriff existiert. Das Suchergebnis als solches ist ohne Bedeutung.

Die über die Lookup-Tabellen zur Verfügung gestellten Informationen werden vom Administrator des Postfix Mail-Servers zunächst in gewöhnlichen Textdateien erfasst. Für einen performanten Zugriff auf diese Informationen verwendet Postfix jedoch nicht die vom Administrator erstellten Textdateien (Quelldateien), sondern so genannte Index-Dateien (indizierte Dateien), die der Administrator mithilfe der Programme *postmap* (siehe Seite 346) oder *postalias* (siehe Seite 348) aus den Quelldateien generiert.

postalias unterscheidet sich von *postmap* durch das für *postalias*-Quelldateien (Alias-Dateien) geforderte Format, das wegen der Kompatibilität zum Sendmail-Server geringfügig vom Quelldatei-Format der anderen Postfix-Quelldateien für Lookup-Tabellen abweicht (siehe Seite 338).

Zwei verschiedene Typen von Index-Dateien

Die BS2000-Portierung von Postfix unterstützt zwei verschiedene Typen von Index-Dateien:

- *hash*-Dateien: Die Suche basiert hier auf Hash-Tabellen und -Algorithmen.
- *btree*-Dateien: Die Suche basiert hier auf Balanced-Tree (B-Tree)-Strukturen und -Algorithmen.

Im Standardfall empfiehlt sich die Verwendung des *hash*-Formats. Der Einsatz von *btree*-Dateien kann sinnvoll sein, wenn bei sehr großen Lookup-Tabellen im *hash*-Format Performance-Probleme auftreten.
Die bei Postfix grundsätzlich mögliche Ablage von Lookup-Tabellen in externen Datenbanken oder Verzeichnissen wie NIS, MySQL oder LDAP wird von der BS2000-Portierung derzeit nicht unterstützt.

Allgemeines Postfix-Format für postmap-Quelldateien

Ein Eintrag (logische Zeile) in einer *postmap*-Quelldatei hat die folgende Syntax:

```
Schlüssel Leerraum Wert
```

Schlüssel
: Suchbegriff

Leerraum
: Leerraum besteht aus einer Folge von Leerzeichen und/oder Tabulatorzeichen. Leerraum muss mindestens ein Leerzeichen oder Tabulatorzeichen enthalten.

Wert
: Information, die dem Suchbegriff zugeordnet ist.

Darüber hinaus gelten für den Aufbau einer logischen Zeile die folgenden Regeln:

- Eine logische Zeile kann sich über mehrere Text-Zeilen erstrecken.
- Eine logische Zeile beginnt mit einem vom Leerraum verschiedenen Text.
- Eine Zeile, die mit einem Leerraum beginnt, setzt eine logische Zeile fort.
- Leerzeilen und Zeilen, die - eventuell nach einem Leerraum - mit „#“ beginnen, werden von *postmap* ignoriert.

Format für postalias-Quelldateien (Alias-Dateien)

Mithilfe von Alias-Namen lässt sich der Benutzeranteil einer lokalen Empfängeradresse durch eine oder mehrere Empfängeradressen ersetzen.

Als Empfängeradressen können Sie angeben:

- lokale Adressen
- ferne Adressen
- Programme, an die Nachrichten übergeben werden
- Dateien, in die Nachrichten gesichert werden.

Die Alias-Namen werden durch Einträge in eine Alias-Datei definiert. Der Standard-Dateiname der Alias-Datei lautet */etc/postfix/aliases*.

Ein Alias-Eintrag (Alias-Definition) hat die folgende Syntax:

`Name: Wert`$_1$`, Wert`$_2$`, Wert`$_3$`, ..., Wert`$_n$

Name
Benutzeranteil einer lokalen Empfängeradresse. Enthält der Benutzeranteil einer lokalen Empfängeradresse Sonderzeichen wie „@“ oder Leerzeichen, so muss er in doppelte Hochkommata ("") eingeschlossen werden. Der Wert des Benutzeranteils einer lokalen Empfängeradresse wird stets in Kleinbuchstaben abgespeichert.

Die Alias-Datei muss immer die Einträge für die lokalen Namen „postmaster“ und „MAILER-DAEMON“ enthalten (Anforderung des RFC 822).

$Wert_1$, $Wert_2$, $Wert_3$, ..., $Wert_n$
Eine oder mehrere Empfängeradressen.

Als $Wert_i$, i = 1 ... n, kann angegeben werden:

- lokaler Name (z.B. sysroot)
- ferne Adresse (z.B. user@domain.com)
- */Datei*

  In diesem Fall wird die Nachricht standardmäßig an das Ende der Datei *Datei* angehängt. Mithilfe des Parameters *allow_mail_to_ files* in der Postfix-Konfigurationsdatei *main.cf* können Sie dieses Verhalten unterdrücken.

- *|Programm*

  In diesem Fall wird die Nachricht standardmäßig über eine Pipe an einen Programmaufruf *Programm* übergeben. Mithilfe des Parameters *allow_mail_to_commands* in der Datei *main.cf* können Sie dieses Verhalten unterdrücken. Enthält der Programmaufruf Sonderzeichen (insbesondere Leerzeichen), dann müssen Sie den Programmaufruf in doppelte Hochkommata ("") setzen.

- `:include:`*Datei*

  Datei ist eine Textdatei, mit der Sie z.B. Mailing-Listen definieren können. Die Mails werden an die in diesen Mailing-Listen verzeichneten Empfänger gesendet. Leerzeilen sowie Zeilen, die mit „#“ beginnen, werden ignoriert. Alle anderen Zeilen von *Datei* haben die gleiche Syntax wie die rechten Seiten von Alias-Einträgen, d.h. `Wert`$_1$`, Wert`$_2$`, ..., Wert`$_n$.

  Bei `:include:`*Datei* werden Einträge für das Anhängen an Dateien (*|Datei*) sowie die Übergabe an Programmaufrufe über eine Pipe (*|Programm*) werden standardmäßig ignoriert. Mithilfe der *main.cf*-Parameter *allow_mail_to_ files* und *allow_-mail_to_commands* können Sie das standardmäßige Anhängen an Dateien bzw. die standardmäßige Übergabe an Programmaufrufe aktivieren.

- `owner-`*aliasname: owner_mail_adresse*

  Mit diesem Eintrag definieren Sie für die Mailing-Liste *aliasname* einen Eigentümer bzw. Verwalter, der die Mail-Adresse *owner_mail_adresse* besitzt. Im Fehlerfall (unzustellbare Mail) wird dann eine Benachrichtigung an *owner_mail_adresse* gesendet und nicht an den Mail-Absender, da der Eigentümer/Verwalter der Mailing-Liste in der Regel besser auf Zustellprobleme reagieren kann als der Mail-Absender.

  Wenn z.B. eine Mailing-Liste mit Namen „dbadmin“ definiert ist, definiert der folgende Eintrag die Mail-Adresse (hier: „owner-mail-adresse“) des Eigentümers der Mailing-Liste:

  ```
  owner-dbadmin: owner-mail-adresse
  ```

Steht nach Abschluss der Alias-Umsetzung fest, dass die Nachricht einem lokalen Benutzer zugestellt werden soll, dann prüft Postfix, ob das Home-Verzeichnis dieses Benutzers eine Datei *.forward* enthält. Trifft dies zu, dann wird eine weitere Stufe der Alias-Umsetzung durchgeführt, in der die *.forward*-Datei nach denselben Regeln interpretiert wird wie eine Alias-Datei.

Beispiel

Nachfolgend ist ein Beispiel für eine Alias-Datei abgedruckt.

```
# Alias-Datei
# Fehlermeldungen an postmaster weiterleiten und an die
# Logging-Datei /var/adm/mailerr anhängen
MAILER-DAEMON:   postmaster, /var/adm/mailerr
# Postmaster auf Systemverwalter-Kennung weiterleiten
postmaster:      sysroot
# An Systemverwalter adressierte Nachrichten an
# reale Person weiterleiten
sysroot:         mueller
# Programm fuer automatische Mail-Beantwortung
auto-test:       |"/home/rwk/auto-test -i 3"
# Mailing-Liste
dbadmin:         :include:/home/admin/db-admins
owner-dbadmin:   postmaster
```

Fehler, wie z.B. nicht zustellbare Mails an `dbadmin`, werden durch dieses `owner-dbadmin`-Alias nicht an den ursprünglichen Absender der Mail gesendet, sondern an `postmaster`.

Inhalt von */home/admin/db-admins*:

```
amueller@firma.example
bmeier@firma.example
dhuber@firma.example
/home/admin/db-admins.maillog
```

10.5.2 Programme zum Betrieb des Postfix Mail-Servers

Nachfolgend sind die wichtigsten Programme für den Betrieb des Postfix Mail-Servers beschrieben. Die Beschreibung umfasst die wichtigsten Parameter und Optionen dieser Programme. Eine vollständige Zusammenstellung aller für den Betrieb der Mail-Services verfügbaren Programme und ihrer Parameter/Optionen finden Sie in den Man Pages zu Postfix.

postfix - Postfix-Server starten und stoppen

Mit dem Programm *postfix* starten und stoppen Sie den Postfix-Mail-Server. Außerdem können Sie *postfix* verwenden, um nach einer Modifizierung der Konfigurationsdateien */etc/postfix/master.cf* und */etc/postfix/main.cf* diese Dateien erneut einzulesen. Ein explizites Stoppen des Postfix-Mail-Servers ist hierfür nicht erforderlich.

Aufgrund von POSIX-Besonderheiten sollten Sie das Programm *postfix* nicht direkt aufrufen, sondern für den *postfix*-Aufruf das Einschalungsskript */etc/init.d/MAIL.postfix* verwenden. Dieses Skript generiert vor dem Postfix-Start u.a. alle in der Konfigurationsdatei *main.cf* definierten Index-Dateien neu und verhindert dadurch ein Divergieren von Quell- und Indexdateien.

/etc/init.d/MAIL.postfix
{ **start** | **stop** | **reload** }

start
Startet den Postfix-Mail-Server.

stop
Stoppt den Postfix-Mail-Server.

reload
Liest die (geänderten) Konfigurationsdateien neu ein.

postconf - Postfix-Konfigurationsparameter anzeigen und ändern

Mit dem Programm *postconf* können Sie die Werte der Postfix-Konfigurationsparameter verändern oder sich am Bildschirm anzeigen lassen. Dies betrifft sowohl Parameter, die explizit in der Konfigurationsdatei */etc/postfix/main.cf* gesetzt sind, als auch die per Default voreingestellten Parameter.

postconf
[**-d**] [**-n**] [**-e**]

kein Parameter spezifiziert
: Zeigt alle aktuell gültigen Parameterwerte an.

-d
: Zeigt alle Default-Parameterwerte an.

-n
: Zeigt alle aktuell gültigen Parameterwerte an, die vom zugehörigen Default-Wert abweichen.

-e
: Setzt Postfix-Konfigurationsparameter.
Die Option *-e* bietet sich vor allem an für das automatisierte Setzen von Parametern via Shell-Skript. Ansonsten können Sie die Konfigurationsdatei */etc/postfix/main.cf* auch mit einem beliebigen Editor (z.B EDT) bearbeiten.

postqueue (mailq) - Mail-Queues bearbeiten (als normaler Benutzer)

Mit dem Programm *postqueue* können Sie mit normaler User-Berechtigung Operationen auf den Mail-Queues (Warteschlangen) ausführen, die in Form von Dateien in verschiedenen Unterverzeichnissen organisiert sind.

Jede Mail, die der Postfix-Server zur lokalen Zustellung oder zur Weiterleitung erhält, wird zunächst in Unterverzeichnissen von */var/spool/postfix* zwischengespeichert, z.B. */var/spool/postfix/incoming* oder */var/spool/postfix/active*.

Mit den in den Mail-Queues abgelegten Mails wird wie folgt verfahren:

- Sobald eine Mail erfolgreich zugestellt oder weitergeleitet wurde, wird sie aus den Mail-Queues entfernt.
- Kann eine Mail, z.B. wegen nicht erreichbarer Mail-Server, zunächst nicht weitergeleitet oder zugestellt werden, dann wird sie wieder in eine Mail-Queue eingereiht. Ein erneuter Zustellversuch wird erst nach einer Wartezeit unternommen.

Das Programm *mailq* wird nur wegen der Kompatibilität zum Mail-Server Sendmail unterstützt und liefert die gleiche Funktionalität wie `postqueue -p`.

Da Benutzer mit normaler User-Berechtigung das *sbin* -Verzeichnis nicht in ihrem PATH haben, müssen sie den vollständigen Pfadnamen angeben.

[**/opt/MAIL/postfix/sbin/**]**postqueue**
{ **-p** | **-f** | **-s** <site>}

-p
Listet die Inhalte der Mail-Queues in einer Darstellung auf, wie sie vom Sendmail-Programm *mailq* her bekannt ist.

-f
Veranlasst den Postfix-Server, für alle Mails in den Mail-Queues einen (gegebenenfalls erneuten) Zustellversuch zu unternehmen. Dies ist z.B. nach der Behebung von Verbindungsproblemen nützlich, die die Weiterleitung von Mails temporär verhindert haben. Anstatt die Wartezeit für einen erneuten Zustellversuch verstreichen zu lassen, können Sie so die sofortige Zustellung aller wartenden Nachrichten veranlassen.

-s <site>
Veranlasst die sofortige Zustellung aller für <site> bestimmten Mails, die in den Mail-Queues enthalten sind.

postsuper - Mail-Queues bearbeiten (mit SYSROOT-Berechtigung)

Mit dem Programm *postsuper* können Sie auf den Mail-Queues Operationen ausführen, für die SYSROOT-Berechtigung erforderlich ist.

postsuper
[**-p**] [**-s**] [**-d** <queue-id>] [**-h** <queue-id>] [**-H <**queue-id>] [<directory> ...]

-p
Löscht alte temporäre Dateien, die nach einem System- oder Software-Crash übrig geblieben sind.

-s
Prüft und repariert die Struktur der Mail-Queues. Es wird dringend empfohlen, diese Operation vor jedem Postfix-Start auszuführen.

-d <queue-id>
Löscht in der (den) durch <directory> ... spezifizierten Mail-Queue(s) eine Mail mit der Queue-Id <queue-id>. Wenn Sie für <queue-id> den Wert ALL angeben, werden alle Mails in der (den) spezifizierten Mail-Queue(s) gelöscht.
Default-Wert für <directory> ... : hold, incoming, active, deferred

-h <queue-id>
Versetzt in der (den) durch <directory> ... spezifizierten Mail-Queue(s) eine Mail mit der Queue-Id <queue-id> in den Haltezustand. Diese Mail wird dann vorerst nicht zugestellt oder weitergeleitet. Wenn Sie für <queue-id> den Wert ALL angeben, werden alle Mails der spezifizierten Mail-Queue(s) in den Haltezustand versetzt.
Default-Wert für <directory> ... : incoming, active, deferred

-H <queue-id>
Beendet in der (den) durch <directory> ... spezifizierten Mail-Queue(s) den Haltezustand für eine Mail mit der Queue-Id <queue-id>. Wenn Sie für <queue-id> den Wert ALL angeben, wird für alle Mails der spezifizierten Mail-Queue(s) der Haltezustand beendet.
Default-Wert für <directory> ... : hold

<directory> ...
Spezifiziert ein oder mehrere Mail-Queue-Verzeichnisse.

postcat - Inhalt von Nachrichten der Mail-Queues anzeigen

Mit dem Programm *postcat* kann sich der Administrator den Inhalt einzelner Nachrichten (Mails in den Mail-Queues) in einem lesbaren Format anzeigen lassen.

[**/opt/MAIL/postfix/sbin/**]**postcat**
[**-vq**] [**-c** <config_dir>] [<file> ...]

-v
Aktiviert ausführliches Logging zu Debugging-Zwecken.

-q
In diesem Fall müssen Sie als <file> nur die Queue-Id der anzuzeigenden Mail spezifizieren. *postcat* ermittelt dann selbstständig den vollständigen Pfadnamen, d.h. in welcher Mail-Queue die Datei <file> steht.

-c <config_dir>
Die Postfix-Konfigurationsdatei *main.cf* liegt im Verzeichnis <config_dir> anstatt im Standard-Konfigurationsverzeichnis.

<file> ...
Name(n) der Datei(en)/Mails, deren Inhalt angezeigt werden soll:

– Wenn Sie die Option `-q` angeben, müssen Sie nur die Queue-Id(s) der auszugebenden Nachricht(en) spezifizieren.

– Wenn Sie den Schalter `-q` nicht angeben, müssen Sie den (die) vollständigen Pfadnamen der Nachricht(en) spezifizieren.

Beispiel

Eine Mail mit der Queue-Id 457106EA05 steht in der *deferred*-Queue */var/spool/postfix/deferred/4/*. Somit existiert eine Datei mit dem Namen */var/spool/postfix/deferred/4/457106EA05*.

Sie können sich den Inhalt der Mail 457106EA05 wahlweise wie folgt anzeigen lassen:

- `postcat /var/spool/postfix/deferred/4/457106EA05`

  Hier müssen Sie als Argument den vollständigen Pfadnamen angeben.

- `postcat -q 457106EA05`

  Mit der Option `-q` genügt es, die Queue-Id der anzuzeigenden Mail zu spezifizieren.

postmap - Index-Dateien erzeugen und bearbeiten (Postfix-Format)

Postfix verwendet Index-Dateien (Lookup-Tabellen, siehe Seite 337). Das Programm *postmap* bietet folgende Funktionalität für die Bearbeitung von Lookup-Tabellen:

- Index-Dateien aus Textdateien erzeugen
- Einträge zu einem bestimmten Schlüsselwert anzeigen (Index-Suche)
- Einträge in eine Index-Datei aufnehmen
- Einträge aus einer Index-Datei entfernen

Die BS2000-Portierung von Postfix unterstützt bei Index-Dateien die Formate *hash* und *btree*.

postmap
[**-q** <schlüssel>] [**-d** <schlüssel>] [**-i**] [**hash:**|**btree:**]<pfadname> ...

-q <schlüssel>
: Sucht den Eintrag zum Schlüsselwert <schlüssel> und gibt den ersten zugeordneten aus Wert aus.

-d <schlüssel>
: Löscht den Eintrag mit dem Schlüsselwert <schlüssel>.

-i
: Liest Einträge von der Standard-Eingabe und fügt diese in die Index-Datei <pfadname>.db ein.

hash: | btree:
: Spezifiziert den Typ der zu erzeugenden Index-Datei (`hash` oder `btree`).

<pfadname>
: Name der Datei, zu der die zugehörige Index-Datei <pfadname>.db erzeugt werden soll.

Beispiel

Eine Lookup-Tabelle *canonical*, die BS2000-Benutzernamen (maximal 8 Zeichen lang) auf Mail-Adressen der Form *Vorname.Nachname* abbildet, enthält die folgenden Einträge:

```
maier Georg.Maier
mueller Elisabeth.Mueller
```

Mit dem folgenden Kommando erzeugen Sie die zugehörige Index-Datei (Typ *hash*) */etc/postfix/canonical.db*:

```
postmap hash:/etc/postfix/canonical
```

Das Kommando

```
postmap -q maier /etc/postfix/canonical
```

liefert dann zum Schlüssel „maier“ die folgende Ausgabe: `Georg.Maier`

Das folgende Kommando löscht den Eintrag mit dem Schlüssel „mueller“ in der Index-Datei */etc/postfix/canonical.db*:

```
postmap -d mueller /etc/postfix/canonical
```

Beachten Sie, dass die ursprüngliche Textdatei */etc/postfix/canonical* nicht verändert wird.

postalias - Index-Dateien erzeugen und bearbeiten (Alias-Format)

Das Programm *postalias* unterscheidet sich vom Programm *postmap* nur durch das Format der Eingabedateien (siehe Seite 338).

postalias bietet folgende Funktionalität für die Bearbeitung von Lookup-Tabellen:

- Index-Dateien aus Textdateien erzeugen
- Einträge zu einem bestimmten Schlüsselwert anzeigen (Index-Suche)
- Einträge in eine Index-Datei aufnehmen
- Einträge aus einer Index-Datei entfernen

Die BS2000-Portierung von *postalias* unterstützt bei Index-Dateien die Formate *hash* und *btree*.

postalias
[**-q** <schlüssel>] [**-d** <schlüssel>] [**-i** <schlüssel>] [**hash:**|**btree:**]<pfadname> ...

-q <schlüssel>
: Sucht den Eintrag zum Schlüsselwert <schlüssel> und gibt den ersten zugeordneten aus Wert aus.

-d <schlüssel>
: Löscht den Eintrag mit dem Schlüsselwert <schlüssel>.

-i
: Liest Einträge von der Standard-Eingabe und fügt diese in die Index-Datei <pfadname>.db ein.

hash: | btree:
: Spezifiziert den Typ der zu erzeugenden Index-Datei (`hash` oder `btree`).

<pfadname>
: Name der Datei, zu der die zugehörige Index-Datei <pfadname>.db erzeugt werden soll.

Beispiel

Dieses Beispiel basiert auf der Alias-Datei aus dem Beispiel von Seite 340.

Mit dem folgenden Kommando erzeugen Sie die zugehörige Index-Datei (Typ *hash*) */etc/postfix/aliases.db*:

```
postalias hash:/etc/postfix/aliases
```

Das Kommando

```
postalias -q postmaster /etc/postfix/aliases
```

liefert dann zum Schlüssel „postmaster“ die folgende Ausgabe: `sysroot`

Das folgende Kommando löscht den Eintrag mit dem Schlüssel „ sysroot“ in der Index-Datei */etc/postfix/aliases.db*:

```
postalias -d sysroot /etc/postfix/aliases
```

Beachten Sie, dass die ursprüngliche Textdatei */etc/postfix/aliases* nicht verändert wird.

newaliases - Index-Dateien erzeugen (Alias-Format)

Das Programm *newaliases* generiert zu allen im Konfigurationsparameter *alias_database* genannten Dateien die zugehörigen Index-Dateien. Der Parameter *alias_database* ist in der Konfigurationsdatei *main.cf* definiert.

Das Programm *newaliases* wird aus Gründen der Kompatibilität zum Mail-Server Sendmail unterstützt.

Beispiel

In der Konfigurationsdatei *main.cf* ist der Parameter *alias_database* z.B. wie folgt gesetzt:

```
alias_database = hash:/etc/postfix/aliases
```

In diesem Fall erzeugen Sie durch den Programmaufruf *newaliases* die Index-Datei */etc/postfix/aliases.db*.

10.6 Umstieg von Sendmail auf Postfix

Der Umstieg von Sendmail auf Postfix erfordert relativ wenig Aufwand, da der Postfix Mail-Server das Sendmail Alias-Datei-Format verwendet und außerdem die Kompatibilitätsprogramme *sendmail*, *mailq* und *newaliases* zur Verfügung stehen.

Für den Umstieg vom Sendmail-Server auf den Postfix Mail-Server bieten sich zwei alternative Vorgehensweisen an:

- Postfix Mail-Server erst nach Deinstallation des Sendmail-Servers installieren.
- Postfix Mail-Server parallel zu bestehender Sendmail Server-Installation installieren.

Postfix Mail-Server nach Deinstallation des Sendmail-Servers installieren

Wenn Sie den Sendmail-Server vor der Installation des Postfix Mail-Servers deinstallieren, müssen Sie sicherstellen, dass vor der Sendmail-Deinstallation die in der Mail-Queue des Sendmail-Servers (Default: */var/mqueue*) enthaltenen Mails zugestellt werden. Dies ist erforderlich, weil Postfix ein zum Sendmail Queue-System inkompatibles Queue-System verwendet.

Gehen Sie wie folgt vor:

► Stoppen Sie den *sendmail*-Dämon.

► Starten Sie mit folgendem Kommando einen Sendmail-Lauf zum Leeren der Sendmail-Mail-Queue:

/usr/sbin/sendmail -q

► Falls noch Mails in der Sendmail-Mail-Queue verblieben sind: Unternehmen Sie gegebenenfalls weitere Zustellversuche oder löschen Sie die verbliebenen Mails.

► Starten Sie die Installation des Postfix-Mail-Servers (siehe Seite 323).

Postfix Mail-Server parallel zu bestehender Sendmail Server-Installation installieren

Wenn sich das Bereinigen der Sendmail-Mail-Queue z.B. aufgrund temporär ausgefallener Mail-Server verzögert, empfiehlt es sich, die Sendmail-Installation zunächst bestehen zu lassen und parallel dazu einen Postfix-Mail-Server zu installieren.

Gehen Sie wie folgt vor:

► Starten Sie die Installation des Postfix-Mail-Servers (siehe Seite 323).

Wenn die Postfix-Installationsroutine einen installierten Sendmail findet, gibt sie eine Warnung aus.

► Betätigen Sie die DUE-Taste.

Damit ignorieren Sie die Warnung und die Postfix-Installation wird fortgesetzt.

Die Postfix-Installationsroutine sichert das *sendmail*-Programm des Sendmail-Servers unter dem Pfad */usr/sbin/sendmail.renamed.by.MAIL:postfix* und ersetzt es durch die Postfix-Variante.

Findet die Postfix-Installationsroutine eine Datei */etc/mail/aliases* oder */etc/aliases* (z.B. aus einer früheren Sendmail-Installation), dann kopiert die Postfix-Installationsroutine diese Datei in das Postfix-Konfigurationsverzeichnis. Am Ende der Installation wird über den Skript-Aufruf */etc/init.d/MAIL.postfix start* das *newaliases*-Programm für die Generierung der zugehörigen Index-Datei automatisch aufgerufen.

► Starten Sie mit folgendem Kommando einen Sendmail-Lauf zum Leeren der Sendmail-Mail-Queue:

/usr/sbin/sendmail.renamed.by.MAIL:postfix -q

Vor der Postfix-Installation waren beim Sendmail-Server die Aufrufe */usr/sbin/mailq* und */usr/sbin/newaliases* Links auf das Sendmail-Programm. Nach erfolgreicher Postfix-Installation wird mit diesen Aufrufen jedoch die Postfix-Variante des Sendmail-Programms gestartet.

Wenn Sie auch nach erfolgter Postfix-Installation die auf Sendmail-Dateien und -Queues operierenden Sendmail-Varianten der Programme *mailq* und *newaliases* nutzen wollen, rufen Sie das Sendmail-Programm mit geeigneten Schaltern wie folgt auf:

- */usr/sbin/sendmail.renamed.by.MAIL:postfix -bi* für die *newaliases*-Funktionalität
- */usr/sbin/sendmail.renamed.by.MAIL:postfix -bp* für die *mailq*-Funktionalität

Postfix bietet kompatible Unterstützung für den benutzerspezifischen Alias-Mechanismus, der auf einer *.forward*-Datei basiert, die im Home-Verzeichnis des betreffenden Benutzers liegt. Somit sind bei einem Umstieg von Sendmail auf Postfix keine Änderungen an diesen Dateien erforderlich.

11 Mail-Sender im BS2000

11.1 Mail-Sender installieren und deinstallieren

Nach der Installation der Produktdateien ist noch ein weiterer Installationsschritt nötig:

Die Adresse des Mail-Servers, also sein DNS-Name oder die IP- bzw. IPv6-Adresse, muss mit der Option *mailServer* in der Konfigurationsdatei für das Mail-Sender Backend gesetzt werden (siehe Abschnitt „mailServer“ auf Seite 360).

Bei Problemen sollten Sie die Option *logLevel* in der Konfigurationsdatei setzen, um Diagnose-Informationen in der, mit *logFile* spezifizierten, Protokolldatei abzulegen (siehe Abschnitte „logFile“ auf Seite 357 und „logLevel“ auf Seite 358).

11.2 Option-Dateien

11.2.1 SYSSSI

Die Datei *SYSSSI* spezifiert verschiedene Parameter, die von Teilen des Mail-Sender verwendet werden. Der Standarddateiname der Option-Datei lautet

`$.SYSSSI.MAIL.`*nnn*`.MAILCLNT`

bzw. gleichnamig unter der entsprechenden Installationskennung

Sie können den Dateinamen über die IMON Logical-ID SYSSSI.MAILCLNT ändern.

Notation der Options in der Option-Datei

Die einzelnen Options müssen gemäß den folgenden Regeln in die Option-Datei eingetragen sein:

- Jede Option muss in einer eigenen Zeile stehen.
- Erstrecken sich die Argumente einer Option über mehrere Zeilen, dann muss jede fortzusetzende Zeile mit dem Fortsetzungszeichen „\“ abgeschlossen werden.
- Eine Zeile, die mit dem Zeichen „#“ in Spalte 1 beginnt, wird beim Einlesen ignoriert.
- Bei den Option-Namen wird Klein-/Groß-Schreibung nicht unterschieden.
- Bei den Option-Werten wird, falls nicht anders angegeben, Klein-/Groß-Schreibung nicht unterschieden.

Im Folgenden sind die verfügbaren Optionen aufgeführt:

defaultOptionFileName

Der Dateiname, der in der Option *defaultOptionFileName* spezifiziert ist, wird verwendet, wenn das Kommando SEND-MAIL mit dem Standardwert *STD im Operanden USER-OPTION-FILE aufgerufen wird.

defaultOptionFileName
<dateiname 1..54>

<dateiname 1..54>
Name der Datei, die mit dem Kommando SEND-MAIL aufgerufen werden soll.
Voreinstellung: SYSDAT.MAIL.*nnn*.USER.OPT

backendConfigurationFileName

Die Option *backendConfigurationFileName* spezifiziert den Namen der Konfigurationsdatei für das Mail-Sender Backend (siehe Abschnitt „Konfigurationsdatei für das Mail-Sender Backend“ auf Seite 357).

backendConfigurationFileName
<dateiname 1..54>

<dateiname 1..54>
Name der Konfigurationsdatei.
Voreinstellung: $.SYSDAT.MAIL.*nnn*.SERVICE.OPT

senderSuffix

Wenn die Option *useSenderSuffix* (siehe Seite 356) entsprechend gesetzt ist, dann wird der mit der Option *senderSuffix* spezifizierte Suffix zur Bildung der Absender-Adresse verwendet, wenn diese nicht schon anderweitig angegeben wurde. Die Adresse wird durch Aneinanderhängen von BS2000 User-ID und Suffix gebildet.

senderSuffix
<suffix 1..128>

<suffix 1..128>
Um zu einer gültigen Mail-Adresse zu gelangen, muss dieser Suffix ein @-Zeichen enthalten. Die typische Form für diesen Suffix wird @<vollqualifizierter Domänen-Name> sein, z.B. @fujitsu.com, aber es kann angebracht sein, eine Zeichenkette zur Unterscheidung voranzustellen, z.B. wie bei .BS2000@fujitsu.com. Damit würde im Fall der User-Id TSOS die Absender-Adresse TSOS.BS2000@fujitsu.com gebildet. Falls die solcherart gebildete Adresse keine gültige E-Mail-Adresse des entsprechenden BS2000-Nutzers ist, dann gehen im Fall von Mail-Zustellproblemen die generierten Bounce-Mails verloren. Daher sollte Kontakt mit der Mail-Server-Verwaltung aufgenommen werden, um z.B. diese Mail-Adresse als Alias für eine gültige E-Mail-Adresse zu definieren.

useSenderSuffix

Diese Option gibt an, ob gegebenenfalls eine automatische Generierung der Absender-Adresse durchgeführt werden soll.

useSenderSuffix
NO | **YES**

NO
Es wird keine automatische Generierung der Absender-Adresse durchgeführt. Dies ist die Voreinstellung.

YES
Wenn zusätzlich die Option *senderSuffix* (siehe Seite 355) spezifiziert ist, dann wird die Absender-Adresse automatisch generiert, falls sie nicht schon anderweitig angegeben wurde. Damit sind die Anwender nicht gezwungen, eine Benutzer-Option-Datei anzulegen oder bei jedem Mail-Sende-Auftrag die Absender-Adresse anzugeben.

11.2.2 Konfigurationsdatei für das Mail-Sender Backend

Das Mail-Server Backend ist eine TU-Task und

- bekommt von ASTI einen Mail-Auftrag,
- erzeugt aus diesem Auftrag eine korrekt nach MIME und S/MIME formatierte Mail und
- sendet diese Mail über eine, ggf. über TLS/SSL gesicherte, SMTP-Verbindung an einen Mail-Server.

Die hierfür nötigen Konfigurationsoptionen sind in einer Konfigurationsdatei abgelegt. Der Standard-Dateiname ist in der Datei *SYSSSI* in der Option *backendConfigurationFileName* festgelegt (siehe Abschnitt „SYSSSI“ auf Seite 353). Die Festlegung durch die Option *backendConfigurationFileName* kann mit den Kommandos START-MAIL-SERVICE und MODIFY-MAIL-SERVICE-PARAMETER überschrieben werden.

Im Folgenden sind die verfügbaren Optionen aufgeführt:

logFile

Die Option *logFile* spezifiziert den Namen der Protokolldatei, in der die Diagnose-Meldungen abgelegt werden. Die Option *logLevel* (siehe Seite 358) gibt an, welche Meldungen in die Datei geschrieben werden sollen.

logFile
<dateiname 1..54>

<dateiname 1..54>
Namen der Protokolldatei.
Voreinstellung: $.SYSDAT.MAIL.*nnn*.LOG

logLevel

Die Option *logLevel* spezifiziert die Priorität der Diagnose-Meldungen, die protokolliert werden sollen.

logLevel
<selektor> <level>

<selektor>
legt fest, für welchen funktionalen Satz von Meldungen die Angabe gilt. Folgende Werte sind möglich:

ASTI	Meldungen, die die Auftrags-Behandlung in ASTI betreffen
SMTP	Meldungen, die den Mail-Transfer zum SMTP-Server betreffen
TLS	Meldungen, die den TLS/SSL-Schutz der Verbindung zum SMTP-Server betreffen
SMIME	Meldungen, die die S/MIME-Signierung und/oder -Verschlüsselung von Mails betreffen
OTHER	Alle anderen Meldungen
ALL	Alle Meldungen

<level>
gibt an, dass alle Meldungen mit der angegebenen oder einer höheren Priorität protokolliert werden sollen. Die möglichen Werte sind, mit abfallender Priorität:

ALERT
CRITICAL
ERROR
WARNING
NOTICE
INFO
DEBUG
NONE, unterdrückt die Protokollierung aller Meldungen

Die Option *logLevel* kann mehrfach eingesetzt werden.

Beispiel

```
logLevel ALL WARNING
logLevel SMTP CRITICAL
```

gibt an, dass alle Meldungen mit der Priorität WARNING protokolliert werden sollen. Ausnahme sind die SMTP-Meldungen, die nur mit einer Priorität CRITICAL oder höher protokolliert werden sollen.

Voreinstellung: ALL CRITICAL

logMailContent

Die Option *logMailContent* legt fest, ob z.B. bei einem ASTI-Logging auf der höchsten Stufe ("logLevel ASTI DEBUG") auch Mail-Inhalte (Subject, Mail- und Attachment-Texte) protokolliert werden sollen. Die Protokollierung der Mail-Inhalte bläht zum einen die Logging-Dateien stark auf und wirft zum anderen Datenschutz-Probleme auf, sollte also nur dann aktiviert werden, wenn dies unbedingt notwendig ist und Vorkehrungen getroffen werden, dass nicht Mail-Inhalte in unbefugte Hände geraten.

logMailContent
NO / **YES**

NO
Mail-Inhalte werden nicht protokolliert. Dies ist die Voreinstellung.

YES
Mail-Inhalte werden bei entsprechend hoher Logging-Stufe protokolliert.

mailServer

Die Option *mailServer* gibt den Mail-Server an, an den die Mail weitergeleitet werden soll.

mailServer
<DNS-Name | IP-Adresse | IPv6-Adresse>

<DNS-Name | IP-Adresse | IPv6-Adresse>
DNS-Name, IP- oder IPv6-Adresse des Mail-Servers, an den die Mail weitergeleitet werden soll.

mailServerPort

In der Regel wird der Mail-Server über den Port 25 angesprochen. Die Option *mailServerPort* gibt ggf. einen anderen Port für den Mail-Server an.

mailServerPort
<portnummer>

<portnummer>
Portnummer des Mail-Servers.
Voreinstellung: 25

mailLogLevel

Die Option *mailLogLevel* gibt an, welche Daten protokolliert werden sollen.

mailLogLevel
0 | **1** | **2**

0

Es erfolgt keine Protokollierung (Voreinstellung).

1

Einfache Protokollierung.
In diesem Fall werden folgende Daten protokolliert:

- Zeit
- ASTI-Auftrags-ID
- Absender-Adressen („From“), sowohl Envelope als auch Header
- Empfänder-Adressen („To“), sowohl Envelope als auch Header
- Kopie-Empfänger-Adressen („Cc“) (Header)
- Erfolgs-Status des Transfer zum SMTP-Server inklusive der OK-Meldung des Mail-Servers. Diese Meldung kann, abhängig von der Mail-Server-Software, einen Teil der Message-ID enthalten.

2

Erweiterte Protokollierung.
Zusätzlich zu den Daten der einfachen Protokollierung wird der Subject-Header protokolliert. Da der Subject-Header im Allgemeinen schon Mail-Inhalt darstellt, sind entsprechende Datenschutz-Aspekte zu bedenken.

mailLogFile

Die Option *mailLogFile* gibt den Namen der Mail-Protokolldatei an. In diese Datei wird jeder Mail-Sende-Auftrag eingetragen, der an den Service übergeben wird. Welche Informationen in die Datei geschrieben werden, ist abhängig von der Option *mailLogLevel* (siehe Seite 361).

mailLogFile
<dateiname 1..54>

<dateiname 1..54>
Name der Mail-Protokolldatei.
Voreinstellung: $.SYSDAT.MAIL.*nnn*.MAILLOG

maxQueueLifeTime

Die Option *maxQueueLifeTime* legt die maximale Lebensdauer einer Mail fest, während der ein fehlgeschlagener Mailversand wiederholt wird.

maxQueueLifeTime
<lifetime>[s | m | h | d]

<lifetime>
Voreinstellung: 5d

Ohne Angabe einer Maßeinheit gilt der angegebene *<lifetime>* als Tage. Mit Angabe einer Maßeinheit (*s* für Sekunde, *m* für Minute, *h* für Stunde, *d* für Tag) muss diese unmittelbar hinter *<lifetime>* stehen, d.h. ohne Leerzeichen.

Die Option *retryLimit* ist mit der Einführung von *maxQueueLifeTime* wirkungslos.

retryLimit

Diese Option wird künftig nicht mehr unterstützt.

Verwenden Sie stattdessen die Option *maxQueueLifeTime*, siehe Seite 362.

smtpReadMaxWaitTime

Die Option *smtpReadMaxWaitTime* legt fest, wie lange das Mail-Sender Backend ggf. auf eine Antwort des SMTP-Servers warten soll. Wird ein Mail-Sende-Auftrag wegen zu langer Wartezeit abgebrochen, dann wird er wie bei Fehlermeldungen des SMTP-Servers, die auf ein temporär vorhandenes Problem hinweisen, nach einer gewissen Zeit wiederholt, siehe Optionen *smtpRetryTimeBase* und *smtpRetryTimeMaxExp*.

Die mit dem Mail-Sender Backend kommunizierenden Kommandos MODIFY-MAIL-SERVICE-PARAMETER, SHOW-MAIL-SERVICE-PARAMETER sowie STOP-MAIL-SERVICE und die Kommunikation des Backend mit dem SMTP-Server werden miteinander serialisiert. Daher ist es für die möglichst prompte Abarbeitung dieser Kommandos wünschenswert, einen Wartezustand des Backend - z.B. aufgrund von SMTP-Server-Problemen - zeitlich möglichst zu begrenzen. Anderseits sollte diese Begrenzung auch nicht zu drastisch ausfallen, da sonst z.B. ein überlasteter SMTP-Server durch Transfer-Abbrüche und -Wiederholungen noch stärker belastet wird.

Zeiten im einstelligen Minutenbereich stellen i.A. einen guten Kompromiss dar.

smtpReadMaxWaitTime
<zeit>[s | m | h | d]

<zeit>
Max. Wartezeit
Voreinstellung: 5m

Ohne Angabe einer Maßeinheit gilt die angegebene *<zeit>* als Minuten. Mit Angabe einer Maßeinheit (*s* für Sekunde, *m* für Minute, *h* für Stunde, *d* für Tag) muss diese unmittelbar hinter *<zeit>* stehen, d.h. ohne Leerzeichen. Wird 0 angegeben, dann wird die Wartezeit nicht begrenzt.

smtpRetryTimeBase

Die Option *smtpRetryTimeBase* legt die Zeitbasis fest, welche zur Ermittlung der Zeit verwendet wird, nach der bei einem fehlgeschlagenen Mailversand ein erneuter Mailversand versucht wird. Für Details siehe Option *smtpRetryTimeMaxExp*.

smtpRetryTimeBase
<wert>[s | m | h | d]

<wert>
Zeitbasis
Voreinstellung: 15m

Ohne Angabe einer Maßeinheit gilt der angegebene *<wert>* als Minuten. Mit Angabe einer Maßeinheit (*s* für Sekunde, *m* für Minute, *h* für Stunde, *d* für Tag) muss diese unmittelbar hinter *<wert>* stehen, d.h. ohne Leerzeichen.

smtpRetryTimeMaxExp

Die Option *smtpRetryTimeMaxExp* begrenzt die Erhöhung der Wartezeit zwischen zwei Wiederholungen von Mailversandversuchen. Normalerweise verdoppelt sich die Wartezeit mit jedem fehlgeschlagenen Versandversuch, um bei länger andauernden Problemen den CPU-Verbrauch durch die Versandversuche zu begrenzen. Nach *smtpRetryTimeMaxExp* Verdopplungen bleibt die Wartezeit auf dem dann erreichten Wert.

smtpRetryTimeMaxExp
<wert>

<wert>
Voreinstellung: 6

Bei Fehlern während des Verbindungsaufbaus zum SMTP-Mailserver wird als Wartezeit bis zu einem erneuten Zustellversuch konstant die doppelte *smtpRetryTimeBase* verwendet.

Tritt der Fehler erst später im SMTP-Dialog auf, sodass es sich möglicherweise nicht um ein vergleichsweise schnell bemerktes, allgemeines Server-Problem handelt, sondern um ein mailspezifisches, welches oft erst nach einiger Zeit bemerkt wird, dann wird die Wartezeit zwischen zwei Versandversuchen (beginnend bei *smtpRetryTimeBase*) mit jedem Versuch verdoppelt, bis *smtpRetryTimeMaxExp* Verdopplungen erreicht sind. Daraus ergibt sich die Voreinstellung der max. Wartezeit zwischen zwei Zustellversuchen wie folgt:

max. Wartezeit = $smtpRetryTimeBase * 2^{smtpRetryTimeMaxExp} = 15m * 2^6 = 960m = 16h$

Beispiele

1. Mailserver nicht erreichbar

   Erneute Zustellversuche nach 30min= 2 * 15m

2. Verbindungsaufbau zum Mailserver möglich; mailspezifischer Fehler:

   – Erneuter Zustellversuch nach 15min= $15m * 2^0$
   – Erneuter Zustellversuch nach 30min= $15m * 2^1$
   – Erneuter Zustellversuch nach 1h = $15m * 2^2$
   – Erneuter Zustellversuch nach 2h = $15m * 2^3$
   – Erneuter Zustellversuch nach 4h = $15m * 2^4$
   – Erneuter Zustellversuch nach 8h = $15m * 2^5$
   – Alle weiteren Zustellversuche nach16h = $15m * 2^6$

   bis *maxQueueLifeTime* (Voreinstellung 5 Tage) erreicht ist.

Bei der Reduzierung der *smtpRetryTimeBase* sollte gleichzeitig der Wert für *smtpRetryTimeMaxExp* erhöht werden, ansonsten belasten die häufigen Wiederholungen der Zustellversuche die CPU.

tempFilePrefix

Beim Unterzeichnen oder bei der Verschlüsselung mit S/MIME werden temporäre Dateien verwendet. Die Namen dieser temporären Dateien sind aus einem Präfix und verschiedenen Suffixes zusammengesetzt. Das Präfix wird in der Option *tempFilePrefix* spezifiziert.

Diese Option ermöglicht es, die Dateien auf einem Pubset und/oder unter einer User-ID abzulegen, die vom Standard-Pubset oder der TSOS-Kennung abweicht. Dazu muss im Präfix eine Cat-ID oder eine User-ID angegeben werden.

tempFilePrefix
<präfix>

<präfix>
Präfix für den Namen der temporären Dateien.
Voreinstellung: #SYSDAT.MAIL.SMIME-TMP

tlsSecureConnection

Mit der Option *tlsSecureConnection* wird festgelegt, ob die SMTP-Verbindung zum SMTP-Server mit TLS abgesichert werden soll.

tlsSecureConnection
NONE | **OPTIONAL | REQUIRE**

NONE
Die SMTP-Verbindung wird nie abgesichert (Voreinstellung).

OPTIONAL
Die SMTP-Verbindung wird abgesichert, wenn der SMTP-Server die Absicherung unterstützt. Andernfalls wird eine ungesicherte Verbindung benutzt.

REQUIRE
Die SMTP-Verbindung wird geschlossen, wenn der SMTP-Server die Absicherung nicht unterstützt.

tlsProtocol

OpenSSL unterstützt das SSL-Protokoll in der Version 3 sowie das TLS-Protokoll in den Versionen 1, 1.1 und 1.2. Mit der Option *-tlsProtocol* können einige dieser Protokolle selektiv aktiviert werden.

tlsProtocol
[**+** | **-**] {**SSLv3** | **TLSv1** | **TLSv1**.1 | **TLSv1**.2 | **All** } ...

+
Das nachfolgend spezifizierte Protokoll ist zugelassen.

-
Das nachfolgend spezifizierte Protokoll ist nicht zugelassen.

Wenn weder „+“ noch „-“ angegeben werden, hat dies dieselbe Wirkung wie die Angabe von „+“.

SSLv3
SSL-Protokoll der Version 3

Das SSL-Protokoll in der Version 3 weist einige sicherheitstechnische Mängel auf und sollte nach Möglichkeit nicht verwendet werden.

TLSv1
TLS-Protokoll der Version 1

TLSv1.1
TLS-Protokoll der Version 1.1

TLSv1.2
TLS-Protokoll der Version 1.2

ALL
Alle Protokolle sollen aktiviert werden.

All -SSLv3 ist Voreinstellung.

Beispiel

Die Angaben `-tlsProtocol TLSv1 TLSv1.1 TLSv1.2` und `-tlsProtocol All -SSLv3` haben dieselbe Wirkung, solange keine Unterstützung für die zukünftige TLS-Protokollversion 1.3 zum MAIL-Sender hinzugefügt wird.

tlsCipherSuite

Mit der Option *tlsCipherSuite* wird eine Verschlüsselungsverfahren-Vorzugsliste spezifiziert. Falls diese Option nicht angegeben wird, wird eine voreingestellte Vorzugsliste verwendet.

tlsCipherSuite
<spezifikation>

<spezifikation>
Spezifikation in einer Verschlüsselungsverfahren-Vorzugsliste, siehe Kapitel „Spezifikation einer Vorzugsliste für Verschlüsselungsverfahren“ auf Seite 383.
Voreinstellung: ALL: !EXP: !ADH:!RC4

tlsCertificateFile

Mit der Option *tlsCertificateFile* wird eine Datei spezifiziert, die das X.509-Client-Zertifikat im PEM-Format enthält. Diese Datei kann auch den privaten Client-Schlüssel enthalten. In der Regel werden aber Zertifikat und Schlüssel in getrennten Dateien abgelegt. In diesem Fall wird die Schlüsseldatei mithilfe der Option *tlsKeyFile* (siehe unten) spezifiziert.

tlsCertificateFile
<dateiname 1 .. 54> | ***NONE**

<dateiname 1 .. 54>
Name der Datei, die das X.509-Client-Zertifikat im PEM-Format enthält.

***NONE**
Es wird keine Datei mit Zertifikaten verwendet (Voreinstellung).

tlsKeyFile

Mit der Option *tlsKeyFile* wird eine Datei spezifiziert, die den privaten Client-Schlüssel im PEM-Format enthält.

Wenn sowohl Zertifikat als auch privater Schlüssel innerhalb derselben Datei enthalten sind (siehe Option *tlsCertificateFile* oben), braucht die Option *tlsKeyFile* nicht angegeben zu werden.

Der Client-Schlüssel darf nicht mit einer Pass-Phrase gesichert werden, da beim Start der Service-Task keine Möglichkeit besteht, eine Pass-Phrase einzugeben.

tlsKeyFile
<dateiname 1 .. 54> | ***NONE**

<dateiname 1 .. 54>
Name der Datei, die den privaten Client-Schlüssel enthält.
Voreinstellung: Dateiname, der mit *tlsCertificateFile* spezifiziert wurde.

***NONE**
Es wird keine eigene Datei für den Client-Schlüssel verwendet.

tlsCACertificateFile

Mit der Option *tlsCACertificateFile* wird eine Datei spezifiziert, die die für die Authentifizierung am Server erforderlichen CA-Zertifikate im PEM-Format enthält. Die einzelnen PEM-Zertifikate sind sequenziell in der Datei angeordnet.

Zum Hinzufügen oder Löschen von Zertifikaten können Sie die Datei mit einem beliebigen Text-Editor bearbeiten. Die einzelnen Zertifikate sind wie folgt in der Datei notiert:

```
-----BEGIN CERTIFICATE-----
< CA-Zertifikat in Base64-Codierung >
-----END CERTIFICATE-----
```

Text außerhalb dieser Sequenzen wird ignoriert und kann deshalb zum Kennzeichnen der Zertifikate verwendet werden, die wegen der ASN.1/Base64-Codierung in nicht lesbarer Form vorliegen.

tlsCACertificateFile
<dateiname 1 .. 54> | ***NONE**

<dateiname 1 .. 54>
: Name der Datei, die die für die Authentifizierung am Server erforderlichen Zertifikate im PEM-Format enthält.

***NONE**
: Es wird keine Datei spezifiziert (Voreinstellung).

tlsCARevocationFile

Mit der Option *tlsCARevocationFile* wird eine Datei spezifiziert, die die CRLs (Certificate Revocation List) der Zertifizierungsinstanzen (Certificate Authorithy, CA) enthält. Zertifikate, die von einer Zertifizierungsinstanz herausgegeben wurden, können durch Veröffentlichung einer so genannten Certificate Revocation List (CRL) für ungültig erklärt werden.

tlsCARevocationFile
<dateiname 1 .. 54> | ***NONE**

<dateiname 1 .. 54>
Name der Datei, die die CRLs der Zertifizierungsinstanzen enthält.

***NONE**
Es wird keine Datei mit CRLs spezifiziert (Voreinstellung).

tlsVerifyServer

Mit der Option *tlsVerifyServer* wird festgelegt, ob ein Server-Zertifikat verifiziert werden muss.

tlsVerifyServer
YES | **NO**

YES
Das Zertifikat muss verifiziert werden (Voreinstellung).

NO
Das Zertifikat muss nicht verifiziert werden. In diesem Fall besteht die Gefahr, dass ein Angreifer („man in the middle“) sich unbemerkt in die Verbindung zwischen Mail-Sender Backend und Mail-Server einklinken und so den Daten-Transfer abhören kann.

tlsVerifyDepth

Mit der Option *tlsVerifyDepth* wird die sogenannte Verifizierungstiefe festgelegt, d.h. die Anzahl der maximal zulässigen Zertifikate zwischen dem Server-Zertifikat und dem Zertifikat, das der Service-Task bekannt ist.

- Die Voreinstellung für die maximale Tiefe ist 1. In diesem Fall muss das Server-Zertifikat, damit es akzeptiert wird, direkt von einer Certificate Authority (CA) erteilt worden sein, die der Service-Task bekannt ist.
- Wird die maximale Tiefe überschritten, dann wird die Verbindung abgebrochen, sofern nicht aufgrund von *tlsVerifyServer* (siehe Seite 372) die Verifizierung des Server-Zertifikats ausgeschaltet ist.
- Die Spezifikation der Tiefe 0 ist nicht sinnvoll. In diesem Fall wären nur selbstsignierte Zertifikate zulässig.

tlsVerifyDepth
<tiefe>

<tiefe>
Anzahl der maximal zulässigen Zertifikate zwischen dem Server-Zertifikat und dem Zertifikat, das der Service-Task bekannt ist.
Voreinstellung: 1

11.3 Mail Service-Kommandos

START-MAIL-SERVICE

Das Kommando START-MAIL-SERVICE startet die ASTI-Service-Task, die den SMTP-Dialog mit dem Mail-Server abwickelt.

Domain
SYSTEM-MANAGEMENT

Privileges
TSOS

START-MAIL-SERVICE
ORDER-LIMIT = **255** / <integer 1..32000> **,CONFIGURATION-FILE** = ***STD** / <filename 1..54 without-gen>

Beschreibung der Operanden

ORDER-LIMIT = 255 / <integer 1..32000>
Dieser Operand gibt an, wieviele Aufträge zu einer Zeit aktiv sein dürfen.

CONFIGURATION-FILE = *STD / <filename 1..54 without-gen>
Gibt die Datei an, die die Konfigurationsoptionen für die Service-Task enthält. Den Inhalt der Datei finden Sie im Abschnitt „Konfigurationsdatei für das Mail-Sender Backend“ auf Seite 357.

CONFIGURATION-FILE = *STD
Der Dateiname, der in Option *backendConfigurationFileName* in der Datei *SYSSSI* festgelegt wurde, wird für die Abfrage der Konfigurationsoptionen verwendet (siehe Abschnitt „SYSSSI“ auf Seite 353.

CONFIGURATION-FILE = <filename 1..54 without-gen>
Gibt die Datei an, die die Konfigurationsoptionen enthält.

Kommando-Returncodes

(SC2)	SC1	Maincode	Bedeutung / garantierte Meldungen
	0	CMD0001	Kein Fehler
	1	CMD0202	Syntax-Fehler
	64	CMD0216	Der Benutzer hat keine Berechtigung für das Kommando
	64	YML0120	Subsystem ASTI ist nicht verfügbar
	64	YML0130	Die Konfigurationsdatei ist nicht lesbar oder existiert nicht
	64	YML0132	ASTI meldet einen Fehler
	64	YML0134	Der ASTI-Service läuft schon
	64	YML0136	Das Programm für das Mail-Sender Backend kann nicht gefunden werden.

MODIFY-MAIL-SERVICE-PARAMETER

Mit dem Kommando MODIFY-MAIL-SERVICE-PARAMETER ändern Sie verschiedene Parameter der ASTI-Service-Task. Insbesondere können Sie hier die Datei verändern, die die Konfiguration für das Mail-Sender Backend enthält. Außerdem können Sie einigen Parametern, die die Protokollierung festlegen, Werte zuweisen, die vom Inhalt der Konfigurationsdatei abweichen. Auf diese Weise ist eine dynamische Änderung der Protokoll-Dateien oder der Menge der Logging-Events möglich, ohne dass die Konfigurationsdatei geändert werden muss.

Da das Kommando mit der Service-Task zusammenarbeitet, kann sich der Abschluss des Kommandos verzögern, wenn die Service-Task einen Rückstand von vorher übermittelten Aufträgen hat, die zuerst verarbeitet werden müssen.

Domain
SYSTEM-MANAGEMENT

Privileges
TSOS

MODIFY-MAIL-SERVICE-PARAMETER

CONFIGURATION-FILE = **<u>*UNCHANGED</u>** / <filename 1..54 without-gen>

,MAIL-LOG-FILE = **<u>*UNCHANGED</u>** / <filename 1..54 without-gen>

,TRACE-FILE = ***UNCHANGED** / <filename 1..54 without-gen>

,ASTI-TRACE-LEVEL = **<u>*UNCHANGED</u>** / ***NONE** / ***ALERT** / ***CRITICAL** / ***ERROR** / ***WARNING** / ***NOTICE** / ***INFO** / ***DEBUG**

,SMTP-TRACE-LEVEL = **<u>*UNCHANGED</u>** / ***NONE** / ***ALERT** / ***CRITICAL** / ***ERROR** / ***WARNING** / ***NOTICE** / ***INFO** / ***DEBUG**

,TLS-TRACE-LEVEL = **<u>*UNCHANGED</u>** / ***NONE** / ***ALERT** / ***CRITICAL** / ***ERROR** / ***WARNING** / ***NOTICE** / ***INFO** / ***DEBUG**

,SMIME-TRACE-LEVEL = **<u>*UNCHANGED</u>** / ***NONE** / ***ALERT** / ***CRITICAL** / ***ERROR** / ***WARNING** / ***NOTICE** / ***INFO** / ***DEBUG**

,OTHER-TRACE-LEVEL = **<u>*UNCHANGED</u>** / ***NONE** / ***ALERT** / ***CRITICAL** / ***ERROR** / ***WARNING** / ***NOTICE** / ***INFO** / ***DEBUG**

Beschreibung der Operanden

CONFIGURATION-FILE = <u>*UNCHANGED</u> / <filename 1..54 without-gen>
Gibt die Datei an, die die Konfigurationsoptionen für die Service-Task enthält. Den Inhalt der Datei finden Sie im Abschnitt „Konfigurationsdatei für das Mail-Sender Backend“ auf Seite 357.

CONFIGURATION-FILE = *UNCHANGED
Der Name der Konfigurationsdatei bleibt unverändert.

CONFIGURATION-FILE = <filename 1..54 without-gen>
Gibt die Datei an, die die Konfigurationsoptionen für die Service-Task enthält. Wird der Name der aktuell verwendeten Konfigurationsdatei angegeben, dann bewirkt dies, dass diese Datei erneut eingelesen wird und Änderungen an dieser Datei wirksam werden.

MAIL-LOG-FILE = *UNCHANGED / <filename 1..54 without-gen>
Gibt den Namen der Datei an, in die das Mail-Sende-Ergebnis protokolliert werden soll (siehe Option *mailLogFile* auf Seite 362). Auf die Datei kann nicht zugegriffen werden, wenn der Mail-Service läuft. Um die Datei zu öffnen, muss daher die Zuweisung (temporär) auf eine andere Datei gelegt werden.

MAIL-LOG-FILE = *UNCHANGED
Der Name der Mail-Protokolldatei bleibt unverändert.

MAIL-LOG-FILE = <filename 1..54 without-gen>
Gibt den Namen der Datei an, in die das Mail-Sende-Ergebnis protokolliert werden soll.

TRACE-FILE = *UNCHANGED / <filename 1..54 without-gen>
Gibt den Namen der Datei an, in die Diagnose-Meldungen protokolliert werden sollen (siehe Option *logFile* auf Seite 357). Auf die Datei kann nicht zugegriffen werden, wenn der Mail-Service läuft. Um die Datei zu öffnen, muss daher die Zuweisung (temporär) auf eine andere Datei gelegt werden.

TRACE-FILE = *UNCHANGED
Der Name der Protokolldatei bleibt unverändert.

TRACE-FILE = <filename 1..54 without-gen>
Gibt den Namen der Datei an, in die Diagnose-Meldungen protokolliert werden sollen.

ASTI-TRACE-LEVEL = *UNCHANGED / *NONE / *ALERT / *CRITICAL / *ERROR / *WARNING / *NOTICE / *INFO / *DEBUG
Gibt den Filter-Level für die Protokollierung von Diagnose-Meldungen bezüglich der ASTI-Aktionen an (siehe Option *logLevel* auf Seite 358).

SMTP-TRACE-LEVEL = *UNCHANGED / *NONE / *ALERT / *CRITICAL / *ERROR / *WARNING / *NOTICE / *INFO / *DEBUG
Gibt den Filter-Level für die Protokollierung von Diagnose-Meldungen bezüglich des SMTP-Protokolls an (siehe Option *logLevel* auf Seite 358).

TLS-TRACE-LEVEL = *UNCHANGED / *NONE / *ALERT / *CRITICAL / *ERROR / *WARNING / *NOTICE / *INFO / *DEBUG
Gibt den Filter-Level für die Protokollierung von Diagnose-Meldungen bezüglich des TLS-Protokolls an (siehe Option *logLevel* auf Seite 358).

SMIME-TRACE-LEVEL = *UNCHANGED / *NONE / *ALERT / *CRITICAL / *ERROR / *WARNING / *NOTICE / *INFO / *DEBUG
Gibt den Filter-Level für die Protokollierung von Diagnose-Meldungen bezüglich der S/MIME-Aktionen an (siehe Option *logLevel* auf Seite 358).

OTHER-TRACE-LEVEL = *UNCHANGED / *NONE / *ALERT / *CRITICAL / *ERROR / *WARNING / *NOTICE / *INFO / *DEBUG
Gibt den Filter-Level für die Protokollierung von Diagnose-Meldungen bezüglich anderer Aktionen an (siehe Option *logLevel* auf Seite 358).

Kommando-Returncodes

(SC2)	SC1	Maincode	Bedeutung / garantierte Meldungen
	0	CMD0001	Kein Fehler
	1	CMD0202	Syntax-Fehler
	64	CMD0216	Der Benutzer hat keine Berechtigung für das Kommando
	32	CMD0220	Interner Fehler
	64	YML0120	Subsystem ASTI ist nicht verfügbar
	64	YML0130	Die Konfigurationsdatei ist nicht lesbar oder existiert nicht
	64	YML0131	Fehler beim Zugriff auf Datei
	64	YML0140	Der Mail-Service läuft nicht
	64	YML0148	Das maximale Auftrags-Limit ist erreicht
	32	YML0176	Unerwarteter ASTI-Fehler

SHOW-MAIL-SERVICE-PARAMETER

Das Kommando SHOW-MAIL-SERVICE-PARAMETER gibt die aktuellen Einstellungen der Mail-Service-Parameter aus.

In manchen Fällen (wenn vorher kein Kommando MODIFY-MAIL-SERVICE-PARAMETER abgegeben wurde), arbeitet das Kommando mit der Service-Task zusammen. Daher kann sich der Abschluss des Kommandos verzögern, wenn die Service-Task einen Rückstand von vorher übermittelten Aufträgen hat, die zuerst verarbeitet werden müssen.

Domain
SYSTEM-MANAGEMENT

Privileges
TSOS

SHOW-MAIL-SERVICE-PARAMETER

Beispiel

```
/SHOW-MAIL-SERVICE-PARAMETER
%  Configuration file:    :DEFL:$TSOSDEFL.SYSDAT.MAIL.033.SERVICE.OPT
%  Mail log file:         $.SYSDAT.MAIL.033.MAILLOG
%  Trace file:            $.SYSDAT.MAIL.033.LOG
%  Trace level
%    ASTI:                *ERROR
%    SMTP:                *DEBUG
%    TLS:                 *ERROR
%    SMIME:               *INFO
%    OTHER:               *ERROR
```

Kommando-Returncodes

(SC2)	SC1	Maincode	Bedeutung / garantierte Meldungen
	0	CMD0001	Kein Fehler
	1	CMD0202	Syntax-Fehler
	64	CMD0216	Der Benutzer hat keine Berechtigung für das Kommando
	32	CMD0220	Interner Fehler
	64	YML0120	Subsystem ASTI ist nicht verfügbar
	64	YML0140	Der Mail-Service läuft nicht
	128	YML0148	Das maximale Auftrags-Limit ist erreicht
	32	YML0176	Unerwarteter ASTI-Fehler

STOP-MAIL-SERVICE

Das Kommando STOP-MAIL-SERVICE stoppt die ASTI-Service-Task, die den SMTP-Dialog mit dem Mail-Server abwickelt.

Domain
SYSTEM-MANAGEMENT

Privileges
TSOS

STOP-MAIL-SERVICE

Kommando-Returncodes

(SC2)	SC1	Maincode	Bedeutung / garantierte Meldungen
	0	CMD0001	Kein Fehler
	1	CMD0202	Syntax-Fehler
	64	CMD0216	Der Benutzer hat keine Berechtigung für das Kommando
	64	YML0120	Subsystem ASTI ist nicht verfügbar

11.4 Meldungen

Die Meldungen des Mail-Senders im BS2000 haben den Meldungsschlüssel `YMLnnnn`.

Ausgabe von Meldungen mit /HELP-MSG-INFORMATION

Mit dem BS2000-Kommando `/HELP-MSG-INFORMATION MSG-ID=YMLnnnn` können Sie die Bedeutungs- und Maßnahmetexte zu einer Meldung im laufenden Betrieb ausgeben.

Ausgabe von Meldungen im Internet

Die Meldungen finden Sie über eine HTML-Anwendung auf dem Manual-Server (*http://manuals.ts.fujitsu.com*) und auf der DVD „BS2000 SoftBooks“.

12 Spezifikation einer Vorzugsliste für Verschlüsselungsverfahren

Die Spezifikation besteht aus einem oder mehreren Chiffre-Mnemonics, die durch einen Doppelpunkt (:) getrennt sind.

Ein Chiffre-Mnemonic kann folgende Formen annehmen:

- Ein Chiffre-Mnemonic kann aus einer einzelnen Verschlüsselungs-Suite wie z.B. DES-CBC-SHA bestehen.
- Ein Chiffre-Mnemonic kann repräsentieren:
  - Liste von Verschlüsselungs-Suites, die einen bestimmten Algorithmus enthalten
  - Verschlüsselungs-Suites eines bestimmten Typs

  Beispielsweise repräsentiert SHA1 alle Verschlüsselungs-Suiten, die den Digest-Algorithmus SHA1 benutzen und SSLv3 repräsentiert alle SSL-Version 3-Algorithmen.
- Listen von Verschlüsselungs-Suiten können mithilfe des „+“-Zeichens zu einem einzelnen Chiffre-Mnemonic kombiniert werden. Dies wird dann als logische UND-Operation interpretiert. So repräsentiert SHA1+DES alle Verschlüsselungs-Suiten, die die SHA1- und DES-Algorithmen enthalten.

Jedem Chiffre-Mnemonic kann optional eines der Zeichen „!“, „-“ oder „+“ vorangestellt werden:

- Bei Voranstellen von „!“ werden die betreffenden Verschlüsselungs-Suiten dauerhaft aus der Vorzugsliste gelöscht. Sie erscheinen auch dann nicht wieder in der Vorzugsliste, wenn sie explizit angegeben werden.
- Bei Voranstellen von „-“ werden die betreffenden Verschlüsselungs-Suiten aus der Vorzugsliste gelöscht, aber einige von ihnen oder alle können durch nachfolgende Optionen wieder hinzugefügt werden.
- Bei Voranstellen von „+“ werden die betreffenden Verschlüsselungs-Suiten an das Ende der Vorzugsliste verschoben. Hiermit werden keine Verschlüsselungs-Suiten zur Vorzugsliste hinzugefügt, sondern nur existierende verschoben.

  - Wenn keines der drei Zeichen „!“, „-“ oder „+“ vorangestellt ist, wird der Chiffre-Mnemonic als eine Liste von Verschlüsselungs-Suiten interpretiert, die an die aktuelle Vorzugsliste angehängt wird. Wenn dies eine Verschlüsselungs-Suite einschließt, die schon in der aktuellen Vorzugsliste enthalten ist, dann wird diese ignoriert, sie wird nicht an das Ende der Vorzugsliste verschoben.

- Der Chiffre-Mnemonic @STRENGTH kann an beliebiger Stelle eingefügt werden, um die aktuelle Vorzugsliste nach der Länge der Verschlüsselungsschlüssel zu sortieren.

Zulässige Chiffre-Mnemonics

Nachfolgend sind die zulässigen Chiffre-Mnemonics beschrieben.

ALL
: Alle Verschlüsselungs-Suiten mit Ausnahme der eNULL-Chiffren. Letztere müssen explizit aktiviert werden.

HIGH
: Verschlüsselungs-Suiten mit Schlüssellängen größer 128 Bit.

MEDIUM
: Verschlüsselungs-Suiten mit Schlüssellänge 128 Bit oder aus anderen Gründen heruntergestufte Verschlüsselungs-Suiten.

LOW
: Verschlüsselungs-Suiten mit 64 oder 56 Bit Schlüssellänge, ausgenommen Export-Verschlüsselungs-Suiten.

EXP, EXPORT
: Export-Verschlüsselungs-Algorithmen einschließlich 40- und 56-Bit-Algorithmen.

EXPORT40
: 40-Bit-Export-Verschlüsselungs-Algorithmen.

EXPORT56
: 56-Bit-Export-Verschlüsselungs-Algorithmen.

eNULL, NULL
: „NULL“-Verschlüsselungs-Algorithmen, d.h. solche ohne Verschlüsselung. Da diese keine Verschlüsselung bieten und damit ein Sicherheitsrisiko sind, werden sie standardmäßig deaktiviert und müssen gegebenenfalls explizit angegeben werden.

aNULL
: Verschlüsselungs-Suiten ohne Authentifizierung. Dies sind im Augenblick die anonymen Diffie-Hellman-Algorithmen. Diese Algorithmen sind anfällig für „man in the middle“-Angriffe, so dass von ihrer Benutzung abgeraten wird.

kRSA, RSA
: Verschlüsselungs-Suiten mit RSA-Schlüsselaustausch.

aRSA
: Verschlüsselungs-Suiten mit RSA-Authentifizierung, d.h. die Zertifikate enthalten RSA-Schlüssel.

aDSS, DSS
: Verschlüsselungs-Suiten mit DSS-Authentifizierung, d.h. die Zertifikate enthalten DSS-Schlüssel.

TLSv1.2, TLSv1.0, SSLv3
: TLSv1.2, TLSv1.0 bzw. SSLv3-Verschlüsselungs-Suiten.

  Hinweis: Es gibt keine TLSv1.1-spezifischen Verschlüsselungs-Suiten.

DH
: Verschlüsselungs-Suiten mit Diffie-Hellman-Schlüsselaustausch, einschließlich anonymem Austausch.

ADH
: Verschlüsselungs-Suiten mit anonymem Diffie-Hellman-Schlüsselaustausch.

kEDH, kDHE
: Verschlüsselungs-Suiten mit kurzlebiger (ephemeral) Diffie-Hellman-Schlüsselvereinbarung, einschließlich anonymen Suiten.

kEECDH, kECDHE
: Verschlüsselungs-Suiten mit kurzlebiger (ephemeral) Elliptic Curve Diffie-Hellman-Schlüsselvereinbarung, einschließlich anonymen Suiten.

EECDH, ECDHE
: Verschlüsselungs-Suiten mit kurzlebiger (ephemeral) Elliptic Curve Diffie-Hellman-Schlüsselvereinbarung, ohne anonyme Suiten.

AECDH
: Anonyme Verschlüsselungs-Suiten mit Elliptic Curve Diffie-Hellman-Schlüsselvereinbarung.

ECDH
: Verschlüsselungs-Suiten mit Elliptic Curve Diffie-Hellman-Schlüsselvereinbarung, einschließlich anonymem, kurzlebigem und fixiertem ECDH.

AES128, AES256, AES
: Verschlüsselungs-Suiten, die 128-Bit AES, 256-Bit AES oder eins von beiden verwenden.

3DES
: Verschlüsselungs-Suiten mit Triple-DES-Verschlüsselung.

DES
: Verschlüsselungs-Suiten mit DES-Verschlüsselung (kein Triple-DES).

RC4
: Verschlüsselungs-Suiten mit RC4-Verschlüsselung.

RC2
: Verschlüsselungs-Suiten mit RC2-Verschlüsselung.

MD5
: Verschlüsselungs-Suiten mit MD5-Hash-Funktion.

SHA1, SHA
: Verschlüsselungs-Suiten mit SHA1-Hash-Funktion.

Da praktikable Angriffe auf SHA1 immer näher rücken, sollte so schnell wie möglich auf Verschlüsselungs-Suiten gewechselt werden, die z.B. die Hash-Funktionen SHA256 bzw. SHA384 verwenden. Dies impliziert aber in der Regel auch den Wechsel auf TLS-Protokollversion 1.2.

SHA256, SHA384
: Verschlüsselungs-Suiten, die die SHA256- bzw. SHA384-Hash-Funktion für die MAC-(Message Authentication Code)-Berechnung verwenden. Bei Verschlüsselungs-Suiten, die AESGCM und damit AEAD (Authenticated Encryption with Associated Data) als MAC-Methode verwenden, hat das SHA256 bzw. SHA384 im Namen eine andere Bedeutung,

aECDSA
: Verschlüsselungs-Suiten, die ECDSA-Authentifizierung verwenden, d.h. die Zertifikate beinhalten ECDSA-Schlüssel.

AESGCM
: Verschlüsselungs-Suiten, die AES im "Galois Counter Mode (GCM)" verwenden. Diese Verschlüsselungs-Suiten werden nur durch TLSv1.2 unterstützt.

CAMELLIA128, CAMELLIA256, CAMELLIA
: Verschlüsselungs-Suiten, die 128-Bit CAMELLIA, 256-Bit CAMELLIA oder eins von beiden verwenden.

Die Auswahlwirkung einer Vorzugslistenspezifikation kann mit der Prozedur SHOW.CIPHERLIST (siehe “InterNet Services Benutzerhandbuch“) überprüft werden.

In der nachfolgenden Tabelle sind die verfügbaren Verschlüsselungs-Suiten zusammengefasst.

Name	Version	Schlüssel-Austausch	Authenti-fizierung	Verschlüsse-lung	Digest	Export
DHE-RSA-AES256-SHA	SSLv3	DH	RSA	AES(256)	SHA1	
DHE-DSS-AES256-SHA	SSLv3	DH	DSS	AES(256)	SHA1	

Verfügbare Verschlüsselungs-Suiten

Name	Version	Schlüssel-Austausch	Authenti-fizierung	Verschlüsse-lung	Digest	Export
AES256-SHA	SSLv3	RSA	RSA	AES(256)	SHA1	
DHE-RSA-AES128-SHA	SSLv3	DH	RSA	AES(128)	SHA1	
DHE-DSS-AES128-SHA	SSLv3	DH	DSS	AES(128)	SHA1	
AES-128-SHA	SSLv3	RSA	RSA	AES(128)	SHA1	
DHE-DSS-RC4-SHA	SSLv3	DH	DSS	RC4(128)	SHA1	
EDH-RSA-DES-CBC3-SHA	SSLv3	DH	RSA	3DES(168)	SHA1	
EDH-DSS-DES-CBC3-SHA	SSLv3	DH	DSS	3DES(168)	SHA1	
DES-CBC3-SHA	SSLv3	RSA	RSA	3DES(168)	SHA1	
RC4-SHA	SSLv3	RSA	RSA	RC4(128)	SHA1	
RC4-MD5	SSLv3	RSA	RSA	RC4(128)	MD5	
EDH-RSA-DES-CBC-SHA	SSLv3	DH	RSA	DES(56)	SHA1	
EDH-DSS-DES-CBC-SHA	SSLv3	DH	DSS	DES(56)	SHA1	
DES-CBC-SHA	SSLv3	RSA	RSA	DES(56)	SHA1	
DES-CBC3-MD5	SSLv2	RSA	RSA	3DES(168)	MD5	
RC2-CBC-MD5	SSLv2	RSA	RSA	RC2(128)	MD5	
RC4-MD5	SSLv2	RSA	RSA	RC4(128)	MD5	
RC4-64-MD5	SSLv2	RSA	RSA	RC4(64)	MD5	
DES-CBC-MD5	SSLv2	RSA	RSA	DES(56)	MD5	
EXP1024-DHE-DSS-RC4-SHA	SSLv3	DH(1024)	DSS	RC4(56)	SHA1	export
EXP1024-RC4-SHA	SSLv3	RSA(1024)	RSA	RC4(56)	SHA1	export
EXP1024-DHE-DSS-DES-CBC-SHA	SSLv3	DH(1024)	DSS	DES(56)	SHA1	export
EXP1024-DES-CBC-SHA	SSLv3	RSA(1024)	RSA	DES(56)	SHA1	export
EXP1024-RC2-CBC-MD5	SSLv3	RSA(1024)	RSA	RC2(56)	MD5	export
EXP1024-RC4-MD5	SSLv3	RSA(1024)	RSA	RC4(56)	MD5	export
EXP-EDH-RSA-DES-CBC-SHA	SSLv3	DH(512)	RSA	DES(40)	SHA1	export
EXP-EDH-DSS-DES-CBC-SHA	SSLv3	DH(512)	DSS	DES(40)	SHA1	export
EXP-DES-CBC-SHA	SSLv3	RSA(512)	RSA	DES(40)	SHA1	export
EXP-RC2-CBC-MD5	SSLv3	RSA(512)	RSA	RC2(40)	MD5	export
EXP-RC4-MD5	SSLv3	RSA(512)	RSA	RC4(40)	MD5	export
EXP-RC2-CBC-MD5	SSLv2	RSA(512)	RSA	RC2(40)	MD5	export
EXP-RC4-MD5	SSLv2	RSA(512)	RSA	RC4(40)	MD5	export
ADH-AES256-SHA	SSLv3	DH	keine	AES(256)	SHA1	

Verfügbare Verschlüsselungs-Suiten

Name	Version	Schlüssel-Austausch	Authenti-fizierung	Verschlüsse-lung	Digest	Export
ADH-AES128-SHA	SSLv3	DH	keine	AES(128)	SHA1	
ADH-DES-CBC3-SHA	SSLv3	DH	keine	3DES(168)	SHA1	
ADH-DES-CBC-SHA	SSLv3	DH	keine	DES(56)	SHA1	
ADH-RC4-MD5	SSLv3	DH	keine	RC4(128)	MD5	
EXP-ADH-DES-CBC-SHA	SSLv3	DH(512)	keine	DES(40)	SHA1	export
EXP-ADH-RC4-MD5	SSLv3	DH(512)	keine	RC4(40)	MD5	export
NULL-SHA	SSLv3	RSA	RSA	keine	SHA1	
NULL-MD5	SSLv3	RSA	RSA	keine	MD5	
ECDHE-ECDSA-AES128-SHA	SSLv3	ECDH	ECDSA	AES(128)	SHA1	
ECDHE-ECDSA-AES256-SHA	SSLv3	ECDH	ECDSA	AES(256)	SHA1	
ECDHE-ECDSA-DES-CBC3-SHA	SSLv3	ECDH	ECDSA	3DES(168)	SHA1	
ECDHE-ECDSA-RC4-SHA	SSLv3	ECDH	ECDSA	RC4(128)	SHA1	
ECDHE-ECDSA-NULL-SHA	SSLv3	ECDH	ECDSA	keine	SHA1	
ECDHE-RSA-AES256-SHA	SSLv3	ECDH	RSA	AES(256)	SHA1	
ECDHE-RSA-AES128-SHA	SSLv3	ECDH	RSA	AES(128)	SHA1	
ECDHE-RSA-DES-CBC3-SHA	SSLv3	ECDH	RSA	3DES(168)	SHA1	
ECDHE-RSA-RC4-SHA	SSLv3	ECDH	RSA	RC4(128)	SHA1	
ECDHE-RSA-NULL-SHA	SSLv3	ECDH	RSA	keine	SHA1	
AECDH-AES256-SHA	SSLv3	ECDH	keine	AES(256)	SHA1	
AECDH-AES128-SHA	SSLv3	ECDH	keine	AES(128)	SHA1	
AECDH-DES-CBC3-SHA	SSLv3	ECDH	keine	3DES(168)	SHA1	
AECDH-RC4-SHA	SSLv3	ECDH	keine	RC4(128)	SHA1	
AECDH-NULL-SHA	SSLv3	ECDH	keine	keine	SHA1	
DHE-RSA-CAMELLIA256-SHA	SSLv3	DH	RSA	Camellia(256)	SHA1	
DHE-RSA-CAMELLIA128-SHA	SSLv3	DH	RSA	Camellia(128)	SHA1	
DHE-DSS-CAMELLIA256-SHA	SSLv3	DH	DSS	Camellia(256)	SHA1	
DHE-DSS-CAMELLIA128-SHA	SSLv3	DH	DSS	Camellia(128)	SHA1	
CAMELLIA256-SHA	SSLv3	RSA	RSA	Camellia(256)	SHA1	
CAMELLIA128-SHA	SSLv3	RSA	RSA	Camellia(128)	SHA1	
ADH-CAMELLIA256-SHA	SSLv3	DH	keine	Camellia(256)	SHA1	
ADH-CAMELLIA128-SHA	SSLv3	DH	keine	Camellia(128)	SHA1	
ECDHE-ECDSA-AES256-GCM-SHA384	TLSv1.2	ECDH	ECDSA	AESGCM(256)	AEAD	

Verfügbare Verschlüsselungs-Suiten

Name	Version	Schlüssel-Austausch	Authenti-fizierung	Verschlüsse-lung	Digest	Export
ECDHE-ECDSA-AES128-GCM-SHA256	TLSv1.2	ECDH	ECDSA	AESGCM(128)	AEAD	
ECDHE-RSA-AES256-GCM-SHA384	TLSv1.2	ECDH	RSA	AESGCM(256)	AEAD	
ECDHE-RSA-AES128-GCM-SHA256	TLSv1.2	ECDH	RSA	AESGCM(128)	AEAD	
AES256-GCM-SHA384	TLSv1.2	RSA	RSA	AESGCM(256)	AEAD	
AES128-GCM-SHA256	TLSv1.2	RSA	RSA	AESGCM(128)	AEAD	
DHE-RSA-AES256-GCM-SHA384	TLSv1.2	DH	RSA	AESGCM(256)	AEAD	
DHE-RSA-AES128-GCM-SHA256	TLSv1.2	DH	RSA	AESGCM(128)	AEAD	
DHE-DSS-AES256-GCM-SHA384	TLSv1.2	DH	DSS	AESGCM(256)	AEAD	
DHE-DSS-AES128-GCM-SHA256	TLSv1.2	DH	DSS	AESGCM(128)	AEAD	
ADH-AES256-GCM-SHA384	TLSv1.2	DH	keine	AESGCM(256)	AEAD	
ADH-AES128-GCM-SHA256	TLSv1.2	DH	keine	AESGCM(128)	AEAD	
ECDHE-ECDSA-AES256-SHA384	TLSv1.2	ECDH	ECDSA	AES(256)	SHA384	
ECDHE-ECDSA-AES128-SHA256	TLSv1.2	ECDH	ECDSA	AES(128)	SHA256	
ECDHE-RSA-AES256-SHA384	TLSv1.2	ECDH	RSA	AES(256)	SHA384	
ECDHE-RSA-AES128-SHA256	TLSv1.2	ECDH	RSA	AES(128)	SHA256	
DHE-RSA-AES256-SHA256	TLSv1.2	DH	RSA	AES(256)	SHA256	
DHE-RSA-AES128-SHA256	TLSv1.2	DH	RSA	AES(128)	SHA256	
DHE-DSS-AES256-SHA256	TLSv1.2	DH	DSS	AES(256)	SHA256	
DHE-DSS-AES128-SHA256	TLSv1.2	DH	DSS	AES(128)	SHA256	
AES256-SHA256	TLSv1.2	RSA	RSA	AES(256)	SHA256	
AES128-SHA256	TLSv1.2	RSA	RSA	AES(128)	SHA256	
ADH-AES256-SHA256	TLSv1.2	DH	keine	AES(256)	SHA256	
ADH-AES128-SHA256	TLSv1.2	DH	keine	AES(128)	SHA256	

Verfügbare Verschlüsselungs-Suiten

Literatur

Die Handbücher sind online unter *http://manuals.ts.fujitsu.com* zu finden oder in gedruckter Form gegen gesondertes Entgelt unter *http://manualshop.ts.fujitsu.com* zu bestellen.

openNet Server
BCAM
Benutzerhandbuch

interNet Services
Benutzerhandbuch

openNet Server
IPv6 Einführung und Umstellhandbuch Stufe 1
Benutzerhandbuch

openNet Server
IPSec
Benutzerhandbuch

openNet Server, interNet Services
SNMP-Management für openNet Server und interNet Services
Benutzerhandbuch

SOCKETS(BS2000)
SOCKETS für BS2000/OSD
Benutzerhandbuch

POSIX (BS2000/OSD)
SOCKETS/XTI für POSIX
Benutzerhandbuch

CMX (BS2000)
Kommunikationsmethode im BS2000
Benutzerhandbuch

SNMP Management V5.0
SNMP Management für BS2000/OSD
Benutzerhandbuch

SNMP Management V6.0
SNMP Management für BS2000/OSD
Benutzerhandbuch

C-Bibliotheksfunktionen (BS2000/OSD)
für POSIX-Anwendungen
Referenzhandbuch

XHCS (BS2000/OSD)
8-bit-Code-Verarbeitung im BS2000/OSD
Benutzerhandbuch

BS2000
Benutzerkommandos (ISP-Format)
Benutzerhandbuch

BS2000 OSD-BC
Kommandos
Benutzerhandbuch

BS2000 OSD-BC
Makroaufrufe an den Ablaufteil
Benutzerhandbuch

IMON (BS2000/OSD)
Installationsmonitor
Benutzerhandbuch

BS2000 OSD-BC
Einführung in die Systembetreuung
Benutzerhandbuch

Zusätzliche Literatur

SSL and TLS
Designing and Building Secure Systems
von Eric Rescorla
ISBN 0-201-61598-3

Inhalt
Ausführliche Beschreibung von SSL und TLS und des Anwendungumfelds

Secrets & Lies
IT-Sicherheit in einer vernetzten Welt
von Bruce Schneier
ISBN 3-89864-113-9

Inhalt
Tour d'horizon durch die IT-Sicherheit

Die englische Originalausgabe "Secrets & Lies" ist unter der ISBN 0-471-25311-1 erhältlich.

Postfix
The Definitive Guide
von Kyle D. Dent
ISBN 0-596-00212-2 (Original-Ausgabe)
ISBN 3-89721-372-9 (Deutsche Übersetzung)

Inhalt
Relativ kompakte und aktuelle Einführung in Konfiguration und Nutzung des Postfix-Mail-Servers.

http://shop.oreilly.com/product/9780596002121.do

Das Postfix-Buch
Sichere Mail-Server mit Linux

von Peter Heinlein
ISBN 1-53693991-9

Inhalt
Eine Linux-zentrierte Postfix-Beschreibung, die relativ breit auch nicht-Postfix-spezifische Mail-Themen abhandelt (Rechtliche Aspekte, allgemeine Server-Sicherheit).

Postfix
Einrichtung, Betrieb und Wartung
von Ralf Hildebrandt und Patrick Koetter
ISBN 3-89864-518-5

Inhalt
Breite Darstellung der Themen Mail-Transport-Beschränkungen und Mail-Filterung. Außerdem erhält das Buch von den hier genannten Büchern die detaillierteste Beschreibung der TLS-Nutzung. Theorie-orientierte Kapitel werden durch ausführliche praktische Fall-Beispiele ergänzt (meist anhand von Linux-Systemen).

http://www.postfix-buch.com/

RFCs

Umfassende Informationen zu den Request for Comments (RFCs) finden Sie auf der Home Page der Internet Engineering Task Force (IETF):

www.ietf.org

Stichwörter

A

E

N

T