Deutsch

FUJITSU

openFT V12.0 für Unix-Systeme

Installation und Administration

Systemverwalterhandbuch

Ausgabe September 2012

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

Die openFT-Produktfamilie überträgt und verwaltet Daten

– automatisiert
– sicher
– kostengünstig.

Das sichere und komfortable Übertragen von Daten - der File Transfer - ist eine wichtige Funktion in einem leistungsfähigen Rechnerverbund. Innerhalb eines Unternehmens sind die Arbeitsplatz-PCs untereinander vernetzt und meistens mit einem Mainframe, einem Unix-basierten Server oder einem Windows-Server gekoppelt. So kann ein großer Teil der Verarbeitungsleistung direkt am Arbeitsplatz erbracht werden, während für andere Fälle Daten via File Transfer zum Mainframe übertragen und dort weiterverarbeitet werden. Dabei können die Standorte der einzelnen Rechner weit voneinander entfernt liegen. Fujitsu Technology Solutions bietet eine umfangreiche File-Transfer-Produktlinie, die openFT-Produktfamilie, für folgende Systemplattformen:

- BS2000/OSD®
- Solaris™ (SPARC®/Intel™), LINUX®, AIX®, HP-UX®
- Microsoft® Windows Vista™, Windows™ 7, Windows Server 2008™ und Windows Server 2008 R2™
- z/OS (IBM®)

1.1 Kurzbeschreibung des Produkts

openFT für Unix-Systeme ist das File-Transfer-Produkt für Rechner mit einem Unix-basierten Betriebssystem.

Alle openFT-Produkte kommunizieren untereinander über das durch Fujitsu festgelegte openFT-Protokoll (früher: FTNEA-Protokoll). Da auch etliche andere FT-Produkte dieses Protokoll unterstützen, bestehen vielfältige Kopplungsmöglichkeiten zu anderen Betriebssystemen.

Wird zusätzlich openFT-FTAM eingesetzt, dann unterstützt openFT außerdem das in der ISO-Norm FTAM (ISO - International Organization for Standardization, FTAM - File Transfer Access and Management) standardisierte File-Transfer-Protokoll. Dadurch sind weitere Kopplungen zu Systemen anderer Hersteller möglich, deren File-Transfer-Produkte diese Norm ebenfalls unterstützen.

Wird zusätzlich openFT-FTP eingesetzt, dann unterstützt openFT auch das FTP-Protokoll. Damit ist eine Kopplung zu beliebigen FTP-Servern möglich.

openFT bietet mit der integrierten FTAC-Funktion einen erweiterten Zugangs- und Zugriffsschutz (FTAC steht für **F**ile **T**ransfer **A**ccess **C**ontrol).

1.2 Zielsetzung und Zielgruppen des Handbuchs

Dieses Handbuch enthält die Informationen, die der openFT-, der FTAC- und der ADM-Verwalter eines Unix-Systems für ihre Arbeit brauchen und die nicht im Benutzerhandbuch beschrieben sind.

Für allgemeine Informationen zur Dateiübertragung und zum Dateimanagement benötigen Sie zusätzlich das Benutzerhandbuch. Weitere Literaturhinweise finden Sie im Literaturverzeichnis.

Das Handbuch ist gültig für Oracle Solaris-Systeme sowie für die Portierungen auf andere Unix-Plattformen. Die betriebssystemabhängigen Unterschiede werden ausführlich in der Freigabemitteilung beschrieben, die auf der jeweiligen Produkt-CD mit ausgeliefert wird.

1.3 Handbuchkonzept von openFT für Unix-Systeme

Die vollständige Beschreibung von openFT und seinen optionalen Komponenten umfasst vier Handbücher. Die Beschreibung ist folgendermaßen auf die Handbücher verteilt:

- openFT für Unix-Systeme - Installation und Administration
  Das Systemverwalterhandbuch richtet sich an FT-, FTAC- und ADM-Verwalter. Es beschreibt:
  – die Installation von openFT und seinen optionalen Komponenten
  – Betrieb, Steuerung und Überwachung des FT-Systems und der FTAC-Umgebung
  – die Administrationskommandos für FT- und FTAC-Verwalter
  – die Konfiguration und den Betrieb eines Fernadministrations-Servers und eines ADM-Trap-Servers
  – wichtige CMX-Kommandos
- openFT für Unix-Systeme - Managed File Transfer in der offenen Welt
  Das Benutzerhandbuch richtet sich an den openFT-Benutzer und beschreibt:
  – die grundsätzlichen Funktionen der openFT-Produktfamilie
  – die Konventionen für den File Transfer zu Rechnern mit verschiedenen Betriebssystemen
  – Details zur Realisierung von FTAM
  – die openFT-Benutzerkommandos
  – die openFT-Script-Kommandos
  – Meldungen der verschiedenen Komponenten
- openFT für Unix- und Windows-Systeme - C-Programmschnittstelle
  Dieses Handbuch richtet sich an C-Programmierer und beschreibt die C-Programmschnittstelle auf Unix- und Windows-Systemen.
- openFT für Unix- und Windows-Systeme - openFT-Script-Schnittstelle
  Dieses Handbuch richtet sich an XML-Programmierer und beschreibt:
  – die openFT-Script-Kommandos
  – die XML-Anweisungen der openFT-Script-Schnittstelle

Viele der in den Handbüchern beschriebenen Funktionen sind auch über die grafische Oberfläche von openFT, den openFT Explorer, verfügbar. Mit dem openFT Explorer wird eine ausführliche Online-Hilfe ausgeliefert, in der die Bedienung mit allen Dialogen beschrieben wird.

1.4 Änderungen gegenüber der vorigen Version

In diesem Abschnitt finden Sie die Änderungen von openFT V12.0 für Unix-Systeme gegenüber openFT V11.0 für Unix-Systeme.

Die funktionalen Erweiterungen der openFT-Kommandos, die entweder den Verwalter oder den Benutzer betreffen, stehen auch im openFT Explorer zur Verfügung. Details finden Sie in der zugehörigen Online-Hilfe unter dem Thema *Neue Funktionen*.

Konfigurations-Editor für Fernadministration

Mit dem neuen Konfigurations-Editor bietet openFT eine grafische Oberfläche, mit der eine Konfigurationsdatei für die Fernadministration erstellt oder geändert werden kann. Die Konfiguration ist sofort im Konfigurations-Editor als Baumstruktur sichtbar und entspricht der späteren Darstellung im openFT Explorer.

Der Konfigurations-Editor wird über den openFT Explorer gestartet.

Erweiterte Logging-Funktionen

Die Logging-Funktionen wurden wie folgt erweitert:

- Umschalten der Logging-Datei und Offline-Logging

  Die Logging-Datei kann im laufenden Betrieb gewechselt werden. Nach dem Umschalten werden neue Logging-Sätze in eine neue Logging-Datei geschrieben. Die bisherige Logging-Datei bleibt als Offline-Logging-Datei bestehen; ihre Logging-Sätze können weiterhin mit openFT-Mitteln angesehen werden.

  Dazu wurde die Kommandoschnittstelle wie folgt erweitert:

  – *ftmodo*:

    Neue Option *-lf=c* zum Umschalten der Logging-Datei.

  – *ftshwl*:

    Neue Optionen *-lf*, *-tlf* und *-plf* , um Logging-Sätze aus Offline-Logging-Dateien anzusehen.

    Neue Option *-llf*, um die Namen aller Logging-Dateien (einschließlich Offline-Logging-Dateien) auszugeben.

  – *ftdell*:

    Neues Selektionskriterium*-tlf*, um Offline-Logging-Dateien zu löschen.

- Automatisches Löschen von Logging-Sätzen

  Per Betriebsparameter können Zeitintervalle für das automatische Löschen von Logging-Sätzen eingestellt werden. Dazu wurde das Kommando *ftmodo* um die neuen Optionen *-ld*, *-lda*, *-ldd* und *-ldt* erweitert. Die Einstellungen können über das Kommando *ftshwo* angezeigt werden.

- Pollingfunktion für die Ausgabe von Logging-Sätzen

  Bei *ftshwl* lassen sich mit den neuen Optionen *-po* und *-pnr* Zeitintervall und Anzahl der Wiederholungen (Polling) einstellen.

- Wildcards für Partnernamen bei der Ausgabe von Logging-Sätzen

  Bei *ftshwl* kann man für den Partnernamen (*-pn=*) auch die Wildcard-Symbole „*“ und „?“ angeben.

Erweiterte Security-Funktionen

- Importieren von Schlüsseln

  Mit dem neuen Kommando *ftimpk* lassen sich sowohl extern erzeugte private Schlüssel als auch öffentliche Schlüssel von Partnersystemen importieren.

- Verfallsdatum und Authentifizierungsstufe von RSA-Schlüsseln

  – Mit dem neuen Kommando *ftmodk* kann man für Schlüssel, die zur Authentifizierung von Partnersystemen verwendet werden, ein Verfallsdatum festlegen und die Authentifizierungsstufe (1 oder 2) ändern.

  Die Authentifizierungsstufe 2 wurde mit openFT V11.0B eingeführt und erfüllt höhere Sicherheitsanforderungen.

  – Mit dem neuen Kommando *ftshwk* kann man die Eigenschaften der im System hinterlegten Schlüssel ausgeben.

  – Bei *ftshwl* wird die Authentifizierungsstufe angezeigt (Ausgabeparameter SEC-OPTS, neue Werte LAUTH2 und RAUTH2).

- Datenverschlüsselung erzwingen

  Mit der neuen Option *-c* im Kommando *ftmodo* kann die Datenverschlüsselung für Dateiübertragungs- und Administrations-Aufträge generell erzwungen werden. Die Einstellung ist getrennt für Inbound- und Outbound-Aufträge möglich.

- Nach Neuinstallation verwendet openFT standardmäßig einen RSA-Schlüssel mit der Länge 2048 Bit.

- PAM-Unterstützung

  Die Pluggable Authentication Modules (PAM) als Authentisierungsdienste zur Kennwortverschlüsselung im openFT werden für alle Plattformen unterstützt. Die Unterstützung für Solaris war schon in V11.0 vorhanden, aber noch nicht im Handbuch beschrieben.

- Dateizugriff und Berechtigungsprüfung unter Benutzerrechten

  Alle Zugriffe und Berechtigungsprüfungen durch openFT auf Dateien und Verzeichnisse eines Benutzers finden unter den Rechten des jeweiligen Benutzers statt.

Erweiterte Partnerverwaltung

- Ein Partner in der Partnerliste kann auch für Inbound-Aufträge explizit deaktiviert werden.

  Dazu wurde bei den Kommandos *ftaddptn* und *ftmodptn* die neue Option *-ist* eingeführt. Der aktuelle Zustand (aktiviert/deaktiviert) wird bei *ftshwptn* im Ausgabeparameter INBND angezeigt.

- Serialisierung von asynchronen Outbound-Aufträgen zu bestimmten Partnern

  Mit der neuen Option *-rqp* in den Kommandos *ftaddptn* und *ftmodptn* lässt sich steuern, ob asynchrone Outbound-Aufträge zu einem bestimmten Partner grundsätzlich seriell ausgeführt werden oder ob parallele Verbindungen erlaubt sind. Diese Eigenschaft wird bei *ftshwptn* im Ausgabeparameter REQU-P angezeigt.

Erweiterte Auftragsverwaltung

- Globale Auftrags-Identifikation

  Bei einem FT-Auftrag wird die Auftragsnummer des Initiators an den Responder übermittelt und ist dort als globale Auftrags-Identifikation sichtbar. Damit lässt sich ein Auftrag zwischen Initiator und Responder eindeutig zuordnen.

  Die Kommandos *ftshwr* und *ftshwl* wurden wie folgt erweitert:

  – Im Responder wird die globale Auftrags-Identifikation jeweils im neuen Ausgabeparameter GLOB-ID angezeigt.

  – Mit dem neuen Parameter *-gid* kann in beiden Kommandos nach einer globalen Auftrags-Identifikation selektiert werden.

Betrieb mit und ohne CMX

Mit der neuen Option *-cmx* im Kommando *ftmodo* kann zwischen den Betriebsmodi „mit CMX“ und „ohne CMX“ gewechselt werden. Der aktuelle Modus wird beim Kommando *ftshwo* im Ausgabeparameter USE CMX angezeigt.

Nach Neuinstallation ist der Betriebsmodus „ohne CMX“ eingestellt.

Erweiterte Diagnose

Mit der neuen Option -*troll* im Kommando *ftmodo* kann der Trace für die unteren Protokollschichten im laufendem Betrieb ein- und ausgeschaltet und der Trace-Umfang gesteuert werden.

Die aktuelle Einstellung wird beim Kommando *ftshwo* im Ausgabeparameter OPTIONS-LL (Zeile FUNC) angezeigt.

Erweiterung der C-Programmschnittstelle und der openFT-Script-Schnittstelle

Die Programmschnittstelle wurde um folgende Funktionsgruppen erweitert:

- *ft_sd** zur Ermittlung der Attribute aller Dateien eines Dateiverzeichnisses im fernen System.
- *ft_xc** zur synchronen Ausführung eines Kommandos im fernen System.

Die openFT-Script-Schnittstelle wurde um folgende Kommandos zum variablen Ablegen von openFT-Script-Aufträgen erweitert:

- *ft_modsuo* zum Ändern von openFT-Script-Benutzer-Optionen.
- *ft_shwsuo* zum Anzeigen von openFT-Script-Benutzer-Optionen.

Integration in Solaris SMF

openFT wird auf Solaris Systemen in das Service Management Facility (SMF) Konzept eingebunden:

- Die Installation sowie die Kommandos *ftstart*, *ftstop*, *ftcrei* und *ftdeli* wurden an das SMF-Verfahren angepasst.
- Das *ftalarm*-Manifest wird jetzt für jede Instanz mitinstalliert.

Sonstige Änderungen

- Die Kommandos *ft* und *ncopy* erhalten die zusätzlichen Aliasnamen *ftacopy* (für *ft*) und *ftscopy* (für *ncopy*), um Verwechslungen mit Kommandos des Betriebssystems oder anderer Hersteller zu vermeiden.
- Das Kommando *ftinfo* wurde erweitert und gibt zusätzliche Informationen aus.
- Die maximale Satzlänge bei Dateiübertragungsaufträgen und beim Setzen lokaler Dateiattribute wurde auf 65535 erhöht. Dies betrifft folgende Kommandos und Optionen:
  - *ncopy -r=*
  - *ft -r=*
  - *ftmodf -rl=*
- openFT unterstützt auf Solaris Systemen die Installation in ein alternatives root-Verzeichnis.
- Migrationshilfe für Ablösung des TNS

  Für den Umstieg auf den TNS-losen Betrieb steht das Tool *tns2ptn* zur Verfügung. *tns2ptn* ist dazu gedacht, aus TNS-Einträgen mit Adressformat RFC1006 Kommandos zu erzeugen, mit denen passende Einträge in der Partnerliste erstellt werden können.
- Die Beschreibung von dynamischen Partnern wurde präzisiert. In diesem Zusammenhang wurden die Partnertypen "Benannte Partner", "Eingetragene dynamische Partner" und "Freie dynamische Partner" eingeführt.
- Die Beschreibung der CSV-Ausgaben für die SHOW-Kommandos (*ftshw*, *ftshwa*, ...) wurde erheblich erweitert.

Entfallene Funktionen

Die BSFT-Schnittstelle wird nicht mehr unterstützt. Die zugehörigen Kapitel im Handbuch „openFT für Unix-Systeme - Managed File Transfer in der Offenen Welt“ sind entfallen.

1.5 Darstellungsmittel

In diesem Handbuch werden folgende Darstellungsmittel verwendet:

`dicktengleiche Schrift`
: Dicktengleiche Schrift wird für Eingaben und Beispiele verwendet.

kursive Schrift
: Kursive Schrift wird im Fließtext verwendet, um Namen, Variablen und Werte auszuzeichnen, z.B. Dateinamen, Instanznamen, Menüs, Kommandos und deren Optionen.


für Hinweistexte


für Warnhinweise.

Für die Kommandobeschreibung werden zusätzliche Darstellungsmittel verwendet, siehe Abschnitt „Syntax der Kommandobeschreibung“ auf Seite 168.

1.6 Readme-Datei

Funktionelle Änderungen und Nachträge der aktuellen Produktversion zu diesem Handbuch entnehmen Sie bitte gegebenenfalls den produktspezifischen Readme-Dateien.

1.7 Aktuelle Informationen im Internet

Aktuelle Informationen zur openFT-Produktfamilie finden Sie im Internet unter *http://de.ts.fujitsu.com/openft*.

1.8 Lizenzrechtliche Bestimmungen

Die folgenden Bestimmungen betreffen die Nutzung von *libxml2*, Secure FTP und xerces-J für openFT-Script.

Nutzung von libxml2

Für die Verarbeitung der XML-Daten wird die *libxml2* verwendet, die den XML C Parser und ein XML Toolkit enthält. *libxml2* wurde ursprünglich für das Gnome Project entwickelt, ist jedoch auch außerhalb von Gnome verwendbar. Es handelt sich bei *libxml2* um freie Software, die unter der MIT-Lizenz verfügbar ist:

```
Copyright (c) <2008> <Daniel Veillard>

Permission is hereby granted, free of charge, to any person obtaining a copy of
this software and associated documentation files (the "Software"), to deal in
the Software without restriction, including without limitation the rights to
use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies
of the Software, and to permit persons to whom the Software is furnished to do
so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all
copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IM-
PLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS
FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR
COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER
IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNEC-
TION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
```

Nutzung von openSSL für Secure FTP

Die folgenden Bestimmungen betreffen den Betrieb mit Secure FTP.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/). This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

```
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 BSD-style Open Source
licenses. In case of any license issues related to OpenSSL please contact
openssl-core@openssl.org.

OpenSSL License
```

```
---------------

=============================================================================
Copyright (c) 1998-2006 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 permis-
   sion. 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 acknowledg-
   ment:
   "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, INDI-
RECT, 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 LIA-
BILITY, 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.]

Nutzung von xerces-J für openFT-Script

Die folgenden Bestimmungen betreffen den Betrieb mit openFT-Script.

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

```
/* ====================================================================
 * The Apache Software License, Version 1.1
 *
 * Copyright (c) 2000 The Apache Software Foundation.  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. The end-user documentation included with the redistribution,
 *    if any, must include the following acknowledgment:
 *       "This product includes software developed by the
 *        Apache Software Foundation (http://www.apache.org/)."
 *    Alternately, this acknowledgment may appear in the software itself,
 *    if and wherever such third-party acknowledgments normally appear.
 *
 * 4. The names "Apache" and "Apache Software Foundation" must
 *    not be used to endorse or promote products derived from this
 *    software without prior written permission. For written
 *    permission, please contact apache@apache.org.
 *
 * 5. Products derived from this software may not be called "Apache",
 *    nor may "Apache" appear in their name, without prior written
 *    permission of the Apache Software Foundation.
 *
 * THIS SOFTWARE IS PROVIDED ``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 APACHE SOFTWARE FOUNDATION 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 software consists of voluntary contributions made by many
* individuals on behalf of the Apache Software Foundation.  For more
* information on the Apache Software Foundation, please see
* <http://www.apache.org/>.
*
* Portions of this software are based upon public domain software
* originally written at the National Center for Supercomputing Applications,
* University of Illinois, Urbana-Champaign.
*/
```

2 Installation

In diesem Kapitel wird die Installation und die Konfiguration von openFT beschrieben.

Mit openFT wird auch ein Kommunikationsmanager ausgeliefert.
Dieser Kommunikationsmanager wird im Folgenden als CMX bezeichnet (Communications Manager for Unix systems), auch wenn er auf den einzelnen Plattformen unterschiedliche Package-Namen besitzt (wie z.B. CMX, PCMX, CMX.all, SMAWcmx, SMAWpcmx).

2.1 Installation von openFT

Die Installation von openFT müssen Sie unter der Kennung *root* ausführen.

Die Installationstechnik von openFT hängt vom Betriebssystem ab und ist in der Freigabemitteilung beschrieben. Je nachdem ob oder welche FT-Version schon vorher auf Ihrem Rechner installiert war, sind drei Installationsvarianten zu unterscheiden:

- Neuinstallation
  Es existiert noch kein openFT oder openFT < V10.0 auf Ihrem Rechner.
- Update-Installation
  Es existiert openFT V10.0 oder V11.0 auf Ihrem Rechner.
- Installation einer Korrekturversion
  Es existiert schon openFT V12.0 auf Ihrem Rechner.

Was Sie vor der Installation von openFT beachten müssen ...

- Ab openFT V12 wird der Betrieb ohne CMX unterstützt. Falls Sie mit CMX arbeiten wollen und auf dem System noch kein CMX installiert ist, müssen Sie
  - das CMX, das sich auf dem Datenträger befindet, installieren,
  - anschließend in openFT den Betrieb mit CMX aktivieren, z.B. per Kommando *ftmodo -cmx=y*.
- Die Sprache von openFT (Deutsch, Englisch) wird bei einer Neuinstallation entsprechend der Umgebungsvariable *LANG* eingestellt (Ausnahme: auf HP-UX wird immer Englisch eingestellt). Siehe dazu Abschnitt „Sprachoberfläche wechseln“ auf Seite 61.

- Wenn Sie die Verschlüsselung der Dateiinhalte nutzen wollen, müssen Sie zusätzlich openFT-CR V12.0 für Unix-Systeme installieren. Diese Software wird lizenzfrei gegen eine Schutzgebühr zur Verfügung gestellt. Wenn bereits ein openFT-CR mit Version < V10.0 installiert ist, dann müssen Sie diese Version vor der Installation von openFT deinstallieren. openFT-CR V12.0 dürfen Sie erst nach der Installation von openFT V12.0 installieren.
- Wenn Sie die openFT-Script-Schnittstelle oder das Java-API nutzen wollen, dann muss auf Ihrem System mindestens das J2SE™ Runtime Environment 5.0 (JRE 5.0) installiert sein.

  Das Binärverzeichnis, das das Executable *java* enthält, wird unter einem der folgenden Pfade erwartet:
  ```
  /opt/*/bin
  /opt/*/*/bin
  /usr/*/bin
  /usr/*/*/bin oder
  /etc/alternatives/bin
  ```

  Die openFT-Installationsprozedur erstellt im openFT-Verzeichnis den auf Unix-Systemen benötigten Verweis auf das Java-Executable.

  Andernfalls gibt die Installationsprozedur eine Warnung aus, dass Java nicht gefunden wurde. Es wird empfohlen, Java in eines der oben genannten Verzeichnisse zu installieren und den Verweis darauf zu erstellen. Dazu geben Sie folgendes Kommando ein:

  ```
  ftsetjava @s
  ```

  Mit dem Kommando `ftsetjava` können Sie auch überprüfen, ob oder welches Java installiert ist (`ftsetjava @a`) oder welche Java-Datei verwendet wird (`ftsetjava` ohne Parameter). Außerdem können Sie einen Pfad einstellen, der sich nicht unter den oben genannten Pfaden befindet (`ftsetjava Dateiname`).
- Instanzenverzeichnis

  Das Instanzenverzeichnis wird beim Installieren eingerichet und enthält Unterverzeichnisse für anwendungsspezifische Daten der jeweiligen openFT-Instanz wie z.B. Logging-Datei, Schlüsselpaarsätze und Trace-Dateien. Bei Unix-Systemen lautet der Pfadname für das Instanzenverzeichnis standardmäßig */var/openFT/instanz*.

  instanz ist der Name der jeweiligen Instanz. Die Standard-Instanz mit dem Namen *std* ist immer vorhanden.

  Beim Erzeugen einer neuen Instanz mit *ftcrei* können Sie den Pfadnamen des Instanzenverzeichnisses frei wählen.

In den folgenden Abschnitten werden für die Installationsvarianten jeweils die notwendigen Schritte, die Sie als Systemverwalter vornehmen müssen, sowie die von der Installations-Prozedur automatisch ausgeführten Schritte beschrieben.

2.1.1 Neuinstallation

Haben Sie auf Ihrem Rechner bisher kein openFT installiert oder ist ein openFT mit einer Version < V10.0 installiert, dann handelt es sich um eine Neuinstallation.

Notwendige Arbeitsschritte des Systemverwalters

1. Falls schon ein openFT < V10.0 sowie eventuelle Zusatzprodukte installiert sind, gehen Sie wie folgt vor:
   - Sichern Sie noch benötigte Berechtigungsprofile und Berechtigungssätze mit *ftexpe* in eine externe Datei.
   - Deinstallieren Sie openFT-CR, openFT und die Zusatzprodukte.
2. Installieren Sie die Produktsoftware zu openFT V12.

   Dabei beachten Sie bitte Folgendes:

   Bei Systemen, bei denen die openFT-Installation im Dialog stattfindet, werden Sie während der Installation gefragt, ob eine gültige openFT-FTAM-Lizenz und eine gültige openFT-FTP-Lizenz vorliegen. Aktivieren Sie diese Optionen nur, wenn eine gültige Lizenz für openFT-FTAM bzw. openFT-FTP vorliegt! Abhängig von den Antworten werden openFT-FTAM und/oder openFT-FTP installiert oder nicht.

   Falls Sie mit HP, AIX oder Linux arbeiten, wird diese Frage nicht gestellt. Wenn Sie auf diesen Systemen die FTAM und/oder FTP-Funktionalität nutzen wollen, müssen Sie openFT-FTAM und/oder openFT-FTP nach der openFT-Installation über das Kommando *install.ftam* bzw. *install.ftp* aktivieren (siehe dazu Abschnitt „install.ftam - Installation von openFT-FTAM“ auf Seite 380 und Abschnitt „install.ftp - Installation von openFT-FTP“ auf Seite 381).
3. Importieren Sie die gesicherten Berechtigungssätze und Berechtigungsprofile mit *ftimpe* falls gewünscht. Wenn die Berechtigungssätze und Berechtigungsprofile aus einer openFT Version < V8.1 exportiert wurden, werden automatisch alle Sicherheitsstufen in den Berechtigungssätzen, die vorher auf 1 standen, auf 90 umgesetzt. Der Standardberechtigungssatz wird neu gesetzt.

Nun ist openFT betriebsbereit und wird bei jedem Systemstart aktiviert.

Automatisch ausgeführte Arbeitsschritte

Bei der Installation werden folgende Schritte automatisch ausgeführt:

- Wenn CMX installiert ist, dann werden Standard-TNS-Einträge für openFT erzeugt, falls noch keine TNS-Einträge existieren. Andernfalls werden sie angepasst, siehe Abschnitt „Automatisch erzeugte TNS-Einträge“ auf Seite 436.

  Wenn CMX nachinstalliert wird, können Sie Standard-TNS-Einträge auch nachträglich per Tool erstellen, siehe Seite 435.

- Das Instanzverzeichnis der Standard-Instanz wird eingerichtet, siehe Seite 26.

  Dabei werden die Betriebsparameter auf Standardwerte gesetzt, z.B. maximale Anzahl der Aufträge, die simultan bearbeitet werden, maximale Blocklänge, Umfang des FT- und FTAC-Logging, Einstellung des CCS, Portnummern für die asynchronen Inbound-Server, siehe auch Abschnitt „Standardeinstellungen überprüfen“ auf Seite 38.

  CMX-Betrieb, FTP-Server und die Verwendung des TNS sind deaktiviert.

- Als Prozessorname wird der Name des Rechners eingetragen (entspricht der Ausgabe bei *uname -n*).
- Als Instanzidentifikation für die Standardinstanz wird der DNS-Name (falls vorhanden) des Rechners voreingestellt, ohne DNS-Name wird auch die Instanzidentifikation mit dem Namen des Rechners vorbelegt.
- Es wird ein Standardberechtigungssatz erzeugt, mit dem alle File-Transfer-Funktionen erlaubt sind.
- Es wird ein Schlüsselpaarsatz erzeugt (siehe Seite 81).
- Für die Plattformen Linux, HP-UX und AIX werden folgende Startup- und Shutdown-Dateien eingerichtet:
  - die instanzenübergreifende Startup- und Shutdown-Datei (z.B. */sbin/init.d/openFT* auf HP-UX)
  - die Startup- und Shutdown-Datei der Instanz *std* (Pfadname */var/openFT/std/etcinit/openFTinst*).

  Mit Hilfe dieser Dateien wird openFT beim Systemstart automatisch gestartet und beim Herunterfahren des Systems automatisch beendet (siehe dazu auch Abschnitt „openFT-Instanzen und Cluster-Betrieb“ auf Seite 98).

  Für die Plattform Solaris wird ab openFT V12.0 SMF unterstützt, siehe Abschnitt „Solaris SMF“ auf Seite 41. Damit werden keine Startup- und Shutdown-Dateien mehr eingerichtet.

- Die man pages werden wie folgt installiert:
  - Auf den Plattformen Solaris, AIX und HP werden die openFT man pages abhängig von der LANG-Variable in der gleichen Sprache installiert wie openFT.
  - Auf Linux werden die deutschen und englischen openFT man pages installiert, d.h. ein Benutzer erhält die man pages in der Sprache, die bei seiner login-Session eingestellt ist (abhängig von der LANG-Variable).
- openFT wird gestartet (gilt nicht auf HP-Systemen).
- Es wird ein passendes Java-Executable gesucht und openFT bekannt gemacht. Wenn keines gefunden wird, gehen Sie vor wie auf Seite 26 beschrieben.

2.1.2 Update-Installation von openFT

Es wird eine Update-Installation ausgeführt, wenn bereits openFT V10.0 oder V11.0 installiert ist.

Was Sie vor der Update-Installation beachten sollten

Bei einer Update-Installation werden für alle aktiven Instanzen einschließlich der Standardinstanz folgende Aktionen durchgeführt:

- Die Logging-Datei wird gelöscht. Werten Sie deshalb die Logging-Sätze aus, bevor Sie die Update-Installation durchführen.
- Laufende openFT-Script-Aufträge werden während der Installation abgebrochen. Alle alten, abgebrochenen openFT-Script-Aufträge gelten in der neuen openFT-Version als nicht wiederanlauffähig. Beenden Sie daher alle laufenden openFT-Script-Aufträge, bevor Sie eine Update-Installation durchführen.
- Bestehende Aufträge werden bedingungslos aus dem Auftragsbuch gelöscht. Wurde bei der Auftragserstellung mit dem Schalter *-lf=* eine Folgeverarbeitung angegeben, wird diese dabei ausgeführt.
- Evtl. vorhandene Trace-Dateien, Diagnosesätze und Konsolkommandos werden gelöscht.

Wenn Sie openFT-Instanzen weiter verwenden möchten, die mit *ftdeli* deaktiviert wurden, dann sollten Sie diese vor der Update-Installation wieder mit *ftcrei* aktivieren. Die entsprechenden Instanzdateibäume werden dann während der Installation automatisch aktualisiert. Andernfalls müssen Sie diese Instanzen nach der Installation per Kommando *ftupdi* aktualisieren (siehe Seite 378).

Notwendige Arbeitsschritte des Systemverwalters

1. Installieren Sie openFT von dem Datenträger.
2. Während der Installation werden Sie bei Systemen, bei denen die openFT-Installation im Dialog stattfindet, gefragt, ob eine gültige openFT-FTAM-Lizenz und eine gültige openFT-FTP-Lizenz vorliegen. Aktivieren Sie diese Optionen nur, wenn eine gültige Lizenz für openFT-FTAM bzw. openFT-FTP vorliegt! Abhängig von den Antworten werden openFT-FTAM und/oder openFT-FTP installiert oder nicht.

   Falls Sie mit HP, AIX oder Linux arbeiten, werden diese Fragen nicht gestellt. Wenn Sie auf diesen Systemen die FTAM- oder FTP-Funktionalität nutzen wollen, müssen Sie openFT-FTAM und openFT-FTP nach der openFT-Installation über das Kommando *install.ftam* bzw. *install.ftp* aktivieren (siehe dazu Abschnitt „install.ftam - Installation von openFT-FTAM“ auf Seite 380 und Abschnitt „install.ftp - Installation von openFT-FTP“ auf Seite 381)

3. Falls Sie in den alten Startup- und Shutdown-Dateien Änderungen vorgenommen haben, so müssen Sie diese
   - für Linux, HP-UX und AIX bei einer Update-Installation ggf. auch in den neuen Startup- und Shutdown-Dateien vornehmen,
   - bei Solaris ggf. in SMF nachziehen, siehe Abschnitt „Solaris SMF“ auf Seite 41.

   Siehe dazu auch Abschnitt „openFT-Instanzen und Cluster-Betrieb“ auf Seite 98.

Automatisch ausgeführte Arbeitsschritte

Bei einer Update-Installation werden folgende Schritte automatisch ausgeführt:

- Laufende openFT-Prozesse und der openFT Explorer werden beendet.
- openFT-Script-Aufträge werden abgebrochen.
- Bei einer Update-Installation von openFT V10.0 werden die Standard-TNS-Einträge für openFT wie folgt behandelt:
  - Nicht mehr benötigte Standard-TNS-Einträge aus alten openFT Versionen < V10.0 werden gelöscht.
  - Fehlende benötigte Standard-TNS-Einträge werden erstellt.
  - Existierende benötigte Standard-TNS-Einträge bleiben unverändert.
- Die Spracheinstellung wird aus der Vorgängerversion übernommen. Auf der Plattform Linux werden jedoch die openFT man pages in Deutsch und Englisch installiert, d.h. ein Benutzer erhält die man pages in der Sprache, die bei seiner login-Session eingestellt ist.
- Die Instanzverzeichnisse aktuell vorhandener Instanzen einschließlich der Standardinstanz werden aktualisiert, d.h.:
  - Die Logging-Datei wird gelöscht.
  - Die alten instanzspezifischen Startup- und Shutdown-Dateien werden gesichert unter */var/openFT/instanz/etcinit/openFTinst.old* (*instanz* = Name der Instanz). Anschließend werden auf Linux, HP-UX und AIX die neuen instanzspezifischen Startup- und Shutdown-Dateien eingespielt. Auf Solaris wird SMF unterstützt, siehe Abschnitt „Solaris SMF“ auf Seite 41. Die Startup- und Shutdown-Dateien werden nicht mehr installiert.

  - Es werden folgende Konfigurationsdaten übernommen:
    - Betriebsparameter (der Betrieb mit CMX bleibt eingeschaltet)
    - Instanzidentifikation
    - Einträge der Partnerliste
    - FTAM-Katalog
    - Berechtigungssätze und -profile
    - Schlüsselpaarsätze
    - Konfigurationsdaten für die zentrale Administration (bei Update von V11.0).
  - Bei einer Update-Installation von V10.0 auf V12.0 wird der FTP-Server aktiviert, falls für den FTP-Server zuvor eine Portnummer ungleich 0 gesetzt war.
- openFT wird für die Instanzen gestartet, für die er vor der Installation gestartet war (gilt nicht auf HP-Systemen).
- Es wird ein passendes Java-Executable gesucht und openFT bekannt gemacht. Wenn keines gefunden wird, gehen Sie vor wie auf Seite 26 beschrieben.

2.1.3 Installation einer Korrekturversion

Installation einer Korrekturversion heißt, dass schon openFT V12.0 auf Ihrem Rechner existiert. Dabei ist Folgendes zu beachten:

- Laufende openFT-Script-Aufträge werden während der Installation abgebrochen. Beenden Sie daher alle laufenden openFT-Script-Aufträge, bevor Sie eine Korrekturversion installieren.
- Eventuell vorhandene Trace-Dateien, Diagnosesätze und Dateien mit Konsolkommandos werden gelöscht.

Notwendige Arbeitsschritte des Systemverwalters

1. Installieren Sie openFT V12.0 von dem Datenträger.
2. Während der Installation werden Sie, sofern die openFT-Installation im Dialog stattfindet, gefragt, ob eine gültige openFT-FTAM-Lizenz und eine gültige openFT-FTP-Lizenz vorliegen. Aktivieren Sie diese Optionen nur, wenn eine gültige Lizenz für openFT-FTAM bzw. openFT-FTP vorliegt! Abhängig von den Antworten werden openFT-FTAM und/oder openFT-FTP installiert oder nicht.

   Falls Sie mit HP, AIX oder Linux arbeiten, wird diese Frage nicht gestellt. Auf diesen Systemen werden openFT-FTAM und openFT-FTP automatisch installiert, wenn diese bereits installiert waren.

Automatisch ausgeführte Arbeitsschritte

Bei der Installation einer Korrekturversion werden folgende Schritte automatisch ausgeführt:

- Laufende openFT-Prozesse und der openFT Explorer werden beendet, laufende openFT-Script-Aufträge werden abgebrochen.
- Die Berechtigungsprofile und -sätze, die Logging-Dateien, die Startup- und Shutdown-Dateien (Linux, HP-UX, AIX) bzw. die SMF-Anbindung (Solaris), der FTAM-Katalog, Betriebsparameter und Aufträge, die Partnerliste, die Schlüsselpaarsätze sowie die Konfigurationsdaten für die zentrale Administration werden für alle openFT-Instanzen unverändert übernommen.
- Die Spracheinstellung wird von der Vorgängerversion übernommen.
- Falls Sie mit den Systemen HP, AIX oder Linux arbeiten, werden openFT-FTAM und openFT-FTP automatisch installiert, wenn diese bereits installiert waren.
- openFT wird für die Instanzen gestartet, für die er vor der Installation gestartet war (gilt nicht auf HP-Systemen).

2.1.4 Installation in ein alternatives root-Verzeichnis (Solaris)

openFT V12 unterstützt für die Plattform Solaris die Installation in ein alternatives root-Verzeichnis. Dies bedeutet, dass die Dateien und Verzeichnisse des openFT Paketes nicht in das root-Verzeichnis des laufenden Systems installiert werden, sondern in ein anderes Verzeichnis, das bereits eine Betriebssystemumgebung enthält und von dem das System zu einem späteren Zeitpunkt gebootet wird.

Die Installation in ein alternatives root-Verzeichnis ist Voraussetzung für die Unterstützung von Live-Upgrade-Verfahren. Bei Live-Upgrade-Verfahren wird das root-Dateisystem in ein alternatives root-Dateisystem dupliziert. Anschließend wird die Software (Update des Betriebssystems und zusätzliche Softwarepakete) in das alternative root-Dateisystem installiert und von dort das System später neu gebootet.

Variable openFT-Dateien

Die variablen openFT-Dateien werden in das Verzeichnis */var/openFT* installiert. Es ist nicht möglich, mit einem /var Verzeichnis zu arbeiten, das zwischen dem root-Verzeichnis und dem alternativen root-Verzeichnis geshared ist.

Für die Synchronisierung der variablen openFT-Dateien zwischen dem root-Dateisystem und dem alternativen root-Dateisystem ist der Administrator verantwortlich; d.h. er muss die variablen openFT-Dateien vor dem Start des neuen Systems abgleichen.

Installation von openFT

Bei einer Update-Installation enthält das alternative root-Verzeichnis bereits eine openFT-Version V10.0 oder V11.0, bei Installation einer Korrekturversion eine openFT Version V12.0.

Wenn auf einem System openFT < V10.0 installiert ist, darf die Installation in ein alternatives root-Verzeichnis nicht genutzt werden.

Gehen Sie wie folgt vor:

1. Installieren Sie die Produktsoftware zu openFT V12 in das alternative root-Verzeichnis. Die Installationstechnik ist in der Freigabemitteilung beschrieben.

   Damit werden die fixen Dateien und Verzeichnisse des openFT Paketes in das alternative root-Verzeichnis installiert, z. B. */altroot/opt/openFT*.

2. Nach einer Neuinstallation oder einer Update-Installation sind noch folgende Schritte notwendig, um die variablen openFT-Dateien zu erzeugen (Neuinstallation) bzw. in das openFT V12 Format zu konvertieren (Update-Installation):

   a) Booten Sie vom alternativen root-Verzeichnis ohne openFT zu starten.

      Der automatische Start von openFT über SMF ist zu diesem Zeitpunkt noch nicht aktiviert.

   b) Rufen Sie die Shellprozedur *ftconfig* auf:

      ```
      /opt/openFT/bin/ftbin/ftconfig
      ```

      Damit ist openFT V12 vollständig installiert.

   c) Starten Sie openFT.

Nach einer Korrekturinstallation wird openFT beim ersten Startup des neuen Systems automatisch konfiguriert und gestartet. Der Aufruf der Shellprozedur *ftconfig*, sowie der Start von openFT durch den Administrator entfällt hier.

Einschränkung bei einer Update-Installation

Nach einer Update-Installation gibt es folgende Einschränkung:

Beim Zurückschalten auf das ursprüngliche root-Dateisystem ist eine Synchronisierung der variablen openFT Dateien nicht möglich, da mit openFT V12 aktualisierte Konfigurationsdateien nicht in ältere Versionen zurück konvertiert werden. D.h. openFT-Aufträge und -Einstellungen, die in dem alternativen root-Dateisystem gemacht wurden, sowie neue Logging-Sätze, Trace-Dateien, Diagnosesätze, usw. gehen verloren.

2.1.5 Automatische Installation

Sie können auf Solaris-Systemen zur Installation von openFT auch die automatische Installation wählen. In dem Fall erfolgt die Installation ohne Abfrage am Bildschirm. Die für die Installation von openFT erforderlichen Zusatzangaben zu openFT-FTAM und openFT-FTP werden der Datei *response* entnommen. Im Installationspaket ist eine Standard response Datei integriert mit folgendem Inhalt:

```
FTAM='NO'
FTP='NO'
```

Bedeutung der Umgebungsvariablen

FTAM

gibt an, ob Sie berechtigt sind, die FTAM-Funktionalität zu benutzen, d.h. ob Sie eine openFT-FTAM-Lizenz besitzen. In der Standard-response-Datei ist die Umgebungsvariable mit dem Wert *NO* vorbelegt, d.h. openFT-FTAM wird nicht installiert.

Möglicher weiterer Wert:
YES, d.h. es liegt eine openFT-FTAM-Lizenz vor, die Nutzung von openFT-FTAM wird freigeschaltet.

FTP

gibt an, ob Sie berechtigt sind, die FTP-Funktionalität zu benutzen, d.h. ob Sie eine openFT-FTP-Lizenz besitzen. In der Standard-response-Datei ist die Umgebungsvariable mit dem Wert *NO* vorbelegt, d.h. openFT-FTP wird nicht installiert.

Möglicher weiterer Wert:
YES, d.h. es liegt eine openFT-FTP-Lizenz vor, die Nutzung von openFT-FTP wird freigeschaltet.

Beispiel

Eine response Datei zur automatischen Installation von FTAM sieht wie folgt aus:

```
FTAM='YES'
FTP='NO'
```

Andere Dienste wie z.B. der asynchrone openFT-Server werden beim Ändern oder Reparieren automatisch beendet.

2.2 Wichtige Tätigkeiten nach der Installation

Nach der Installation von openFT müssen Sie je nach Anforderung an Ihr System eventuell noch weitere Schritte vornehmen. Dazu gehören folgende Punkte:

- Standardeinstellungen überprüfen, siehe Seite 38
- openFT-CR installieren (wenn Verschlüsselung von Dateiinhalten gewünscht wird)
- CMX nachinstallieren, falls openFT mit CMX betrieben werden soll und CMX nicht vor openFT installiert wurde. Sie finden das Paket auf der Produkt-CD.
- Konfigurationsdaten importieren, siehe Seite 39
- automatischen openFT-Start deaktivieren; siehe Seite 40
- *ftalarm*-Funktion aktivieren, siehe Seite 40
- openFT-Subagenten automatisch starten, siehe Seite 41
- openFT-FTAM auf HP-UX, AIX und Linux installieren oder deinstallieren. siehe Seite 45
- openFT-FTP auf HP-UX, AIX und Linux installieren oder deinstallieren, siehe Seite 45
- Authentifizierung über PAM (Pluggable Authentication Modules) aktivieren/deaktivieren, siehe Seite 45
- Partnerliste aus TNS erzeugen, siehe Seite 48
- Fernadministrations-Server konfigurieren
  Wenn Sie Ihr System als Fernadministrations-Server einsetzen möchten, müssen Sie diesen konfigurieren, siehe Abschnitt „Fernadministrations-Server konfigurieren“ auf Seite 120.
- ADM-Trap-Server konfigurieren
  Wenn Sie Ihr System als ADM-Trap-Server einsetzen möchten, müssen Sie diesen konfigurieren, siehe Abschnitt „ADM-Trap-Server konfigurieren“ auf Seite 152.
- TNS-Einträge erstellen
  Falls Sie den TNS verwenden, müssen Sie ggf. TNS-Einträge erstellen, siehe Abschnitt „Transportsystem-Anwendungen in TNS eintragen“ auf Seite 435.

  Wenn noch keine oder keine aktuellen TNS-Einträge für openFT V12 vorhanden sind (weil CMX nachinstalliert wurde), dann können Sie diese nachträglich per Skript erstellen bzw. aktualisieren, siehe Abschnitt „Standard-TNS-Einträge per Skript erzeugen“ auf Seite 435.

  Beachten Sie bitte, dass eine Cluster-Konfiguration nur für TCP/IP unterstützt wird. Deshalb wird empfohlen ohne CMX und TNS zu arbeiten.

2.2.1 Standardeinstellungen überprüfen

Bei einer Neuinstallation setzt openFT Standardwerte für die Betriebsparameter und die FTAC-Einstellungen. Diese sind so gewählt, dass sie für den normalen openFT-Betrieb in der Regel ausreichen. Sie sollten jedoch überprüfen, ob diese Einstellungen auch für Ihren Einsatzfall geeignet sind. Die Sonderfunktionen wie z.B. Fernadministrations-Server, Trace, Traps, automatisches Löschen von Logging-Sätzen usw. sowie die Nutzung von TNS und CMX sind ausgeschaltet.

Der Standardberechtigungssatz ist so eingestellt, dass File Transfer uneingeschränkt möglich ist. Als FTAC-Verwalter sollten Sie daher den Standardberechtigungssatz umgehend dem Schutzbedürfnis des Rechners anpassen (siehe auch Abschnitt „Berechtigungssätze verwalten“ auf Seite 92).

Betriebsparameter-Einstellungen

Nach einer Neuinstallation (einschließlich der Installation von openFT-FTAM, openFT-FTP und openFT-CR) erhalten Sie mit dem Kommando *ftshwo* die Einstellungen angezeigt:

```
ftshwo
STARTED PROC-LIM CONN-LIM ADM-CLIM RQ-LIM MAX-RQ-LIFE TU-SIZE KEY-LEN CCS-NAME
  YES     NONE      16       8      2000      30       65535   2048   ISO88591
PTN-CHK DYN-PART SEC-LEV  FTAC-LOG FT-LOG ADM-LOG     USE TNS USE CMX ENC-MAND
  STD       ON   B-P-ATTR    ALL    ALL    ALL          NO      NO       NO
OPENFT-APPL      FTAM-APPL         FTP-PORT           ADM-PORT        ADM-CS
*STD             *STD              21                 11000             NO
ACTIVE           ACTIVE            DISABLED           ACTIVE
HOST-NAME        IDENTIFICATION / LOCAL SYSTEM NAME
*NONE            mc011.mynet.local / $FJAM,MC011

DEL-LOG  ON  AT     RETPD    ADM-TRAP-SERVER
 OFF   DAILY 00:00    14     *NONE

TRAP: SS-STATE FT-STATE PART-STATE PART-UNREA RQ-STATE TRANS-SUCC TRANS-FAIL
CONS    OFF      OFF       OFF        OFF       OFF       OFF        OFF
ADM              OFF       OFF        OFF       OFF       OFF        OFF

FUNCT:  SWITCH PARTNER-SELECTION    REQUEST-SELECTION    OPTIONS    OPTIONS-LL
MONITOR  OFF   ALL                  ALL
TRACE    OFF   ALL                  ALL                  NONE       OFF
```

Die detaillierte Beschreibung der einzelnen Werte finden Sie auf Seite 342.

Überprüfen Sie vorrangig folgende Einstellungen:

- Instanzidentifikation

  Diese ist mit dem Namen des Rechners im lokalen Netz vorbelegt. Wenn dies nicht für die netzweite Eindeutigkeit ausreicht, ändern Sie bitte den Wert (*ftmodo -id*), siehe auch Abschnitt „Instanzidentifikationen“ auf Seite 80.

- Lokale Portnummern für die Protokolle (OPENFT-APPL, FTAM-APPL, FTP-PORT).

  Wenn Sie für die Adressierung andere Portnummern verwenden, z.B. für openFT, FTAM oder FTP, dann passen Sie diese an (Kommando *ftmodo*, Optionen *-openft*, *-ftam* und *-ftp*).

- Dynamische Partner (DYN-PART)

  Dynamische Partner sind zugelassen. Wenn Sie diese aus Sicherheitsgründen sperren möchten, dann setzen Sie den Wert mit *ftmodo -dn=f* auf OFF.

Die Betriebsparameter-Einstellungen können Sie auch über den openFT Explorer ändern. Wählen Sie dazu im Menü *Administration* den Befehl *Betriebsparameter*.

FTAC-Einstellungen

Nach einer Neuinstallation stehen alle Werte für den Standardberechtigungssatz auf 100. D.h. das System ist offen für alle Benutzer mit gültigem Kennwort, für alle Partner und für alle Aktionen. Abhängig vom Schutzbedürfnis des Systems sollten Sie den Standardberechtigungssatz anpassen. Dazu verwenden Sie das Kommando *ftmoda*, siehe Seite 228. Alternativ können Sie auch den openFT Explorer benutzen, indem Sie im Objektfenster *Berechtigungssätze* den Berechtigungssatz *STD anpassen.

2.2.2 Konfigurationsdaten importieren

Sie können die Konfigurationsdaten importieren, die Sie z.B. per Export in einem anderen System erstellt haben:

- Betriebsparameter-Einstellungen importieren Sie, indem Sie die Exportdatei in der Shell ausführen.
- Die FTAC-Umgebung importieren Sie per Kommando *ftimpe* oder über den openFT Explorer mit dem Menü *Administration,* Befehl *FTAC-Umgebung - FTAC-Umgebung importieren*.
- Eine Partnerliste importieren Sie, indem Sie die Exportdatei in der Shell ausführen.
- Die Konfiguration für einen Fernadministrations-Server importieren Sie mit dem Kommando *ftimpc* oder über den openFT Explorer mit dem Menü *Administration,* Befehl *Fernadministration - Konfiguration importieren*.

2.2.3 Automatischen openFT-Start deaktivieren

Dieser Abschnitt gilt nicht für Solaris, da openFT V12 den automatischen Start von openFT auf Solaris ohne SMF nicht unterstützt. Für Solaris mit SMF wird ein anderer Mechanismus verwendet, siehe Abschnitt „Solaris SMF“ auf Seite 41.

Bei der Installation wird die Startup-Datei installiert, z.B. */sbin/rc2.d/S910openFT* auf HP-UX, */etc/rc3.d/S50openFT* auf RedHat Linux und */etc/rc.ft* auf AIX.
Dieses Script ruft beim Systemstart die Datei */var/openFT/std/etcinit/openFTinst* auf, die openFT automatisch startet.

Wurden mit dem Kommando *ftcrei* openFT-Instanzen erzeugt, so ruft dieses Script auch die Startup- und Shutdown-Datei dieser Instanzen auf (siehe dazu Abschnitt „openFT-Instanzen und Cluster-Betrieb“ auf Seite 98).

Diese Dateien starten dann die jeweilige openFT-Instanz.

Falls openFT nicht automatisch gestartet werden soll, muss die entsprechende Kommandozeile in der Datei */var/openFT/std/etcinit/openFTinst* bzw. in der Startup- und Shutdown-Datei der Instanzen auskommentiert werden.

openFT automatisch beenden

Bei der Installation wird die Shutdown-Datei installiert (z.B. */sbin/rc1.d/K200openFT* auf HP-UX oder */etc/rc0.d/K50openFT* auf RedHat Linux). Dieses Script ruft beim Herunterfahren des Systems die Datei */var/openFT/std/etcinit/openFTinst* auf, die openFT automatisch beendet.

Wurden mit dem Kommando *ftcrei* openFT-Instanzen erzeugt, so ruft dieses Script auch die Shutdown-Dateien dieser Instanzen auf (siehe dazu Abschnitt „openFT-Instanzen und Cluster-Betrieb“ auf Seite 98). Diese Dateien beenden dann die jeweilige openFT-Instanz.

2.2.4 ftalarm-Kommando aktivieren

Dieser Abschnitt gilt nicht für Solaris. Dort wird ein anderer Mechanismus verwendet, siehe Abschnitt „ftalarm automatisch aktivieren“ auf Seite 42.

Wenn Sie über eine Häufung fehlgeschlagener FT-Aufträge informiert werden wollen, empfiehlt es sich, das *ftalarm*-Kommando zu verwenden, siehe Seite 186.

Falls Sie das *ftalarm*-Kommando beim Hochfahren des Systems automatisch starten wollen, können Sie in die Startup- und Shutdown-Datei */var/openFT/std/etcinit/openFTinst* bzw. in die Startup- und Shutdown-Datei weiterer Instanzen eine entsprechende Zeile mit dem *ftalarm*-Kommando einfügen.

2.2.5 openFT-Subagent automatisch starten

Dieser Abschnitt gilt nicht für Solaris. Dort wird ein anderer Mechanismus verwendet, siehe Abschnitt „Solaris SMF“ auf Seite 41.

Falls Sie den openFT-Subagenten zur Administration über SNMP beim Hochfahren des Systems automatisch starten wollen, müssen Sie in der Startup-Datei */var/openFT/std/etcinit/openFTinst* bzw. in der Startup-Datei weiterer Instanzen die entsprechende Zeile mit dem *ftagt*-Kommando aktivieren.

Näheres entnehmen Sie bitte dem Kapitel „openFT über SNMP administrieren“ auf Seite 105.

Bitte beachten Sie bei der Cluster-Umschaltung, dass SNMP nur mit einer openFT-Instanz zusammenarbeiten kann.
Es ist entscheidend, welche Instanz beim Start des Agenten eingestellt ist (siehe dazu Abschnitt „openFT-Instanzen und Cluster-Betrieb“ auf Seite 98).

2.2.6 Solaris SMF

Mit SMF (Service Management Facility) können die Abhängigkeiten eines Dienstes zu anderen Diensten, Dateien oder Meilensteinen (entspricht den früheren Runlevels), sowie Instanzen des Dienstes in einem Manifest detailliert beschrieben werden.

Dadurch werden u.a. wesentlich kürzere Startzeiten erreicht, da viele Dienste parallel gestartet werden können und die Startreihenfolge durch die Beschreibung der Abhängigkeiten optimiert werden kann.

Die verschiedenen Dienste des Systems werden mit einer einheitlichen Schnittstelle verwaltet. Ebenso wird dafür gesorgt, dass der Betrieb robuster wird, d.h. wenn sich z.B. ein Dienst außerplanmäßig beendet (z.B. ein unbeabsichtigtes *kill -9*) wird er automatisch wieder gestartet.

Mit SMF ergeben sich folgende Unterschiede im Vergleich zum Betrieb ohne SMF:

- Die Startscripts */etc/init.d/openFT* und */var/openFT/instanz/etcinit/openFTinst* werden mit Solaris SMF **nicht** installiert. *ftalarm* wird per SMF aktiviert, siehe Abschnitt Abschnitt „Solaris SMF“ auf Seite 42.
- Das automatische Prüfen der Profildateien und die automatische Bereinigung der Loggingdaten entfällt.

- Die Abhängigkeit zu CMX ist nicht definiert, da CMX nicht am SMF Installationsverfahren teilnimmt. Wird openFT mit CMX eingesetzt, dann kann es während des Bootens zu Diagnosesätzen bei openFT kommen. Diese entstehen in der Zeit, in der CMX noch nicht verfügbar ist. Grund ist, dass zuerst alle SMF Meilensteine aktiviert und dann die RC Scripte gestartet werden, so dass CMX erst nach openFT gestartet wird. Mit openFT V12.0 ist das Vorhandensein von CMX im RFC1006 Fall nicht mehr zwingend.

Folgende Kommandos wurden an das SMF Verfahren angepasst, so dass sie wie gewohnt funktionieren:

- *ftstart* übernimmt Umgebungsvariablen und startet openFT via SMF. Das SMF Kommando (ohne Übernahme der Umgebungsvariablen) lautet:

  ```
  svcadm enable openFT:instanz
  ```

  Die gewohnten openFT-Meldungen werden bei *svcadm* nicht angezeigt.

- *ftstop* stoppt openFT via SMF. Das SMF Kommando lautet:

  ```
  svcadm disable openFT:instanz
  ```

  Die gewohnten openFT Meldungen werden bei *svcadm* nicht angezeigt.

- *ftcrei* erzeugt zusätzlich zur Instanz ein Manifest und trägt dieses in SMF ein.
- *ftdeli* löscht die Instanz und trägt das zugehörige Manifest aus SMF aus.

ftalarm automatisch aktivieren

ftalarm kann, wie weiter unten beschrieben, manuell über die Kommandozeile gestartet oder beendet werden. Unter Solaris kann *ftalarm* auch über SMF verwaltet werden. Das dafür notwendige *ftalarm* Manifest wird für jede Instanz automatisch erzeugt und installiert.

Eine Mischform (händischer Betrieb und Steuerung über SMF) wird nicht empfohlen, da SMF eine Änderung nicht erfährt. *ftalarm* ist für SMF ein sogenannter transienter Dienst, d.h. es gibt keinen überwachbaren Prozess.

Beispiel

ftalarm kann für die Instanz *inst001* mit den folgenden Kommandos gestartet bzw. gestoppt werden:

```
# svcadm enable ftalarm:inst001
# svcadm disable ftalarm:inst001
```

Erzeugen der Instanz *inst001*:

```
# ftcrei 001 -addr=inst001
# svcs *:inst001
STATE          STIME    FMRI
disabled       16:31:50 svc:/application/openFT:inst001
disabled       16:31:51 svc:/application/ftalarm:inst001
# svcadm enable ftalarm:inst001
# svcs *:inst001
STATE          STIME    FMRI
disabled       16:31:50 svc:/application/openFT:inst001
offline        16:32:14 svc:/application/ftalarm:inst001
#. ftseti inst001
# ftstart
ftstart: openFT 12.0A00 starting. Protocols: openFT,FTAM,ADM
# svcs *:inst001
STATE          STIME    FMRI
online         16:32:37 svc:/application/openFT:inst001
online         16:32:38 svc:/application/ftalarm:inst001
```

Der *ftalarm* cronjob für die Instanz *inst001* wird erst gestartet, wenn auch die Instanz *inst001* gestartet wurde. Entsprechend wird *ftalarm* beendet, wenn die Instanz *inst001* mit *ftstop* beendet wird.

Die Anzahl der fehlerhaften FTAC-Sätze kann über die SMF-Umgebungsvariable ERRORS der *ftalarm* Instanz eingestellt werden, z.B. wie folgt für die Instanz *inst001*:

1. Beenden Sie *ftalarm* für die Instanz *inst001* mit dem Kommando:

   ```
   # svcadm disable ftalarm:inst001
   ```

2. Ändern Sie die Anzahl der Fehler für die Überwachung (z.B. auf 42) mit dem Kommando:

   ```
   # svccfg -s ftalarm:inst001  setenv -i ERRORS 42
   ```

3. Übernehmen Sie die Einstelllungen mit dem Kommando:

   ```
   # svcadm refresh ftalarm:inst001
   ```

4. Starten Sie *ftalarm* für die Instanz *inst001* mit dem Kommando:

   ```
   # svcadm enable ftalarm:inst001
   ```

5. Sie können sich die Einstelllungen anzeigen lassen mit:

   ```
   # svcprop -t -p method_context/environment ftalarm:inst001
   method_context/environment astring OPENFTINSTANCE=inst001 ERRORS=42
   ```

openFT-Instanz per SNMP überwachen

Mit *ftagt* können Sie genau eine openFT-Instanz per SNMP überwachen. *ftagt* wird auf Solaris mit SMF administriert.

Sie können

- sich die aktuell zu überwachende SNMP-Instanz anzeigen lassen:

```
# svcprop -t -p method_context/environment ftagt
method_context/environment astring OPENFTINSTANCE=std
```

- sich den Status des *ftagt* anzeigen lassen:

```
# svcs ftagt
STATE          STIME    FMRI
disabled       Jul_11   svc:/application/ftagt:default
```

- den *ftagt* für die mit OPENFTINSTANCE gesetzte Instanz aktivieren:

```
svcadm enable ftagt
```

- den *ftagt* für die mit OPENFTINSTANCE gesetzte Instanz beenden:

```
svcadm disable ftagt
```

- die zu überwachende Instanz ändern (z.B. auf *hugo*):
  - *ftagt* ausschalten

    ```
    svcadm disable ftagt
    ```

  - Umgebung ändern

    ```
    svccfg -s ftagt:default setenv -i OPENFTINSTANCE hugo
    ```

  - Umgebung aktivieren

    ```
    svcadm refresh ftagt
    ```

  - *ftagt* für *hugo* aktivieren

    ```
    svcadm enable ftagt
    ```

Eine openFT-Instanz kann genau dann mit SNMP administriert werden, wenn

- die openFT-Instanz existiert
- die openFT-Instanz gestartet ist
- OPENFTINSTANCE für *ftagt* korrekt gesetzt ist
- *ftagt* gestartet ist

2.2.7 openFT-FTAM auf HP-UX, AIX und Linux installieren oder deinstallieren

Bei den Systemen HP, AIX und Linux wird openFT-FTAM bei einer Neuinstallation oder bei einer Update-Installation nicht mehr zusammen mit openFT installiert. Dasselbe gilt für Korrektur-Installationen, wenn openFT-FTAM vorher nicht installiert war.

In diesen Fällen müssen Sie openFT-FTAM mit dem Kommando *install.ftam* nachträglich installieren. Sie finden das Kommando im Verzeichnis */opt/openFT/bin/ftbin*, siehe dazu Abschnitt „install.ftam - Installation von openFT-FTAM“ auf Seite 380.

Die Installation ist nur erlaubt, wenn eine gültige openFT-FTAM-Lizenz vorliegt.

Mit *install.ftam* können Sie openFT-FTAM auch wieder deinstallieren, falls es nicht mehr benötigt wird. openFT-FTAM muss deinstalliert werden, falls keine entsprechende Lizenz vorliegt.

2.2.8 openFT-FTP auf HP-UX, AIX und Linux installieren oder deinstallieren

Bei den Systemen HP, AIX und Linux wird openFT-FTP bei einer Neuinstallation oder bei einer Update-Installation nicht zusammen mit openFT installiert. Dasselbe gilt für Korrektur-Installationen, wenn openFT-FTP vorher nicht installiert war.

In diesen Fällen müssen Sie openFT-FTP mit dem Kommando *install.ftp* nachträglich installieren. Sie finden das Kommando im Verzeichnis */opt/openFT/bin/ftbin*, siehe dazu Abschnitt „install.ftp - Installation von openFT-FTP“ auf Seite 381.

Die Installation ist nur erlaubt, wenn eine gültige openFT-FTP-Lizenz vorliegt.

Mit *install.ftp* können Sie openFT-FTP auch wieder deinstallieren, falls es nicht mehr benötigt wird. openFT-FTP muss deinstalliert werden, falls keine entsprechende Lizenz vorliegt.

2.2.9 Authentifizierung über PAM

PAM (Pluggable Authentication Modules) ist eine Sammlung von Programmbibliotheken, die den Systemverwalter auswählen lassen, wie Anwendungen Benutzer authentifizieren. openFT unterstützt die PAM-Schnittstelle für die Benutzerauthentifizierung für die Betriebssysteme Linux, Solaris, HP-UX und AIX.

Nach der Installation ist die PAM-Funktion auf Linux, Solaris und HP-UX aktiviert, auf AIX dagegen deaktiviert. Daher müssen Sie auf AIX die PAM-Funktion explizit aktivieren, siehe "PAM-Funktion aktivieren und deaktivieren".

In manchen Fällen ist es notwendig, die Konfigurationsdateien zu überprüfen und die Einträge anzupassen, siehe "PAM-Konfigurationsdateien überprüfen und ändern".

PAM-Funktion aktivieren und deaktivieren

Zur Laufzeit können Sie die PAM-Funktion auf allen Plattformen über die Umgebungsvariable OPENFTPAM aktivieren und deaktivieren Dazu müssen Sie den asynchronen openFT-Server beenden (z.B. Kommando *ftstop*), die Variable setzen und anschließend den asynchronen openFT-Server wieder starten (z.B. Kommando *ftstart)*:

```
OPENFTPAM=ON
export OPENFTPAM
```

PAM-Funktion wird aktiviert.

```
OPENFTPAM=OFF
export OPENFTPAM
```

PAM-Funktion wird deaktiviert.

PAM-Konfigurationsdateien überprüfen und ändern

Der PAM-Mechanismus wird durch anwendungs- und plattformspezifische Konfigurationsdateien gesteuert.

- Linux

  In Linux wird der PAM-Mechanismus gesteuert über Dateien im Verzeichnis */etc/pam.d* bzw. durch einen Eintrag in der Datei */etc/pam.conf*, falls */etc/pam.d* nicht existiert.

  openFT verwendet beim Anmelden an PAM den Service-Namen *openft*. Bei einer Update-/Neuinstallation von openFT wird daher im Verzeichnis */etc/pam.d* eine Konfigurationsdatei mit dem Namen *openft* angelegt, falls diese noch nicht existiert. In dieser Datei wird der zu verwendende Authentifizierungsmechanismus festgelegt. Falls der Systemverwalter über die Datei */etc/pam.d/common-auth* ein bestimmtes Authentifizierungverfahren definiert hat, so wird dieses auch von openFT verwendet. Andernfalls wird das PAM-Modul *pam_unix.so* für die Benutzerauthentifizierung unter Linux benutzt.

  Falls das Verzeichnis */etc/pam.d* nicht existiert, dann muss der Systemverwalter für den Service-Namen *openft* einen entsprechenden Eintrag in der Datei */etc/pam.conf* vornehmen.

- Solaris, HP-UX und AIX

  Der PAM-Mechanismus funktioniert auf diesen Plattformen für openFT, wenn es in der Datei */etc/pam.conf* einen Eintrag für OTHER mit dem service module type *auth* gibt, der die installierten Anwendungen auf dem jeweiligen Betriebssystem die PAM Funktionalität nutzen lässt.

Wenn dies nicht der Fall ist, dann müssen Sie in der Datei */etc/pam.conf* folgende Einträge machen:

– Solaris

  Abhängig von Ihrer Solaris Version können folgende Einträge notwendig sein:

```
openft auth required pam_unix.so.1
openft auth requisite pam_authtok_get.so.1
openft auth required pam_unix_auth.so.1
```

– HP-UX

```
openft auth required libpam_unix.1
```

  bzw. ggf. auch

```
openft auth required libpam_unix.so.1
```

– AIX

  Auf AIX kann es vorkommen, dass der Eintrag für OTHER defaultmäßig folgendermaßen konfiguriert ist und damit den Service unterbindet:

```
OTHER auth required pam_prohibit
```

  In diesem Fall muss man den Eintrag für openFT nachtragen:

```
openft auth required pam_aix
```

2.2.10 Partnerliste aus TNS erzeugen

openFT bietet durch die Partnerliste die Möglichkeit, ohne TNS zu arbeiten, sofern openFT über TCP/IP mit den Partnern kommuniziert. Die Partnerliste hat gegenüber dem TNS den Vorteil, dass Sie dort neben allen notwendigen Adressinformationen auch weitere Eigenschaften wie z.B. die Sicherheitsstufe eines Partners hinterlegen können.

Für den Umstieg auf den TNS-losen Betrieb steht Ihnen das Tool *tns2ptn* zur Verfügung. *tns2ptn* ist dazu gedacht, aus TNS-Einträgen mit Adressformat RFC1006 neue Partnerlisten-Einträge zu erzeugen.

Um TNS-Einträge in die Partnerliste einzubringen, sind folgende Schritte nötig:

1. Exportieren Sie die TNS-Einträge in eine Datei:

   Geben Sie dazu das Kommando `tnsxprop > openft.tns` ein (*openft.tns* ist der wählbare Dateiname).

2. Bereinigen Sie die Exportdatei (hier *openft.tns*) falls nötig, indem Sie die Einträge löschen, die nicht zu openFT gehören, nicht mehr benötigt werden oder nicht das Adressformat RFC1006 haben.

3. Rufen Sie das Tool *tns2ptn* auf:

   ```
   /opt/openFT/bin/ftbin/tns2ptn openft.tns > ft_list
   ```

   ft_list ist der frei wählbare Name der Ausgabedatei. *ft_list* enthält für jeden Partner ein *ftaddptn*-Kommando mit den Adressinformationen.

   Wenn ein Eintrag nicht konvertiert werden kann, wird dieser auf *stderr* ausgegeben.

4. Führen Sie die Ausgabedatei (hier *ft_list*) als FT-Verwalter auf der Kommando-Ebene aus (z.B. *sh ft_list*).

Beachten Sie, dass nur die Adressinformationen aus dem TNS übernommen werden. Zusätzliche Partnereigenschaften (Sicherheitsstufe, Priorität, Überwachung, ...) können Sie anschließend mit dem Kommando *ftmodptn* oder über den openFT Explorer festlegen.

3 Aufgaben des Verwalters

Dieses Kapitel beschreibt die wichtigsten Aufgaben, die Sie bei der Verwaltung des laufenden openFT-Betriebs haben. openFT können Sie sowohl über den openFT Explorer als auch über Kommandos verwalten. Dazu gibt es

– Funktionen und Kommandos, die nur der Verwalter verwenden darf (z.B. openFT starten oder Logging-Sätze löschen),

– Funktionen und Kommandos, die sowohl für den Benutzer als auch den Verwalter zugelassen sind, bei denen der Verwalter jedoch mehr darf als der Benutzer (z.B. Berechtigungssätze ändern).

Zu den Aufgaben des Verwalters gehören:

– Betriebsparameter einstellen [1) 2)]
– openFT starten und beenden [1) 2)]
– Auftragsbuch verwalten [1)]
– Logging-Sätze ansehen und löschen [1)]
– Berechtigungssätze und -profile sichern [1)]
– Diagnosemöglichkeiten, z.B. den Überwachungszustand für die Fehlerdiagnose ein- und ausschalten [1) 2)]
– Instanzen erzeugen und verwalten, um openFT im Cluster einzusetzen
– Schlüsselpaarsätze erzeugen[1)] und Partnersystemen einen aktuellen öffentlichen Schlüssel zur Verfügung stellen. Dadurch kann das lokale System vom Partner authentifiziert werden.
– Öffentliche Schlüssel von Partnersystemen entgegennehmen und im lokalen System passend hinterlegen, damit die Partnersysteme vom lokalen System authentifiziert werden können.

Die mit [1)] gekennzeichneten Verwaltungsfunktionen können auch über den openFT Explorer ausgeführt werden, sofern ein X-Terminal oder eine entsprechende Emulation zur Verfügung steht. Weitere Informationen zum openFT Explorer finden Sie im Benutzerhandbuch zu „openFT für Unix-Systeme“ sowie in der Online-Hilfe.

Die mit [2)] gekennzeichneten Verwaltungsfunktionen können auch über eine SNMP-Managementstation ausgeführt werden, siehe Kapitel „openFT über SNMP administrieren“ auf Seite 105.

Die Verwaltung der FTAC-Funktionen kann auch an eine andere Person übertragen werden, den so genannten FTAC-Verwalter. Die zentrale Administration mit Einrichten eines Fernadministrations-Servers ist eine eigenständige Aufgabe, siehe Seite 51 und Kapitel „Zentrale Administration“ auf Seite 113.

Wer ist FT-Verwalter?

openFT kann von allen Benutzerkennungen verwaltet werden, die die root-Berechtigung (UID=0) besitzen, d.h. alle Kennungen mit UID=0 besitzen FT-Verwalterrechte.

Wer ist FTAC-Verwalter?

Nach der Neuinstallation sind FT-Verwalter und FTAC-Verwalter identisch. Das heißt, dass alle Benutzer, die auf dem System FT-Verwalterrechte besitzen, auch FTAC-Verwalter sind.

Der FTAC-Verwalter ist dadurch ausgezeichnet, dass in seinem Berechtigungssatz das entsprechende Privileg definiert ist. Diese Eigenschaft können Sie mit dem Kommando *ftmoda* auf eine andere Kennung übertragen. Dies ist z.B. sinnvoll, wenn der Datenschutzverantwortliche jemand anderes ist als der Systemverwalter des Rechners. Der FTAC-Verwalter besitzt die folgenden Rechte:

- Berechtigungsprofile verwalten, siehe Seite 94
- Berechtigungssätze verwalten, siehe Seite 92
- FTAC-Umgebung sichern, Seite 96

Außerdem kann der FTAC-Verwalter das Logging verwalten, ebenso wie der FT-Verwalter und der ADM-Verwalter, siehe Seite 89.

Je nachdem, unter welcher Kennung der FTAC-Verwalter eingerichtet ist, sind seine Rechte und Möglichkeiten unterschiedlich:

- Standardeinstellung (FT-Verwalter ist FTAC-Verwalter)
  Jede andere Kennung mit FT-Verwalterrechten ist ebenfalls FTAC-Verwalter, d.h. jeder FTAC-Verwalter verfügt über die Rechte des FT-Verwalters.
- Übertragung des FTAC-Privilegs auf genau eine spezifische Kennung mit FT-Verwalterrechten:
  Damit besitzt nur noch diese Kennung sowohl FT- als auch FTAC-Verwalterrechte. Alle anderen bisherigen FT-Verwalter verlieren die expliziten FTAC-Verwalterrechte.
- Übertragung auf eine Kennung ohne FT-Verwalterrechte:
  Ein FT-Verwalter darf keine Berechtigungssätze und Berechtigungsprofile mehr verwalten oder die FTAC-Umgebung sichern. Der FTAC-Verwalter verfügt nur über die oben aufgeführten FTAC-Verwalterrechte, nicht jedoch über die Rechte des FT-Verwalters.

Mit dem Kommando *ftmoda @ftadm -priv=y* können sowohl FTAC-Verwalter als auch FT-Verwalter die FTAC-Verwaltung wieder auf die Standardeinstellung zurücksetzen, d.h. FT-Verwalter und FTAC-Verwalter sind wieder identisch.

ADM-Verwalter

Der ADM-Verwalter ist die einzige Person, die den Fernadministrations-Server verwalten darf. Das Arbeiten mit einem Fernadministrations-Server und die Rolle des ADM-Verwalters sind im Kapitel „Zentrale Administration“ auf Seite 113 ausführlich beschrieben. Nach der Neuinstallation gibt es noch keinen ADM-Verwalter. Dieser muss erst durch den FTAC-Verwalter festgelegt werden, siehe Abschnitt „ADM-Verwalter festlegen“ auf Seite 121.

3.1 Betriebsparameter einstellen

Zum Steuern des openFT-Betriebs gibt es eine Reihe von Parametern, die Sie über das Kommando *ftmodo* festlegen können, z.B.:

- Die Instanzidentifikation der lokalen openFT-Instanz.
- Die maximale Anzahl der asynchronen Aufträge, die openFT gleichzeitig bearbeiten soll (Verbindungslimit).
- Die maximale Anzahl der Prozesse, die für die Bearbeitung asynchroner Aufträge zur Verfügung stehen (Prozesslimit).
- Die Obergrenze für die Länge der zu übertragenden Blöcke.
  Nach der Installation von openFT/openFT-FTAM ist die maximale Blocklänge auf 65535 Zeichen eingestellt.
- Den Umfang, in dem der openFT-Betrieb protokolliert werden soll.
- Die Länge des RSA-Schlüssels, der beim Verschlüsseln verwendet werden soll.
- Die Codetabelle, die standardmäßig für lokale Textdateien verwendet werden soll.

Sie können sich die aktuellen Werte der Parameter einer openFT-Instanz ansehen. Dazu dient das Kommando *ftshwo*.

Die aktuellen Betriebsparameter können Sie auch über den openFT Explorer ansehen und verändern. Dazu öffnen Sie das Dialogfenster *Betriebsparameter* aus dem Menü *Administration*. Eine detaillierte Beschreibung zu den einzelnen Funktionen finden Sie in der Online-Hilfe.

Tipps zur Performancesteuerung

Bei der Festlegung der Werte für das Prozesslimit (PROC-LIM) und das Verbindungslimit (CONN-LIM) müssen Sie folgende Punkte berücksichtigen:

Auf Unix-Systemen können Sie das Prozesslimit nur auf 1 oder auf „Unbeschränkt“ setzen. Im Falle "Unbeschränkt" wird die Anzahl der Prozesse durch das Verbindungslimit (CONN-LIM) bestimmt, da jeder Prozess nur eine Verbindung bearbeitet.

- Ein niedriger Wert für das Prozesslimit bedeutet, dass sich die Aufträge auf wenige Prozesse verteilen und deshalb langsamer abgearbeitet werden, dass aber andererseits die Performance anderer Anwendungen auf Ihrem Rechner nicht nennenswert beeinträchtigt wird.

- Ein hoher Wert für das Prozesslimit bedeutet, dass die Aufträge sich auf mehr Prozesse verteilen und deshalb schneller ablaufen. Allerdings kann eine zu starke Anhebung des Prozesslimits dazu führen, dass der Durchsatz stagniert oder sogar wieder fällt. Zudem wird die Performance anderer Anwendungen auf Ihrem Rechner stärker beeinträchtigt.
- Ein niedriger Wert für das Verbindungslimit bedeutet, dass wenige Dateiübertragungen parallel laufen können, und dass Verbindungswünsche von fernen Partnern öfter zurückgewiesen werden, weil das Limit überschritten wird. Die Performance anderer Anwendungen auf Ihrem Rechner wird aber nicht nennenswert schlechter.
- Ein hoher Wert für das Verbindungslimit bedeutet, dass ein hohes Aufkommen an Dateiübertragungsaufträgen parallel und in kurzer Zeit abgearbeitet wird, und Verbindungswünsche ferner Partner im Regelfall angenommen werden. Die Performance anderer Anwendungen auf Ihrem Rechner wird aber unter Umständen stärker beeinträchtigt.

3.2 Code-Tabellen verwalten

Eine Code-Tabelle definiert einen Zeichensatz (Coded Character Set, kurz CCS) und die Codierung dieser Zeichen in einer Datei. Einem CCS ist ein bis zu 8 Zeichen langer Name zugeordnet, über den der CCS angesprochen werden kann.

Als FT-Verwalter stellen Sie über das Kommando *ftmodo -ccs* einen Standard-CCS für openFT ein. Zusätzlich können Sie noch eigene 8bit-CCS erstellen.

Der Standard-CCS wird für alle FT-Aufträge verwendet. Der Benutzer kann jedoch im *ft-/ncopy*-Auftrag und im openFT Editor einen anderen CCS einstellen.

Folgende CCS liefert openFT standardmäßig aus:

Name des CCS	**Bedeutung**
ISO88591 bis ISO8859B und ISO8859D bis ISO8859G	für die ASCII-Tabellen ISO8859-1 bis ISO8859-11 und ISO8859-13 bis ISO8859-16
ISO646	für die internationale 7-bit ASCII Tabelle
ISO646DE	für die deutsche 7-bit ASCII Referenzversion
EDF041 bis EDF04A, EDF04D und EDF04F	für die EBCDIC-Tabellen DF04-1 bis DF04-10, DF04-13 und DF04-15
EDF03IRV	für die internationale 7-bit EBCDIC Tabelle
EDF03DRV	für die deutsche 7-bit EBCDIC Tabelle
UTF16	für Unicode in der UTF-16 Codierung (plattformgemäßer Endian)
UTF8	für Unicode in der UTF-8 Codierung
UTFE	für Unicode in der UTF-E Codierung
UTF16LE	für Unicode in der UTF-16 Codierung (Little Endian)
UTF16BE	für Unicode in der UTF-16 Codierung (Big Endian)
UTFEIBM	für Unicode in der von IBM definierten UTF-EBCDIC Codierung
IBM037	für den von IBM definierten US/Canada EBCDIC Zeichensatz
IBM273	für den von IBM definierten deutsch/österreichischen EBCDIC Zeichensatz
IBM500	für den von IBM definierten International EBCDIC Zeichensatz
IBM1047	für den von IBM definierten OpenExtensions EBCDIC Zeichensatz

Name des CCS	Bedeutung
CP437	für den von Microsoft definierten OEM-Zeichensatz für Englisch (USA)
CP720	für den von Microsoft definierten OEM-Zeichensatz für Arabisch
CP737	für den von Microsoft definierten OEM-Zeichensatz für Griechisch
CP775	für den von Microsoft definierten OEM-Zeichensatz für Lettisch
CP850	für den von Microsoft definierten OEM-Zeichensatz für Westeuropa
CP852	für den von Microsoft definierten OEM-Zeichensatz für Polnisch
CP855	für den von Microsoft definierten OEM-Zeichensatz für Serbisch
CP857	für den von Microsoft definierten OEM-Zeichensatz für Türkisch
CP858	für den von Microsoft definierten OEM-Zeichensatz CP850 mit Euro
CP862	für den von Microsoft definierten OEM-Zeichensatz für Hebräisch
CP866	für den von Microsoft definierten OEM-Zeichensatz für Kyrillisch
CP874	für den von Microsoft definierten Windows-Zeichensatz für Thai
CP1250	für den von Microsoft definierten Windows-Zeichensatz für Zentraleuropa
CP1251	für den von Microsoft definierten Windows-Zeichensatz für Kyrillisch
CP1252	für den von Microsoft definierten Windows-Zeichensatz für Westeuropa mit Euro
CP1253	für den von Microsoft definierten Windows-Zeichensatz für Griechisch
CP1254	für den von Microsoft definierten Windows-Zeichensatz für Türkisch
CP1255	für den von Microsoft definierten Windows-Zeichensatz für Hebräisch

Name des CCS	Bedeutung
CP1256	für den von Microsoft definierten Windows-Zeichensatz für Arabisch
CP1257	für den von Microsoft definierten Windows-Zeichensatz für Baltisch
CP1258	für den von Microsoft definierten Windows-Zeichensatz für Vietnamesisch

Benutzerdefinierte CCS erstellen

Sie können als FT-Verwalter eigene CCS (Coded Character Set) erzeugen. Dazu erstellen Sie eine Textdatei, die im Unterverzeichnis *sysccs* der openFT- Instanz abgelegt wird. Der CCS-Name ist gleich dem Namen dieser Datei.

Die Textdatei muss folgenden Aufbau besitzen:

- Die erste Zeile beginnt mit einem '#'.

  Das zweite Zeichen ist ein Leerzeichen. Der Rest der Zeile enthält einen Kommentar, der den enthaltenen Code charakterisiert.

- Die zweite Zeile enthält einen Buchstaben, der derzeit nur den Wert 'S' annehmen kann. 'S' steht für Single-Byte Code, d.h. ein Zeichen ist immer 1 Byte lang.

- Die dritte Zeile enthält drei Zahlen.

  Die erste Zahl ist eine vierstellige hexadezimale Zahl. Diese definiert das Ersatzzeichen, das verwendet werden soll, wenn ein Unicode-Zeichen nicht auf den Code abbildbar ist.

  Die zweite Zahl ist derzeit immer '0'.

  Die dritte Zahl ist eine Dezimalzahl, die die Anzahl der folgenden Codepages definiert, sie hat derzeit immer den Wert '1'.

- Die dann folgenden Zeilen legen die Codepages fest und haben folgenden Aufbau:
  - Die erste dieser Zeilen enthält die Nummer der Codepage als zweistellige hexadezimale Zahl.
  - Alle folgenden Zeilen enthalten die Abbildung der Zeichen des zu definierenden Codes in UTF-16 als vierstellige hexadezimale Zahl. Die Werte sind in 16 Zeilen mit jeweils 16 vierstelligen hexadezimalen Zahlen ohne Zwischenraum angeordnet.

Beispiel ISO8859-15 (Westeuropa mit Euro-Zeichen)

```
# Encoding file: iso8859-15, single-byte
S
003F 0 1
00
000000010002000300040005000600070008000900A000B000C000D000E000F
001000110012001300140015001600170018001900 1A001B001C001D001E001F
002000210022002300240025002600270028002900 2A002B002C002D002E002F
003000310032003300340035003600370038003900 3A003B003C003D003E003F
004000410042004300440045004600470048004900 4A004B004C004D004E004F
005000510052005300540055005600570058005900 5A005B005C005D005E005F
006000610062006300640065006600670068006900 6A006B006C006D006E006F
007000710072007300740075007600770078007900 7A007B007C007D007E007F
008000810082008300840085008600870088008900 8A008B008C008D008E008F
009000910092009300940095009600970098009900 9A009B009C009D009E009F
00A000A100A200A320AC00A5016000A7016100A900AA00AB00AC00AD00AE00AF
00B000B100B200B3017D00B500B600B7017E00B900BA00BB0152015301780 0BF
00C000C100C200C300C400C500C600C700C800C900CA00CB00CC00CD00CE00CF
00D000D100D200D300D400D500D600D700D800D900DA00DB00DC00DD00DE00DF
00E000E100E200E300E400E500E600E700E800E900EA00EB00EC00ED00EE00EF
00F000F100F200F300F400F500F600F700F800F900FA00FB00FC00FD00FE00FF
```

3.3 openFT starten und beenden

Standardmäßig wird openFT (d.h. der asynchrone openFT-Server) beim Systemstart automatisch gestartet.

Der automatische Start ist in der Startup-Datei voreingestellt. Falls openFT nicht automatisch gestartet werden soll, muss die entsprechende Kommandozeile in der Startup-Datei auskommentiert werden (siehe Abschnitt „Automatischen openFT-Start deaktivieren“ auf Seite 40).

Hinweis: Auf Solaris erfolgt der automatische Start über SMF.

Läuft der asynchrone openFT-Server nicht, werden nur synchrone Aufträge ausgeführt. Asynchrone Aufträge werden im Auftragsbuch abgespeichert. Außerdem werden auch keine Aufträge aus Partnersystemen angenommen.

Nach dem Start des asynchronen openFT-Servers führt openFT auch lokal gestellte asynchrone sowie fern gestellte Dateiübertragungsaufträge aus.

Zum manuellen Starten und Beenden des asynchronen openFT-Servers verwenden Sie die Kommandos *ftstart* und *ftstop* oder im openFT Explorer die Funktionen *Administration/Asynchronen Server starten* und *Administration/Asynchronen Server beenden*.

3.4 Schutzbiteinstellung für neu angelegte Dateien

Sie können die Schutzbiteinstellung für Dateien, die beim Empfangen neu angelegt werden, auf einen Wert setzen, der die Dateizugriffsrechte für den Eigentümer, die Gruppenmitglieder und für die Anderen einschränkt.

Die Standardschutzbiteinstellung können Sie mit dem Kommando *umask* ändern. Um die Änderung zu aktivieren, müssen Sie den asynchronen openFT-Server nach der Änderung neu starten.

Damit beim Start von openFT die Schutzbiteinstellung entsprechend vorbelegt ist, ist in der Startup-Datei der Standardinstanz *std* die Kommandozeile *umask 027* aktiviert.
Diese Startup-Datei steht unter */var/openFT/std/etcinit/openFTinst.*

Da Sie ab openFT V12 in Solaris immer SMF nutzen, müssen Sie SMF-Kommandos verwenden, um die Schutzbiteinstellung zu ändern.

Unter Solaris ändern Sie die umask-Einstellung wie folgt:

1. Beenden Sie openFT mit dem Kommando *ftstop*.
2. Ändern Sie die umask-Einstellung (z.B. auf 022) mit dem Kommando:

   ```
   svccfg -s openFT:std setenv -i OPENFTUMASK 022
   ```

3. Übernehmen Sie die Einstelllungen mit dem Kommando:

   ```
   svcadm refresh openFT:std
   ```

4. Starten Sie openFT mit dem Kommando *ftstart*.
5. Sie können sich die Einstelllungen anzeigen lassen, indem Sie das Kommando *svcprop* eingeben (hier für die Standardinstanz):

   ```
   svcprop -t -p method_context/environment openFT:std
   ```

   Ausgabe:
   ```
   method_context/environment astring OPENFTINSTANCE=std OPENFTUMASK=022
   ```

3.5 Dateizugriff unter Benutzerrechten

Ab openFT V12 findet auf Unix-Systemen der Dateizugriff standardmäßig unter Benutzerrechten statt - im Gegensatz zu früheren openFT Versionen. Damit führt openFT alle Berechtigungsprüfungen und Zugriffe auf Dateien und Verzeichnisse eines Benutzers unter den Rechten des jeweiligen Benutzers durch, d.h. openFT wechselt für die Berechtigungsprüfung und den Zugriff vom privilegierten *root*-Kontext in den Rechte-Kontext des Benutzers und anschließend wieder zurück.

Der Wechsel in den Benutzer-Kontext hat z.B. bei gemounteten NFS-Verzeichnissen den Vorteil, dass die Kennung *root* keinen Zugriff auf die Benutzerdateien mehr benötigt, da alle Zugriffe nur noch unter den Rechten des jeweiligen Benutzers erfolgen.

3.6 Sprachoberfläche wechseln

Während der Installation wird auf Solaris, Linux und AIX die Umgebungsvariable *LANG* des installierenden Verwalters ausgewertet und als Standard für die Sprachoberfläche eingestellt. Auf HP-UX ist standardmäßig Englisch eingestellt.

Diese Einstellung lässt sich wie folgt ändern:

- Mit dem Tool *ftlang* kann der FT-Verwalter die Standardeinstellung ändern, siehe Seite 227. Für die Ausgabe der man pages ist auf den Plattformen Solaris, AIX und HP-UX allein die über *ftlang* getroffene Einstellung relevant. Auf Linux werden die deutschen und englischen openFT man pages installiert, d.h. ein Benutzer erhält die man pages in der Sprache, die bei seiner login-Session eingestellt ist (abhängig von der LANG-Variable).
- Mit der Umgebungsvariable *OPENFTLANG* kann jeder Benutzer seine Spracheinstellung ändern. Hierzu muss er die ersten beiden Zeichen der *LANG*-Variablen in Kleinbuchstaben angeben (*de* bzw. *en*) und die Umgebungsvariable exportieren.

  Beispiel

  `OPENFTLANG=de; export OPENFTLANG` entspricht z.B.
  `LANG=De_DE.88591,De_DE.646...`

  oder

  `OPENFTLANG=en; export OPENFTLANG` entspricht z.B.
  `LANG=En_US.ASCII,En_US.88591...`

Die folgende Tabelle zeigt, wie das Setzen bzw. Nichtsetzen von OPENFTLANG und LANG wirkt:

OPENFTLANG	**LANG**	**Resultat**
nicht gesetzt oder leer	nicht gesetzt oder leer	Standardeinstellung
nicht gesetzt oder leer	ungültiger Wert	Standardeinstellung
nicht gesetzt oder leer	gültige Sprache (Deutsch oder Englisch)	mit LANG gesetzte Sprache
ungültiger Wert oder nicht installierte Sprache	wird nicht ausgewertet	Standardeinstellung
gültiger Wert (de oder en)	wird nicht ausgewertet	mit OPENFTLANG gesetzte Sprache

Die geänderte Spracheinstellung wirkt, sobald ein Programm wie z.B. der openFT Explorer, der openFT Editor oder die Shell neu aufgerufen wird. War ein Programm vor der Umstellung aktiv, müssen Sie es zuerst beenden und dann neu starten.

3.7 Aufträge administrieren

Im Auftragsbuch werden alle asynchronen Outbound-Aufträge sowie alle Inbound-Aufträge gespeichert. Als Verwalter können Sie

- sich über alle noch nicht abgeschlossenen asynchronen Aufträge auf Ihrem Rechner *informieren*. Dazu gehört auch das Recht, Informationen über Aufträge aller Benutzer abzufragen. Das Auftragsbuch lassen Sie sich ausgeben mit dem Kommando *ftshwr*.
- die *Bearbeitungsreihenfolge* aller Aufträge Ihres Rechners *ändern*, auch von Aufträgen anderer Benutzer. Dazu steht Ihnen das Kommando *ftmodr* zur Verfügung.
- asynchrone Aufträge Ihres Rechners *löschen*, auch die anderer Benutzer. Dazu dient das Kommando *ftcanr*.

Sie können sich das Auftragsbuch auch über den openFT Explorer ansehen, indem Sie auf das Objektverzeichnis *Auftragsbuch* klicken. Außerdem können Sie
folgende Funktionen über den openFT Explorer ausführen:
– asynchrone Aufträge löschen
– Auftragsbuch aktualisieren
– Prioritäten für Aufträge verändern
– Aufträge an den Anfang oder das Ende der Warteschlange verschieben

Eine detaillierte Beschreibung zu den einzelnen Funktionen finden Sie in der Online-Hilfe des openFT Explorer.

3.8 Partner administrieren

Mit openFT können Sie File Transfer mit einer Vielzahl von Partnersystemen durchführen. Diese Partnersysteme können über unterschiedliche Transportsysteme und Protokolle erreichbar sein. Um diese Partnersysteme effizient zu verwalten und sich die Arbeit zu erleichtern, bietet openFT

- die Partnerliste, siehe Abschnitt „Partnerliste einrichten und verwalten“ auf Seite 66
- den **Transport Name Service** (TNS),

  openFT kann den TNS nur verwenden, wenn CMX installiert ist und wenn der Betrieb mit CMX und mit TNS per Betriebsparameter aktiviert ist (z.B. per *ftmodo -cmx=y -tns=y*).

  CMX stellt den TNS und Funktionen für den Zugriff auf den TNS zur Verfügung.

Zusätzlich gibt es im openFT Explorer das Objektverzeichnis *Partner*, in dem der jeweilige Benutzer seine bevorzugten Kopplungspartner einrichten kann. Details dazu sind in der Online-Hilfe beschrieben.

Transport Name Service

Partnersysteme müssen Sie nur dann in den TNS eintragen, wenn diese nicht über das Transportsystem TCP/IP gekoppelt werden.

Um den TNS nutzen zu können, müssen Sie folgende Voraussetzungen schaffen:

- Sie müssen die Funktion in den Betriebsparametern explizit aktivieren. Dazu geben Sie entweder das Kommando *ftmodo -tns=y* ein oder aktivieren über den openFT Explorer die Betriebsparameter-Option *TNS benutzen*.
- Der Betrieb mit CMX muss eingeschaltet sein. Wenn der Betrieb mit CMX ausgeschaltet ist, wird kein TNS verwendet.

Details sind im Abschnitt „Transportsystem-Anwendungen in TNS eintragen“ auf Seite 435 beschrieben.

3.8.1 Partnertypen

Eine wichtige Rolle bei der Administration von Partnern spielt die Partnerliste. Je nachdem, ob und in welcher Form ein Partnersystem in die Partnerliste eingetragen wird, unterscheidet man drei Partnertypen:

- Benannte Partner:
  Alle Partner, die mit Namen in der Partnerliste eingetragen sind
- Eingetragene dynamische Partner:
  Alle Partner, die ohne Namen in der Partnerliste eingetragen sind
- Freie dynamische Partner:
  Alle Partner, die nicht in der Partnerliste eingetragen sind

Eingetragene dynamische Partner und freie dynamische Partner werden kurz auch als dynamische Partner bezeichnet.

Benannte Partner

Benannte Partner werden in FT-Aufträgen über ihren in der Partnerliste definierten Partnernamen angesprochen.

Benannte Partner tragen Sie wie folgt in die Partnerliste ein:

`ftaddptn` *partnername* `-pa=`*adresse* `...`

Diese Partner bleiben so lange in der Partnerliste, bis sie über das Kommando *ftremptn* gelöscht werden. Wenn eine Verbindung zu einem Partner mit Authentifizierung arbeiten soll, dann sollte dieser Partner in der Partnerliste eingetragen sein.

Die Verwendung von benannten Partnern bietet folgende Vorteile:

– Kompliziertere Partneradressen müssen nicht in openFT-Kommandos explizit angegeben werden.
– Die Sicherheit wird erhöht, da nur wirklich bekannte Partner zugelassen werden können.

Ein benannter Partners kann zwar auch über seine Adresse angesprochen werden, aber in allen Ausgaben von openFT wie z.B. beim Logging oder Auftragsbuch wird der Partnername angezeigt.

Eingetragene dynamische Partner

Eingetragene dynamische Partner sind alle Partner, die nur mit Adresse, aber ohne Namen in der Partnerliste eingetragen sind. Sie können ausschließlich über ihre Adresse angesprochen werden und besitzen mindestens ein Attribut, das vom Standard eines freien dynamischen Partners abweicht (siehe Abschnitt „Freie dynamische Partner“ auf Seite 65).

Partner dieses Typs tragen Sie z.B. wie folgt in die Partnerliste ein:

```
ftaddptn –pa=adresse –tr=n
```

D.h. Sie vergeben ein oder mehrere vom Standard abweichende Attribute (in diesem Beispiel *-tr=n*, d.h.Trace einschalten).

Beachten Sie bitte:
- Sicherheitsstufe gemäß Partnereinstellung (*-sl=p*) ist die Standardeinstellung für freie dynamische Partner und zählt daher nicht als abweichendes Attribut.
- Sicherheitsstufe gemäß Betriebsparameter-Einstellung (*-sl=*; ohne Parameter, Standardeinstellung des Kommandos *ftaddptn*) ist dagegen ein abweichendes Attribut.

Wenn Sie für einen Partner dieses Typs mit *ftmodptn* alle Attribute auf die Standardwerte zurücksetzen, dann verschwindet dieser Partner aus der Partnerliste und wird zu einem freien dynamischen Partner.

Freie dynamische Partner

Freie dynamische Partner sind alle Partner, die nicht in der Partnerliste eingetragen sind. Daher werden sie bei *ftshwptn* ohne Angabe eines Partnernamens oder einer Partneradresse nicht angezeigt.

Partner dieses Typs werden nur über ihre Adresse angesprochen und besitzen mit Ausnahme der Sicherheitsstufe (*-sl*) die Standard-Attribute, so wie sie beim Kommando *ftaddptn* beschrieben sind. Die Sicherheitsstufe ist bei einem freien dynamischen Partner *-sl=p* (und nicht *-sl=* ohne Parameter).

Zur Bedeutung dieser Attribute siehe Kommandos *ftaddptn* oder *ftmodptn*.

Sie können mit dem Kommando *ftmodptn* aus einem freien dynamischen Partner einen eingetragenen dynamischen Partner machen:

```
ftmodptn adresse ... (weitere Optionen)
```

Sie geben eine Partneradresse an, die auf keinen bereits existierenden Partnerlisteneintrag verweist, und legen ein oder mehrere vom Standard abweichende Attribute (siehe oben) fest.

Das Konzept der freien dynamischen Partner bietet den Vorteil, dass ein Benutzer beliebige Partner adressieren kann, die nicht in der Partnerliste eingetragen sind. Als Administrator haben Sie dadurch weniger Verwaltungsaufwand. Nachteilig ist das erhöhte Sicherheitsrisiko, weshalb Sie die Verwendung dynamischer Partner auch untersagen können, siehe Seite 66.

Wenn sich der Zustand eines freien dynamischen Partners ändert, (z.B. in NOCON = Partner nicht verfügbar) und damit vom Standardwert abweicht, wird er in der Partnerliste angezeigt. Er wird aber wieder zum freien dynamischen Partner, sobald er wieder verfügbar ist (Status ACTIVE).

Dynamische Partner ein-/ausschalten

Sie können als Systemverwalter die Verwendung dynamischer Partner aus Sicherheitsgründen untersagen. Dazu verwenden Sie folgendes Kommando:

```
ftmodo –dp=f
```

In diesem Fall muss ein Partner über seinen Namen in der Partnerliste adressiert werden; er kann nicht mehr direkt über seine Adresse angesprochen werden. Auch Inbound werden dann nur noch Partner zugelassen, die mit einem Partnernamen in der Partnerliste eingetragen sind.

Mit *ftmodo -dp=n* lassen Sie dynamische Partner wieder zu.

Diese Funktion steht auch im openFT Explorer zur Verfügung: Menü *Administration*, Befehl *Betriebsparameter*, Registerblatt *Allgemein*.

3.8.2 Partnerliste einrichten und verwalten

Nach der Neuinstallation ist die Partnerliste leer. Daher sollten Sie die Partnerliste sofort nach der Installation erstellen und insbesondere häufig verwendete Partner in die Partnerliste eintragen.

Zum Verwalten der Partnerliste stehen Ihnen folgende Kommandos zur Verfügung:

– *ftaddptn*: Neuen Partner in die Partnerliste eintragen
– *ftmodptn*: Eigenschaften eines Partners in der Partnerliste ändern
– *ftremptn*: Partner aus der Partnerliste entfernen
– *ftshwptn*: Eigenschaften von Partnern in der Partnerliste anzeigen und Partnerliste exportieren

Die Partnerliste können Sie auch über den openFT Explorer verwalten:

– Mit dem Menübefehl *Datei - Neu - Partnerlisteneintrag*... können Sie einen neuen Partner in die Partnerliste eintragen.

  Alternative: Klicken Sie im Objektbaum auf *Administration* und wählen Sie bei *Partnerliste* den Kontextmenü-Befehl *Neuer Partnerlisteneintrag...* .

– Über folgende Kontextmenü-Befehle im Objektfenster *Partnerliste:*
  – *Neuer Partnerlisteneintrag...* : neue Partner eintragen
  – *Löschen*: Partner entfernen
  – *Eigenschaften*: Eigenschaften von Partnern ändern.

Weitere Einzelheiten finden Sie in der Online-Hilfe.

Partnerliste exportieren

Sie können die Einträge in der Partnerliste mit dem Kommando *ftshwptn* in eine Datei exportieren, z.B. um die Einträge zu sichern oder für andere Systeme zu verwenden. Beim Exportieren werden die Einträge in entsprechende Kommandos umgesetzt (*ftmodptn*), die Sie nur noch einzulesen brauchen.

Bei *ftshwptn* geben Sie an, für welche Plattform die Kommandos erzeugt werden.

Beispiele

– Sichern der Partnerliste im Format für Unix-Systeme in die Datei *ftpartner.sav*:

```
ftshwptn -px > ftpartner.sav
```

  Sie können die Partnerliste wieder importieren, indem Sie die Datei als Prozedurdatei aufrufen, z.B. mit

```
sh ftpartner.sav
```

– Exportieren der Partnerliste im BS2000-Format in die Datei *ftpartner.bs2*:

```
ftshwptn -p2 > ftpartner.bs2
```

3.8.3 Aufbau der Partneradressen

Eine Partneradresse hat folgenden Aufbau:

[protocol://]host[:[port].[tsel].[ssel].[psel]]

host (= Rechnername, siehe Seite 68) muss immer angegeben werden, alle anderen Angaben sind optional. In vielen Fällen werden sie durch Standardwerte abgedeckt, so dass der Rechnername als Partneradresse ausreicht, siehe „Beispiele“ auf Seite 71. Abschließende '.' oder ':' können weggelassen werden.

Die Adressbestandteile bedeuten im Einzelnen:

protocol://
: Protokollstack, über den der Partner angesprochen wird. Mögliche Werte für *protocol*, wobei Groß-/Kleinschreibung nicht unterschieden wird:

  openft openFT-Partner, d.h. Kommunikation über das openFT-Protokoll

  ftam FTAM-Partner, d.h. Kommunikation über das FTAM-Protokoll

  ftp FTP-Partner, d.h. Kommunikation über das FTP-Protokoll

  ftadm ADM-Partner, d.h. Kommunikation über das FTADM-Protokoll für Fernadministration und ADM-Traps

  Standardwert: **openft**

  Ausnahme: falls für *host* ein globaler Name aus dem TNS verwendet wird, dem dort ein Presentation-Selektor zugeordnet ist, dann ist **ftam** Standardwert.

host
: Rechnername, über den der Partner angesprochen wird. Mögliche Angaben:

  – Internet-Hostname (z.B. DNS-Name), Länge 1 bis 80 Zeichen
  – Globaler Name aus dem Transport Name Service (TNS), maximal 78 Zeichen lang mit voller Unterstützung der 5 Namensteile. In diesem Fall gilt:
    – Der TNS muss aktiviert sein (*ftmodo -tns=y*) und der Betrieb mit CMX muss eingeschaltet sein, damit ein globaler Name aus dem TNS in Aufträgen verwendet werden kann. In diesem Fall hat der TNS-Name gegenüber dem Internet-Hostnamen Vorrang.
    – Die Partneradresse muss mit *host* enden und darf keine weiteren Adresskomponenten enthalten wie z.B. *port*, *tsel* etc.
    – Bei *protocol* ist *ftp* nicht erlaubt, da openFT-FTP den TNS-Betrieb nicht unterstützt.
    – Enthält der TNS-Eintrag zu diesem globalen Namen einen Presentation-Selektor, so ist bei *protocol* nur *ftam* erlaubt.
    – Enthält der TNS-Eintrag keinen Presentation-Selektor, so ist *ftam* bei *protocol* nicht erlaubt.

– IPv4-Adresse mit dem Präfix %ip, also z.B. %ip139.22.33.44
  Sie sollten die IP-Adresse immer mit Präfix %ip angeben, weil die Angabe dann sofort als IP-Adresse behandelt wird. Wenn Sie das Präfix weglassen, dann bringt dies Performance-Nachteile, da in diesem Fall erst im TNS gesucht wird und dann in der Datei /etc/hosts.
  Die IP-Adresse selbst muss immer als eine Folge durch Punkte getrennter Dezimalzahlen ohne führende Nullen angegeben werden.
– IPv6-Adresse mit dem Präfix %ip6, also z.B.
  `%ip6[FEDC:BA98:7654:3210:FEDC:BA98:7654:3210]` (IPv6) oder
  `%ip6[FE80::20C:29ff:fe22:b670%5]` (IPv6 mit Scope-Id)

  Die eckigen Klammern [..] müssen angegeben werden.

  Die Scope-Id bezeichnet die lokale Netzwerkkarte, über die der ferne Partner im gleichen LAN-Segment zu erreichen ist. Sie muss mit einem %-Zeichen an die Adresse angehängt werden. Auf Windows-Systemen ist dies ein numerischer Wert (z.B. 5), auf anderen Systemen kann dies auch ein symbolischer Name sein (z.B. *eth0*). Die Scope-Id kann mit dem Kommando *ifconfig* ermittelt werden.

port
: Bei einer Kopplung über TCP/IP können Sie hier die Portnummer angeben, unter der die File-Transfer-Anwendung im Partnersystem erreichbar ist.
  Zulässiger Wertebereich: 1 bis 65535.

  Standardwert: **1100** bei openFT-Partnern.
  Per Betriebsparameter kann mit *ftmodo -ftstd=* auch ein anderer Standardwert eingestellt werden.

  4800 bei FTAM-Partnern.

  21 bei FTP-Partnern

  11000 bei ADM-Partnern

tsel
: Transport-Selektor, unter dem die Filetransfer-Anwendung im Partnersystem erreichbar ist. Der Transport-Selektor ist nur für openFT- und FTAM-Partner relevant.
  Sie können den Selektor abdruckbar oder hexadezimal (im Format 0xnnnn...) angeben. Die Angabe hängt von der Art des Partners ab:

  – openFT-Partner:
    Länge 1 bis 8 Zeichen, erlaubt sind alphanumerische Zeichen und die Sonderzeichen # @ $. Ein abdruckbarer Selektor wird im Protokoll in EBCDIC codiert und ggf. intern mit Leerzeichen auf acht Zeichen aufgefüllt.

    Standardwert: **$FJAM**

– FTAM-Partner:
Länge 1 bis 10 Zeichen, ein abdruckbarer Selektor wird im Protokoll in ASCII mit variabler Länge codiert. Ausnahme: T-Selektoren, die mit $FTAM (Standardwert) beginnen, werden in EBCDIC codiert und mit Leerzeichen auf 8 Zeichen aufgefüllt.

Bei ASCII-Selektoren können alle alphanumerischen Zeichen und die Sonderzeichen @ $ # _ - + = und * verwendet werden.

Standardwert: **$FTAM**

Für Windows-Partner mit openFT-FTAM bis V10 muss in der Regel **SNI-FTAM** angegeben werden. Ab openFT-FTAM V11 für Windows wurde der Standardwert auf **$FTAM** geändert und kann somit weggelassen werden.

Hinweis:
Abdruckbare Transport-Selektoren werden in openFT immer mit Großbuchstaben verwendet, auch wenn sie in Kleinbuchstaben angegeben oder ausgegeben werden.

ssel
Session-Selektor, unter dem die Filetransfer-Anwendung im Partnersystem erreichbar ist. Sie können den Selektor abdruckbar oder hexadezimal (im Format 0xnnnn...) angeben. Länge 1 bis 10 Zeichen, es sind alphanumerische Zeichen und die Sonderzeichen @ $ # _ - + = * erlaubt. Ein abdruckbarer Selektor wird im Protokoll in ASCII mit variabler Länge codiert.

Standardwert: leer

Hinweis:
Abdruckbare Session-Selektoren werden in openFT immer mit Großbuchstaben verwendet, auch wenn sie in Kleinbuchstaben angegeben oder ausgegeben werden.

psel
Nur bei FTAM-Partnern relevant.
Presentation-Selektor, unter dem die Filetransfer-Anwendung im Partnersystem erreichbar ist. Sie können den Selektor abdruckbar oder hexadezimal (im Format 0xnnnn...) angeben. Länge 1 bis 10 Zeichen, es sind alphanumerische Zeichen und die Sonderzeichen @ $ # _ - + = * erlaubt. Ein abdruckbarer Selektor wird im Protokoll in ASCII mit variabler Länge interpretiert.

Standardwert: leer

Hinweis:
Abdruckbare Presentation-Selektoren werden in openFT immer mit Großbuchstaben verwendet, auch wenn sie mit Kleinbuchstaben angegeben oder ausgegeben werden.

Beispiele

Der Partnerrechner mit dem Hostnamen FILESERV soll über unterschiedliche Protokolle/Kopplungsarten angesprochen werden:

Kopplungsart/Protokoll	**Adressangabe**
openFT-Partner	FILESERV
FTAM-Partner (Windows-System ab V11.0, BS2000- oder Unix-System mit Default-Einstellung)	ftam://FILESERV
FTAM-Partner (Windows-System mit Default-Einstellung bis V10.0)	ftam://FILESERV:.SNI-FTAM
Fremder FTAM-Partner	ftam://FILESERV:102.TS0001.SES1.PSFTAM
FTP-Partner	ftp://FILESERV

3.8.4 FTAC-Sicherheitsstufen für Partner in der Partnerliste

Für den Fall, dass die FTAC-Funktionalität genutzt werden soll, sollte der FT-Verwalter in Abstimmung mit dem FTAC-Verwalter für jeden Partner in der Partnerliste zusätzlich die für FTAC relevante Sicherheitsstufe definieren. Dazu verwendet der FT-Verwalter im Kommando *ftaddptn* oder *ftmodptn* die Option *-sl* . Alternative im openFT Explorer: Verwenden Sie im Dialogfeld *Partnerlisteneintrag* die Optionen im Bereich *Sicherheitsstufe*.

Die Sicherheitsstufen sind die Maßeinheit für das Schutzbedürfnis gegenüber dem Partnersystem. Großes Schutzbedürfnis führt zu einer großen Sicherheitsstufe, kleines Schutzbedürfnis zu einer kleinen Sicherheitsstufe. Beim ersten Einsatz von FTAC sollten die Sicherheitsstufen in Zehnerschritten vergeben werden. Dadurch wird die Möglichkeit offen gelassen, neu hinzukommende Partnersysteme flexibel in die bestehende Hierarchie einzubetten.

Sollte sich das Schutzbedürfnis gegenüber einem Partnersystem ändern, wird die Sicherheitsstufe des Partnersystems mit dem Kommando *ftmodptn* den neuen Bedürfnissen angepasst.

Sie können bei *ftaddptn* und *ftmodptn* über *-sl=p* auch folgenden Automatismus für die Sicherheitsstufen einschalten:

- Partner, die von openFT authentifiziert werden, erhalten die Sicherheitsstufe 10.
- Partner, die im Transportsystem bekannt sind, erhalten die Sicherheitsstufe 90.
- Partner, die nur über ihre IP-Adresse adressiert werden (z.B. FTP-Partner) erhalten Sicherheitsstufe 100.

Dieser Automatismus kann sowohl partnerspezifisch (*ftaddptn* und *ftmodptn*) als auch global per *ftmodo* aktiviert werden.

Dieser Automatismus gilt auch für alle Partner, die nicht in der Partnerliste eingetragen sind (freie dynamische Partner), unabhängig davon, was in den Betriebsparametern eingestellt ist.

Wurde beim Erzeugen eines Partners (mit *ftaddptn* oder über den openFT Explorer) keine Sicherheitsstufe angegeben, so verwendet openFT die globale Einstellung in den Betriebsparametern (*ftmodo*). Dort kann auch eine feste Sicherheitsstufe als Standard eingestellt werden.

Die Sicherheitsstufe eines Partnereintrags kommt zum Tragen, wenn ein Benutzer über diesen Partnereintrag einen Auftrag abwickeln will. Die Sicherheitsstufe des Partnereintrags wird von FTAC mit der im Berechtigungssatz des Benutzers vergebenen Sicherheitsstufe für die benötigte Funktion (zum Beispiel inbound Senden) verglichen. Ist die Sicherheitsstufe im Berechtigungssatz kleiner als die des Partnereintrags, so wird der Auftrag von FTAC abgelehnt. Wird für den Auftrag ein privilegiertes FTAC-Profil verwendet, so kann der Benutzer sich über die im Berechtigungssatz definierten Einschränkungen hinwegsetzen.

3.8.5 Outbound- und Inbound-Deaktivierung von benannten Partnern

Sie haben die Möglichkeit, benannte Partner gezielt für asynchrone Outbound-Aufträge oder für Inbound-Aufträge zu deaktivieren.

Für Outbound-Aufträge können Sie zusätzlich die automatische Deaktivierung einschalten, sodass nach fünf fehlgeschlagenen Verbindungsaufbauversuchen der Partner für Outbound-Aufträge deaktiviert wird. Vor einem erneuten Versuch zum Verbindungsaufbau muss dieses Partnersystem manuell wieder aktiviert werden. Dadurch wird verhindert, dass unnötige Kosten entstehen, da u.U. auch erfolglose Verbindungsaufbauversuche kostenpflichtig sind.

Diese Einstellungen können Sie schon beim Einrichten des Partnersystems mit dem Kommando *ftaddptn* oder später mit dem Kommando *ftmodptn* zuweisen.

3.8.6 Serialisierung von asynchronen Outbound-Aufträgen

Sie können für ein Partnersystem die Serialisierung von asynchronen Outbound-Aufträgen erzwingen. Dazu verwenden Sie bei den Kommandos *ftaddptn* und *ftmodptn* die Option *-rqp=s* oder aktivieren im openFT Explorer die Option *Serielle Ausführung asynchroner Outbound-Aufträge*.

Dadurch werden Überholeffekte vermieden, die bei paralleler Bearbeitung von Aufträgen auftreten können. Im Einzelnen gilt für die serielle Bearbeitung:

- Ein Folgeauftrag wird erst gestartet, wenn der vorhergehende Auftrag beendet ist.
- Die Serialisierung schließt Vor- und Nachverarbeitungen mit ein, nicht aber Folgeverarbeitungen, da diese unabhängig vom Auftrag sind.

Diese Funktion kann z.B. in einer Filial-Zentral-Konfiguration eingesetzt werden, bei der die Filialen zeitgleich mehrere Dateien an die Zentrale schicken (Tages-, Wochen- oder Monatsabschluss). Wird in den Filialrechnern für den Partner „Zentralrechner“ die Serialisierung aktiviert, dann kann pro Filialrechner immer nur eine Verbindung zum Zentralrechner aktiv sein. Dadurch werden Engpässe auf dem Zentralrechner verhindert wie z.B. eine regelmäßige Überschreitung des Verbindungslimits (siehe auch Parameter CONN-LIM bei *ftshwo*).

3.9 Messdatenerfassung mit openFT

openFT bietet die Möglichkeit, eine Reihe von charakteristischen Daten des openFT-Betriebs zu messen und anzuzeigen. Die Daten lassen sich in drei Gruppen einteilen:

- Durchsatz, z.B gesamter durch openFT bedingter Netzdurchsatz
- Zeitdauer, z.B. Bearbeitungsdauer für asynchrone Aufträge
- Status, z.B. Anzahl der aktuell wartenden Aufträge

Um die Messdatenerfassung ein- oder auszuschalten und zu konfigurieren, müssen Sie FT-Verwalter sein.

Wenn der asynchrone openFT-Server gestartet und die Messdatenerfassung eingeschaltet ist (*ftmodo*), kann jeder beliebige Benutzer die Daten abrufen und sich nach bestimmten Kriterien ausgeben lassen (*ftshwm*).

3.9.1 Messdatenerfassung konfigurieren

Sie konfigurieren die Messdatenerfassung über das Kommando *ftmodo* (Seite 236) oder den openFT Explorer (Menüpunkt *Administration* - *Betriebsparameter*, Registerblatt *Überwachung*). Dabei haben Sie folgende Möglichkeiten:

- Erfassung einschalten und ausschalten (*ftmodo -mon=*)
- Erfassung nach Partnertyp selektieren (*ftmodo -monp=*)
- Erfassung nach Auftragstyp selektieren (*ftmodo -monr=*)

Die einmal gewählten Einstellungen bleiben solange erhalten, bis Sie sie explizit ändern. Sie sind also auch nach einem Neustart des Rechners unverändert verfügbar.

Mit dem Kommando *ftshwo* können Sie die aktuellen Einstellungen überprüfen. Die Zeile MONITOR zeigt an, ob die Messdatenerfassung eingeschaltet ist und nach welchen Kriterien selektiert wird.

3.9.2 Messdaten anzeigen

Wenn die Messdatenerfassung eingeschaltet und der asynchrone openFT-Server gestartet ist, können Sie jederzeit die Messdaten abrufen. Die Daten können Sie sich auf folgende Arten ausgeben lassen:

- über das Kommando *ftshwm*
- über den openFT Monitor
- über Vorverarbeitung

3.9.2.1 Lokale Messdaten über das Kommando ftshwm anzeigen

ftshwm gibt die Messdaten in Form von Tabellen aus, die Sie bei Bedarf per Editor oder Programm weiterverarbeiten können.

Bei Aufruf von *ftshwm* geben Sie an, welche Messdaten ausgegeben werden, in welcher Form sie ausgegeben werden (aufbereitet, nicht aufbereitet, im Tabellenformat oder im CSV-Format), und in welchem Zeitintervall die Ausgabe aktualisiert werden soll.

Details zu *ftshwm* finden Sie auf Seite 333.

3.9.2.2 Lokale oder entfernte Messdaten über den openFT Monitor anzeigen

Für die Ausgabe mit dem openFT Monitor ist ein grafikfähiges Terminal nötig. Der openFT Monitor gibt die Daten standardmäßig in Form eines oder mehrerer Diagramme aus. Die Diagramme zeigen den aktuellen Stand und Verlauf der Messdaten an. Im openFT Monitor können Sie einstellen, welche Werte angezeigt werden sollen, und diese Einstellung auch für spätere Sitzungen abspeichern. Auch eine tabellarische Anzeige aller Messdaten in einem Grafikfenster ist möglich.

Sie starten den openFT Monitor entweder über den openFT Explorer (Menü *Extras* bzw. Kontextmenü eines Partnereintrags) oder über das Kommando *ftmonitor* (siehe Seite 284). Beim Starten geben Sie auch das Zeitintervall an, in dem die Ausgabe aktualisiert werden soll. Weitere Details zum openFT Monitor sind in der Online-Hilfe beschrieben.

Entfernte Messdaten mit openFT Monitor anzeigen

Über den openFT Monitor können Sie sich die Messdaten von openFT-Instanzen auf anderen Systemen anzeigen lassen. Beim Aufruf des openFT Monitors werden hierfür der Partner und die Zugangsberechtigung angegeben. Im openFT Explorer geschieht dies implizit, wenn Sie den openFT Monitor aus dem Kontextmenü eines Eintrags im Objektverzeichnis *Partner* starten. Dazu müssen Sie in den Eigenschaften dieses Partners die Optionen *Ferne Kommandoausführung* und *Administrationsobjekte* aktivieren.

3.9.2.3 Entfernte Messdaten über Vorverarbeitung anzeigen

Sie können den Zugriff aus einem fernen System auf die Übertragung von Messdaten einschränken. Dazu definieren Sie für die Zugangsberechtigung ein Berechtigungsprofil, in dem Sie ein Dateinamen-Präfix mit dem Schlüsselwort *FTMONITOR als Vorverarbeitungskommando angeben. *FTMONITOR ist ein Schlüsselwort für openFT, das die Übermittlung von Monitordaten in der vom grafischen openFT Monitor gewünschten Form bewirkt.

Sie können sich Messdaten von anderen Systemen auch als Zeilenausgaben anzeigen lassen. Dazu verwenden Sie die Dateiübertragungs-Kommandos *ft* und *ncopy* zusammen mit einem Berechtigungsprofil, welches das Vorverarbeitungskommando *FTMONITOR enthält. .

Beispiel

Dieses Beispiel zeigt, wie Sie ein Berechtigungsprofil für die Vorverarbeitung auf dem fernen System einrichten (1.) und wie Sie es für die Ausgabe über den openFT Monitor (2.) und die Zeilenausgabe (3.) nutzen können.

1. Definieren Sie auf dem fernen System *Partner1* ein Berechtigungsprofil *monitor1*, das nur die Ausgabe von Messdaten erlaubt. Als Zugangsberechtigung vergeben Sie *onlyftmonitor*.

   – Unix- oder Windows-System:

   ```
   ftcrep monitor1 onlyftmonitor -ff=tp -fnp="|*FTMONITOR "
   ```

   – BS2000-System:

   ```
   /CREATE-FT-PROFILE NAME=MONITOR1 -
      ,TRANSFER-ADMISSION=ONLYFTMONITOR, -
      ,FILE-NAME=*EXPANSION('|*FTMONITOR ') -
      ,FT-FUNCTION=(*TRANSFER-FILE,*FILE-PROCESSING)
   ```

   – z/OS-System:

   ```
   FTCREPRF NAME=MONITOR1
      .TRANSFER-ADMISSION=ONLYFTMONITOR -
      ,FILE-NAME=*EXPANSION('|*FTMONITOR ') -
      ,FT-FUNCTION=(*TRANSFER-FILE,*FILE-PROCESSING)
   ```

   Der Stern (*) bei *FTMONITOR im Profil *monitor1* muss angegeben werden. Außerdem wird empfohlen, schon im Profil ein Leerzeichen hinter *FTMONITOR zu schreiben, damit nachfolgende Optionen automatisch vom Kommando getrennt werden.

2. Die Zugangsberechtigung dieses Profils können Sie im Kommando *ftmonitor* angeben, wenn Sie sich von einem fernen System aus die openFT-Messdaten anzeigen lassen wollen. .

   ```
   ftmonitor -po=10 Partner1 onlyftmonitor
   ```

   Für den Aufruf des grafischen openFT Monitors aus dem openFT Explorer definieren Sie im Objektverzeichnis *Partner* einen Partner mit dieser Zugangsberechtigung

3. Alternativ können Sie mit diesem FTAC-Profil die Messdaten als Zeilenausgaben erhalten und für eine Weiterverarbeitung mit einem *ft*- bzw. *ncopy*-Kommando in eine Datei umleiten. Bitte beachten Sie, dass an dieser Stelle nur das Zeitintervall eingestellt, aber keine Messwertauswahl getroffen werden kann. Die Ausgabe erfolgt stets im CSV-Format. Mit folgendem Kommando können Sie sich die aktuellen Messwerte von *Partner1* im Abstand von 10 Sekunden ausgeben lassen:

   ```
   ncopy Partner1!"-po=10" partner1_data onlyftmonitor
   ```

   Die Messdaten werden in die Datei *partner1_data* ausgegeben. Innerhalb der Anführungszeichen können Sie als einzigen Parameter *-po=polling intervall* angeben. Wenn Sie das standardmäßige Polling-Intervall von 1 Sekunde verwenden wollen, schreiben Sie ein Leerzeichen zwischen die Anführungszeichen.

3.10 Sicherheit im openFT-Betrieb

Jeder Benutzer, der auf Betriebsmittel oder Ressourcen eines Systems zugreifen will, muss dem System gegenüber seine Berechtigung für diesen Zugriff nachweisen. Für File-Transfer-Aktivitäten muss die Zugangsberechtigung im fernen System nachgewiesen werden. Dieser Nachweis setzt sich in der Regel aus der Angabe der Benutzerkennung und des entsprechenden Passworts zusammen.

Weitergehenden Schutz beim File Transfer bieten die folgenden Funktionen:

- Authentifizierung
- Verschlüsselung bei der Dateiübertragung, siehe Seite 86
- Nutzung der FTAC-Funktionen, siehe Seite 92

Außerdem bietet openFT eine erweiterte Absenderüberprüfung (siehe Seite 86), falls z.B. nicht mit Authentifizierung gearbeitet werden kann, sowie Schutzmechanismen gegen Dateiinkonsistenz (siehe Seite 88).

3.10.1 Authentifizierung

Sollen sicherheitskritische Daten übertragen werden, so ist es wichtig, das jeweilige Partnersystem vor der Übertragung einer sicheren Identitätsprüfung zu unterziehen („Authentifizierung“). Die beiden an einer Übertragung beteiligten openFT-Instanzen müssen gegenseitig mit kryptografischen Mitteln überprüfen können, ob sie mit der „richtigen“ Partnerinstanz verbunden sind.

Ab den openFT Versionen V8.1 für Unix- und Windows-Systeme bzw. V9.0 für BS2000 und z/OS wird daher für openFT-Partner ein erweitertes Adressierungs- und Authentifizierungskonzept unterstützt. Es basiert auf der Adressierung der openFT-Instanzen durch netzweit eindeutige Identifikationen sowie dem Austausch von partnerspezifischen Schlüsselinformationen.

Bei Kommunikation mit Partnern, die eine openFT Version 8.0 (oder älter) einsetzen, sind die im Folgenden beschriebenen Funktionen nicht nutzbar. Das bisherige Adressierungskonzept wird für diese Partner noch kompatibel unterstützt. Für FTAM-Partner steht die Authentifizierung in dieser Form nicht zur Verfügung, da das von der ISO genormte FTAM-Protokoll keine vergleichbare Funktionalität vorsieht.

3.10.1.1 Einsatzfälle für die Authentifizierung

Für die gegenseitige Authentifizierung gilt grundsätzlich: Diejenige Instanz, die eine andere authentifizieren möchte, braucht deren öffentlichen Schlüssel.

Es sind drei Einsatzfälle zu unterscheiden:

- Fall 1:
  Für die lokale openFT-Instanz ist es wichtig, dass die bezogenen Daten aus einer sicheren Quelle kommen.

  Dazu überprüft die lokale openFT-Instanz die Identität der Partnerinstanz. Das setzt voraus, dass lokal ein aktueller öffentlicher Schlüssel der Partnerinstanz abgelegt wurde, siehe Abschnitt „Schlüssel von Partnersystemen verwalten“ auf Seite 84.

  Eine derartige Konfiguration macht beispielsweise Sinn, wenn per openFT auf Dateien eines Servers zugegriffen werden soll. Für die lokale openFT-Instanz ist es wichtig, dass die bezogenen Daten aus einer sicheren Quelle (dem authentifizierten Partner) kommen, umgekehrt ist es für den Server unerheblich, wer dort zugreift.

- Fall 2:
  Für die Partnerinstanz ist es wichtig, dass nur von einer sicheren lokalen openFT-Instanz auf ihre Daten zugegriffen wird.

  Dazu überprüft die Partnerinstanz die Identität der lokalen openFT-Instanz. Das setzt voraus, dass ein aktueller öffentlicher Schlüssel der lokalen openFT-Instanz in der Partnerinstanz hinterlegt ist (bei BS2000- und z/OS- bzw. OS/390-Partnern umcodiert), siehe Abschnitt „Schlüssel an Partnersysteme verteilen“ auf Seite 85.

  Eine solche Konfiguration wäre beispielsweise denkbar, wenn von einem zentralen Rechner per openFT auf Partnersysteme in mehreren Filialen zugegriffen werden soll, und die Filialrechner nur Zugriffe des Zentralrechners (und wirklich nur dieses Rechners) zulassen dürfen.

- Fall 3:
  Sowohl für die lokale openFT-Instanz als auch für die Partnerinstanz ist es wichtig, dass die Daten aus einer sicheren Quelle stammen und in sichere Hände gelangen (Kombination aus Fall 1 und Fall 2).

  Dazu überprüfen beide Instanzen jeweils die Identität des Anderen. Das setzt voraus, dass beide Systeme einen aktuellen öffentlichen Schlüssel ausgetauscht und in der Partnerinstanz hinterlegt haben.

3.10.1.2 Instanzidentifikationen

Die Instanzidentifikation ist ein bis zu 64 Zeichen langer Name, dessen Eindeutigkeit unabhängig von Groß- und Kleinschreibung **netzweit** gelten muss. Sie spielt insbesondere dann eine Rolle, wenn mit Authentifizierung gearbeitet wird.

Bei der Installation wird standardmäßig der Name des Rechners im lokalen Netz als Instanzidentifikation festgelegt. Falls die netzweite Eindeutigkeit nicht gesichert ist, müssen Sie die Instanzidentifikation ändern.
Dazu verwenden Sie das Kommando *ftmodo*, Option *-id*.

Lokale Instanzidentifikation ändern

Eine Instanzidentifikation darf aus alphanumerischen Zeichen sowie Sonderzeichen bestehen. Es wird empfohlen, nur die Sonderzeichen ".", "-", ":" und "%" zu verwenden. Das erste Zeichen muss alphanumerisch oder das Sonderzeichen "%" sein. Das Zeichen "%" darf nur als erstes Zeichen vorkommen. Nach einem "." muss ein alphanumerisches Zeichen folgen.

Um die netzweite Eindeutigkeit für Instanzidentifikationen zu gewährleisten, sollten Sie bei der Vergabe von Instanzidentifikationen folgendermaßen vorgehen:

- Falls die openFT-Instanz eine Netzadresse mit einem **DNS-Namen** besitzt, sollten Sie diesen als Identifikation benutzen. Sie können einen "künstlichen" DNS-Namen für eine openFT-Instanz erzeugen, indem Sie einem vorhandenen „benachbarten“ DNS-Namen mit Punkt abgetrennt einen weiteren Namensteil voranstellen.
- Wenn die openFT-Instanz keinen DNS-Namen besitzt, aber an ein TCP/IP-Netz angebunden ist, sollten Sie die folgende Identifikation verwenden:
  - IPv4: **%ip***n.n.n.n* (*n.n.n.n* ist die IPv4-Adresse der lokalen openFT-Instanz ohne führende Nullen in den Adressbestandteilen).
  - IPv6:
    %ip6[*x***:***x***:***x***:***x***:***x***:***x***:***x***:***x***]** (ohne Scope-Id) oder
    %ip6[*x***:***x***:***x***:***x***:***x***:***x***:***x***:***x***%***s***]** (mit Scope-Id)
    Dabei ist *x:x:x:x:x:x:x:x* die IPv6-Adresse der lokalen openFT-Instanz und *s* die Scope-Id der lokalen Netzwerkkarte.

Instanzidentifikation von Partnern

Instanzidentifikationen von Partnersystemen sollten aus Sicht Ihres lokalen Systems mit der Partneradresse übereinstimmen, unter der das Partnersystem im openFT bekannt ist. Ist dies nicht der Fall, dann müssen Sie den Partner in die Partnerliste eintragen und dabei dessen Instanzidentifikation explizit angeben.

Beachten Sie bitte Folgendes:

– Wenn Sie beim Eintrag in die Partnerliste die Instanzidentifikation nicht spezifizieren, dann wird bei openFT- und ADM-Partnern als Standardwert die Partneradresse gesetzt (ohne Portnummer und/oder Transport-Selektor, falls diese bei der Partneradresse angegeben wurden). D. h. die Instanzidentifikation des Partners muss dann mit der angegebenen Partneradresse (ohne Portnummer/T-Selektor) übereinstimmen.

– Falls Ihr Partnersystem noch ein openFT der Version V8.0 oder älter ist, wird Authentifizierung noch nicht unterstützt. In diesem Fall sollten Sie beim Eintrag in die Partnerliste als Ersatz-Identifikation %.<prozessor>.<entity> mit dem Prozessor- und Stationsnamen des Partners angeben, damit von diesem Partner ankommende Aufträge diesem Eintrag zugeordnet werden können.

Es besteht alternativ dazu auch die Möglichkeit, den Namen über DNS auflösen zu lassen oder einen Eintrag in der */etc/hosts* oder im TNS vorzunehmen. Bei einem Eintrag im TNS muss der Globale Name dann mit der Instanzidentifikation des Partners übereinstimmen.

Anhand der Instanzidentifikationen der Partnersysteme verwaltet openFT die diesen Partnern zugeordneten Betriebsmittel wie z.B. Auftragswarteschlangen und kryptografische Schlüssel.

3.10.1.3 Lokale RSA-Schlüsselpaare erzeugen und verwalten

RSA-Schlüssel werden für die Authentifizierung und die Aushandlung des AES-Schlüssels verwendet, mit dem die Auftragsbeschreibungsdaten und Dateiinhalte verschlüsselt werden.

Zum Erzeugen und Verwalten von lokalen RSA-Schlüsseln stehen Ihnen folgende Kommandos zur Verfügung:

- Mit *ftcrek* (oder über den openFT Explorer) erzeugen Sie für die lokale openFT-Instanz RSA-Schlüsselpaare, die jeweils aus einem privaten (private key) und einem öffentlichen Schlüssel (public key) bestehen.
- Mit *ftshwk* geben Sie die Eigenschaften aller Schlüssel im lokalen System aus.
- Mit *ftupdk* aktualisieren Sie öffentliche Schlüssel.
- Mit *ftdelk* löschen Sie lokale Schlüsselpaare.
- Mit *ftmodk* modifizieren Sie RSA-Schlüssel.
- Mit *ftimpk* importieren Sie RSA-Schlüssel.

Sie können RSA-Schlüsselpaare auch über den openFT Explorer erzeugen und verwalten. Wählen Sie dazu im Menü *Administration* - *Schlüsselverwaltung* den entsprechenden Befehl aus.

Eigenschaften von Schlüsselpaaren

Ein RSA-Schlüsselpaarsatz im UnixWindows-System besteht aus drei Schlüsselpaaren mit den Längen 768, 1024 und 2048 Bit.

Private Schlüssel werden von openFT intern verwaltet. Öffentliche Schlüssel werden im Verzeichnis *config* des Instanzdateibaums (siehe „Instanzenverzeichnis“ auf Seite 26) der openFT-Instanz unter folgendem Namen abgespeichert:

```
syspkf.r<schlüsselreferenz>.l<schlüssellänge>
```

Die Schlüsselreferenz ist ein numerischer Bezeichner für die Version des Schlüsselpaares. Die öffentlichen Schlüsseldateien sind Textdateien, die im Zeichencode des jeweiligen Betriebssystems erzeugt werden, d.h. standardmäßig:

– BS2000/OSD: Wert des Systemparameters HOSTCODE
– z/OS: IBM1047
– Unix-Systeme: ISO8859-1
– Windows-Systeme: CP1252

Kommentare hinterlegen

In der Datei *syspkf.comment* im Verzeichnis *config* des Instanzdateibaums können Sie Kommentare hinterlegen, die beim Erzeugen eines Schlüsselpaarsatzes in die ersten Zeilen der öffentlichen Schlüsseldateien geschrieben werden. Die Datei *syspkf.comment* ist eine Textdatei, die Sie editieren können. Kommentare könnten beispielsweise die Kontaktdaten des zuständigen FT-Verwalters, den Rechnernamen oder ähnliche für Partner wichtige Informationen enthalten. Die Zeilen in der Datei *syspkf.comment* dürfen maximal 78 Zeichen lang sein. Mit dem Kommando *ftupdk* können Sie auch nachträglich aktualisierte Kommentare aus dieser Datei in existierende öffentliche Schlüsseldateien einbringen.

Schlüssel aktualisieren und ersetzen

Wurde eine öffentliche Schlüsseldatei versehentlich gelöscht, können Sie mit *ftupdk* die öffentlichen Schlüsseldateien der bestehenden Schlüsselpaarsätze neu erzeugen.

Wenn Sie einen Schlüsselpaarsatz durch einen komplett neuen ersetzen wollen, können Sie mit *ftcrek* einen neuen Schlüsselpaarsatz erzeugen. Sie erkennen den aktuellsten öffentlichen Schlüssel an der höchstwertigen Schlüsselreferenz im Namen der Datei. openFT unterstützt maximal drei Schlüsselpaarsätze gleichzeitig. Mehrere Schlüssel sollten aber nur temporär existieren, bis Sie allen Partnersystemen den aktuellsten öffentlichen Schlüssel zur Verfügung gestellt haben. Danach können Sie nicht mehr benötigte Schlüsselpaarsätze mit *ftdelk* löschen. Gelöschte Schlüsselpaarsätze lassen sich nicht mit *ftupdk* wieder herstellen.

3.10.1.4 Schlüssel importieren

Sie können mit dem Kommando *ftimpk* oder dem openFT Explorer (*Administration* - *Schlüsselverwaltung*) folgende Schlüssel importieren:

- Private Schlüssel, die mit einem externen Tool (d.h. nicht über openFT) erzeugt wurden. openFT erzeugt beim Importieren eines privaten Schlüssels den zugehörigen öffentlichen Schlüssel und legt ihn im Verzeichnis *config* im Instanzendateibaum ab, siehe „Eigenschaften von Schlüsselpaaren“ auf Seite 82. Dieser Schlüssel kann wie ein mit *ftcrek* erzeugter Schlüssel verwendet und an Partnersysteme verteilt werden.
- Öffentliche Schlüssel von Partnerinstanzen. Diese Schlüssel müssen das openFT-Schlüsselformat (syspkf) besitzen, d.h. sie müssen von der openFT-Instanz des Partners erzeugt worden sein. openFT legt den Schlüssel im Verzeichnis *syskey* ab, siehe Abschnitt „Schlüssel von Partnersystemen verwalten“ auf Seite 84.

Jedes importierte Schlüsselpaar erhält eine eindeutige Referenznummer. Importiert werden RSA-Schlüssel in den unterstützten Schlüssellängen (768, 1024 und 2048 Bit).

openFT unterstützt Schlüsseldateien in den folgenden Formaten:

- PEM-Format (native PEM)

  Die PEM-codierten Dateien müssen im EBCDIC-Format vorliegen.
- PKCS#8 Format ohne Passphrase oder nach v1/v2 mit einer Passphrase verschlüsselt (PEM-codiert).

  Die zur Verschlüsselung verwendete Passphrase müssen Sie beim Importieren im Passwort-Parameter angeben.
- PKCS#12 v1 Format in Form einer Binärdatei. Die Datei wird nach einem privaten Schlüssel durchsucht, nicht unterstützte Bestandteile (z.B. Zertifikate, CRLs) werden beim Import ignoriert. Ist das Zertifikat per Signatur oder Hash geschützt, so wird von openFT keine Gültigkeitsprüfung durchgeführt. Die Gültigkeit der Datei muss durch externe Mittel sichergestellt werden. Der erste private Schlüssel, der in der Datei gefunden wird, wird importiert, weitere werden ignoriert.

  Die zur Verschlüsselung verwendete Passphrase müssen Sie beim Importieren im Passwort-Parameter angeben.

3.10.1.5 Schlüssel von Partnersystemen verwalten

Die öffentlichen Schlüssel der Partnersysteme müssen auf Unix-Systemen als Dateien im Verzeichnis *syskey* des Instanzdateibaums der lokalen openFT-Instanz hinterlegt werden, siehe „Instanzenverzeichnis“ auf Seite 26 (Standard: */var/openFT/std/syskey*). Als Dateiname muss die Instanzidentifikation des Partnersystems gewählt werden.

Sie haben folgende Möglichkeiten, den öffentlichen Schlüssel eines Partnersystems zu importieren:

- Sie rufen das Kommando *ftimpk* auf und geben dort den Namen der Schlüsseldatei an. openFT speichert den Schlüssel im Verzeichnis *syskey* und verwendet als Dateinamen die Instanzidentifikation des Partners mit der richtigen Schreibweise (Kleinschreibung).
- Sie speichern die Schlüsseldatei mit Betriebssystem-Mitteln im Verzeichnis *syskey* unter dem Namen der Instanzidentifikation des Partners ab. Der Dateiname darf keine Großbuchstaben enthalten. Enthält die Identifikation Großbuchstaben, müssen diese im Dateinamen in Kleinbuchstaben umgesetzt werden.

Wenn ein aktualisierter öffentlicher Schlüssel von der Partnerinstanz zur Verfügung gestellt wird, muss die alte Schlüsseldatei damit überschrieben werden.

Mit dem Kommando *ftshwk* können Sie die Schlüssel von Partnersystemen anzeigen (Option *-pn)* und dabei auch nach Verfallsdatum filtern (Option *-exp*).

Für Secure FTP gelten verschiedene Besonderheiten, siehe „Hinweis zu Secure FTP“ auf Seite 88.

Schlüssel von Partnersystemen modifizieren

Sie können mit dem Kommando *ftmodk* die Schlüssel von Partnersystemen modifizieren, indem Sie ein Verfallsdatum festlegen oder die Authentifizierungsstufe (1 oder 2) ändern:

- Wenn Sie ein Verfallsdatum festlegen, dann kann der Schlüssel nach Ablauf dieses Datums nicht mehr verwendet werden.
- Wenn Sie Authentifizierungsstufe 2 einstellen, dann führt openFT zusätzliche interne Prüfungen durch. Stufe 2 wird für alle openFT-Partner ab Version 11.0B unterstützt. Ein Authentifizierungsversuch nach Stufe 1 wird zu diesem Partner abgelehnt.

Sie können diese Einstellungen wahlweise für einen bestimmten Partner oder für alle Partner festlegen oder nachträglich ändern.

3.10.1.6 Schlüssel an Partnersysteme verteilen

Die Verteilung der öffentlichen Schlüsseldateien an Ihre Partnersysteme sollte auf gesichertem Weg geschehen, also z.B. durch

– kryptografisch abgesicherte Verteilung per E-Mail
– Verteilung per CD (persönliche Übergabe oder per Einschreiben)
– Verteilung über einen zentralen openFT-Fileserver, dessen öffentlichen Schlüssel die Partner besitzen.

Sie müssen darauf achten, dass Ihre öffentlichen Schlüsseldateien umcodiert werden (z.B. durch eine Übertragung als Textdatei per openFT), wenn Sie sie an Partnersysteme mit BS2000, z/OS (bzw. OS/390) oder Windows übermitteln.

Die öffentliche Schlüsseldatei Ihrer lokalen openFT-Instanz wird im Partnersystem an folgender Stelle abgelegt:

- Bei Partnern mit openFT für BS2000 als PLAM-Element vom Typ D in der Bibliothek *SYSKEY* auf der Konfigurations-Userid der Partnerinstanz. Als Elementname muss der in der fernen Partnerliste SYSPTF für Ihre openFT-Instanz vergebene Partnername gewählt werden.
- Bei Partnern mit openFT für Unix-Systeme im Verzeichnis *syskey* des Instanzdateibaums. Bei der Standardinstanz lautet der Pfadname */var/openFT/std/syskey*. Als Dateiname muss die Instanzidentifikation Ihrer lokalen openFT-Instanz gewählt werden. Der Dateiname darf keine Großbuchstaben enthalten. Enthält die Instanzidentifikation Großbuchstaben, müssen diese im Dateinamen in Kleinbuchstaben umgesetzt werden.
- Bei Partnern mit openFT für Windows im Verzeichnis *syskey* des Instanzdateibaums. Bei der Standardinstanz lautet der Pfadname auf Windows 7 *%ProgramData%\Fujitsu Technology Solutions\openFT\var\std\syskey*.
  Auf älteren openFT-Versionen mit Windows XP lautet der Pfadname *openFT-installationsverzeichnis\var\std\syskey*.
  Als Dateiname muss die Instanzidentifikation Ihrer lokalen openFT-Instanz gewählt werden.
- Bei Partnern mit openFT für z/OS bzw. OS/390 als PO-Element in der Bibliothek *admuser.instanz.SYSKEY*. Dabei ist *instanz* der Name der Instanz. Als Elementname muss der, in der fernen Partnerliste SYSPTF für Ihre openFT-Instanz vergebene, Partnername gewählt werden.

3.10.2 Erweiterte Absenderüberprüfung

openFT-Partner mit openFT-Versionen ab V8.1 unterstützen den Mechanismus der Authentifizierung (siehe Seite 78). Wenn das lokale System über einen öffentlichen Schlüssel des Partners verfügt, wird mit kryptografischen Mitteln die Identität des Partners geprüft.

Für Partnersysteme, die nicht mit Authentifizierung arbeiten, wird bei inbound-Aufträgen anhand der Instanzidentifikation überprüft, ob das "rufende" System über einen gültigen Eintrag in der Partnerliste verfügt. openFT bietet mit der erweiterten Absenderüberprüfung die Möglichkeit, nicht nur die Instanzidentifikation, sondern zusätzlich auch die Transportadresse zu überprüfen.

Die erweiterte Absenderüberprüfung kann für openFT-Partner global oder partnerspezifisch eingeschaltet werden:

- global mit *ftmodo -ptc=a*
  oder im openFT Explorer mit *Betriebsparameter* - *Allgemein*, *Partnerüberprüfung*
- partnerspezifisch mit *ftaddptn* / *ftmodptn -ptc=a*
  oder im openFT Explorer im Dialog *Partnerlisteneintrag* Abschnitt *Partnerüberprüfung*

Die globale Einstellung gilt für alle Partner, bei denen die Partnerüberprüfung auf Standard gesetzt ist (Ausgabe FTOPT bei *ftshwptn*).

Bei FTAM- und FTP-Partnern läuft die Absenderüberprüfung ausschließlich über die Transportadresse. Deshalb bleibt die Eigenschaft "erweiterte Absenderüberprüfung" für FTAM- und FTP-Partner wirkungslos und wird auch nicht angezeigt.

Für dynamische Partner hat die erweiterte Absenderüberprüfung keine Bedeutung, da diese immer über die Transportadresse identifiziert werden.

Fällt die Absenderüberprüfung negativ aus, wird der Auftrag abgewiesen.

3.10.3 Verschlüsselung bei der Dateiübertragung

openFT bietet die Möglichkeit, Auftragsbeschreibungsdaten und Dateiinhalte zu verschlüsseln.

Falls Sie neben der Verschlüsselung von Auftragsbeschreibungsdaten auch die Verschlüsselung von Dateiinhalten einsetzen wollen, installieren Sie zusätzlich openFT-CR V12.0. openFT-CR muss auch auf dem Partnersystem installiert sein. openFT-CR ist aus rechtlichen Gründen nicht in allen Staaten verfügbar.

openFT verwendet für die Verschlüsselung nach Möglichkeit das Verfahren RSA/AES mit einer Schlüssellänge von 256 Bit. Bei der Kopplung zu älteren Partnern kann auch RSA/AES mit 128 Bit bzw. RSA/DES zum Einsatz kommen. Es wird jeweils das sicherste, von beiden Partner unterstützte Verfahren verwendet.

Damit Ihr openFT Auftragsbeschreibungsdaten und Dateiinhalte verschlüsselt übertragen kann, muss im lokalen System ein RSA-Schlüsselpaarsatz existieren und die Verschlüsselung darf nicht ausgeschaltet sein (z.B. durch Angabe von *ftmodo -kl=0*). Mit dem Kommando *ftshwo* können Sie dies überprüfen. Der Ausgabearameter KEY-LEN zeigt die Länge des aktuell verwendeten RSA-Schlüssels in Bit an (0, 768, 1024 oder 2048). 0 bedeutet, dass die Verschlüsselung ausgeschaltet ist. Sie können die gewünschte Länge des RSA-Schlüssels per Betriebsparameter einstellen. Verwenden Sie dazu die Option *-kl* im Kommando *ftmodo* oder den openFT Explorer (Menü *Administration*, Befehl *Betriebsparameter*). Der Standardwert nach Neuinstallation ist 2048.

Bei der Neuinstallation von openFT wird ein RSA-Schlüsselpaarsatz erzeugt, bestehend aus privaten und öffentlichen Schlüsseln passender Länge. Weitere Schlüsselpaarsätze können Sie (falls nötig) mit *ftcrek* erzeugen oder mit *ftimpk* importieren. Obsolete Schlüsselpaarsätze löschen Sie mit *ftdelk*. Weitere Details zu lokalen Schlüsseln finden Sie in Abschnitt „Lokale RSA-Schlüsselpaare erzeugen und verwalten“ auf Seite 81.

Verschlüsselung erzwingen

Die Verschlüsselung der Dateiinhalte ist optional und wird normalerweise beim Übertragungsauftrag angefordert. Sie können aber auch per Betriebsparametereinstellung eine Verschlüsselung erzwingen (Pflicht-Verschlüsselung). Dazu verwenden Sie im Kommando *ftmodo* die Option *-c*. Alternative im openFT Explorer: Menü *Administration* - *Betriebsparameter*, Registerblatt *Allgemein*, Abschnitt *Verschlüsselung von Benutzerdaten*.

Die Pflicht-Verschlüsselung kann differenziert eingestellt werden (nur Inbound, nur Outbound oder alle Aufträge). Die Einstellungen gelten für Dateiübertragungsaufträge über das openFT-Protokoll und für Administrationsaufträge. FTAM-Aufträge und inbound FTP-Aufträge werden abgelehnt, da keine Verschlüsselung unterstützt wird, Dateimanagement wird unabhängig von den Einstellungen weiterhin unverschlüsselt durchgeführt. Zusätzlich gilt:

- Ist die Outbound-Verschlüsselung aktiviert, dann wird bei einem Outbound-Auftrag der Dateiinhalt verschlüsselt, auch wenn im Auftrag selber keine Verschlüsselung angefordert wurde. Wenn der Partner keine Verschlüsselung unterstützt (z.B. weil sie ausgeschaltet ist oder openFT-CR nicht installiert ist), dann wird der Auftrag abgelehnt.
- Ist die Inbound-Verschlüsselung aktiviert und soll ein unverschlüsselter Inbound-Auftrag bearbeitet werden, dann wird dieser Auftrag abgelehnt.

3.10.4 Schutzmechanismen gegen Datenmanipulation

openFT prüft bei Kommunikation mit openFT-Partnern ab V8.1 auch implizit die Integrität der übertragenen Daten. Der Umfang wird beim Übertragungsauftrag festgelegt:

– Bei Aufträgen mit Verschlüsselung wird auch der übertragene Dateiinhalt überprüft.

– Bei Aufträgen ohne Verschlüsselung kann explizit eine Integritätsprüfung des Dateiinhalts eingeschaltet werden. Verwenden Sie dazu die Option *-di* beim Kommando *ft* oder *ncopy* oder im openFT Explorer die Option *Integritätsgeprüft* im Dialog *Datei übertragen - Optionen*.

– Sind weder Verschlüsselung noch die Integritätsprüfung eingeschaltet, dann wird nur die Integrität der Auftragsbeschreibungsdaten geprüft.

Wird ein Fehler erkannt, versuchen wiederanlauffähige Aufträge eine erneute Übertragung. Nicht wiederanlauffähige Aufträge werden abgebrochen.

3.10.5 Hinweis zu Secure FTP

Für die Verschlüsselung stellt ein Secure-FTP-Server der openFT-Instanz seinen Schlüssel und das Zertifikat zur Verfügung. Eine gegenseitige Authentifizierung findet nicht statt.

openFT kann outbound verschlüsselte Dateiinhalte mit einem Secure-FTP-Server austauschen, wenn auf openFT-Seite openFT-CR installiert ist und der FTP-Server das Protokoll TLS (**T**ransport **L**ayer **S**ecurity) unterstützt. Als Verschlüsselungsverfahren wird AES (Advanced Encryption Standard) verwendet.

Inbound unterstützt openFT keine verschlüsselte Dateiübertragung über das FTP Protokoll.

Wenn openFT die Verschlüsselung des Dateiinhalts verlangt, der FTP-Server aber das Protokoll TLS nicht unterstützt, wird der Auftrag abgelehnt. Wenn openFT keine Verschlüsselung des Dateiinhalts verlangt, werden die Auftragsbeschreibungsdaten nur verschlüsselt, wenn der FTP-Server das Protokoll TLS akzeptiert, sonst werden die Auftragsbeschreibungsdaten unverschlüsselt übertragen.

3.11 Logging von openFT

Als FT- oder FTAC- Verwalter können Sie

- Logging-Sätze aller Benutzer ansehen
- die Logging-Datei umschalten und das Offline-Logging verwalten, siehe Seite 90
- Logging-Einstellungen ändern, siehe Seite 90
- Logging-Sätze aller Benutzer sichern und löschen, siehe Seite 91

Als ADM-Verwalter können Sie

- Logging-Sätze aller Benutzer ansehen (und damit in Datei sichern)
- Logging-Sätze aller Benutzer löschen

Logging-Dateien werden im Verzeichnis *log* der jeweiligen openFT-Instanz abgelegt. Eine Logging-Datei hat folgenden Namen

`syslog.L`*yymmdd*`.L`*hhmmss*

Dabei ist:

yy = Jahreszahl, 2-stellig.
mm = Monat, 2-stellig.
dd = Tag, 2-stellig.
hh = Stunde, 2-stellig.
mm = Minute, 2-stellig.
ss = Sekunde, 2-stellig.

Datum und Uhrzeit bezeichnen den Zeitpunkt (GMT), zu dem die Logging-Datei angelegt wurde. Durch dieses Suffix lassen sich die aktuelle und die Offline-Logging-Dateien voneinander unterscheiden, siehe Seite 90.

Logging-Sätze ansehen

Sie können sich mit dem Kommando *ftshwl* alle Logging-Sätze im System anschauen. Mit den Polling-Optionen von *ftshwl* können Sie außerdem die Ausgabe neuer Logging-Sätze in regelmäßigen Abständen wiederholen.

In der Ausgabe eines Logging-Satzes gibt es eine Spalte RC, in der mit einem vierstelligen Reason-Code die Ursache für die Ablehnung oder den Abbruch eines Auftrags steht. Hier kann aber auch eine positive Bestätigung zu einem Auftrag stehen (Reason-Code 0000). Die Bedeutung des Reason-Codes können Sie mit dem Kommando *fthelp* ermitteln.

Sie können sich auch über den openFT Explorer auch Logging-Sätze ansehen. Dazu klicken Sie im Navigationsbereich unter *Administration* auf *Logging*.

Im Objektfenster *Logging* können Sie dann u.a. folgende Funktionen ausführen:

– Details zu einem Logging-Satz ansehen
– Filterkriterien für die anzuzeigenden Logging-Sätze festlegen
– Logging-Sätze löschen

Logging-Datei umschalten und Offline-Logging verwalten

Sie können die Logging-Datei mit dem Kommando *ftmodo -lf=c* umschalten. Damit wird die aktuelle Logging-Datei geschlossen, bleibt aber als Offline-Logging-Datei erhalten. Für die folgenden Logging-Sätze wird eine neue Logging-Datei mit aktuellem Datum im Suffix erzeugt. Sie können die Logging-Datei beliebig oft umschalten und damit mehrere Offline-Logging-Dateien führen.

Das Umschalten hat folgende Vorteile:

– Beschleunigte Logging-Zugriffe durch kleinere Logging-Datei.

– Bessere Verwaltbarkeit der Logging-Sätze durch regelmäßiges Umschalten und Sichern der Offline-Logging-Dateien, siehe Seite 91.

– Möglichkeit einer umfangreichen Offline-Logging-Recherche ohne Beeinflussung des laufenden openFT-Betriebs.

Auch über den openFT Explorer können Sie die Logging-Datei umschalten (*Administration - Betriebsparameter - Logging*). Im openFT Explorer sehen Sie auch alle Offline-Logging-Dateien und deren Logging-Sätze (Teilbaum *Administration - Logging - Offline-Logging*).

Logging-Einstellungen ändern

Sie können den Umfang der Logging-Funktion einstellen sowie Zeitpunkte und Zeitintervalle für das automatische Löschen von Logging-Sätzen festlegen.

Umfang des Logging einstellen

Den Umfang des Logging, d.h. welche Logging-Sätze also protokolliert werden sollen, können Sie im openFT Explorer unter *Administration - Betriebsparameter - Logging* oder mit dem Kommando *ftmodo* (Optionen *-lt*, *-lc* und *-la*) einstellen.

Nach der Installation ist das Logging in vollem Umfang eingeschaltet. Sie können FT-, FTAC- und Administrationsfunktionen in unterschiedlichem Umfang protokollieren.

Automatisches Löschen von Logging-Sätzen einstellen

Die Intervalle für das automatische Löschen von Logging-Sätzen können Sie im openFT Explorer unter *Administration - Betriebsparameter - Logging* oder mit dem Kommando *ftmodo* (Option *-ld, -lda, -ldd* und *-ldt*) einstellen. Damit werden Logging-Sätze ab einem festgelegten Mindestalter in regelmäßigen Abständen zu einer bestimmten Uhrzeit gelöscht. Diese

automatische Löschfunktion ist nur dann aktiv, wenn openFT gestartet ist. Ist openFT zu einem vorgesehenen Löschtermin nicht gestartet, so wird der Löschauftrag beim nächsten Start nicht nachgeholt.

Nach der Installation ist das automatische Löschen von Logging-Sätzen ausgeschaltet. Sie sollten diese Funktion nur einschalten, wenn das lückenlose Protokollieren von Logging-Sätzen nicht notwendig ist.

Logging-Sätze in Datei sichern und Logging-Sätze löschen

Im Prinzip schreibt openFT beliebig viele Logging-Sätze. Wenn kein Plattenspeicherplatz mehr verfügbar ist, werden FT-Aufträge abgewiesen. Es ist daher unbedingt erforderlich, die Anzahl der zu schreibenden Logging-Sätze auf den notwendigen Umfang einzugrenzen, die Logging-Datei regelmäßig zu überwachen und nicht mehr benötigte Logging-Sätze zu löschen bzw. auszulagern.

Als FT-Verwalter, FTAC-Verwalter oder ADM-Verwalter dürfen Sie alle Logging-Sätze löschen. Dazu verwenden Sie das Kommando *ftdell*. Alternativ dazu können Sie Logging-Sätze auch im openFT Explorer löschen (Logging-Objektfenster, Kontextmenü-Befehl *Logging-Sätze löschen*).

Wenn Bedarf an einer lückenlosen Dokumentation über einen längeren Zeitraum hinweg besteht, sollten Sie von Zeit zu Zeit die Logging-Sätze aus der aktuellen Logging-Datei oder aus der/den Offline-Logging-Datei(en) sichern (z.B. als Datei, auf CD oder DVD). Dazu leiten Sie die Ausgabe von *ftshwl* in eine Datei um und löschen anschließend diese Logging-Sätze bzw. Offline-Logging-Dateien:

- Wenn Sie aktuelle Logging-Sätze sichern möchten, rufen Sie *ftshwl* ohne Angabe von *-lf*, *-tlf* oder *-plf* auf. Wählen Sie dabei die Logging-Sätze aus, die Sie sichern möchten. Entfernen Sie anschließend diese Logging-Sätze aus der aktuellen Logging-Datei, indem Sie *ftdell* mit passenden Auswahlkriterien aufrufen.
- Wenn Sie Offline-Logging-Sätze sichern möchten, rufen Sie *ftshwl -nb=@a* mit Angabe von *-lf*, *-tlf* oder *-plf* auf. Mit diesen Optionen wählen Sie die Offline-Logging-Dateien aus. Anschließend löschen Sie diese Logging-Datei(en), indem Sie *ftdell* mit der Option *-tlf* aufrufen.

Dadurch bleiben zum einen die Logging-Sätze für eine lückenlose Dokumentation über einen längeren Zeitraum erhalten, zum anderen wird die aktuelle Logging-Datei nicht überflüssig groß, was zu entsprechend langen Zugriffszeiten führen würde.

Beim Löschen von Logging-Sätzen ändert sich die Größe der Datei, da der Speicherplatz beim Löschen sofort freigegeben wird.

3.12 FTAC-Umgebung verwalten

Unter FTAC-Umgebung versteht man die auf Ihrem System vorhandenen Berechtigungssätze und Berechtigungsprofile.

3.12.1 Berechtigungssätze verwalten

Als FTAC-Verwalter legen Sie den Standardberechtigungssatz fest und können für alle Benutzer des Systems Berechtigungssätze ansehen, ändern und löschen.

Zusätzlich hat der FTAC-Verwalter auch die Aufgabe, erstmalig den ADM-Verwalter festzulegen, indem er im Berechtigungssatz des ADM-Verwalters das ADM-Privileg setzt (siehe Abschnitt „ADM-Verwalter festlegen“ auf Seite 121).

Standardberechtigungssatz

Der Standardberechtigungssatz ist die Vorgabe für alle Benutzerkennungen. Der Benutzer darf diese Vorgabe für seinen Berechtigungssatz weiter einschränken.

Über die Vorgaben des Standardberechtigungssatzes kann sich ein Benutzer jedoch nur dann hinwegsetzen,
– wenn Sie als FTAC-Verwalter seinen Berechtigungssatz entsprechend ändern,
– oder wenn Sie ihm ein privilegiertes Berechtigungsprofil einrichten.

Nach einer Erstinstallation oder einer Vollinstallation von openFT ist der Standardberechtigungssatz so eingestellt, dass File Transfer uneingeschränkt möglich ist. Als FTAC-Verwalter sollten Sie daher den Standardberechtigungssatz umgehend dem Schutzbedürfnis des Rechners anpassen.

Berechtigungssätze ansehen und ändern

Berechtigungssätze können Sie sich mit dem Kommando *ftshwa* ansehen. Die Vorgaben des FTAC-Verwalters sind dort unter MAX-ADM-LEVELS aufgeführt, die Vorgaben des Benutzers unter MAX-USER-LEVELS. Gültig ist der jeweils kleinere Wert.

Sie können sich die Berechtigungssätze auch über den openFT Explorer ansehen, indem Sie auf das Objekt *Berechtigungssätze* klicken. Eine detaillierte Beschreibung zu den einzelnen Funktionen finden Sie in der Online-Hilfe.

Für jeden Benutzer gelten zunächst einmal die Einstellungen des Standardberechtigungssatzes. Als FTAC-Verwalter können Sie für jeden Benutzer im System einen individuellen Berechtigungssatz vergeben oder einen gegebenen Berechtigungssatz modifizieren. Dazu steht Ihnen das Kommando *ftmoda* zur Verfügung.

Berechtigungssätze sinnvoll einsetzen

Die im Berechtigungssatz festgelegte Berechtigung wird bei einem openFT-Auftrag (Outbound und Inbound) mit der FTAC-Sicherheitsstufe des jeweiligen Partners verglichen, siehe auch Seite 71.

Um den Rechner vor Einbruchversuchen zu schützen, sollten Sie für alle administrationsberechtigten Kennungen die Inbound-Eigenschaften im Berechtigungssatz stets so restriktiv wie möglich einstellen, d.h. zumindest die Inbound-Verarbeitung verbieten.

1. Für einen sicheren Betrieb sollten Sie im Standardberechtigungssatz alle Inbound-Berechtigungen verbieten, z.B. mit dem Kommando:

   ```
   ftmoda @s -os=100 -or=100 -is=0 -ir=0 -if=0 -ip=0
   ```

2. Für jeden Benutzer, zu dem Inbound Aufträge durchgeführt werden dürfen, setzen Sie als FTAC-Verwalter alle Parameter des entsprechenden Berechtigungssatzes auf 100.
3. Anschließend sollte jeder Benutzer seine Inbound-Werte auf 0 ändern. Er hat dann die Möglichkeit, über Profile und "ignore ... level" jeden gewünschten Zugriffsmodus zuzulassen. Inbound Aufträge, deren zugehörige Berechtigungslevel auf 0 stehen, sind nur noch über FTAC-Zugangsberechtigung, jedoch nicht mehr über Login und Passwort möglich.

Zusätzlich gibt es die Möglichkeit,

– partnerspezifische Sicherheitsstufen zu vergeben, siehe Seite 71

– und openFT-Partner einer gesicherten Identitätsprüfung mit kryptografischen Mitteln zu unterziehen (siehe Abschnitt „Authentifizierung“ auf Seite 78).

Zusätzliche Sicherheit bringt auch die Verwendung eines Dateinamen-Präfix im Berechtigungsprofil. Dadurch kann der Wechsel in ein übergeordnetes Verzeichnis ausgeschlossen werden.

Wichtig

Wenn Sie hohe Sicherheitsansprüche haben, sind diese Maßnahmen nur dann wirklich sinnvoll, wenn keine anderen Netzwerkzugänge möglich sind, mit denen die Schutzmechanismen umgangen werden können. D.h. insbesondere, dass TCP/IP-Dienste wie *ftp*, *tftp* nicht aktiv sein dürfen.

3.12.2 Berechtigungsprofile verwalten

Als FTAC-Verwalter können Sie für jeden Benutzer im Rechner Berechtigungsprofile anlegen und bearbeiten. Der FTAC-Verwalter ist der einzige, der Berechtigungsprofile auch privilegieren kann.

Berechtigungsprofile anlegen

Berechtigungsprofile legen Sie mit dem Kommando *ftcrep* an. Wenn Sie dabei für eine andere Kennung gleich eine Zugangsberechtigung vergeben möchten, müssen Sie als FTAC-Verwalter entweder FT-Verwalterrechte besitzen oder das Passwort für die jeweilige Benutzerkennung angeben. Ohne FT-Verwalterrechte oder Angabe des Passworts wird das Profil ohne Zugangsberechtigung angelegt; diese muss der Benutzer später selber vergeben.

Beim Anlegen können Sie das Profil privilegieren.

Sie können neue Berechtigungsprofile auch über den openFT Explorer anlegen, indem Sie das Dialogfenster *Berechtigungsprofil* über das Menü *Datei/Neu*, öffnen. Eine detaillierte Beschreibung zu einzelnen Funktionen finden Sie in der Online-Hilfe.

Berechtigungsprofile ansehen und ändern

Mit dem Kommando *ftshwp* können Sie sich Berechtigungsprofile aller Benutzer ansehen. Die Zugangsberechtigung eines Profils wird nicht ausgegeben, d.h. durch Ihre Verwaltereigenschaft bekommen Sie keine Zugriffsrechte auf Dateien fremder Benutzerkennungen.

Sie können sich die Berechtigungsprofile auch über den openFT Explorer ansehen, indem Sie auf das Objekt *Berechtigungsprofile* klicken. Ebenso können Sie Berechtigungsprofile im Dialogfenster *Berechtigungsprofil* ändern. Eine detaillierte Beschreibung zu den einzelnen Funktionen finden Sie in der Online-Hilfe.

Mit dem Kommando *ftmodp* können Sie insbesondere folgende Änderungen an einem Berechtigungsprofil vornehmen:

– privilegieren oder eine Privilegierung zurücknehmen
– die Zugangsberechtigung eines Profils ändern, das einer anderen Benutzerkennung gehört. Dazu müssen Sie FT-Verwalterrechte haben oder Ihnen muss das Passwort des Profileigentümers bekannt sein.
– das Profil einer anderen Benutzerkennung zuordnen

Wenn der FTAC-Verwalter nicht über die FT-Verwalterrechte verfügt, oder das Passwort des Profileigentümers mit angibt, wird das Profil nach einer solchen Änderung gesperrt. Der Profileigentümer muss die Änderung quittieren, indem er das Profil entsperrt, z.B. mit dem Kommando *ftmodp ... -v=y*.
Ist das Berechtigungsprofil privat (*-u=pr*, siehe Abschnitt „ftcrep - Berechtigungsprofil anlegen“ auf Seite 193) und wird eine zugehörige Zugangsberechtigung zum zweiten Mal vergeben, dann wird die schon vorhandene Zugangsberechtigung gesperrt.

Berechtigungsprofil sperren/entsperren

Es gibt folgende zwei Arten von Sperren:

- Die Sperre ist eine auf "ungültig" gesetzte Zugangsberechtigung.

  Hierfür gibt es vier verschiedene Ursachen:

  – Die Sperre wird explizit mit *-v=n* gesetzt.

  – Der FTAC-Verwalter ändert die Eigenschaften eines Profils, das ihm nicht gehört.

  – Der FTAC-Verwalter importiert Profile, die ihm nicht gehören.

  – Die Zugangsberechtigung eines privaten Profils (*-u=pr*) wird zufällig – oder böswillig – "entdeckt".

  Um die Sperre aufzuheben, setzen Sie die Zugangsberechtigung auf gültig (*-v=y*).

- Das Ablaufdatum eines Profils ist abgelaufen.

  Um die Sperre aufzuheben, setzen Sie das Ablaufdatum in die Zukunft oder löschen es.

Berechtigungsprofile löschen

Berechtigungsprofile eines Benutzers löschen Sie mit dem Kommando *ftdelp*. Diese Funktion ist z.B. notwendig, nachdem eine Benutzerkennung gelöscht wurde, da mit dem Löschen der Kennung nicht automatisch die Profile mit gelöscht werden. Wenn Sie Profile von aktiven Kennungen löschen, sollten Sie dies erst nach Rücksprache mit dem Benutzer tun.

Sie können Berechtigungsprofile auch über den openFT Explorer löschen, indem Sie über das Kontextmenü den Befehl *Löschen* auswählen. Eine detaillierte Beschreibung zu den Objektfenstern finden Sie in der Online-Hilfe.

Berechtigungsprofile privilegieren

Ein privilegiertes Berechtigungsprofil ist für Ausnahmefälle gedacht, bei denen es notwendig ist, dass sich ein Benutzer über Vorgaben hinwegsetzen kann. Ein Profil privilegieren Sie z.B. durch das Kommando *ftmodp ... -priv=y*.

Ist ein Profil einmal privilegiert, kann der Profil-Eigentümer nur noch die Zugangsberechtigung ändern und die Privilegierung wieder zurücknehmen. Andere Änderungen sind nicht mehr erlaubt, um Missbrauch auszuschließen.

Sie können die Berechtigungsprofile auch über den openFT Explorer im Dialogfenster *Berechtigungsprofil* privilegieren. Eine detaillierte Beschreibung zu den einzelnen Funktionen finden Sie in der Online-Hilfe.

3.12.3 FTAC-Umgebung sichern

Beim Umzug von einzelnen Benutzern auf einen anderen Rechner oder beim Umzug des kompletten Rechners ist es durch Sichern und Wiedereinspielen der Berechtigungssätze und -profile möglich, den Benutzern auf dem neuen Rechner die gleiche FTAC-Umgebung zur Verfügung zu stellen. Außerdem können Sie damit Sicherungskopien der FTAC-Umgebung des Rechners erstellen.

Berechtigungssätze und -profile sichern

Zum Sichern verwenden Sie das Kommando *ftexpe*. Dabei können Sie differenzieren, ob und welche Berechtigungssätze und -profile für welche Benutzer Sie sichern wollen. Den Namen der Sicherungsdatei müssen Sie angeben.

In allen Fällen wird der Standardberechtigungssatz nicht mitgesichert. Dadurch werden alle Werte eines Berechtigungssatzes, die sich auf den Standardberechtigungssatz beziehen (bei Ausgabe mit einem Stern (*) gekennzeichnet), als Variable gesichert. D.h. sie erhalten beim Wiedereinspielen den Wert des dann gültigen Standardberechtigungssatzes.

Sie können die Berechtigungssätze und -profile auch über den openFT Explorer sichern, indem Sie im Menü *Administration* den Befehl *FTAC-Umgebung exportieren* auswählen. Eine detaillierte Beschreibung dazu finden Sie in der Online-Hilfe.

Gesicherte Berechtigungssätze und -profile ansehen

Gesicherte Berechtigungssätze und -profile können Sie sich mit dem Kommando *ftshwe* ansehen, wobei Sie den Namen der Sicherungsdatei angeben müssen.

Gesicherte Berechtigungssätze und -profile können Sie sich auch über den openFT Explorer ansehen, indem Sie die Exportdatei in das Verzeichnis *Exportierte Berechtigungen* ziehen, oder den Befehl *Exportdatei öffnen...* aus dem Kontextmenü des Objekts *Exportierte Berechtigungen* aufrufen.

Gesicherte Berechtigungssätze und -profile einspielen

Mit dem Kommando *ftimpe* können Sie gesicherte Berechtigungssätze und -profile wieder einspielen. Dabei können Sie nach Sätzen, Profilen und Kennungen differenzieren, d.h. Sie müssen nicht den kompletten Sicherungsstand übernehmen. Beachten Sie bitte, dass die Werte, die sich auf den Standardberechtigungssatz beziehen, immer den Wert des aktuell gültigen Standardberechtigungssatzes zugeordnet bekommen.

Haben Sie als FTAC-Verwalter die FT-Verwalterrechte, so sind eingespielte Berechtigungsprofile sofort mit dem beim Export eingestellten Status verfügbar. Haben Sie keine FT-Verwalterrechte, so sind eingespielte Profile für alle Benutzerkennungen zunächst gesperrt.

Sie können die Berechtigungssätze und -profile auch über den openFT Explorer einspielen, indem Sie im Menü *Administration* den Befehl *FTAC-Umgebung importieren* auswählen. Eine detaillierte Beschreibung dazu finden Sie in der Online-Hilfe.

3.13 openFT-Instanzen und Cluster-Betrieb

Mit openFT haben Sie die Möglichkeit, mehrere openFT-Instanzen auf einem Rechner gleichzeitig laufen zu lassen. Durch diese Instanzen ist man in der Lage, bei einem Rechnerausfall die Funktionalität des openFT auf einen anderen Rechner umzuschalten, auf dem bereits ein openFT läuft. Beispiele zum Einsatz von openFT in einem Unix-Cluster finden Sie im Anhang.

Voraussetzung ist, dass openFT nur das Transportsystem TCP/IP verwendet. Andere Transportsysteme werden im Cluster nicht unterstützt und dürfen auch nicht im TNS konfiguriert sein. Deshalb wird empfohlen ohne TNS und CMX zu arbeiten. Wenn Sie ohne CMX arbeiten, arbeiten Sie auch automatisch ohne TNS. In einem Cluster muss auf allen Rechnern dieselbe openFT-Version eingesetzt werden.

Auf Systemen ohne TCP/IP gibt es jeweils nur die sogenannte Standardinstanz.

openFT-Kommandos, die in einer Vor-, Nach- oder Folgeverarbeitung aufgerufen werden, laufen unter der gleichen Instanz ab, wie der Auftrag, der die Vor-, Nach- oder Folgeverarbeitung initiiert hat.

Falls Sie openFT über SNMP administrieren, beachten Sie bitte bei der Cluster-Umschaltung, dass SNMP nur mit einer Instanz zusammenarbeiten kann.
Es ist entscheidend, welche Instanz beim Start des Agenten eingestellt ist (siehe dazu Kapitel „openFT über SNMP administrieren“ auf Seite 105).

Kommandos zum Verwalten von Instanzen

Als FT-Verwalter können Sie Instanzen erzeugen, modifizieren und löschen. Außerdem können Sie Instanzen einstellen und sich über Instanzen informieren.

- Erzeugen bzw. Aktivieren einer Instanz

  Mit dem Kommando *ftcrei* können Sie eine Instanz neu erzeugen bzw. eine deaktivierte Instanz wieder aktivieren (zuschalten).

  Beim Erzeugen einer Instanz werden die Betriebsparameter, die Profildateien und die Startup- und Shutdown-Datei wie bei einer Neuinstallation initialisiert.

  Beim Aktivieren einer vorhandenen Instanz wird der vorhandene Instanzdateibaum mit den Betriebsmitteln der Instanz in das Verzeichnis */var/openFT* gelinkt.

  Wenn Sie eine neue Instanz erzeugen und die Standardinstanz *std* weiter verwenden möchten, dann müssen Sie der Standardinstanz eine eigene Adresse zuweisen, um Adresskollisionen zu vermeiden.

- Modifizieren einer Instanz

  Mit dem Kommando *ftmodi* können Sie einer Instanz einen anderen Internet-Hostnamen zuordnen.

  Bitte beachten Sie:
  Wenn Sie der Standardinstanz *std* einen Hostnamen zuordnen, dann sind lokale Aufträge an die z.B. zu Testzwecken verwendete Adresse 127.0.0.1 nicht mehr möglich.

- Deaktivieren einer Instanz

  Mit dem Kommando *ftdeli* können Sie eine Instanz deaktivieren. Das Deaktivieren einer Instanz entfernt ausschließlich den symbolischen Link im lokalen */var/openFT* Verzeichnis. Der Instanzdateibaum wird nicht verändert.

- Einstellen einer Instanz

  Mit dem Kommando *ftseti* können Sie die openFT-Instanz auswählen, mit der Sie arbeiten möchten.

  Das Kommando setzt die Umgebungsvariable OPENFTINSTANCE auf den Instanznamen.

  Sie können die Instanz auch über den openFT Explorer einstellen. Sobald mehrere Instanzen vorhanden sind, erscheint in der Symbolleiste des openFT Explorer ein Listenfeld zur Auswahl der Instanz.

  Das Listenfeld wird nur angezeigt wenn die Instanz beim Start des openFT Explorers bereits vorhanden ist.
  Wird die Instanz nach dem Start des openFT Explorers erzeugt, dann muss der dieser neu gestartet werden.

- Ausgabe von Informationen über Instanzen

  Mit dem Kommando *ftshwi* können Sie Informationen über die Instanzen abfragen.

- Aktualisieren eines Instanzdateibaums

  Mit dem Kommando *ftupdi* können Sie den Instanzdateibaum einer älteren openFT-Version für den Einsatz in der aktuellen Version modifizieren. Das ist nur für Instanzen nötig, die zum Zeitpunkt einer Update-Installation nicht aktiv waren.

Wenn Sie mit mehreren Instanzen arbeiten, dann ist für jede der Instanzen im gegebenen Fall ein eigener Aufruf *ftalarm* erforderlich (siehe dazu Abschnitt „ftalarm - fehlgeschlagene Aufträge melden“ auf Seite 186).

Eine detaillierte Beschreibung zu den Kommandos *ftcrei*, *ftmodi*, *ftupdi* und *ftdeli* finden Sie unter Kapitel „openFT-Kommandos für den Verwalter“ ab Seite 163. Die Kommandos *ftseti* und *ftshwi* sind im Benutzerhandbuch zu „openFT für Unix-Systeme“ beschrieben.

Startup- und Shutdown-Datei

In openFT auf Linux, HP-UX und AIX gibt es eine instanzenübergreifende Startup- und Shutdown-Datei. Außerdem hat jede vorhandene Instanz eine eigene Startup- und Shutdown-Datei.

Beim Systemstart / Shutdown wird die instanzenübergreifende Startup- und Shutdown-Datei aufgerufen. Diese ruft wiederum die Startup- und Shutdown-Dateien aller openFT-Instanzen auf.

- Instanzenübergreifende Startup- und Shutdown-Datei:

  Sie wird unter */etc/init.d* (Linux) bzw. einem entsprechenden Verzeichnis auf anderen Unix-Plattformen bei der Installation von openFT eingerichtet. Diese Startup- und Shutdown-Datei ruft beim Systemstart bzw. beim Herunterfahren des Systems die Startup- und Shutdown-Dateien aller Instanzen auf.

- Instanzenspezifische Startup- und Shutdown-Datei:

  Bei der Installation von openFT wird für die Instanz *std* im Verzeichnis */var/openFT/std/etcinit* die Startup- und Shutdown-Datei *openFTinst* angelegt.

  Wenn Sie mit *ftcrei* eine weitere Instanz erzeugen, dann wird für diese Instanz ebenfalls eine Startup- und Shutdown-Datei *openFTinst* eingerichtet. Diese Datei befindet sich im Verzeichnis *etcinit* des openFT-Instanzenbaums.

  Auf Solaris erfolgt der automatische Start/Stopp über Manifeste. Für jede Instanz wird automatisch ein Manifest erzeugt.

3.14 Diagnose

Zur Unterstützung der Fehlerdiagnose können Sie einen Überwachungszustand (Trace) ein- und ausschalten, Trace-Dateien aufbereiten und Diagnoseinformationen ausgeben. Diese Funktionen sind in erster Linie für den Kundendienst von Fujitsu Technology Solutions vorgesehen.

Überwachungszustand ein/ausschalten

Den Überwachungszustand schalten Sie mit dem FT-Kommando *ftmodo* oder über den openFT Explorer ein und aus (im Dialog *Betriebsparameter - Überwachung* aus dem Menü *Administration)*. Bei eingeschaltetem Überwachungszustand werden die Diagnosedaten in Trace-Dateien geschrieben, die zur weiteren Auswertung aufbereitet werden müssen.

Trace-Dateien aufbereiten

Die Trace-Dateien befinden sich im Dateiverzeichnis *traces* der jeweiligen openFT-Instanz, siehe „Instanzenverzeichnis“ auf Seite 26. Bei der Standardinstanz lautet der Pfadname */var/openFT/std/traces*.

Trace-Dateien können Sie über den openFT Explorer ansehen:

– für lokale Instanzen mit dem Befehl *Trace-Datei öffnen* aus dem Menü *Administration*,

– für fernadministrierte Instanzen über das Objektverzeichnis *Traces* der betreffenden Instanz.

Weitere Möglichkeit: Navigieren Sie im openFT Explorer auf das Verzeichnis *traces* und öffnen Sie im Objektfenster eine Trace-Datei per Kontextmenü-Befehl *Ansehen*. Eine detaillierte Beschreibung zu den einzelnen Funktionen finden Sie in der Online-Hilfe.

Diagnosesätze ausgeben

Diagnosesätze werden im Gegensatz zu Trace-Dateien nur geschrieben, wenn ein Fehler aufgetreten ist. Sie können sich diese Diagnosesätze über das Kommando *ftshwd* ausgeben lassen.

Im openFT Explorer können Sie sich die Diagnosesätze mit dem Befehl *Diagnoseinformationen anzeigen* im Menü *Administration* ausgeben lassen.

Meldungsdatei für Konsolkommandos

Konsolausgaben kommen auf die Unix-Konsole. Zur Verfolgung über einen längeren Zeitraum werden diese von openFT erzeugten Konsolausgaben zusätzlich auch in die *conslog*-Datei geschrieben. *conslog* liegt im Verzeichnis *log* der jeweiligen openFT-Instanz, siehe „Instanzenverzeichnis“ auf Seite 26. Bei der Standardinstanz lautet der Pfadname */var/openFT/std/log/conslog*.

Im openFT Explorer können Sie sich die Meldungen mit dem Befehl *Konsolmeldungen anzeigen* im Menü *Administration* ausgeben lassen.

3.15 Konfigurationsdaten sichern und wiederherstellen

Sie sollten die Konfigurationsdaten Ihrer openFT-Instanz in regelmäßigen Abständen sichern. Dadurch ist gewährleistet, dass Sie den openFT-Betrieb z.B. nach einem Ausfall oder Austausch eines Rechners in kurzer Zeit wieder mit der ursprünglichen Ablaufumgebung aufnehmen können.

Sie sollten auf jeden Fall die Partnerliste, die FTAC-Umgebung und die Betriebsparameter-Einstellungen in Sicherungsdateien speichern. Dazu können Sie wie folgt vorgehen (die Dateinamen sind beispielhaft):

- Sichern Sie die Partnerliste mit folgendem Kommando:

  ```
  ftshwptn -px > partner_save
  ```

  Die Datei *partner_save* enthält *ftmodptn*-Kommandos.

  Zum Wiederherstellen der Partnerliste führen Sie die Datei einfach aus.

- Sichern Sie die FTAC-Umgebung (Berechtigungssätze und -profile) mit folgendem Kommando:

  ```
  ftexpe ftac_save
  ```

  Zum Wiederherstellen der FTAC-Umgebung importieren Sie die Datei mit dem Kommando `ftimpe ftac_save`.

- Sichern Sie die Betriebsparameter-Einstellungen mit folgendem Kommando:

  ```
  ftshwo -px > option_save
  ```

  Die Datei *option_save* enthält ein *ftmodo*-Kommando.

  Zum Wiederherstellen der Betriebsparameter-Einstellungen führen Sie die Datei einfach aus.

- Sichern Sie gegebenenfalls die Konfigurationsdatei der zentralen Administration.

  ```
  ftexpc remadmin_cfg_save.xml
  ```

4 openFT über SNMP administrieren

Damit openFT über SNMP administriert werden kann, muss auf Ihrem Rechner ein EMANATE-Master-Agent vorhanden sein.

Der openFT-Subagent ist auf den Plattformen Solaris/Sparc und HP-UX verfügbar. Er ist in openFT enthalten und wird während der Installation von openFT eingerichtet.

4.1 Tätigkeiten nach der Installation

Nach der Installation von openFT sind verschiedene Tätigkeiten erforderlich:

1. Wird Ihr Rechner noch nicht über SNMP administriert, müssen Sie die Administration über SNMP aktivieren.

   Sie benötigen für die Administration von openFT über den openFT-Subagenten einen Community String mit Schreibberechtigung. Falls Sie als Zugriffsrecht nur *read* vergeben, können über SNMP nur Informationen ausgegeben werden. Das Ändern von Werten (auch Starten bzw. Stoppen) ist dann nicht möglich (siehe auch Seite 107).

   Sehen Sie bitte in Ihrer plattformspezifischen Dokumentation nach, wie Sie die SNMP-Administration aktivieren können.

2. Starten Sie den Agenten (siehe nächste Seite)

Die Tätigkeiten des SNMP-Administrators müssen der Dokumentation der eingesetzten Management-Station entnommen werden.

Die Sicherheitsmechanismen entnehmen Sie bitte ebenfalls Ihrer SNMP-Dokumentation.

4.2 openFT-Subagenten starten

Es gibt folgende Möglichkeiten, den openFT-Subagenten zu starten:

- Geben Sie `/opt/bin/ftagt &` ein.

  Der openFT-Subagent wird dann gestartet und bleibt bis zum Herunterfahren des Rechners aktiv.

- Auf Solaris können Sie den openFT-Subagenten via SMF automatisch starten, siehe Abschnitt „Solaris SMF“ auf Seite 41.

- Auf HP-UX entfernen Sie das Kommentarzeichen in der Zeile der Startup-Datei, in der *ftagt* steht (z.B.: */var/openFT/std/etcinit/openFTinst*) sowie in der entsprechenden Zeile in der Startup-Datei weiterer Instanzen. Dann wird der openFT-Subagent bei jedem Hochfahren des Systems mitgestartet.
  Falls Sie den openFT-Subagenten beenden wollen, können Sie das mit einem *kill -2* auf die Prozessnummer des openFT-Subagenten tun.

Bitte beachten Sie bei der Cluster-Umschaltung, dass SNMP nur mit einer Instanz zusammenarbeiten kann.
Es ist entscheidend, welche Instanz beim Start des Agenten eingestellt ist (siehe dazu Abschnitt „openFT-Instanzen und Cluster-Betrieb“ auf Seite 98).

4.3 SNMP-Management für openFT

Der openFT-Subagent dient

- zur Information über den Status des asynchronen openFT-Servers
- zum Starten und Stoppen des asynchronen openFT-Servers
- zur Informationsbeschaffung über Systemparameter
- zum Ändern von Systemparametern
- zum neu Erzeugen des Public-Key zur Verschlüsselung/Authentifizierung
- zur Ausgabe von Statistikdaten
- zur Steuerung der Diagnose

Die MIB (Management Information Base) zu openFT bietet Objekte zu den oben genannten Management-Aufgaben. Sie befindet sich in der Datei */opt/openFT/snmp/openFT.asn1*.

Die Objekte zum Starten und Stoppen, zur Verschlüsselung des Public-Key, zum Ändern von Systemparametern und zur Steuerung der Diagnose setzen schreibende Zugriffe voraus.

4.3.1 Starten und Stoppen von openFT

MIB-Definition

Objektname/Objekt Identifier	Zugriff	Bedeutung
ftStartandStop/ 1.3.6.1.4.1.231.2.18.1.1.0	read-write	openFT Protokoll

Eingabe

Syntax	Integer	Bedeutung
start stop	1 2	der asynchrone openFT-Server wird gestartet der asynchrone openFT-Server wird gestoppt

Ausgabe

Syntax	Integer	Bedeutung
on off	3 4	der asynchrone openFT-Server ist gestartet der asynchrone openFT-Server ist gestoppt

Mit Setzen der Werte "start" bzw. "stop" wird durch den openFT-Subagenten das Starten bzw. Stoppen des asynchronen openFT-Servers veranlasst. Ein lesender Zugriff liefert Informationen über den aktuellen Zustand des openFT-Systems ("on" bzw. "off").

4.3.2 Systemparameter

MIB-Definition

Objektname/ Objekt Identifier	**Zugriff**	**Bedeutung**	**Kommando *ftmodo***
ftSysparVersion/ 1.3.6.1.4.1.231.2.18.2.1.0	read-only	Version	
ftSysparTransportUnitSize/ 1.3.6.1.4.1.231.2.18.2.2.0	read-write	Transport Unit Size	*-tu*
ftSysparMaxOSP/ 1.3.6.1.4.1.231.2.18.2.7.0	read-write	Max OSP[1]	*-cl*
ftSysparMaxISP/ 1.3.6.1.4.1.231.2.18.2.8.0	read-write	Max ISP[1]	*-cl*
ftSysparProcessorName/ 1.3.6.1.4.1.231.2.18.2.9.0	read-write	Processor Name	*-p*
ftSysparStationName/ 1.3.6.1.4.1.231.2.18.2.10.0	read-write	Station Name	*-l*
ftSysparCode/ 1.3.6.1.4.1.231.2.18.2.11.0	read-write	Code Table Folgende Werte werden unterstützt: iso8859-1 (1), iso8859-2 (2), iso8859-5 (5), iso8859-6 (6), iso8859-7 (7), iso8859-9 (9), undefined (255)	*-ccs*
ftSysparMaxInboundReqs/ 1.3.6.1.4.1.231.2.18.2.12.0	read-write	Max Inbound Requests	*-rql*
ftSysparMaxLifeTime/ 1.3.6.1.4.1.231.2.18.2.13.0	read-write	Max Life Time	*-rqt*

[1] Die Unterscheidung zwischen *Max OSP* (maximale Anzahl paralleler Outbound-Verbindungen) und *Max ISP* (maximale Anzahl paralleler Inbound-Verbindungen) wird ab openFT V11 nicht mehr unterstützt. Beide Werte korrespondieren mit dem Parameter *-cl* (Verbindungslimit) des Kommandos *ftmodo* nach der Formel *Max OSP = Max ISP = Verbindungslimit*2/3* (auf ganzzahlige Werte gerundet).

Die Erklärung der möglichen Werte finden Sie beim Kommando *ftmodo* ab Seite 236.

4.3.3 Statistikinformationen

MIB-Definition

Objektname/Objekt Identifier	Zugriff	Bedeutung
ftStatSuspend/1.3.6.1.4.1.231.2.18.4.1.0	read-only	Aufträge im Status SUSPEND
ftStatLocked/1.3.6.1.4.1.231.2.18.4.2.0	read-only	Aufträge im Status LOCKED
ftStatWait/1.3.6.1.4.1.231.2.18.4.3.0	read-only	Aufträge im Status WAIT
ftStatActive/1.3.6.1.4.1.231.2.18.4.4.0	read-only	Aufträge im Status ACTIVE
ftStatCancelled/1.3.6.1.4.1.231.2.18.4.5.0	read-only	Aufträge im Status CANCELLED
ftStatFinished/1.3.6.1.4.1.231.2.18.4.6.0	read-only	Aufträge im Status FINISHED
ftStatHold/1.3.6.1.4.1.231.2.18.4.7.0	read-only	Aufträge im Status HOLD
ftStatLocalReqs/1.3.6.1.4.1.231.2.18.4.8.0	read-only	lokale Aufträge
ftStatRemoteReqs/1.3.6.1.4.1.231.2.18.4.9.0	read-only	ferne Aufträge

Die einzelnen Status haben folgende Bedeutung:

SUSPEND
Der Auftrag wurde unterbrochen.

LOCKED
Der Auftrag ist für einen gewissen Zeitraum von der Bearbeitung ausgeschlossen. Dieser Zustand kann sowohl bei openFT- als auch bei FTAM-Partnern auftreten.
Bei openFT-Partnern, z.B. wenn ein Betriebsmittelengpass vorliegt oder wenn externe Datenträger erst noch verfügbar gemacht werden müssen.
Bei FTAM-Partnern, wenn einer der Partner über das FTAM-Protokoll eine Wartezeit bis zum nächsten Start- oder Recovery-Versuch vorschlägt, die über der normalerweise vorgesehenen Verzögerung liegt.

WAIT
Der Auftrag wartet.

ACTIVE
Der Auftrag wird gerade bearbeitet.

CANCELLED
Der Auftrag wurde im lokalen System gelöscht. Er ist aber im fernen System schon bekannt, weil z.B. der Auftrag schon einmal aktiv war. Deshalb kann der Auftrag erst nach erneutem Verbindungsaufbau zum Partner aus dem Auftragsbuch entfernt werden.

FINISHED
Dieser Zustand kommt bei Aufträgen mit FTAM-Partnern vor, wenn der Auftrag beendet oder abgebrochen wurde, aber der Benutzer noch nicht über das Ende des Auftrags informiert wurde.

HOLD
Der bei der Auftragserteilung angegebene Startzeitpunkt ist noch nicht erreicht.

4.3.4 Steuerung der Diagnose

MIB-Definition

Objektname/Objekt Identifier	Zugriff	Bedeutung
ftDiagStatus/1.3.6.1.4.1.231.2.18.5.1.0	read-write	Diagnose Management

Eingabe

Syntax	Integer	Bedeutung
off	1	Diagnose Management wird ausgeschaltet
on	18	Diagnose Management wird eingeschaltet

Mit Setzen der Werte "on" bzw. "off" wird durch den openFT-Subagenten das Starten bzw. Stoppen des Diagnose Managements (Trace) veranlasst. Ein lesender Zugriff liefert Informationen über den aktuellen Zustand des Diagnose Managements (ein- oder ausgeschaltet).

4.3.5 Public Key zur Verschlüsselung

MIB-Definition

Objektname/Objekt Identifier	Zugriff	Bedeutung
ftEncryptKey/1.3.6.1.4.1.231.2.18.3.1.0	write-only	public key

Eingabe

Syntax	Integer	Bedeutung
create-new-key	1	Es wird ein neuer public key erzeugt.

Eine detaillierte Beschreibung zum Erzeugen und Verwalten von öffentlichen und privaten Schlüsseln finden Sie im Abschnitt „Lokale RSA-Schlüsselpaare erzeugen und verwalten“ auf Seite 81.

5 Zentrale Administration

Die zentrale Administration von openFT umfasst die Funktionen **Fernadministration** und **ADM-Traps**. openFT für Unix-Systeme unterstützt beide Funktionen in vollem Umfang.

Diese Funktionen bieten im Vergleich zu openFT bis V10.0 erhebliche Vorteile, die insbesondere dann zum Tragen kommen, wenn Sie eine größere Anzahl von openFT-Instanzen administrieren und überwachen möchten, z.B.:

- Einfaches Konfigurieren

  Die Konfigurationsdaten werden zentral auf dem **Fernadministrations-Server** gehalten und sind dadurch nur einmal vorhanden. Rollenbildung in Form von **Fernadministratoren** und Gruppierung mehrerer Instanzen erlauben es, auch komplexe Konfigurationen einfach und übersichtlich zu realisieren. Spätere Änderungen sind leicht einzubringen und machen die Konfiguration damit wartungsfreundlich.

  Der Fernadministrations-Server läuft auf einem Unix- oder Windows-System.

- Einfacheres Authentifizierungsverfahren

  Wenn Sie aus Sicherheitsgründen mit Authentifizierung arbeiten möchten, dann müssen nur wenige öffentliche Schlüssel verteilt werden:

  – Für die Strecke zum Fernadministrations-Server müssen die Schlüssel der Rechner, von denen aus administriert werden soll, auf dem Fernadministrations-Server hinterlegt werden.

  – Für die Strecke vom Fernadministrations-Server zu den zu administrierenden Instanzen muss nur der öffentliche Schlüssel des Fernadministrations-Servers auf den zu administrierenden openFT-Instanzen hinterlegt werden.

- Hohe Leistungsfähigkeit

  Die Fernadministrations-Schnittstelle ermöglicht wesentlich längere Kommando-Sequenzen als in openFT bis V10.0.

  Außerdem kann der Fernadministrations-Server so konfiguriert werden, dass er ausschließlich für die zentrale Administration zur Verfügung steht. In diesem Falle gibt es keine Abhängigkeiten zum normalen FT-Betrieb und damit auch keine gegenseitige Beeinträchtigung.

- Einfaches Administrieren

  Fernadministratoren benötigen nur eine (zentrale) Zugangsberechtigung. Bis zur openFT V10 mussten sich die Fernadministratoren die Zugangsdaten von jeder zu administrierenden openFT-Instanz merken.

- Zentrale Protokollierung wichtiger Ereignisse

  Bei bestimmten Ereignissen auf openFT-Instanzen können ADM-Traps erzeugt werden, die an den (zentralen) ADM-Trap-Server geschickt und dort dauerhaft gespeichert werden. Damit haben Fernadministratoren die Möglichkeit, wichtige Ereignisse auch nachträglich und instanzspezifisch auszuwerten.

- Kompatible Integration früherer openFT-Versionen

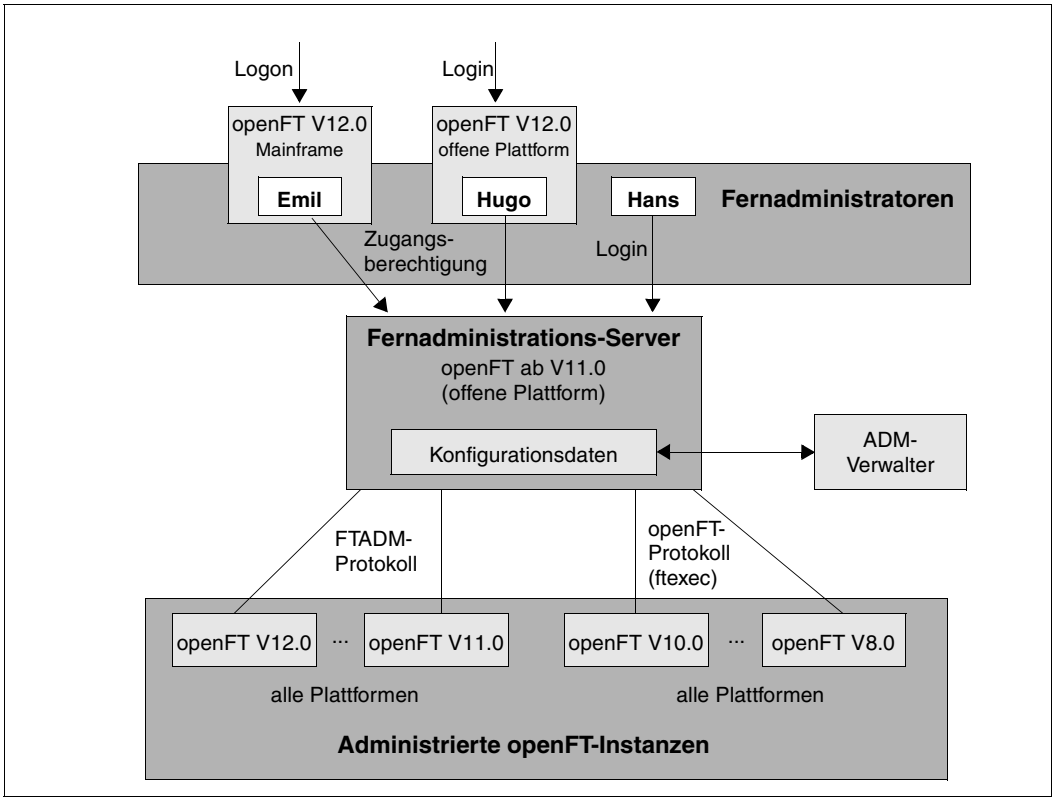
  Instanzen mit openFT-Versionen ab V8.0 können einfach in die Konfiguration aufgenommen werden und auf dieselbe Art und Weise administriert werden wie Instanzen ab V11.0. Dabei lassen sich alle Administrationsfunktionen nutzen, die die jeweilige openFT-Version bietet.

5.1 Fernadministration

Mit openFT können Sie einen Fernadministrations-Server einrichten, über den Sie Ihre openFT-Instanzen auf den unterschiedlichen Plattformen administrieren können.
Als Administrations-Arbeitsplatz können Sie eine beliebige openFT-Instanz wählen.

5.1.1 Konzept der Fernadministration

Das folgende Bild zeigt anhand eines Einsatz-Szenarios die Komponenten der Fernadministration und die wichtigsten Konfigurationsmöglichkeiten.



Komponenten der Fernadministration

Die Fernadministration besteht aus folgenden Komponenten:

Fernadministrations-Server

Zentrale Komponente der Fernadministration. Diese läuft auf einem Unix- oder Windows-System mit openFT ab V11.0 und enthält sämtliche Konfigurationsdaten für die Fernadministration.

In einer Gesamtkonfiguration können mehrere Fernadministrations-Server definiert werden, siehe Seite 117.

ADM-Verwalter

Person, die den Fernadministrations-Server verwaltet. Sie erstellt die Konfigurationsdaten für die Fernadministration, in denen z.B. die Fernadministratoren und die administrierten openFT-Instanzen festgelegt sind. Der ADM-Verwalter ist die einzige Person, die die Konfigurationsdaten ändern darf.

Fernadministrator

Rolle, die im Fernadministrations-Server konfiguriert wird und dazu berechtigt, bestimmte Administrationsfunktionen auf bestimmten openFT-Instanzen auszuführen. Ein Fernadministrator kann sich

– direkt am Fernadministrations-Server anmelden (Single Sign-on)

– an eine andere openFT-Instanz (ab V11.0) anmelden und mittels FTAC-Zugangsberechtigung auf den Fernadministrations-Server zugreifen.
Die openFT-Instanz kann sowohl auf Mainframes (BS2000/OSD, z/OS) als auch auf Unix- oder Windows-Systemen ablaufen. Für die Kommunikation wird das FTADM-Protokoll verwendet.

Es können mehrere Fernadministratoren mit unterschiedlichen Rechten konfiguriert werden.

Administrierte openFT-Instanz

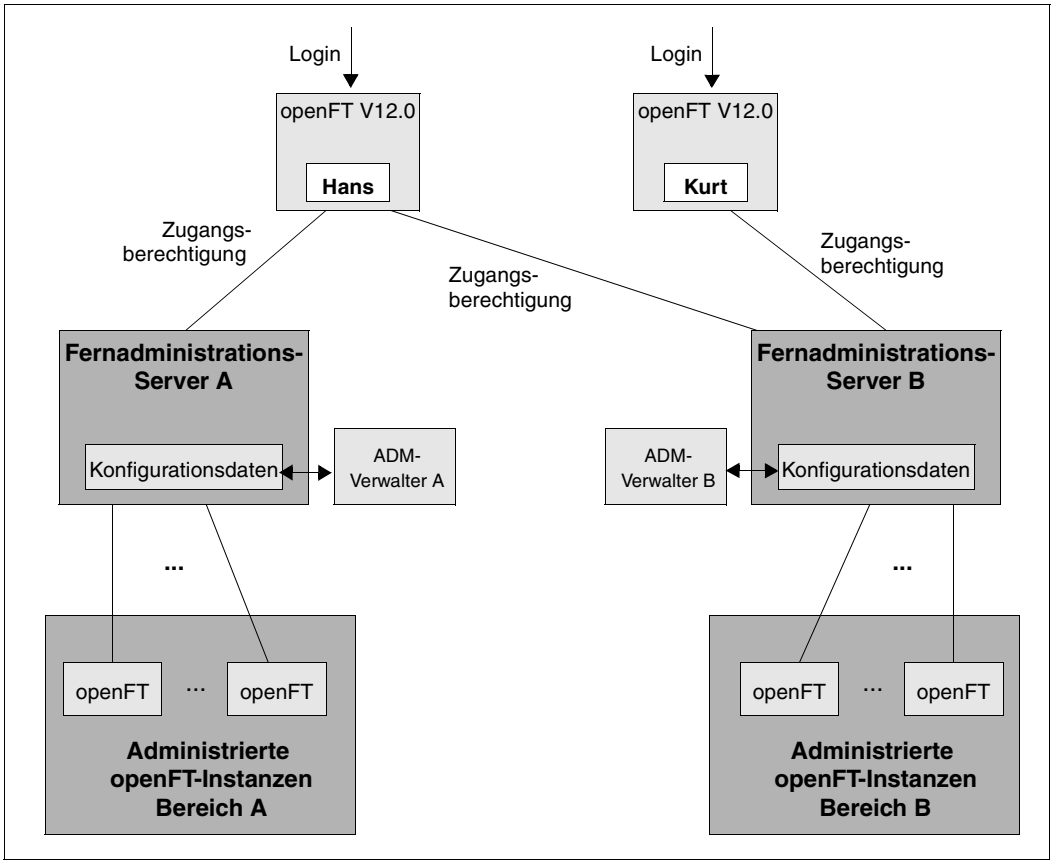
openFT-Instanz, die durch Fernadministratoren im laufenden Betrieb administriert werden kann. Der Zugriff erfolgt über ein Berechtigungsprofil. Je nachdem, welche openFT-Version die openFT-Instanz besitzt, gilt:

– Bei openFT-Instanzen ab V11.0 wird das FTADM-Protokoll verwendet, es kann der volle Funktionsumfang der Fernadministration genutzt werden.

– Bei openFT-Instanzen von V8.0 bis V10.0 wird die Administration über das openFT-Protokoll und das Kommando *ftexec* durchgeführt. Der Funktionsumfang richtet sich nach der openFT-Version der administrierten Instanz.

Konfiguration mit mehreren Fernadministrations-Servern

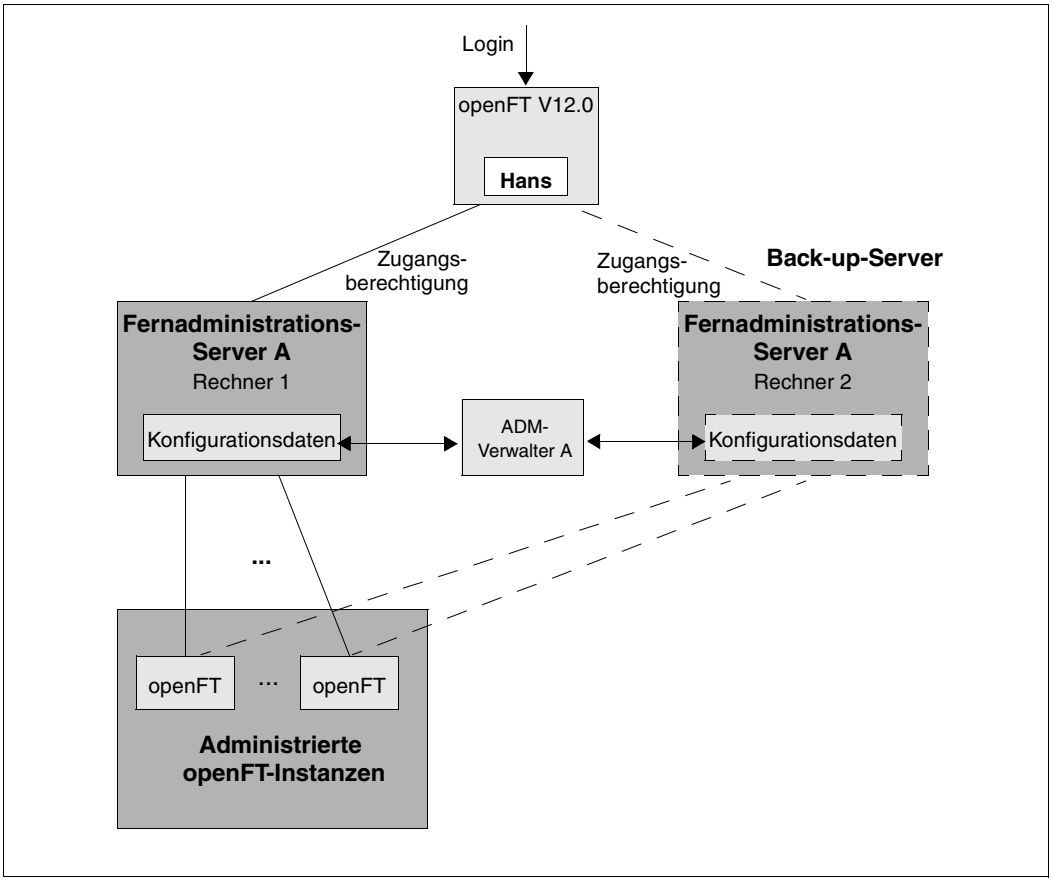
Es lassen sich auch komplexe Konfigurationen definieren, bei denen Fernadministratoren auf mehrere Fernadministrations-Server zugreifen. Das folgende Diagramm zeigt dies an einem Beispiel.



Getrennte Konfigurationen mit zwei Fernadministrations-Servern

Bereich A und B sind zwar strikt getrennt, aber *Hans* darf Instanzen aus den Bereichen A und B administrieren, *Kurt* dagegen nur aus dem Bereich B.

Dieselbe Methode kann auch dazu verwendet werden, eine redundante Konfiguration mit einem zweiten Fernadministrations-Server zu definieren. Damit lässt sich eine einfache Back-up-Lösung realisieren.



Redundante Konfiguration mit zweitem Fernadministrations-Server als Back-up

Bei Ausfall von Rechner 1 kann der Fernadministrator den Rechner 2 als Fernadministrations-Server nutzen. Voraussetzung ist, dass

- der ADM-Verwalter die Konfigurationsdaten auf beiden Rechnern immer konsistent hält,
- die Berechtigungsprofile für den Zugang zum Fernadministrations-Server sowie die Partnerlisteneinträge (falls verwendet) auf Rechner 1 und Rechner 2 identisch sind,
- auf den administrierten Instanzen die Berechtigungsprofile so definiert sind, dass sie beide Fernadministrations-Server als Partner akzeptieren.

Wenn mit Authentifizierung gearbeitet wird, dann müssen Sie zusätzlich beachten, dass

– die Schlüssel der Rechner, von denen aus administriert wird, auf beiden Fernadministrations-Servern vorhanden sind,

– die administrierten Instanzen die Schlüssel von beiden Fernadministrations-Servern benötigen.

Daher sollten Sie vor allem bei komplexen Konfigurationen die Ausfallsicherheit des Fernadministrations-Servers mit Hilfe eines Clusters realisieren. Beispiele für das Einrichten eines Clusters finden Sie im Abschnitt „openFT im Cluster mit Unix-Systemen“ auf Seite 444.

5.1.2 Fernadministrations-Server konfigurieren

Der Fernadministrations-Server hält die für die Fernadministration notwendigen Daten und muss explizit in mehreren Schritten konfiguriert werden. Einige dieser Schritte kann nur der ADM-Verwalter durchführen, der zuvor festgelegt werden muss.

Überblick über die Konfigurationsschritte

Wenn Ihr System als Fernadministrations-Server konfiguriert werden soll, muss darauf openFT ab V11.0 installiert sein. Die Beschreibung in diesem Unterkapitel gilt für openFT V12.0.

Die folgende Tabelle zeigt,

- welche Schritte notwendig sind, um eine Konfiguration zu erstellen wie auf Seite 115 dargestellt,
- und wer sie durchführt.

Schritt	Wer
1. ADM-Verwalter festlegen	FTAC-Verwalter
2. openFT-Instanz als Fernadministrations-Server deklarieren	FT-Verwalter
3. Berechtigungsprofile für den Zugang zum Fernadministrations-Server einrichten	ADM-Verwalter
4. Zu administrierende openFT-Instanzen in die Partnerliste eintragen	FT-Verwalter
5. Konfigurationsdatei per Text-Editor oder Konfigurations-Editor erstellen	ADM-Verwalter
6. Konfiguration importieren	ADM-Verwalter

Damit ist der Fernadministrations-Server betriebsbereit. Der ADM-Verwalter kann die aktuelle Konfiguration jederzeit exportieren und ändern, siehe Seite 140.

Jetzt müssen noch openFT-Instanzen auf den Partnersystemen für die Fernadministration konfiguriert werden, siehe Seite 142.

5.1.2.1 ADM-Verwalter festlegen

Der ADM-Verwalter ist die einzige Person, die den Fernadministrations-Server verwalten darf. Da nach der Installation von openFT standardmäßig noch kein ADM-Verwalter definiert ist, wird dringend empfohlen, diesen zuerst festzulegen. Diese Eigenschaft ist an den Berechtigungssatz geknüpft und muss daher vom FTAC-Verwalter zugewiesen werden.

Rufen Sie als FTAC-Verwalter folgendes Kommando auf:

```
ftmoda kennung –admpriv=y
```

Damit ist die Benutzerkennung *kennung* der ADM-Verwalter. Ist der ADM-Verwalter einmal festgelegt, dann kann nur der ADM-Verwalter selber die Berechtigung an eine andere Kennung übertragen! Es reicht dann nicht aus, dass Sie FT- oder FTAC-Verwalter sind.

Wenn Sie keine Kennung angeben (`ftmoda –admpriv=y`), dann sind Sie als FTAC-Verwalter auch der ADM-Verwalter.

Der ADM-Verwalter wird beim Kommando *ftshwa* in der Spalte ATTR angezeigt. Dort steht beim zugehörigen Berechtigungssatz der Wert ADMPR.

Anstelle der Kommandos können Sie auch die Funktionen des openFT Explorers verwenden, z.B. über das Objektverzeichnis *Berechtigungssätze* im Objektbaum auf der linken Seite oder unter dem Menü *Datei* - *Neu* - *Berechtigungssatz*.

5.1.2.2 openFT-Instanz als Fernadministrations-Server deklarieren

Damit eine openFT-Instanz als Fernadministrations-Server fungieren kann, muss dies explizit in den Betriebsparametern der Instanz festgelegt werden.

Dazu geben Sie als FT-Verwalter folgendes Kommando ein:

```
ftmodo –admcs=y
```

Alternativ können Sie diesen Betriebsparameter über den openFT Explorer einstellen: Menü *Administration* - *Betriebsparameter*, Registerblatt *Protokolle*, Option *Fernadministrations-Server*.

– Sobald eine openFT-Instanz als Fernadministrations-Server deklariert wird, wird implizit auch der Betriebsparameter *Administrationsverbindungen* geändert und auf 64 gesetzt! Wenn hohe Last zu erwarten ist, dann können Sie diesen Wert als FT-Verwalter erhöhen, insbesondere dann, wenn die openFT-Instanz zusätzlich als ADM-Trap-Server eingesetzt wird, siehe Seite 152.

– Es wird aus Performancegründen empfohlen, als Fernadministrations-Server einen separaten Rechner zu verwenden, der nur Aufgaben der Fernadministration und ggf. die Rolle des ADM-Trap-Servers übernimmt und nicht für den normalen FT-Betrieb eingesetzt wird.

5.1.2.3 Berechtigungsprofile für den Zugang zum Fernadministrations-Server einrichten

Damit die Fernadministratoren Zugang zum Fernadministrations-Server erhalten, muss der ADM-Verwalter spezielle Berechtigungsprofile mit der Eigenschaft "Zugang zum Fernadministrations-Server" (ACCESS-TO-ADMINISTRATION) einrichten. Der Eigentümer dieser Berechtigungsprofile ist immer der ADM-Verwalter, aber niemals der Fernadministrator, für dessen Zugang ein solches Profil eingerichtet wird.

Es wird dringend empfohlen, für jeden Fernadministrator ein eigenes Berechtigungsprofil einzurichten, damit nachvollziehbar ist, welcher Fernadministrator auf welcher openFT-Instanz eine Änderung durchgeführt hat.

Geben Sie als ADM-Verwalter das Kommando *ftcrep* mit der Option *-ff=c* ein:

```
ftcrep profilname zugangsberechtigung –ff=c
```

profilname
: bezeichnet den Profilnamen. Diesen Namen müssen Sie in die Konfigurationsdatei eintragen, wenn Sie den Fernadministrator definieren, siehe Seite 129.

zugangsberechtigung
: bezeichnet die FTAC-Zugangsberechtigung. Diese muss der Fernadministrator beim Fernadministrations-Auftrag angeben, siehe Seite 145.

Zusätzlich können Sie aus Sicherheitsgründen mit *-pn=part1,part2,..,partn* den oder die Partner festlegen, von dem/denen ein Fernadministrator auf den Fernadministrations-Server zugreifen darf.

Sie können das Profil auch über den openFT Explorer einrichten, indem Sie im Dialog *Berechtigungsprofil* auf dem Registerblatt *Optionen* folgende Einstellungen vornehmen:

– Aktivieren Sie die Option *Zugang zum Fernadministrations-Server.*

– Deaktivieren Sie alle File-Transfer-Funktionen unter *Erlaubte File-Transfer-Funktionen*.

5.1.2.4 Zu administrierende openFT-Instanzen in die Partnerliste eintragen

Auf dem Fernadministrations-Server sollte der FT-Verwalter die openFT-Instanzen, die administriert werden sollen, in die Partnerliste eintragen. Damit können die Instanzen über den Namen in der Partnerliste referenziert werden, was folgende Vorteile hat:

- Bei Adress-Änderungen muss nur der Partnerlisteneintrag geändert werden. Damit wird das Modifizieren und erneute Importieren der Konfigurationsdatei vermieden.
- Man kann gezielt mit Partnerüberprüfung und Authentifizierung arbeiten und damit Sicherheitsrisiken auf der Strecke zwischen Fernadministrations-Server und administrierter openFT-Instanz ausschalten.

Die Partner tragen Sie als FT-Verwalter in die Partnerliste ein. Verwenden Sie dazu das Kommando *ftaddptn*, siehe Abschnitt „ftaddptn - Partner in die Partnerliste eintragen“ auf Seite 173. Alternativ dazu können Sie im openFT Explorer z.B. über den Objektbaum auf das Objektverzeichnis *Partnerliste* gehen und den Kontextmenü-Befehl *Neuer Partnerlisteneintrag...* auswählen.

Adressformat der Partner

Partner mit openFT ab V11.0 und openFT < V11.0 unterscheiden sich im Adressformat.

- Partner mit openFT ab V11.0 müssen als ADM-Partner eingetragen werden. Ein ADM-Partner hat folgendes Adressformat:

  ```
  ftadm://host[:portnummer]
  ```

  portnummer muss nur angegeben werden, wenn auf dem Rechner *host* der zu administrierenden Instanz nicht der ADM-Standardport (11000) verwendet wird.

- Partner mit openFT < V11.0 müssen als openFT-Partner eingetragen werden, da für die Fernadministration intern das Kommando *ftexec* verwendet wird:

  ```
  host[:portnummer]
  ```

  portnummer muss nur angegeben werden, wenn auf dem Rechner *host* der zu administrierenden Instanz nicht der openFT-Standardport (1100) verwendet wird.

  Der ADM-Verwalter muss für solche Partner in der Konfigurationsdatei zusätzlich das Attribut *Mode="Legacy"* angeben, siehe Abschnitt „Instanzen definieren“ auf Seite 133ff.

5.1.2.5 Konfigurationsdatei per Konfigurations-Editor erstellen

Dieses Unterkapitel richtet sich an den **ADM-Verwalter**.

Mit dem Konfigurations-Editor bietet openFT eine grafische Oberfläche, mit der Sie eine Konfigurationsdatei erstellen oder ändern können. Die Konfigurationsdatei ist eine Eingabedatei im XML-Format, in der Sie als ADM-Verwalter Folgendes definieren:

- die Fernadministratoren
- die openFT-Instanzen und Gruppen von Instanzen, die von diesen Fernadministratoren verwaltet werden sollen
- die Fernadministrations-Rechte, welche die Fernadministratoren auf den jeweiligen openFT-Instanzen haben (die Zugriffsliste)

Diese Datei müssen Sie anschließend importieren, siehe Abschnitt „Konfiguration importieren“ auf Seite 140.

Die Darstellung der Konfiguration entspricht dem, was Sie später auch unter *Fernadministration* im openFT Explorer sehen, siehe Beispiel bei „Konfigurationsdatei ändern“ auf Seite 126.

Neue Konfigurationsdatei erstellen

Im Folgenden werden die wichtigsten Schritte beschrieben. Details zu den Dialogen und den einzelnen Parametern finden Sie in der Online-Hilfe.

1. Starten Sie den openFT Explorer.
2. Starten Sie den Konfigurations-Editor mit dem Menü *Extras*, Befehl *Konfigurations-Editor starten*.

   Sie erhalten das Startfenster des Konfigurations-Editors.
3. Wählen Sie im Menü *Datei* den Befehl *Neue Konfiguration*.

   Im Navigationsbereich wird der Knoten *Konfiguration* angezeigt. Dort definieren Sie über Kontextmenü-Befehle die einzelnen Objekte der Konfiguration:

   - Administratoren

     Für den ersten Administrator wählen Sie im Knoten *Konfiguration* den Kontextmenü-Befehl *Neuer Administrator*. Definieren Sie im Dialog *Administrator* die Eigenschaften.

     Wiederholen Sie diesen Schritt für jeden Administrator, den Sie definieren möchten.

- Gruppen

  Wählen Sie im Knoten *Konfiguration* den Kontextmenü-Befehl *Neue Gruppe* und definieren Sie im Dialog *Gruppe* die Eigenschaften.

  Wiederholen Sie diesen Schritt für alle weiteren Gruppen, die Sie definieren möchten.

  Sie können zu jeder Gruppe Untergruppen erzeugen, indem Sie im Kontextmenü einer Gruppe den Befehl *Neue Gruppe* wählen.

- Instanzen

  Wählen Sie den Kontextmenü-Befehl *Neue Instanz*. Sie können diesen Befehl im Knoten *Konfiguration* (erzeugt eine Instanz auf oberster Ebene) oder im Knoten einer Gruppe aufrufen (erzeugt eine Instanz innerhalb einer Gruppe). Im Dialog *Instanz* definieren Sie die Eigenschaften der Instanz.

  Wiederholen Sie diesen Schritt für alle weiteren Instanzen, die Sie definieren möchten.

- Zugriffslisten

  Zugriffslisten können Sie für die komplette Konfiguration (globale Zugriffsliste), für Gruppen oder für einzelne Instanzen erstellen:

  Wählen Sie den Kontextmenü-Befehl *Zugriffsliste erstellen.* Sie können diesen Befehl im Knoten *Konfiguration* (globale Zugriffsliste), im Knoten einer Gruppe (gilt für alle Instanzen einer Gruppe einschließlich der Instanzen in den Untergruppen) oder einer Instanz auswählen.

  Damit wird zunächst nur das Element *Zugriffsliste* eingerichtet. Geben Sie jetzt in *Zugriffsliste* den Kontextmenü-Befehl *Neuer Zugriffseintrag* ein und definieren Sie im Dialog *Zugriffseintrag* die Berechtigungen für den Zugriff.

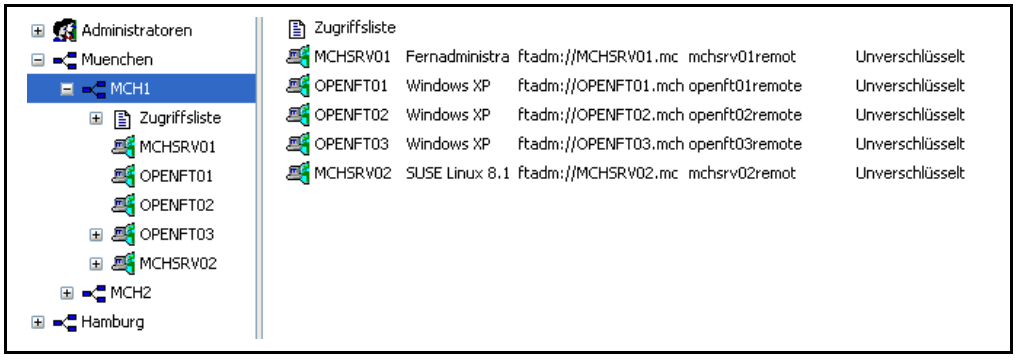
  Mit dem Befehl *Eigenschaften* aus dem Kontextmenü einer Zugriffsliste öffnen Sie den Dialog *Zugriffsliste*. Dort können Sie festlegen, ob Zugriffsrechte von übergeordneten Zugriffslisten geerbt werden sollen. Außerdem werden in diesem Dialog die ggf. geerbten Zugriffsrechte angezeigt.

4. Sichern Sie am Schluss die gesamte Konfiguration mit dem Befehl *Speichern unter* im Menü *Datei*. Beim Speichern prüft openFT die Gültigkeit der Konfigurationsdatei. Werden Fehler festgestellt, erhalten Sie eine entsprechende Meldung und werden gefragt, ob die Datei trotzdem gespeichert werden soll.

Konfigurationsdatei ändern

Sie können mit dem Konfigurations-Editor eine bestehende Konfiguration ändern, unabhängig davon, wie diese erstellt wurde.

1. Starten Sie den Konfigurations-Editor wie beim Erstellen einer neuen Konfigurationsdatei.
2. Wählen Sie im Menü *Datei* den Befehl *Öffnen*.
3. Wählen Sie im Folgedialog *Öffne Konfigurationsdatei* die Datei mit der Konfiguration aus, die Sie ändern möchten.
4. Die Konfiguration wird im Navigationsbereich in Form einer Baumstruktur angezeigt. Durch Aufklappen der einzelnen Knoten können Sie zu jedem Objekt navigieren, siehe folgendes Beispiel:



5. Sie können neue Objekte per Kontextmenü-Befehl hinzufügen (wie beim Erstellen einer neuen Konfigurationsdatei). Außerdem können Sie

   - Eigenschaften eines Objekts ändern:
     Wählen Sie für das Objekt den Kontextmenü-Befehl *Eigenschaften*. Im nachfolgenden Eigenschaftsdialog des Objekts lassen sich die Eigenschaften ändern.
   - Objekte verschieben:
     Wählen Sie für ein Objekt den Kontextmenü-Befehl *Kopieren* oder *Ausschneiden*, navigieren Sie an die gewünschte Stelle und wählen Sie dort den Kontextmenü-Befehl *Einfügen*. Alternativ können Sie Objekte im Navigationsbereich auch per Maus verschieben (entspricht *Ausschneiden* + *Einfügen*).
   - Objekte löschen:
     Wählen Sie für das Objekt den Kontextmenü-Befehl *Löschen* (Alternative: Taste *Entf*). Sie müssen das Löschen immer explizit bestätigen.

6. Sichern Sie am Schluss die geänderte Konfiguration, indem Sie im Menü *Datei* den Befehl *Speichern* (überschreibt die alte Konfigurationsdatei) oder den Befehl *Speichern unter* auswählen.

5.1.2.6 Konfigurationsdatei per Text- oder XML-Editor erstellen

Dieses Unterkapitel richtet sich an den **ADM-Verwalter**.

Die Konfigurationsdatei ist eine Eingabedatei im XML-Format, in der Sie als ADM-Verwalter die Konfiguration definieren. Sie können die Datei im Prinzip auf einem beliebigen System mit einem Text-Editor erstellen. Es hat jedoch Vorteile, wenn Sie auf dem (künftigen) Fernadministrations-Server arbeiten und einen XML-Editor verwenden, z. B. unter Windows den kostenlosen XML-Editor XML Notepad 2007 von Microsoft. In diesem Fall können Sie die mit ausgelieferte Vorlage samt Schema verwenden, so dass Ihre Eingaben sofort geprüft werden, siehe XML-Vorlage und XML-Schema verwenden.

Die Beschreibung der Konfigurationsdaten im XML-Format bietet eine einfache Möglichkeit, eine komplexe Konfiguration über Gruppenbildung übersichtlich darzustellen.

In der Konfigurationsdatei definieren Sie:

- die Konfiguration, siehe Seite 128,
- die Fernadministratoren, siehe Seite 129,
- die openFT-Instanzen und Gruppen von Instanzen, die von diesen Fernadministratoren verwaltet werden sollen, siehe Seite 131,
- die Fernadministrations-Rechte, welche die Fernadministratoren auf den jeweiligen openFT-Instanzen haben (die Zugriffsliste), siehe Seite 136.

Die Konfigurationsdatei müssen Sie als ADM-Verwalter anschließend auf dem Fernadministrations-Server mit dem Kommando *ftimpc* importieren, siehe Seite 140. Mit dem Kommando *ftexpc* (siehe Seite 216) können Sie aus den internen Konfigurationsdaten jederzeit wieder eine XML-Datei erzeugen, um beispielsweise die Konfiguration zu ändern.

Der Aufbau der XML-Datei wird in den folgenden Abschnitten erklärt. Ein vollständiges Beispiel ist im Abschnitt „Beispiel für eine XML-Konfigurationsdatei“ auf Seite 156 zu finden.

XML-Vorlage und XML-Schema verwenden

Unter dem openFT-Installationsverzeichnis befindet sich im Verzeichnis *samples/ftadm* die Datei *config.xml*, die eine einfache Beispielkonfiguration enthält und als Vorlage verwendet und angepasst werden kann.

Das der XML-Datei zugrunde liegende Schema ist in der Datei *config.xsd* festgelegt, die nach der Installation im *include*-Verzeichnis von openFT zu finden ist. Wenn Sie einen XML-Editor einsetzen, dann können Sie die Datei *config.xml* als Basis verwenden. Dort ist der Installationspfad für die Schemadatei *config.xsd* eingetragen. Damit verwendet der XML-Editor dieses Schema, um Ihre Eingaben sofort zu verifizieren. Falls *config.xsd* umkopiert oder umbenannt wurde, müssen Sie in *config.xml* den Installationspfad von *config.xsd* anpassen.

Konfiguration definieren

Die Konfigurationsdatei enthält genau eine Konfiguration für einen Fernadministrations-Server. Sie ist hierarchisch aufgebaut, d.h. untergeordnete Elemente stehen geschachtelt innerhalb eines übergeordneten Elements.

Eine Konfiguration beginnt mit dem XML-Tag <Configuration> und besteht aus folgenden Attributen:

- obligatorisches Attribut *Version*. Der Wert des Attributs *Version* ist eine Zeichenfolge, die die Version der Konfigurationsdaten festlegt. Die maximale Länge der Zeichenfolge beträgt 4 Byte. In openFT V12.0 ist für die Version `"1100"` anzugeben.
- optionales Attribut *Description*. Der Wert des Attributs *Description* ist eine Zeichenfolge, die die Konfigurationsdaten näher beschreibt. Die maximale Länge der Zeichenfolge beträgt 100 Byte.

Beispiel:

```
<Configuration
    Version="1100"
    Description="Konfiguration f. zentralen Server MCHSRV01">
    <...
    .../>

</Configuration>
```

Elemente einer Konfiguration

Eine Konfiguration enthält folgende Elemente:

- mindestens ein Element *AdministratorID* mit dem Tag <AdministratorID> zur Definition eines Fernadministrators. Sie können bis zu 100 Fernadministratoren definieren. Die detaillierte Beschreibung entnehmen Sie dem Abschnitt „Fernadministratoren definieren“ auf Seite 129.
- optionales Element *Zugriffsliste* mit dem Tag <AccessList>. Über eine Zugriffsliste definieren Sie für die einzelnen Fernadministratoren die Administrations-Rechte auf den openFT-Instanzen. Die detaillierte Beschreibung der Zugriffsliste entnehmen Sie dem Abschnitt „Zugriffsliste definieren“ auf Seite 136.
- optionale Elemente *Gruppe* mit dem Tag <Group>. Gruppen können geschachtelt werden, wodurch sich z.B. die räumliche oder organisatorische Struktur eines Unternehmens abbilden lässt. Die maximale Schachtelungstiefe ist begrenzt, siehe Hinweis auf Seite 129. Die detaillierte Beschreibung einer Gruppe entnehmen Sie dem Abschnitt „Gruppen und zu administrierende openFT-Instanzen definieren“ auf Seite 131.

- mindestens ein Element *Instanz* mit dem Tag <Instance> für die openFT-Instanzen. Sie können bis zu 5000 Instanzen angeben. Die detaillierte Beschreibung einer Instanz entnehmen Sie dem Abschnitt „Gruppen und zu administrierende openFT-Instanzen definieren“ auf Seite 131.

Aus dem Namen der Instanz und dem Namen der Gruppe (ggf. mit Untergruppen) wird nach folgendem Schema ein Pfadname gebildet:

```
Gruppe/Untergruppe1/Untergruppe2/.../Instanz
```

Der Fernadministrator muss im Fernadministrationsauftrag an die Instanz genau diesen Pfadnamen angeben, siehe auch Seite 146.

Dieser Pfadname darf maximal 200 Zeichen lang sein. Die maximale Anzahl der Untergruppen hängt daher von der Länge der einzelnen Namen ab.

Fernadministratoren definieren

Sie legen in der Konfigurationsdatei fest, welche Fernadministratoren eine Fernadministration durchführen können. Dazu gehen Sie wie folgt vor:

- Definieren Sie einen oder mehrere Fernadministratoren
- Ordnen Sie jedem Fernadministrator jeweils einen Profilnamen und/oder eine Benutzerkennung auf dem Fernadministrations-Server zu.

Ein Fernadministrator wird mit dem XML-Tag <AdministratorID> definiert. Sie dürfen in der XML-Datei maximal 100 Fernadministratoren eintragen. Die <AdministratorID>-Tags müssen unmittelbar nach dem Tag <Configuration> definiert werden, weil in den folgenden Definitionen für die Gruppen und Instanzen darauf Bezug genommen wird.

<AdministratorID> besitzt folgende Attribute:

- obligatorisches Attribut *Name*. Der Wert des Attributs *Name* ist eine Zeichenfolge, die den Namen des Fernadministrators angibt. Die maximale Länge der Zeichenfolge beträgt 32 Byte. Der Name muss eindeutig sein, d.h. in der Konfigurationsdatei dürfen keine weiteren <AdministratorID>-Tags gleichen Namens existieren. Der Name wird sowohl intern in den Konfigurationsdaten als auch extern in Logging-Sätzen verwendet, um den Initiator eines Fernadministrations-Auftrages eindeutig zu identifizieren.
- optionales Attribut *Description*. Der Wert des Attributs *Description* ist eine Zeichenfolge, die den Fernadministrator näher beschreibt. Die maximale Länge der Zeichenfolge beträgt 100 Byte.
- optionale Attribute *UserID* und *Profile*. Diese Attribute identifizieren den Fernadministrator abhängig von der Art des Zugangs zum Fernadministrations-Server. Sie müssen daher mindestens eines der beiden Attribute *UserID* oder *Profile* angeben. Es ist auch möglich, beide Attribute einzutragen.

Für *UserID* und *Profile* gilt:

– Der Wert des Attributs *UserID* ist eine Zeichenfolge mit dem Namen einer gültigen Login-Kennung auf dem Fernadministrations-Server. Die maximale Länge der Zeichenfolge ist plattformabhängig und beträgt maximal 36 Byte.

  Der Benutzer, der sich unter dieser Kennung lokal am Fernadministrations-Server anmeldet, ist damit Fernadministrator und besitzt die Administrationsrechte, die für diese *AdministratorID* gelten. Eine bestimmte Login-Kennung darf daher immer nur bei einer *AdministratorID* angegeben werden, da sonst die Zuordnung Benutzerkennung <-> Fernadministrator nicht mehr eindeutig ist.

– Der Wert des Attributs *Profile* ist eine Zeichenfolge mit dem Namen eines gültigen FTAC-Profils. Die maximale Länge der Zeichenfolge beträgt 8 Byte. Der ADM-Verwalter des Fernadministrations-Servers muss Eigentümer des Profils sein. Jeder FTAC-Profilname darf nur bei jeweils genau einer *AdministratorID* verwendet werden.

  Dieses Profil wird verwendet, wenn der Fernadministrator einen Fernadministrations-Auftrag in einem fernen Rechner absetzt und mittels FTADM-Protokoll zum Fernadministrations-Server schickt. In diesem Fall muss er im Auftrag die zugehörige Zugangsberechtigung angeben.

  Das Profil muss die Funktion ACCESS-TO-ADMINISTRATION besitzen (entspricht *ftcrep -ff=c*), siehe Abschnitt „Berechtigungsprofile für den Zugang zum Fernadministrations-Server einrichten“ auf Seite 122.

Beispiel:

```
<Configuration
    Version="1100">
    <AdministratorID
        Name="Hans"
        Description="Verwalter der Domaenen Controller"
        UserID="rz\hans"
        Profile="Profil01"/>
    <AdministratorID
        Name="Fritz"
        Profile="Profil02"/>
    <...
           .../>
</Configuration>
```

Gruppen und zu administrierende openFT-Instanzen definieren

Die Konfigurationsdatei enthält alle openFT-Instanzen, die über diesen Fernadministrations-Server per Fernadministration verwaltet werden können.

Gruppen definieren

Durch die Definition von Gruppen und Untergruppen mit frei wählbaren Bezeichnungen lassen sich die zu verwaltenden openFT-Instanzen nach den jeweiligen Erfordernissen zusammenfassen. Wenn Gruppen gebildet werden, dann setzt sich der Pfad einer Instanz aus den durch Schrägstrich getrennten *Name*-Attributen der übergeordneten Gruppen und der jeweiligen Instanz zusammen, z.B. *Muenchen/MCH1/OPENFT01*. Die gesamte Pfadlänge darf die Gesamtlänge von 200 Byte nicht überschreiten, die maximale Schachtelungstiefe hängt daher von der Länge der einzelnen Namen ab.

Eine Gruppe beginnt mit dem XML-Tag <Group>. Die maximale Anzahl der Gruppen in der XML-Datei ist unbeschränkt. Die Gruppen müssen in der XML-Datei **nach** den Fernadministratoren definiert werden, weil in den folgenden Definitionen für die Gruppen und Instanzen auf die Fernadministratoren Bezug genommen wird.

Eine Gruppe besteht aus folgenden Attributen:

- obligatorisches Attribut *Name*. Der Wert des Attributs *Name* ist eine Zeichenfolge, die den Namen der Gruppe angibt. Die maximale Länge der Zeichenfolge beträgt 24 Byte, sie darf keinen Schrägstrich (/) enthalten. Der Name könnte beispielsweise der Name der Stadt, einer Niederlassung oder einer Dienststelle sein oder einfach eine Funktionsbezeichnung einer Gruppe von openFT-Instanzen.
- optionales Attribut *Description*. Der Wert des Attributs *Description* ist eine Zeichenfolge, die die Gruppe näher beschreibt. Die maximale Länge der Zeichenfolge beträgt 100 Byte.

Einer Gruppe können folgende Elemente zugeordnet werden:

- optionales Element *Zugriffsliste* mit dem Tag <AccessList>. Über die Zugriffsliste definieren Sie für die einzelnen Fernadministratoren die Fernadministrations-Rechte auf den openFT-Instanzen, die zu dieser Gruppe und ggf. zu untergeordneten, nachfolgenden Gruppen gehören. Die detaillierte Beschreibung der Zugriffsliste entnehmen Sie dem Abschnitt „Zugriffsliste definieren“ auf Seite 136.
- optionale Elemente *Gruppe* mit dem Tag <Group>. Sie können beliebig viele Gruppen angeben. Durch die Angabe weiterer geschachtelter Gruppen ist eine hierarchische Abbildung der Gruppenbeziehungen möglich, wobei die Gesamtpfadlänge nicht mehr als 200 Byte betragen darf, siehe Hinweis auf Seite 129.
- optionale Elemente *Instanz* mit dem Tag <Instance> für die openFT-Instanzen, die zu dieser Gruppe gehören. Sie können in einer Konfiguration bis zu 5000 Instanzen angeben.

Die Angabe der Elemente *Gruppe* und *Instanz* innerhalb einer Gruppe ist zwar optional, aber eine Gruppe muss mindestens eine weitere Gruppe oder eine Instanz enthalten.

Beispiel:

```
<Configuration

    ...>
    <AdministratorID

            .../>
    <Group
           Name="Muenchen"
           Description="Rechenzentrum Muenchen">
       <Group
           Name="MCH1"
           Description="Rechenzentrum Muenchen Schwabing">
           <AccessList>
              <AccessEntry
                  .../>
           </AccessList>
           <Instance
              Name="MCHSRV01"
             ... />
           <Instance
              Name="OPENFT01"
             ... />
       </Group>
       <Group
           Name="MCH2"
           Description="Rechenzentrum Muenchen Freimann">
            ...
       </Group>
        ...
    </Group>
    ...
</Configuration>
```

Instanzen definieren

Eine openFT-Instanz beginnt mit dem XML-Tag <Instance>. Sie dürfen in einer XML-Datei maximal 5000 Instanzen definieren.

Eine Instanz kann einer Gruppe zugeordnet oder auch gruppenlos definiert werden. Dabei müssen Sie folgende Zuordnungshierarchie einhalten:

- Mit Gruppe(n):

  Konfiguration
  Fernadministrator(en)
  optionale Zugriffsliste
  Gruppe(n)
  optionale Zugriffsliste
  Instanz
  optionale instanzspezifische Zugriffsliste

- Ohne Gruppe:

  Konfiguration
  Fernadministrator(en)
  optionale Zugriffsliste
  Instanz
  optionale instanzspezifische Zugriffsliste

Details zur Zugriffsliste finden Sie auf Seite 136.

Eine Instanz besteht aus folgenden Attributen:

- obligatorisches Attribut *Name*. Der Wert des Attributs *Name* ist eine Zeichenfolge, die den Namen der openFT-Instanz angibt. Die maximale Länge der Zeichenfolge beträgt 24 Byte, sie darf keinen Schrägstrich (/) enthalten. Der Name der Instanz ist frei wählbar.
- optionales Attribut *Description*. Der Wert des Attributs *Description* ist eine Zeichenfolge, die die Instanz näher beschreibt. Die maximale Länge der Zeichenfolge beträgt 100 Byte.
- obligatorisches Attribut *Address*. Der Wert des Attributs *Address* ist eine maximal 200 Byte lange Zeichenfolge, die die Adresse der zu administrierenden openFT-Instanz angibt. Sie können den Namen aus der Partnerliste angeben oder die Adresse direkt eintragen.

Das Adressformat der verwalteten openFT-Instanz hängt von deren Version ab:

– openFT ab V11.0:
Die Adresse muss das Protokollpräfix *ftadm://* besitzen, d.h. mit diesem Präfix in der Partnerliste eingetragen sein bzw. hier angegeben werden. Andernfalls wird die openFT-Instanz wie eine openFT-Instanz < V11.0 per *ftexec* administriert.

– openFT < V11.0:
Die Adresse muss das Standardformat besitzen, d.h. ohne Präfix in der Partnerliste eingetragen sein bzw. hier angegeben werden. Gleichzeitig müssen Sie auch das Attribut *Mode* auf den Wert *"Legacy"* setzen, siehe unten.

- obligatorisches Attribut *Admission*. Der Wert des Attributs *Admission* ist eine Zeichenfolge mit der FTAC-Zugangsberechtigung. Die maximale Länge der Zeichenfolge beträgt 36 Byte (bei hexadezimaler Angabe 67 Byte). In der openFT-Instanz, die administriert werden soll, muss ein Berechtigungsprofil mit dieser Zugangsberechtigung definiert sein. Abhängig von der Version der zu administrierenden Instanz muss dieses Profil folgende Funktion(en) erlauben, siehe Abschnitt „Zu administrierende openFT-Instanz konfigurieren“ auf Seite 142:

  – openFT ab V11.0:
  REMOTE-ADMINISTRATION (entspricht *ftcrep ... -ff=a*)

  – openFT < V11.0:
  TRANSFER-FILE + FILE-PROCESSING (entspricht *ftcrep ... -ff=tp*)

  Sind in der zu administrierenden openFT-Instanz FT- und FTAC- Verwalter getrennt, dann tragen Sie für das Attribut *Admission* eine der beiden Zugangsberechtigungen (für FT-Verwalter oder FTAC-Verwalter) ein. Bei Bedarf müssen Sie eine zweite Instanz mit der jeweils anderen Zugangsberechtigung anlegen.

- optionales Attribut *Mode*. Für das Attribut *Mode* kann als Wert die Zeichenfolge *"Legacy"* angegeben werden. Dies bedeutet, dass es sich bei der openFT-Instanz um eine Instanz < V11.0 handelt, die nur über *ftexec* administriert werden kann. In diesem Fall darf in der Partneradresse kein Protokollpräfix *ftadm://* angegeben werden.

- optionales Attribut *DataEncryption*. Für das Attribut *DataEncryption* kann als Wert die Zeichenfolge *"Yes"* angegeben werden. Damit werden die Nutzdaten, die zwischen dem Fernadministrations-Server und der zu administrierenden openFT-Instanz ausgetauscht werden, verschlüsselt übertragen. Wenn das Attribut *DataEncryption* fehlt, werden die Nutzdaten unverschlüsselt übertragen.

  DataEncryption="Yes" darf nur angegeben werden, wenn sowohl auf dem Fernadministrations-Server als auch auf der zu administrierenden Instanz openFT-CR installiert ist.

Eine Instanz darf folgendes Element enthalten:

- optionale Zugriffsliste mit dem Tag <AccessList>. Über die Zugriffsliste können Sie für einzelne Fernadministratoren abweichende Rechte definieren, die nur für diese Instanz gelten. Sie können die vererbten Rechte erweitern oder einschränken oder die Vererbung abschalten und andere Rechte festlegen. Die detaillierte Beschreibung der Zugriffsliste entnehmen Sie dem Abschnitt "Zugriffsliste definieren".

Beispiel:

```
...

   <Group
      Name="MCH1"
      Description="Rechenzentrum Muenchen Schwabing">
      <AccessList>
         <AccessEntry
             .../>
      </AccessList>
      <Instance
         Name="MCHSRV01"
         Description="Fernadministrations-Server"
         Address="ftadm://MCHSRV01.mch.mycompany.net"
         Admission="mchsrv01remote"/>
      <Instance
         Name="OPENFT01"
         Description="Windows XP"
         Address="ftadm://OPENFT01.mch.mycompany.net:11009"
         Admission="openft01remote">
         <AccessList>
            <AccessEntry
             .../>
         </AccessList>
      </Instance>
   </Group>

...
```

Zugriffsliste definieren

In der Zugriffsliste legen Sie fest, welche Fernadministratoren Zugriff auf die jeweilige zu administrierende openFT-Instanz haben und welche Fernadministrations-Rechte mit dem jeweiligen Fernadministrator verbunden sind.

Es gelten folgende Regeln:

- Eine Zugriffsliste kann an folgenden Stellen definiert werden:
  - vor allen Gruppen und/oder Instanzen. Dann gilt sie für alle nachfolgenden Gruppen bzw. Instanzen, sofern für diese nicht eine eigene Zugriffsliste definiert wird.
  - als Element einer Gruppe. Dann gilt sie grundsätzlich für alle openFT-Instanzen, die zu dieser Gruppe gehören; sie wird auf untergeordnete Gruppen vererbt.
  - als Element einer openFT-Instanz, die administriert werden soll. Dann gilt sie nur für diese Instanz.
- Jede zu verwaltende openFT-Instanz benötigt eine Zugriffsliste, die entweder explizit bei der Instanz definiert ist oder von übergeordneten Elementen geerbt wird (zugehörige Gruppe, übergeordnete Gruppe oder eine vor allen Gruppen/Instanzen definierte Zugriffsliste).

  Eine openFT-Instanz ohne explizit gesetzte bzw. implizit geerbte Zugriffsliste(n) kann nicht administriert werden!
- In einer Zugriffsliste einer untergeordneten Gruppe bzw. für eine openFT-Instanz können Sie den Umfang der Vererbung gezielt steuern:
  - Sie können die Vererbung über das optionale Attribut *InheritFromParent* ausschalten. In diesem Fall müssen Sie für diese Instanz eine eigene Zugriffsliste definieren, in der Sie die Administrations-Rechte der Fernadministratoren festlegen.
  - Sie können vererbte Rechte für bestimmte Fernadministratoren erweitern oder einschränken (Attribute *AllowFunction* und *DenyFunction* bei <AccessEntry>). Einträge, die eine Funktion für einen bestimmten Fernadministrator verbieten, haben Vorrang vor Einträgen, die eine Funktion für einen bestimmten Fernadministrator erlauben. Zusätzliche Einträge bei Zugriffslisten für Gruppen werden ebenfalls an untergeordnete Gruppen vererbt.

Zugriffsliste definieren

Eine Zugriffsliste beginnt mit dem XML-Tag <AccessList>. Die maximale Anzahl der Zugriffslisten in der Konfigurationsdatei ist unbeschränkt. Die Zugriffsliste kann in der Datei an verschiedenen Stellen definiert werden, siehe Seite 136.

Eine Zugriffsliste besitzt folgendes Attribut:

- optionales Attribut *InheritFromParent*.
  Der Wert des Attributes *InheritFromParent* kann die Zeichenfolge *"No"* annehmen. Bei Angabe von *"No"* wird die Vererbung von Zugriffslisten übergeordneter Gruppen abgeschaltet. Da Zugriffslisten standardmäßig von übergeordneten Gruppen vererbt werden, muss das Attribut *InheritFromParent* nur dann angegeben werden, wenn die Vererbung explizit ausgeschaltet werden soll.

Eine Zugriffsliste darf folgende Elemente enthalten:

- ein oder mehrere *Zugriffseinträge* mit dem XML-Tag <AccessEntry>.
  Die Anzahl von Zugriffseinträgen ist beliebig, allerdings darf eine Zugriffsliste für jeden Fernadministrator maximal einen Zugriffseintrag enthalten. Mit einem Zugriffseintrag können Sie die Zugriffsrechte für einen Fernadministrator explizit definieren, d.h. Sie können angeben, welche Fernadministrations-Funktionen für ihn erlaubt oder verboten sind.

  Bitte beachten Sie dabei, dass übergeordnete Zugriffsrechte vererbt werden, sofern Sie dies nicht per *InheritFromParent="No"* ausschalten.

Zugriffseintrag definieren

Ein Zugriffseintrag ist Element einer Zugriffsliste und beginnt mit dem XML-Tag <AccessEntry>. Die maximale Anzahl der Zugriffseinträge in der Konfigurationsdatei ist unbeschränkt. Ein Zugriffseintrag besteht aus folgenden Attributen:

- obligatorisches Attribut *AdministratorID*. Der Wert des Attributs *AdministratorID* ist eine Zeichenfolge, die den Namen des Fernadministrators angibt. Dieser Fernadministrator muss am Anfang der Konfigurationsdatei mit einem Tag <AdministratorID> definiert sein, siehe Seite 129. Ein Fernadministrator darf in einer Zugriffsliste nur bei jeweils einem Zugriffseintrag angegeben werden.
- Attribute *AllowFunction* und *DenyFunction*. Mit diesen Attributen wird festgelegt, welche Fernadministrations-Funktionen erlaubt (*AllowFunction*) und welche verboten (*DenyFunction*) sind. Die Attribute *AllowFunction* und *DenyFunction* sind zwar optional, Sie müssen in einem Zugriffseintrag jedoch mindestens eines der beiden Attribute angeben.

  Sind beide Attribute angegeben, dann beachten Sie bitte, dass Einträge beim Attribut *DenyFunction*, die eine Funktion für den Fernadministrator verbieten, Vorrang haben vor Einträgen beim Attribut *AllowFunction*, die diese Funktion für den Fernadministrator erlauben.

Im Einzelnen gilt:

– Der Wert des Attributs *AllowFunction* gibt an, welche Fernadministrations-Funktionen der Fernadministrator durchführen darf. Die Zeichenfolge kann folgende Werte (Fernadministrations-Rechte) annehmen:

```
"FTOP"
"FT"
"FTAC"
"FT FTAC"
"FTAC FT"
"FTAC FTOP"
"FTOP FTAC"
```

  – Die Angabe von *"FTOP"* (FT-Operator) erlaubt nur lesende FT-Zugriffe.
  – Die Angabe von *"FT"* erlaubt lesende und modifizierende FT-Zugriffe.
  – Die Angabe von *"FTAC"* erlaubt lesende und modifizierende FTAC-Zugriffe.

  Kombinationen bedeuten, dass der Fernadministrator beide Rechte besitzt.

– Der Wert des Attributs *DenyFunction* bestimmt, welche Fernadministrations-Funktionen für den Fernadministrator verboten sind. Die Zeichenfolge kann folgende Werte annehmen:

```
"FT"
"FTMOD"
"FTAC"
"FT FTAC"
"FTAC FT"
"FTAC FTMOD"
"FTMOD FTAC"
```

  – Die Angabe von *"FTMOD"* verbietet modifizierende FT-Zugriffe.
  – Die Angabe von *"FT"* verbietet lesende und modifizierende FT-Zugriffe.
  – Die Angabe von *"FTAC"* verbietet lesende und modifizierende FTAC-Zugriffe.

  Kombinationen bedeuten, dass beides verboten ist.
  Z.B. bedeutet `"FTAC FTMOD"`, dass weder FTAC-Zugriffe noch modifizierende FT-Zugriffe erlaubt sind. D.h. es sind höchstens lesende FT-Zugriffe erlaubt, was der Angabe von *"FTOP"* bei *AllowFunction* entspricht.

Beispiel:

```
<Group
    Name="HH1"
    Description="QA Rechenzentrum">
    <AccessList>
       <AccessEntry
          AdministratorID="Emil"
          AllowFunction="FT FTAC"/>
       <AccessEntry
          AdministratorID="Hugo"
          AllowFunction="FT FTAC"/>
    </AccessList>
    <Instance
       Name="HHWSRV02"
       Description="HP-11"
       Address="ftadm://HHWSRV02.hhw.mycompany.net"
       Admission="hhwsrv02remote"/>
    <Instance
       Name="HHWSRV11"
       Description="Solaris 9"
       Address="HHWSRV11.hhw.mycompany.net"
       Admission="hhwsrv11remote"
       Mode="Legacy">
       <AccessList>
          <AccessEntry
             AdministratorID="Hugo"
             DenyFunction="FTAC"/>
       </AccessList>
    </Instance>
</Group>
```

5.1.2.7 Konfiguration importieren

Die in der Konfigurationsdatei definierte Konfiguration muss noch in das interne, optimierte Format umgewandelt und dadurch aktiviert werden.

Dazu geben Sie als ADM-Verwalter auf dem Fernadministrations-Server das Kommando *ftimpc* ein:

`ftimpc` *xml-datei*

xml-datei bezeichnet die Konfigurationsdatei, die Sie zuvor erstellt haben, siehe Seite 127.

Alternativ dazu können Sie die Aktion auch im openFT Explorer ausführen: Menü *Administration*, Menüpunkt *Fernadministration* - *Konfiguration importieren...*

Der Import ist während des laufenden Betriebs möglich.

Nach dem Importieren der Konfigurationsdatei ist der Fernadministrations-Server betriebsbereit. Er kann Fernadministrations-Aufträge entgegennehmen und an die zu administrierenden openFT-Instanzen weiterleiten.

5.1.2.8 Konfiguration exportieren und ändern

openFT bietet dem ADM-Verwalter eine Exportfunktion, um die Konfigurationsdaten zu sichern, zu überprüfen oder zu ändern.

Ein direktes Ändern der Konfigurationsdaten auf dem Fernadministrations-Server ist nicht möglich.

Beachten Sie bitte, dass das Kommando *ftshwc* nicht dazu dient, Ihnen als ADM-Verwalter die gesamte Konfiguration auszugeben. Es dient vielmehr dazu, einem Fernadministrator die von ihm zu verwaltenden openFT-Instanzen anzuzeigen, inklusive der Fernadministrations-Rechte, die er für die Instanzen hat.

Näheres siehe Abschnitt „ftshwc - Fernadministrierbare openFT-Instanzen anzeigen“ auf Seite 298.

Konfiguration exportieren

Wenn Sie als ADM-Verwalter die Konfiguration exportieren möchten, dann geben Sie auf dem Fernadministrations-Server folgendes Kommando ein:

`ftexpc` *xml-datei*

Alternative im openFT Explorer:
Menü *Administration*, Menüpunkt *Fernadministration* - *Konfiguration exportieren...* .

Die Konfigurationsdaten werden in der Datei *xml-datei* im XML-Format abgelegt. Die Notation ist dieselbe wie beim Erstellen der Konfigurationsdatei, siehe Seite 127 ff.

Der Export ist während des laufenden Betriebs möglich.

Konfiguration ändern

Wenn Sie als ADM-Verwalter eine Konfiguration ändern möchten, z.B. um Instanzen hinzuzufügen oder Adressen zu ändern, dann sind folgende Schritte nötig:

1. Exportieren Sie die Konfiguration in eine Datei wie oben beschrieben, z.B. mit *ftexpc xml-datei*.
2. Bringen Sie die Änderungen in die Datei ein, Details siehe Abschnitt „Konfigurationsdatei per Konfigurations-Editor erstellen“ auf Seite 124 oder Abschnitt „Konfigurationsdatei per Text- oder XML-Editor erstellen“ auf Seite 127.
3. Importieren Sie die geänderte Datei, z.B. mit *ftimpc xml-datei*, siehe auch Seite 140.

   Das Importieren ist während des laufenden Betriebs möglich. Falls die Änderungen der Konfiguration jedoch sehr umfangreich sind, werden Sie durch eine entsprechende Meldung aufgefordert, den asynchronen openFT-Server vor dem Import zu stoppen. Zum Stoppen und späteren Starten können Sie die Kommandos *ftstop* und *ftstart* oder die entsprechenden Befehle im openFT Explorer im Menü *Administration* verwenden.

Die Änderungen werden sofort wirksam, laufende ADM-Aufträge mit der alten Konfiguration werden jedoch nicht abgebrochen. Die neue Konfiguration wird im openFT Explorer angezeigt, wenn Sie für den betreffenden Fernadministrations-Server den Kontextmenü-Befehl *Aktualisieren* wählen.

5.1.3 Zu administrierende openFT-Instanz konfigurieren

Der Fernadministrations-Server benutzt FTAC-Zugangsberechtigungen, um auf die openFT-Instanzen zuzugreifen. Diese müssen in der Konfigurationsdatei beim Definieren der openFT-Instanz eingetragen sein, siehe Seite 133.

Daher müssen in den zu administrierenden openFT-Instanzen passende Berechtigungsprofile definiert werden. Die Eigenschaften dieser Profile hängen davon ab, welche Version die zu administrierende openFT-Instanz besitzt.

5.1.3.1 Berechtigungsprofil für openFT-Instanz ab V11.0 konfigurieren

Für die Fernadministration muss auf der zu administrierenden Instanz ein Berechtigungsprofil mit der Funktion "Fernadministration" (REMOTE-ADMINISTRATION) eingerichtet werden. Dabei sind folgende Fälle zu unterscheiden:

- Ein Berechtigungsprofil mit dem Recht FT (lesende und modifizierende FT-Zugriffe) oder FTOP (lesende FT-Zugriffe) muss dem FT-Verwalter gehören.
- Ein Berechtigungsprofil mit dem Recht FTAC (lesende und modifizierende FTAC-Zugriffe) muss dem FTAC-Verwalter gehören.
- Ein Berechtigungsprofil mit dem Recht FT+FTAC (lesende und modifizierende FT- und FTAC-Zugriffe) kann nur eingerichtet werden, wenn der FT- auch FTAC-Verwalter ist. Wenn dies nicht der Fall ist, dann müssen zwei Profile erzeugt werden (für FT und für FTAC). In der Konfigurationsdatei des Fernadministrations-Servers ist die Instanz dann auch zweimal zu konfigurieren, einmal für FT-Fernadministration und einmal für FTAC-Fernadministration.

Beispiel

Für ein Berechtigungsprofil gibt der FT-Verwalter z.B. folgendes Kommando ein:

– Unix- oder Windows-System:

```
ftcrep profilname zugangsberechtigung -ff=a
```

Mögliche Alternative über den openFT Explorer: Dialog *Berechtigungsprofil* öffnen, z.B. mit *Datei* - *Neu* - *Berechtigungsprofil*, dann im Registerblatt *Optionen* die Option *Fernadministration durch zentralen Fernadministrations-Server* aktivieren.

– BS2000/OSD:

```
CREATE-FT-PROFILE NAME=profilname -
             ,TRANSFER-ADMISSION=zugangsberechtigung -
             ,FT-FUNCTION=*REMOTE-ADMINISTRATION
```

– z/OS:

```
FTCREPRF NAME=profilname -
     ,TRANSFER-ADMISSION=zugangsberechtigung -
     ,FT-FUNCTION=*REMOTE-ADMINISTRATION
```

Wenn Sie zusätzlich sicherstellen möchten, dass dieses Profil nur durch einen bestimmten Fernadministrations-Server genutzt werden kann, dann geben Sie diesen mit *-pn=server* (Unix- und Windows-System) bzw. *PARTNER=server* (BS2000/OSD und z/OS) an.

5.1.3.2 Berechtigungsprofil für openFT-Instanz < V11.0 konfigurieren

Für die Fernadministration muss auf der zu administrierenden Instanz ein Berechtigungsprofil eingerichtet werden, das die FT-Funktionen "Datei übertragen" (TRANSFER-FILE) und "Vor-/Nachverarbeitung" (FILE-PROCESSING) erlaubt. Es gelten dieselben Anmerkungen wie im Falle einer openFT-Instanz ab V11.0 (siehe Seite 142).

Beispiel

Für ein Berechtigungsprofil gibt der FT-Verwalter z.B. folgendes Kommando ein:

– Unix- oder Windows-System:

```
ftcrep profilname zugangsberechtigung -ff=tp
```

Mögliche Alternative über den openFT Explorer: Dialog *Berechtigungsprofil* öffnen, z.B. mit *Datei* - *Neu* - *Berechtigungsprofil*, dann im Registerblatt *Optionen* die Optionen *Dateien übertragen und/oder Dateien löschen* und *Vor-/Nachverarbeitung* aktivieren.

– BS2000/OSD:

```
CREATE-FT-PROFILE NAME=profilname -
             ,TRANSFER-ADMISSION=zugangsberechtigung -
             ,FT-FUNCTION=(*TRANSFER-FILE, -
                           *FILE-PROCESSING)
```

– z/OS:

```
FTCREPRF NAME=profilname -
     ,TRANSFER-ADMISSION=zugangsberechtigung -
     ,FT-FUNCTION=(*TRANSFER-FILE, -
                   *FILE-PROCESSING)
```

5.1.4 Fernadministrations-Aufträge stellen

Dieser Abschnitt richtet sich an alle **Fernadministratoren**, für die in der Konfiguration des Fernadministrations-Servers bestimmte Rechte für die Fernadministration festgelegt wurden.

Als Fernadministrator können Sie die Fernadministration über Kommando (siehe unten) oder über den openFT Explorer (siehe Seite 147) durchführen.

Die Aufträge können Sie auf dem Fernadministrations-Server selber oder auf einem fernen Rechner stellen:

- Wenn Sie Aufträge auf dem Fernadministrations-Server stellen, dann müssen Sie sich unter der Benutzerkennung anmelden, die der ADM-Verwalter in den Konfigurationsdaten eingetragen hat, um Sie als Fernadministrator auszuweisen.

  Wenn Sie sich auf dem Fernadministrations-Server unter einer Benutzerkennung anmelden, die nicht in den Konfigurationsdaten eingetragen ist, dann können Sie den Fernadministrations-Server nur über das FTADM-Protokoll ansprechen. Dies entspricht dem Fall, dass Sie den Auftrag auf einem fernen Rechner stellen, siehe nächster Abschnitt.

- Wenn Sie Aufträge auf einem fernen Rechner stellen, benötigen Sie folgende Daten, die Ihnen der ADM-Verwalter bekannt geben muss:

  – Adresse des Fernadministrations-Servers

  – FTAC-Zugangsberechtigung für den Zugang zum Fernadministrations-Server

  Die Adresse des Fernadministrations-Servers muss immer mit dem Protokoll-Präfix *ftadm://* angegeben werden, z.B. *ftadm://server01*. Daher lassen Sie den Fernadministrations-Server am besten vom FT-Verwalter in die Partnerliste eintragen.

Die Namen der openFT-Instanzen, die Sie administrieren dürfen, können Sie dagegen immer selbst ermitteln, siehe Abschnitt "Namen der openFT-Instanzen ermitteln".

5.1.4.1 Fernadministration über Kommando-Schnittstelle

Wenn Sie für die Fernadministration die Kommando-Schnittstelle verwenden, dann müssen Sie zuerst die Namen der openFT-Instanzen ermitteln, die Sie administrieren dürfen.

Namen der openFT-Instanzen ermitteln

Die Namen der openFT-Instanzen erhalten Sie über das Kommando *ftshwc*. Auf dem Fernadministrations-Server können Sie das Kommando direkt angeben, auf einem fernen Rechner müssen Sie es mit Hilfe des Kommandos *ftadm* "verpacken":

- *ftshwc* auf dem Fernadministrations-Server eingeben:

  ```
  ftshwc –rt=i
  ```

- *ftshwc* auf einem fernen Rechner eingeben:

  ```
  ftadm –cs=server "ftshwc –rt=i" zugangsberechtigung
  ```

  Erläuterung

  server
  : Name des Fernadministrations-Servers aus der Partnerliste oder Adresse des Fernadministrations-Servers im Format *ftadm://host...* .

  zugangsberechtigung
  : FTAC-Zugangsberechtigung für den Zugang zum Fernadministrations-Server. Das zugehörige Profil muss die Eigenschaft ACCESS-TO-ADMINISTRATION besitzen (siehe Seite 122) und der Profilname muss in der Konfigurationsdatei einem Fernadministrator zugeordnet sein (siehe Seite 129).

Beispiel für die Ausgabe

```
TYPE    = *INSTANCE     ACCESS = FT+FTOP+FTAC
   NAME = Muenchen/Jonny
   DESC = Rechner Test-en-lp
TYPE    = *INSTANCE     ACCESS = FTOP
   NAME = Muenchen/Servus
   DESC = Rechner servus
```

NAME gibt den Namen der Instanz an, den Sie beim Fernadministrations-Auftrag genau in dieser Form eingeben müssen. Bei ACCESS sind Ihre Fernadministrations-Rechte für diese Instanz aufgelistet, siehe auch Beschreibung von *ftshwc* auf Seite 298.

Fernadministrations-Auftrag stellen

Sie stellen einen Fernadministrations-Auftrag mit Hilfe des Kommandos *ftadm*.

Die Syntax für den Fernadministrations-Auftrag hängt davon ab, ob Sie das Kommando *ftadm* direkt auf dem Fernadministrations-Server oder auf einem anderen, fernen Rechner eingeben.

- Kommando *ftadm* auf Fernadministrations-Server eingeben

  Melden Sie sich am Fernadministrations-Server unter der Benutzerkennung an, die der ADM-Verwalter in der Konfigurationsdatei als Fernadministrator konfiguriert hat, siehe Attribut *UserID* im Abschnitt „Fernadministratoren definieren“ auf Seite 129.

  Geben Sie das Kommando *ftadm* in folgender Form ein:

  ```
  ftadm –ri=instanz "kommando"
  ```

- Kommando *ftadm* auf fernem Rechner eingeben

  Melden Sie sich auf dem fernen Rechner unter einer beliebigen Benutzerkennung an und geben Sie das Kommando *ftadm* in folgender Form ein:

  ```
  ftadm –cs=server –ri=instanz "kommando" zugangsberechtigung
  ```

Erläuterung

server
: Nur auf fernem Rechner: Name des Fernadministrations-Servers aus der Partnerliste oder Adresse des Fernadministrations-Servers im Format *ftadm://host...* .

instanz
: Routing-Name der openFT-Instanz, auf der das Administrations-Kommando ausgeführt werden soll. Sie müssen ihn genauso angeben wie er beim Kommando *ftshwc* angezeigt wird, siehe Seite 145.

kommando
: Gibt das Administrations-Kommando an, das auf der openFT-Instanz ausgeführt werden soll. *kommando* sollten Sie immer in Anführungszeichen setzen. Wenn *kommando* Leerzeichen oder Sonderzeichen enthält, sind die Anführungszeichen Pflicht. Weitere Details siehe „ftadm - Fernadministrations-Kommando ausführen“ auf Seite 178.

zugangsberechtigung
: Nur auf fernem Rechner: FTAC-Zugangsberechtigung für den Zugang zum Fernadministrations-Server. Das zugehörige Profil muss die Eigenschaft ACCESS-TO-ADMINISTRATION besitzen (siehe Seite 122) und der Profilname muss in der Konfigurationsdatei einem Fernadministrator zugeordnet sein (siehe Seite 129).

5.1.4.2 Fernadministration über openFT Explorer

Im openFT Explorer gibt es im Objektbaum den Punkt *Fernadministration* mit folgendem Symbol:

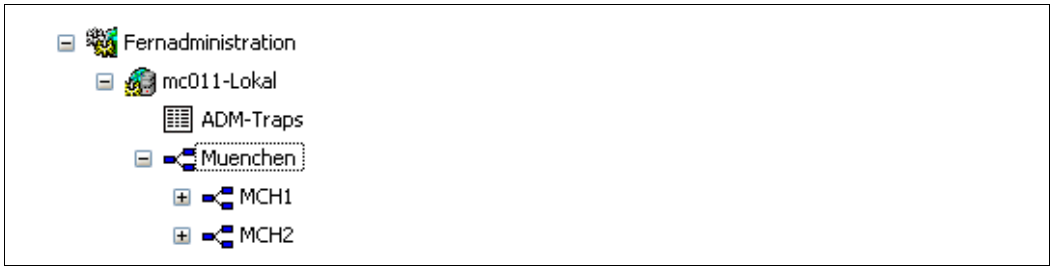
Sie können sich lokal am Fernadministrations-Server anmelden oder die Fernadministration von einem fernen Rechner aus durchführen.

Lokal am Fernadministrations-Server anmelden

Wenn Sie sich lokal auf dem Fernadministrations-Server anmelden und Ihre Benutzerkennung dort als Fernadministrator konfiguriert ist, dann wird im Objektbaum zusätzlich ein Symbol für den lokalen Fernadministrations-Server angezeigt.

Der lokale Fernadministrations-Server hat den Namen *servername*`-Lokal`, wobei *servername* der Rechnername des Fernadministrations-Servers ist.

Wenn Sie auf diesen Knoten klicken, dann werden alle openFT-Instanzen angezeigt, die Sie administrieren dürfen.



Lokaler Fernadministrations-Server

In diesem Beispiel wird die Gruppe *Muenchen* mit den zwei Untergruppen MCH1 und MCH2 angezeigt, die Sie administrieren dürfen.

Fernadministration über fernen Rechner durchführen

Wenn sich der Fernadministrations-Server auf einem anderen Rechner befindet, dann müssen Sie ihn zuerst im openFT Explorer einrichten. Außerdem sollte der FT-Verwalter ihn auch in die Partnerliste eintragen.

Es sind folgende Schritte notwendig:

- Fernadministrations-Server in Partnerliste eintragen

  Der FT-Verwalter trägt den Fernadministrations-Server in folgendem Adressformat in die Partnerliste ein:

  ```
  ftadm://host[:portnummer]
  ```

  portnummer muss nur angegeben werden, wenn auf dem Fernadministrations-Server *host* nicht der ADM-Standardport (11000) verwendet wird. Entsprechendes gilt, wenn Sie als Fernadministrator die Adresse im Fernadministrations-Auftrag direkt angeben.

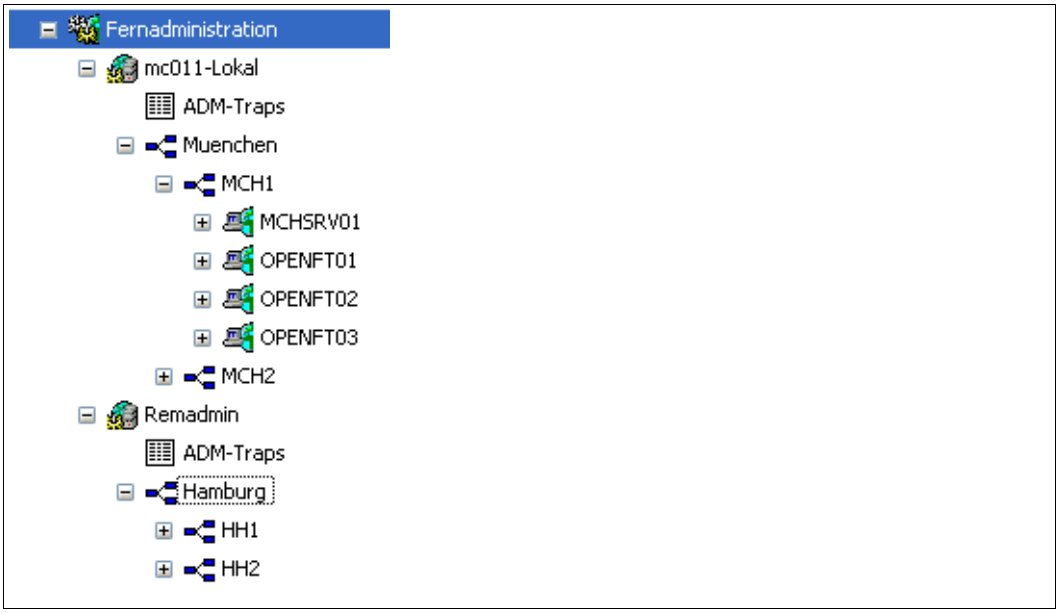
- Fernadministrations-Server im openFT Explorer eintragen

  1. Wählen Sie im Objektbaum beim Objektverzeichnis *Fernadministration* den Kontextmenü-Befehl *Neuer Fernadministrations-Server...* .
  2. Tragen Sie im Dialogfenster *Fernadministrations-Server* Folgendes ein:
     - Den Partner (möglichst den Namen aus der Partnerliste).
     - Die FTAC-Zugangsberechtigung für den Zugang zum Fernadministrations-Server. Das zugehörige Profil auf dem Fernadministrations-Server muss die Eigenschaft ACCESS-TO-ADMINISTRATION besitzen (siehe Seite 122) und der Profilname muss in der Konfigurationsdatei einem Fernadministrator zugeordnet sein (siehe Seite 129).

     Wenn Sie auch die Option *Zugangsberechtigung abspeichern* aktivieren, dann hat dies den Vorteil, dass Sie die Zugangsberechtigung bei künftigten Aufrufen des openFT Explorers nicht jedes Mal angeben müssen.

  Wenn Sie auf *OK* klicken, erscheint im Objektbaum ein neues Symbol mit diesem Fernadministrations-Server.

Per Klick auf den Namen eines Fernadministrations-Servers öffnen Sie das zugehörige Objektverzeichnis. In folgendem Beispiel ist neben dem lokalen Fernadministrations-Server *mc011-Lokal* (siehe Seite 147) ein weiterer Server *Remadmin* eingerichtet.

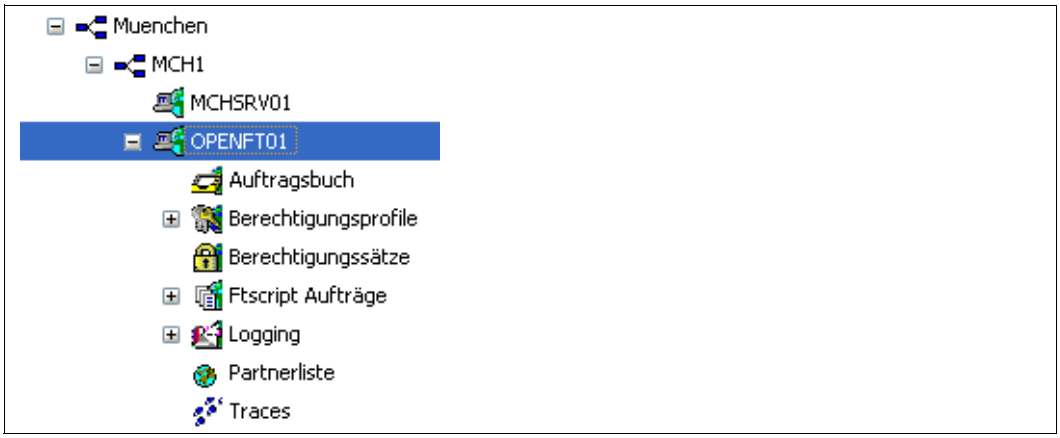


Lokaler und ferner Fernadministrations-Server im openFT Explorer

Fernadministrations-Aufträge stellen

Unter den jeweiligen Gruppen (im Beispiel *Muenchen* und *Hamburg*) werden alle administrierbaren Instanzen aufgeführt. Über das Kontextmenü einer Instanz können Sie auf die Betriebsparameter und die Diagnoseinformationen der Instanz zugreifen und sich die Eigenschaften anzeigen lassen.

Wenn Sie den Teilbaum einer Instanz aufklappen, werden die Symbole für alle Administrationsobjekte der Instanz angezeigt:



Administrationsobjekte einer Instanz im openFT Explorer

Diese Objekte der Instanz (im Beispiel *OPENFT01*) können Sie so administrieren wie Sie es beim lokalen openFT gewohnt sind. Details finden Sie in der Online-Hilfe. Zusätzlich haben Sie über das Objektverzeichnis *Traces* Zugriff auf die Trace-Dateien der Instanz.

5.1.5 Logging der Fernadministration

Bei Fernadministrations-Aufträgen werden in jeder der beteiligten openFT-Instanzen ADM-Logging-Sätze erzeugt.

ADM-Logging-Sätze sind durch einen bestimmten Typ gekennzeichnet (A). Sie werden ähnlich wie FT- oder FTAC-Logging-Sätze behandelt, d.h. Sie können ADM-Logging-Sätze

- mit dem Kommando *ftshwl* ansehen, siehe Abschnitt „ftshwl - Logging-Sätze und Offline-Logging-Dateien anzeigen“ auf Seite 307,
- und mit dem Kommando *ftdell* löschen, sofern Sie die Berechtigung dazu haben, siehe Abschnitt „ftdell - Logging-Sätze oder Offline-Logging-Dateien löschen“ auf Seite 211.

Alternativ dazu können Sie ADM-Logging-Sätze auch über den openFT Explorer ansehen und löschen (Objektverzeichnis *Logging* im Objektbaum).

ADM-Logging steuern

Den Umfang des ADM-Loggings steuern Sie als FT-Verwalter über die Betriebsparameter. Dabei haben Sie folgende Möglichkeiten:

- alle Administrations-Aufträge protokollieren
- modifizierende Administrations-Aufträge protokollieren
- Administrations-Aufträge protokollieren, bei denen Fehler aufgetreten sind
- kein ADM-Logging

Dazu verwenden Sie das Kommando *ftmodo -la* oder den openFT Explorer (Menü *Administration* - *Betriebsparameter*, Registerblatt *Logging*).

5.2 ADM-Traps

ADM-Traps sind kurze Meldungen, die openFT bei bestimmten Ereignissen, die während des openFT-Betriebs eintreten, an einen so genannten **ADM-Trap-Server** schickt. Zu diesen Ereignissen können z.B. fehlerhafte FT-Aufträge, Statuswechsel oder Nichterreichbarkeit von Partnern gehören.

ADM-Traps werden auf dem ADM-Trap-Server dauerhaft gespeichert. Damit lassen sich openFT-Systeme an zentraler Stelle überwachen. Der FT-Verwalter des ADM-Trap-Servers kann sich dabei mittels des openFT Explorers oder des Kommandos *ftshwatp* auf einfache Weise einen Überblick über Ereignisse verschaffen, die auf von ihm überwachten openFT-Instanzen aufgetreten sind.

Wenn der ADM-Trap-Server gleichzeitig auch als Fernadministrations-Server eingesetzt wird, dann können Fernadministratoren ADM-Traps auch von anderen Systemen aus einsehen und damit die Systeme überwachen, die sie administrieren.

5.2.1 ADM-Trap-Server konfigurieren

Damit eine openFT-Instanz als ADM-Trap-Server fungieren kann, müssen Sie als FT-Verwalter folgende Aktionen durchführen:

- Auf dem ADM-Trap-Server muss die Funktion "Fernadministrations-Server" eingeschaltet sein. Dazu geben Sie das Kommando *ftmodo -admcs=y* ein.
  Alternative: Öffnen Sie im openFT Explorer über *Administration* - *Betriebsparameter* das Registerblatt *Adressen* und aktivieren Sie dort die Option *Fernadministrations-Server*.

  Es ist zwar nicht notwendig, dass ein ADM-Trap-Server gleichzeitig auch als Fernadministrations-Server benutzt wird, hat aber den Vorteil, dass sich dann jeder Fernadministrator "seine" ADM-Traps per Fernadministration ansehen kann, siehe Seite 154.

- Im ADM-Trap-Server richten Sie ein Berechtigungsprofil ein, das für die Administrationsfunktion "ADM-Traps empfangen" benutzt werden darf. Dazu verwenden Sie das Kommando *ftcrep* mit Option *-ff=l*.
  Alternative: Öffnen Sie im openFT Explorer im Dialog *Berechtigungsprofil* das Registerblatt *Optionen* und aktivieren Sie die Option *ADM-Traps empfangen.*

  Die Zugangsberechtigung für dieses Profil muss in den Betriebsparametern der openFT-Instanzen eingetragen werden, die die Traps an den ADM-Trap-Server schicken sollen, siehe "ADM-Traps in der openFT-Instanz konfigurieren".

Die ADM-Traps werden in der Datei *sysatpf* abgelegt, die sich im Verzeichnis *log* der jeweiligen openFT-Instanz befindet. Bei der Standardinstanz lautet der Pfadname */var/openFT/std/log/sysatpf*.

Die Datei *sysatpf* wird zyklisch beschrieben, d.h. nach Erreichen einer maximalen Größe wird der jeweils älteste ADM-Trap-Eintrag gelöscht.

ADM-Traps können nicht gezielt gelöscht werden.

5.2.2 ADM-Traps in der openFT-Instanz konfigurieren

Damit eine openFT-Instanz ADM-Traps an den ADM-Trap-Server schicken kann, muss der FT-Verwalter der openFT-Instanz bestimmte Einstellungen in den Betriebsparametern vornehmen, siehe unten. Außerdem muss der asynchrone openFT-Server gestartet sein.

Im Folgenden wird das Vorgehen bei Unix- und Windows-Systemen beschrieben. Die Beschreibung für BS2000/OSD- und z/OS-Systeme finden Sie im jeweiligen openFT-Handbuch "Installation und Administration".

Als FT-Verwalter führen Sie folgende Aktionen durch:

- Im Kommando *ftmodo* geben Sie bei der Option *-atpsv* an:
  - den Namen des ADM-Trap-Servers:
    Der ADM-Trap-Server muss ein ADM-Partner sein, d.h. er muss entweder in der Partnerliste mit dem Adressformat *ftadm://host...* definiert sein oder die Adresse muss direkt im Format *ftadm://host...* angegeben werden.
  - die Zugangsberechtigung für das Berechtigungsprofil, das im ADM-Trap-Server für diesen Zweck definiert ist, siehe Seite 152.
- Im Kommando *ftmodo* legen Sie bei der Option *-atp* fest, bei welchen Ereignissen ADM-Traps an den ADM-Trap-Server gesendet werden sollen:
  - Statuswechsel des asynchronen openFT-Servers
  - Statuswechsel von Partnern
  - Nichterreichbarkeit von Partnern
  - Statuswechsel der Auftragsverwaltung
  - Erfolgreich abgeschlossene Aufträge
  - Fehlgeschlagene Aufträge

  Aus Perfomancegründen sollten Sie den Umfang der ADM-Traps auf das Notwendige beschränken, z.B. auf fehlgeschlagene Aufträge oder Nichterreichbarkeit von Partnern. Wenn z.B. ADM-Traps für alle erfolgreich abgeschlossenen Aufträge von mehreren Instanzen an den ADM-Trap-Server geschickt werden, dann kann dies das lokale openFT-System, den ADM-Trap-Server und das Netz stark belasten.

Alternativ können Sie die Aktionen auch mit dem openFT Explorer durchführen:

1. Öffnen Sie über das Menü *Administration*, Befehl *Betriebsparameter...* das Registerblatt *Traps*.
2. Tragen Sie im Bereich *ADM-Trap-Server* den Namen des ADM-Trap-Servers sowie die Zugangsberechtigung ein.
3. Markieren Sie im Bereich *Typ* in der Spalte *ADM* die Ereignisse, bei denen ADM-Traps gesendet werden sollen.

5.2.3 ADM-Traps ansehen

Der FT-Verwalter des ADM-Trap-Servers ist dazu berechtigt, sich die ADM-Traps anzusehen. Wird der ADM-Trap-Server zusätzlich als Fernadministrations-Server genutzt, dann können sich auch der ADM-Verwalter und die Fernadministratoren ADM-Traps ansehen.

Im Einzelnen gilt:

- Wenn Sie sich als FT-Verwalter oder als ADM-Verwalter auf dem ADM-Trap-Server anmelden, dann können Sie sich alle ADM-Traps ansehen. Sie haben dazu zwei Möglichkeiten:
  - Mit dem Kommando *ftshwatp*. Dabei können Sie nach verschiedenen Kriterien selektieren (Quelle, Zeitraum, Anzahl etc.), Details siehe Abschnitt „ftshwatp - ADM-Traps ausgeben“ auf Seite 291.
  - Mit dem openFT Explorer: Klicken Sie im Objektbaum unter *Administration* auf *ADM-Traps* oder in der Statuszeile im Kontextmenü des Alarmsymbols (sofern vorhanden) auf *ADM-Traps anzeigen*:

    ADM-Traps als FT-Verwalter im openFT Explorer ansehen

    Die Selektionskriterien können Sie über das Kontextmenü einstellen. Die ADM-Traps werden im openFT Explorer in Listenform dargestellt.
    Weitere Details finden Sie in der Online-Hilfe.
- Als Fernadministrator können Sie sich Ihre „eigenen“ ADM-Traps ansehen. Dies sind die ADM-Traps der openFT-Instanzen, für die Sie mindestens die Berechtigung FTOP haben, siehe auch Abschnitt „Namen der openFT-Instanzen ermitteln“ auf Seite 145. Dabei gibt es folgende Möglichkeiten:
  - Wenn Sie sich direkt am Fernadministrations-Server anmelden, dann geben Sie das Kommando *ftshwatp* ein.

Alternative: Klicken Sie im openFT Explorer im Objektbaum unter *Fernadministration* beim lokalen Server auf *ADM-Traps*.

– Wenn Sie sich auf einem fernen Rechner anmelden, dann geben Sie folgendes Kommando ein:

```
ftadm –cs=server "ftshwatp optionen" zugangsberechtigung
```

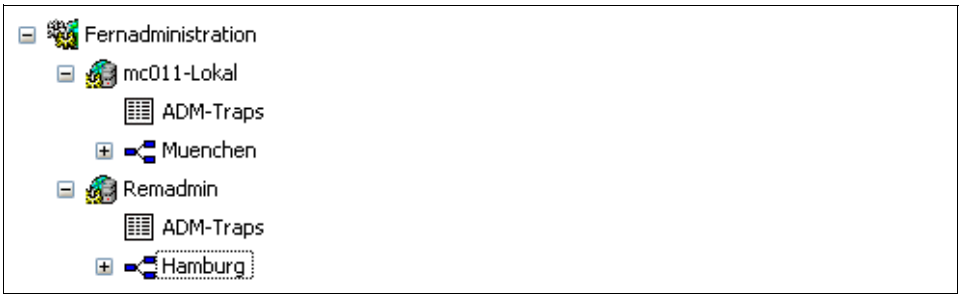
Erläuterung

optionen
: Optionen des Kommandos *ftshwatp*, mit denen Sie die Selektionskriterien für die ADM-Traps und das Ausgabeformat festlegen, siehe Seite 291. Wenn Sie keine Optionen angeben, dann wird der jüngste ADM-Trap in Kurzform ausgegeben.

server
: Name des Fernadministrations-Servers aus der Partnerliste oder Adresse des Fernadministrations-Servers im Format *ftadm://host...*

zugangsberechtigung
: FTAC-Zugangsberechtigung für den Zugang zum Fernadministrations-Server. Das zugehörige Profil muss die Eigenschaft ACCESS-TO-ADMINISTRATION besitzen (siehe Seite 122) und der Profilname muss in der Konfigurationsdatei einem Fernadministrator zugeordnet sein (siehe Seite 129).

Alternative über openFT Explorer: Öffnen Sie im Objektbaum unter *Fernadministration* das Objektverzeichnis des Fernadministrations-Servers und klicken auf *ADM-Traps*, siehe folgendes Bild:



ADM-Traps per Fernadministration im openFT Explorer ansehen

Die Selektionskriterien können Sie über das Kontextmenü einstellen. Die ADM-Traps werden im openFT Explorer in Listenform dargestellt.
Weitere Details finden Sie in der Online-Hilfe.

5.3 Beispiel für eine XML-Konfigurationsdatei

Die Konfiguration der Firma *mycompany* besteht aus vier Rechenzentren, zwei in München (MCH1, MCH2) und zwei in Hamburg (HH1, HH2). Für jedes Rechenzentrum wird eine eigene Untergruppe gebildet. Der Fernadministrationsrechner MCHSRV01 steht in MCH1.

Es werden die vier Fernadministratoren *Hans*, *Fritz*, *Emil* und *Hugo* konfiguriert. Die folgende Tabelle zeigt die Gruppen, Untergruppen und openFT-Instanzen und gibt an, welcher Fernadministrator welche Rechte besitzt.

Gruppe	**Untergruppe**	**Instanz**	**Rechte des Fernadministrators**			
			Hans	**Fritz**	**Emil**	**Hugo**
Muenchen	MCH1	MCHSRV01	FT	FT, FTAC		
		OPENFT01	FT	FT, FTAC		
		OPENFT02	FT	FT, FTAC		
		OPENFT03	FTOP	FT, FTAC		
		MCHSRV02			FT, FTAC	
	MCH2	MCHSRV03	FT, FTAC			
Hamburg	HH1	HHWSRV01			FT, FTAC	FT, FTAC
		HHWSRV02			FT, FTAC	FT, FTAC
		HHWSRV11			FT, FTAC	FT
	HH2	HHWSRV99			FT, FTAC	FTOP

XML-Konfigurationsdatei

Die Konfiguration aus der Tabelle wird über folgende Konfigurationsdatei definiert. Die Ziffern am rechten Rand werden im Anschluss erläutert.

```
<?xml version="1.0" encoding="UTF-8"?>
<Configuration
    Version="1100"
    Description="Konfiguration fuer zentralen Server MCHSRV01">
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:noNamespaceSchemaLocation="/opt/openFT/include/config.xsd">
    <AdministratorID
          Name="Hans"
          Description="Verwalter der Domaenen Controller"
          UserID="rz\hans"                                    1.
          Profile="Profil01"/>                                2.

    <AdministratorID
          Name="Fritz"
          Description="Verwalter der Produktivrechner"
```

```
       UserID="rz\fritz"                                          1.
       Profile="Profil02"/>                                       2.

<AdministratorID
       Name="Emil"
       Description="Verwalter Rechner Personalabteilung in HH"
       Profile="Profil03"/>                                       2.

<AdministratorID
       Name="Hugo"
       Description="Verwalter der QA Rechner in HH"
       Profile="Profil04"/>                                       2.

<Group
       Name="Muenchen"
       Description="Rechenzentrum Muenchen">

   <Group
       Name="MCH1"
       Description="Rechenzentrum Muenchen Schwabing">

       <AccessList>                                               3.
          <AccessEntry
             AdministratorID="Hans"
             AllowFunction="FT"/>
          <AccessEntry
             AdministratorID="Fritz"
             AllowFunction="FT FTAC"/>
       </AccessList>

       <Instance
          Name="MCHSRV01"                                         4.
          Description="Fernadministrations-Server"
          Address="ftadm://MCHSRV01.mch.mycompany.net"
          Admission="mchsrv01remote"/>

       <Instance
          Name="OPENFT01"                                         4.
          Description="Windows XP"
          Address="ftadm://OPENFT01.mch.mycompany.net"
          Admission="openft01remote"/>

       <Instance
          Name="OPENFT02"                                         4.
          Description="Windows XP"
          Address="ftadm://OPENFT02.mch.mycompany.net"
          Admission="openft02remote"/>
```

```
        <Instance
           Name="OPENFT03"                                          4.
           Description="Windows XP"
           Address="ftadm://OPENFT03.mch.mycompany.net"
           Admission="openft03remote">
           <AccessList>                                             5.
              <AccessEntry
                 AdministratorID="Hans"
                 DenyFunction="FTMOD"/>
           </AccessList>
        </Instance>

        <Instance
           Name="MCHSRV02"                                          4.
           Description="SUSE Linux 8.1, Sourceverwaltung"
           Address="ftadm://MCHSRV02.mch.mycompany.net"
           Admission="mchsrv02remote">
           <AccessList                                              5.
              InheritFromParent="No">
              <AccessEntry
                 AdministratorID="Emil"
                 AllowFunction="FT FTAC"/>
           </AccessList>
        </Instance>

     </Group>

     <Group
        Name="MCH2"
        Description="Rechenzentrum in Muenchen Freimann">
        <AccessList                                                 5.
           <AccessEntry
              AdministratorID="Hans"
              AllowFunction="FT FTAC"/>
        </AccessList>

        <Instance
           Name="MCHSRV03"                                          4.
           Description="Windows Server 2003 Domain Controller"
           Address="ftadm://MCHSRV03.mch.mycompany.net"
           Admission="mchsrv03remote">
        </Instance>

     </Group>

  </Group>
```

```
<Group
    Name="Hamburg"
    Description="Rechenzentrum Nord in Hamburg Wandsbek">

    <Group
        Name="HH1"
        Description="QA Rechenzentrum">

        <AccessList>                                          3.
           <AccessEntry
              AdministratorID="Emil"
              AllowFunction="FT FTAC"/>
           <AccessEntry
              AdministratorID="Hugo"
              AllowFunction="FT FTAC"/>
        </AccessList>

        <Instance
           Name="HHWSRV01"                                    4.
           Description="Solaris 10"
           Address="ftadm://HHWSRV01.hhw.mycompany.net"
           Admission="hhwsrv01remote"/>

        <Instance
           Name="HHWSRV02"                                    4.
           Description="HP-11"
           Address="ftadm://HHWSRV02.hhw.mycompany.net"
           Admission="hhwsrv02remote"/>

        <Instance
           Name="HHWSRV11"                                    4.
           Description="Solaris 9"
           Address="HHWSRV11.hhw.mycompany.net"
           Admission="hhwsrv11remote"
           Mode="Legacy">                                     6.
           <AccessList>                                       5.
              <AccessEntry
                 AdministratorID="Hugo"
                 DenyFunction="FTAC"/>
           </AccessList>
        </Instance>

    </Group>
```

```
        <Group
            Name="HH2"
            Description="Personalabteilung">

            <AccessList>                                              3.
               <AccessEntry
                  AdministratorID="Emil"
                  AllowFunction="FT FTAC"/>
               <AccessEntry
                  AdministratorID="Hugo"
                  AllowFunction="FTOP"/>
            </AccessList>

            <Instance
               Name="HHWSRV99"                                        4.
               Description="Mainframe-System (BS2000/OSD)"
               Address="ftadm://HHWSRV99.hhw.mycompany.net"
               Admission="hhwsrv99remote"/>

        </Group>

    </Group>

</Configuration>
```

Erläuterung

1. Benutzerkennung, die auf dem Fernadministrations-Server die angegebenen Administratorrechte hat. Damit kann Fernadministration direkt am Fernadministrations-Server betrieben werden. Wenn hier keine Benutzerkennung angegeben wird, dann ist Fernadministration nur über die FTAC-Zugangsberechtigung möglich (siehe 2).
2. Name des Berechtigungsprofils für den Zugang zum Fernadministrations-Server. Das Profil muss die Funktion ACCESS-TO-ADMINISTRATION besitzen (entspricht *ftcrep -ff=c*). Bei Fernadministration von einem fernen Rechner muss der Fernadministrator die zugehörige FTAC-Zugangsberechtigung angeben.
3. Definiert die Berechtigungen für die ganze Gruppe. Für jeden berechtigten Fernadministrator wird ein <AccessEntry>-Tag angegeben. Diese Berechtigung kann in einer Instanz erweitert oder eingeschränkt werden (siehe 5).
4. Definiert eine Instanz. Im Attribut *Address* kann die komplette Adresse (wie im Beispiel) oder auch der Name aus der Partnerliste angegeben werden. Partner mit openFT ab V11.0 müssen mit *ftadm://...* definiert sein.

   Admission gibt die Zugangsberechtigung auf der zu administrierenden Instanz an. Das zugehörige Berechtigungsprofil muss dort eingerichtet sein und die Funktion REMOTE-ADMINISTRATION besitzen (entspricht *ftcrep -ff=a*).

5. Der <AccessList>-Tag bei einer Instanz definiert Berechtigungen, die nur für diese Instanz gelten:
   - Durch das Attribut *InheritFromParent="No"* wird eine übergeordnete (vererbte) Berechtigung abgeschaltet.
   - Mit dem Attribut *DenyFunction* bei <AccessEntry> werden vererbte Berechtigungen eingeschränkt, z.B. wird das Recht *FT* durch *DenyFunction="FTMOD"* zu *FTOP* reduziert.
   - Mit *AllowFunction* werden Berechtigungen definiert bzw. erweitert.
6. Das Attribut *Mode="Legacy"* gibt an, dass auf der Instanz eine openFT-Version < V11.0 läuft. Die Instanz wird als openFT-Partner adressiert, d.h. die Adresse wird ohne Präfix angegeben. Beim Fernadministrations-Auftrag wird dann intern das Kommando *ftexec* verwendet.

6 openFT-Kommandos für den Verwalter

In diesem Kapitel sind die Kommandos aufgeführt, die nur dem Verwalter zur Verfügung stehen, die dem Verwalter mehr Möglichkeiten als dem Benutzer bieten oder die vorrangig vom Verwalter benutzt werden.

Die Kommandos zur openFT-Script-Schnittstelle sind im Benutzerhandbuch sowie im Handbuch "openFT-Script-Schnittstelle" beschrieben.

6.1 Übersicht über die Kommandos

Die folgende Übersicht zeigt Ihnen aufgabenbezogen alle Kommandos.

Die mit [b] gekennzeichneten Kommandos richten sich in erster Linie an den FT-Benutzer und sind daher nur im Benutzerhandbuch beschrieben.

Für die mit [g] gekennzeichneten Kommandos benötigen Sie ein grafikfähiges Terminal.

openFT verwalten

ftstart	asynchronen openFT-Server starten
ftstop	asynchronen openFT-Server beenden
ftshwo	Betriebsparameter anzeigen
ftmodo	Betriebsparameter ändern
ftlang	Sprachoberfläche einstellen
install.ftam	openFT-FTAM installieren/deinstallieren
install.ftp	openFT-FTP installieren/deinstallieren
ftsetjava	Link auf das Java Executable verwalten
ftshwd	Diagnosesätze ausgeben
fttrace	Trace-Dateien aufbereiten Dieses Kommando ist nicht in diesem Kapitel, sondern in Abschnitt „Trace-Dateien aufbereiten mit fttrace“ auf Seite 394 beschrieben.

Partner verwalten

ftaddptn	Partner in die Partnerliste eintragen
ftshwptn	Eigenschaften von Partnern anzeigen
ftmodptn	Eigenschaften von Partnern ändern
ftremptn	Partner aus der Partnerliste löschen

Schlüsselpaarsätze für die Authentifizierung verwalten

ftcrek	Schlüsselpaarsatz erzeugen
ftimpk	Schlüssel importieren
ftshwk	Eigenschaften von Schlüsseln anzeigen

ftupdk	Öffentliche Schlüssel aktualisieren
ftmodk	Schlüssel modifizieren
ftdelk	Schlüsselpaarsatz löschen

Fernadministration und ADM-Traps

ftadm	Fernadministrations-Kommando eingeben
ftshwc	Fernadministrierbare openFT-Instanzen ausgeben
ftshwatp	ADM-Traps ausgeben
ftexpc	Konfiguration des Fernadministrations-Servers exportieren
ftimpc	Konfiguration des Fernadministrations-Servers importieren

Dateiübertragung und Auftragsverwaltung

ncopy [b] / ftscopy	synchronen Dateiübertragungsauftrag stellen
ft [b] / ftacopy	asynchronen Dateiübertragungsauftrag stellen
ftshwr	Eigenschaften und Zustände von Aufträgen anzeigen
ftalarm	fehlgeschlagene Aufträge melden
ftmodr	Reihenfolge der Aufträge im Auftragsbuch ändern
ftcanr	asynchrone Dateiübertragungsaufträge löschen

Ferne Kommandoausführung

ftexec [b]	Betriebssystemkommandos im fernen System ausführen

Dateimanagement

ftcredir [b]	Ferne Verzeichnisse erzeugen
ftshw [b]	Attribute einer Datei / eines Verzeichnisses im fernen System anzeigen
ftshwf [b]	FTAM-Attribute einer lokalen Datei anzeigen
ftmod [b]	Dateiattribute in einem fernen System ändern
ftmoddir [b]	Attribute ferner Verzeichnisse ändern
ftmodf [b]	FTAM-Attribute einer lokalen Datei ändern
ftdel [b]	Datei in einem fernen System löschen
ftdeldir [b]	Ferne Verzeichnisse löschen

Logging

ftshwl	Logging-Sätze oder Logging-Dateien anzeigen
ftdell	Logging-Sätze oder Logging-Dateien löschen
fthelp	Information zu den Reason-Codes in den Logging-Sätzen ausgeben

FTAC-Funktion

ftcrep	Berechtigungsprofil anlegen
ftshwp	Berechtigungsprofile anzeigen
ftmodp	Berechtigungsprofile ändern
ftdelp	Berechtigungsprofile löschen
ftshwa	Berechtigungssätze anzeigen
ftmoda	Berechtigungssätze ändern
ftexpe	Berechtigungsprofile und -sätze exportieren
ftshwe	Berechtigungsprofile und -sätze aus Datei anzeigen
ftimpe	Berechtigungsprofile und -sätze importieren

Instanzen verwalten

ftcrei	Erzeugen einer Instanz
ftseti [b]	Einstellen einer Instanz
ftshwi [b]	Ausgabe von Informationen über Instanzen
ftmodi	Modifizieren einer Instanz
ftupdi	Instanzdateibaum aktualisieren
ftdeli	Deaktivieren einer Instanz

Messdaten ausgeben

ftshwm	Messwerte des openFT-Betriebs ausgeben
ftmonitor [g]	Messwerte des openFT-Betriebs im openFT Monitor ausgeben

Ausgabe allgemeiner Informationen und sonstige Kommandos

ftinfo [b]	Informationen zum openFT-System ausgeben
ftedit [bg]	lokale oder entfernte Dateien in den openFT Editor laden
ftmsg [bg]	Messagebox auf einem grafischen Display ausgeben
openFT	openFT Explorer starten

[b] Kommando ist nur im Benutzerhandbuch beschrieben
[g] für dieses Kommando benötigen Sie ein grafikfähiges Terminal

Bei den nachfolgend aufgeführten Kommandos können Sie als **Verwalter** mit den zusätzlichen Optionen die entsprechenden Aktionen **systemweit** durchführen. Das heißt im einzelnen:

Mit *ftcanr* können Sie beliebige File Transfer-Aufträge löschen.

Mit *ftcrep* können Sie Berechtigungsprofile für beliebige Kennungen anlegen.

Mit *ftdelp* können Sie beliebige Berechtigungsprofile löschen.

Mit *ftmoda* können Sie beliebige Berechtigungssätze ändern und privilegieren.

Mit *ftmodp* können Sie beliebige Berechtigungsprofile ändern.

Mit *ftmodr* können Sie die Reihenfolge aller Aufträge im Auftragsbuch ändern, unabhängig von der Benutzerkennung.

Mit *ftshwa* können Sie sich beliebige Berechtigungssätze anzeigen lassen.

Mit *ftshwl* können Sie sich beliebige Logging-Sätze anzeigen lassen.

Mit *ftshwp* können Sie sich beliebige Berechtigungsprofile anzeigen lassen.

Mit *ftshwr* können Sie sich über alle Aufträge von allen Benutzerkennungen informieren.

6.2 Syntax der Kommandobeschreibung

Die Darstellung der Kommandosyntax entspricht der Ausgabe, die Sie beim jeweiligen Kommando durch Angabe des Schalters *-h* bekommen. Bei der Darstellung wird folgende Auszeichnung verwendet:

< > spitze Klammern kennzeichnen Parameter, die Sie durch jeweils aktuelle Werte ersetzen. Die spitzen Klammern < > und die erlaubten Wertebereiche dürfen Sie nicht mit angeben.

[ ] steht für Angaben, die Sie weglassen können. Welche Auswirkungen das auf die Funktion des Kommandos hat, finden Sie bei den einzelnen Parametern beschrieben.

␣ steht für mindestens ein Leerzeichen, das Sie zwischen verschiedene Angaben schreiben.

| steht für Alternativen. Sie dürfen nur einen der Werte angeben.

fette Schrift
wird im Abschnitt "Beschreibung" für einzelne Zeichen oder Zeichenketten verwendet, die genau in dieser Form anzugeben sind, z.B. Optionen oder Werte.
Im Fließtext werden diese dann *kursiv* ausgezeichnet.

Längenangaben und Zeichenvorräte

Die Werte, die Sie für Parameter in den Kommandos einsetzen, müssen bestimmte Längenvorgaben und Zeichenvorräte einhalten:

Dateiname
den Dateinamen können Sie absolut oder relativ angeben. Der angegebene Dateiname im lokalen und fernen System darf maximal 512 Zeichen lang sein, wobei die Länge des absoluten Pfadnamens maßgebend ist. Dabei beachten Sie bitte, dass lange Dateinamen zwar an den Schnittstellen von openFT angegeben werden können, jedoch nicht alle Plattformen diese maximale Länge unterstützen. Beispielsweise erlauben Unix-Systeme maximal 512, Windows-Systeme dagegen nur maximal 256 Zeichen.

Enthält der Dateiname Leerzeichen, dann müssen Sie ihn in Anführungszeichen (") einschließen (z.B. "datei name").

Datum
numerisch, genau 8 Zeichen der Form `yyyymmdd` mit:
`yyyy` für Jahr, `mm` für Monat und `dd` für Tag

Grundsätzlich gilt für alle Datumsangaben bei den Kommandos, dass ausschließlich Werte bis einschließlich 20380119 (19. Januar 2038) angegeben werden dürfen.

Benutzerkennung
: Benutzerkennung für den Zugang zum jeweiligen System, maximal 64 Zeichen + 3 Zeichen für sedezimale Eingabe (X' '). Die maximale Länge ist systemabhängig: In Unix-Systemen maximal 32 Zeichen und in den ersten 8 Zeichen eindeutig, in Windows-Systemen maximal 36 Zeichen.

Kommando
: maximal 1000 Zeichen (Ausnahme: *ftadm*). Handelt es sich um Folgeverarbeitungskommandos, dann dürfen die Kommandos für den Erfolgs- und den Fehlerfall zusammen nur 1000 Zeichen lang sein.

Kommandos werden von openFT in Windows-Systemen im Zeichensatz UTF-8 verwaltet. Die maximale Länge von Vor-, Nach- oder Folgeverarbeitungskommandos (1000 Bytes) bezieht sich daher auf die UTF-8-Darstellung des Kommandos. In Unix-Systemen entspricht die Anzahl der Bytes der Anzahl der Zeichen. In Windows-Systemen kann die Anzahl der Bytes hingegen von der Anzahl der Zeichen abweichen, da die Zeichen, die üblicherweise verwendet werden, aber nicht im Zeichensatz ISO646 (ASCII-Zeichen) enthalten sind, in UTF-8 zwei oder drei Bytes lang sind (z.B. das Euro-Zeichen).

Partner
: Name des Partnersystems aus der Partnerliste (1 bis 8 Zeichen lang) oder Adresse des Partnersystems (maximal 200 Zeichen lang). Die Adresse des Partnersystems wird in folgender Form angegeben:

  [protocol://]host[:[port].[tsel].[ssel].[psel]]

  Weitere Einzelheiten siehe Abschnitt „Aufbau der Partneradressen“ auf Seite 68.

Profilname
: alphanumerisch (a..z, A..Z, 0..9), maximal 8 Zeichen

Zugangsberechtigung
: die Zugangsberechtigung besteht in der Regel aus abdruckbaren Zeichen und darf nicht mit Bindestrich anfangen, minimal 8 Zeichen, maximal 67 Zeichen für sedezimale Eingabe. Die maximale Länge ist system-abhängig: in Unix-Systemen maximal 32 und in Windows-Systemen maximal 36 Zeichen. Besteht eine Zugangsberechtigung aus nicht abdruckbaren Zeichen, dann muss sie sedezimal in der Form x\'...\' oder X\'...\' angegeben werden.

Sonderzeichen

Sonderzeichen in den Angaben für *Dateiname, Dateinamen-Präfix*, *Zugangsberechtigung*, *Benutzerkennung*, *Account*, *Kennwort, Folgeverarbeitung* (siehe Angaben zu den Kommandos) müssen Sie durch Gegenschrägstrich (\) entwerten. Sie müssen hierbei zwischen Sonderzeichen für den File Transfer und für das Unix-basierte Betriebssystem unterscheiden und sie entsprechend entwerten.

Beachten Sie, dass die Angaben für Kommandostrings, Dateinamen und frei vergebbare Texte in Hochkommas (') oder Anführungszeichen (") eingeschlossen werden müssen.

Beinhaltet die Angabe zur Folgeverarbeitung ebenfalls Hochkommas ('), dann ist es sinnvoll, die gesamte Angabe in Anführungszeichen (") einzuschließen. Die Hochkommas im Kommando für die Folgeverarbeitung (z.B. die Hochkommas für das Kennwort im BS2000) können dann so geschrieben werden wie sie das Partnersystem (z.B. das BS2000) erwartet.

Beispiel

In der Login-Berechtigung wird die Abrechnungsnummer 1111111,00000000,88888888 angegeben. Das Komma ist ein Sonderzeichen für den File Transfer zur Trennung von *Benutzerkennung*, *Account* und *Kennwort* und muss deshalb hier mit dem Gegenschrägstrich (\) entwertet werden. Dieser Gegenschrägstrich ist wiederum Sonderzeichen für die Shell und muss deshalb ebenfalls entwertet werden. Die Eingabe sieht dann folgendermaßen aus:

"1111111\\,00000000\\,88888888"

Reihenfolge der Angaben

Die Anordnung der Angaben im Kommando ist frei.
Ausgenommen davon sind Angaben, die in der Beschreibung der Kommandosyntax **nicht** mit einem Minuszeichen beginnen, sofern mehr als eine solche Angabe vorliegt (z.B. die Zugangsberechtigung oder das System-Login).

Fortsetzungszeilen

openFT-Kommandos können durch die Vielzahl von Parametern sehr lang werden. Wenn Sie über die Tastatur Kommandos eingeben wollen, die länger als 256 Zeichen sind, müssen Sie mit Fortsetzungszeilen arbeiten. Fortsetzungszeilen erhalten Sie durch die Eingabefolge "\" (Gegenschrägstrich) gefolgt von der Returntaste.

6.3 Ausgabe im CSV-Format

openFT bietet für einige Show-Kommandos eine Ausgabe im CSV-Format an. Das CSV-Format (CSV = **C**haracter **S**eparated **V**alues) ist ein im PC-Umfeld weit verbreitetes Format, das tabellenartige Daten durch Zeilen beschreibt. Ausgabe im CSV-Format wird von folgenden Kommandos angeboten:

- ftshw
- ftshwa
- ftshwatp
- ftshwc
- ftshwe
- ftshwk
- ftshwl
- ftshwm
- ftshwo
- ftshwp
- ftshwptn
- ftshwr

Die Ausgabe im CSV-Format steht außerdem für die openFT-Script-Kommandos *ftshwact* und *ftshws* zur Verfügung, siehe Handbuch "openFT-Script-Schnittstelle".

Viele Programme wie Tabellenkalkulationen, Datenbanken usw. können Daten im CSV-Format importieren. Damit können die Bearbeitungs- und Präsentationsmöglichkeiten dieser Programme auf die Daten angewendet werden.

Die Ausgabefelder sind im Anhang ab Seite 400 beschrieben.

Jeder Datensatz wird als eine Zeile ausgegeben. Ein Datensatz enthält alle Informationen zu einem Objekt. Falls Daten vorhanden sind, enthält die erste Zeile immer die Überschrift mit den Feldnamen der jeweiligen Spalten. **Garantiert werden nur die Feldnamen, nicht die Reihenfolge der Felder in einem Datensatz.** Die Reihenfolge der Felder wird also durch die Reihenfolge der Feldnamen in der Überschriftenzeile bestimmt. Innerhalb einer Ausgabezeile werden Felder durch Strichpunkte (;) voneinander getrennt.

Folgende Datentypen werden in der Ausgabe unterschieden:

Number

String

Da das Zeichen ";" (Semikolon) in der CSV-Ausgabe eine besondere Bedeutung als Feldtrenner hat, wird ein Text für den Fall, dass ein Semikolon darin enthalten ist, in Anführungszeichen (") eingeschlossen. Dies gilt auch für die anderen Sonderzeichen, z.B. auch den Zeilenvorschub.
Schlüsselworte werden grundsätzlich nicht in Anführungszeichen eingeschlossen und beginnen **immer** mit dem Zeichen "*" (Stern).

Date, Time
: Datum und Zeit werden immer in der Form `yyyy-mm-dd hh:mm:ss`, ein Datum alleine in der Form `yyyy-mm-dd` ausgegeben. Die Uhrzeit wird in der Form hh:mm:ss oder nur hh:mm ausgegeben.

Als Beispiel für eine mögliche Auswerteprozedur steht Ihnen eine Formatvorlage im Microsoft-Excel-Format in der Datei */opt/openFT/samples/ftaccnt.xlt*
zur Verfügung.

Diese Vorlage wertet mittels eines automatisch ablaufenden Makros eine CSV-Loggingdatei aus. Als Ergebnis werden die In- und Outbound-Aufträge und die jeweils übertragenen Kilobytes für alle Benutzer angezeigt.

6.4 ftaddptn - Partner in die Partnerliste eintragen

Mit dem Kommando *ftaddptn* tragen Sie ein Partnersystem in die Partnerliste des lokalen Systems ein.

Format

ftaddptn -h |
[<Partnername 1..8>]
-pa=<Partneradresse 1..200>
[-id=<Identifikation 1..64> | -id=]
[-ri=<Routing-Info 1..8> | -ri=@i | -ri=]
[-ptc=i | -ptc=a | -ptc=]
[-sl=1..100 | -sl=p | -sl=]
[-pri=l | -pri=n | -pri=h]
[-st=a | -st=d | -st=ad]
[-ist=a | -ist=d]
[-am=y | -am=n]
[-rqp=p | -rqp=s]
[-tr=n | -tr=f | -tr=]

Beschreibung

-h gibt die Kommandosyntax am Bildschirm aus. Weitere Angaben nach *-h* werden ignoriert.

Partnername
ist der Name, mit dem das Partnersystem in die Partnerliste eingetragen werden soll. Der Name darf aus 1 bis 8 alphanumerischen Zeichen bestehen, das erste Zeichen muss ein Buchstabe sein, Groß-/Kleinschreibung wird nicht unterschieden. Der Name ist frei wählbar und muss nur innerhalb von openFT eindeutig sein.

Partnername nicht angegeben
Gibt an, dass es sich um einen dynamischen Partner handelt.

-pa=Partneradresse
mit *-pa* geben Sie die Adresse des Partnersystems in folgender Form an:

[protocol**://**]host[**:**[port]**.**[tsel]**.**[ssel]**.**[psel]]

host (= Rechnername) muss immer angegeben werden, alle anderen Angaben sind optional.

Weitere Einzelheiten zur Adressangabe finden Sie im Abschnitt „Aufbau der Partneradressen“ auf Seite 68.

-id=Identifikation | **-id=**

Netzweit eindeutige Identifikation der openFT-Instanz im Partnersystem.

Bei FTAM-Partnern kann ein Application Entity Title in der Form *n1.n2.n3.n4..mmm* als Identifikation angegeben werden. *n1*, *n2* usw. sind positive ganze Zahlen, die den "Application Process Title" beschreiben. *n1* kann nur die Werte 0, 1 oder 2 annehmen, *n2* ist auf Werte zwischen 0 und 39 beschränkt, wenn *n1* nicht den Wert 2 hat. Der optionale Application Entity Qualifier *mmm* ist durch zwei Punkte von den Werten des Application Process Title getrennt. Details siehe Benutzerhandbuch zu openFT.

Bei FTP-Partnern darf *-id* nicht angegeben werden!

Identifikation nicht angegeben

Mit *-id=* wird für das openFT- und FTADM-Protokoll *host* (Rechnername) als Identifikation genommen.

Standardwert: *host* (Rechnername) beim openFT- und FTADM-Protokoll, sonst leer.

-ri=Routing-Info | **-ri=@i** | **-ri=**

Wenn das Partnersystem nur über eine Zwischeninstanz erreichbar ist, dann geben Sie mit *Routing-Info* die Adressinformation an, mit der die Zwischeninstanz weiterroutet.

@i für *Routing-Info*

Es wird die in *-id=* angegebene Instanzidentifikation als Routinginformation verwendet.

weder *@i* noch *Routing-Info* angegeben (Standardwert)

Die Angabe von *-ri=* (ohne Parameter) bedeutet, dass das Partnersystem direkt erreichbar ist, d.h. ohne Zwischeninstanz.

-ptc=i | **-ptc=a**

Mit *-ptc* können Sie die Betriebsparameter-Einstellung für die Absenderüberprüfung partnerspezifisch ändern. Diese Einstellungen wirken nur für Partner, die über das openFT-Protokoll verbunden sind und nicht mit Authentifizierung arbeiten (z.B. Partner mit openFT V8.0 oder älter).

i (identification)

Überprüfung der Transportadresse ausschalten. Es wird ausschließlich die Identifikation des Partners geprüft. Die Transportadresse des Partners wird auch dann nicht überprüft, wenn die erweiterte Absenderüberprüfung global eingeschaltet ist (siehe Kommando *ftmodo* auf Seite 236).

a (address)

Überprüfung der Transportadresse einschalten. Die Transportadresse des Partners wird auch dann überprüft, wenn die Überprüfung der Transportadresse global ausgeschaltet ist (siehe Kommando *ftmodo* auf Seite 236).

Stimmt die Transportadresse, unter der sich der Partner anmeldet, nicht mit dem Eintrag in der Partnerliste überein, dann wird der Auftrag abgelehnt.

weder *i* noch *a* angegeben (Standardwert)
-ptc= (ohne Parameter) bedeutet, dass die Betriebsparameter-Einstellung für die Absenderüberprüfung gilt.

-sl=1..100 | **-sl=p** | **-sl=**
Mit dieser Option ordnen Sie dem Partnersystem eine Sicherheitsstufe zu.

Eine niedrige Sicherheitsstufe bedeutet, dass das Schutzbedürfnis gegenüber diesem Partner niedrig ist, weil z.B. seine Identität durch Authentifizierung mit kryptografischen Mitteln überprüft wird und man dadurch sicher sein kann, dass es sich tatsächlich um den betreffenden Partner handelt.

Eine hohe Sicherheitsstufe bedeutet, dass das Schutzbedürfnis gegenüber diesem Partner hoch ist, da die Identität des Partners z.B. nur über seine Adresse ermittelt wird und keine Authentifizierung mit kryptografischen Mitteln stattgefunden hat.

1..100
ordnet dem Partner eine feste Sicherheitsstufe zu. 1 bedeutet die niedrigste und 100 die höchste Sicherheitsstufe.

Es sind alle ganzzahligen Werte von 1 bis 100 erlaubt.

p ordnet dem Partner die Sicherheitsstufe anhand seiner Attribute zu, d.h.:

- Sicherheitsstufe 10, wenn der Partner authentifiziert ist.
- Sicherheitsstufe 90, wenn der Partner im Transportsystem bekannt ist und über seinen im Transportsystem bekannten Namen identifiziert wird.
- Sicherheitsstufe 100, wenn der Partner nur über seine Adresse identifiziert wird.

Sicherheitsstufe nicht angegeben (Standardwert)
-sl= (ohne Parameter) bedeutet, dass die Betriebsparameter-Einstellung für die Sicherheitsstufe gilt (siehe Kommando *ftmodo* auf Seite 236).

-pri=l | **-pri=n** | **-pri=h**
Mit *-pri* legen Sie die Priorität eines Partners bezüglich der Abarbeitung von Aufträgen mit gleicher Auftragspriorität fest. D.h. die Partnerpriorität kommt nur unter Aufträgen zum Tragen, die dieselbe Auftragspriorität haben, aber zu Partnern mit unterschiedlicher Partnerpriorität gehen.

l (low)
Der Partner erhält eine niedrige Priorität.

n (normal, Standardwert)
Der Partner erhält eine normale Priorität.

h (high)
Der Partner erhält eine hohe Priorität.

-st=a | **-st=d** | **-st=ad**
Mit dieser Option können Sie steuern, wie lokal gestellte asynchrone Dateiübertragungsaufträge an das angegebene Partnersystem bearbeitet werden.

a (active, Standardwert)
Lokal gestellte asynchrone Dateiübertragungsaufträge an dieses Partnersystem werden bearbeitet, wenn der asynchrone openFT-Server gestartet ist.

d (deactivated)
Lokal gestellte asynchrone Dateiübertragungsaufträge an dieses Partnersystem werden zunächst nicht bearbeitet, sondern nur im Auftragsbuch abgelegt.

ad (automatic deactivation)
Mehrere direkt aufeinander folgende fehlgeschlagene Verbindungsaufbauversuche zu diesem Partnersystem führen zu dessen Deaktivierung. Um wieder File Transfer mit diesem Partnersystem betreiben zu können, muss es explizit mit *ftmodptn -st=a* aktiviert werden.

Die maximale Anzahl solcher Fehlversuche beträgt 5, nach einem erfolgreichen Verbindungsaufbau wird der Zähler wieder auf 0 gesetzt.

-ist=a | **-ist=d**
Mit dieser Option steuern Sie, wie fern gestellte Dateiübertragungsaufträge vom angegebenen Partnersystem bearbeitet werden.

a (active, Standardwert)
Fern gestellte Dateiübertragungsaufträge von diesem Partnersystem werden bearbeitet, wenn der asynchrone openFT-Server gestartet ist.

d (deactivated)
Fern gestellte synchrone Dateiübertragungsaufträge von diesem Partnersystem werden abgelehnt. Fern gestellte asynchrone Dateiübertragungsaufträge von diesem Partner bleiben dort gespeichert und können erst dann bearbeitet werden, wenn dieser Partner mit *-ist=a* wieder aktiv gesetzt ist.

-am=n | **-am=y**
Mit dieser Option können Sie die Authentifizierung eines Partners erzwingen.

n (Standardwert)
Die Authentifizierung wird nicht erzwungen, d.h. dieser Partner ist bezüglich Authentifizierung nicht eingeschränkt.

y Die Authentifizierung wird erzwungen, d.h. Aufträge werden nur bearbeitet, wenn das lokale System den Partner erfolgreich authentifizieren kann, siehe Seite 78.

-rqp=p | **-rqp=s**
Mit dieser Option (rqp = request processing) steuern Sie, ob asynchrone Outbound-Aufträge zu diesem Partner grundsätzlich seriell durchgeführt werden oder ob parallele Verbindungen erlaubt sind.

p (parallel, Standardwert)
Parallele Verbindungen zu diesem Partner sind erlaubt.

s (seriell)
Parallele Verbindungen zu diesem Partner sind nicht erlaubt. Wenn mehrere Dateiübertragungsaufträge zu diesem Partnersystem anstehen, dann werden sie seriell abgearbeitet. Ein Folgeauftrag wird erst gestartet, wenn der vorausgegangene Auftrag beendet ist.

-tr=n | **-tr=f** | **-tr=**
Mit dieser Option können Sie die Betriebsparameter-Einstellungen für die Partner-Selektion der openFT-Überwachungsfunktion partnerspezifisch ändern.

n (on)
Die Überwachungsfunktion ist für diesen Partner eingeschaltet. Es wird jedoch nur dann ein Trace geschrieben, wenn auch die openFT-Überwachungsfunktion per Betriebsparameter eingeschaltet ist. In diesem Fall hat diese Einstellung bei *ftaddptn* Vorrang gegenüber der Partnerselektion für die Überwachungsfunktion in den Betriebsparametern, siehe auch Seite 236ff, *ftmodo*, Optionen *-tr.* und *-trp*.

f (off)
Die Überwachungsfunktion ist für diesen Partner ausgeschaltet.

weder *n* noch *f* angegeben (Standardwert)
-tr= (ohne Parameter) bedeutet, dass die globale Einstellung für die Partner-Selektion der openFT-Überwachungsfunktion gilt (siehe Kommando *ftmodo* auf Seite 236).

6.5 ftadm - Fernadministrations-Kommando ausführen

Mit dem Kommando *ftadm* administrieren Sie als Fernadministrator eine openFT-Instanz über einen Fernadministrations-Server. Der Fernadministrations-Server nimmt den Administrations-Auftrag entgegen, prüft die Berechtigung und leitet den Auftrag an die zu administrierende openFT-Instanz weiter.

Außerdem können Sie als Fernadministrator mit *ftadm* noch folgende Informationen vom Fernadministrations-Server abfragen, siehe Abschnitt „Fernadministrations-Kommandos“ auf Seite 185:

– Sie können ermitteln, für welche openFT-Instanzen Sie administrationsberechtigt sind und welche Fernadministrations-Rechte Sie für diese Instanzen haben.

– Sie können die ADM-Traps lesen, welche die von Ihnen administrierten openFT-Instanzen an den Fernadministrations-Server gesendet haben. Voraussetzung ist, dass der Fernadministrations-Server gleichzeitig als ADM-Trap-Server für die administrierten openFT-Instanzen konfiguriert ist. Details siehe Abschnitt „ADM-Traps“ auf Seite 152.

Format

ftadm -h |
[-c]
[-cs=<Partner 1..200>]
[-ri=<Routing-Info 1..200>]
<Kommando 1..8192> | -
[<Zugangsberechtigung 8..67> | @d]

Beschreibung

-h gibt die Kommandosyntax am Bildschirm aus. Weitere Angaben nach *-h* werden ignoriert.

-c Gibt an, ob die Nutzdaten (d.h. Kommando und Kommandoausgabe) verschlüsselt übertragen werden sollen. Die Angabe von *-c* ist nur möglich, wenn openFT-CR installiert ist. Ist openFT-CR nicht installiert, dann wird *-c* in der Kommandosyntax (*-h*) unterdrückt und die Angabe von *-c* führt zu einem Syntaxfehler.

-cs=Partner
Gibt den Namen des Fernadministrations-Servers in der Partnerliste oder die Adresse des Fernadministrations-Servers an. Der Fernadministrations-Server muss als ADM-Partner adressiert werden, Details siehe Abschnitt „Aufbau der Partneradressen“ auf Seite 68.

-cs nicht angegeben

Wenn Sie *-cs* nicht angeben, dann wird das lokale System als Fernadministrations-Server angenommen, d.h. das System, auf dem Sie sich angemeldet haben. Daher dürfen Sie *-cs* nur dann weglassen, wenn Sie *ftadm* direkt auf dem Fernadministrations-Server eingeben.

-ri=Routing-Info

Gibt den Pfadnamen der openFT-Instanz an, die Sie administrieren möchten. Der Pfadname wird vom ADM-Verwalter auf dem Fernadministrations-Server konfiguriert und wird dazu benötigt, den Fernadministrations-Auftrag an die openFT-Instanz weiterzuleiten. Sie können den Pfadnamen ermitteln, indem Sie das Kommando *ftshwc* auf dem Fernadministrations-Server ausführen, siehe Abschnitt „Fernadministrations-Kommandos“ auf Seite 185.

-ri nicht angegeben

Wenn Sie *-ri* nicht angeben, dann wird das in *Kommando* angegebene Kommando auf dem Fernadministrations-Server ausgeführt, z.B. *ftshwc* oder *ftshwatp*, siehe Abschnitt „Fernadministrations-Kommandos“ auf Seite 185.

Kommando

Das auszuführende Fernadministrations-Kommando. Die maximal unterstützte Kommandolänge beträgt 8192 Zeichen.

- (Bindestrich) für *Kommando*

Der Bindestrich steht für die Standardeingabe *stdin*, d.h. Sie geben das Kommando von der Tastatur ein. Die Eingabe beenden Sie mit <END> bzw. CTRL+D.

Bei einer dunkelgesteuerten Eingabe (*@d*) für *Zugangsberechtigung* wird zuerst die Zugangsberechtigung abgefragt, anschließend geben Sie das Kommando ein.

Zugangsberechtigung | **@d**

FTAC-Zugangsberechtigung für den Zugang zum Fernadministrations-Server. Die Angabe der Zugangsberechtigung ist obligatorisch, wenn Sie *-cs* angegeben haben, und darf nicht angegeben werden, wenn Sie *-cs* nicht angegeben haben.

@d für *Zugangsberechtigung*

Wenn Sie *@d* (dunkelgesteuert) angeben, wird die Zugangsberechtigung nach Abschicken des Kommandos am Bildschirm abgefragt. Die Eingabe bleibt unsichtbar, um zu verhindern, dass Unbefugte die Zugangsberechtigung sehen.

Zugangsberechtigung nicht angegeben

Wenn Sie keine FTAC-Zugangsberechtigung angeben, dann gibt es zwei mögliche Situationen:

- Wenn Sie gleichzeitig *-cs* angeben, dann wird die Zugangsberechtigung nach Abschicken des *ftadm*-Kommandos am Bildschirm abgefragt.
- Wenn Sie *-cs* nicht angeben, d.h. *ftadm* auf dem Fernadministrations-Server eingeben, dann wird Ihre Benutzerkennung als Berechtigungsnachweis für die Fernadministration verwendet.

6.5.1 Fernadministrations-Kommandos

In den folgenden Tabellen sind die möglichen Fernadministrations-Kommandos auf den einzelnen openFT-Plattformen sowie auf dem Fernadministrations-Server aufgelistet. Die Spalte Berechtigung gibt die Berechtigung an, die notwendig ist, um das Kommando als Fernadministrations-Kommando ausführen zu können. Es gibt folgende Berechtigungen:

FTOP	lesende FT-Zugriffe (FT-Operator)
FT	lesende und modifizierende FT-Zugriffe (FT-Verwalter)
FTAC	lesende und modifizierende FTAC-Zugriffe (FTAC-Verwalter)

Wenn mehrere Berechtigungen angegeben sind, z.B. FT | FTAC, dann reicht es, wenn eine dieser Berechtigungen zutrifft, also FT oder FTAC.

Beim Fernadministrations-Auftrag werden diese Berechtigungen gegen die Rechte abgeglichen, die Sie als Fernadministrator für die betreffende Instanz besitzen. Die Rechte legt der ADM-Verwalter in den Konfigurationsdaten des Fernadministrations-Servers fest.

Wenn Ihre Rechte nicht ausreichen, um das Fernadministrations-Kommando für eine bestimmte Instanz auszuführen, dann wird der Auftrag zurückgewiesen, z.B. mit:

```
ftadm: Administrationsauftrag vom Fernadministrations-Server zurueckgewiesen
```

In diesem Fall wird auf dem Fernadministrations-Server ein ADM-Logging-Satz mit einem Reason-Code ungleich 0000 geschrieben. Der Reason-Code gibt den genauen Ablehnungsgrund an (*fthelp reason-code*).

Kommandos für openFT-Partner im BS2000

Die Kommandos müssen immer mit "/" (Schrägstrich) vor dem Kommandonamen eingegeben werden.

BS2000-Kommando	Kurzformen und Aliasnamen	Berechtigung
ADD-FT-PARTNER	ADD-FT-PART FTADDPTN	FT
CANCEL-FILE-TRANSFER	CAN-FILE-T, CNFT NCANCEL, NCAN FTCANREQ	FT
CREATE-FT-KEY-SET	CRE-FT-KEY FTCREKEY	FT
CREATE-FT-PROFILE	CRE-FT-PROF	FTAC
DELETE-FT-KEY-SET	DEL-FT-KEY FTDELKEY	FT
DELETE-FT-LOGGING-RECORDS	DEL-FT-LOG-REC FTDELLOG	FT | FTAC
DELETE-FT-PROFILE	DEL-FT-PROF	FTAC
IMPORT-FT-KEY [2)]	IMP-FT-KEY FTIMPKEY	FT
MODIFY-FILE-TRANSFER	MOD-FILE-T FTMODREQ	FT
MODIFY-FT-ADMISSION-SET	MOD-FT-ADM	FTAC
MODIFY-FT-KEY [2)]	MOD-FT-KEY FTMODKEY	FT
MODIFY-FT-OPTIONS	MOD-FT-OPT FTMODOPT	FT
MODIFY-FT-PARTNER	MOD-FT-PART FTMODPTN	FT
MODIFY-FT-PROFILE	MOD-FT-PROF	FTAC
REMOVE-FT-PARTNER	REM-FT-PART FTREMPTN	FT
SHOW-FILE-TRANSFER	SHOW-FILE-T, SHFT NSTATUS, NSTAT, FTSHWREQ	FT | FTOP
SHOW-FT-ADMISSION-SET	SHOW-FT-ADM-S	FTAC
SHOW-FT-DIAGNOSTIC	SHOW-FT-DIAG FTSHWD	FT | FTOP | FTAC
SHOW-FT-INSTANCE	SHOW-FT-INST	FT | FTOP
SHOW-FT-KEY [2)]	FTSHWKEY	FT | FTOP

BS2000-Kommando	Kurzformen und Aliasnamen	Berechtigung
SHOW-FT-LOGGING-RECORDS	SHOW-FT-LOG-REC FTSHWLOG	FT | FTOP | FTAC
SHOW-FT-MONITOR-VALUES [1)]	SHOW-FT-MON-VAL FTSHWMON	FT | FTOP
SHOW-FT-OPTIONS	SHOW-FT-OPT FTSHWOPT	FT | FTOP
SHOW-FT-PARTNERS	SHOW-FT-PART FTSHWPTN	FT | FTOP
SHOW-FT-PROFILE	SHOW-FT-PROF	FTAC
START-FTTRACE	FTTRACE	FT | FTOP
STOP-FT	FTSTOP	FT
UPDATE-FT-PUBLIC-KEYS	UPD-FT-PUB-KEY FTUPDKEY	FT

[1)] Ab V11.0

[2)] Ab V12.0

Kommandos für openFT-Partner im z/OS

z/OS-Kommando	Aliasnamen	Berechtigung
FTADDPTN		FT
FTCANREQ	NCANCEL, NCAN	FT
FTCREKEY		FT
FTCREPRF		FTAC
FTDELKEY		FT
FTDELLOG		FT | FTAC
FTDELPRF		FTAC
FTHELP		FT | FTOP | FTAC
FTIMPKEY [2)]		FT
FTMODADS		FTAC
FTMODKEY [2)]		FT
FTMODOPT		FT
FTMODPRF		FTAC
FTMODPTN		FT
FTMODREQ		FT
FTREMPTN		FT
FTSHWADS		FTAC
FTSHWD		FT | FTOP | FTAC
FTSHWKEY [2)]		FT | FTOP
FTSHWINS		FT | FTOP
FTSHWLOG		FT | FTOP | FTAC
FTSHWMON [1)]		FT | FTOP
FTSHWNET		FT | FTOP
FTSHWOPT		FT | FTOP
FTSHWPRF		FTAC
FTSHWPTN		FT | FTOP
FTSHWREQ	NSTATUS, NSTAT	FT | FTOP
FTSTOP		FT
FTTRACE		FT | FTOP
FTUPDKEY		FT

[1)] Ab V11.0

[2)] Ab V12.0

Kommandos für openFT-Partner in Unix- und Windows-Systemen

Kommando	Bemerkung	Berechtigung
fta	bis V10.0	FT
ftaddlic	nur Windows-Systeme ab V12.0	FT
ftaddptn		FT
ftc	bis V10.0	FT
ftcanr		FT
ftcans	openFT-Script-Kommando	FT
ftcrek		FT
ftcrep		FTAC
ftdelk		FT
ftdell		FT | FTAC
ftdelp		FTAC
ftdels	openFT-Script-Kommando	FT
fthelp		FT | FTOP | FTAC
fti	bis V10.0	FT | FTOP
ftimpk	ab V12.0	FT
ftinfo		FT | FTOP | FTAC
ftmoda		FTAC
ftmodk	ab V12.0	FT
ftmodo		FT
ftmodp		FTAC
ftmodptn		FT
ftmodr		FT
ftremlic	nur Windows-Systeme ab V12.0	FT
ftremptn		FT
ftrs	bis V10.0	FT
ftsetpwd	nur Windows-Systeme	FT | FTOP
ftshwa		FTAC
ftshwact	openFT-Script-Kommando	FT | FTOP
ftshwd		FT | FTOP | FTAC
ftshwi		FT | FTOP
ftshwk	ab V12.0	FT | FTOP
ftshwl		FT | FTOP | FTAC

Kommando	Bemerkung	Berechtigung
ftshwlic	nur Windows-Systeme ab V12.0	FT
ftshwm	ab V11.0	FT | FTOP
ftshwo		FT | FTOP
ftshwp		FTAC
ftshwptn		FT | FTOP
ftshwr		FT | FTOP
ftshws	openFT-Script-Kommando	FT | FTOP
ftstop		FT
fttrace		FT | FTOP
ftupdk		FT

Kommandos auf dem Fernadministrations-Server

Mit *ftadm* können Sie auf dem Fernadministrations-Server die Kommandos *ftshwc* und *ftshwatp* ausführen. Dabei dürfen Sie die Option *-ri* nicht angeben:

Kommando	Bemerkung	Berechtigung
ftshwc	Ermittelt die Instanzen, die der Fernadministrator administrieren darf	FT | FTOP | FTAC (d.h. alle Instanzen werden angezeigt, für die der Fernadministrator eine dieser Berechtigungen besitzt)
ftshwatp	Gibt die ADM-Traps der administrierbaren openFT-Instanzen aus	FT | FTOP (d.h. es werden ADM-Traps von all denjenigen Instanzen angezeigt, für die der Fernadministrator eine dieser Berechtigungen besitzt)

6.6 ftalarm - fehlgeschlagene Aufträge melden

Das *ftalarm*-Kommando dient dazu, einen Alarm auszulösen, wenn innerhalb von zwei Minuten mehr als eine vom Benutzer wählbare Anzahl von FT-Aufträgen fehlgeschlagen ist. Die fehlerhaften FT-Aufträge werden anhand eines Returncodes ungleich 0 bei FTAC-Logging-Sätzen identifiziert. *ftalarm* benutzt die *cron*-Funktionen.

Für jede Instanz ist ein eigener Aufruf *ftalarm* erforderlich.
Dazu gehen Sie wie folgt vor: Aktivieren Sie die Instanz mit *ftseti* und rufen Sie *ftalarm* auf.

Wird *ftalarm* auf Solaris über SMF gestartet, dann wird vom händischen Start des ftalarm Kommandos abgeraten, da SMF eine Änderung nicht erfährt. *ftalarm* ist für SMF ein sogenannter transienter Dienst, d.h. es gibt keinen überwachbaren Prozess.

Format

ftalarm [-h |
-s <number of errors 1..99999999> |
-t]

Beschreibung

-h gibt die Kommandosyntax am Bildschirm aus. Weitere Angaben nach *-h* werden ignoriert.

-s number of errors
startet die *ftalarm*-Funktion. Beim Erreichen und Überschreiten der angegebenen Anzahl *number of errors* von fehlerhaften FTAC-Logging-Sätzen innerhalb von zwei Minuten wird an der Konsole und in die Datei *conslog* folgende Meldung ausgegeben:

```
openFTalarm: Anzahl or more access control error loggings within 2
minutes
```

Der Teilstring *openFTalarm:* innerhalb dieser Meldung wird von openFT auch für weitere Versionen garantiert und kann von Systemmanagement-Tools zur automatischen Bearbeitung ausgewertet werden.

Die Meldungen werden von der cron-Funktion in einem festen Zeitraster ausgegeben und können sich daher beim Einschalten der *ftalarm*-Funktion bis zu einer Minute verzögern.

conslog liegt im Verzeichnis *log* der jeweiligen openFT-Instanz. Bei der Standardinstanz lautet der Pfadname */var/openFT/std/log/conslog*.

-t beendet die *ftalarm*-Funktion.

6.7 ftcanr - asynchrone Aufträge löschen

Mit dem *ftcanr*-Kommando löschen Sie asynchrone Aufträge, die bereits bearbeitet werden oder noch im Auftragsbuch auf die Bearbeitung warten. Als Benutzer können Sie nur Aufträge löschen, die unter Ihrer eigenen Benutzerkennung eingetragen sind.

Als Verwalter können Sie beliebige Aufträge löschen. Außerdem können Sie als Verwalter Aufträge bedingungslos löschen, d.h. ohne Aushandlung mit dem Partnersystem.

Bei bereits gestarteten Dateiübertragungsaufträgen kann sich die Zieldatei in einem undefinierten Zustand befinden.

Format

```
ftcanr  -h  |
        [ -f ]
        [ -ua=<Benutzerkennung 1..32> | @a ]
        [ -ini=l | -ini=r | -ini=lr | -ini=rl ]
        [ -pn=<Partner 1..200> ]
        [ -fn=<Dateiname 1..512> ]
          <Auftrags-Id 1..2147483647> [<Auftrags-Id 1..2147483647> ...] | @a
```

Beschreibung

-h gibt die Kommandosyntax am Bildschirm aus. Weitere Angaben nach *-h* werden ignoriert.

-f Mit *-f* löschen Sie einen Auftrag bedingungslos aus dem lokalen Auftragsbuch, d.h. ohne Aushandlung mit dem Partnersystem. Beachten Sie, dass dadurch im Auftragsbuch des Partners Aufträge ohne definierten Zustand entstehen können.

Diese Option können Sie nur als FT-Verwalter aufrufen. Voraussetzung ist, dass der Auftrag zuvor mit *ftcanr* ohne Option *-f* abgebrochen wurde.

-ua=Benutzerkennung | **@a**

Mit *-ua* legt man fest, für welche Benutzerkennung Aufträge gelöscht werden sollen.

Benutzerkennung

Als FT-Verwalter dürfen Sie hier jede beliebige Benutzerkennung angeben.

@a Diese Option ist nur für den FT-Verwalter sinnvoll. Als FT-Verwalter können Sie durch Angabe von *@a* Aufträge aller Benutzerkennungen löschen.

-ua= nicht angegeben

Die eigene Benutzerkennung ist das Auswahlkriterium.
Ausnahme: Der FT-Verwalter hat das Kommando aufgerufen und dabei auch Auftrags-Ids angegeben: in diesem Fall ist die Voreinstellung *@a*.

-ini=l | **-ini=r** | **-ini=lr** | **-ini=rl**
: Mit *-ini* legen Sie fest, für welche Initiatorseite Sie Aufträge löschen wollen. Sie können angeben: l, r, lr, rl

  l Nur lokal gestellte Aufträge werden gelöscht.

  r Nur fern gestellte Aufträge werden gelöscht.

  lr, rl Sowohl lokale als auch fern gestellte Aufträge werden gelöscht

-ini nicht angegeben
: Der Initiator ist nicht Auswahlkriterium (entspricht *lr* bzw. *rl*).

-pn=Partner
: Mit *-pn* können Sie das Partnersystem angeben, für das Sie Aufträge löschen wollen. *Partner* ist der Name oder die Adresse des Partnersystems. Sie sollten den Partner in der gleichen Form angeben wie bei der Auftragsvergabe oder der Ausgabe des Kommandos *ftshwr*.

-fn=Dateiname
: Mit *-fn* legen Sie fest, für welchen Dateinamen Aufträge gelöscht werden sollen. Es werden Aufträge gelöscht, die im lokalen System auf diese Datei zugreifen.
  Es muss der Dateiname angegeben werden, der bei der Auftragserstellung verwendet wurde. Der Dateiname wird auch beim *ftshwr*-Kommando ausgegeben. Wildcards im Dateinamen sind nicht erlaubt.

Auftrags-Id1 [Auftrags-Id2] [Auftrags-Id3] ... | **@a**
: Für *Auftrags-Id* geben Sie die Identifikation des Auftrags an, der gelöscht werden soll (mit oder ohne führende Nullen). Die *Auftrags-Id* erhalten Sie bei der Bestätigung der Auftragsannahme am Bildschirm oder über das Kommando *ftshwr*, falls Sie sie vergessen haben. Sie können auch mehrere Auftrags-Identifikationen gleichzeitig angeben.
  Werden zusätzlich zur *Auftrags-Id* weitere Auswahlkriterien angegeben, so wird ein Auftrag mit einer ausgewählten *Auftrags-Id* nur dann gelöscht, wenn auch die anderen Bedingungen erfüllt sind.

  @a für *Auftrags-Id*
  : Mit *@a* werden alle Aufträge ausgewählt.

Falls Auftrags-Ids angegeben wurden und die übrigen angegebenen Auswahlkriterien nicht zu dem Auftrag passen, wird der Auftrag nicht gelöscht und es erscheint die folgende Fehlermeldung:

`ftcanr: Auftrag` *Auftrags-Id* `nicht gefunden`

Auftrags-Id ist die Identifikation des letzten nicht passenden Auftrags.

Beispiele

1. Der asynchrone Auftrag mit der Auftrags-Identifikation 65546 soll gelöscht werden.

   ```
   ftcanr␣65546
   ```

2. Es sollen alle lokalen Aufträge zum Partner *ux1* gelöscht werden, die die Datei *file1* betreffen.

   ```
   ftcanr -pn=ux1 -fn=file1 -ini=l @a
   ```

6.8 ftcrei - Erzeugen bzw. Aktivieren einer Instanz

Mit dem Kommando *ftcrei* können Sie eine neue Instanz erzeugen oder eine deaktivierte Instanz wieder zuschalten.

Wenn eine Instanz erzeugt wird, wird der Instanzdateibaum mit den Betriebsmitteln einer Instanz in das Verzeichnis */var/openFT* gelinkt.

Falls der angegebene Instanzdateibaum noch nicht existiert, wird er erzeugt.

Beim Erzeugen des Instanzdateibaums werden die Betriebsparameter, die Startup- und Shutdown-Datei (nicht bei Solaris mit SMF) und die Profildateien wie bei einer Neuinstallation initialisiert. Bei Solaris mit SMF wird ein Manifest erzeugt und in SMF eingetragen, siehe Abschnitt „Solaris SMF“ auf Seite 41.

Wenn der Instanzdateibaum schon existiert, prüft *ftcrei* die Version. Wurde der Instanzdateibaum mit einer älteren openFT-Version erzeugt, muss er zunächst mit dem Kommando *ftupdi* aktualisiert werden, bevor die Instanz wieder aktiviert werden kann.

Wichtige Hinweise zur Nutzung mehrerer Instanzen

– Die Nutzung von mehreren openFT-Instanzen ist nur mit dem Transportsystem TCP/IP möglich. Wenn Sie mehrere Instanzen einsetzen möchten und mit CMX und eingeschaltetem TNS arbeiten (*ftmodo -cmx=y -tns=y*), dann müssen Sie alle openFT-spezifischen TNS-Einträge löschen, die nicht TCP/IP betreffen (also alles außer LANINET und RFC1006).

– Sie müssen allen Instanzen mit *-addr=* explizit eine eigene Adresse zuordnen.

– Wenn die Instanz in Partnersystemen authentifiziert werden soll, muss ihr eine eindeutige Instanzidentifikation zugeordnet werden (mit *ftmodo -id=*). Außerdem muss den Partnersystemen ein öffentlicher Schlüssel der Instanz zur Verfügung gestellt werden.

Format

ftcrei -h |
<Instanz 1..8> [<Verzeichnis 1..128>][-addr=<Hostname>]

Beschreibung

-h gibt die Kommandosyntax am Bildschirm aus. Weitere Angaben nach *-h* werden ignoriert.

Instanz
: Name der Instanz, die erzeugt werden soll.
Instanznamen haben eine maximale Länge von 8 Zeichen. Erlaubte Zeichen sind A-Z, a-z und 0-9, wobei das erste Zeichen nicht numerisch sein darf.

  Der Name der Instanz darf nicht mit der Instanzidentifikation verwechselt werden (siehe *ftmodo -id=*).

Verzeichnis
: Verzeichnis, in dem der Instanzdateibaum liegen soll. Das Verzeichnis darf noch nicht existieren.

  Wenn Sie *Verzeichnis* nicht angeben, wird der Instanzdateibaum standardmäßig angelegt in:

  `/var/openFT/.`*Instanz*

-addr=Hostname
: Internet-Hostname, mit dem die Instanz angesprochen wird. Wenn Ihr System einen DNS-Namen hat, sollten Sie hier den vollen DNS-Namen angeben. Die ersten 8 Zeichen des ersten Namensteiles (Hostname Qualifier) belegt openFT dann als Prozessornamen vor (*ftmodo -p=*), den gesamten Namen als Instanzidentifikation (*ftmodo -id=*).

Meldungen des ftcrei-Kommandos

Konnte *ftcrei* nicht ordnungsgemäß ausgeführt werden, dann wird eine selbsterklärende Meldung ausgegeben; der Exitcode ist dann ungleich 0.

Beispiele

1. Im Verzeichnis */cluster/inst1* soll die Instanz *inst1* neu erzeugt werden. Der DNS-Name ist *hugo.abc.net*. Das Verzeichnis */cluster/inst1* darf nicht existieren!

   ```
   ftcrei inst1 /cluster/inst1 –addr=hugo.abc.net
   ```

   Damit wird der Betriebsparameter *ftmodo -p=* mit *hugo* vorbelegt und *ftmodo -id=* mit *hugo.abc.net*.

2. Die bestehende Instanz *inst2* aus dem Verzeichnis */cluster/inst2* soll wieder aktiviert werden. Es darf kein Hostname angegeben werden.

   ```
   ftcrei inst2 /cluster/inst2
   ```

6.9 ftcrek - Schlüsselpaarsatz erzeugen

Mit diesem Kommando erzeugen Sie einen Schlüsselpaarsatz für die Authentifizierung Ihrer openFT-Instanz in Partnersystemen (RSA-Verfahren). Weitere Informationen zum Verwalten von Schlüsseln finden Sie in Abschnitt „Authentifizierung“ auf Seite 78.

Wird die maximale Anzahl von Schlüsselpaarsätzen überschritten, erhalten Sie die Fehlermeldung:

```
ftcrek: Maximale Anzahl Schluesselpaarsaetze ueberschritten
```

Format

ftcrek [-h]

Beschreibung

-h gibt die Kommandosyntax am Bildschirm aus.

6.10 ftcrep - Berechtigungsprofil anlegen

ftcrep steht für "create profile", also Anlegen eines Berechtigungsprofils. Mit *ftcrep* können Sie sich Berechtigungsprofile einrichten.

Als FTAC-Verwalter können Sie auch auf anderen Benutzerkennungen Berechtigungsprofile einrichten, und zwar mit oder ohne Festlegung einer Zugangsberechtigung.

Beim Anlegen erhält das Profil einen Zeitstempel, der bei jeder Modifikation (z.B. mit *ftmodp*) aktualisiert wird.

Format

```
ftcrep  -h |
        <Profilname 1..8>  | @s
        <Zugangsberechtigung 8..32> | @n
        [ -ua=[<Benutzerkennung 1..32>][,[ <Kennwort 1..20> | @n ]] ]
        [ -v=y | -v=n ] [ -d=yyyymmdd ]
        [ -u=pr | -u=pu ]
        [ -priv=y | -priv=n ]
        [ -iml=y | -iml=n ]
        [ -iis=y | -iis=n ] [ -iir=y | -iir=n ]
        [ -iip=y | -iip=n ] [ -iif=y | -iif=n ]
        [ -ff=[t][m][p][r][a][l] | -ff=c ]
        [ -dir=f | -dir=t | -dir=ft ]
        [ -pn=<Partner 1..200>,...,<Partner(50) 1..200> | -pn= ]
        [ -fn=<Dateiname 1..512> | -fn= ]
        [ -fnp=<Dateinamen-Praefix 1..511> ]
        [ -ls= | -ls=@n | -ls=<Kommando1 1..1000> ]
        [ -lsp=<Kommando2 1..999> ] [ -lss=<Kommando3 1..999> ]
        [ -lf= | -lf=@n | -lf=<Kommando4 1..1000> ]
        [ -lfp=<Kommando5 1..999> ] [ -lfs=<Kommando6 1..999> ]
        [ -wm=o | -wm=n | -wm=e | -wm=one ]
        [ -c=y | -c=n ]
        [ -txt=<Text 1..100> ]
```

Beschreibung

-h gibt die Kommandosyntax am Bildschirm aus. Weitere Angaben nach *-h* werden ignoriert.

Profilname | **@s**
: gibt dem Berechtigungsprofil einen Namen. Mit diesem Namen kann das Berechtigungsprofil beispielsweise angesprochen werden, wenn es geändert oder gelöscht werden soll. Der Profilname darf nicht mit der Zugangsberechtigung verwechselt werden (siehe unten). Der Profilname muss unter allen Berechtigungsprofilen auf Ihrer Benutzerkennung eindeutig sein, andernfalls lehnt FTAC das *ftcrep* ab mit der Meldung *FT-Profil existiert bereits*.
Mit *ftshwp* (ohne Optionen) können Sie sich über Ihre bereits vergebenen Profilnamen informieren.

@s für *Profilname*
: Legt das Standard-Berechtigungsprofil für die Benutzerkennung an. Als Zugangsberechtigung müssen Sie *@n* angeben, da ein Standard-Berechtigungsprofil im Auftrag über Kennung und Passwort angesprochen wird.

Die Optionen *-v*, *-d* und *-u* dürfen Sie bei einem Standard-Berechtigungsprofil nicht angeben.

Zugangsberechtigung | **@n**
: Die Zugangsberechtigung ersetzt die sonst in Inbound-Aufträgen notwendige login-Berechtigung für Ihren Unix-Rechner. Wenn diese Zugangsberechtigung in einem File Transfer-Auftrag angegeben wird, dann gelten die in diesem Berechtigungsprofil definierten Zugriffsrechte.

Zugangsberechtigung
: Die Zugangsberechtigung muss in Ihrem Unix-Rechner eindeutig sein, damit es keine Kollisionen mit Zugangsberechtigungen gibt, die andere FTAC-Benutzer für andere Zugriffsrechte definiert haben. Wenn die von Ihnen gewählte Zugangsberechtigung bereits vergeben ist, lehnt FTAC das *ftcrep* ab mit der Meldung: `Zugangsberechtigung existiert bereits.`

Sie können auch eine binäre Zugangsberechtigung mit beliebigen, auch nicht abdruckbaren Zeichen definieren. Dazu müssen Sie die Zugangsberechtigung wie folgt in sedezimaler Form angeben: x\'...\' oder X\'...\', z.B. x\'f1f2f3f4f5f6f6f8\'.

Als FTAC-Verwalter können Sie sowohl Zugangsberechtigungen für sich, unter Ihrer eigenen Kennung, als auch Zugangsberechtigungen für eine beliebige Benutzerkennung festlegen.
In diesem Fall müssen Sie, sofern Sie nicht FT-Verwalterrechte besitzen, die vollständige login-Berechtigung angeben, d.h. Kennung und Kennwort.

@n für *Zugangsberechtigung*

Damit richten Sie ein Berechtigungsprofil ohne Zugangsberechtigung ein.

Als FTAC-Verwalter haben Sie damit die Möglichkeit, für andere Benutzerkennungen Berechtigungsprofile anzulegen, ohne dass Sie dafür Zugangsberechtigungen definieren.

Wenn es sich nicht um ein Standard-Berechtigungsprofil handelt, dann ist das Profil solange gesperrt, bis Sie bzw. der Eigentümer des Profils mit *ftmodp* eine gültige Zugangsberechtigung vergeben.

@n müssen Sie angeben, wenn Sie ein Standard-Berechtigungsprofil anlegen.

Zugangsberechtigung nicht angegeben

Wenn Sie die Zugangsberechtigung nicht im Kommando angeben, fordert FTAC Sie nach dem Abschicken des Kommandos auf, die Zugangsberechtigung einzugeben. Ihre Eingabe bleibt unsichtbar, um zu verhindern, dass Unbefugte die Zugangsberechtigung sehen. Um Schreibfehler auszuschließen, wird als Kontrolleingabe von Ihnen ein zweites Mal die Zugangsberechtigung erwartet.

-ua=[Benutzerkennung][**,**[Kennwort | **@n**]]

Mit *-ua* geben Sie als FTAC-Verwalter an, für welche Benutzerkennung Sie ein Berechtigungsprofil anlegen wollen.

Benutzerkennung

Als Benutzer ohne Administrations-Privilegien können Sie hier nur Ihre eigene Benutzerkennung angeben.
Als FTAC-Verwalter dürfen Sie hier jede beliebige Benutzerkennung angeben.

,Kennwort

gibt das Kennwort zu der Benutzerkennung an, ein binäres Kennwort muss sedezimal in der Form x\'...\' oder X\'...\' angegeben werden. Das Berechtigungsprofil für die Kennung ist nur so lange gültig wie das Kennwort für die Kennung gültig ist. Wenn das Kennwort geändert wird, dann ist das Profil nicht mehr verwendbar.

Wenn Sie als FTAC-Verwalter für einen anderen Benutzer ein Berechtigungsprofil einrichten und gleichzeitig eine Zugangsberechtigung für das Profil vergeben wollen, müssen Sie zusätzlich zur Benutzerkennung hier das Kennwort angeben, sofern Sie nicht FT-Verwalterrechte besitzen.

@n für *Kennwort*

Darf nur der FTAC-Verwalter angeben! Bei der Angabe *@n* dürfen Sie als FTAC-Verwalter keine Zugangsberechtigung für das Berechtigungsprofil erteilen, sofern Sie nicht FT-Verwalterrechte besitzen.

nur Komma (,) ohne *Kennwort*
: Bei Komma (,) ohne *Kennwort* wird das Kennwort nach der Kommandoabgabe am Bildschirm abgefragt. Die Eingabe bleibt unsichtbar, um zu verhindern, dass Unbefugte das Kennwort sehen. Hochkommas dürfen in diesem Fall nicht mit Gegenschrägstrich (\) entwertet werden.

nur *Benutzerkennung* (ohne Komma und *Kennwort*) angegeben
: Das Profil gilt für alle Kennwörter der Benutzerkennung.

-ua=␣ angegeben oder *-ua* nicht angegeben
: Das Berechtigungsprofil wird auf der eigenen Benutzerkennung eingerichtet.

-v=y | **-v=n**
: Mit *-v* definieren Sie den Zustand der Zugangsberechtigung.

  Mögliche Werte:

  y (Standardwert)
  : Die Zugangsberechtigung ist nicht gesperrt (sie ist valid).

  n Die Zugangsberechtigung ist gesperrt (sie ist nicht valid).

  -v darf bei einem Standard-Berechtigungsprofil nicht angegeben werden.

-d=yyyymmdd
: Mit *-d* legen Sie die Frist fest, innerhalb der die Zugangsberechtigung verwendet werden darf. Nach Ablauf der Frist ist das Berechtigungsprofil gesperrt.
  Sie können ein achtstelliges Datum angeben (z.B. 20170602 für 2.6.2017). Die Verwendung der Zugangsberechtigung ist ab 00:00 Uhr des angegebenen Tages nicht mehr möglich. Der größtmögliche Wert für das anzugebende Datum ist 20380119 (19. Januar 2038).

  -d darf bei einem Standard-Berechtigungsprofil nicht angegeben werden.

-d nicht angegeben (Standardwert)
: Die Verwendung der Zugangsberechtigung ist zeitlich nicht eingeschränkt.

-u=pr | **-u=pu**
: Mit *-u* können Sie das Verhalten von FTAC für den Fall steuern, dass jemand versucht, ein Berechtigungsprofil mit der gleichen Zugangsberechtigung anzulegen. Im Normalfall sollte eine Zugangsberechtigung sofort gesperrt werden.

  Zugangsberechtigungen, die nicht so schutzbedürftig sind, können Sie als öffentlich (public) kennzeichnen. In dem Fall wird die Zugangsberechtigung nicht gesperrt, auch wenn versucht wird, eine gleichnamige Zugangsberechtigung zu vergeben.

pr (Standardwert)
Die Zugangsberechtigung wird gesperrt, sobald jemand von einer anderen Kennung aus versucht, eine gleichnamige Zugangsberechtigung zu vergeben (private).
Gleichzeitig werden in dem Fall die Werte für *-u* und *-d* auf die Standardwerte gesetzt.

pu Die Zugangsberechtigung wird nicht gesperrt, auch wenn jemand versucht, eine gleichnamige Zugangsberechtigung zu vergeben (public).

-u darf bei einem Standard-Berechtigungsprofil nicht angegeben werden.

-priv=n | **-priv=y**
Mit dieser Angabe können Sie als FTAC-Verwalter Berechtigungsprofile privilegieren.

n (Standardwert)
Das Berechtigungsprofil ist (zunächst) nicht privilegiert.

y Das Berechtigungsprofil ist privilegiert.

-iml=y | **-iml=n**
Mit *-iml* (ignore max. level) wird festgelegt, ob das Berechtigungsprofil an die Vorgaben des Berechtigungssatzes gebunden ist. Sie können Ihre eigenen Vorgaben (die MAX. USER LEVELS) für Aufträge, die mit diesem Berechtigungsprofil arbeiten, außer Kraft setzen.

Wenn das Berechtigungsprofil zudem vom FTAC-Verwalter privilegiert wird, können auch die Vorgaben des FTAC-Verwalters ignoriert werden (die MAX. ADM LEVELS). Das bedeutet, dass mit diesem Berechtigungsprofil *inbound*-Grundfunktionen genutzt werden können, die im Berechtigungssatz gesperrt sind.

y Mit dem Profil können die Vorgaben des Berechtigungssatzes ignoriert werden.

n (Standardwert)
Das Profil unterliegt den Vorgaben des Berechtigungssatzes.

-iis=y | **-iis=n**
Mit *-iis* (ignore inbound send) kann die Vorgabe für die Grundfunktion *inbound senden* im Berechtigungssatz ignoriert werden, Näheres siehe *-iml*.

y Mit dem Profil kann die Grundfunktion *inbound senden* auch dann genutzt werden, wenn sie im Berechtigungssatz gesperrt ist. Gleichzeitig kann die Teilkomponente "Ansehen von Dateiattributen" der Grundfunktion *inbound Dateimanagement* genutzt werden, siehe Tabelle bei *-iif*.

Wenn Sie im Berechtigungssatz die Grundfunktion *inbound senden* gesperrt haben, reicht diese Angabe aus. Wenn sie vom FTAC-Verwalter gesperrt wurde, muss er zusätzlich das Berechtigungsprofil privilegieren.

n (Standardwert)
Das Profil unterliegt der Vorgabe des Berechtigungssatzes für die Grundfunktion *inbound senden*.

-iir=y | -iir=n
Mit *-iir* (ignore inbound receive) kann die Vorgabe für die Grundfunktion *inbound empfangen* im Berechtigungssatz ignoriert werden, Näheres siehe *-iml*.

y Mit dem Profil kann die Grundfunktion *inbound empfangen* auch dann genutzt werden, wenn sie im Berechtigungssatz gesperrt ist. Gleichzeitig können Teilkomponenten der Grundfunktion *inbound Dateimanagement* genutzt werden (siehe Tabelle bei *-iif*).

Wenn die Grundfunktion *inbound empfangen* von Ihnen gesperrt wurde, reicht diese Angabe dafür aus. Wenn sie vom FTAC-Verwalter gesperrt wurde, muss er zusätzlich das Berechtigungsprofil privilegieren.

n (Standardwert)
Das Profil unterliegt der Vorgabe des Berechtigungssatzes für die Grundfunktion *inbound empfangen*.

-iip=y | -iip=n
Mit *-iip* (ignore inbound processing) kann die Vorgabe für die Grundfunktion *inbound Folgeverarbeitung + Vorverarbeitung + Nachverarbeitung* im Berechtigungssatz ignoriert werden, Näheres siehe *-iml*.

y Mit dem Profil kann die Grundfunktion *inbound Folgeverarbeitung + Vorverarbeitung + Nachverarbeitung* auch dann genutzt werden, wenn sie im Berechtigungssatz gesperrt ist. Wenn sie von Ihnen gesperrt wurde, reicht diese Angabe dafür aus. Wenn sie vom FTAC-Verwalter gesperrt wurde, muss er zusätzlich das Berechtigungsprofil privilegieren.

n (Standardwert)
Das Profil unterliegt der Vorgabe des Berechtigungssatzes für die Grundfunktion *inbound Folgeverarbeitung + Vorverarbeitung + Nachverarbeitung*.

-iif=y | -iif=n
Mit *-iif* (ignore inbound filemanagement) kann die Vorgabe für die Grundfunktion *inbound Dateimanagement* im Berechtigungssatz ignoriert werden, Näheres siehe *-iml*.

y Mit dem Profil kann die Grundfunktion *inbound Dateimanagement* auch dann genutzt werden, wenn sie im Berechtigungssatz gesperrt ist. Wenn die Grundfunktion *inbound Dateimanagement* von Ihnen gesperrt wurde, reicht diese Angabe dafür aus. Wenn sie vom FTAC-Verwalter gesperrt wurde, muss er zusätzlich das Berechtigungsprofil privilegieren.

n (Standardwert)

Das Profil unterliegt der Vorgabe des Berechtigungssatzes für die Grundfunktion *inbound Dateimanagement*.

Die folgende Tabelle zeigt, welche Teilkomponenten des Dateimanagements unter welchen Voraussetzungen genutzt werden können.

Inbound Dateimanagement-Funktion	**Einstellung im Berechtigungssatz bzw. Erweiterung im Profil**
Dateiattribute anzeigen	Inbound Senden (IBS) erlaubt
Dateiattribute ändern	Inbound Empfangen (IBR) **und** Inbound Dateimanagement (IBF) erlaubt
Dateien umbenennen	Inbound Empfangen (IBR) **und** Inbound Dateimanagement (IBF) erlaubt
Dateien löschen	Inbound Empfangen (IBR) erlaubt **und** Schreibregel = überschreiben im Profil
Dateiverzeichnisse anzeigen	Inbound Dateimanagement (IBF) erlaubt
Dateiverzeichnisse anlegen, umbenennen, löschen	Inbound Dateimanagement (IBF) erlaubt **und** Richtung = vom Partner im Profil

-ff=[t][m][p][r][a][l] | **-ff=c**

Mit *-ff* legen Sie fest, für welche Funktion das Berechtigungsprofil benutzt werden darf. Mit Ausnahme von *c* ist jede beliebige Kombination aus diesen Buchstaben (*tm, mt, mr,* ...) möglich. *c* darf nicht mit anderen Werten kombiniert werden.

t (transfer) Das Berechtigungsprofil darf für die File-Transfer-Funktionen "Dateien übertragen", "Dateiattribute ansehen" und "Dateien löschen" benutzt werden.

m (modify file attributes) Das Berechtigungsprofil darf für die File-Transfer-Funktionen "Dateiattribute ansehen" und "Dateiattribute modifizieren" benutzt werden.

p (processing) Das Berechtigungsprofil darf für die File-Transfer-Funktionen "Dateivorverarbeitung" bzw. "Dateinachverarbeitung" benutzt werden. Zusätzlich muss die Funktion "Dateien übertragen" erlaubt sein.

Für Profile mit einem Dateinamen-Präfix (*-fnp=*) bzw. einem Dateinamen (*-fn=*) ist die Angabe von *p* bedeutungslos, weil in diesem Fall das erste Zeichen des Dateinamens oder Dateinamen-Präfix darüber entscheidet, ob das Profil nur für Vor- und Nachverarbeitung verwendet werden kann ("|") oder ausschließlich Dateiübertragung bzw. Dateimanagement ermöglicht (kein "|").
Die Verwendung von Folgeverarbeitung wird nicht über *-ff=*, sondern über *-lf=* und *-ls=* gesteuert.

r (read directory) Das Berechtigungsprofil darf für die File-Transfer-Funktionen "Dateiverzeichnisse ansehen" und "Dateiattribute ansehen" benutzt werden.

a (administration)
Das Berechtigungsprofil darf für die Funktion "Fernadministration" genutzt werden. D.h. es berechtigt einen Fernadministrations-Server, auf die lokale openFT-Instanz zuzugreifen. Dazu muss die zugehörige Zugangsberechtigung im Fernadministrations-Server konfiguriert sein.
Die Angabe von *-ff=a* ist nur dem FT- oder FTAC-Verwalter erlaubt.

l (logging)
Das Berechtigungsprofil darf für die Funktion "ADM-Traps" benutzt werden. Damit kann eine andere openFT-Instanz ihre ADM-Traps über dieses Profil an den Fernadministrations-Server schicken. Diese Angabe ist nur sinnvoll, wenn die lokale openFT-Instanz als Fernadministrations-Server gekennzeichnet ist (Kommando *ftmodo -admcs=y*).
Die Angabe von *-ff=l* ist nur dem FT-Verwalter erlaubt.

c (client access)
Das Berechtigungsprofil darf für die Funktion "Zugang zum Fernadministrations-Server" benutzt werden (ADM-Profil). Damit kann ein Fernadministrator auf einem fernen Rechner über dieses Profil auf den lokalen Fernadministrations-Server zugreifen und Fernadministrationsaufträge absetzen. Die lokale openFT-Instanz muss als Fernadministrations-Server gekennzeichnet sein (Kommando *ftmodo -admcs=y*).

Der Wert *c* darf mit keinem anderen Wert kombiniert werden. Die Angabe von *-ff=c* ist nur dem ADM-Verwalter erlaubt.

-ff nicht angegeben
Entspricht der Angabe *-ff=tmr*, d.h. das Berechtigungsprofil kann für alle File-Transfer-Funktionen außer "Dateiverarbeitung" benutzt werden, nicht jedoch für Funktionen zur Fernadministration (*a*, *c*) und zu ADM-Traps (*l*).

-dir=f | -dir=t | -dir=ft
Mit *-dir* legen Sie fest, für welche Übertragungsrichtung(en) das Berechtigungsprofil benutzt werden darf.

f Es dürfen nur Daten vom Partnersystem zum lokalen System übertragen werden.

t Es dürfen nur Daten vom lokalen System zum Partnersystem übertragen werden. Damit ist auch kein Anlegen, Umbenennen oder Löschen von Verzeichnissen möglich.

ft, tf Beide Übertragungsrichtungen sind erlaubt.

-dir nicht angegeben
: Das Berechtigungsprofil schränkt die Übertragungsrichtung nicht ein.

-pn=Partner1[,Partner2, ...] | **-pn=**
: Mit *-pn* können Sie festlegen, dass dieses Berechtigungsprofil nur für FT-Aufträge benutzt werden kann, die mit einem bestimmten Partnersystem abgewickelt werden. Sie können den Namen des Partnersystems in der Partnerliste oder die Adresse des Partnersystems angeben. Einzelheiten zur Adressangabe finden Sie in Abschnitt „Aufbau der Partneradressen“ auf Seite 68.

  Sie können hier maximal 50 Partnersysteme angeben, insgesamt maximal 1000 Zeichen.

-pn nicht angegeben (oder **-pn=**)
: Das Berechtigungsprofil kann von jedem Partnersystem aus benutzt werden.

-fn=Dateiname | **-fn=**
: Mit *-fn* legen Sie fest, auf welche Datei unter Ihrer Benutzerkennung mit diesem Berechtigungsprofil zugegriffen wird. Wenn Sie hier einen vollqualifizierten Dateinamen angeben, darf nur noch die Datei mit diesem Namen übertragen werden. Endet der Dateiname mit %unique oder %UNIQUE, so wird diese Zeichenfolge beim File Transfer durch einen String ersetzt, der bei jedem erneuten Aufruf wechselt. Dieser String ist in Unix-Systemen 14 Zeichen lang. Nach %unique oder %UNIQUE darf noch ein durch einen Punkt getrenntes Suffix angegeben werden, z.B. `datei1%unique.txt`. Sowohl im Logging als auch bei Meldungen wird nur noch der bereits konvertierte Dateiname angezeigt.
  Wenn *Dateiname* mit einem "|" (Pipezeichen) beginnt, dann wird er als Vor- bzw. Nachverarbeitungskommando interpretiert, siehe auch entsprechender Abschnitt im Benutzerhandbuch.

-fn nicht angegeben (oder **-fn=**)
: Das Berechtigungsprofil erlaubt uneingeschränkten Zugriff auf alle Ihre Dateien (Ausnahme siehe *-fnp*).

-fnp=Dateinamen-Praefix
: Durch diese Angabe kann der Zugriff auf eine Menge von Dateien beschränkt werden, deren Namen mit demselben Präfix anfangen. FTAC setzt die mit *Dateinamen-Praefix* spezifizierte Zeichenfolge vor den Dateinamen, der im Auftrag steht und versucht, die Datei mit dem ergänzten Namen zu übertragen. Wenn Sie zum Beispiel *-fnp=dagobert/* angeben und im Auftrag der Dateiname *boerse* steht, dann wird die Datei *dagobert/boerse* übertragen.

  So lassen sich die für den File Transfer freigegebenen Dateien kennzeichnen. Wenn mit *-fnp* ein Präfix spezifiziert wurde, darf in dem Dateinamen, der im Auftrag steht, die Zeichenfolge *../* nicht vorkommen. Hiermit wird ein Wechsel des Dateiver-

zeichnisses unterbunden. Sie sollten aber darauf achten, dass nicht durch einen symbolischen Verweis an eine andere Stelle im Dateibaum gesprungen werden kann!

%unique oder %UNIQUE kann bei einem Dateinamen-Präfix nicht verwendet werden. Bei einem File Transfer-Auftrag kann vom Benutzer ein Dateiname mit der Endung %UNIQUE (oder %UNIQUE.*suffix*, %unique oder %unique.*suffix*) verwendet werden, um eindeutige Dateinamen mit dem hier festgelegten Präfix zu generieren.

Ein Dateinamen-Präfix, das mit dem Zeichen | (Pipe) beginnt, legt fest, dass das FTAC-Profil ausschließlich für Dateiübertragung mit Vor- und Nachverarbeitung verwendet werden kann, da der aus dem Präfix und dem beim *ncopy*- oder *ft*-Kommando angegebenen Namen gebildete Dateiname ebenfalls mit dem Zeichen | beginnt. In diesem Fall dürfen keine Folgekommandos angegeben werden.

Auf Unix-Systemen dürfen die Shell-Metazeichen | ; & < > sowie "newline" nur angegeben werden, wenn sie mit '...' (Hochkommas) oder "..." (Anführungszeichen) eingeschalt oder einzeln mit "\" (Gegenschrägstrich) entwertet werden. Das Zeichen ` (Accent grave) und die Zeichenfolge $((Dollar+Klammer auf) dürfen nur angegeben werden, wenn sie mit '...' (Hochkommas) eingeschalt oder direkt nach "\" (Gegenschrägstrich) angegeben werden.

Nicht angegeben werden dürfen bei dem beim *ncopy*- oder *ft*-Kommando angegebenen Namen die Zeichenfolgen
– .. (zwei Punkte)
– .\ (Punkt+Gegenschrägstrich)
– .' (Punkt+Hochkomma)
Damit wird ein Navigieren auf übergeordnete Verzeichnisse verhindert.

Das Dateinamen-Präfix darf maximal 511 Bytes lang sein (Darstellung in UTF-8, siehe Seite 168).

Sonderfälle

- Für FTAC-Profile, die ausschließlich für das *ftexec*-Kommando genutzt werden sollen, ist ein Dateiname oder Dateinamen-Präfix anzugeben, der bzw. das mit der Zeichenfolge "|ftexecsv␣" beginnt. Soll darüber hinaus ein Kommando-Präfix festgelegt werden, dann müssen Sie dieses wie folgt angeben:

  -fnp="|ftexecsv␣-p=*Kommando-Präfix***"**
  (z.B.: `-fnp="|ftexecsv␣-p=\"ftshwr␣\""`)

  Für den Kommandostring des *ftexec*-Aufrufs gelten dieselben Beschränkungen wie für das Dateinamen-Präfix bei Vor- und Nachverarbeitung.

- Für FTAC-Profile, die ausschließlich für das Abrufen von Messdaten verwendet werden sollen, geben Sie das Dateinamen-Präfix "|*FTMONITOR " an. Die Funktion des Profils muss Dateivorverarbeitung erlauben (*-ff=tp*). Details siehe Beispiel 3 auf Seite 208.

-fnp nicht angegeben
: FTAC setzt kein Präfix vor den Dateinamen.

-ls= | **-ls=@n** | **-ls=**Kommando1
: Mit *-ls* können Sie eine Folgeverarbeitung vorgeben, die nach erfolgreicher Dateiübertragung unter Ihrer Benutzerkennung durchgeführt werden soll. Wenn mit *-ls* eine Festlegung getroffen wurde, darf im File Transfer-Auftrag keine Folgeverarbeitung nach erfolgreicher Übertragung verlangt werden! Eine Festlegung für *-ls* ist nur sinnvoll, wenn Sie durch entsprechende Festlegungen für *-lf* (siehe unten) verhindern, dass sie durch einen mutwillig misslungenen Auftrag umgangen werden kann. Wenn Sie mit *-fnp* ein Dateinamen-Präfix definiert haben und eine Folgeverarbeitung mit dieser Datei planen, müssen Sie hier den vollständigen Dateinamen angeben.

  @n für *Kommando1*
  : Wenn Sie *-ls=@n* eingeben, erlaubt das Berechtigungsprofil keine Folgeverarbeitung nach erfolgreicher Dateiübertragung.

-ls nicht angegeben (oder **-ls=**)
: Das Berechtigungsprofil schränkt die Folgeverarbeitung im lokalen System nach erfolgreicher Dateiübertragung nicht ein (siehe auch *-lsp* bzw. *-lss*).

-lsp=Kommando2
: Mit *-lsp* können Sie ein Präfix für die Folgeverarbeitung nach erfolgreicher Dateiübertragung im lokalen System definieren. FTAC setzt dann die Zeichenfolge *Kommando2* vor die im File Transfer-Auftrag verlangte Folgeverarbeitung und versucht, das so entstandene Kommando auszuführen.
  Wenn Sie zum Beispiel *-lsp='lpr␣'* angeben und im Auftrag für die Folgeverarbeitung *Dateiname* steht, dann führt FTAC die Folgeverarbeitung *lpr␣Dateiname* aus.

  Präfix (und evtl. Suffix) und Folgeverarbeitungskommando dürfen zusammen maximal 1000 Bytes lang sein (Darstellung in UTF-8, siehe Seite 169).

  Beachten Sie bitte die Informationen zur Option *-ls*!

  Wenn mit *-lsp* ein Präfix definiert wurde, ist der Zeichenvorrat für die Folgeverarbeitung im File Transfer-Auftrag begrenzt auf:
  – alphanumerische Zeichen (Buchstaben und Ziffern)
  – die Sonderzeichen + = / ! ␣ - , @ _ " $ '
  – einen Punkt (.) zwischen alphanumerischen Zeichen

-lsp nicht angegeben
: FTAC setzt kein Präfix vor die im Auftrag verlangte Folgeverarbeitung nach erfolgreicher Dateiübertragung.

-lss=Kommando3
: Mit *-lss* können Sie ein Suffix für die Folgeverarbeitung nach erfolgreicher Dateiübertragung im lokalen System definieren. FTAC setzt dann die Zeichenfolge *Kommando3* hinter die im File Transfer-Auftrag verlangte Folgeverarbeitung und versucht, das so entstandene Kommando auszuführen.
Wenn Sie zum Beispiel *-lss=␣datei.txt* angeben und im Auftrag für die Folgeverarbeitung *lpr* steht, dann führt FTAC die Folgeverarbeitung *lpr␣datei.txt* aus.

Suffix (und evtl. Präfix) und Folgeverarbeitungskommando dürfen zusammen maximal 1000 Bytes lang sein (Darstellung in UTF-8, siehe Seite 169).

Beachten Sie bitte die Informationen zur Option *-ls*!

Wenn mit *-lss* ein Suffix definiert wurde, ist der Zeichenvorrat für die Folgeverarbeitung im File-Transfer-Auftrag begrenzt auf:
- alphanumerische Zeichen (Buchstaben und Ziffern)
- die Sonderzeichen + = / ! ␣ - , @ _ " $ '
- einen Punkt (.) zwischen alphanumerischen Zeichen

-lss nicht angegeben
: FTAC setzt kein Suffix hinter die im Auftrag verlangte Folgeverarbeitung nach erfolgreicher Dateiübertragung.

-lf=Kommando4 | **@n**
: Mit *-lf* können Sie eine Folgeverarbeitung vorgeben, die unter Ihrer Benutzerkennung durchgeführt werden soll, wenn die **Dateiübertragung abgebrochen** wurde. Wenn mit *-lf* eine Festlegung getroffen wurde, darf im File Transfer-Auftrag keine Folgeverarbeitung nach misslungener Übertragung verlangt werden! Eine Festlegung für *-lf* ist nur sinnvoll, wenn Sie durch entsprechende Festlegungen für *-ls* (siehe oben) verhindern, dass sie durch einen erfolgreichen Auftrag umgangen werden kann. Wenn Sie mit *-fnp* ein Präfix für den Dateinamen definiert haben und eine Folgeverarbeitung mit dieser Datei planen, müssen Sie hier den vollständigen Dateinamen angeben.

  @n für *Kommando4*
  : Wenn Sie *-lf=@n* eingeben, erlaubt das Berechtigungsprofil keine Folgeverarbeitung nach misslungener Dateiübertragung.

-lf nicht angegeben
: Das Berechtigungsprofil schränkt die Folgeverarbeitung im lokalen System nach misslungener Dateiübertragung nicht ein (Ausnahme siehe *-lfp* bzw. *-lfs*).

-lfp=Kommando5

Mit *-lfp* können Sie ein Präfix für die Folgeverarbeitung nach **misslungener Dateiübertragung** im lokalen System definieren. FTAC setzt dann die Zeichenfolge *Kommando5* vor die im File Transfer-Auftrag verlangte Folgeverarbeitung und versucht, das so entstandene Kommando auszuführen.
Wenn Sie zum Beispiel *-lfp='lpr␣'* angeben und im Auftrag für die Folgeverarbeitung *datei.txt* steht, dann führt FTAC die Folgeverarbeitung *lpr␣datei.txt* aus.

Präfix (und evtl. Suffix) und Folgeverarbeitungskommando dürfen zusammen maximal 1000 Bytes lang sein (Darstellung in UTF-8, siehe Seite 169).

Beachten Sie bitte die Informationen zur Option *-lf*!

Wenn mit *-lfp* ein Präfix definiert wurde, ist der Zeichenvorrat für die Folgeverarbeitung im File Transfer-Auftrag begrenzt auf:
- alphanumerische Zeichen (Buchstaben und Ziffern)
- die Sonderzeichen + = / ! ␣ - , @ _ " $ '
- einen Punkt (.) zwischen alphanumerischen Zeichen

-lfp nicht angegeben

FTAC setzt kein Präfix vor die im Auftrag verlangte Folgeverarbeitung nach misslungener Dateiübertragung.

-lfs=Kommando6

Mit *-lfs* können Sie ein Suffix für die Folgeverarbeitung nach **misslungener Dateiübertragung** im lokalen System definieren. FTAC setzt dann die Zeichenfolge *Kommando6* hinter die im File Transfer-Auftrag verlangte Folgeverarbeitung und versucht, das so entstandene Kommando auszuführen.
Wenn Sie zum Beispiel *-lfs=␣error.txt* angeben und im Auftrag für die Folgeverarbeitung *lpr* steht, dann führt FTAC die Folgeverarbeitung *lpr␣error.txt* aus.

Suffix (und evtl. Präfix) und Folgeverarbeitungskommando dürfen zusammen maximal 1000 Bytes Zeichen lang sein (Darstellung in UTF-8, siehe Seite 169).

Beachten Sie bitte die Informationen zur Option *-lf*!

Wenn mit *-lfs* ein Suffix definiert wurde, ist der Zeichenvorrat für die Folgeverarbeitung im File Transfer-Auftrag begrenzt auf:
- alphanumerische Zeichen (Buchstaben und Ziffern)
- die Sonderzeichen + = / ! ␣ - , @ _ " $ '
- einen Punkt (.) zwischen alphanumerischen Zeichen

-lfs nicht angegeben

FTAC setzt kein Suffix hinter die im Auftrag verlangte Folgeverarbeitung nach misslungener Dateiübertragung.

-wm=o | **-wm=n** | **-wm=e** | **-wm=one**

Mit *-wm* können Sie festlegen, welche Schreibregeln im File-Transfer-Auftrag benutzt werden dürfen und wie sie wirken.

o (overwrite) Im FT-Auftrag darf bei openFT- oder FTAM-Partnern als Schreibregel nur *-o* oder *-e* angegeben werden.
Eine schon vorhandene Empfangsdatei wird überschrieben, eine noch nicht vorhandene Empfangsdatei wird neu eingerichtet.

Bei FTP-Partnern ist im FT-Auftrag auch *-n* erlaubt, falls die Datei noch nicht existiert.

n (no overwrite) Im FT-Auftrag darf als Schreibregel *-o*, *-n* oder *-e* angegeben werden. Eine noch nicht vorhandene Empfangsdatei wird neu eingerichtet. Wenn die Empfangsdatei schon existiert, wird der Auftrag nicht durchgeführt.

e (extend) Im FT-Auftrag darf als Schreibregel nur *-e* angegeben werden, d.h. die übertragene Datei wird an das Ende einer bereits vorhandenen Datei angehängt. Eine noch nicht vorhandene Empfangsdatei wird neu eingerichtet.

one (Standardwert)
Die Verwendung der Schreibregel wird durch das Berechtigungsprofil nicht eingeschränkt.

-c=y | **-c=n**

Voraussetzung: openFT-CR ist installiert.
Mit *-c* können Sie festlegen, ob Datenverschlüsselung vorgeschrieben oder verboten wird. Stimmt die Einstellung im Profil nicht mit der Einstellung im Auftrag überein, dann wird der Auftrag abgelehnt. Die Einstellung gilt nicht für Dateimanagement-Aufträge, da es für diese Aufträge keine Verschlüsselung gibt.

y Über dieses Profil dürfen nur Aufträge *mit* Datenverschlüsselung abgewickelt werden.

n Über dieses Profil dürfen nur Aufträge *ohne* Datenverschlüsselung abgewickelt werden.

-c nicht angegeben
Die Datenverschlüsselung wird weder vorgeschrieben noch verboten.

-txt=Text

Mit *-txt* können Sie einen Kommentar im Berechtigungsprofil ablegen (maximal 100 Zeichen).

-txt nicht angegeben
Das Berechtigungsprofil wird ohne Kommentar abgelegt.

VORSICHT!
Wenn Sie die Optionen *-ff=p*, *-fn*, *-fnp*, *-ls* , *-lsp*, *-lss*, *-lf*, *-lfp* oder *-lfs* benutzen, müssen Sie bedenken, dass

- eine Einschränkung für den Dateinamen durch Umbenennen umgangen werden kann, wenn nicht auch die Folgeverarbeitung eingeschränkt wird.
- eine Einschränkung für die Folgeverarbeitung sowohl die erfolgreiche als auch die misslungene Dateiübertragung umfassen muss und ggf. äquivalente Einschränkungen für eine eventuell zugelassene Vorverarbeitung vorliegen müssen.
- Präfixe für Dateinamen und Folgeverarbeitungen aufeinander abgestimmt sein müssen.
- in dem Teil Ihres Dateibaums, der hinter einem Dateinamen-Präfix möglich ist, keine symbolischen Verweise vorkommen sollten.
- eine Beschränkung einer Vor-, Nach- oder Folgeverarbeitung auf ein Kommando umgangen werden kann, wenn es möglich ist, dieses Kommando z.B. durch ein "trojanisches Pferd" zu ersetzen.

Beispiele

1. Sie wollen ein Berechtigungsprofil zu folgendem Zweck anlegen:

   Sie möchten Ihren Monatsbericht regelmäßig per File Transfer von Ihrem Rechner *goldmine* an den Chef in der Zentrale schicken können. Die Datei *monatsbericht_filiale01* soll nach der Übertragung ausgedruckt werden. Das zum Anlegen eines solchen Berechtigungsprofils in der Zentrale nötige Kommando lautet:

   ```
   ftcrep␣monatsbe␣fuerdenChef␣-d=20171231␣-dir=f \
   ␣-pn=goldmine␣-fn=monatsbericht_filiale01 \
   ␣-ls='lpr␣monatsbericht_filiale01'␣-lf=@n␣-wm=o
   ```

   Das Berechtigungsprofil hat den Namen *monatsbe* und die Zugangsberechtigung *fuerdenChef* und erlaubt nur das Übertragen der Datei *monatsbericht_filiale01* zur Zentrale. Nach erfolgreicher Dateiübertragung wird die Datei in der Zentrale ausgedruckt, Folgeverarbeitung nach misslungener Dateiübertragung ist verboten. Die Zugangsberechtigung ist nur bis zum 30. Dezember 2017 gültig, ab 00:00 Uhr des 31.12.2017 ist das Berechtigungsprofil gesperrt.

2. Sie möchten sich für Ihre Kennung das Standard-Berechtigungsprofil so einrichten, dass nur File Transfer und das Neuanlegen von Dateien erlaubt sein soll. Dieses Profil kann z.B. von FTAM-Partnern genutzt werden, die für den Inbound-Zugriff immer Kennung und Kennwort angeben müssen.

   Das Kommando lautet:

   ```
   ftcrep␣@s␣@n␣-wm=n␣-ff=t
   ```

3. Sie möchten ein Berechtigungsprofil *monitor1* definieren, das nur die Ausgabe von Messdaten erlaubt. Als Zugangsberechtigung vergeben Sie *onlyftmonitor*. Das Kommando lautet:

   ```
   ftcrep monitor1 onlyftmonitor -ff=tp -fnp="|*FTMONITOR "
   ```

   Das Leerzeichen hinter *FTMONITOR dient dazu, dass die beim Aufruf angegebenen Optionen automatisch vom Kommando getrennt werden. Ein solches Profil kann dann sowohl zum Aufruf des openFT Monitors (z.B. per Kommando *ftmonitor*) als auch im *ncopy*-Kommando verwendet werden. Das Berechtigungsprofil ist nur für die Kommunikation über das openFT-Protokoll gültig.

   Näheres finden Sie im Abschnitt „Messdatenerfassung mit openFT“ auf Seite 74.

6.11 ftdeli - Deaktivieren einer Instanz

Mit dem Kommando *ftdeli* können Sie eine Instanz deaktivieren. Das Deaktivieren einer Instanz entfernt ausschließlich den symbolischen Link im lokalen */var/openFT* Verzeichnis. Der Instanzendateibaum wird nicht verändert. Die Standardinstanz *std* und die aktuell eingestellte Instanz können nicht deaktiviert werden.

Format

ftdeli -h |
<Instanz 1..8>

Beschreibung

-h gibt die Kommandosyntax am Bildschirm aus. Weitere Angaben nach *-h* werden ignoriert.

Instanz
Name der Instanz, die deaktiviert werden soll.
Mit dem Kommando *ftshwi @a* können Sie sich die Namen aller Instanzen anzeigen lassen.

Meldungen des ftdeli-Kommandos

Konnte *ftdeli* nicht ordnungsgemäß ausgeführt werden, dann wird eine selbsterklärende Meldung ausgegeben; der Exitcode ist dann ungleich 0.

Beispiele

1. Die Instanz *inst1* aus dem Verzeichnis */CLUSTER/inst1* soll auf dem Rechner *CLUSTER1* deaktiviert werden, da sie auf *CLUSTER2* umgeschaltet wurde. Das Verzeichnis */CLUSTER/inst1* bleibt erhalten.

```
ftdeli inst1
```

2. Die Instanz *inst2* mit dem Verzeichnis */CLUSTER/inst2* soll inklusive Instanzdateibaum gelöscht werden.

```
ftdeli inst2
rm -r /CLUSTER/inst2
```

3. Es wurde mit *. ftseti* in die Instanz *inst3* gewechselt. Dort wird versucht, die Instanz *inst3* zu deaktivieren.

```
ftdeli inst3
ftdeli: openFT Instanz 'inst3' kann nicht entfernt werden.
```

6.12 ftdelk - Schlüsselpaarsatz löschen

Mit diesem Kommando löschen Sie die Schlüsselpaarsätze einer Referenz. Ihr System kann danach von Partnersystemen, die noch den zugehörigen öffentlichen Schlüssel verwenden, nicht mehr authentifiziert werden. Weitere Informationen zum Verwalten von Schlüsseln finden Sie im Abschnitt „Authentifizierung“ auf Seite 78.

Es sollte immer ein Schlüsselpaarsatz in Ihrer openFT-Instanz vorhanden sein, da andernfalls alle Aufträge unverschlüsselt durchgeführt werden, d.h. es werden weder Auftragsbeschreibungsdaten noch Dateiinhalte verschlüsselt.

Format

ftdelk -h |
<Schlüsselreferenz 1..9999999>

Beschreibung

-h gibt die Kommandosyntax am Bildschirm aus. Weitere Angaben nach *-h* werden ignoriert.

Schlüsselreferenz
Dient zur Auswahl des zu löschenden Schlüsselpaarsatzes. Sie finden die Referenz im Namen der öffentlichen Schlüsseldatei, siehe Abschnitt „Lokale RSA-Schlüsselpaare erzeugen und verwalten“ auf Seite 81.

6.13 ftdell - Logging-Sätze oder Offline-Logging-Dateien löschen

Mit *ftdell* können Sie als FT- , FTAC- oder ADM-Verwalter Logging-Sätze aller Benutzerkennungen löschen.

Außerdem können Sie nicht mehr benötigte Offline-Logging-Dateien löschen. Pro *ftdell*-Kommando können Sie bis zu 1024 Logging-Dateien löschen. Wollen Sie mehr Dateien löschen, dann müssen Sie das Kommando wiederholen.

Dieses Kommando ist nicht für den normalen Benutzer erlaubt.

Sichern Sie die Logging-Sätze, indem Sie die Ausgabe des *ftshwl* in eine Datei oder auf einen Drucker umleiten, siehe Abschnitt „ftshwl - Logging-Sätze und Offline-Logging-Dateien anzeigen“ auf Seite 307.

Beim Löschen von Logging-Sätzen ändert sich die Größe der Datei, da der Speicherplatz beim Löschen sofort freigegeben wird.

Den Zeitpunkt, bis zu dem die Logging-Sätze gelöscht werden sollen, können Sie entweder als fixen Zeitpunkt mit Datum und Uhrzeit angeben oder als relativen Zeitpunkt, zum Beispiel in der Form: alle Sätze löschen, bis auf die der letzten 10 Tage.

Sie können das Löschen von Logging-Sätzen auch automatisieren, indem Sie in den Betriebsparametern mit *ftmodo* entsprechende Optionen (*-ld*, *-lda*, *-ldd*, *-ldt*) setzen. Dies ist empfehlenswert, wenn Sie Logging-Informationen nur bis zu einem bestimmten Alter behalten wollen. Diese Methode sollte aber nicht verwendet werden, wenn eine lückenlose Langzeit-Archivierung der Logging-Sätze gewünscht ist.

Format

ftdell -h |
[-rg=[[[yyyy]mm]dd]hhmm | -rg=#1..999999999999 | -rg=0..999] |
[-tlf=yyyymmdd[hh[mm[ss]]]]

Beschreibung

-h gibt die Kommandosyntax am Bildschirm aus. Weitere Angaben nach *-h* werden ignoriert.

-rg=[[[yyyy]mm]dd]hhmm
Hier geben Sie mit *-rg* das Ende eines Logging-Zeitbereichs an.

Bei Wahl einer Zeit wird dies wie folgt interpretiert:
- 4-stellig als Uhrzeit in Stunden und Minuten,
- 6-stellig als Tag (Datum) und Uhrzeit in Stunden und Minuten,
- 8-stellig als Monat, Tag und Uhrzeit in Stunden und Minuten,
- 12-stellig als Jahr, Monat, Tag und Uhrzeit in Stunden und Minuten

Der größtmögliche Wert für das anzugebende Datum ist 20380119 (19. Januar 2038).

openFT löscht dann alle Logging-Sätze, die älter sind als die angegebene Zeit. Die optionalen Daten ([...]) werden automatisch durch aktuelle Werte ersetzt.

-rg=#1..999999999999
Hier geben Sie mit *-rg* die Ende-Logging-Id an. Sie ist durch ein führendes #-Zeichen gekennzeichnet, gefolgt von der 1- bis 12-stelligen ID.

openFT löscht dann alle Logging-Sätze, die zu dieser Logging-Id oder einer kleineren Logging-Id gehören.

-rg=0..999
Hier geben Sie mit *-rg* eine relative Zeitdistanz als Vielfaches von 24 Stunden - also die Anzahl von Tagen - an.

openFT löscht dann alle Logging-Sätze, die älter sind als die angegebene Zeit. Man blickt also in der Zeit rückwärts. Wenn Sie z.B. *-rg=2* angeben, so werden alle Logging-Sätze gelöscht, die älter als zwei Tage (48 Stunden) sind.

-rg nicht angegeben
Der Bereich ist nicht Auswahlkriterium, d.h. zu löschen sind alle Logging-Sätze bis 00:00 Uhr des aktuellen Datums.

-tlf=yyyymmdd[hh[mm[ss]]]
Mit *-tlf* löschen Sie alle Offline-Logging-Dateien, die an oder vor dem angegebenen Zeitpunkt (Ortszeit!) durch Umschalten der Logging-Datei auf offline gesetzt wurden. Damit werden nur Logging-Sätze gelöscht, die mindestens so alt sind wie der angegebene Zeitpunkt.

Sie müssen auf jeden Fall das Datum angeben, 8-stellig als Jahr, Monat und Tag, das Jahr muss größer oder gleich 2000 sein. Die Uhrzeit (hhmmss) können Sie teilweise oder ganz weglassen, fehlende Komponenten werden durch 00 ergänzt.

Wenn Sie das aktuelle Datum oder ein Datum in der Zukunft angeben, dann werden alle vorhandenen Offline-Logging-Dateien gelöscht.

Die Optionen *-rg* und *-tlf* dürfen nicht gleichzeitig angegeben werden!

Beispiele

1. Der FT- oder FTAC-Verwalter will alle Logging-Sätze löschen, die bis 00:00 Uhr des aktuellen Datums geschrieben wurden:

   ```
   ftdell
   ```

2. Der FT- oder FTAC-Verwalter will alle Logging-Sätze löschen, die bis zur aktuellen Uhrzeit geschrieben wurden:

   ```
   ftdell -rg=0
   ```

3. Der FT- oder FTAC-Verwalter will alle Logging-Sätze löschen, die vor einem Zeitraum von 7 Tagen (7 mal 24 Stunden vor der aktuellen Zeit) geschrieben wurden:

   ```
   ftdell -rg=7
   ```

4. Der FT- oder FTAC-Verwalter will alle Logging-Sätze von Beginn an bis zu dem mit der Logging-Id Nr. 1450 löschen:

   ```
   ftdell -rg=#1450
   ```

5. Der FT- oder FTAC-Verwalter will alle Offline-Logging-Dateien löschen, die vor dem 01.04.2012 auf offline gesetzt wurden:

   ```
   ftdell -tlf=20120331235959
   ```

6.14 ftdelp - Berechtigungsprofile löschen

ftdelp steht für "delete profile", also Löschen eines Berechtigungsprofils. Durch gelegentliches Durchforsten Ihres Bestandes (mit *ftshwp*) sollten Sie dafür sorgen, dass keine veralteten Berechtigungsprofile stehen bleiben, die unter Umständen die Sicherheit Ihres Systems beeinträchtigen könnten.

Als FTAC-Verwalter dürfen Sie auch Berechtigungsprofile anderer Eigentümer löschen.

Als ADM-Verwalter dürfen Sie auch ADM-Profile löschen (d.h. Berechtigungsprofile mit der Eigenschaft "Zugang zum Fernadministrations-Server").

Format

```
ftdelp  -h  |
          <Profilname 1..8> | @s | @a
        [ -s=[<Zugangsberechtigung 8..32> | @a | @n]
             [,<Benutzerkennung 1..32> | @a | @adm] ]
```

Beschreibung

-h gibt die Kommandosyntax am Bildschirm aus. Weitere Angaben nach *-h* werden ignoriert.

Profilname | **@s** | **@a**
: Hier können Sie den Namen des Berechtigungsprofils angeben, das Sie löschen wollen.

  @s für *Profilname*
  : Löscht das Standard-Berechtigungsprofil der Kennung.

  @a für *Profilname*
  : Sie benutzen den Namen des Berechtigungsprofils nicht als Auswahlkriterium. Wenn Sie nicht mit *-s* (siehe unten) ein Berechtigungsprofil auswählen, löschen Sie alle Ihre Berechtigungsprofile.

-s=[Zugangsberechtigung | **@a** | **@n**][**,**Benutzerkennung | **@a** | **@adm**]
: Mit *-s* können Sie Auswahlkriterien angeben, welche Berechtigungsprofile Sie löschen wollen.

  Zugangsberechtigung
  : Sie wollen das Berechtigungsprofil mit dieser Zugangsberechtigung löschen. Eine binäre Zugangsberechtigung muss in der Form x\'...\' oder X\'...\' angegeben werden.

@a für *Zugangsberechtigung*
: Wenn Sie hier *@a* angeben, löschen Sie entweder das mit Profilname (siehe oben) angesprochene Berechtigungsprofil oder alle Ihre Berechtigungsprofile.

  @a müssen Sie als FTAC-Verwalter angeben, wenn Sie Berechtigungsprofile fremder Benutzerkennungen löschen wollen. Die Zugangsberechtigung sollen Sie nämlich gar nicht kennen.

@n für *Zugangsberechtigung*
: *@n* können Sie als FTAC-Verwalter angeben, wenn Sie nur Berechtigungsprofile fremder Benutzerkennungen löschen wollen, die keine definierte Zugangsberechtigung haben.

Zugangsberechtigung nicht angegeben
: Die Zugangsberechtigung wird nach der Kommandoabgabe am Bildschirm abgefragt. Sie bleibt unsichtbar, um zu verhindern, dass Unbefugte die Zugangsberechtigung sehen. Um Eingabefehler zu vermeiden, wird eine Kontrolleingabe verlangt. Wenn Sie die Eingabeanforderungen nur durch Drücken der Returntaste beantworten, wirkt das wie die Angabe von *@a* im Kommando.

Benutzerkennung
: Als FTAC-Verwalter dürfen Sie jede beliebige Benutzerkennung angeben.

@a für *Benutzerkennung*
: Als FTAC-Verwalter löschen Sie mit *@a* Berechtigungsprofile aller Benutzerkennungen.

@adm für *Benutzerkennung*
: Als FTAC- oder ADM-Verwalter löschen Sie mit *@adm* ADM-Profile.

Benutzerkennung nicht angegeben
: Es werden (unabhängig davon, wer das Kommando absetzt) nur Profile der eigenen Benutzerkennung gelöscht.

-s nicht angegeben
: Falls *@a* für *Profilname* angegeben wurde, werden alle Berechtigungsprofile unter der Benutzerkennung gelöscht, von der aus das *ftdelp* abgesetzt wird. Sonst wird das Berechtigungsprofil mit dem angegebenen Namen gelöscht.

6.15 ftexpc - Konfiguration des Fernadministrations-Servers exportieren

ftexpc steht für "export configuration". Mit *ftexpc* exportieren Sie als Verwalter des Fernadministrations-Servers (= ADM-Verwalter) die Konfigurationsdaten des Fernadministrations-Servers in eine XML-Datei. Der Inhalt der XML-Datei mit der exportierten Konfiguration ist in UTF-8 codiert.

ftexpc können Sie verwenden, wenn Sie eine vorhandene Konfiguration ändern möchten. Dazu exportieren Sie die bestehende Konfiguration mit *ftexpc* in eine XML-Datei, passen diese Datei an (siehe Abschnitt „Konfigurationsdatei per Konfigurations-Editor erstellen“ auf Seite 124 und Abschnitt „Konfigurationsdatei per Text- oder XML-Editor erstellen“ auf Seite 127) und importieren die geänderte Datei anschließend wieder mit *ftimpc*.

Format

ftexpc -h |
<Dateiname 1..512>

Beschreibung

-h gibt die Kommandosyntax am Bildschirm aus. Weitere Angaben nach *-h* werden ignoriert.

Dateiname
gibt den Namen der XML-Datei an, in der die exportierten Konfigurationsdaten abgespeichert werden sollen.

Die Datei wird vom Kommando *ftexpc* angelegt und darf vorher nicht existieren.

6.16 ftexpe - Berechtigungsprofile und -sätze in Datei schreiben

ftexpe steht für "export environment", also Exportieren der FTAC-Umgebung, sprich: Exportieren von Berechtigungsprofilen und -sätzen.

Mit *ftexpe* können Sie als FTAC-Verwalter die Berechtigungsprofile und Berechtigungssätze beliebiger Benutzerkennungen in Dateien schreiben und damit sichern lassen.

Der Standardberechtigungssatz wird nicht mit gesichert. Außerdem werden die variablen Werte in einem Berechtigungssatz (die mit Stern (*) gekennzeichneten Werte), die sich auf den Standardberechtigungssatz beziehen, als Variable gesichert. Das heißt, in der Sicherung liegt kein fester Wert für die betreffende Grundfunktion vor. Wird ein Berechtigungssatz eingespielt, dann erhält die betreffende Grundfunktion den Wert des aktuell gültigen Standardberechtigungssatzes.

So gesicherte Berechtigungsprofile und -sätze können mit dem Kommando *ftimpe* wieder übernommen werden.

Der Zeitstempel eines Berechtigungsprofils wird beim Exportieren oder Importieren nicht geändert.

Format

ftexpe -h |
<Dateiname 1..512>
[-u=<Benutzerkennung 1..32>[,...,<Benutzerkennung(100) 1..32>]]
[-pr=<Profilname 1..8>[,...,<Profilname(100) 1..8>] | -pr=@n]
[-as=y | -as=n]
[-adm=y | -adm=n]

Beschreibung

-h gibt die Kommandosyntax am Bildschirm aus. Weitere Angaben nach *-h* werden ignoriert.

Dateiname
Mit *Dateiname* geben Sie den Namen für die Datei an, in die die Berechtigungsprofile und -sätze geschrieben werden sollen. Sie dürfen auf diese Datei nur mit den Kommandos *ftimpe* und *ftshwe* zugreifen. *Dateiname* darf maximal 512 Zeichen lang sein, und es darf keine gleichnamige Datei in dem Dateiverzeichnis existieren.

-u=Benutzerkennung1[**,**Benutzerkennung2][**,**Benutzerkennung3] ...
Mit *-u* geben Sie die Benutzerkennungen an, deren Berechtigungsprofile und -sätze in einer Datei gesichert werden sollen. Sie können maximal 100 Benutzerkennungen gleichzeitig angeben.

-u nicht angegeben
: Alle Berechtigungsprofile und -sätze, die auf dem Rechner vorhanden sind, werden in der angegebenen Datei gesichert.

-pr=Profilname1[**,**Profilname2][**,**Profilname3]... | **@n**
: Mit *-pr* geben Sie die Berechtigungsprofile an, die in der angegebenen Datei gesichert werden sollen (maximal 100).

  @n für *Profilname*
  : Es werden keine Berechtigungsprofile gesichert.

-pr nicht angegeben
: Es werden alle Berechtigungsprofile gesichert, die zu den beim Parameter *-u* angegebenen Kennungen existieren.

-as=y | **-as=n**
: Mit *-as* geben Sie an, ob die Berechtigungssätze in der angegebenen Datei gesichert werden sollen oder nicht. Mögliche Werte:

  y (Standardwert)
  : Es werden alle Berechtigungssätze gesichert, die zu den beim Parameter *-u* angegebenen Kennungen existieren.

  n Es werden keine Berechtigungssätze gesichert.

-adm=y | **-adm=n**
: Mit *-adm* geben Sie an, ob die ADM-Profile (d.h. Berechtigungsprofile mit der Eigenschaft "Zugang zum Fernadministrations-Server", entspricht *ftcrep -ff=c*) in der angegebenen Datei gesichert werden sollen oder nicht. Mögliche Werte:

  y (Standardwert)
  : Es werden alle ADM-Profile gesichert.

  n ADM-Profile werden nicht gesichert.

Beispiel

Der Berechtigungssatz und die Berechtigungsprofile der Benutzerkennung *donald* sollen gesichert werden. Als Name für die Sicherungsdatei wird *ftacsich* angeben.

```
ftexpe␣ftacsich␣-u=donald
```

6.17 fthelp - Information zu Reason-Codes in den Logging-Sätzen ausgeben

Mit *fthelp* können Sie sich die Bedeutung der Reason-Codes der Logging-Funktion am Bildschirm ausgeben lassen (Spalte RC in der Ausgabe des *ftshwl*).

Außerdem können Sie sich zu den Exitcodes bestimmter FT-Kommandos die zugehörigen Meldungstexte ausgeben lassen.

Format

fthelp -h | <Nummer 1..ffff>

Beschreibung

-h gibt die Kommandosyntax am Bildschirm aus. Weitere Angaben nach *-h* werden ignoriert.

Nummer
steht für einen vierstelligen Reason-Code der Logging-Funktion oder den Exitcode eines FT-Kommandos, der zu einem synchronen FT-Auftrag gehört. Der Reason-Code enthält verschlüsselte Information zu einem Auftrag, der von openFT angenommen worden ist.

Eine Liste der Reason-Codes und ihrer Bedeutungen finden Sie im Abschnitt „Reason-Codes der Logging-Funktion“ auf Seite 331.

Die Exitcodes und die zugehörigen Meldungstexte sind im Abschnitt „Exitcodes und Meldungen zu Administrationskommandos“ auf Seite 453 aufgelistet.

Beispiel

Die Bedeutung des Reason-Codes 3001 soll ermittelt werden.

```
fthelp␣3001

3001 Auftrag zurueckgewiesen. User-Identification ungueltig
```

Der Reason-Code 3001 bedeutet also, dass die angegebene Benutzerkennung oder Zugangsberechtigung ungültig ist.

6.18 ftimpc - Konfiguration des Fernadministrations-Servers importieren

ftimpc steht für "import configuration". Mit *ftimpc* importieren Sie als ADM-Verwalter eine XML-Datei mit Konfigurationsdaten am Fernadministrations-Server. Beim Importieren wird die bestehende Konfiguration überschrieben.

Die XML-Datei muss ein Format besitzen, das dem in der Datei *config.xsd* definierten Schema entspricht. *config.xsd* befindet sich im openFT-Installationsverzeichnis unter dem Verzeichnis *include*. Näheres zum Erstellen einer Konfigurationsdatei finden Sie im Abschnitt „Konfigurationsdatei per Konfigurations-Editor erstellen“ auf Seite 124 und Abschnitt „Konfigurationsdatei per Text- oder XML-Editor erstellen“ auf Seite 127 .

Während des Importierens wird die Konfiguration in der XML-Datei durch den XML-Parser und den XML-Schemavalidierer auf korrekte Syntax und Semantik überprüft. Treten Fehler auf, wird auf *stderr* eine Meldung ausgegeben, bei welchem Element bzw. in welcher Zeile/Spalte der Fehler aufgetreten ist. Die generierten Meldungen sind grundsätzlich in englischer Sprache.

In einigen Fällen kann es vorkommen, dass Sie beim Importieren die Meldung erhalten, dass die Konfigurationsdaten nicht importiert werden können und der asynchrone openFT beendet werden muss. In diesem Fall beenden Sie den asynchronen openFT-Server (z.B. mit dem Kommando *ftstop*), rufen das Kommando *ftimpc* erneut auf und starten den asynchronen openFT-Server wieder (z.B. mit dem Kommando *ftstart*).

ftimpc können Sie verwenden, wenn Sie eine vorhandene Konfiguration ändern möchten. Dazu exportieren Sie die bestehende Konfiguration mit *ftexpc* in eine XML-Datei, passen diese Datei an und importieren die geänderte Datei anschließend wieder mit *ftimpc*.

Der Inhalt der XML-Datei, die mit *ftexpc* exportiert wurde, ist in UTF-8 codiert (siehe Abschnitt „ftexpc - Konfiguration des Fernadministrations-Servers exportieren“ auf Seite 216). Daher sollten Sie eine Import-Datei ebenfalls in UTF-8 codieren.

Format

ftimpc -h |
<Dateiname 1..512>

Beschreibung

-h gibt die Kommandosyntax am Bildschirm aus. Weitere Angaben nach *-h* werden ignoriert.

Dateiname
gibt den Namen der XML-Datei an, die importiert werden soll.

6.19 ftimpe - Berechtigungsprofile und -sätze aus Datei lesen

ftimpe steht für "import environment", also Importieren der FTAC-Umgebung, sprich: Importieren von Berechtigungsprofilen und -sätzen.
Mit *ftimpe* können Sie als FTAC-Verwalter die Berechtigungsprofile und Berechtigungssätze beliebiger Benutzerkennungen aus einer Datei übernehmen, die mit dem Kommando *ftexpe* angelegt wurde.

Es werden nur die Berechtigungsprofile übernommen, deren Profilnamen auf der Kennung noch nicht für andere Berechtigungsprofile vergeben sind.

Wenn schon ein Profil mit demselben Namen vorhanden ist, können Sie anhand des Zeitstempels (LAST-MODIF bei *ftshwp -l*) ersehen, welches den aktuelleren Stand besitzt.

Ein Berechtigungsprofil, dessen Zugangsberechtigung schon für ein anderes Berechtigungsprofil auf dem Rechner vergeben ist, wird zwar eingespielt, hat aber keine definierte Zugangsberechtigung. Es muss vor Gebrauch mit dem Kommando *ftmodp* eine neue Zugangsberechtigung erhalten.
Falls das schon vorhandene Berechtigungsprofil auf dem Rechner als privat gekennzeichnet ist, wird es sofort gesperrt. Das Profil muss ebenfalls vor Gebrauch mit dem Kommando *ftmodp* eine neue Zugangsberechtigung erhalten.

Die eingespielten Berechtigungsprofile sind automatisch gesperrt und müssen vor Gebrauch mit dem Kommando *ftmodp* und dem Parameter *-v=y* entsperrt werden, falls der FTAC-Verwalter keine FT-Verwalterrechte besitzt. Privilegierten Berechtigungsprofilen wird dann beim Einlesen das Privileg entzogen. Wenn der FTAC-Verwalter auch FT-Verwalterrechte besitzt, kann er das Verhalten mit der Option *-sec* steuern.

Da der Standardberechtigungssatz beim Exportieren nicht gesichert wird, bleibt beim Importieren der auf dem Rechner vorliegende Standardberechtigungssatz gültig. Variable Werte in den importierten Berechtigungssätzen, die sich auf den Standardberechtigungssatz beziehen und deshalb mit einem Stern (∗) gekennzeichnet sind, erhalten den Wert des aktuell gültigen Standardberechtigungssatzes.

Format

```
ftimpe -h  |
          <Dateiname 1.512>
        [ -u=<Benutzerkennung 1..32>[,...,<Benutzerkennung(100) 1..32>] ]
        [ -pr=<Profilname 1..8>[,...,<Profilname(100) 1..8>] | -pr=@n ]
        [ -as=y | -as=n ]
        [ -sec=s | -sec=h ]
        [ -adm=y | -adm= n ]
```

Beschreibung

-h gibt die Kommandosyntax am Bildschirm aus. Weitere Angaben nach *-h* werden ignoriert.

Dateiname
: Mit *Dateiname* geben Sie den Namen der Sicherungsdatei an, aus der die Berechtigungsprofile und -sätze übernommen werden sollen.

-u=Benutzerkennung1[**,**Benutzerkennung2][**,**Benutzerkennung3]...
: Mit *-u* geben Sie die Benutzerkennungen an, deren Berechtigungsprofile und -sätze übernommen werden sollen. Sie können maximal 100 Benutzerkennungen gleichzeitig angeben.

-u nicht angegeben
: Es werden alle Berechtigungsprofile und -sätze übernommen.

-pr=Profilname1[**,**Profilname2][**,**Profilname3]...| **-pr=@n**
: Mit *-pr* geben Sie die Berechtigungsprofile an, die übernommen werden sollen (maximal 100).

  @n für *Profilname*
  : Es werden keine Berechtigungsprofile übernommen.

-pr nicht angegeben
: Es werden alle Berechtigungsprofile übernommen, die zu den beim Parameter *-u* angegebenen Kennungen existieren. Ausnahme: Unter dem Profilnamen existiert schon ein Berechtigungsprofil auf der Kennung. Dann wird das Profil nicht eingespielt.

-as=y | **-as=n**
: Mit *-as* geben Sie an, ob Berechtigungssätze übernommen werden sollen oder nicht. Mögliche Werte:

  y (Standardwert)
  : Es werden alle Berechtigungssätze übernommen, die zu den beim Parameter *-u* angegebenen Kennungen existieren.

  n Es werden keine Berechtigungssätze übernommen.

-sec=s | **-sec=h**

Mit *-sec* geben Sie die Sicherheitsstufe beim Importieren von Berechtigungsprofilen an. Die Option *-sec* ist nur sinnvoll, wenn Sie als FTAC-Verwalter auch FT-Verwalterrechte besitzen.

s (standard) Wenn Sie FT-Verwalterrechte haben, dann werden die Attribute der Berechtigungsprofile beim Importieren nicht verändert.

Wenn Sie keine FT-Verwalterrechte haben, dann wirkt dies wie *-sec=h*, d.h. die Profile werden gesperrt.

-sec=s ist Standardwert.

h (high) Die Berechtigungsprofile werden gesperrt (LOCKED (by import)) und erhalten die Attribute *privat* sowie *nicht-privilegiert*.

-adm=y | **-adm=n**

Mit *-adm* geben Sie an, ob ADM-Profile (d.h. Berechtigungsprofile mit der Eigenschaft "Zugang zum Fernadministrations-Server", entspricht *ftcrep -ff=c*) übernommen werden sollen oder nicht. Mögliche Werte:

y (Standardwert)
ADM-Profile werden übernommen. Diese Option ist nur erlaubt, wenn auf dem Zielrechner ein ADM-Verwalter konfiguriert ist.

n ADM-Profile werden nicht übernommen.

Beispiel

Der Berechtigungssatz und die Berechtigungsprofile der Benutzerkennung *donald* wurden mit *ftexpe* in die Datei *ftacsich* gesichert. Sie sollen auf einem anderen Rechner unter der gleichen Kennung wieder eingespielt werden.

```
ftimpe␣ftacsich␣-u=donald
```

Als FTAC-Verwalter können Sie zum Beispiel folgende Meldungen erhalten:

```
OWNER    NAME
donald   geheim1     FT-Profil existiert bereits.
         geheim2
```

Daraus können Sie schließen, dass *donald* auf dem neuen Rechner schon die Berechtigungsprofile *geheim1* und *geheim2* angelegt hat und somit diese Profile nicht eingespielt wurden.

Wollen Sie nach dem Importieren einen Berechtigungssatz für eine auf Ihrem Rechner nicht existierende Kennung löschen, geben Sie das Kommando *ftmoda␣kennung␣-ml=s* ein. Diese Situation kann zum Beispiel dadurch entstehen, dass Sie eine mit *ftexpe* auf einem anderen Rechner erzeugte Datei auf Ihrem Rechner eingespielt haben.

6.20 ftimpk - RSA-Schlüssel importieren

Mit dem Kommando *ftimpk* (import key) können Sie als FT-Verwalter den öffentlichen Schlüssel eines Partners oder ein RSA-Schlüsselpaar aus einer Datei importieren. Die Datei wird vom Erzeuger des Schlüssels/RSA-Schlüsselpaars zur Verfügung gestellt. Der Partnerschlüssel bzw. das RSA-Schlüsselpaar werden beim Importieren an der "richtigen" Stelle im openFT-Instanzenverzeichnis abgelegt und können danach für die Authentifizierung verwendet werden.

Öffentlichen Schlüssel eines Partnes importieren

Wenn Sie einen öffentlichen Schlüssel eines Partners importieren möchten, dann muss dieser Partner in der Partnerliste eingetragen sein. Der Schlüssel wird im Unterverzeichnis *syskey* mit der Partner-Identifikation als Dateiname abgelegt.

RSA-Schlüsselpaar importieren

Sie können ein RSA-Schlüsselpaar importieren, das aus einem öffentlichen und einem privaten Schlüssel besteht. Das Schlüsselpaar kann wie ein von openFT erzeugter Schlüssel für die Datenverschlüsselung und die Authentifizierung verwendet werden.

Das Schlüsselpaar kann mit einem externen Tool erzeugt worden sein. Die Schlüssel müssen die Länge 768, 1024 oder 2048 Bit besitzen. Die Schlüssel können im PEM-Format vorliegen (native PEM oder PKCS#8 Format ohne Passwort-Phrase oder nach v1 / v2 mit einer Passwort-Phrase) oder im Format PKCS#12 V1.0.

Verlangt das Schlüsselpaar eine Passwort-Phrase (Kennwort), dann muss diese beim Importieren angegeben werden.

Beim Importieren gilt dasselbe wie für Schlüsselpaare, die mit *ftcrek* erzeugt werden:

- Das Schlüsselpaar erhält eine eindeutige Referenznummer.
- Der öffentliche Schlüssel wird abgelegt unter dem Namen **syspkf.r<schlüsselreferenz>.l<schlüssellänge>** im Verzeichnis *config* des Instanzdateibaums der openFT-Instanz.

Einzelheiten siehe Abschnitt „Lokale RSA-Schlüsselpaare erzeugen und verwalten“ auf Seite 81.

Format

ftimpk -h |
[-pr=<Dateiname 1..512>]
[-pu=<Dateiname 1..512>]
[-p=<Kennwort 1..64> | -p=]
[-p12]

Beschreibung

-h gibt die Kommandosyntax am Bildschirm aus. Weitere Angaben nach *-h* werden ignoriert.

-pr=Dateiname
(private) gibt an, dass ein privater und ein öffentlicher Schlüssel importiert werden. *Dateiname* ist der absolute oder relative Pfadname der Datei, die die beiden Schlüssel enthält.

-pu=Dateiname
(public) gibt an, dass nur ein öffentlicher Schlüssel importiert wird. *Dateiname* ist der absolute oder relative Pfadname der Datei, die den Schlüssel enthält.

Sie müssen immer entweder *-pr* oder *-pu* angeben!

-p=Kennwort | **-p=**
gibt das Kennwort an, wenn der/die Schlüssel mit einem Kennwort geschützt ist/sind.

kein Kennwort angegeben
Wenn Sie *-p=* ohne Kennwort angeben, dann wird das Kennwort nach Abschicken des Kommandos am Bildschirm abgefragt. Ihre Eingabe bleibt unsichtbar, um zu verhindern, dass Unbefugte das Kennwort sehen.

-p nicht angegeben
Der/die Schlüssel ist/sind nicht durch ein Kennwort geschützt, Standard.

-p12 Die Schlüsseldatei enthält ein Zertifikat und einen privaten Schlüssel entsprechend dem Standard PKCS#12 V1.0. Die Datei wird nach einem privaten Schlüssel durchsucht, nicht unterstützte Bestandteile (z.B. Zertifikate, CRLs) werden beim Importieren ignoriert. Der erste private Schlüssel, der in der Datei gefunden wird, wird importiert, weitere werden ignoriert.

Ist das Zertifikat per Signatur oder Hash geschützt, dann führt openFT keine Gültigkeitsprüfung durch. Die Gültigkeit der Datei muss durch externe Mittel sichergestellt werden.

-p12 nicht angegeben
Der private Schlüssel liegt im PEM-Format vor, Standard.

Beispiele

1. Sie möchten den öffentlichen Schlüssel aus der Datei clientkey1 importieren (ohne Kennwort).

   ```
   ftimpk -pu=clientkey1
   ```

2. Sie möchten einen per Tool erzeugten RSA-Schlüssel im PEM-Format aus der Datei rsakeys20120303 importieren. Die Schlüssel sind mit einem Kennwort geschützt, das Sie unsichtbar am Bildschirm (dunkel) eingeben möchten.

   ```
   ftimpk -pr=rsakeys20120303 -p=
   ```

6.21 ftlang - Standardeinstellung für Sprache wechseln

Während der Installation wird durch Auswerten der Umgebungsvariablen LANG die Standardsprache für openFT festgelegt (Linux, Solaris, AIX) bzw. in HP-UX standardmäßig auf Englisch gesetzt.

Sie können diese Festlegung nachträglich ändern, indem Sie die Shellprozedur */opt/openFT/bin/ftbin/ftlang* verwenden. Weitere Einzelheiten zur Spracheinstellung finden Sie in Abschnitt „Sprachoberfläche wechseln“ auf Seite 61.

Format

```
ftlang [ -h  |
         -i |
         de |
         en ]
```

Beschreibung

-h gibt die Kommandosyntax am Bildschirm aus. Weitere Angaben nach *-h* werden ignoriert.

-i mit diesem Schalter können Sie die aktuell eingestellte Sprachvariante abfragen.

de openFT wird standardmäßig auf deutsche Sprache umgeschaltet.

en openFT wird standardmäßig auf englische Sprache umgeschaltet.

In beiden Fällen werden die jeweils benötigten Meldungsdateien, die *fthelp*-Prozedur, die man pages (Solaris, AIX und HP-UX) sowie der openFT Explorer einschließlich der Hilfetexte für die gewählte Sprache aktiviert.

Beispiel

1. Prüfen welche Sprache eingestellt ist:

   ```
   /opt/openFT/bin/ftbin/ftlang -i
   en
   ```

2. Die Standardeinstellung der Sprache wird von Englisch auf Deutsch umgeschaltet:

   ```
   /opt/openFT/bin/ftbin/ftlang␣de
   ```

6.22 ftmoda - Berechtigungssätze ändern

ftmoda steht für "modify admission set", also Ändern des Berechtigungssatzes.

Als FTAC-Verwalter können Sie mit diesem Kommando Festlegungen für den Standardberechtigungssatz und für jeden Berechtigungssatz von jedem Benutzer im System treffen. Die Festlegungen des Verwalters für Berechtigungssätze anderer Benutzer sind die MAX. ADM LEVELS.

Sie können für jede Grundfunktion eine Sicherheitsstufe zwischen 0 und 100 vergeben. Diese Werte haben folgende Bedeutung:

0 Die Grundfunktion ist gesperrt, d.h. sie ist für kein Partnersystem freigegeben.

1 bis **99**
Die Grundfunktion ist nur für Partnersysteme mit gleicher oder niedrigerer Sicherheitsstufe freigegeben. Die Sicherheitsstufe eines Partnersystems können Sie sich mit dem Kommando *ftshwptn* anzeigen lassen.

100 Die Grundfunktion ist für alle Partnersysteme freigegeben.

Beachten Sie zu den Grundfunktionen auch die Tabelle auf Seite 231.

Zusätzlich haben Sie als FTAC- bzw. ADM-Verwalter die Möglichkeit, mit *ftmoda* die FTAC-Verwalterrechte bzw. die ADM-Verwalterrechte auf eine andere Benutzerkennung zu übertragen.

Format

```
ftmoda -h |
        [ <Benutzerkennung 1..32> | @s ]
        [ -priv=y ]
        [ -admpriv=y ]
        [ -ml=s | -ml=0..100 ]
        [ -os=s | -os=0..100 ]
        [ -or=s | -or=0..100 ]
        [ -is=s | -is=0..100 ]
        [ -ir=s | -ir=0..100 ]
        [ -ip=s | -ip=0..100 ]
        [ -if=s | -if=0..100 ]
```

Beschreibung

-h gibt die Kommandosyntax am Bildschirm aus. Weitere Angaben nach *-h* werden ignoriert.

Benutzerkennung | **@s** Als FTAC-Verwalter dürfen Sie jede beliebige Benutzerkennung sowie *@s* angeben.

@s für *Benutzerkennung*
Mit *@s* können Sie als FTAC-Verwalter den Standardberechtigungssatz ändern.

Benutzerkennung nicht angegeben
Damit wird der Berechtigungssatz der Kennung geändert, unter der das Kommando eingegeben wurde.

-priv=y
Mit dieser Angabe können Sie als FTAC-Verwalter die Verwaltereigenschaft an die mit *Benutzerkennung* spezifizierte Benutzerkennung weitergeben.

-priv nicht angegeben
Der FTAC-Verwalter bleibt derselbe.

-admpriv=y
Mit dieser Angabe können Sie als ADM-Verwalter die Administrationsberechtigung für den Fernadministrations-Server an die mit *Benutzerkennung* spezifizierte Benutzerkennung weitergeben.
Zusätzlich werden alle mit *-ff=c* definierten Profile an die neue Benutzerkennung weitergeleitet. Falls es auf der neuen Benutzerkennung gleichnamige Profile gibt, wird das Kommando abgelehnt.

Falls es noch keinen ADM-Verwalter auf dem Fernadministrations-Server gibt, müssen Sie als FTAC-Verwalter **zuerst** den ADM-Verwalter mit *-admpriv=* festlegen. Andernfalls lässt sich der Fernadministrations-Server nicht administrieren, d.h. dass beispielsweise auch die Konfigurationsdatei nicht mit *ftimpc* importiert werden kann.

-admpriv nicht angegeben
Der ADM-Verwalter bleibt derselbe.

-ml=s | **-ml=0**..**100**
trifft für alle sechs Grundfunktionen dieselbe Festlegung.

Mögliche Werte:

s Für alle Grundfunktionen gelten die Vorgaben des Standardberechtigungssatzes.

0 Alle Grundfunktionen werden gesperrt.

1 bis **99**
Sämtliche Grundfunktionen werden nur für die Partnersysteme freigegeben, deren Sicherheitsstufe kleiner oder gleich dem angegebenen Wert ist.

100 Alle Grundfunktionen werden für alle Partnersysteme freigegeben. Für Outbound-Datei-Management-Funktionen findet keine Prüfung statt.

-ml nicht angegeben
Die Festlegungen des Berechtigungssatzes bleiben unverändert, falls nicht eine der folgenden Angaben gemacht wird.

-os=s | **-os=0**..**100**
trifft die Festlegung für die Grundfunktion *outbound senden*, mögliche Werte siehe Seite 231. *outbound senden* bedeutet, dass mit Initiative im lokalen Rechner Daten an ein Partnersystem geschickt werden.

-or=s | **-or=0**..**100**
trifft die Festlegung für die Grundfunktion *outbound empfangen*, mögliche Werte siehe Seite 231. *outbound empfangen* bedeutet, dass mit Initiative im lokalen Rechner Daten aus einem Partnersystem geholt werden.

-is=s | **-is=0**..**100**
trifft die Festlegung für die Grundfunktion *inbound senden*, mögliche Werte siehe Seite 231. *inbound senden* bedeutet, dass ein Partnersystem Daten vom lokalen Rechner holt.

-ir=s | **-ir=0**..**100**
trifft die Festlegung für die Grundfunktion *inbound empfangen*, mögliche Werte siehe Seite 231. *inbound empfangen* bedeutet, dass ein Partnersystem Daten zum lokalen Rechner schickt.

-ip=s | **-ip=0**..**100**
trifft die Festlegung für die Grundfunktion *inbound Folgeverarbeitung + Vorverarbeitung + Nachverarbeitung*, mögliche Werte siehe Seite 231. Es wird festgelegt, ob ein Partnersystem eine Folge-, Vor- oder Nachverarbeitung auf dem lokalen Rechner ausführen darf.

-if=s | **-if=0**..**100**
trifft die Festlegung für die Grundfunktion *inbound Dateimanagement*, mögliche Werte siehe Seite 231.

Beachten Sie bitte, dass einige Teilkomponenten von *inbound Dateimanagement* auch von anderen Einstellungen abhängen, siehe „Abhängigkeiten bei Inbound Dateimanagement“ auf Seite 231.

-os, *-or*, *-is*, *-ir*, *-ip* oder *-if* nicht angegeben
Die Vorgabe für die betreffende Grundfunktion wird nicht geändert.

Mögliche Werte für die Grundfunktionen

Für die einzelnen Grundfunktionen (*-os*, *-or, -is, -ir*, *-ip* und *-if*) sind folgende Werte möglich:

s Für die Grundfunktion gelten die Vorgaben des Standardberechtigungssatzes.

0 Die Grundfunktion wird gesperrt.
Dies kann sich bei einigen Grundfunktionen auch auf Komponenten von Inbound Dateimanagement auswirken, siehe Tabelle auf Seite 231.

1 bis **99**
Die Grundfunktion wird nur für die Partnersysteme freigegeben, deren Sicherheitsstufe kleiner oder gleich dem angegebenen Wert ist.

100 Die Grundfunktion wird für alle Partnersysteme freigegeben.

Abhängigkeiten bei Inbound Dateimanagement

Die Teilkomponente "Dateiattribute anzeigen" wird über die Grundfunktion *inbound senden* gesteuert, außerdem gibt es bei einigen Komponenten folgende Abhängigkeiten von anderen Einstellungen:

Inbound Dateimanagement-Funktion	**Einstellung im Berechtigungssatz bzw. Erweiterung im Profil**
Dateiattribute anzeigen	Inbound Senden (IBS) erlaubt
Dateiattribute ändern	Inbound Empfangen (IBR) **und** Inbound Dateimanagement (IBF) erlaubt
Dateien umbenennen	Inbound Empfangen (IBR) **und** Inbound Dateimanagement (IBF) erlaubt
Dateien löschen	Inbound Empfangen (IBR) erlaubt **und** Schreibregel = überschreiben im Profil
Dateiverzeichnisse anzeigen	Inbound Dateimanagement (IBF) erlaubt
Dateiverzeichnisse anlegen, umbenennen, löschen	Inbound Dateimanagement (IBF) erlaubt **und** Richtung = vom Partner im Profil

6.23 ftmodi - Modifizieren einer Instanz

Mit dem Kommando *ftmodi* können Sie einer Instanz einen anderen Internet-Hostnamen zuordnen.

Hinweis zur Nutzung mehrerer Instanzen

Sie müssen allen Instanzen explizit einen eigenen Hostnamen zuordnen (Option *-addr* bei *ftmodi* bzw. *ftcrei*). Dies gilt auch für die Standardinstanz.

Format

ftmodi -h | <Instanz 1..8> [-addr=<Hostname> | -addr=@n]

Beschreibung

-h gibt die Kommandosyntax am Bildschirm aus. Weitere Angaben nach *-h* werden ignoriert.

Instanz

Name der Instanz, die modifiziert werden soll.
Instanznamen haben eine maximale Länge von 8 Zeichen und müssen aus alphanumerischen Zeichen zusammengesetzt sein, wobei das erste Zeichen nicht numerisch sein darf.

-addr=Hostname | **-addr=@n**

Internet-Hostname, über dessen zugeordnete IP-Adresse die Instanz von außen angesprochen wird (Zieladresse) bzw. die als Absenderadresse bei abgehenden Verbindungen verwendet wird. Eine Änderung von *-addr* wirkt sich nicht auf die Betriebsparameter *Instanzidentifikation* und *Prozessor* der Instanz aus.

Hostname

Hiermit kann der Instanz ein bestimmter bzw. ein anderer Internet-Hostname zugeordnet werden.

@n für *Hostname*

Diese Angabe ist nur für die Standardinstanz *std* zulässig.

Der Standardinstanz ist damit keine bestimmte Hostadresse mehr zugewiesen, sie meldet sich daher für alle Adressen des Systems an.

Auf diese Weise kann von einem Mehrinstanzen-Betrieb auf einen Eininstanzen-Betrieb zurückgeschaltet werden.

Beispiele

1. Der Standardinstanz wird der Host mit dem Namen AHORN zugewiesen. Lokale Aufträge an 127.0.0.1 sind damit nicht mehr möglich.
   Das Kommando lautet:

   ```
   ftmodi std -addr=AHORN
   ```

2. Die Standardinstanz soll sich wieder an alle IP-Adressen eines Systems anmelden und an allen Adressen horchen. Das Kommando lautet:

   ```
   ftmodi std -addr=@n
   ```

Meldungen des ftmodi-Kommandos

Konnte *ftmodi* nicht ordnungsgemäß ausgeführt werden, dann wird eine selbsterklärende Meldung ausgegeben; der Exitcode ist dann ungleich 0.

6.24 ftmodk - RSA-Schlüssel modifizieren

Mit dem Kommando *ftmodk* können Sie das Verfallsdatum und die Authentifizierungsstufe von Schlüsseln ändern, die zur Authentifizierung von Partnersystemen verwendet werden. Die Änderungen werden in der jeweiligen Schlüsseldatei gespeichert.

Nachdem das Verfallsdatum eines Schlüssels erreicht wurde, wird die Authentifizierung mit diesem Schlüssel abgelehnt. Sie können das Verfallsdatum jedoch noch nach Ablauf modifizieren, z.B. um einen Schlüssel kurzzeitig wieder freizuschalten, damit ein aktueller Schlüssel sicher übertragen werden kann.

Format

ftmodk –h |
[-id=<Identifikation 1..64> | -id=@a] |
[-pn=<Partner 1..200> | -pn=@a]
[-al=1 | -al=2]
[-exp=[yyyymmdd]]

Beschreibung

-h gibt die Kommandosyntax am Bildschirm aus. Weitere Angaben nach *-h* werden ignoriert.

-id=Identifikation | **-id=@a**
Identifikation ist die Instanzidentifikation des Partners, dessen Schlüssel modifiziert wird. *-id* darf nicht zusammen mit *-pn* angegeben werden.

@a Es werden die installierten Schlüssel von allen Partnersystemen modifiziert.

-pn=Partner | **-pn=@a**
Partner ist der Name des Partnersystems in der Partnerliste oder die Adresse des Partnersystems, dessen Schlüssel modifiziert wird.
-pn darf nicht zusammen mit *-id* angegeben werden.

Einzelheiten zur Adressangabe finden Sie in Abschnitt „Aufbau der Partneradressen“ auf Seite 68.

@a Es werden die installierten Schlüssel von allen Partnersystemen modifiziert.

weder *-id* noch *-pn* angegeben
Es werden die installierten Schlüssel von allen Partnersystemen modifiziert.

-al=1 | **-al=2**
(authentication level) Gibt die Authentifizierungsstufe für den/die Schlüssel an.

1 Die Authentifizierungsstufe für den/die Partner wird auf 1 gesetzt. Dies entspricht den Möglichkeiten bis openFT V11.0A.

Wird das Partnersystem zu einem späteren Zeitpunkt nach Stufe 2 authentifiziert, wird automatisch AUTHENTICATION-LEVEL=2 in seiner Schlüsseldatei vermerkt.

2 Das Partnersystem unterstützt das mit openFT V11.0B eingeführte Authentifizierungsverfahren der Stufe 2. Ein Authentifizierungsversuch nach Stufe 1 wird abgelehnt.

-al nicht angegeben
Die Authentifizierungsstufe bleibt unverändert.

-exp=[yyyymmdd]
legt das Verfallsdatum des Schlüssels / der Schlüssel fest.

yyyymmdd
Verfallsdatum im Format yyyymmdd, z.B. 20121231 für den 31.12.2012. Der/die Schlüssel kann/können maximal bis zum angegebenen Datum 00:00 Uhr zur Authentifizierung verwendet werden.

kein Datum angegeben
exp= ohne Datumsangabe bedeutet kein Verfallsdatum für den/die Schlüssel.

-exp nicht angegeben
Das Verfallsdatum des Schlüssels / der Schlüssel bleibt unverändert.

6.25 ftmodo - Betriebsparameter ändern

Mit *ftmodo* können Sie folgende Parameter des openFT-Betriebes festlegen und ändern:

- die Schlüssellänge des RSA-Schlüssels
- die Maximalwerte für die Dateiübertragung
- die Identifikation und den Namen des lokalen Systems
- den Standardwert für die Sicherheitsstufe
- den Modus für die Absenderüberprüfung
- den Umfang der Protokollierung (Traces, Logging, Konsolen-Traps und ADM-Traps)
- das automatische Löschen von Logging-Sätzen
- das Umschalten der Logging-Datei und der Trace-Datei
- den Umfang der Messdatenerfassung
- die Variante der verwendeten Code-Tabelle
- die Adressen für die einzelnen Protokolle
- die Einstellungen für den Fernadministrations-Server
- die Verwendung von TNS und CMX
- die Einstellungen für die Benutzerdatenverschlüsselung

Für den FTAM-Betrieb können Sie außerdem den Application Entity Title (AET) ein- oder ausschalten.

Sie können die Betriebsparameter (Ausnahme: Ausschalten des Application Entity Title) auch über den openFT Explorer ändern.

Format

```
ftmodo  -h
        [ -kl=0 | -kl=768 | -kl=1024 | -kl=2048 ]
        [ -tu=<Nachrichtenlänge 512..65535>]
        [ -pl=1 | -pl= ]
        [ -cl=<Verbindungslimit 1..255> ]
        [ -admcl=<Verbindungslimit 1..255> ]
        [ -admcs=n | -admcs=y ]
        [ -rql=<Maximale Anzahl Aufträge 2..32000> ]
        [ -rqt=<Auftrags-Lebensdauer 1..400> | -rqt= ]
        [ -id=<Identifikation 1..64> ]
        [ -p=<Prozessorname 1..8>] [ -l=<Stationsname 1..8> ]
        [ -sl=<Sicherheitsstufe 1..100> | -sl=p ][ -ptc=i | -ptc=a ]
        [ -lf=c ][ -lt=a | lt=f | lt=n] [ -lc=a | -lc=m | -lc=r ]
        [ -la=a | -la=f | -la=m | -la=n ]
        [ -ld=n | -ld=f ][ -lda=<0..999> ][ -ldt=hhmm ]
        [ -ldd=@d | Mo | Tu | We | Th | Fr | Sa | Su | <1..31> ]
        [ -mon=n | -mon=f ][ -monr=[l|r][a|s] ]
        [ -monp=a | -monp=[openft][,][ftam][,][ftp] ]
        [ -tr=n | -tr=f | -tr=c ]
        [ -trp=a | -trp=[openft][,][ftam][,][ftp][,][adm] ]
        [ -trr=[l | r][a | s] ][ -tro=[b] ][ -troll=[s | d] ]
        [ -atpsv=[<Partner 1..200>][,][<Zugangsberechtigung 8..67> | @d ] ]
        [ -atp=a | -atp=n | -atp=[[-]fts],[[-]rqs],[[-]rqc],
                                [[-]rqf],[[-]pts],[[-]ptu] ]
        [ -tpc=a | -tpc=n | -tpc=[[-]sss],[[-]fts],
                            [[-]rqs],[[-]rqc],[[-]rqf],[[-]pts],[[-]ptu] ]
        [ -ccs=<CCS-Name 1..8> ]
        [ -acta=a | -acta=[openft][,][ftam][,][ftp][,][adm] ]
        [ -ftp=<Portnummer 1..65535> | -ftp=@s]
        [ -openft=[<Portnummer 1..65535>][.<T-Sel 1..8>]  |
          -openft=@s ]
        [ -ftam=[<Portnummer 1..65535>][.<T-Sel>[.<S-Sel>[.<P-Sel>]]] |
          -ftam=@s ]
        [ -adm=<Portnummer 1..65535> | -adm=@s ]
        [ -ftstd=<Portnummer 1..65535> | -ftstd=@s ]
        [ -tns=y | -tns=n ]
        [ -cmx=y | -cmx=n ]
        [ -ae=y | -ae=n ]
        [ -dp=n | -dp=f ]
        [ -c= | -c=i | -c=o | -c=io | -c=oi ]
```

Beschreibung

-h gibt die Kommandosyntax am Bildschirm aus. Weitere Angaben nach *-h* werden ignoriert.

-kl=0 | **-kl=768** | **-kl=1024** | **-kl=2048**
Mit dem Parameter *-kl* kann die Länge des beim Verschlüsseln verwendeten RSA-Schlüssels verändert werden. Der Wert des *-kl*-Parameters gibt die neue RSA-Schlüssellänge in Bit an. Der RSA-Schlüssel dient nur zum Verschlüsseln des zwischen den Partnern vereinbarten AES-Schlüssels (bzw. des DES-Schlüssels bis openFT V7.0).
openFT verwendet den AES-Schlüssel für die Verschlüsselung der Auftragsbeschreibungsdaten und ggf. auch des Dateiinhalts.

Das Kommando *ftmodo -kl=*... kann im laufenden openFT-Betrieb gegeben werden.

Mit *-kl=0* wird die Verschlüsselung explizit abgeschaltet. Dies bewirkt im laufenden Betrieb, dass bereits eingestellte, aber noch nicht gestartete Aufträge mit Verschlüsselung (vor dem *ftmodo -kl=0*) mit Fehler abgebrochen werden. Laufende Aufträge werden abgearbeitet, die Verschlüsselung bleibt erhalten. Neue Aufträge mit Verschlüsselung werden abgewiesen.

Voreinstellung nach Neuinstallation: *-kl=2048*.

-tu=Nachrichtenlänge
Mit dem Parameter *-tu* legen Sie die Obergrenze für die Nachrichtenlänge auf Transportebene fest (Blocklänge). Der Wert kann von 512 bis 65535 gewählt werden.

Die Blocklänge gilt nur für Aufträge zu openFT-Partnern.

Voreinstellung nach Neuinstallation: *-tu=65535*.

-pl=1 | **-pl=**
Maximale Anzahl der Prozesse, die für die Bearbeitung asynchroner Aufträge verwendet werden.

1 Alle asynchronen Aufträge werden von demselben Prozess bearbeitet.

keine Anzahl angegeben
Wenn Sie *-pl=* ohne Parameter angeben, dann entspricht die Anzahl der Prozesse der Anzahl der Verbindungen, d.h. jede Verbindung wird von einem eigenen Prozess bearbeitet.

Voreinstellung nach Neuinstallation: *-pl=* (d.h. keine Anzahl angegeben).

-cl=Verbindungslimit
: Maximale Anzahl der asynchronen Aufträge, die simultan bearbeitet werden. Mögliche Werte: 1 bis 255.

  Voreinstellung nach Neuinstallation: *-cl=16*.

-admcl=Verbindungslimit
: Maximale Anzahl der Verbindungen, die für Fernadministrations-Aufträge bereitgestellt werden. Mögliche Werte: 1 bis 255.

  Beachten Sie bitte den Hinweis bei *-admcs*.

  Voreinstellung nach Neuinstallation: *-admcl=8*.

-admcs=n | **-admcs=y**
: legt fest, ob die lokale openFT-Instanz als Fernadministrations-Server gekennzeichnet ist.

  y kennzeichnet die lokale openFT-Instanz als Fernadministrations-Server. Damit kann diese Instanz auch ADM-Trap-Server sein.

  n Die lokale openFT-Instanz ist nicht (mehr) als Fernadministrations-Server gekennzeichnet. Damit können auch keine ADM-Traps (mehr) empfangen werden. Dies ist der Standardwert nach Neuinstallation.

  Wenn Sie *-admcs* angeben, *-admcl* aber nicht, dann setzt openFT das Verbindungslimit (*-admcl*) auf folgenden Wert:

  64 bei *-admcs=y*.

  8 bei *-admcs=n*.

  Voreinstellung nach Neuinstallation: *-admcs=n*.

-rql=Maximale Anzahl Aufträge
: Mit *-rql* geben Sie die maximale Anzahl von Einträgen im Auftragsbuch an. Der Wert kann von 2 bis 32000 gewählt werden.

  Voreinstellung nach Neuinstallation: *-rql=2000*.

-rqt=Auftrags-Lebensdauer | **-rqt=**
: Mit *-rqt* geben Sie die maximale Lebensdauer von Aufträgen im Auftragsbuch an. Der Wert gilt für Inbound- und Outbound-Aufträge und wird in Tagen angegeben, erlaubt sind Werte von 1 bis 400 Tagen. Nach Ablauf dieser Frist werden Aufträge aus dem Auftragsbuch gelöscht.

  Auftrags-Lebensdauer nicht angegeben:
  : Wenn Sie *-rqt=* ohne Parameter angeben, dann ist die maximale Lebensdauer unbegrenzt.

  Voreinstellung nach Neuinstallation: *-rqt=30*.

-id=Identifikation
: Angabe der Instanzidentifikation Ihrer Instanz. Partnersysteme mit openFT ab Version 8.1 adressieren Ihr System über diesen String. Umgekehrt verwendet openFT gegenüber diesen Partnern die Instanzidentifikation als Absenderadresse. Die Instanzidentifikation muss unabhängig von Groß- und Kleinschreibung eindeutig sein (siehe auch Abschnitt „Instanzidentifikationen“ auf Seite 80). Wenn Sie die Instanzidentifikation ändern, werden die gültigen öffentlichen Schlüsseldateien automatisch aktualisiert.

  Voreinstellung nach Neuinstallation: *-id= lokaler DNS-Name oder Host-Name*.

-p=Prozessorname
: Hier geben Sie den für Ihren Rechner vergebenen Prozessornamen an.

  Nach einer Neuinstallation ist kein Prozessorname angegeben.

-l=Stationsname
: Stationsname der openFT-Anwendung.

  Voreinstellung nach Neuinstallation: *-l=$FJAM*.

Die Angaben für *Prozessorname* und *Stationsname* hängen davon ab, wie Ihr Rechner an das Netz angeschlossen ist. Näheres dazu finden Sie im Kapitel „Installation“ auf Seite 25.

-sl=Sicherheitsstufe | **-sl=p**
: Mit dieser Option wird die Standard-Sicherheitsstufe festgelegt. Diese gilt für Partner in der Partnerliste, denen beim Eintragen mit *ftaddptn* kein expliziter Wert für die Sicherheitsstufe zugeordnet wurde. Die Wirkung hängt auch von den Einstellungen des Berechtigungssatzes ab, siehe Kommando *ftmoda* auf Seite 228.

  Sicherheitsstufe
  : Legt eine feste Standard-Sicherheitsstufe fest. Erlaubt sind Werte von 1 bis 100. 1 bedeutet sehr niedriges Schutzbedürfnis und 100 bedeutet sehr hohes Schutzbedürfnis gegenüber den Partnern.

  p Die Standard-Sicherheitsstufe hängt von den Attributen des Partners ab:

  – Sicherheitsstufe 10, wenn der Partner authentifiziert ist.

  – Sicherheitsstufe 90, wenn der Partner im Transportsystem bekannt ist und über seinen im Transportsystem bekannten Namen identifiziert wird.

  – Sicherheitsstufe 100 sonst, d.h. wenn der Partner nur über seine Adresse identifiziert wird.

  Voreinstellung nach Neuinstallation: *-sl=p*.

-ptc=i | **-ptc=a**
Hiermit können Sie die globalen Einstellungen für die Absenderüberprüfung ändern. Diese Einstellungen wirken nur für benannte Partner, die über das openFT-Protokoll verbunden sind und nicht mit Authentifizierung arbeiten. Für dynamische Partner sowie für FTAM- und FTP-Partner hat diese Einstellung keine Bedeutung.

i (identification)
Überprüfung der Transportadresse ausschalten. Es wird ausschließlich die Identifikation des Partners geprüft.

a (address)
Überprüfung der Transportadresse einschalten.
Stimmt die Transportadresse, unter der sich der Partner anmeldet, nicht mit dem Eintrag in der Partnerliste überein, dann wird der Auftrag abgelehnt.

Voreinstellung nach Neuinstallation: *-ptc=i*.

-lf=c Die Logging-Datei wird gewechselt.

Die neue Logging-Datei wird unter dem Namen *syslog.Lyymmdd.Lhhmmss* angelegt:
– *yymmdd* ist das Datum (Jahr, Monat, Tag), an dem die Datei angelegt wurde,
– *hhmmss* ist die Uhrzeit (Stunde, Minute, Sekunde für GMT), zu der die Datei angelegt wurde.

-lt=a | **-lt=f** | **-lt=n**
Mit diesem Schalter können Sie das FT-Logging selektiv abschalten. Folgende Parameter stehen Ihnen zur Verfügung:

a (all)
Es werden zu allen FT-Aufträgen Logging-Sätze geschrieben.

f (failure case)
Es werden nur zu fehlerhaften FT-Aufträgen Logging-Sätze geschrieben.

n (none)
Es werden keine Logging-Sätze geschrieben.

Voreinstellung nach Neuinstallation: *-lt=a*.

-lc=a | **-lc=m** | **-lc=r**
Mit diesem Schalter können Sie das FTAC-Logging selektiv einstellen. Folgende Parameter stehen Ihnen zur Verfügung:

a (all)
Es werden zu allen FTAC-Zugriffsprüfungen Logging-Sätze geschrieben.

m (modifying FM calls)
Es werden Logging-Sätze zu allen modifizierenden Inbound Dateimanagement-Aufträgen sowie zu allen abgelehnten FTAC-Zugriffsprüfungen geschrieben.

r (reject case)
Es werden nur zu abgelehnten FTAC-Zugriffsprüfungen Logging-Sätze geschrieben.

Voreinstellung nach Neuinstallation: *-lc=a*.

-la=a | **-la=f** | **-la=m** | **-la=n**
Mit diesem Schalter können Sie das Logging von Administrationsaufträgen selektiv einschalten. Folgende Parameter stehen Ihnen zur Verfügung:

a (all)
Es werden zu allen Administrationsaufträgen Logging-Sätze geschrieben.

f (failure)
Es werden nur zu fehlerhaften Administrationsaufträgen Logging-Sätze geschrieben.

m (modifying)
Es werden Logging-Sätze zu allen modifizierenden Administrationsaufträgen geschrieben.

n (none)
Es werden keine Logging-Sätze zu Administrationsaufträgen geschrieben.

Voreinstellung nach Neuinstallation: *-la=a*.

-ld=n | **-ld=f**
Mit dieser Option steuern Sie das automatische Löschen von Logging-Sätzen.

n (on) Schaltet das automatische Löschen von Logging-Sätzen ein. Damit werden die in *-lda*, *-ldt* und *-ldd* angegebenen Kriterien (Mindestalter und Löschintervalle) aktiviert.

f (off) Schaltet das automatische Löschen von Logging-Sätzen aus. Damit haben auch die Einstellungen in *-lda*, *-ldt* und *-ldd* keine Wirkung.

Voreinstellung nach Neuinstallation: *-ld=f*.

-lda=0..999
Mindestalter der zu löschenden Logging-Sätze in Tagen. Die Tage werden ab der bei *-ldt* angegebenen Löschzeit zurückgerechnet. Der Wert 0 löscht alle Logging-Sätze, die vor oder an der bei *-ldt* angegebenen Zeit des aktuellen Tages geschrieben wurden.

Voreinstellung nach Neuinstallation: *-lda=14*.

-ldt=hhmm
gibt die Uhrzeit (als Ortszeit) an, wann die Logging-Sätze gelöscht werden sollen. Die Löschfunktion kann systembedingt jeweils bis zu 5 Minuten nach dieser Uhrzeit ausgeführt werden.

Voreinstellung nach Neuinstallation: *-ldt=0000* (d.h. 00:00 Uhr).

-ldd=@d | **Mo** | **Tu** | **We** | **Th** | **Fr** | **Sa** | **Su** | 1..31
gibt den Tag an, an dem die Logging-Sätze gelöscht werden sollen.

Mo | **Tu** | **We** | **Th** | **Fr** | **Sa** | **Su**
wöchentliches Löschen am ausgewählten Wochentag (Mo=Montag, .. Su= Sonntag).

1..31 monatliches Löschen an einem bestimmten Tag des Monats (1-31). Wird als Tag des Monats 29, 30 oder 31 angegeben, hat der Monat aber weniger Tage, so wird am letzten Tag des Monats gelöscht.

@d die Logging-Sätze werden täglich gelöscht.

Voreinstellung nach Neuinstallation: *-ldd=@d* (d.h. tägliches Löschen).

-mon=n | **-mon=f**
Hiermit können Sie die openFT-Messdatenerfassung ein- und ausschalten.

n (on)
Die openFT-Messdatenerfassung wird eingeschaltet.

f (off)
Die openFT-Messdatenerfassung wird ausgeschaltet.

Voreinstellung nach Neuinstallation: *-mon=f* .

-monr=[**l** | **r**][**a** | **s**]
Hiermit können Sie die openFT-Messdatenerfassung nach Art der Aufträge selektieren. Der Wert *l* oder *r* kann mit *a* oder *s* kombiniert werden (logisches UND, z.B. *la*, *al*, *ls*, *rs*, ...).

l (local)
Es werden Messdaten für lokal gestellte Aufträge erfasst.

r (remote)
Es werden Messdaten für entfernt gestellte Aufträge erfasst.

a (asynchronous)
Es werden Messdaten für asynchrone Aufträge erfasst. Entfernt gestellte Aufträge werden immer als asynchron betrachtet.

s (synchronous)
Es werden Messdaten für synchrone Aufträge erfasst. Synchrone Aufträge sind immer lokal gestellt.

keine Auftragsart angegeben
: Wenn Sie *-monr=* angeben, dann werden Messdaten für alle Aufträge erfasst.

Bitte beachten Sie, dass *-monr=rs* die Messdatenerfassung nicht komplett abschaltet. *-monr=rs* wirkt wie *-monp=*, siehe Abschnitt „Beschreibung der Messwerte“ auf Seite 335.

Voreinstellung nach Neuinstallation: *-monr=*.

-monp= | **-monp=a** | **-monp=**[**openft**][**,**][**ftam**][**,**][**ftp**]
: Hiermit können Sie die openFT-Messdatenerfassung nach Art der für die Partner verwendeten Protokolle selektieren. Wenn Sie die Protokolle einzeln angeben, sind auch Kombinationen erlaubt (getrennt durch Komma).

a Es werden Messdaten für alle Partner erfasst.

openft
: Es werden Messdaten für openFT-Partner erfasst.

ftam Es werden Messdaten für FTAM-Partner erfasst.

ftp Es werden Messdaten für FTP-Partner erfasst.

keine Protokollart angegeben
: Wenn Sie *-monp=* ohne Parameter angeben, dann wird die Messdatenerfassung für Partner ausgeschaltet. In diesem Fall werden nur bestimmte Messdaten mit Werten versorgt, siehe Abschnitt „Beschreibung der Messwerte“ auf Seite 335.

Voreinstellung nach Neuinstallation: *-monp=a*.

-tr=n | **-tr=f** | **-tr=c**
: Hiermit können Sie die openFT-Überwachungsfunktion ein- und ausschalten.

n (on)
: Die openFT-Überwachungsfunktion wird eingeschaltet.

f (off)
: Die openFT-Überwachungsfunktion wird ausgeschaltet.

c (change)
: Die aktuelle Überwachungsdatei wird geschlossen und eine neue geöffnet.

Voreinstellung nach Neuinstallation: *-tr=f*.

-trp=a | **-trp=**[**openft**][**,**][**ftam**][**,**][**ftp**][**,**][**adm**]]
Hiermit können Sie die openFT-Überwachungsfunktion nach Art der für die Partner verwendeten Protokolle selektieren, indem Sie eine durch Komma getrennte Liste von einem oder mehreren Protokolltypen angeben. Es werden dann alle Partner überwacht, die über diese(n) Protokolltyp(en) angesprochen werden.

Die hier getroffene Auswahl kann partnerspezifisch abgeändert werden, siehe Option *-tr* des Kommandos *ftmodptn* auf Seite 280.

a (all)
Es werden alle Protokolltypen und damit alle Partner für die Überwachung ausgewählt.

openft
Es werden alle Partner für die Überwachung ausgewählt, die über das openFT-Protokoll angesprochen werden.

ftam Es werden alle Partner für die Überwachung ausgewählt, die über das FTAM-Protokoll angesprochen werden.

ftp Es werden alle Partner für die Überwachung ausgewählt, die über das FTP-Protokoll angesprochen werden.

adm Es werden alle Partner für die Überwachung ausgewählt, die über das FTADM-Protokoll angesprochen werden.

kein Protokolltyp angegeben
Wenn Sie *-trp=* ohne Parameter angeben, dann wird kein Partner für die Überwachung ausgewählt. In diesem Fall werden nur noch die Partner überwacht, für die die Überwachung partnerspezifisch mit *ftmodptn ... tr=n* eingeschaltet wurde, siehe Seite 280.

Voreinstellung nach Neuinstallation: *-trp=a*.

-trr=[**l** | **r**][**a** | **s**]
Mit dieser Option können Sie die Auftragsarten auswählen, die überwacht werden sollen. Der Wert *l* oder *r* kann mit *a* oder *s* kombiniert werden (logisches UND, z.B. *la*, *al*, *ls*, *rs*, ...).

l (local)
Es werden alle lokal gestellten Aufträge für die Überwachung ausgewählt.

r (remote)
Es werden alle entfernt gestellten Aufträge für die Überwachung ausgewählt.

a (asynchron)
Es werden alle asynchronen Aufträge für die Überwachung ausgewählt. Entfernt gestellte Aufträge werden immer als asynchron betrachtet.

s (synchron)
Es werden alle synchronen Aufträge für die Überwachung ausgewählt. Synchrone Aufträge sind immer lokal gestellt.

keine Auftragsart angegeben
Wenn Sie *-trr=* ohne Parameter angeben, dann werden alle Aufträge für die Überwachung ausgewählt.

Bitte beachten Sie, dass *-trr=rs* die Überwachung nicht komplett abschaltet. Es werden z.B. weiterhin Schnittstellen-Trace-Dateien erzeugt.

Voreinstellung nach Neuinstallation: *-trr=*.

-tro=[**b**]
Mit *-tro* können Sie Optionen für die Überwachungsfunktion auswählen. Diese Optionen wirken nur, wenn die Überwachungsfunktion eingeschaltet ist.

b (no bulk data)
Minimaltrace, es werden nur Protokollelemente in die Überwachungsdatei geschrieben, die keine Dateiinhalte (bulk data, d.h. Massendaten) enthalten. Für Protokollelemente mit Dateiinhalten wird stattdessen in der Überwachungsdatei vermerkt, dass an dieser Stelle Sätze unterdrückt wurden. Dieser Vermerk wird für eine Folge gleichartiger Sätze nur einmal geschrieben.

keine Option angegeben
Wenn Sie *-tro=* ohne Parameter angeben, dann wird der Trace im Standard-Umfang geschrieben.

Voreinstellung nach Neuinstallation: *-tro=*.

-troll=[**s** | **d**]
Mit *-troll* definieren Sie den Überwachungsumfang für die unteren Protokollschichten. Diese Option wirkt nur, wenn die Überwachungsfunktion eingeschaltet ist.

s (standard) Für die unteren Schichten werden zusätzliche Einträge im Standardumfang geschrieben. Der Standardumfang umfasst eine ausführliche Protokollierung der Aufrufe, ihrer Argumente, des Inhalts eventueller Optionen und der Benutzerdaten.

d (detail) Für die unteren Schichten werden zusätzlich zum Standardumfang noch interne Ereignisse und Informationen des Transportsystems (z.B. Systemaufrufe) protokolliert.

keine Option angegeben
Wenn Sie *-troll=* ohne Parameter angeben, dann wird die Überwachung der unteren Protokollschichten ausgeschaltet.

Hinweis zum Betrieb mit und ohne CMX:
- Im Betrieb ohne CMX werden die Trace-Einträge der unteren Protokollschichten mit in den openFT-Trace geschrieben
- Im Betrieb mit CMX werden CMX-Traces erzeugt, die im Verzeichnis *traces* der zugehörigen openFT-Instanz abgespeichert werden, sodass auch diese z.B. im openFT Explorer ausgewählt und angezeigt werden können (Menü *Administration*, Befehl *Trace-Datei öffnen*).
  Mit dieser Option ist es daher im Betrieb mit CMX möglich, CMX-Traces im laufenden Betrieb ein- und auszuschalten.

Voreinstellung nach Neuinstallation: *-troll=*.

-atpsv=[Partner][**,**][Zugangsberechtigung | **@d**]

Mit *-atpsv=* geben Sie die Einstellungen für den ADM-Trap-Server an. Wenn Sie den ADM-Trap-Server erstmals eintragen, müssen Sie sowohl den Partner als auch die Zugangsberechtigung angeben. Später können Sie jeden der beiden Parameter einzeln ändern.

Partner

Name oder Adresse des Partners, an den die ADM-Traps gesendet werden. Dies muss entweder ein Name aus der Partnerliste sein oder die Adresse muss in der Form *ftadm://host...* angegeben werden, siehe Abschnitt „Syntax der Kommandobeschreibung“ auf Seite 168.

Zugangsberechtigung

FTAC-Zugangsberechtigung für den ADM-Trap-Server.

@d für *Zugangsberechtigung*

Wenn Sie *@d* (dunkelgesteuert) angeben, dann wird die Zugangsberechtigung nach Abschicken des Kommandos am Bildschirm abgefragt. Die Eingabe bleibt unsichtbar.

weder *Partner* noch *Zugangsberechtigung* angegeben

Mit *-atpsv=* ohne Parameter tragen Sie den ADM-Trap-Server aus. Damit werden keine ADM-Traps mehr verschickt.

Voreinstellung nach Neuinstallation: *-atpsv=*.

-atp=a | **-atp=n** | **-atp=**ADM-Trap-Liste (durch Komma getrennt)

Mit *-atp* können Sie ADM-Traps ein- und ausschalten. Der ADM-Trap-Server, an den die ADM-Traps gesendet werden sollen, wird mit *-atpsv* festgelegt.

Bei *-atp* können Sie Folgendes angeben:

a (all)

Es werden alle ADM-Traps geschrieben.

n (none)

Es werden keine ADM-Traps geschrieben.

fts Schaltet die ADM-Traps zum Status des asynchronen Servers ein.

-fts Schaltet die ADM-Traps zum Status des asynchronen Servers aus.

rqs Schaltet die ADM-Traps zum Status des Auftragsbuchs (request queue) ein.

-rqs Schaltet die ADM-Traps zum Status des Auftragsbuchs aus.

rqc Schaltet die ADM-Traps beim erfolgreichen Beenden eines Auftrags ein.

-rqc Schaltet die ADM-Traps beim erfolgreichen Beenden eines Auftrags aus.

rqf Schaltet die ADM-Traps beim Beenden eines fehlgeschlagenen Auftrags ein.

-rqf Schaltet die ADM-Traps beim Beenden eines fehlgeschlagenen Auftrags aus.

pts Schaltet die ADM-Traps zum Status von Partnersystemen ein.

-pts Schaltet die ADM-Traps zum Status von Partnersystemen aus.

ptu Schaltet die ADM-Traps bei Nichterreichbarkeit eines Partnersystems ein.

-ptu Schaltet die ADM-Traps bei Nichterreichbarkeit eines Partnersystems aus.

Voreinstellung nach Neuinstallation: *-atp=n*.

-tpc=a | **-tpc=n** | **-tpc=**Konsolen-Trap-Liste (durch Komma getrennt)
Mit *-tpc* können Sie Konsolen-Traps ein- und ausschalten.

Konsolen-Traps werden auf Unix- und Windows-Systemen in die openFT-Datei *conslog* geschrieben. Auf Unix-, BS2000- und z/OS-Systemen werden sie außerdem auf die Konsole und auf Windows-Systemen an das Event-Log ausgegeben.

Bei *-tpc* können Sie Folgendes angeben:

a (all)
Es werden alle Traps geschrieben.

n (none)
Es werden keine Traps geschrieben.

sss Schaltet die Traps zum Status des openFT-Subsystems ein.

-sss Schaltet die Traps zum Status des openFT-Subsystems aus.

fts Schaltet die Traps zum Status des asynchronen Servers ein.

-fts Schaltet die Traps zum Status des asynchronen Servers aus.

rqs Schaltet die Traps zum Status des Auftragsbuchs (request queue) ein.

-rqs Schaltet die Traps zum Status des Auftragsbuchs aus.

rqc Schaltet die Traps beim erfolgreichen Beenden eines Auftrags ein.

-rqc Schaltet die Traps beim erfolgreichen Beenden eines Auftrags aus.

rqf Schaltet die Traps beim Beenden eines fehlgeschlagenen Auftrags ein.

-rqf Schaltet die Traps beim Beenden eines fehlgeschlagenen Auftrags aus.

pts Schaltet die Traps zum Status von Partnersystemen ein.

-pts Schaltet die Traps zum Status von Partnersystemen aus.

ptu Schaltet die Traps bei Nichterreichbarkeit eines Partnersystems ein.

-ptu Schaltet die Traps bei Nichterreichbarkeit eines Partnersystems aus.

Voreinstellung nach Neuinstallation: *-tpc=n*.

-ccs=CCS-Name

Mit *CCS-Name* stellen Sie einen neuen Zeichensatz ein, der durch eine Codetabelle repräsentiert wird. Dieser Zeichensatz wird dann als neuer Standardwert für Übertragungsaufträge (*ft, ncopy*) angenommen. Die Angabe der Codetabelle ist nur für Aufträge an openFT-Partner relevant.

Bei *ft* und *ncopy* sowie beim *ftexec* kann explizit ein anderer Zeichensatz zugewiesen werden (Optionen *-lc* und *-rc*).

Sie können auch einen eigenen Zeichensatz definieren. Details zu den CCS-Namen und den zugehörigen Code-Tabellen siehe Abschnitt „Code-Tabellen verwalten“ auf Seite 54.

Voreinstellung nach Neuinstallation: *-ccs=iso88591* (entspricht ISO8859-1).

-acta=a | **-acta=**[**openft**][**,**][**ftam**][**,**][**ftp**][**,**][**adm**]

Mit dieser Option aktivieren oder deaktivieren Sie die asynchronen Inbound-Server. Sie können die asynchronen Inbound-Server protokollspezifisch aktivieren (openFT, FTP, FTAM, ADM), indem Sie eine durch Komma getrennte Liste von einem oder mehreren Protokolltypen angeben.

a Die asynchronen Inbound-Server werden für alle installierten Protokolltypen aktiviert.

openft
aktiviert den asynchronen Inbound-Server für Aufträge über das openFT-Protokoll.

ftam aktiviert den asynchronen Inbound-Server für Aufträge über das FTAM-Protokoll. Ist das FTAM-Protokoll nicht installiert, dann wird eine Warnung ausgegeben.

ftp aktiviert den asynchronen Inbound-Server für Aufträge über das FTP-Protokoll. Ist das FTP-Protokoll nicht installiert, dann wird eine Warnung ausgegeben.

adm aktiviert den asynchronen Inbound-Server für Administrationsaufträge.

kein Protokolltyp angegeben
-acta= ohne Parameter deaktiviert alle asynchronen Inbound-Server.

Wenn Sie eine Liste von Protokolltypen angeben, werden die asynchronen Inbound-Server der nicht angegebenen Protokolltypen deaktiviert!

Voreinstellung nach Neuinstallation: *-acta=openft,ftam,adm*.

-ftp=Portnummer | **-ftp=@s**
Mit *Portnummer* legen Sie die Portnummer fest, die der FTP-Server verwendet. Mögliche Werte: 1 bis 65535

@s setzt die Portnummer für den FTP-Server auf den Standardwert 21.

Voreinstellung nach Neuinstallation: *-ftp=@s*.

-openft=[Portnummer][**.**T-Selektor] | **-openft=@s**
Portnummer
Sie können hier mit *Portnummer* eine vom Standard abweichende Portnummer für den lokalen openFT-Server festlegen.

Mögliche Werte für *Portnummer*: 1 bis 65535

T-Selektor
Zusätzlich kann ein T-Selektor in der Länge von 1 bis 8 Zeichen angegeben werden. Sie können den Selektor abdruckbar oder hexadezimal (im Format 0xnnnn...) angeben. Bei einem abdruckbaren Selektor sind alphanumerische Zeichen und die Sonderzeichen # @ $ erlaubt. Ein abdruckbarer Selektor wird im Protokoll in Großbuchstaben konvertiert, in EBCDIC codiert und ggf. intern mit Leerzeichen auf acht Zeichen aufgefüllt. Portnummer und T-Selektor müssen dann durch einen Punkt getrennt sein.

@s Mit *-openft=@s* werden die Portnummer und der T-Selektor des lokalen openFT-Servers auf ihren Standardwert gesetzt, d.h.
1100 und $FJAM.

Bitte benutzen Sie diese Funktion mit Vorsicht, denn wenn die Portnummer oder der T-Selektor vom Standard abweichen, dann wird den openFT-Partnern die Adressierung des lokalen Systems erschwert!

Voreinstellung nach Neuinstallation: *-openft=@s* (d.h. *1100* und *$FJAM*).

Hinweise zum Betrieb mit TNS

– Wenn Sie vom TNS-losen Betrieb auf den Betrieb mit TNS umstellen (*-tns=y*) und wenn vorher bei *-openft* nur der T-Selektor ohne Portnummer eingestellt war, dann müssen Sie die Portnummer explizit angeben, auch wenn sie dem Standardwert entspricht. Dies ist notwendig, damit der T-Selektor nicht mit dem Globalen Namen im TNS verwechselt werden kann.

– Für den Betrieb mit TNS können Sie einen vom Standard abweichenden TNS-Namen für den lokalen openFT-Server angeben. Vor dem TNS-Namen muss ein Punkt stehen z. B. *-openft=.OPNFTSRV*, der TNS-Name selber darf keinen Punkt enthalten.

Beim Betrieb mit TNS ist der Standardwert für den TNS-Namen $FJAM.

-ftam=[Portnummer][**.**T-Selektor[**.**S-Selektor[**.**P-Selektor]]] | **-ftam=@s**

Portnummer

Sie können hier mit *Portnummer* eine vom Standard abweichende Portnummer für den lokalen FTAM-Server festlegen.

Mögliche Werte für *Portnummer*: 1 bis 65535
Der Standardwert für *Portnummer* ist 4800

T-Selektor**.**S-Selektor**.**P-Selektor

Zusätzlich können ein T-Selektor, ein Session-Selektor und ein Presentation-Selektor angegeben werden, jeweils in der Länge von 1 bis 10 Zeichen. Portnummer, T-Selektor, S-Selektor und P-Selektor müssen dann durch einen Punkt getrennt sein. Sie können die Selektoren abdruckbar oder hexadezimal (im Format 0xnnnn...) angeben.

T-Selektoren, die mit $FTAM (Standardwert) beginnen, werden in EBCDIC codiert und mit Leerzeichen auf 8 Zeichen aufgefüllt. Alle anderen abdruckbaren T-Selektoren sowie alle abdruckbaren Session- und Presentation-Selektoren werden im Protokoll in Großbuchstaben konvertiert und in ASCII mit variabler Länge codiert.

Der Standardwert für *T-Selektor* ist $FTAM

S-Selektor und *P-Selektor* haben keinen Standardwert, da openFT-FTAM diese Selektoren standardmäßig nicht verwendet.

Bitte stimmen Sie die Angaben für Portnummer, Transport-Selektor, Session-Selektor und Presentation-Selektor (in diesem Schalter, bzw. im entsprechenden TNS-Eintrag) sorgfältig mit Ihren FTAM-Partnern ab!

@s Mit *-ftam=@s* werden die Portnummer und der T-Selektor des lokalen FTAM-Servers auf ihren Standardwert gesetzt, d.h. 4800 und $FTAM.

Voreinstellung nach Neuinstallation: *-ftam=@s*.

Hinweise zum Betrieb mit TNS

– Wenn Sie wieder auf den Betrieb mit TNS umstellen (*-tns=y*) und wenn vorher bei *-ftam* nur der T-Selektor ohne Portnummer eingestellt war, dann müssen Sie die Portnummer explizit angeben, auch wenn sie dem Standardwert entspricht. Dies ist notwendig, damit der T-Selektor nicht mit dem Globalen Namen im TNS verwechselt werden kann.

– Für den Betrieb mit TNS können Sie einen vom Standard abweichenden TNS-Namen für den lokalen FTAM-Server angeben. Vor dem TNS-Namen muss ein Punkt stehen z. B. *-ftam=.FTAMSERV*, der TNS-Name selber darf keinen Punkt enthalten.

Beim Betrieb mit TNS ist der Standardwert für den TNS-Namen $FTAM.

-adm=Portnummer | **-adm=@s**

Mit *Portnummer* legen Sie die Portnummer fest, über die die Fernadministration durchgeführt wird.

Mögliche Werte: 1 bis 65535

@s Mit *-adm=@s* wird die Portnummer für die Fernadministration auf den Standardwert 11000 zurückgesetzt.

Voreinstellung nach Neuinstallation: *-adm=@s*.

-ftstd=Portnummer | **-ftstd=@s**

Mit *Portnummer* legen Sie für die Adressierung von openFT-Partnern über Partneradressen den Standardwert der Portnummer fest.

Mögliche Werte: 1 bis 65535

Bitte benutzen Sie diese Funktion mit Vorsicht, denn wenn Sie den Wert dieser Option ändern, dann können openFT-Partner, die die openFT-Standard-Portnummer 1100 verwenden, nur mit expliziter Angabe der Portnummer erreicht werden!

@s Mit *-ftstd=@s* wird der Standardwert der Portnummer für die Adressierung von fernen openFT-Partnern über Partneradressen zurückgesetzt. Damit gilt wieder die Standard-Portnummer 1100.

Voreinstellung nach Neuinstallation: *-ftstd=@s*.

-tns=y | **-tns=n**

Mit dieser Option können Sie die Verwendung von TNS-Namen ein- oder ausschalten. Die Verwendung von TCP/IP-Hostnamen, IP-Adressen und das Partnermanagement, sowie die explizite Angabe von Portnummer und Selektoren bei den Schaltern *-openft=* und *-ftam=* sind davon nicht betroffen.
Der Betrieb mit TNS setzt voraus, dass der Betrieb mit CMX eingeschaltet ist (*ftmodo -cmx=y*).

y Mit dieser Auswahl wird die Verwendung von TNS-Namen für die openFT- und FTAM-Übertragung eingeschaltet.

Dies ist z.B. notwendig, wenn außer TCP/IP auch andere Transportprotokolle verwendet werden sollen.

n Mit dieser Auswahl wird die Verwendung der TNS-Namen ausgeschaltet. Damit kann nur das Transportprotokoll TCP/IP verwendet werden. Für die Kommunikation werden standardmäßig die bei den Betriebsparametern eingestellten Portnummern verwendet (Optionen *-openft*, *-ftam* und *-ftstd*).

Achtung!
Diese Option sollte nicht verändert werden, solange Aufträge gespeichert oder aktiv sind. Durch das Zu- und Wegschalten der TNS-Datenbasis kann sich die Umsetzung des Partnernamens auf eine Partneradresse verändern, was zu Fehlerabbrüchen (vor allem bei Wiederanlauf) oder unerwünschten Zustellungen von Dateien führen könnte. Temporäre Partnereinträge können nach einer Umschaltung vorübergehend auch doppelt in der Partnerliste erscheinen (siehe *ftshwptn*), selbst wenn der Partnername in beiden Fällen auf dieselbe Adresse umgesetzt wird.

Voreinstellung nach Neuinstallation: *-tns=n*.

-cmx=y | **-cmx=n**

Mit dieser Option können Sie zwischen dem Betrieb mit CMX und dem Betrieb ohne CMX umschalten. Das Umschalten ist nur möglich, wenn der asynchrone openFT Server nicht gestartet ist. Ggf. müssen Sie den asynchronen openFT-Server zuerst beenden, z.B. mit *ftstop*.

Für den Betrieb mit TNS muss der Betrieb mit CMX eingeschaltet sein.

y Es wird in den Betrieb mit CMX umgeschaltet. Dies ist nur möglich, wenn die für diese openFT-Version vorausgesetzte Mindestversion von CMX installiert ist. Falls CMX nicht oder nicht in der passenden Version installiert ist, wird das Kommando *ftmodo* mit einer Fehlermeldung abgelehnt.

n Es wird in den Betrieb ohne CMX umgeschaltet.

Voreinstellung nach Neuinstallation: *-cmx=n*.

-ae=y | **-ae=n**
Mit dieser Option können Sie den AET (Application Entity Title) ein- oder ausschalten.

y Mit dieser Auswahl wird bei Übertragungen mit dem FTAM-Protokoll ein "nil-Application Entity Title" als calling bzw. called Application Entity Title (AET) mitgeschickt.

n Der AET wird ausgeschaltet. Der Schalter muss nur dann auf *-ae=n* zurückgesetzt werden, wenn FTAM-Kopplungspartner erwarten, dass sie als Responder keinen AET bekommen.

Voreinstellung nach Neuinstallation: *-ae=y*.

-dp=n | **-dp=f**
Mit dieser Option legen Sie fest, ob dynamische Partner zugelassen sind oder nicht.

n (on) Dynamische Partner werden zugelassen. Partner können damit über ihre Adresse angesprochen werden, unabhängig davon, ob sie in der Partnerliste eingetragen sind oder nicht.

f (off) Dynamische Partner sind nicht zugelassen, d.h. Partner können nicht über ihre Adresse angesprochen werden. Damit können nur die Partner genutzt werden, die mit Namen in der Partnerliste eingetragen sind und mit dem Partnernamen angesprochen werden.

Voreinstellung nach Neuinstallation: *-dp=n*.

-c= | **-c=i** | **-c=o** | **-c=io** | **-c=oi**
Mit dieser Option steuern Sie die systemweite Benutzerdaten-Verschlüsselung. Die Einstellung gilt für Übertragungsaufträge und Administrationsaufträge.

i Schaltet die Inbound-Verschlüsselung ein:
Inbound-Aufträge müssen die Benutzerdaten verschlüsselt übertragen, ansonsten werden sie abgelehnt.

o Schaltet die Outbound-Verschlüsselung ein:
Outbound-Aufträge übertragen die Benutzerdaten verschlüsselt, auch wenn im Auftrag (z.B. *ft*, *ncopy*, Programmschnittstelle, openFT Explorer) keine Verschlüsselung angefordert wurde.

io, **oi** Schaltet die Inbound- und Outbound-Verschlüsselung ein:
Inbound-Aufträge müssen die Benutzerdaten verschlüsselt übertragen, ansonsten werden sie abgelehnt. Outbound-Aufträge übertragen die Benutzerdaten verschlüsselt, auch wenn im Auftrag keine Verschlüsselung angefordert wurde.

keine Verschlüsselungsoption angegeben

Mit *-c=* schalten Sie die systemweite Benutzerdaten-Verschlüsselung aus. Wenn Verschlüsselung gewünscht wird, dann muss dies explizit im Auftrag angegeben werden.

- Die systemweite Verschlüsselung darf nur eingeschaltet werden, wenn openFT-CR installiert ist.
- Ist die Inbound-Verschlüsselung eingeschaltet, dann werden Inbound-FTAM-Aufträge und Inbound-FTP-Aufträge abgelehnt.
- Ist die Outbound-Verschlüsselung eingeschaltet, dann werden Outbound-FTAM-Aufträge abgelehnt, Outbound-FTP-Aufträge sind dagegen erlaubt.
- Dateimanagement-Aufträge werden unabhängig von der Angabe bei Option *-c* unverschlüsselt ausgeführt.

Voreinstellung nach Neuinstallation: *-c=*.

Beispiele

1. Die Identifikation der eigenen Instanz soll auf host.hugo.net gesetzt werden:

   ```
   ftmodo -id=host.hugo.net
   ```

2. Es sollen nur noch Partner aus der Partnerliste zugelassen werden:

   ```
   ftmodo -dp=f
   ```

3. Die lokale openFT-Instanz soll als Fernadministrations-Server gekennzeichnet werden:

   ```
   ftmodo -admcs=y
   ```

4. Es sollen nur die asynchronen Inbound-Server der Protokolle openFT und FTAM aktiviert werden.

   ```
   ftmodo -acta=openft,ftam
   ```

6.26 ftmodp - Berechtigungsprofile ändern

ftmodp steht für "modify profile", also Ändern eines Berechtigungsprofils.
Als FTAC-Verwalter können Sie mit diesem Kommando Berechtigungsprofile anderer Benutzer ändern oder privilegieren.

Als ADM-Verwalter können Sie ADM-Profile ändern (d.h. Berechtigungsprofile mit der Eigenschaft "Zugang zum Fernadministrations-Server", entspricht ***-ff=c***).

Beim Ändern eines Profils wird der Zeitstempel aktualisiert.

Falls der FTAC-Verwalter nicht zugleich FT-Verwalterrechte hat, sind Berechtigungsprofile anderer Benutzer nach einer Änderung gesperrt (außer nach *-priv=y*). Das kann durch die Angabe von *-ua=Benutzerkennung,Kennwort* umgangen werden. Ändert der Benutzer danach sein Passwort, so ist das Profil nicht mehr ohne eine weitere Änderung verwendbar.

Format

```
ftmodp -h |
        <Profilname 1..8> | @s | @a
        [ -s=[<Zugangsberechtigung 8..32> | @a | @n ]
              [,<Benutzerkennung 1..32> | @a | @adm] ]
        [ -ua=[ <Benutzerkennung 1..32> ][,[<Kennwort 1..20> | @n ]] ]
        [ -nn=<Profilname 1..8> | @s ]
        [ -tad= | -tad=<Zugangsberechtigung 8..32> | -tad=@n ]
        [ -v=y | -v=n ][ -d=yyyymmdd | -d= ]
        [ -u=pr | -u=pu ]   [ -priv=y | -priv=n ]
        [ -iml=y | -iml=n ]
        [ -iis=y | -iis=n ]   [ -iir=y | -iir=n ]
        [ -iip=y | -iip=n ]   [ -iif=y | -iif=n ]
        [ -ff= | -ff=[t][m][p][r][a][l] | -ff=c ]
        [ -dir=f | -dir=t | -dir=ft ]
        [ -pn=<Partner 1..200>,...,<Partner(50) 1..200> | -pn= ]
        [ -pna=<Partner 1..200>,...,<Partner(50) 1..200> ]
        [ -pnr=<Partner 1..200>,...,<Partner(50) 1..200> ]
        [ -fn=<Dateiname 1..512> | -fn= ][ -fnp=<Dateinamen-Praefix 1..511> ]
        [ -ls= | -ls=@n | -ls=<Kommando1 1..1000> ]
        [ -lsp= | -lsp=[<Kommando2 1..999> ][ -lss= | -lss=Kommando3 1..999> ]
        [ -lf= | -lf=@n | -lf=<Kommando4 1..1000> ]
        [ -lfp= | -lfp=<Kommando5 1..999> ][ -lfs= | -lfs=<Kommando6 1..999> ]
        [ -wm=o | -wm=n | -wm=e | -wm=one ]
        [ -c= | -c=y | -c=n ]
        [ -txt=<Text 1..100> | -txt= ]
```

Beschreibung

-h gibt die Kommandosyntax am Bildschirm aus. Weitere Angaben nach *-h* werden ignoriert.

Profilname
: gibt den Namen des Berechtigungsprofils an, das geändert werden soll. Mit *ftshwp* (ohne Optionen) können Sie sich über Ihre bereits vergebenen Profilnamen informieren.

  @s für *Profilname*
  : Mit *@s* ändern Sie die Eigenschaften des Standard-Berechtigungsprofils der Kennung.

    Die Optionen *-v*, *-d* und *-u* werden bei einem Standard-Berechtigungsprofil ignoriert.

  @a für *Profilname*
  : Mit der Angabe *@a* für den Profilnamen ändern Sie alle in Frage kommenden Berechtigungsprofile gleichzeitig, falls Sie nicht mit der Option *-s* ein bestimmtes Profil auswählen.

  Mit der Angabe *ftmodp Profilname* ohne weitere Parameter erzwingen Sie, dass der Zeitstempel des Profils aktualisiert wird.

-s=[Zugangsberechtigung | **@a** | **@n**][**,**Benutzerkennung | **@a** | **@adm**]
: Mit *-s* können Auswahlkriterien für das zu ändernde Berechtigungsprofil angegeben werden.

  Zugangsberechtigung
  : Das Berechtigungsprofil mit dieser Zugangsberechtigung soll geändert werden. Eine binäre Zugangsberechtigung müssen Sie in der Form x\'...\' oder X\'...\' angeben.

  @a für *Zugangsberechtigung*
  : Wenn Sie hier *@a* angeben, werden entweder das mit *Profilname* (siehe oben) angesprochene Berechtigungsprofil oder (falls kein Profilname angegeben wurde) alle in Frage kommenden Berechtigungsprofile geändert.

  @n für *Zugangsberechtigung*
  : Wenn Sie hier *@n* angeben, werden alle Berechtigungsprofile ohne Zugangsberechtigung ausgewählt.

  Zugangsberechtigung nicht angegeben
  : Die Zugangsberechtigung wird nach der Kommandoabgabe am Bildschirm abgefragt. Sie bleibt unsichtbar, um zu verhindern, dass Unbefugte die Zugangsberechtigung sehen. Um Eingabefehler zu vermeiden, wird eine Kon-

trolleingabe verlangt. Wenn Sie die Eingabeanforderungen nur durch Drücken der Returntaste beantworten, wirkt das wie die Angabe von *@a* im Kommando.

,Benutzerkennung
: Als FTAC-Verwalter dürfen Sie hier jede beliebige Benutzerkennung angeben.

@a für *Benutzerkennung*
: Wenn Sie als FTAC-Verwalter *@a* angeben, ändern Sie Berechtigungsprofile für alle Benutzerkennungen.

@adm für *Benutzerkennung*
: Wenn Sie als FTAC- oder ADM-Verwalter *@adm* angeben, können Sie ADM-Profile ändern (entspricht Option *-ff=c*). Sie dürfen dabei jedoch weder diese Eigenschaft (*-ff=c*) noch die Kennung (Option *-ua*) ändern.

Benutzerkennung nicht angegeben
: Es werden unabhängig davon, wer das Kommando absetzt, nur Profile der eigenen Benutzerkennung geändert.

-s nicht angegeben
: Falls *@a* für *Profilname* angegeben wurde, werden alle Berechtigungsprofile unter der Kennung geändert, von der aus das *ftmodp* abgesetzt wird. Sonst wird das Berechtigungsprofil mit dem angegebenen Namen geändert.

-ua=[Benutzerkennung][**,**[Kennwort | **@n**]]
: Mit *-ua* kann der FTAC-Verwalter Berechtigungsprofile einer beliebigen Benutzerkennung einer anderen Benutzerkennung zuordnen.

Benutzerkennung
: Als FTAC-Verwalter dürfen Sie hier jede beliebige Benutzerkennung angeben.

,Kennwort
: Gibt das Kennwort zu der Benutzerkennung an. Ein binäres Kennwort muss in der Form x\'...\' oder X\'...\' angegeben werden. Das Berechtigungsprofil ist für die Kennung nur so lange gültig, wie das Kennwort *Kennwort* für die Kennung gültig ist. Wenn das Kennwort geändert wird, dann ist das Profil nicht mehr verwendbar (nicht gesperrt!).

@n für *Kennwort*
: Als FTAC-Verwalter dürfen Sie in diesem Fall keine Zugangsberechtigung für das Berechtigungsprofil erteilen, sofern Sie nicht FT-Verwalterrechte besitzen. Eine vorhandene Zugangsberechtigung wird in diesem Fall automatisch gelöscht.

nur Komma (**,**) ohne *Kennwort* angegeben
: Bei Komma (,) ohne *Kennwort* wird das Kennwort nach der Kommandoabgabe am Bildschirm abgefragt. Die Eingabe bleibt unsichtbar, um zu verhindern, dass Unbefugte das Kennwort sehen. Hochkommas dürfen in diesem Fall nicht mit Gegenschrägstrich (\) entwertet werden.

nur *Benutzerkennung* (ohne Komma und *Kennwort*) angegeben
: Das Profil gilt wieder für alle Kennwörter der Benutzerkennung.

-ua nicht angegeben
: Die Kennung dieses Berechtigungsprofils bleibt unverändert.

-nn=Profilname | **@s**
: Mit *-nn* können Sie Ihrem Berechtigungsprofil einen neuen Namen geben.

@s für *Profilname*
: Das Berechtigungsprofil wird zum Standard-Berechtigungsprofil der Kennung. Wenn das Berechtigungsprofil vorher eine Zugangsberechtigung besaß, dann müssen Sie zusätzlich *-tad=@n* angeben.

-nn nicht angegeben
: Der Profilname bleibt unverändert.

-tad=[Zugangsberechtigung | **@n**]
: Mit *-tad* können Sie die Zugangsberechtigung eines Berechtigungsprofils ändern. Als FTAC-Verwalter können Sie, sofern Sie über die FT-Verwalterrechte verfügen, auch die Zugangsberechtigungen fremder Benutzerkennungen ändern.

Wenn das modifizierte Berechtigungsprofil ein Standard-Berechtigungsprofil ist (*ftmodp @s* oder *-nn=@s*), dann ist nur *-tad=@n* erlaubt.

Zugangsberechtigung
: Die Zugangsberechtigung muss in Ihrem Unix-Rechner eindeutig sein, damit es keine Kollisionen mit Zugangsberechtigungen gibt, die andere FTAC-Benutzer für andere Zugriffsrechte definiert haben. Eine binäre Zugangsberechtigung muss sedezimal in der Form x\'...\' oder X\'...\' angegeben werden. Wenn die von Ihnen gewählte Zugangsberechtigung bereits vergeben ist, lehnt FTAC das *ftmodp* ab mit der Meldung: `Zugangsberechtigung existiert bereits.`

@n für *Zugangsberechtigung*
: Mit *@n* wird die alte Zugangsberechtigung gelöscht.

@n muss angegeben werden, wenn Sie ein Berechtigungsprofil, das eine Zugangsberechtigung besitzt, per *-nn=@s* zu einem Standard-Berechtigungsprofil umwandeln.

Zugangsberechtigung nicht angegeben
: Wenn Sie *-tad=* angeben, fordert FTAC Sie nach dem Abschicken des Kommandos auf, die Zugangsberechtigung einzugeben. Ihre Eingabe bleibt unsichtbar, um zu verhindern, dass Unbefugte die Zugangsberechtigung sehen. Um Schreibfehler auszuschließen, wird als Kontrolleingabe von Ihnen ein zweites Mal die Zugangsberechtigung erwartet.

  Beim Ändern des Standard-Berechtigungsprofils wird die Zugangsberechtigung nicht abgefragt. Sie erhalten die Meldung: `Zugangsberechtigung vom Standardprofil muss @n sein`.

-tad nicht angegeben
: Die Zugangsberechtigung des Berechtigungsprofils wird nicht geändert.

-v=y | **-v=n**
: Mit *-v* definieren Sie den Zustand der Zugangsberechtigung.

  Mögliche Werte:

  y Die Zugangsberechtigung ist nicht gesperrt (sie ist valid).

  n Die Zugangsberechtigung ist gesperrt (sie ist nicht valid).

  -v wird ignoriert, wenn das modifizierte Profil ein Standard-Berechtigungsprofil ist.

-v nicht angegeben
: Der Zustand der Zugangsberechtigung bleibt unverändert.

-d=[yyyymmdd]
: Mit *-d* legen Sie die Frist fest, innerhalb der die Zugangsberechtigung verwendet werden darf. Nach Ablauf der Frist ist das Berechtigungsprofil gesperrt.

  Sie können ein achtstelliges Datum angeben (z.B. 20170602 für 02.06.2017). Die Verwendung der Zugangsberechtigung ist ab 00:00 Uhr des angegebenen Tages nicht mehr möglich. Der größtmögliche Wert für das anzugebende Datum ist 20380119 (19. Januar 2038).

  yyyymmdd nicht angegeben
  : Mit der Angabe *-d=* wird die bisherige Festlegung rückgängig gemacht, d.h. die Verwendung der Zugangsberechtigung ist zeitlich nicht mehr eingeschränkt.

  -d wird ignoriert, wenn das modifizierte Profil ein Standard-Berechtigungsprofil ist.

-d nicht angegeben
: Die bisherige Festlegung bezüglich der Verwendungsdauer der Zugangsberechtigung bleibt unverändert.

-u=pr | **-u=pu**

Mit *-u* können Sie das Verhalten von FTAC für den Fall steuern, dass jemand versucht, ein Berechtigungsprofil mit der gleichen Zugangsberechtigung anzulegen. Im Normalfall sollte eine Zugangsberechtigung sofort gesperrt werden. Dazu müssen Sie die Zugangsberechtigung als privat kennzeichnen.

Zugangsberechtigungen, die nicht so schutzbedürftig sind, können Sie als öffentlich (public) kennzeichnen. In dem Fall wird die Zugangsberechtigung nicht gesperrt, auch wenn versucht wird, eine gleichnamige Zugangsberechtigung zu vergeben.
Mögliche Werte:

pr (Standardwert)
Die Zugangsberechtigung wird gesperrt, sobald jemand von einer anderen Kennung aus versucht, eine gleichnamige Zugangsberechtigung anzulegen (private).
Gleichzeitig wird in dem Fall der Wert von *-d* auf *zeitlich nicht eingeschränkt* gesetzt.

pu Die Zugangsberechtigung wird nicht gesperrt, auch wenn jemand versucht, eine gleichnamige Zugangsberechtigung anzulegen (public).

-u wird ignoriert, wenn das modifizierte Profil ein Standard-Berechtigungsprofil ist.

-u nicht angegeben
Die bisherige Festlegung bleibt unverändert.

-priv=y | **-priv=n**

Mit dieser Angabe können Sie als FTAC-Verwalter Berechtigungsprofile privilegieren.

y Das Berechtigungsprofil wird privilegiert. Für Aufträge, die mit einem privilegierten Berechtigungsprofil abgewickelt werden, werden die Vorgaben des Verwalters im Berechtigungssatz des Benutzers außer Kraft gesetzt. D.h. wenn der Benutzer im Berechtigungsprofil die Optionen *-iml, -iis, -iir, -iip* oder *-iif* nutzt, werden nicht nur die Vorgaben seines Berechtigungssatzes (MAX. USER LEVELS), sondern auch die Vorgaben des Verwalters (MAX. ADM LEVELS) ignoriert.

n Eine etwaige Privilegierung des Berechtigungsprofils wird zurückgenommen.

-priv nicht angegeben
Die Privilegierungseigenschaft des Profils bleibt unverändert.

-iml=y | **-iml=n**

Mit *-iml* (ignore max. level) wird festgelegt, ob das Berechtigungsprofil an die Vorgaben des Berechtigungssatzes gebunden ist. Sie können Ihre eigenen Vorgaben (die MAX. USER LEVELS) für Aufträge, die mit diesem Berechtigungsprofil arbeiten, außer Kraft setzen. Wenn das Berechtigungsprofil zudem vom FTAC-Verwalter privilegiert wird, können auch die Vorgaben des FTAC-Verwalters ignoriert werden (die MAX. ADM LEVELS). Das bedeutet, dass mit diesem Berechtigungsprofil *inbound*-Grundfunktionen genutzt werden können, die im Berechtigungssatz gesperrt sind.

y Mit dem Profil können die Vorgaben des Berechtigungssatzes ignoriert werden.

n Das Profil unterliegt den Vorgaben des Berechtigungssatzes.

-iml nicht angegeben

Die bisher bestehenden Festlegungen des Profils zu den Grundfunktionen gelten weiter.

-iis=y | **-iis=n**

Mit *-iis* (ignore inbound send) kann die Vorgabe für die Grundfunktion *inbound senden* im Berechtigungssatz ignoriert werden
(Näheres siehe *-iml*).

y Mit dem Profil kann die Grundfunktion *inbound senden* auch dann genutzt werden, wenn sie im Berechtigungssatz gesperrt ist. Gleichzeitig kann die Teilkomponente "Ansehen von Dateiattributen" der Grundfunktion *inbound Dateimanagement* genutzt werden (siehe Tabelle bei *-iif*).

Wenn die Grundfunktion *inbound senden* von Ihnen gesperrt wurde, reicht diese Angabe dafür aus. Wenn sie vom FTAC-Verwalter gesperrt wurde, muss er zusätzlich das Berechtigungsprofil privilegieren.

n Das Profil unterliegt der Vorgabe des Berechtigungssatzes für die Grundfunktion *inbound senden*.

-iis nicht angegeben

Die bisher bestehenden Festlegungen des Profils für *inbound senden* gelten weiter.

-iir=y | **-iir=n**

Mit *-iir* (ignore inbound receive) kann die Vorgabe für die Grundfunktion *inbound empfangen* im Berechtigungssatz ignoriert werden
(Näheres siehe *-iml*).

y Mit dem Profil kann die Grundfunktion *inbound empfangen* auch dann genutzt werden, wenn sie im Berechtigungssatz gesperrt ist. Gleichzeitig können Teilkomponenten der Grundfunktion *inbound Dateimanagement* genutzt werden (siehe Tabelle bei *-iif*).

Wenn die Grundfunktion *inbound empfangen* von Ihnen gesperrt wurde, reicht diese Angabe dafür aus. Wenn sie vom FTAC-Verwalter gesperrt wurde, muss er zusätzlich das Berechtigungsprofil privilegieren.

n Das Profil unterliegt der Vorgabe des Berechtigungssatzes für die Grundfunktion *inbound empfangen*.

-iir nicht angegeben
Die bisher bestehenden Festlegungen des Profils für *inbound empfangen* gelten weiter.

-iip=y | **-iip=n**
Mit *-iip* (ignore inbound processing) kann die Vorgabe für die Grundfunktion *inbound Folgeverarbeitung + Vorverarbeitung + Nachverarbeitung* im Berechtigungssatz ignoriert werden (Näheres siehe *-iml*).

y Mit dem Profil kann die Grundfunktion *inbound Folgeverarbeitung + Vorverarbeitung + Nachverarbeitung* auch dann genutzt werden, wenn sie im Berechtigungssatz gesperrt ist. Wenn sie von Ihnen gesperrt wurde, reicht diese Angabe dafür aus. Wenn sie vom FTAC-Verwalter gesperrt wurde, muss er zusätzlich das Berechtigungsprofil privilegieren.

n Das Profil unterliegt der Vorgabe des Berechtigungssatzes für die Grundfunktion *inbound Folgeverarbeitung + Vorverarbeitung + Nachverarbeitung*.

-iip nicht angegeben
Die bisher bestehenden Festlegungen des Profils für *inbound Folgeverarbeitung + Vorverarbeitung + Nachverarbeitung* gelten weiter.

-iif=y | **-iif=n**
Mit *-iif* (ignore inbound filemanagement) kann die Vorgabe für die Grundfunktion *inbound Dateimanagement* im Berechtigungssatz ignoriert werden (Näheres siehe *-iml*).

y Mit dem Profil kann die Grundfunktion *inbound Dateimanagement* auch dann genutzt werden, wenn sie im Berechtigungssatz gesperrt ist.

Wenn die Grundfunktion *inbound Dateimanagement* von Ihnen gesperrt wurde, reicht diese Angabe dafür aus. Wenn sie vom FTAC-Verwalter gesperrt wurde, muss er zusätzlich das Berechtigungsprofil privilegieren.

n Das Profil unterliegt der Vorgabe des Berechtigungssatzes für die Grundfunktion *inbound Dateimanagement*.

Die folgende Tabelle zeigt, welche Teilkomponenten des Dateimanagements unter welchen Voraussetzungen genutzt werden können.

Inbound Dateimanagement-Funktion	**Einstellung im Berechtigungssatz bzw. Erweiterung im Profil**
Dateiattribute anzeigen	Inbound Senden (IBS) erlaubt
Dateiattribute ändern	Inbound Empfangen (IBR) **und** Inbound Dateimanagement (IBF) erlaubt
Dateien umbenennen	Inbound Empfangen (IBR) **und** Inbound Dateimanagement (IBF) erlaubt
Dateien löschen	Inbound Empfangen (IBR) erlaubt **und** Schreibregel = überschreiben im Profil
Dateiverzeichnisse anzeigen	Inbound Dateimanagement (IBF) erlaubt
Dateiverzeichnisse anlegen, umbenennen, löschen	Inbound Dateimanagement (IBF) erlaubt **und** Richtung = vom Partner im Profil

-iif nicht angegeben

Die bisher bestehenden Festlegungen des Profils für *inbound Dateimanagement* gelten weiter.

-ff= | **-ff=**[**t**][**m**][**p**][**r**][**a**][**l**] | **-ff=c**

Mit *-ff* legen Sie fest, für welche Funktion das Berechtigungsprofil benutzt werden darf. Mit Ausnahme von *c* ist jede beliebige Kombinationen aus diesen Buchstaben (*tm, mt, mr,* ...) möglich. Bitte beachten Sie den Hinweis auf Seite 265 bei der Beschreibung von *-ff=c*.

t (transfer) Das Berechtigungsprofil darf für die File-Transfer-Funktionen "Dateien übertragen", "Dateiattribute ansehen" und "Dateien löschen" benutzt werden.

m (modify file attributes) Das Berechtigungsprofil darf für die File-Transfer-Funktionen "Dateiattribute ansehen" und "Dateiattribute modifizieren" benutzt werden.

p (processing) Das Berechtigungsprofil darf für die File-Transfer-Funktionen "Dateivorverarbeitung" bzw. "Dateinachverarbeitung" benutzt werden. Zusätzlich muss die Funktion "Dateien übertragen" erlaubt sein.

Für Profile mit einem Dateinamen-Präfix (*-fnp=*) bzw. einem Dateinamen (*-fn=*) ist die Angabe von *p* bedeutungslos, weil in diesem Fall das erste Zeichen des Dateinamens oder Dateinamen-Präfix darüber entscheidet, ob das Profil nur für Vor- und Nachverarbeitung verwendet werden kann ("|") oder ausschließlich Dateiübertragung bzw. Dateimanagement ermöglicht (kein "|").

Die Verwendung von Folgeverarbeitung wird nicht über *-ff*=, sondern über *-lf*= und *-ls*= gesteuert.

r (read directory) Das Berechtigungsprofil darf für die File-Transfer-Funktionen "Dateiverzeichnisse ansehen" und "Dateiattribute ansehen" benutzt werden.

a (administration)
Das Berechtigungsprofil darf für die Funktion "Fernadministration" genutzt werden. D.h. es berechtigt einen Fernadministrations-Server, auf die lokale openFT-Instanz zuzugreifen. Dazu muss die zugehörige Zugangsberechtigung im Fernadministrations-Server konfiguriert sein.
Die Angabe von *-ff=a* ist nur dem FT- oder FTAC-Verwalter erlaubt.

l (logging)
Das Berechtigungsprofil darf für die Funktion "ADM-Traps empfangen" benutzt werden. Damit kann eine andere openFT-Instanz ihre ADM-Traps über dieses Profil an den Fernadministrations-Server schicken. Diese Angabe ist nur sinnvoll, wenn die lokale openFT-Instanz als Fernadministrations-Server gekennzeichnet ist (Kommando *ftmodo -admcs=y*).
Die Angabe von *-ff=l* ist nur dem FT-Verwalter erlaubt.

c (client access)
Das Berechtigungsprofil darf für die Funktion "Zugang zum Fernadministrations-Server" benutzt werden (ADM-Profil). Damit kann ein Fernadministrator auf einem fernen Rechner über dieses Profil auf den lokalen Fernadministrations-Server zugreifen und Fernadministrationsaufträge absetzen. Die lokale openFT-Instanz muss als Fernadministrations-Server gekennzeichnet sein (Kommando *ftmodo -admcs=y*).

Die Angabe von *-ff=c* ist nur dem ADM-Verwalter erlaubt.

Der Wert *c* darf nicht mit anderen Werten kombiniert werden. Außerdem kann ein Berechtigungsprofil, das mit *-ff=c* erzeugt wurde, nicht in ein Profil mit anderen FT-Funktionen (*t, m, p, r, a* oder *l*) umgewandelt werden und umgekehrt.

keine Funktion angegeben
Mit der Angabe *-ff*= können Sie eine Festlegung zu den Funktionen wieder rückgängig machen. Es sind dann alle File-Transfer-Funktionen erlaubt (entspricht *tmpr*), nicht jedoch die Funktionen zur Fernadministration (*a*, *c*) und zu ADM-Traps (*l*).

-ff nicht angegeben
Die bisherige Festlegung zu den Funktionen bleibt unverändert.

-dir=f | **-dir=t** | **-dir=ft**
: Mit *-dir* legen Sie fest, für welche Übertragungsrichtung(en) das Berechtigungsprofil benutzt werden darf. Mögliche Angaben für Richtung: *f*, *t*, *ft*, *tf*.

  f Es dürfen nur Daten vom Partnersystem zum lokalen System übertragen werden.

  t Es dürfen nur Daten vom lokalen System zum Partnersystem übertragen werden. Damit ist auch kein Anlegen, Umbenennen oder Löschen von Verzeichnissen möglich.

  ft, tf Beide Übertragungsrichtungen sind erlaubt.

-dir nicht angegeben
: Die Festlegungen des Berechtigungsprofils zur Übertragungsrichtung bleiben unverändert.

-pn=[Partner1[**,**Partner2, ...]]
: Mit *-pn* können Sie festlegen, dass dieses Berechtigungsprofil nur für FT-Aufträge benutzt werden kann, die mit einem bestimmten Partnersystem abgewickelt werden. Sie können den Namen des Partnersystems in der Partnerliste oder die Adresse des Partnersystems angeben. Einzelheiten zur Adressangabe finden Sie in Abschnitt „Aufbau der Partneradressen“ auf Seite 68.

  Sie können hier maximal 50 Partnersysteme angeben, insgesamt maximal 1000 Zeichen.

  Partner1[,*Partner2, ...*] nicht angegeben
  : Mit der Angabe *-pn=* können Sie eine bisherige Einschränkung der Partnersysteme wieder rückgängig machen. Das Berechtigungsprofil kann dann von jedem Partnersystem aus benutzt werden.

-pna=Partner1[**,**Partner2, ...]
: Mit *-pna* können Sie ein oder mehrere Partnersysteme in die Liste der zugelassenen Partnersysteme einfügen. Insgesamt können maximal 50 Partnersysteme in die Liste aufgenommen werden (maximal 1000 Zeichen).

  War die Liste bisher leer, dann wird das Profil auf die angegebenen Partnersysteme eingeschänkt.

-pnr=Partner1[**,**Partner2, ...]
: Mit *-pnr* können Sie ein oder mehrere Partnersysteme aus der Liste der zugelassenen Partnersysteme löschen.

  Bitte beachten Sie: Sobald Sie den letzten Partner aus der Liste löschen, kann das Profil von jedem Partnersystem aus benutzt werden.

-pn, *-pna* und *-pnr* nicht angegeben
: Die Festlegungen bezüglich der zugelassenen Partnersysteme bleiben unverändert.

-fn=[Dateiname]

Mit *-fn* legen Sie fest, auf welche Dateien unter Ihrer Benutzerkennung mit diesem Berechtigungsprofil zugegriffen wird. Wenn Sie hier einen vollqualifizierten Dateinamen angeben, darf nur noch die Datei mit diesem Namen übertragen werden. Endet der Dateiname mit %unique oder %UNIQUE, so wird diese Zeichenfolge beim Dateiübertragungs- oder Dateimanagementauftrag durch einen String ersetzt, der bei jedem erneuten Aufruf wechselt. Dieser String ist in Unix-Systemen 14 Zeichen lang. Nach %unique oder %UNIQUE darf noch ein durch einen Punkt getrenntes Suffix angegeben werden, z.B. `datei1%unique.txt`. Sowohl im Logging als auch bei Meldungen wird nur noch der bereits konvertierte Dateiname angezeigt.
Wenn *Dateiname* mit einem "|" (Pipezeichen) beginnt, dann wird er als Vor- bzw. Nachverarbeitungskommando interpretiert.

Dateiname nicht angegeben

Mit der Angabe *-fn=* können Sie eine Festlegung des Dateinamens wieder rückgängig machen. Das gilt auch für ein mit *-fnp* vergebenes Präfix. Das Berechtigungsprofil erlaubt dann uneingeschränkten Zugriff auf alle Ihre Dateien.

-fn nicht angegeben

Die Festlegungen des Berechtigungsprofils zum Dateinamen bleiben unverändert.

-fnp=Dateinamen-Praefix

Durch diese Angabe kann der Zugriff auf eine Menge von Dateien beschränkt werden, deren Namen mit demselben Präfix anfangen. FTAC setzt die mit *Dateinamen-Praefix* spezifizierte Zeichenfolge vor den Dateinamen, der im Auftrag steht und versucht die Datei mit dem ergänzten Namen zu übertragen.
Wenn Sie zum Beispiel *-fnp=dagobert/* angeben und im Auftrag der Dateiname *boerse* steht, dann überträgt FTAC die Datei *dagobert/boerse*.

So lassen sich die für openFT freigegebenen Dateien kennzeichnen. Wenn mit *-fnp* ein Präfix spezifiziert wurde, darf in dem Dateinamen, der im Auftrag steht, die Zeichenfolge ../ nicht vorkommen, d.h. es ist nicht möglich durch Eingabe von ../ in ein übergeordnetes Verzeichnis zu wechseln und von dort auf andere Verzeichnisse zuzugreifen. Außerdem sollten Sie darauf achten, dass nicht durch einen symbolischen Verweis an eine andere Stelle des Dateibaums gesprungen werden kann! %unique oder %UNIQUE kann bei einem Dateinamen-Präfix nicht verwendet werden. Bei einem Dateiübertragungsauftrag kann vom Benutzer ein Dateiname mit der Endung %UNIQUE (oder %UNIQUE.*suffix*, %unique oder %unique.*suffix*) verwendet werden, um eindeutige Dateinamen mit dem hier festgelegten Präfix zu generieren.

Ein Dateinamen-Präfix, das mit dem Zeichen | beginnt, legt fest, dass das FTAC-Profil ausschließlich für Dateiübertragung mit Vor- und Nachverarbeitung verwendet werden kann, da der aus dem Präfix und dem beim *ncopy*- oder *ft*-Kommando angegebenen Namen gebildete Dateiname ebenfalls mit dem Zeichen | beginnt. In diesem Fall dürfen keine Folgekommandos angegeben werden.

Auf Unix-Systemen dürfen die Shell-Metazeichen | ; & < > sowie "newline" nur angegeben werden, wenn sie mit '...' (Hochkommas) oder "..." (Anführungszeichen) eingeschalt oder einzeln mit "\" (Gegenschrägstrich) entwertet werden. Das Zeichen ` (Accent grave) und die Zeichenfolge $((Dollar+Klammer auf) dürfen nur angegeben werden, wenn sie mit '...' (Hochkommas) eingeschalt oder direkt nach "\" (Gegenschrägstrich) angegeben werden.

Nicht angegeben werden dürfen im Kommando, das das Profil verwendet, die Zeichenfolgen
– .. (zwei Punkte)
– .\ (Punkt+Gegenschrägstrich)
– .' (Punkt+Hochkomma)
Damit wird ein Navigieren auf übergeordnete Verzeichnisse verhindert.

Das Dateinamen-Präfix darf maximal 511 Bytes lang sein.

Eine Festlegung für ein Dateinamen-Präfix können Sie mit der Angabe *-fn=* wieder rückgängig machen (siehe oben).

Sonderfälle

- Für FTAC-Profile, die ausschließlich für das *ftexec*-Kommando genutzt werden sollen, ist ein Dateiname oder Dateinamen-Präfix anzugeben, der mit der Zeichenfolge "|ftexecsv␣" beginnt. Soll darüber hinaus ein Kommando-Präfix festgelegt werden, dann müssen Sie dieses wie folgt angeben:

  -fnp="\|ftexecsv␣-p=*Kommando-Präfix***"**
  (z.B.: `-fnp="|ftexecsv␣-p=\"ftshwr␣\""`)

  Für den Kommandostring des *ftexec*-Aufrufs gelten dieselben Beschränkungen wie für das Dateinamen-Präfix bei Vor- und Nachverarbeitung.

- Für FTAC-Profile, die ausschließlich für das Abrufen von Messdaten verwendet werden sollen, geben Sie das Dateinamen-Präfix "|*FTMONITOR " an. Die Funktion des Profils muss Dateivorverarbeitung erlauben (*-ff=tp*). Details siehe Kommando *ftcrep*, Beispiel 3 auf Seite 208.

-fnp nicht angegeben
Die Festlegungen des Berechtigungsprofils zum Dateinamen-Präfix bleiben unverändert.

-ls= | **-ls=@n** | **-ls=**Kommando1

Mit *-ls* können Sie eine Folgeverarbeitung vorgeben, die nach **erfolgreicher Dateiübertragung** unter Ihrer Benutzerkennung durchgeführt werden soll. Wenn mit *-ls* eine Festlegung getroffen wurde, darf im Dateiübertragungsauftrag keine Folgeverarbeitung nach erfolgreicher Übertragung verlangt werden! Eine Festlegung für *-ls* ist nur sinnvoll, wenn Sie durch entsprechende Festlegungen für *-lf* (siehe unten) verhindern, dass sie durch einen mutwillig misslungenen Auftrag umgangen werden kann. Wenn Sie mit *-fnp* ein Präfix für den Dateinamen definiert haben und eine Folgeverarbeitung mit dieser Datei planen, müssen Sie hier den vollständigen Dateinamen angeben.

@n für *Kommando1*

Wenn Sie *-ls=@n* eingeben, erlaubt das Berechtigungsprofil keine Folgeverarbeitung nach erfolgreicher Dateiübertragung.

Kommando1 nicht angegeben

Mit der Angabe *-ls=* können Sie eine Festlegung zur Folgeverarbeitung wieder rückgängig machen. Das Berechtigungsprofil schränkt dann die Folgeverarbeitung im lokalen System nach erfolgreicher Dateiübertragung nicht mehr ein. So können Sie auch ein mit *-lsp* definiertes Präfix für die Folgeverarbeitung zurücknehmen.

-ls nicht angegeben

Die Festlegungen des Berechtigungsprofils zur Folgeverarbeitung nach erfolgreicher Dateiübertragung bleiben unverändert.

-lsp=[Kommando2]

Mit *-lsp* können Sie ein Präfix für die Folgeverarbeitung nach **erfolgreicher Dateiübertragung** im lokalen System definieren. FTAC setzt dann die Zeichenfolge *Kommando2* vor die im File Transfer-Auftrag verlangte Folgeverarbeitung und versucht, das so entstandene Kommando auszuführen. Wenn Sie zum Beispiel *'lpr␣'* angeben und im Auftrag für die Folgeverarbeitung *datei.txt* steht, dann führt FTAC die Folgeverarbeitung *lpr␣datei.txt* aus.
Präfix, Suffix und Folgeverarbeitungskommando dürfen zusammen maximal 1000 Bytes lang sein (Darstellung in UTF-8, siehe Seite 169).

Beachten Sie bitte die Informationen zur Option *-ls*!

Wenn mit *-lsp* ein Präfix definiert wurde, ist der Zeichenvorrat für die Folgeverarbeitung im File Transfer-Auftrag begrenzt auf:
- alphanumerische Zeichen (Buchstaben und Ziffern)
- die Sonderzeichen + = / ! ␣ - , @ _ " $ '
- einen Punkt (.) zwischen alphanumerischen Zeichen.

Ein bereits definiertes Präfix können Sie mit der Angabe *-ls=* wieder zurücknehmen.

Kommando2 nicht angegeben

Mit der Angabe *-lsp=* wird die Festlegung im Berechtigungsprofil für ein Präfix der Folgeverarbeitung nach erfolgreicher Dateiübertragung rückgängig gemacht.

-lsp nicht angegeben

Die Festlegungen des Berechtigungsprofils für ein Präfix der Folgeverarbeitung nach erfolgreicher Dateiübertragung bleiben unverändert.

-lss=[Kommando3]

Mit *-lss* können Sie ein Suffix für die Folgeverarbeitung nach **erfolgreicher Dateiübertragung** im lokalen System definieren. FTAC setzt dann die Zeichenfolge *Kommando3* hinter die im File Transfer-Auftrag verlangte Folgeverarbeitung und versucht, das so entstandene Kommando auszuführen. Wenn Sie zum Beispiel *-lss=␣datei.txt* angeben und im Auftrag für die Folgeverarbeitung *lpr* steht, dann führt FTAC die Folgeverarbeitung *lpr␣datei.txt* aus.
Präfix, Suffix und Folgeverarbeitungskommando dürfen zusammen maximal 1000 Bytes lang sein (Darstellung in UTF-8, siehe Seite 169).
Beachten Sie bitte die Informationen zur Option *-ls*!
Wenn mit *-lss* ein Suffix definiert wurde, ist der Zeichenvorrat für die Folgeverarbeitung im File Transfer-Auftrag begrenzt auf:

- alphanumerische Zeichen (Buchstaben und Ziffern)
- die Sonderzeichen + = / ! ␣ - , @ _ " $ '
- einen Punkt (.) zwischen alphanumerischen Zeichen

Kommando3 nicht angegeben

Mit der Angabe *-lss=* wird die Festlegung im Berechtigungsprofil für ein Suffix der Folgeverarbeitung nach erfolgreicher Dateiübertragung rückgängig gemacht.

-lss nicht angegeben

Die Festlegungen des Berechtigungsprofils für ein Suffix der Folgeverarbeitung nach erfolgreicher Dateiübertragung bleiben unverändert.

-lf= | **-lf=@n** | **-lf=**Kommando4

Mit *-lf* können Sie eine Folgeverarbeitung vorgeben, die unter Ihrer Benutzerkennung durchgeführt werden soll, wenn die **Dateiübertragung abgebrochen** wurde. Wenn mit *-lf* eine Festlegung getroffen wurde, darf im File Transfer-Auftrag keine Folgeverarbeitung nach misslungener Übertragung verlangt werden! Eine Festlegung für *-lf* ist nur sinnvoll, wenn Sie durch entsprechende Festlegungen für *-ls* (siehe oben) verhindern, dass sie durch einen erfolgreichen Auftrag umgangen werden kann. Wenn Sie mit *-fnp* ein Präfix für den Dateinamen definiert haben und eine Folgeverarbeitung mit dieser Datei planen, müssen Sie hier den vollständigen Dateinamen angeben.

@n für *Kommando4*
wenn Sie *-lf=@n* eingeben, erlaubt das Berechtigungsprofil keine Folgeverarbeitung nach misslungener Dateiübertragung.

Kommando4 nicht angegeben
Mit der Angabe *-lf=* können Sie eine Festlegung zur Folgeverarbeitung nach misslungener Dateiübertragung wieder rückgängig machen. Das Berechtigungsprofil schränkt dann die Folgeverarbeitung im lokalen System nach misslungener Dateiübertragung nicht mehr ein. So können Sie auch ein mit *-lfp* definiertes Präfix zurücknehmen.

-lf nicht angegeben
Die Festlegungen des Berechtigungsprofils zur Folgeverarbeitung nach misslungener Dateiübertragung bleiben unverändert.

-lfp=[Kommando5]
Mit *-lfp* können Sie ein Präfix für die Folgeverarbeitung nach **misslungener Dateiübertragung** im lokalen System definieren. FTAC setzt dann die Zeichenfolge *Kommando5* vor die im File Transfer-Auftrag verlangte Folgeverarbeitung und versucht, das so entstandene Kommando auszuführen. Wenn Sie zum Beispiel *-lfp='lpr␣'* angeben und im Auftrag für die Folgeverarbeitung *error.txt* steht, dann führt FTAC die Folgeverarbeitung *lpr␣error.txt* aus.

Präfix, Suffix und Folgeverarbeitungskommando dürfen zusammen maximal 1000 Bytes lang sein (Darstellung in UTF-8, siehe Seite 169).

Beachten Sie bitte die Informationen zur Option *-lf* !

Wenn mit *-lfp* ein Präfix definiert wurde, ist der Zeichenvorrat für die Folgeverarbeitung im File Transfer-Auftrag begrenzt auf:
– alphanumerische Zeichen (Buchstaben und Ziffern)
– die Sonderzeichen + = / ! ␣ - , @ _ " $ '
– einen Punkt (.) zwischen alphanumerischen Zeichen.

Ein bereits definiertes Präfix können Sie mit der Angabe *-lf=* wieder zurücknehmen.

Kommando5 nicht angegeben
Mit der Angabe *-lfp=* wird die Festlegung im Berechtigungsprofil für ein Präfix der Folgeverarbeitung nach misslungener Dateiübertragung rückgängig gemacht.

-lfp nicht angegeben
Die Festlegungen des Berechtigungsprofils für ein Präfix der Folgeverarbeitung nach misslungener Dateiübertragung bleiben unverändert.

-lfs=[Kommando6]
: Mit *-lfs* können Sie ein Suffix für die Folgeverarbeitung nach **misslungener Dateiübertragung** im lokalen System definieren. FTAC setzt dann die Zeichenfolge *Kommando6* hinter die im File Transfer-Auftrag verlangte Folgeverarbeitung und versucht, das so entstandene Kommando auszuführen. Wenn Sie zum Beispiel *-lfs=error.txt* angeben und im Auftrag für die Folgeverarbeitung *lpr* steht, dann führt FTAC die Folgeverarbeitung *lpr␣error.txt* aus.

  Präfix, Suffix und Folgeverarbeitungskommando dürfen zusammen maximal 1000 Bytes lang sein (Darstellung in UTF-8, siehe Seite 169).

  Beachten Sie bitte die Informationen zur Option *-lf* !

  Wenn mit *-lfs* ein Suffix definiert wurde, ist der Zeichenvorrat für die Folgeverarbeitung im File Transfer-Auftrag begrenzt auf:
  – alphanumerische Zeichen (Buchstaben und Ziffern)
  – die Sonderzeichen + = / ! ␣ - , @ _ " $ '
  – einen Punkt (.) zwischen alphanumerischen Zeichen

  Kommando6 nicht angegeben
  : Mit der Angabe *-lfs=* wird die Festlegung im Berechtigungsprofil für ein Suffix der Folgeverarbeitung nach misslungener Dateiübertragung rückgängig gemacht.

-lfs nicht angegeben
: Die Festlegungen des Berechtigungsprofils für ein Suffix der Folgeverarbeitung nach misslungener Dateiübertragung bleiben unverändert.

-wm=o | **-wm=n** | **-wm=e** | **-wm=one**
: Mit *-wm* können Sie festlegen, welche Schreibregeln im File-Transfer-Auftrag benutzt werden dürfen und wie sie wirken.

  o (overwrite) Im FT-Auftrag darf bei openFT- oder FTAM-Partnern als Schreibregel nur *-o* oder *-e* angegeben werden.
  Eine schon vorhandene Empfangsdatei wird überschrieben, eine noch nicht vorhandene Empfangsdatei wird neu eingerichtet.

  Bei FTP-Partnern ist im FT-Auftrag auch *-n* erlaubt, falls die Datei noch nicht existiert.

  n (no overwrite) Im FT-Auftrag darf als Schreibregel *-o*, *-n* oder *-e* angegeben werden. Eine noch nicht vorhandene Empfangsdatei wird neu eingerichtet. Wenn die Empfangsdatei schon existiert, wird der Auftrag nicht durchgeführt.

e (extend) Im FT-Auftrag darf als Schreibregel nur *-e* angegeben werden, d.h. die übertragene Datei wird an das Ende einer bereits vorhandenen Datei angehängt. Eine noch nicht vorhandene Empfangsdatei wird neu eingerichtet.

one Die Schreibregel wird durch das Berechtigungsprofil nicht eingeschränkt.

-wm nicht angegeben
Die Festlegungen des Berechtigungsprofils für die Schreibregel bleiben unverändert.

-c= | **-c=y** | **-c=n**
Mit *-c* können Sie festlegen, ob Datenverschlüsselung vorgeschrieben oder verboten wird. Stimmt die Einstellung im Profil nicht mit der Einstellung im Auftrag überein, dann wird der Auftrag abgelehnt. Die Einstellung gilt nicht für Dateimanagement-Aufträge, da es für diese Aufträge keine Datenverschlüsselung gibt.

y Über dieses Profil dürfen nur Aufträge mit Datenverschlüsselung abgewickelt werden.

n Über dieses Profil dürfen nur Aufträge ohne Datenverschlüsselung abgewickelt werden.

weder *y* noch *n* angegeben
Durch *-c=* wird die aktuelle Einstellung zurückgesetzt, d.h. es werden sowohl Aufträge mit Datenverschlüsselung als auch Aufträge ohne Datenverschlüsselung akzeptiert.

-c nicht angegeben
Die Verschlüsselungsoption bleibt unverändert.

-txt=Text | **-txt=**
Mit *-txt* können Sie einen neuen Kommentar im Berechtigungsprofil ablegen (maximal 100 Zeichen).

Text nicht angegeben
Mit der Angabe *-txt=* wird ein vorhandener Kommentar gelöscht.

-txt nicht angegeben
Ein vorhandener Kommentar bleibt unverändert.

Sobald Sie ein Berechtigungsprofil modifizieren, wird auch der Zeitstempel aktualisiert. Der Zeitstempel wird bei *ftshwp -l* ausgegeben (LAST-MODIF). Der Zeitstempel wird auch dann aktualisiert, wenn Sie die Eigenschaften des Profils nicht ändern, d.h. *ftmodp* ohne Parameter angeben.

VORSICHT!
Wenn Sie die Optionen *-ff=p*, *-fn*, *-fnp*, *-ls* , *-lsp*, *-lss*, *-lf*, *-lfp* oder *-lfs* benutzen, müssen Sie bedenken, dass

- eine Einschränkung für den Dateinamen durch Umbenennen umgangen werden kann, wenn nicht auch die Folgeverarbeitung eingeschränkt wird.
- eine Einschränkung für die Folgeverarbeitung sowohl die erfolgreiche als auch die misslungene Dateiübertragung umfassen muss und ggf. äquivalente Einschränkungen für eine eventuell zugelassene Vorverarbeitung vorliegen müssen.
- Präfixe für Dateinamen und Folgeverarbeitungen aufeinander abgestimmt sein müssen.
- in dem Teil Ihres Dateibaums, der hinter einem Dateinamen-Präfix möglich ist, keine symbolischen Verweise vorkommen sollten.
- eine Beschränkung einer Vor-, Nach- oder Folgeverarbeitung auf ein Kommando umgangen werden kann, wenn es möglich ist, dieses Kommando z.B. durch ein "trojanisches Pferd" zu ersetzen.

Beispiel

Bei dem im Abschnitt „Beispiele“ auf Seite 207 angelegten Berechtigungsprofil *monatsbe* soll die Zugangsberechtigung in *fuerDagobert* geändert werden. Die Übertragungsrichtung wird nicht mehr eingeschränkt. Das Profil wird zum Übertragen von beliebigen Dateien genutzt, die alle das Präfix *mine/* erhalten. Die Folgeverarbeitung soll ganz verboten werden.

Das Kommando lautet:

```
ftmodp␣monatsbe␣-tad=fuerDagobert␣-dir=tf \
␣-fnp=mine/␣-ls=@n␣-lf=@n
```

6.27 ftmodptn - Partnereigenschaften ändern

Mit dem Kommando *ftmodptn* ändern Sie die Eigenschaften von Partnersystemen in der Partnerliste des lokalen Systems.

Beim Ändern der Partneradresse ist zu beachten, dass damit aus einem openFT-Partner kein FTP-Partner oder FTAM-Partner bzw. umgekehrt gemacht werden kann.

Sie können einen eingetragenen dynamischen Partner mit *ftmodptn* aus der Partnerliste entfernen, indem Sie alle Eigenschaften auf die Standardwerte für freie dynamische Partner setzen. Die Standardwerte stimmen mit den Standardwerten beim Kommando *ftaddptn* überein bis auf die Sicherheitsstufe (Option *-sl*), die auf *-sl=p* gesetzt werden muss.

Umgekehrt können Sie einen freien dynamischen Partner in die Partnerliste aufnehmen, indem Sie mindestens eines seiner Attribute auf einen vom Standard abweichenden Wert setzen. Dies ist möglich, wenn *Partner* keinen Partnerlisten-Eintrag referenziert und *-pa* nicht angegeben wird.

Wenn in *Partner* ein Partnername angegeben ist, zu dem es noch keinen Partnerlisteneintrag gibt, und zusätzlich *-pa* spezifiziert ist, wird ein neuer benannter Partnerlisteneintrag erzeugt. Diese Funktion ist für das Re-Importieren exportierter Partnereinträge vorgesehen. Für die explizite Neuanlage von Partnereinträgen sollten Sie *ftaddptn* verwenden.

Format

```
ftmodptn  -h |
          <Partner 1..200> | @a
        [ -pa=<Partneradresse 1..200> ]
        [ -id=<Identifikation 1..64> | -id= ]
        [ -ri=<Routing-Info 1..8> | -ri=@i | -ri= ]
        [ -ptc=i | -ptc=a | -ptc= ]
        [ -pri=l | -pri=n | -pri=h ]
        [ -sl=1..100 | -sl=p | -sl= ]
        [ -st=a | -st=d | -st=ad ]
        [ -ist=a | -ist=d ]
        [ -am=n | -am=y ]
        [ -rqp=p | -rqp=s ]
        [ -tr=n | -tr=f | -tr= ]
```

Beschreibung

-h gibt die Kommandosyntax am Bildschirm aus. Weitere Angaben nach *-h* werden ignoriert.

Partner | **@a**
: *Partner* ist der Name des Partnersystems in der Partnerliste oder die Adresse des Partnersystems, dessen Eigenschaften Sie ändern möchten.

  @a für *Partner*
  : Partner ist kein Auswahlkriterium, d.h. Sie ändern die Eigenschaften aller Partnersysteme, die in der Partnerliste vorhanden sind. Diese Angabe ist nur in Verbindung mit den Optionen *-ptc*, *-sl*, *-st*, *-ist*, *-am*, *-rqp* und *-tr* möglich.

    @a sollte vor allem in Verbindung mit *-sl* (Sicherheitsstufe) mit Vorsicht eingesetzt werden!

-pa=Partneradresse
: mit *-pa* geben Sie die Adresse des Partnersystems in folgender Form an:

  [protocol**://**]host[**:**[port]**.**[tsel]**.**[ssel]**.**[psel]]

  Weitere Einzelheiten zur Adressangabe finden Sie im Abschnitt „Aufbau der Partneradressen“ auf Seite 68.

-pa nicht angegeben
: Die Partneradresse bleibt unverändert.

-id=Identifikation | **-id=**
: Netzweit eindeutige Identifikation der openFT-Instanz im Partnersystem.

  Bei FTAM-Partnern kann ein Application Entity Title in der Form *n1.n2.n3.n4..mmm* als Identifikation angegeben werden. *n1*, *n2* usw. sind positive ganze Zahlen, die den "Application Process Title" beschreiben. *n1* kann nur die Werte 0, 1 oder 2 annehmen, *n2* ist auf Werte zwischen 0 und 39 beschränkt, wenn *n1* nicht den Wert 2 hat. Der optionale Application Entity Qualifier *mmm* ist durch zwei Punkte von den Werten des Application Process Title getrennt. Details siehe Benutzerhandbuch zu openFT.

  Bei FTP-Partnern darf *-id* nicht angegeben werden!

  Identifikation nicht angegeben
  : Mit *-id=* ohne weitere Angabe wird die Identifikation bei Partnereinträgen mit openFT- und FTADM-Protokoll auf *host* (Rechnername) gesetzt. Bei FTAM-Partnern wird die Identifikation durch *-id=* gelöscht.

-id nicht angegeben
: Die Einstellung für die Identifikation bleibt unverändert.

-ri=Routing-Info | | **-ri=@i** | **-ri=**

Wenn das Partnersystem nur über eine Zwischeninstanz erreichbar ist, dann geben Sie mit *Routing-Info* die Adressinformation an, mit der die Zwischeninstanz weiterroutet.

@i für *Routing-Info*

Es wird die in *-id=* angegebene Instanzidentifikation als Routinginformation verwendet.

weder *@i* noch *Routing-Info* angegeben

Die Angabe von *-ri=* (ohne Parameter) bedeutet, dass das Partnersystem direkt erreichbar ist, d.h. ohne Zwischeninstanz.

-ri nicht angegeben

Die Einstellung für die Routing-Information bleibt unverändert.

-ptc=i | **-ptc=a** | **-ptc=**

Mit *-ptc* können Sie die Betriebsparameter-Einstellungen für die Absenderüberprüfung partnerspezifisch ändern. Diese Einstellungen wirken nur für Partner, die über das openFT-Protokoll verbunden sind und nicht mit Authentifizierung arbeiten (z.B. Partner mit openFT V8.0 oder älter).

i (identification)

Überprüfung der Transportadresse ausschalten. Es wird ausschließlich die Identifikation eines Partners geprüft. Die Transportadresse eines Partners wird auch dann nicht überprüft, wenn die erweiterte Absenderüberprüfung per Betriebsparameter eingeschaltet ist (siehe Kommando *ftmodo* auf Seite 236).

a (address)

Überprüfung der Transportadresse einschalten. Die Transportadresse eines Partners wird auch dann überprüft, wenn die Überprüfung der Transportadresse per Betriebsparameter ausgeschaltet ist (siehe Kommando *ftmodo* auf Seite 236).

Stimmt die Transportadresse, unter der sich ein Partner anmeldet, nicht mit dem Eintrag in der Partnerliste überein, dann wird der Auftrag abgelehnt.

weder *i* noch *a* angegeben

-ptc= (ohne Parameter) bedeutet, dass die Betriebsparameter-Einstellung für die Absenderüberprüfung gilt.

-ptc nicht angegeben

Die Einstellung für die Absenderüberprüfung bleibt unverändert.

-sl=1..100 | **-sl=p** | **-sl=**
Mit dieser Option ordnen Sie dem angegebenen Partnersystem bzw. allen Partnersystemen eine Sicherheitsstufe zu.

Eine niedrige Sicherheitsstufe bedeutet, dass das Schutzbedürfnis gegenüber diesem Partner niedrig ist, weil z.B. seine Identität durch Authentifizierung mit kryptografischen Mitteln überprüft wird und man dadurch sicher sein kann, dass es sich tatsächlich um den betreffenden Partner handelt.

Eine hohe Sicherheitsstufe bedeutet, dass das Schutzbedürfnis gegenüber diesem Partner hoch ist, da die Identität des Partners z.B. nur über seine Adresse ermittelt wird und keine Authentifizierung mit kryptografischen Mitteln stattgefunden hat.

1..100
ordnet dem Partner eine feste Sicherheitsstufe zu. 1 bedeutet die niedrigste und 100 die höchste Sicherheitsstufe.

Es sind alle ganzzahligen Werte von 1 bis 100 erlaubt.

p ordnet dem Partner die Sicherheitsstufe anhand seiner Attribute zu, d.h.:

- Sicherheitsstufe 10, wenn der Partner authentifiziert ist.
- Sicherheitsstufe 90, wenn der Partner im Transportsystem bekannt ist und über seinen im Transportsystem bekannten Namen identifiziert wird.
- Sicherheitsstufe 100, wenn der Partner nur über seine Adresse identifiziert wird.

Sicherheitsstufe nicht angegeben
-sl= (ohne Parameter) bedeutet, dass die Betriebsparameter-Einstellung für die Sicherheitsstufe gilt (siehe Kommando *ftmodo* auf Seite 236)

-sl nicht angegeben
Die Einstellung für die Sicherheitsstufe bleibt unverändert.

-pri=l | **-pri=n** | **-pri=h**
Mit *-pri* legen Sie die Priorität eines Partners bezüglich der Abarbeitung von Aufträgen mit gleicher Auftragspriorität fest. D.h. die Partnerpriorität kommt nur unter Aufträgen zum Tragen, die dieselbe Auftragspriorität haben, aber zu Partnern mit unterschiedlicher Partnerpriorität gehen.

l (low)
Der Partner erhält eine niedrige Priorität.

n (normal)
Der Partner erhält eine normale Priorität.

h (high)
Der Partner erhält eine hohe Priorität.

-pri nicht angegeben
: Die Einstellung für die Priorität bleibt unverändert.

-st=a | **-st=d** | **-st=ad**
: Mit dieser Option können Sie steuern, wie lokal gestellte asynchrone Dateiübertragungsaufträge an das angegebene Partnersystem bzw. die Partnersysteme bearbeitet werden.

  a (active)
  : Lokal gestellte asynchrone Dateiübertragungsaufträge werden bearbeitet, wenn der asynchrone openFT-Server gestartet ist.

  d (deactivated)
  : Lokal gestellte asynchrone Dateiübertragungsaufträge werden zunächst nicht bearbeitet, sondern nur im Auftragsbuch abgelegt.

  ad (automatic deactivation)
  : Mehrere direkt aufeinander folgende fehlgeschlagene Verbindungsaufbauversuche zu diesem Partnersystem führen zu dessen Deaktivierung. Um wieder File-Transfer mit diesem Partnersystem betreiben zu können, muss es explizit mit *ftmodptn -st=a* aktiviert werden.

    Die maximale Anzahl solcher Fehlversuche beträgt 5, nach einem erfolgreichen Verbindungsaufbau wird der Zähler wieder auf 0 gesetzt.

-st nicht angegeben
: Der Bearbeitungsmodus bleibt unverändert.

-ist=a | **-ist=d**
: Mit dieser Option können Sie steuern, wie fern gestellte Dateiübertragungsaufträge vom angegebenen Partnersystem bzw. den Partnersystemen bearbeitet werden.

  a (active)
  : Fern gestellte Dateiübertragungsaufträge werden bearbeitet, wenn der asynchrone openFT-Server gestartet ist.

  d (deactivated)
  : Fern gestellte synchrone Dateiübertragungsaufträge von diesem Partnersystem werden abgelehnt. Fern gestellte asynchrone Dateiübertragungsaufträge von diesem Partner bleiben dort gespeichert und können erst dann bearbeitet werden, wenn dieser Partner mit *-ist=a* wieder aktiv gesetzt ist.

-ist nicht angegeben
: Der Bearbeitungsmodus bleibt unverändert.

-am=n | **-am=y**

Mit *-am* (authentication mode) können Sie die Authentifizierung eines Partners erzwingen.

n Die Authentifizierung wird nicht erzwungen, d.h. dieser Partner ist bezüglich Authentifizierung nicht eingeschränkt.

y Die Authentifizierung wird erzwungen, d.h. Aufträge werden nur bearbeitet, wenn das lokale System den Partner erfolgreich authentifizieren kann, siehe Seite 78.

-am nicht angegeben

Der Authentifizierungsmodus bleibt unverändert.

-rqp=p | **-rqp=s**

Mit dieser Option (rqp = request processing) steuern Sie, ob asynchrone Outbound-Aufträge zu diesem Partner grundsätzlich seriell durchgeführt werden oder ob parallele Verbindungen erlaubt sind.

p (parallel)

Parallele Verbindungen zu diesem Partner sind erlaubt.

s (seriell)

Parallele Verbindungen zu diesem Partner sind nicht erlaubt. Wenn mehrere Dateiübertragungsaufträge zu diesem Partnersystem anstehen, dann werden diese seriell abgearbeitet. Ein Folgeauftrag wird damit erst gestartet, wenn der vorausgegangene Auftrag beendet ist.

-rqp nicht angegeben

Der Bearbeitungsmodus bleibt unverändert.

-tr=n | **-tr=f** | **-tr=**

Mit dieser Option können Sie die Betriebsparameter-Einstellungen für die Partner-Selektion der openFT-Überwachungsfunktion partnerspezifisch ändern.

n (on)

Die Überwachungsfunktion ist für diesen Partner eingeschaltet. Es wird jedoch nur dann ein Trace geschrieben, wenn auch die openFT-Überwachungsfunktion per Betriebsparameter eingeschaltet ist. In diesem Fall hat diese Einstellung bei *ftmodptn* Vorrang gegenüber der Partnerselektion für die Überwachungsfunktion in den Betriebsparametern, siehe auch Seite 236ff, *ftmodo*, Optionen *-tr* und *-trp*.

f (off)

Die Überwachungsfunktion wird für diesen Partner bzw. alle Partner ausgeschaltet.

weder *n* noch *f* angegeben

-tr= (ohne Parameter) bedeutet, dass die Betriebsparameter-Einstellung für die Partner-Selektion der openFT-Überwachungsfunktion gilt (siehe Kommando *ftmodo* auf Seite 236).

-tr nicht angegeben

Die Einstellung für die Überwachungsfunktion bleibt unverändert.

6.28 ftmodr - Eigenschaften von Aufträgen ändern

Mit dem *ftmodr*-Kommando können Sie die Priorität der von Ihnen gestellten Aufträge oder auch einer Gruppe von Aufträgen ändern, z.B. die Priorität aller Aufträge an einen bestimmten Partner oder für einen bestimmten Dateinamen. Außerdem haben Sie die Möglichkeit, die Reihenfolge der Aufträge innerhalb einer Priorität zu ändern.

Als FT-Verwalter können Sie die Priorität aller Aufträge im System ändern.

Format

ftmodr -h |
[-ua=<Benutzerkennung 1..32> | -ua=@a]
[-pn=<Partner 1..200>]
[-fn=<Dateiname 1..512>]
[-pr=n | -pr=l][-qp=f | -qp=l]
[<Auftrags-Id 1..2147483647>]

Beschreibung

-h gibt die Kommandosyntax am Bildschirm aus. Weitere Angaben nach *-h* werden ignoriert.

-ua=Benutzerkennung | **-ua=@a**
Mit *-ua* legt man fest, für welche Benutzerkennung Aufträge modifiziert werden sollen.

Benutzerkennung
Als FT-Verwalter dürfen Sie hier jede beliebige Benutzerkennung angeben.

@a Als FT-Verwalter können Sie durch Angabe von *@a* Aufträge aller Benutzerkennungen modifizieren.

-ua= nicht angegeben
Die eigene Benutzerkennung ist das Auswahlkriterium. Ausnahme: Sie haben das Kommando als FT-Verwalter aufgerufen und dabei auch eine Auftrags-Id angegeben: in diesem Fall ist die Voreinstellung *@a*.

-pn=Partner
Mit *-pn* können Sie einen Namen oder eine Adresse für das Partnersystem angeben, für das Sie Aufträge modifizieren wollen. Der Partner sollte so angegeben werden, wie er bei der Auftragseingabe angegeben wurde oder wie er beim Kommando *ftshwr* ohne Option *-s*, *-l* oder *-csv* ausgegeben wird. Wenn openFT zu einer angegebenen Partneradresse einen Partner in der Partnerliste findet, so zeigt *ftshwr* den Namen des Partners an, selbst wenn bei der Auftragseingabe eine Partneradresse angegeben wurde.

-fn=Dateiname
: Mit *-fn* legen Sie fest, für welchen Dateinamen Aufträge modifiziert werden sollen. Es werden Aufträge modifiziert, die im lokalen System auf diese Datei zugreifen.

  Es muss der Dateiname angegeben werden, der auch bei der Auftragserstellung verwendet wurde. Dieser Dateiname wird auch beim Kommando *ftshwr* ohne Option *-fn* ausgegeben.

  Wildcards im Dateinamen sind nicht erlaubt.

-pr=n | **-pr=l**
: gibt die neue Priorität an. Folgende Werte sind möglich:

  n (normal)
  : der Auftrag erhält die Priorität "normal"

  l (low)
  : der Auftrag erhält die Priorität "niedrig"

-qp=f | **-qp=l**
: gibt die neue Position des Auftrags innerhalb der gleichen Priorität an. Folgende Werte sind möglich:

  f (first)
  : Der Auftrag wird als erster Auftrag innerhalb der Aufträge mit der gleichen Priorität eingereiht.

  l (last)
  : Der Auftrag wird als letzter Auftrag innerhalb der Aufträge mit der gleichen Priorität eingereiht.

Auftrags-Id
: Mit *Auftrags-Id* geben Sie die Identifikation eines bestimmten Auftrags an, der modifiziert werden soll. Die Auftrags-Id wird bei der Bestätigung der Auftragsannahme am Bildschirm ausgegeben. Sie können sie sich auch über das Kommando *ftshwr* anzeigen lassen.

Wenn Sie eine Auftrags-Id angegeben haben und die übrigen angegebenen Auswahlkriterien passen nicht zu dem Auftrag, dann wird der Auftrag nicht modifiziert und folgende Fehlermeldung ausgegeben:

```
ftmodr: Auftrag Auftrags-Id nicht gefunden
```

6.29 ftmonitor - openFT Monitor zur Messdatenanzeige aufrufen

Mit dem Kommando *ftmonitor* rufen Sie den openFT Monitor auf, in dem die Messwerte des openFT-Betriebs angezeigt werden. openFT kann auf dem lokalen System oder auch auf einem fernen System laufen. Der openFT Monitor kann nur aufgerufen werden, wenn die Messdatenermittlung auf dem betreffenden System explizit per Administration eingeschaltet (z.B. per Kommando *ftmodo -mon=n*) und der asynchrone openFT-Server gestartet ist.

> Bitte beachten Sie, dass Sie für die Verwendung des Kommandos *ftmonitor* ein grafikfähiges Terminal benötigen.

Format

ftmonitor -h |
[-lay=<Monitor Layout Dateiname 1..512>]
[-po=<Polling Intervall 1..600>]
[<Partner 1..200> [
<Zugangsberechtigung 8..67> |
<Benutzerkennung 1..67>[,[<Account 1..64>][,[<Kennwort 1..64>]]]]]

Beschreibung

-h gibt die Kommandosyntax aus. Weitere Angaben nach *-h* werden ignoriert.

-lay=Monitor Layout Dateiname
Name der Monitor Layout-Datei. Diese beschreibt, welche Messdaten ausgegeben werden und wie sie dargestellt werden.

Der Name der Layout-Datei muss mit dem Suffix *.ftmc* angegeben werden. Dieses Suffix wird vom Monitor beim Abspeichern automatisch vergeben, wenn es dort nicht explizit angegeben wurde.

Der Inhalt der Layout-Datei wird ebenfalls vom Monitor erzeugt. Sie dürfen den Inhalt der Layout-Datei nicht ändern.

Nach dem ersten Öffnen des Standard-Monitorfensters (ohne Angabe von *-lay*) kann eine eigene Layout-Datei erstellt und gespeichert werden. Dazu wählen Sie z.B. im Monitorfenster über das Menü *Ansicht* ein anderes Layout aus oder stellen über das Auswahlsymbol rechts oben einen anderen Wert ein und speichern die Einstellung unter einem selbstgewählten Namen ab. Details siehe Online-Hilfe zum openFT Monitor.

-lay nicht angegeben
Wenn Sie *-lay* nicht angeben, dann wird das Standard-Monitorfenster geöffnet. Dieses enthält ein Diagramm, das den zeitlichen Verlauf des Messwertes *Netzbytes/sec aller Aufträge* anzeigt (entspricht dem Parameter *ThNetbTtl* im Kommando *ftshwm*).

-po=Polling Intervall
: Polling Intervall in Sekunden.

  Mögliche Werte: 1 bis 600.
  Standardwert: 1

Partner
: Name oder Adresse des Partnersystems, dessen Messdaten angezeigt werden sollen. Der Partner muss ein openFT-Partner sein (d.h. Kommunikation über das openFT-Protokoll) und die Messdatenerfassung unterstützen, seine openFT-Version muss also mindestens V11 sein.

  Außerdem muss sein asynchroner openFT-Server gestartet und die Messdatenerfassung in seinen Betriebsparametern aktiviert sein.

Partner nicht angegeben
: Wenn Sie keinen Partner angeben, dann werden die Messdaten der openFT-Instanz auf dem lokalen Rechner ausgegeben.

Zugangsberechtigung | Benutzerkennung[**,**[Account][**,**[Kennwort]]]
: Zugangsberechtigung für das Partnersystem. Unter der angegebenen Zugangsberechtigung muss Dateiübertragung und Vor-/Nachverarbeitung erlaubt sein.

  Diese Zugangsberechtigung können Sie angeben

  – als FTAC-Zugangsberechtigung, wenn im fernen System bzw. der Zielinstanz FTAC eingesetzt wird. Im Partnersystem kann zu diesem Zweck ein spezielles Berechtigungsprofil mit dem Dateinamen-Präfix "|*FTMONITOR " eingerichtet werden, welches nur das Ermitteln von Messdaten erlaubt. Ein Beispiel finden Sie bei *ftcrep* auf Seite 208.

  – oder als Login/LOGON-Kennung in der Syntax des fernen Systems (*Benutzerkennung*, ggf. mit *Account* und/oder *Kennwort*).

Zugangsberechtigung nicht angegeben
: Wenn Sie für ein fernes Partnersystem keine Zugangsberechtigung angeben, so wird diese in einer Dialogbox nachgefordert. Die Eingabe des Passworts bzw. der FTAC-Zugangsberechtigung bleibt unsichtbar, es werden stattdessen Sternchen (*****) angezeigt.

Meldungen des openFT Monitors

Der openFT Monitor gibt Fehlermeldungen in Form einer Dialogbox aus. Er beendet sich, wenn ein Fehler auftritt oder wenn die Messdatenerfassung im zu vermessenden System beendet wird.

Wird das Layout des Monitorfensters geändert und wird openFT beendet, bevor das geänderte Layout gespeichert wurde, dann gibt der openFT Monitor eine Meldung aus und fragt ab, ob das Layout gesichert werden soll.

6.30 ftremptn - Partner aus der Partnerliste entfernen

Mit *ftremptn* können Sie einen Partner aus der Partnerliste entfernen.

Format

ftremptn -h |
<Partner 1..200>

Beschreibung

-h gibt die Kommandosyntax am Bildschirm aus. Weitere Angaben nach *-h* werden ignoriert.

Partner
gibt den Partner an, der aus der Partnerliste entfent werden soll. Sie können den Namen in der Partnerliste oder die Adresse des Partners angeben. Der Name und die Adresse werden beim Kommando *ftshwptn* angezeigt.

Alle Aufträge, die zu diesem Partner im Auftragsbuch gespeichert sind, werden gelöscht. Dies geschieht auch dann, wenn der Auftrag in einem Zustand ist, in dem auch das Partnersystem den Auftrag bereits kennt. Da dadurch Inkonsistenzen entstehen können, sollten Sie einen Partner erst dann aus der Partnerliste entfernen, wenn entweder keine Aufträge mehr zu diesem Partner im Auftragsbuch gespeichert sind oder wenn sichergestellt ist, dass das Partnersystem nicht mehr aktiv werden wird.

6.31 ftsetjava - Link auf das Java-Executable verwalten

ftsetjava wird verwendet, um den Verweis auf das Java-Executable zu setzen.

ftsetjava wird bei der Installation von openFT implizit verwendet. Darüberhinaus können Sie als Verwalter *ftsetjava* aufrufen, um

- sich anzusehen, auf welche Datei der von openFT verwendete Verweis auf das Java-Executable zeigt
- den Verweis zu setzen, falls Java zum Zeitpunkt der openFT-Installation noch nicht oder nicht in der richtigen Version installiert war oder falls sich der Installationspfad des Java-Executables geändert hat.
- sich anzusehen, welche Java-Installationen in den von openFT durchsuchten Verzeichnissen vorhanden sind.

Format

ftsetjava [@s | @a | <Dateiname 1..512>]

Beschreibung

@s Setzt den Verweis auf das Java-Executable.
Schlägt der Versuch fehl, einen Verweis auf das Java-Executable zu setzen, weil keine geeignete Java-Installation vorhanden ist, so wird eine entsprechende Meldung auf die Standardfehlerausgabe ausgegeben. Während der Installation von openFT wird in diesem Falle ebenfalls eine Warnung ausgegeben.

@a Zeigt alle im Suchpfad installierten Java-Executables an. Ein nachfolgender Aufruf von *ftsetjava @s* ist genau dann erfolgreich, wenn mindestens eine dieser Installationen den von openFT vorausgesetzten Bedingungen an die Version entspricht. Als Quelle des Verweises wird dann die Datei verwendet, deren Version der vorausgesetzten Java-Version 1.5 am nächsten kommt. Sind mehrere Java-Executables mit der selben Version installiert, so wird das in der Liste zuerst angezeigte verwendet.

Dateiname
Setzt den Verweis auf das angegebene Java-Executable. Es ist der vollqualifizierte Dateiname eines ausführbaren Java-Executables anzugeben, das den von openFT vorausgesetzten Bedingungen an die Version entspricht. Schlägt der Versuch fehl, einen Verweis auf das Java-Executable zu setzen, so wird eine entsprechende Meldung auf die Standardfehlerausgabe ausgegeben.

weder *@s* noch *@a* noch *Dateiname* angegeben
ftsetjava ohne Parameter gibt den vollständigen Pfad des von openFT verwendeten Java-Executables aus.

6.32 ftshwa - Berechtigungssätze anzeigen

ftshwa steht für "show admission set", also Zeigen des Berechtigungssatzes.

Als FTAC-Verwalter können Sie sich alle Berechtigungssätze des Systems ansehen.

Als FT-Verwalter können Sie den FTAC-Verwalter und den ADM-Verwalter ermitteln.

Sie erhalten folgende Informationen:

- welche Grenzwerte der Eigentümer der Benutzerkennung bei den einzelnen Grundfunktionen eingestellt hat,
- welche Grenzwerte der FTAC-Verwalter für die Benutzerkennung bei den einzelnen Grundfunktionen eingestellt hat,
- ob der Berechtigungssatz das FTAC-Privileg besitzt, d.h. ob der Eigentümer des Berechtigungssatzes FTAC-Verwalter ist.
- ob der Berechtigungssatz das ADM-Privileg besitzt, d.h. ob der Eigentümer des Berechtigungssatzes ADM-Verwalter ist.

Format

ftshwa -h |
[<Benutzerkennung 1..32> | @a | @s][-csv]

Beschreibung

-h gibt die Kommandosyntax am Bildschirm aus. Weitere Angaben nach *-h* werden ignoriert.

Benutzerkennung | **@a** | **@s**
gibt die Benutzerkennung an, deren Berechtigungssatz Sie sich ansehen wollen.

Benutzerkennung
Als FTAC-Verwalter dürfen Sie jede beliebige Benutzerkennung angeben.

Falls eine mehr als 8 Bytes lange Benutzerkennung angegeben war, werden die ersten sieben Zeichen gefolgt von einem * ausgegeben.

@a für *Benutzerkennung*
Als FTAC-Verwalter erhalten Sie Informationen über den Standardberechtigungssatz und alle Berechtigungssätze, die vom Standardberechtigungssatz abweichen.

Als FT-Verwalter (aber nicht FTAC-Verwalter) erhalten Sie Informationen über Ihren Berechtigungssatz, den Standardberechtigungssatz sowie den Berechtigungssatz des FTAC-Verwalters und den Berechtigungssatz des ADM-Verwalters.

@s für *Benutzerkennung*
Mit dieser Angabe erhalten Sie Informationen über den Standardberechtigungssatz.

Geben Sie für *Benutzerkennung* eine nicht existierende Kennung an, so erhalten Sie für diese Kennung die Werte des aktuellen Standardberechtigungssatzes.

Benutzerkennung nicht angegeben
FTAC gibt Informationen über den Berechtigungssatz der Benutzerkennung aus, unter der *ftshwa* eingegeben wird.

-csv Mit *-csv* geben Sie an, dass die FT-Berechtigungssätze im CSV-Format ausgegeben werden sollen. Die Werte der Ausgabe werden durch Strichpunkte getrennt ausgegeben.

-csv nicht angegeben
Sie bekommen die FT-Berechtigungssätze im Standardformat ausgegeben.

6.32.1 Ausgabeformat von ftshwa

Beispiel für die Ausgabe aller Berechtigungssätze:

```
ftshwa @a

                MAX. USER LEVELS              MAX. ADM LEVELS          ATTR
 USER-ID  OBS  OBR  IBS  IBR  IBP  IBF  OBS  OBR  IBS  IBR  IBP  IBF
 *STD     100  100  100  100  100  100  100  100  100  100  100  100
 root      50   50    1    1    1    1   50   50    1    1    1    1  PRIV,ADMPR
 mueller   90   90    0    0    0   90  100* 100* 100* 100* 100* 100*
```

Erläuterung

USER-ID
In der Spalte USER-ID steht die Benutzerkennung, zu der der jeweilige Berechtigungssatz gehört. Falls eine mehr als 8 Bytes lange Benutzerkennung angegeben war, werden die ersten sieben Zeichen gefolgt von einem * ausgegeben.

MAX. USER LEVELS / MAX. ADM LEVELS

In den sechs Spalten im Bereich MAX. USER LEVELS sind die Grenzwerte angegeben, die der Benutzer für seinen Berechtigungssatz festgelegt hat. Entsprechend enthalten die sechs Spalten im Bereich
MAX. ADM LEVELS die Grenzwerte, die der FTAC-Verwalter eingestellt hat. Der kleinere der Grenzwerte gibt an, ob der Benutzer die jeweilige Grundfunktion nutzen darf.

Die Grundfunktionen sind in der Ausgabe folgendermaßen abgekürzt:

```
OBS = OUTBOUND-SEND
OBR = OUTBOUND-RECEIVE
IBS = INBOUND-SEND
IBR = INBOUND-RECEIVE
IBP = INBOUND-PROCESSING
IBF = INBOUND-FILE-MANAGEMENT
```

Die Werte in der Anzeige haben folgende Bedeutung:

0	Die Grundfunktion ist gesperrt.
1..99	Die Grundfunktion ist nur für Partnersysteme mit gleicher oder niedrigerer Sicherheitsstufe freigegeben. Die Sicherheitsstufe eines Partnersystems können Sie sich mit dem Kommando *ftshwptn* anzeigen lassen.
100	Die Grundfunktion ist für alle Partnersysteme freigegeben.

Ein Stern hinter dem Wert bedeutet, dass diese Angabe aus dem Standardberechtigungssatz übernommen wurde. Beim Ändern des Standardberechtigungssatzes wird sie dann automatisch mitgeändert.

ATTR PRIV in der Spalte ATTR kennzeichnet den privilegierten Berechtigungssatz. Also ist *root* der FTAC-Verwalter.

ADMPR in der Spalte ATTR kennzeichnet den ADM-Verwalter. Damit ist *root* zusätzlich auch Verwalter des Fernadministrations-Servers.

6.33 ftshwatp - ADM-Traps ausgeben

Mit *ftshwatp* informieren Sie sich als FT-Verwalter des ADM-Trap-Servers über die ADM-Traps, die an den ADM-Trap-Server geschickt und dort in der ADM-Trap-Log-Datei gespeichert werden.

Wird der ADM-Trap-Server zusätzlich als Fernadministrations-Server genutzt, dann können sich auch der ADM-Verwalter und die Fernadministratoren ADM-Traps ansehen:

- Als ADM-Verwalter des Fernadministrations-Servers können Sie alle ADM-Traps ansehen.
- Als Fernadministrator können Sie sich (lokal oder via *ftadm*) jeweils "Ihre" ADM-Traps ansehen. Das heißt, Sie sehen nur die ADM-Traps der openFT-Instanzen, für die Sie mindestens FTOP-Berechtigung haben, siehe Abschnitt „ftshwc - Fernadministrierbare openFT-Instanzen anzeigen“ auf Seite 298.

Die ADM-Traps werden durch Trap-Ids identifiziert. Die Trap-Ids werden aufsteigend vergeben, die Nummerierung ist aus technischen Gründen nicht immer lückenlos. Ohne weitere Angaben gibt openFT immer den aktuellsten ADM-Trap aus. Bei entsprechender Anforderung gibt openFT alle ADM-Traps bis zur im Kommando spezifizierten Anzahl aus.

Die ADM-Traps werden in der ADM-Trap-Log-Datei gespeichert. Die maximale Anzahl von gespeicherten ADM-Traps hängt von der maximal möglichen Größe der ADM-Trap-Log-Datei ab. Wird die maximale Anzahl von ADM-Traps überschritten, dann werden die Sätze mit der jeweils kleinsten Trap-Id durch aktuelle Sätze überschrieben. Weitere Details siehe Seite 152.

Sie können zwischen drei Ausgabeformaten wählen, der Kurzform, der ausführlichen Form der Ausgabe und dem CSV-Ausgabeformat (**C**haracter **S**eparated **V**alue).

Die Ausgabe erfolgt auf der Standardausgabe.

Format

```
ftshwatp -h |
        [ -rg=[[[[yyyy]mm]dd]hhmm |
                  #1..99999999999999999 ][-
                [[[[yyyy]mm]dd]hhmm |
                [ #1..99999999999999999 ] ]
        [ -src=<Partner 1..200> ]
        [ -tt=[fts][,][pts][,][ptu][,][rqc][,][rqf][,][rqs] ]
        [ -nb=1.. 9999999 | -nb=@a ]
        [ -l | -csv ]
```

Beschreibung

-h gibt die Kommandosyntax am Bildschirm aus. Weitere Angaben nach *-h* werden ignoriert.

-rg=[[[[yyyy]mm]dd]hhmm][**-**[[[[yyyy]mm]dd]hhmm]
Hier geben Sie mit *-rg* wahlweise den Beginn und/oder das Ende eines Zeitbereichs an.

[[[yyyy]mm]dd]hhmm
Bei Wahl einer Zeit wird dies 4-stellig als Uhrzeit in Stunden und Minuten, 6-stellig als Tag (Datum) und Uhrzeit in Stunden und Minuten, 8-stellig als Monat, Tag und Uhrzeit in Stunden und Minuten, 12-stellig als Jahr, Monat, Tag und Uhrzeit in Stunden und Minuten interpretiert. Der größtmögliche Wert für das anzugebende Datum ist 20380119 (19. Januar 2038). openFT gibt dann die ADM-Traps aus, die innerhalb der angegebenen Grenzen liegen.

-rg=[[[yyyy]mm]dd]hhmm
Es werden die ADM-Traps ausgegeben, die zur angegebenen Zeit aufgetreten sind.

-rg=[[[yyyy]mm]dd]hhmm**-**[[[yyyy]mm]dd]hhmm
Der Zeitbereich beginnt mit der Startzeit und endet mit der zweiten angegebenen Zeit.

Ist mit *-nb* eine Anzahl angegeben, die kleiner ist als die Anzahl der in dem Bereich vorhandenen ADM-Traps, so wird bis zur Endezeit die gewünschte Anzahl von ADM-Traps ausgegeben.

-rg=[[[yyyy]mm]dd]hhmm**-**
Der Zeitbereich beginnt mit der Startzeit und ist am Ende begrenzt durch den aktuellsten ADM-Trap-Eintrag.

Ist mit *-nb* eine Anzahl angegeben, die kleiner ist als die Anzahl der in dem Bereich vorhandenen ADM-Traps, so werden die aktuellsten ADM-Traps ausgegeben.

-rg=-[[[yyyy]mm]dd]hhmm
Der Zeitbereich endet mit der angegebenen Zeit.

Ist mit *-nb* eine Anzahl angegeben, die kleiner ist als die Anzahl der in dem Bereich vorhandenen ADM-Traps, so wird bis zur Endezeit die gewünschte Anzahl von ADM-Traps ausgegeben.

-rg=[**#**1..99999999999999999][**-**[**#**1..99999999999999999]]
Hier geben Sie mit *-rg* wahlweise den Beginn und/oder das Ende eines Trap-Id-Bereichs an.

#1..99999999999999999
Die Wahl einer Trap-Id wird gekennzeichnet durch das führende #-Zeichen. openFT gibt die ADM-Traps aus, die innerhalb des angegebenen Bereichs liegen.

-rg=#1..99999999999999999
Es wird genau der ADM-Trap mit dieser Trap-Id ausgegeben. Existiert diese nicht (Nummerierungslücken sind möglich), dann wird folgende Meldung ausgegeben: `Keine ADM-Traps zum Auswahlkriterium gefunden.`

-rg=#1..99999999999999999**-#**1..99999999999999999
Der Bereich beginnt mit dem ADM-Trap der ersten angegebenen Trap-Id und endet mit der zweiten angegebenen Trap-Id.

Ist mit *-nb* eine Anzahl angegeben, die kleiner ist als die Anzahl der in dem Bereich vorhandenen ADM-Traps, so wird bis zur "Ende"-Id die gewünschte Anzahl von Sätzen ausgegeben.

-rg=#1..99999999999999999**-**
Der Bereich beginnt mit dem ADM-Trap mit der angegebenen Trap-Id und ist am Ende begrenzt durch den aktuellsten ADM-Trap.

Ist mit *-nb* eine Anzahl angegeben, die kleiner ist als die Anzahl der in dem Bereich vorhandenen ADM-Traps, so werden die aktuellsten ADM-Traps ausgegeben.

-rg=-#1..99999999999999999
Der Bereich endet mit dem ADM-Trap mit der angegebenen Trap-Id.

Ist mit *-nb* eine Anzahl angegeben, die kleiner ist als die Anzahl der in dem Bereich vorhandenen ADM-Traps, so wird bis zur "Ende"-Id die gewünschte Anzahl von ADM-Traps ausgegeben.

-rg nicht angegeben
Der Trap-Id-Bereich bzw. der Zeitbereich ist nicht Auswahlkriterium, d.h. die Ausgabe beginnt beim aktuellen (letzten) ADM-Trap.

-src=Trap-Source
Mit *-src* legen Sie fest, dass nur ADM-Traps angezeigt werden, welche von einem bestimmten Partner stammen. Sie können den Namen aus der Partnerliste oder die Partneradresse angeben.

-src nicht angegeben
Der Name des Partners ist nicht Auswahlkriterium.

-tt=[**fts**][**,**][**pts**][**,**][**ptu**][**,**][**rqc**][**,**][**rqf**][**,**][**rqs**]

Mit *-tt* legen Sie fest, welcher Typ von ADM-Traps ausgegeben werden soll. Sie können mehrere Werte, durch Komma getrennt, angeben:

fts Es werden alle ADM-Traps ausgegeben, die das Starten des asynchronen openFT (*FT-START) oder das Beenden des asynchronen openFT (*FT-STOP) anzeigen.

pts Es werden alle ADM-Traps ausgegeben, die den Statuswechsel eines Partnersystems (*PART-STATE) anzeigen.

ptu Es werden alle ADM-Traps ausgegeben, die anzeigen, dass ein Partnersystem möglicherweise nicht erreichbar sein könnte (*PART-UNREA).

rqs Es werden alle ADM-Traps ausgegeben, die das Erreichen eines Füllungsgrades des Auftragsbuchs von mindestens 85% (*RQ-LIM-HIGH) oder das Unterschreiten von 80% (*RQ-LIM-LOW) anzeigen.

rqf Es werden alle ADM-Traps ausgegeben, die das Fehlschlagen einer Übertragung anzeigen (*TRANS-FAIL).

rqc Es werden alle ADM-Traps ausgegeben, die eine erfolgreiche Datenübertragung anzeigen (*TRANS-SUCC).

-tt nicht angegeben

Der Typ von ADM-Traps ist nicht Auswahlkriterium.

-nb=1.. 9999999 | **@a**

Mit *-nb* geben Sie an, wie viele ADM-Traps ausgegeben werden sollen.

@a für *zahl*

Es werden alle ADM-Traps ausgegeben, die den angegebenen Selektionskriterien entsprechen.

-nb nicht angegeben

Ist *-nb* nicht angegeben, dann hängt die Ausgabe davon ab, ob gleichzeitig *-rg* angegeben ist oder nicht:

– Ist *-rg* angegeben, dann werden alle ADM-Traps ausgegeben, die den angegebenen Selektionskriterien entsprechen (entspricht *-nb=@a*).

– Ist *-rg* nicht angegeben, dann wird maximal ein ADM-Trap ausgegeben (entspricht *-nb=1*).

-l Mit *-l* geben Sie an, dass die ADM-Traps in der ausführlichen Form ausgegeben werden sollen.

-csv Mit *-csv* geben Sie an, dass die ADM-Traps im CSV-Format ausgegeben werden sollen. Die Werte der Ausgabe werden durch Strichpunkte getrennt ausgegeben.

-csv darf nicht gleichzeitig mit *-l* angegeben werden.

weder *-l* noch *-csv* angegeben
Die ADM-Traps werden im Standardformat in Kurzform ausgegeben.

6.33.1 Beschreibung der Ausgabe der ADM-Traps

Bei der Ausgabe der ADM-Traps mit dem Kommando *ftshwatp* können Sie wählen zwischen der kurzen und übersichtlichen Ausgabe, der langen und ausführlichen Ausgabe und, für die Weiterverarbeitung mit externen Programmen, der Ausgabe im CSV-Format.

Die ADM-Traps werden durch Trap-Ids identifiziert. Diese IDs werden aufsteigend vergeben, die Nummerierung kann jedoch aus technischen Gründen Lücken aufweisen. Die Reihenfolge der Einträge in der ADM-Trap-Log-Datei entspricht nicht unbedingt der zeitlichen Reihenfolge, in der die ADM-Traps auf den jeweiligen Systemen aufgetreten sind. Eine Suche nach Sätzen mit bestimmten Selektionskriterien kann daher sehr lange dauern, da im Prinzip alle Einträge eingelesen werden müssen.

6.33.1.1 Kurze Ausgabeform eines ADM-Traps

In diesem Beispiel werden die letzten drei ADM-Traps ausgegeben:

```
$ftshwatp -nb=3
        TRAP-ID TYPE          DATE        TIME      SOURCE
             52 RQ-LIM-HIGH   2012-07-02  10:36:56  fileserv
             51 TRANS-FAIL    2012-07-02  10:36:48  FTSERV01
             50 PART-UNREA    2012-07-02  10:32:01  FTSERV01
```

Erläuterung

TRAP-ID
Nummer des ADM-Traps in der ADM-Trap-Log-Datei, bis zu 18-stellig.

TYPE Trap Typ.

Mögliche Werte:

FT-START
Starten des asynchronen openFT

FT-STOP
Beenden des asynchronen openFT

PART-STATE
Statuswechsel eines Partnersystems

PART-UNREA
: Partnersystem möglicherweise nicht erreichbar

RQ-LIM-HIGH
: Füllungsgrad des Auftragsbuchs hat mindestens 85% erreicht

RQ-LIM-LOW
: Füllungsgrad des Auftragsbuchs hat 80% unterschritten

TRANS-SUCC
: Erfolgreiche Dateiübertragung

TRANS-FAIL
: Fehlgeschlagene Dateiübertragung

DATE Datum, an dem der Trap aufgetreten ist.

TIME Uhrzeit, zu der der Trap aufgetreten ist.

SOURCE
: Name des Partners, auf dem der Trap aufgetreten ist.

6.33.1.2 Lange Ausgabeform eines ADM-Traps

Beispiel für die Ausgabe der letzten beiden ADM-Traps im Langformat:

```
$ftshwatp -nb=2 -l
TRAP-ID      = 52 TYPE = RQ-LIM-HIGH  TIME = 2012-07-02 10:36:56
   SOURCE    = FTSERV01
   PARTNER   =                        PTN-STATE =
   TRANS-ID  =    RC   =              INITIATOR =
   FILENAME  =
   ERROR-MSG =
TRAP-ID      = 51 TYPE = TRANS-FAIL   TIME = 2012-07-02 10:36:48
   SOURCE    = admin001
   PARTNER   = PARTLINU               PTN-STATE =
   TRANS-ID  = 11 RC   = 2169         INITIATOR = user
   FILENAME  = order.txt
   ERROR-MSG = Auftrag 11. Fernes System: Zugangsberechtigung ungültig
```

Erläuterung

TRAP-ID
: Nummer des ADM-Traps in der ADM-Trap-Log-Datei, bis zu 18-stellig.

TYPE Trap Typ.

Die möglichen Werte sind dieselben wie bei der Kurzausgabe, siehe Beschreibung auf Seite 295.

TIME Datum und Uhrzeit, zu der der Trap aufgetreten ist.

SOURCE
: Name des Partners, auf dem der Trap aufgetreten ist.

TRANS-ID
: Transfer-Id des Trap auslösenden Transfers.

RC Reason-Code des Trap auslösenden Transfers.

INITIATOR
: Benutzerkennung bzw. Ort des Trap auslösenden Transfers.

PARTNER
: Partnername des Trap auslösenden Transfers oder Partners.

PTN-STATE
: Partnerzustand des Trap auslösenden Partners.

FILENAME
: Dateiname des Trap auslösenden Transfers.

ERROR-MSG
: Meldungstext des Trap auslösenden Transfers.

6.34 ftshwc - Fernadministrierbare openFT-Instanzen anzeigen

Mit *ftshwc* können Sie sich die openFT-Instanzen ausgeben lassen, die Sie als Fernadministrator administrieren dürfen.

ftshwc können Sie sowohl lokal am Fernadministrations-Server als auch über *ftadm* per Fernadministration eingeben (siehe Seite 178):

– Wenn Sie *ftshwc* lokal am Fernadministrations-Server eingeben, dann werden die openFT-Instanzen anhand der Benutzerkennung ermittelt, unter der Sie das Kommando *ftshwc* absetzen.

– Wenn Sie *ftshwc* per Fernadministrations-Auftrag über *ftadm* eingeben, dann müssen Sie eine FTAC-Zugangsberechtigung angeben. Die openFT-Instanzen werden anhand des Berechtigungsprofils ermittelt, das zu dieser Zugangsberechtigung gehört.

ftshwc durchsucht die Konfigurationsdaten auf dem Fernadministrations-Server nach openFT-Instanzen, die mit der Benutzerkennung bzw. über dieses Berechtigungsprofil fernadministriert werden dürfen, und gibt diese aus.

Wenn Sie keine Instanzen fernadministrieren dürfen, dann erhalten Sie die Meldung:

```
ftshwc: Keine Instanzen gefunden
```

Format

ftshwc -h |
[-rt=i | -rt=gi | -rt=ig]
[-csv]

Beschreibung

-h gibt die Kommandosyntax am Bildschirm aus. Weitere Angaben nach *-h* werden ignoriert.

-rt=i | -rt=gi | -rt=ig
Mit *-rt* legen Sie fest, welche Informationen angezeigt werden sollen.
Sie können angeben: *i*, *gi* (Standardwert), *ig*

i Es werden nur Informationen über Instanzen angezeigt.

gi, ig Es werden Informationen über Gruppen und Instanzen angezeigt.

-csv Mit *-csv* geben Sie an, dass die Daten im CSV-Format ausgegeben werden sollen.

-csv nicht angegeben
Die Ausgabe erfolgt im Standardformat.

6.34.1 Ausgabeformat von ftshwc

Beispiel für eine Ausgabe im Standardformat:

```
ftshwc

TYPE    = *GROUP        ACCESS =                  MODE =
   NAME = Hamburg
   DESC = Rechenzentrum Nord in Hamburg Wandsbek
TYPE    = *GROUP        ACCESS =                  MODE =
   NAME = Hamburg/HH1
   DESC = QA Rechenzentrum
TYPE    = *INSTANCE     ACCESS = FT+FTOP+FTAC     MODE = FTADM
   NAME = Hamburg/HH1/HHWSRV01
   DESC = Solaris 10
TYPE    = *INSTANCE     ACCESS = FT+FTOP+FTAC     MODE = FTADM
   NAME = Hamburg/HH1/HHWSRV02
   DESC = HP-11
TYPE    = *INSTANCE     ACCESS = FT+FTOP          MODE = LEGACY
   NAME = Hamburg/HH1/HHWSRV11
   DESC = Solaris 9
TYPE    = *GROUP        ACCESS =                  MODE =
   NAME = Hamburg/HH2
   DESC = Personalabteilung
TYPE    = *INSTANCE     ACCESS = FTOP             MODE = FTADM
   NAME = Hamburg/HH2/HHWSRV99
   DESC = Mainframe-System (BS2000/OSD)
```

Erläuterung

TYPE gibt an, ob es sich um eine Gruppe oder um eine openFT-Instanz handelt:

*GROUP
: Gruppe

*INSTANCE
: openFT-Instanz

ACCESS
: Wird nur bei *TYPE=*INSTANCE* versorgt und gibt an, welche Fernadministrations-Rechte der Fernadministrator für diese Instanz hat:

  FTOP Nur lesende FT-Zugriffe (FT-Operator).

  FT Lesende und modifizierende FT-Zugriffe, entspricht den Rechten eines FT-Verwalters.

  FTAC Lesende und modifizierende FTAC-Zugriffe, entspricht den Rechten eines FTAC-Verwalters.

MODE

Wird nur bei *TYPE=*INSTANCE* versorgt und gibt an, über welches Protokoll diese Instanz administriert wird:

FTADM Die Instanz wird über das FTADM-Protokoll administriert.

LEGACY

Die Instanz wird über *ftexec* administriert.

NAME

Pfadname der Gruppe bzw. Pfadname der openFT-Instanz.

Bei Fernadministrations-Aufträgen müssen Sie den Namen der openFT-Instanz so angeben wie er hier angezeigt wird, d.h. als kompletten Pfadnamen.

DESC

Beschreibung der Gruppe oder openFT-Instanz.

6.35 ftshwd - Diagnoseinformation ausgeben

Mit dem Kommando *ftshwd* können Sie sich Diagnoseinformation ausgeben lassen.

Die Diagnoseunterlagen dienen dem Kundendienst zur Fehleranalyse.

Format

ftshwd

Beschreibung

Das Kommando besitzt einige Schalter, die jedoch nur für den Kundendienst von Bedeutung sind.

Beispiel

```
ftshwd

DATE     TIME    SSID  COMPONENT    LOCATION-ID       INFO
20120617 100921  FT    251/yfysequ  46/SwinsLwrite    ffffffff
20120617 100923  FTAC  39/yfslogg   1/WriteErr        ffffffff
```

Erläuterung der Ausgabe:

DATE
: Datum wann der Fehler aufgetreten ist

TIME
: Uhrzeit wann der Fehler aufgetreten ist

SSID
: Subsystem-Identifikation. Name des Subsystems, das den Diagnosesatz erzeugt hat.

COMPONENT
: Modulnummer/-name

LOCATION-ID
: Codestelle, an der der Fehler aufgetreten ist.

INFO
: Fehlercode

6.36 ftshwe - Berechtigungsprofile und -sätze aus Datei anzeigen

ftshwe steht für "show environment", also Anzeigen von Berechtigungsprofilen und -sätzen aus einer Datei. Mit *ftshwe* können Sie als FTAC-Verwalter sich Berechtigungsprofile und -sätze anzeigen lassen, die mit dem Kommando *ftexpe* gesichert wurden.

Format

ftshwe -h |
<Dateiname 1..512>
[-u=<Benutzerkennung 1..32>[,...,<Benutzerkennung(100) 1..32>]]
[-pr=<Profilname 1..8>[,...,<Profilname(100) 1..8>] | -pr=@n]
[-as=y | -as=n]
[-l][-csv]

Beschreibung

-h gibt die Kommandosyntax am Bildschirm aus. Weitere Angaben nach *-h* werden ignoriert.

Dateiname
Mit *Dateiname* geben Sie den Namen der Sicherungsdatei an, aus der Sie sich die Berechtigungsprofile und -sätze anzeigen lassen wollen.

-u=kennung1[**,**kennung2][**,**kennung3]...
Mit *-u* geben Sie die Benutzerkennungen an, deren Berechtigungsprofile und -sätze Sie sich anzeigen lassen wollen. Sie können maximal 100 Benutzerkennungen gleichzeitig angeben.

Falls zu der angegebenen Kennung kein Berechtigungssatz vorliegt, wird nur der Standardberechtigungssatz ausgegeben.

Geben Sie für *kennung1* eine nicht existierende Kennung an, so erhalten Sie für *kennung1* den aktuellen Standardberechtigungssatz ausgegeben.

-u nicht angegeben
Es werden alle Berechtigungsprofile und -sätze angezeigt.

-pr=Profilname1[**,**Profilname2][**,**Profilname3]... | **-pr=@n**
Mit *-pr* geben Sie die Berechtigungsprofile an, die Sie sich anzeigen lassen wollen (maximal 100).

@n für *Profilname*
Es werden keine Berechtigungsprofile ausgegeben.

-pr nicht angegeben
: Es werden alle Berechtigungsprofile angezeigt, die zu den beim Parameter *-u* angegebenen Kennungen gesichert wurden.

-as=y | **-as=n**
: Mit *-as* geben Sie an, ob Sie sich Berechtigungssätze anzeigen lassen wollen oder nicht. Mögliche Werte:

  y (Standardwert)
  : Es werden alle Berechtigungssätze angezeigt, die zu den beim Parameter *-u* angegebenen Kennungen existieren.

  n Es werden keine Berechtigungssätze angezeigt.

-l Mit dieser Option geben Sie an, dass Sie den Inhalt der ausgewählten Berechtigungsprofile sehen wollen.

-l nicht angegeben
: Sie erhalten nur die Namen der Berechtigungsprofile ausgegeben. Zusätzlich erhalten Sie durch entsprechende Markierungen Information darüber, ob ein Berechtigungsprofil privilegiert (∗) und ob es gesperrt (!) ist.

-csv Mit *-csv* geben Sie an, dass die FT-Berechtigungsprofile und -sätze im CSV-Format ausgegeben werden sollen. Die Werte der Ausgabe werden durch Strichpunkte getrennt ausgegeben. Die Angabe von *-csv* bewirkt stets die Ausgabe in der ausführlichen Form (analog zu *-l*), gleichgültig, ob *-l* gleichzeitig angegeben wurde oder nicht.

Eine detaillierte Beschreibung dazu entnehmen Sie bitte Abschnitt „ftshwp“ auf Seite 420 und Abschnitt „ftshwa“ auf Seite 401.

-csv nicht angegeben
: Sie bekommen die FT-Berechtigungsprofile und -sätze im Standardformat ausgegeben.

6.37 ftshwk - Eigenschaften von RSA-Schlüsseln anzeigen

Mit dem Kommando *ftshwk* können Sie die Eigenschaften von RSA-Schlüsseln ausgeben. Sie können sich RSA-Schlüssel der eigenen Instanz und RSA-Schlüssel von Partnern anzeigen lassen.

Format

ftshwk -h
[-own]
[-id=<Identifikation 1..64> | -id=@a]
[-pn=<Partner 1..200> | -pn=@a] |
[-exp=n | -exp=e | -exp=yyyymmdd | -exp=1..999]
[-csv]

Beschreibung

-h gibt die Kommandosyntax am Bildschirm aus. Weitere Angaben nach *-h* werden ignoriert.

-own zeigt die Schlüssel der eigenen Instanz an.

-own darf nicht zusammen mit *-pn* oder *-id* angegeben werden.

-id=Identifikation | **-id=@a**
Identifikation ist die Instanzidentifikation des Partners, dessen Schlüssel angezeigt wird.

-id darf nicht zusammen mit *-pn* und *-own* angegeben werden.

@a zeigt die installierten Schlüssel von allen Partnersystemen an.

-pn=Partner | **-pn=@a**
Partner ist der Name des Partnersystems in der Partnerliste oder die Adresse des Partnersystems, dessen Schlüssel angezeigt wird.

-pn darf nicht zusammen mit *-id* und *-own* angegeben werden.

Einzelheiten zur Adressangabe finden Sie in Abschnitt „Aufbau der Partneradressen“ auf Seite 68.

@a zeigt die installierten Schlüssel von allen Partnersystemen an.

weder *-id* noch *-pn* noch *-own* angegeben
zeigt sowohl die Schlüssel der eigenen Instanz als auch die installierten Schlüssel von allen Partnersystemen an.

-exp=n | **-exp=e** | **-exp=**yyyymmdd | **-exp=**1..999
wählt die Schlüssel nach ihrem Verfallsdatum aus.

n (no) Zeigt alle Partnerschlüssel an, die kein Verfallsdatum besitzen.

e (expired) Zeigt alle Partnerschlüssel an, die bereits abgelaufen sind.

yyyymmdd
zeigt alle Partnerschlüssel an, die spätestens am angegebenen Datum um 00:00 Uhr lokale Zeit ablaufen. 20130101 gibt z.B. alle Schlüssel aus, die bis zum 01.01.2013 um 00:00 Uhr ungültig werden.

1..999 Zeigt alle Partnerschlüssel an, die innerhalb der angegebenen Anzahl von Tagen ablaufen.

-exp nicht angegeben
Das Verfallsdatum ist kein Auswahlkriterium.

-csv Mit *-csv* geben Sie an, dass die Schlüsseleigenschaften im CSV-Format ausgegeben werden sollen. Die Werte der Ausgabe werden durch Strichpunkte getrennt ausgegeben.

-csv nicht angegeben
Sie bekommen die Schlüsseleigenschaften im Standardformat ausgegeben.

Beispiel

Sie möchten sich die Eigenschaften aller Schlüssel ausgeben lassen:

```
ftshwk

CRE-DATE   EXP-DATE   KEY-LEN KEY-REF AUTHL IDENTIFICATION
2011-12-31            768     5       2
2011-12-31            1024    5       2
2011-12-31            2048    5       2
2012-01-31            1024    6       2
2012-02-29            2048    7       2
2011-03-28 2012-12-24 2048    7       2     MYOWNID.DOMAIN.NET
2011-07-12 EXPIRED    768     12      2     PC17QD.DOMAIN.NET
2011-05-14            1024    1036    1     PC27ABC.DOMAIN.NET
```

Erläuterung:

CRE-DATE
: Datum, an dem der Schlüssel erzeugt wurde.

EXP-DATE
: Datum, an dem der Schlüssel abläuft, d.h. 00:00 Uhr des angegebenen Tages. EXPIRED bedeutet, dass der Schlüssel bereits abgelaufen ist.

  leer bedeutet kein Ablaufdatum.

KEY-LEN
: Schlüssellänge in Bit: 768, 1024 oder 2048

KEY-REF
: Schlüsselreferenz

AUTHL Authentifizierungsstufe: 1 oder 2

IDENTIFICATION
: Instanzidentifikation des Partners. Bei Schlüsseln der eigenen Instanz bleibt das Feld leer.

6.38 ftshwl - Logging-Sätze und Offline-Logging-Dateien anzeigen

Mit *ftshwl* informieren Sie sich über alle openFT-Aufträge, die openFT bislang protokolliert hat. Außerdem können Sie sich die Namen der aktuellen Logging-Datei sowie der Offline-Logging-Dateien ausgeben lassen.

Als FT-, FTAC- oder ADM-Verwalter können Sie sich Logging-Sätze aller Kennungen anschauen. Die Logging-Sätze werden in der Datei *syslog.Lyymmdd.Lhhmmss* abgelegt, die sich im Verzeichnis *log* der jeweiligen openFT-Instanz befindet, siehe „Instanzenverzeichnis“ auf Seite 26. *yymmdd* ist das Datum (Jahr, Monat, Tag) und *hhmmss* ist die Uhrzeit Stunde, Minute, Sekunde für GMT), zu der die Datei angelegt wurde. Bei der Standardinstanz lautet der Pfadname */var/openFT/std/log/syslog.Lyymmdd.Lhhmmss* .

Details zu neu erzeugten Instanzen siehe Kommando *ftcrei* auf Seite 190.

Die Logging-Sätze sind als FT-, FTAC- und ADM-Logging-Sätze entsprechend gekennzeichnet, so dass Sie der Ausgabe entnehmen können, um welche Art von Logging-Satz es sich handelt.

Zu jedem Auftrag gibt es einen FTAC-Logging-Satz, in dem Sie das Ergebnis der Zugriffsprüfung von FTAC finden. Ob dieser Auftrag dann auch tatsächlich von openFT ausgeführt werden konnte, protokolliert openFT bei Übertragungsaufträgen in FT-Logging-Sätzen und bei Fernadministrations-Aufträgen in ADM-Logging-Sätzen.

Ohne weitere Angaben gibt openFT immer den aktuellsten Logging-Satz aus. Bei entsprechender Anforderung gibt openFT alle Logging-Sätze bis zu dem im Kommando spezifizierten Zeitpunkt aus, den aktuellsten zuerst, danach die anderen in umgekehrter chronologischer Reihenfolge.

Mit den Polling-Optionen können Sie erreichen, dass die Ausgabe von neuen Logging-Sätzen in regelmäßigen Abständen wiederholt wird.

Sie können zwischen drei Ausgabeformen wählen, der Kurzform, der ausführlichen Form der Ausgabe und dem CSV-Ausgabeformat (**C**haracter **S**eparated **V**alue).

Die Ausgabe erfolgt auf der Standardausgabe.

Format

```
ftshwl  -h |
        [ <Benutzerkennung 1..32> | @a ]
        [ -lf=<Dateiname 1..512> | -tlf=yyyymmdd[hh[mm[ss]]] ]
        [ -plf=<0..3> ]
        [ -rg=[[[[yyyy]mm]dd]hhmm|#1..999999999999|0..999|:0..999][-
              [[[[yyyy]mm]dd]hhmm|#1..999999999999|0..999|:0..999]] ]
        [ -rt=[t][c][a] ]
        [ -ff=[t][m][r][d][a][C][D][M][l][f] ]
        [ -ini=l | -ini=r | -ini=lr | -ini=rl ]
        [ -pn=<Partner 1..200> ]
        [ -fn=<Dateiname 1..512> ]
        [ -rc=0..ffff | -rc=@f]
        [ -tid=1..2147483647 ]
        [ -gid=<globale Auftrags-Id 1..4294967295> ]
        [ -adm=<Administrator-Id 1..32> ]
        [ -ri=<Routing-Info 1..200> ]
        [ -llf ]
        [ -nb=1..99999999 | -nb=@a ]
        [ -po=<Polling Intervall 1..600>
              [ -pnr=<Polling Anzahl 1..3600> ] ]
        [ -l ][ -csv ]
```

Beschreibung

-h gibt die Kommandosyntax am Bildschirm aus. Weitere Angaben nach *-h* werden ignoriert.

Benutzerkennung | **@a**
: Gibt die Benutzerkennung(en) an, deren Logging-Sätze ausgegeben werden sollen. Als Verwalter können Sie hier eine beliebige Kennung angeben.

  @a für *Benutzerkennung*
  : Als FT-, FTAC- oder ADM-Verwalter erhalten Sie die Logging-Sätze aller Benutzerkennungen.

Benutzerkennung nicht angegeben
: Es werden nur Logging-Sätze der Benutzerkennung ausgegeben, unter der das Kommando eingegeben wurde.

-lf=Dateiname | **-tlf=**yyyymmdd[hh[mm[ss]]]
: wählt die Logging-Datei(en) aus, deren Logging-Sätze oder Namen ausgegeben werden sollen. Damit können Sie auch Offline-Logging-Sätze ansehen.

  -lf=Dateiname
  : Die Logging-Datei wird über ihren Dateinamen ausgewählt. Sie müssen den relativen oder absoluten Pfadnamen angeben. Gibt es keine Logging-Datei mit dem angegebenen Dateinamen, dann wird eine Fehlermeldung ausgegeben.

  -tlf=yyyymmdd[hh[mm[ss]]]
  : Die Logging-Datei wird über ihren Erstellungszeitpunkt (Ortszeit!) ausgewählt. Es wird die Logging-Datei ausgewählt, die an oder vor dem angegebenen Zeitpunkt erstellt wurde. Gibt es mehrere Logging-Dateien, die zum angegebenen Zeitpunkt passen, dann wird die nächstältere Logging-Datei genommen.

    Sie müssen mindestens das Datum angeben, 8-stellig als Jahr, Monat und Tag. Das Jahr muss größer oder gleich 2000 sein.
    Die Uhrzeit (hhmmss) können Sie teilweise oder ganz weglassen, fehlende Komponenten werden durch 00 ergänzt, siehe auch Beispiel 7.

weder *-lf* noch *-tlf* angegeben
: Es wird die aktuelle Logging-Datei verwendet.

-plf=anzahl
: gibt die Anzahl der vorausgehenden Offline-Logging-Dateien an (0 bis 3), die zusätzlich zur aktuellen bzw. zu der mit *-lf* oder *-tlf* spezifizierten Datei ausgewählt werden sollen.

-plf nicht angegeben
: wählt nur die aktuelle oder die mit *-lf* oder *-tlf* spezifizierte Logging-Datei aus.

Wenn Sie die Optionen *-plf* und *-lf* bzw. *-tlf* weglassen, dann entspricht dies dem Verhalten bis openFT V11.0.

-rg=[[[[yyyy]mm]dd]hhmm]**-**[[[[yyyy]mm]dd]hhmm]
: Hier geben Sie mit *-rg* wahlweise den Beginn und/oder das Ende eines Logging-Zeitbereichs an.

  [[[yyyy]mm]dd]hhmm
  : 4-stellig wird dies als Uhrzeit in Stunden und Minuten, 6-stellig als Tag (Datum) und Uhrzeit in Stunden und Minuten, 8-stellig als Monat, Tag und Uhrzeit in Stunden und Minuten, 12-stellig als Jahr, Monat, Tag und Uhrzeit in Stunden und Minuten interpretiert. Der größtmögliche Wert für das anzugebende Datum ist 20380119 (19. Januar 2038).

openFT gibt dann die Logging-Sätze aus, die innerhalb der angegebenen Grenzen liegen. Als Beginn wird der ältere Zeitpunkt betrachtet, als Ende folglich der jüngere Zeitpunkt.
Wenn optionale Daten (*[[[yyyy]mm]dd]*) weggelassen werden, werden sie automatisch durch aktuelle Werte ersetzt.

Wenn Sie die Grenze hinter dem Minuszeichen weglassen, so bedeutet dies die aktuelle Zeit. Wenn Sie die Grenze vor dem Minuszeichen weglassen, so bedeutet dies den Zeitpunkt des ersten geschriebenen Logging-Satzes.

-rg=- zeigt alles (gleichbedeutend mit *-nb=@a*)

-rg=[[[yyyy]mm]dd]hhmm
Bei Fehlen des Minus-Zeichens ist genau der Bereich der angegebenen Minute gemeint. Der größtmögliche Wert für das anzugebende Datum ist 20380119 (19. Januar 2038). Wenn optionale Daten (*[[[yyyy]mm]dd]*) weggelassen werden, dann werden sie automatisch durch aktuelle Werte ersetzt.

-rg=[**#**1..999999999999]**-**[**#**1..999999999999]
Hier geben Sie mit *-rg* den Beginn und/oder das Ende eines Logging-Id-Bereichs an.

#1..999999999999
Die Wahl einer Logging-Id wird gekennzeichnet durch das führende #-Zeichen. openFT gibt dann die Logging-Sätze aus, die innerhalb der angegebenen Grenzen liegen.

Ist eine Grenze fortgelassen, so bedeutet dies bei der Logging-Id hinter dem Minuszeichen die aktuelle ID und bei der Logging-Id vor dem Minuszeichen die ID des ersten geschriebenen Logging-Satzes.

-rg=#1..999999999999
Bei Fehlen des Minus-Zeichens beschränkt sich der Bereich genau auf die angegebene Logging-Id.

-rg=[0..999][**-**[0..999]]
Hier geben Sie mit *-rg* eine relative Zeitdistanz als Vielfaches von 24 Stunden - also die Anzahl von Tagen - an. Dabei ist zu beachten, dass die Zeitdistanz sekundengenau zur aktuellen Zeit berechnet wird. Sie haben folgende Möglichkeiten (*d1* und *d2* 1- bis 3-stellig):

- *-rg=d1-d2* gibt alle Logging-Sätze aus, die zwischen *d1* und *d2* Tage alt sind, unabhängig davon, ob *d1* größer oder kleiner ist als *d2*.
- *-rg=d1-* gibt alle Logging-Sätze aus, die höchstens *d1* Tage alt sind.
- *-rg=-d2* gibt alle Logging-Sätze aus, die mindestens *d2* Tage alt sind.

-rg=[**:**0..999][**-**[**:**0..999]]
Hier geben Sie mit *-rg* einen relativen Zeitbereich in Minuten an. Dabei haben Sie folgende Möglichkeiten (*m1* und *m2* 1- bis 3-stellig):

- *-rg=:m1-:m2* gibt alle Logging-Sätze aus, die zwischen *m1* und *m2* Minuten alt sind, unabhängig davon, ob *m1* größer oder kleiner ist als *m2*.
- *-rg=:m1* (oder *-rg=:m1-*) gibt alle Logging-Sätze aus, die höchstens *m1* Minuten alt sind.
- *-rg=-:m2* gibt alle Logging-Sätze aus, die mindestens *m2* Minuten alt sind.

-rg nicht angegeben
Der Bereich ist nicht Auswahlkriterium.

-rt=[**t**][**c**][**a**]
Mit *-rt* legen Sie fest, zu welchem Satztyp Sie sich Logging-Sätze anzeigen lassen wollen. Sie können *t*, *c*, *a* sowie alle Kombinationen dieser Werte angeben:

t Es werden die FT-Logging-Sätze angezeigt.

c Es werden die FTAC-Logging-Sätze angezeigt.

a Es werden die ADM-Logging-Sätze angezeigt.

-rt nicht angegeben
Der Satztyp ist nicht Auswahlkriterium.

-ff=[**t**][**m**][**r**][**d**][**a**][**C**][**D**][**M**][**l**][**f**]
Mit *-ff* legen Sie fest, zu welcher FT-Funktion Sie sich Logging-Sätze ausgeben lassen wollen. Sie können folgende Werte angeben: *t*, *m*, *r*, *d*, *a*, *C*, *D*, *M*, *l*, *f* oder eine beliebige Kombination der Buchstaben.
Die Angaben *m*, *r*, *d*, *a*, *C*, *D*, *M* und *l* sind nur für FTAC-Logging-Sätze sinnvoll. Die Angabe *f* ist nur für ADM-Logging-Sätze sinnvoll. *t* ist für alle Logging-Sätze sinnvoll.

t Es werden alle Logging-Sätze zur Funktion "Dateien übertragen" ausgegeben.

m Es werden alle Logging-Sätze zur Funktion "Dateiattribute ändern" ausgegeben.

r Es werden alle Logging-Sätze zur Funktion "Dateiverzeichnisse lesen" ausgegeben.

d Es werden alle Logging-Sätze zur Funktion "Dateien löschen" ausgegeben.

a Es werden alle Logging-Sätze zur Funktion "Dateiattribute lesen" ausgegeben.

C Es werden alle Logging-Sätze zur Funktion "Dateiverzeichnis erzeugen" ausgegeben.

D Es werden alle Logging-Sätze zur Funktion "Dateiverzeichnis löschen" ausgegeben.

M Es werden alle Logging-Sätze zur Funktion "Dateiverzeichnis modifizieren" ausgegeben.

I Mit *l* werden alle Logging-Sätze zur Funktion "Inbound FTP-Zugang" ausgegeben. Diese Logging-Sätze werden geschrieben, wenn beim Inbound-FTP-Zugriff falsche Berechtigungsdaten (FTAC-Zugangsberechtigung oder Kennung/Passwort) angegeben wurden.

f Es werden auf dem Fernadministrations-Server alle ADM-Logging-Sätze der Funktion "Routing" ausgegeben. Die Ausgabe kann noch durch die Optionen *-adm* und *-ri* eingeschränkt werden.

-ff nicht angegeben
Die FT-Funktion ist nicht Auswahlkriterium.

-ini=l | **-ini=r** | **-ini=lr** | **-ini=rl**
Mit *-ini* legen Sie fest, zu welchem Initiator Sie sich Logging-Sätze ausgeben lassen wollen. Sie können angeben: *l*, *r*, *lr*, *rl*.

l (local) Nur die Logging-Sätze werden ausgegeben, die zu lokal gestellten openFT-Aufträgen gehören.

r (remote) Nur die Logging-Sätze werden ausgegeben, die zu fern gestellten openFT-Aufträgen gehören.

lr, rl Die Logging-Sätze werden ausgegeben, die zu lokal und fern gestellten openFT-Aufträgen gehören.

-ini nicht angegeben
Der Initiator ist nicht Auswahlkriterium.

-pn=Partner
Mit *-pn* legen Sie fest, zu welchem Partnersystem Sie sich Logging-Sätze ausgeben lassen wollen. Partner ist der Name des Partners in der Partnerliste oder die Adresse des Partnersystems. Einzelheiten zur Adressangabe finden Sie in Abschnitt „Aufbau der Partneradressen“ auf Seite 68.

Sie können beim Partnernamen auch die Wildcard-Symbole '*' (Stern) und '?' (Fragezeichen) angeben. * steht für eine beliebige Zeichenfolge, ? steht für ein beliebiges einzelnes Zeichen.

-pn nicht angegeben
Das Partnersystem ist nicht Auswahlkriterium.

-fn=Dateiname
: Mit *-fn* legen Sie fest, zu welcher Datei Sie sich Logging-Sätze ausgeben lassen wollen. Beim Dateinamen können Sie auch die Wildcard-Symbole "*" (Stern, d.h. beliebige Zeichenfolge) und "?" (Fragezeichen, d.h. einzelnes Zeichen) angeben.

-fn nicht angegeben
: Der Dateiname ist nicht Auswahlkriterium.

-rc=0..ffff | **@f**
: Mit *-rc* legen Sie fest, zu welchem Reason-Code Sie sich Logging-Sätze ausgeben lassen wollen. Sie können angeben:

  0 .. ffff
  : Es werden Logging-Sätze mit dem angegebenen Reason-Code ausgegeben.

  @f Es werden Logging-Sätze ausgegeben, deren Reason-Code ungleich 0000 ist. Sie erhalten somit Logging-Sätze zu Aufträgen, die mit Fehlermeldung beendet wurden.

-rc nicht angegeben
: Der Reason-Code ist nicht Auswahlkriterium.

-tid=Auftrags-Id
: Mit *-tid* geben Sie die Auftragsnummer an, zu der Sie sich die Logging-Sätze ausgeben lassen wollen.

-tid nicht angegeben
: Die Auftragsnummer ist nicht Auswahlkriterium.

-gid=globale Auftrags-Id
: Mit *-gid* geben Sie die globale Auftrags-Identifikation an, zu der Sie sich die Logging-Sätze anzeigen lassen wollen. Die globale Auftrags-Identifikation ist nur für Inbound-Aufträge von openFT- und FTAM-Partnern relevant. Sie wird vom Initiator des Auftrags vergeben (Transfer-Id) und an das lokale System übermittelt.

-gid= nicht angegeben
: Die globale Auftrags-Identifikation ist nicht Auswahlkriterium.

-adm=Administrator-Id
: Mit *-adm* geben Sie die Administrator-Id an, für die Sie sich ADM-Logging-Sätze ausgeben lassen wollen.

-adm nicht angegeben
: Die Administrator-Id ist nicht Auswahlkriterium.

-ri=Routing-Info
: Mit *-ri* geben Sie die Routing-Info an, für die Sie sich ADM-Logging-Sätze ausgeben lassen wollen.

-ri nicht angegeben
: Die Routing-Info ist nicht Auswahlkriterium.

-llf gibt nur die Namen von Logging-Dateien aus. *-llf* ist nur alleine oder in Kombination mit den Optionen *-lf*, *-tlf*, *-plf*, *-csv* oder *-h* erlaubt, bei allen anderen Kombinationen wird das Kommando abgelehnt.

-llf ohne *-lf*, *-plf* oder *-tlf* gibt die Namen aller Logging-Dateien aus (aktuelle Logging-Datei sowie alle Offline-Logging-Dateien (bis maximal 1024)). Wenn Sie zusätzlich *-lf*, *-plf* oder *-tlf* angeben, können Sie die Ausgabe einschränken, siehe auch Beispiel 6.

-llf nicht angegeben
: Es werden Logging-Sätze gemäß den angegebenen Auswahlkriterien angezeigt.

-nb=zahl | **@a**
: Mit *-nb* geben Sie an, wie viele Logging-Sätze Sie sich ausgeben lassen wollen.

  @a für *zahl*
  : Sie bekommen alle Logging-Sätze ausgegeben.

-nb nicht angegeben
: Bei gleichzeitiger Angabe des Schalters *-rg* wird für *-nb* der Wert *-nb=@a* ersetzt.

  Im Fall, dass *-rg* ebenfalls nicht angegeben ist, wird für *-nb* der Wert *-nb=1* ersetzt.

-po=Polling Intervall
: *Polling Intervall* ist das Wiederholungsintervall in Sekunden. Bei jeder Wiederholung werden alle neuen Logging-Sätze gemäß der angegebenen Auswahlkriterien gefiltert und die gefundenen Datensätze ausgegeben.

  Mit der gleichzeitigen Angabe von *-pnr* können Sie die Anzahl der Ausgaben begrenzen. Wenn Sie *-po* ohne *-pnr* angeben, wird die Ausgabe beliebig oft wiederholt.

  Eine über die Option *-po* angestoßene wiederholte Ausgabe (mit oder ohne *-pnr*) kann durch ein Unterbrechungssignal abgebrochen werden (z.B. STRG+C). Außerdem wird sie im Fehlerfall abgebrochen. Nach dem Stoppen des asynchronen Servers wird die Ausgabe nicht abgebrochen, sondern läuft weiter.

  -po darf nicht zusammen mit *-lf*, *-llf*, *-plf*, *-tlf*, *-tid*, *-gid*, *-nb* oder *-rg* angegeben werden.

  Mögliche Werte: 1 bis 600.

  Während des Pollings sollten keine Logging-Sätze gelöscht werden, da sonst Lücken in der Ausgabe entstehen können!

-po nicht angegeben
: Die Logging-Sätze werden sofort und nur einmal ausgegeben.

-pnr=Polling Anzahl
: Mit *-pnr* geben Sie die Anzahl der Wiederholungen an.
-pnr kann nur zusammen mit *-po* angegeben werden.

  Mögliche Werte: 1 bis 3600.

-pnr nicht angegeben
: Die Ausgabe wird beliebig oft wiederholt.

-l Mit *-l* geben Sie an, dass Sie sich die Logging-Sätze in der ausführlichen Form ausgeben lassen wollen.

-l nicht angegeben
: Sie bekommen die Logging-Sätze in der Kurzform ausgegeben, wenn nicht *-csv* angegeben wurde.

-csv Mit *-csv* geben Sie an, dass die Logging-Sätze im CSV-Format ausgegeben werden sollen. Die Werte der Ausgabe werden durch Strichpunkte getrennt ausgegeben. Die Angabe von *-csv* bewirkt stets die Ausgabe in der ausführlichen Form (analog zu *-l*), gleichgültig, ob *-l* gleichzeitig angegeben wurde oder nicht.

-csv nicht angegeben
: Sie bekommen die Logging-Sätze im Standardformat ausgegeben, d.h. ohne Angabe von *-l* in Kurzform und mit Angabe von *-l* in ausführlicher Form.

Beispiele

Die folgenden Beispiele geben jeweils die Logging-Sätze der eigenen Kennung aus. Wenn Sie als FT-, FTAC- oder ADM-Verwalter die Logging-Sätze aller Kennungen ausgeben möchten, müssen Sie zusätzlich *@a* angeben.

1. Es sollen alle Logging-Sätze ausgegeben werden, die älter sind als zwei Tage (48 Stunden):
   ```
   ftshwl -rg=-2
   ```
2. Es sollen alle Logging-Sätze ausgegeben werden, die älter als 15 Minuten, aber nicht älter als 30 Minuten sind:
   ```
   ftshwl -rg=:15-:30
   ```
3. Es sollen alle Logging-Sätze ausgegeben werden, die nicht älter als 30 Minuten sind:
   ```
   ftshwl -rg=:30
   ```
4. Es sollen alle Logging-Sätze ausgegeben werden, die älter als 30 Minuten sind:
   ```
   ftshwl -rg=-:30
   ```

5. Ausgabe der letzten 10 Logging-Sätze mit fehlgeschlagenen FTAC-Prüfungen (Reason-Code ungleich 0):
   ```
   ftshwl -rc=@f -rt=c -nb=10
   ```
6. Es sollen der Name der aktuellen Logging-Datei sowie die Namen der beiden vorhergehenden Offline-Logging-Dateien ausgegeben werden:
   ```
   ftshwl -llf -plf=2
   ```
7. Ausgabe von 100 Logging-Sätzen aus der Logging-Datei, die an oder vor dem 24.02.2012 00:00 Uhr erzeugt wurde:
   ```
   ftshwl -tlf=20120224 -nb=100
   ```

   Hinweis

   -tlf=20120224 wird ergänzt zu *-tlf=20120224000000*. Gibt es z.B. die drei Logging-Dateien mit Erstellungsdatum 20120224 13:30:00, 20120217 10:00:00 und 20120210 08:00:00, dann wird die Datei mit Datum 20120217 10:00:00 als nächstältere Datei genommen.

6.38.1 Beschreibung der Ausgabe der Logging-Sätze

Die Logging-Sätze können Sie sich mit dem openFT Explorer oder dem Kommando *ftshwl* ansehen. Dabei können Sie zwischen der kurzen und übersichtlichen Ausgabe, der langen und ausführlichen Ausgabe und, für die Weiterverarbeitung mit externen Programmen, der Ausgabe im CSV-Format wählen.

Die Logging-Sätze werden durch Logging-Ids identifiziert. Die Logging-Ids werden aufsteigend vergeben, die Nummerierung ist aus technischen Gründen nicht immer lückenlos.

6.38.1.1 Logging von Aufträgen mit Vor- / Nachverarbeitung

Aus Sicherheitsgründen werden nur die ersten 32 Zeichen (bzw. 42 Zeichen bei *ftexecsv* Vorverarbeitungen) eines Vor- oder Nachverarbeitungskommandos in den Logging-Satz übernommen. Durch entsprechende Anordnung der Aufrufparameter bzw. durch Einfügen von Leerzeichen kann Einfluss darauf genommen werden, welche Kommandoparameter im Logging nicht erscheinen sollen.

6.38.1.2 Kurze Ausgabeform eines FT- oder FTAC-Logging-Satzes

Beispiel: Die Option *-rt=tc* bewirkt, dass nur FT- und FTAC-Logging-Sätze ausgegeben werden.

```
$ftshwl -rt=tc -nb=12
TYP LOG-ID TIME     RC    PARTNER  INITIAT. PROFILE  USER-ADM FILENAME
2012-05-05
CA    8273 09:16:07 0000 >PARTLINU *REMOTE  pr1      user1    file.10
CA    8272 09:16:07 0000 >PARTLINU user1             user1
CD    8271 09:15:30 0000 <PARTLINU *REMOTE  pr1      user1    file.new
CD    8270 09:15:30 0000 <PARTLINU user1             user1
CM    8269 09:15:03 0000 <PARTLINU *REMOTE  pr1      user1    file.rem
CM    8268 09:15:03 0000 <PARTLINU user1             user1    file.new
CR    8267 09:14:14 0000 >PARTLINU *REMOTE  pr1      user1    .
CR    8266 09:14:14 0000 >PARTLINU user1             user1
T     8265 09:13:50 0000 >PARTLINU user1             user1    file.10
T     8264 09:13:50 0000 <PARTLINU *REMOTE           user1    file.rem
C     8263 09:13:49 0000 <PARTLINU *REMOTE  pr1      user1    file.rem
C     8262 09:13:49 0000 >PARTLINU user1             user1    file.10
```

Erläuterung

TYP besteht aus drei Spalten. Die erste Spalte gibt an, ob es sich um einen FT- oder FTAC-Logging-Satz handelt:

- T FT-Logging-Satz
- C FTAC-Logging-Satz

Die zweite und dritte Spalte kennzeichnen die Funktion:

- _ (leer): Datei übertragen
- A Dateiattribute lesen (nur im FTAC-Logging-Satz)
- D Datei löschen (nur im FTAC-Logging-Satz)
- C Datei anlegen (nur im FTAC-Logging-Satz, nur bei Aufträgen möglich, die im fernen Partnersystem gestellt wurden)
- M Dateiattribute modifizieren (nur im FTAC-Logging-Satz)
- R Dateiverzeichnis lesen (nur im FTAC-Logging-Satz)
- CD Dateiverzeichnis anlegen (nur im FTAC-Logging-Satz)
- DD Dateiverzeichnis löschen (nur im FTAC-Logging-Satz)
- MD Dateiverzeichnisattribute modifizieren (nur im FTAC-Logging-Satz)
- L Login: Fehlgeschlagener Inbound FTP-Zugang (nur im FTAC-Logging-Satz)

LOG-ID
Nummer des Logging-Satzes

TIME
gibt den Zeitpunkt an, wann der Logging-Satz geschrieben wurde.

RC Reason-Code. Er gibt an, ob ein Auftrag erfolgreich ausgeführt wurde (RC=0) oder warum er abgelehnt bzw. abgebrochen wurde. Weitere Information zum Reason-Code können Sie mit dem Kommando *fthelp* abfragen.

PARTNER
informiert über das beteiligte Partnersystem. Ausgegeben wird der Name in der Partnerliste oder die ggf. auf 8 Zeichen gekürzte Adresse des Partnersystems oder der Name, mit dem das Partnersystem im TNS eingetragen ist.

Vor dem Namen bzw. der Adresse des Partnersystems steht ein Kennzeichen, dem Sie die Richtung des Auftrags entnehmen können:

> Die Auftragsrichtung ist zu2m Partnersystem. Diese Richtung wird angegeben bei einem
>
> – Sendeauftrag
>
> – Auftrag zum Ansehen von Dateiattributen
>
> – Auftrag zum Ansehen von Dateiverzeichnissen

< Die Auftragsrichtung ist zum lokalen System. Diese Richtung wird angegeben bei einem

– Empfangsauftrag

– Auftrag zum Ändern von Dateiattributen
(Ändert ein FTAM-Partner die Zugriffsrechte einer lokalen Datei, so werden zwei Logging-Sätze geschrieben. Hierbei wird vor PARTNER keine Richtung angegeben.)

– Auftrag zum Löschen von Dateien

INITIAT.
Initiator des Auftrags, bei Initiative im fernen System: ∗REMOTE

PROFILE
Name des Profils, das für die Übertragung verwendet wurde (nur im FTAC-Logging-Satz).

USER-ADM
Benutzerkennung, auf die sich die Aufträge im lokalen System beziehen. Falls eine mehr als 8 Bytes lange Benutzerkennung angegeben war, werden die ersten sieben Zeichen gefolgt von einem ∗ ausgegeben.

FILENAME
lokaler Dateiname

6.38.1.3 Kurze Ausgabeform des ADM-Logging-Satzes

In den folgenden Beispielen bewirkt die Option *-rt=a*, dass nur ADM-Logging-Sätze ausgegeben werden.

1. ADM-Logging-Sätze auf einem Client ausgeben:

```
ftshwl ftadmin -rt=a -nb=5
TYP LOG-ID TIME     RC    PARTNER  INITIAT. PROFILE  USER-ADM FILENAME
2012-05-19
A       39 04:30:35 0000 <flexthom ftadmin           ftadmin
A       36 04:30:15 0000 <flexthom ftadmin           ftadmin
A       33 04:29:49 0000 <flexthom ftadmin           ftadmin
A       30 04:28:15 0000 <flexthom ftadmin           ftadmin
A       27 04:22:56 0000 <flexthom ftadmin           ftadmin
```

2. ADM-Logging-Satz auf der administrierten openFT-Instanz ausgeben:

```
ftshwl -rt=a
TYP LOG-ID TIME     RC    PARTNER  INITIAT. PROFILE  USER-ADM FILENAME
2012-05-19
A     2575 13:30:15 0000 >ftadm:/* *REMOTE  adminrem admin001
```

3. Routing-ADM-Logging-Satz auf dem Fernadministrations-Server ausgeben:

```
ftshwl -rt=a -ff=f
TYP LOG-ID TIME     RC    PARTNER  INITIAT. PROFILE  USER-ADM FILENAME
2012-05-19
AF     396 13:22:54 0000 >Testrech *REMOTE  adminacc admin002
```

Erläuterung

Bei ADM-Logging-Sätzen gibt es im Vergleich zu FT- oder FTAC-Logging-Sätzen folgende Besonderheiten:

– In der Spalte TYP wird für einen ADM-Logging-Satz der Wert *A* ausgegeben. Bei ADM-Logging-Sätzen mit Routing-Info auf dem Fernadministrations-Server (*ftshwl -ff=f*) wird zusätzlich in Spalte 2 der Wert *F* angezeigt.

– Die Spalte FILENAME bleibt bei ADM-Logging-Sätzen leer.

6.38.1.4 Lange Ausgabeform eines FT-Logging-Satzes

Die Logging-Sätze mit den Nummern 103 und 404 sollen im Langformat ausgegeben werden:

```
ftshwl @a -rg=#103 -l
LOGGING-ID  = 103       RC      = 2155        TIME     = 2012-05-23 10:53:22
   TRANS    = FROM      REC-TYPE= FT          FUNCTION = TRANSFER-FILE
   PROFILE  =           PCMD    = NONE        STARTTIME= 2012-05-23 10:53:20
   TRANS-ID = 65539     WRITE   = REPLACE     REQUESTED= 2012-05-23 10:53:20
   TRANSFER =         0 kB                    CCS-NAME = ISO88591
                                              CHG-DATE = SAME
   SEC-OPTS = ENCR+DICHK, RSA-2048 / AES-256
   INITIATOR= maier
   USER-ADM = maier
   PARTNER  = FTSERV01
   FILENAME = test01
   ERRINFO  = CreateFile(Attr.): Das System kann die angegebene Datei nicht
              finden

ftshwl @a -rg=#404 -l

LOGGING-ID  = 404       RC      = 0000        TIME     = 2012-07-06 13:37:17
   TRANS    = FROM      REC-TYPE= FT          FUNCTION = TRANSFER-FILE
   PROFILE  =           PCMD    = NONE        STARTTIME= 2012-07-06 13:37:16
   TRANS-ID = 262164    WRITE   = REPLACE     STORETIME= 2012-07-06 13:37:17
   TRANSFER =         5 kB                    CCS-NAME =
   SEC-OPTS = ENCR+DICHK+RAUTH, RSA-2048 / AES-128
   INITIATOR= *REMOTE                         GLOB-ID  = 67017
   USER-ADM = maier
   PARTNER  = mc122.othernet.local
   FILENAME = example
```

Erläuterung

LOGGING-ID
: Nummer des Logging-Satzes, maximal zwölfstellig.

TRANS
: Übertragungsrichtung

  TO
  : Die Auftragsrichtung ist zum Partnersystem. Diese Richtung wird angegeben bei einem

    – Sendeauftrag
    – Auftrag zum Ansehen von Dateiattributen
    – Auftrag zum Ansehen von Dateiverzeichnissen

FROM
: Die Auftragsrichtung ist zum lokalen System. Diese Richtung wird angegeben bei einem

  – Empfangsauftrag
  – Auftrag zum Ändern von Dateiattributen
  – Auftrag zum Löschen von Dateien

PROFILE
: Name des verwendeten Profils

TRANS-ID
: Auftragsnummer

TRANSFER
: Anzahl der übertragenen Bytes

SEC-OPTS
: Während der Übertragung verwendete Sicherheitsoptionen

  ENCR Verschlüsselung der Auftragsbeschreibung

  DICHK Datenintegritätsprüfung der Auftragsbeschreibung

  DENCR Verschlüsselung des übertragenen Dateiinhalts

  DDICHK Datenintegritätsprüfung des übertragenen Dateiinhalts

  LAUTH Authentifizierung des lokalen Systems im fernen System (Authentifizierungsstufe 1)

  LAUTH2 Authentifizierung des lokalen Systems im fernen System (Authentifizierungsstufe 2)

  RAUTH Authentifizierung des fernen Systems im lokalen System (Authentifizierungsstufe 1)

  RAUTH2 Authentifizierung des fernen Systems im lokalen System (Authentifizierungsstufe 2)

  RSA-nnn Länge des für die Verschlüsselung verwendeten RSA-Schlüssels

  AES-128 / AES-256 / DES
  : Verwendeter Verschlüsselungsalgorithmus

INITIATOR
: Initiator des Auftrags; bei Initiative im lokalen System: Benutzerkennung, bei Initiative im fernen System: ∗REMOTE

USER-ADM
: Benutzerkennung, auf die sich die Aufträge im lokalen System beziehen.

PARTNER
: informiert über das beteiligte Partnersystem. Ausgegeben wird der Name in der Partnerliste oder die Adresse des Partnersystems (siehe Seite 68) oder der Name, mit dem das Partnersystem im TNS eingetragen ist.
Bei fern gestellten Aufträgen kann auch *%strange*, gefolgt von einem Teil der Adresse des Partnersystems, ausgegeben werden, wenn das Partnersystem nicht im TNS eingetragen ist und als Transportsystem nicht TCP/IP-RFC1006 verwendet wurde.

FILENAME
: lokaler Dateiname

ERRINFO
: Zusatzinformation zur Fehlermeldung, wenn eine Übertragung fehlerhaft war.

RC
: Reason-Code. Er gibt an, ob ein Auftrag erfolgreich ausgeführt wurde (RC=0) oder warum er abgelehnt bzw. abgebrochen wurde. Weitere Informationen erhalten Sie mit dem *fthelp*-Kommando.

REC-TYPE
: gibt an, dass es sich um einen FT-Logging-Satz handelt.

PCMD
: gibt an, ob eine Folgeverarbeitung angegeben und gestartet wurde. Mögliche Werte:

  NONE
  : Es war keine Folgeverarbeitung angegeben.

  STARTED
  : Eine Folgeverarbeitung wurde gestartet (beinhaltet keine Information über den Erfolg der Folgeverarbeitung!).

  NOT-STARTED
  : Eine Folgeverarbeitung konnte nicht gestartet werden.

WRITE
: Schreibmodus. Das Feld ist nur im Outbound-Fall belegt, bei Inbound-Aufträgen enthält es Leerzeichen. Mögliche Werte:

  NEW die Datei wird neu angelegt. Gibt es schon eine Datei mit diesem Namen, wird die Übertragung abgebrochen.

  EXT eine existierende Datei wird erweitert, sonst wird sie neu angelegt.

  REPLACE
  : eine existierende Datei wird überschrieben. Wenn sie noch nicht existiert, wird sie neu angelegt.

TIME
: gibt den Zeitpunkt an, wann der Logging-Satz geschrieben wurde.

FUNCTION
: FT-Funktion

  TRANSFER-FILE
  : Datei übertragen

STARTTIME
: Zeitpunkt an dem die Übertragung gestartet wurde.

STORETIME
: bei Initiative im fernen System wird hier der Zeitpunkt des Eintrags in das Auftragsbuch angezeigt.

REQUESTED
: bei Initiative im lokalen System steht hier der Zeitpunkt der Auftragserteilung.

Abhängig vom Initiator des Auftrags (lokal oder fern) wird entweder STORETIME oder REQUESTED ausgegeben, niemals beides zusammen.

CCS-NAME
: Name des Zeichensatzes, der für die Codierung der lokalen Datei verwendet wird.

CHG-DATE
: gibt an, ob das Änderungsdatum der Sendedatei für die Empfangsdatei übernommen wird.

  SAME Das Änderungsdatum der Sendedatei wird übernommen.

GLOB-ID
: globale Auftrags-Identifikation, wird nur bei Inbound-Aufträgen von openFT- und FTAM-Partnern angezeigt (INITIATOR=REMOTE). Sie stimmt mit der Auftrags-Identifikation (=TRANSFER-ID) auf der Initiator-Seite überein.

6.38.1.5 Lange Ausgabeform eines FTAC-Logging-Satzes

Der Logging-Satz mit der Nummer 5172 soll im Langformat ausgegeben werden:

```
ftshwl @a -rg=#5172 -l
LOGGING-ID  = 5172      RC      = 0000        TIME     = 2012-04-03 09:38:06
   TRANS    = TO        REC-TYPE= FTAC        FUNCTION = TRANSFER-FILE
   PROFILE  = remadmin  PRIV    = NO
   INITIATOR= *REMOTE
   USER-ADM = thomasw
   PARTNER  = engel.domain1.de
   FILENAME = |ftexecsv ftshwo -tn -a -u -ccs=ISO8859-1
```

Erläuterung

LOGGING-ID
: Nummer des Logging-Satzes, maximal zwölfstellig

TRANS
: Übertragungsrichtung

  TO
  : Die Auftragsrichtung ist zum Partnersystem. Diese Richtung wird angegeben bei einem
    - Sendeauftrag
    - Auftrag zum Ansehen von Dateiattributen
    - Auftrag zum Ansehen von Dateiverzeichnissen

  FROM
  : Die Auftragsrichtung ist zum lokalen System. Diese Richtung wird angegeben bei einem
    - Empfangsauftrag
    - Auftrag zum Ändern von Dateiattributen
    - Auftrag zum Löschen von Dateien

  BOTH
  : Die Auftragsrichtung ist zum Partnersystem und zum lokalen System. Ändert ein FTAM-Partner die Zugriffsrechte einer lokalen Datei, so werden zwei Logging-Sätze geschrieben. Hierbei wird als Richtung jeweils BOTH angegeben.

PROFILE
: Name des verwendeten Profils

INITIATOR
: Initiator des Auftrags; bei Initiative im lokalen System: Benutzerkennung, bei Initiative im fernen System: *REMOTE.

USER-ADM
: Benutzerkennung, auf die sich die Aufträge im lokalen System beziehen.

PARTNER
: informiert über das beteiligte Partnersystem. Ausgegeben wird der Name in der Partnerliste oder die Adresse des Partnersystems (siehe Seite 68) oder der Name, mit dem das Partnersystem im TNS eingetragen ist.
Bei fern gestellten Aufträgen kann auch *%strange*, gefolgt von einem Teil der Adresse des Partnersystems, ausgegeben werden, wenn das Partnersystem nicht im TNS eingetragen ist und als Transportsystem nicht TCP/IP-RFC1006 verwendet wurde.

FILENAME
: lokaler Dateiname

RC
: Reason-Code. Er gibt an, ob ein Auftrag erfolgreich ausgeführt wurde (RC=0) oder warum er abgelehnt bzw. abgebrochen wurde. Weitere Informationen erhalten Sie mit dem *fthelp*-Kommando.

REC-TYPE
: gibt an, dass es sich um einen FTAC-Logging-Satz handelt.

PRIV
: gibt an, ob das benutzte Berechtigungsprofil privilegiert ist oder nicht.

TIME
: gibt den Zeitpunkt an, wann der Logging-Satz geschrieben wurde.

FUNCTION
: FT-Funktion

  TRANSFER-FILE
  : Datei übertragen

  READ-FILE-ATTR
  : Dateiattribute lesen

  DELETE-FILE
  : Datei löschen

  CREATE-FILE
  : Datei anlegen (nur bei Aufträgen möglich, die im fernen Partnersystem gestellt wurden)

  MODIFY-FILE-ATTR
  : Dateiattribute ändern

  READ-FILE-DIR
  : Dateiverzeichnisse lesen

  CREATE-FILE-DIR
  : Dateiverzeichnis anlegen

DELETE-FILE-DIR
: Dateiverzeichnis löschen

MODIFY-FILE-DIR
: Dateiverzeichnisattribute modifizieren

LOGIN
: Login: Inbound FTP-Zugang.
Dieser Logging-Satz wird geschrieben, wenn beim Inbound-FTP-Zugriff falsche Berechtigungsdaten angegeben wurden.

6.38.1.6 Lange Ausgabeform des ADM-Logging-Satzes

In folgenden Beispielen bewirkt die Option *-rt=a*, dass nur ADM-Logging-Sätze ausgegeben werden.

1. ADM-Logging-Satz auf dem Client:

```
ftshwl -rt=a -l
LOGGING-ID  = 27        RC      = 0000        TIME     = 2012-05-19
04:22:56
   TRANS    = FROM      REC-TYPE= ADM         FUNCTION = REM-ADMIN
   TRANS-ID = 190845    PROFILE =
   SEC-OPTS = ENCR+DICHK, RSA-2048 / AES-256
   INITIATOR= ftadmin
   USER-ADM = ftadmin
   PARTNER  = flexthom
   ADM-CMD  = ftshwo
   ADMIN-ID =
   ROUTING  = Muenchen/Jonny
```

2. ADM-Logging-Sätze auf dem Fernadministrations-Server:

```
ftshwl -rt=a -l -nb=3
LOGGING-ID  = 400       RC      = 0000        TIME     = 2012-05-19
13:22:56
   TRANS    = TO        REC-TYPE= ADM         FUNCTION = REM-ADMIN
   TRANS-ID = 65608     PROFILE = adminacc
   SEC-OPTS = ENCR+DICHK, RSA-2048 / AES-256
   INITIATOR= *REMOTE
   USER-ADM = admin002
   PARTNER  = ftadm://cog2-test-eng.homenet.de
   ADM-CMD  = ftshwo
   ADMIN-ID = Hugo
   ROUTING  = Muenchen/Jonny
LOGGING-ID  = 399       RC      = 0000        TIME     = 2012-05-19
13:22:55
   TRANS    = FROM      REC-TYPE= ADM         FUNCTION = REM-ADMIN
   TRANS-ID = 152973    PROFILE =
   SEC-OPTS = ENCR+DICHK, RSA-2048 / AES-256
   INITIATOR= admin002
   USER-ADM = admin002
   PARTNER  = Testrech
   ADM-CMD  = ftshwo
   ADMIN-ID =
   ROUTING  =
```

```
LOGGING-ID  = 396       RC      = 0000        TIME     = 2012-05-19
13:22:54
   TRANS    = TO        REC-TYPE= ADM         FUNCTION = REM-ADMIN-ROUT
   TRANS-ID =           PROFILE = adminacc
   SEC-OPTS =
   INITIATOR= *REMOTE
   USER-ADM = admin002
   PARTNER  = Testrech
   ADM-CMD  = ftshwo
   ADMIN-ID = Hugo
   ROUTING  = Muenchen/Jonny
```

3. ADM-Logging-Satz auf der administrierten openFT-Instanz:

```
ftshwl -rt=a -l
LOGGING-ID  = 2571      RC      = 0000        TIME     = 2012-05-19
13:29:49
   TRANS    = TO        REC-TYPE= ADM         FUNCTION = REM-ADMIN
   TRANS-ID = 334030    PROFILE = adminrem
   SEC-OPTS = ENCR+DICHK, RSA-2048 / AES-256
   INITIATOR= *REMOTE
   USER-ADM = admin001
   PARTNER  = ftadm://flexthom.homenet.de
   ADM-CMD  = ftshwl
   ADMIN-ID =
   ROUTING  =
```

Erläuterung

LOGGING-ID
: Nummer des Logging-Satzes, maximal zwölfstellig

RC
: Reason-Code des Auftrags

TIME
: gibt den Zeitpunkt an, wann der Logging-Satz geschrieben wurde

REC-TYPE
: Hier wird immer ADM für ADM-Logging-Satz ausgegeben

FUNCTION
: Ausgeführte Administrationsfunktion:

  REM-ADMIN
  : Fernadministrations-Auftrag ausführen

  REM-ADMIN-ROUT
  : Berechtigung für Fernadministrations-Auftrag prüfen und Fernadministrations-Auftrag bei bestandener Berechtigungsprüfung an die zu administrierende openFT-Instanz weiterleiten

TRANS-ID
: Nummer des Administrationsauftrags

PROFILE
: Name des verwendeten Profils

SEC-OPTS
: Während der Ausführung verwendete Sicherheitsoptionen

  ENCR Verschlüsselung der Auftragsbeschreibung

  DICHK Datenintegritätsprüfung der Auftragsbeschreibung

  DENCR Verschlüsselung des übertragenen Dateiinhalts

  DDICHK Datenintegritätsprüfung des übertragenen Dateiinhalts

  LAUTH Authentifizierung des lokalen Systems im fernen System (Authentifizierungsstufe 1)

  LAUTH2 Authentifizierung des lokalen Systems im fernen System (Authentifizierungsstufe 2)

  RAUTH Authentifizierung des fernen Systems im lokalen System (Authentifizierungsstufe 1)

  RAUTH2 Authentifizierung des fernen Systems im lokalen System (Authentifizierungsstufe 2)

  RSA-nnn
  : Länge des für die Verschlüsselung verwendeten RSA-Schlüssels

  AES-128 / AES-256 / DES
  : Verwendeter Verschlüsselungsalgorithmus

INITIATOR
: Initiator des Auftrags; bei Initiative im lokalen System: Benutzerkennung, bei Initiative im fernen System: ∗REMOTE.

USER-ADM
: Benutzerkennung, auf die sich der Fernadministrations-Auftrag im lokalen System bezieht.

PARTNER
: Beteiligtes Partnersystem. Abhängig davon, wo der ADM-Logging-Satz geschrieben wurde, wird Folgendes ausgegeben:

  – Client: Name/Adresse des Fernadministrations-Servers
  – Fernadministrations-Server (inbound): Name/Adresse des Clients
  – Fernadministrations-Server (outbound): Name/Adresse der zu administrierenden openFT-Instanz

– Administrierte openFT-Instanz: Name/Adresse des Fernadministrations-Servers

ADM-CMD
: Administrationskommando ohne Parameter

ADMIN-ID
: Administrator-Id, über die der Auftrag auf dem Fernadministrations-Server abgewickelt wird. Bei ADM-Logging-Sätzen auf einem Client bleibt dieses Feld leer.

ROUTING
: Routing-Information der zu administrierenden openFT-Instanz

6.38.2 Reason-Codes der Logging-Funktion

In den FTAC-Logging-Sätzen wird in einem Reason-Code angegeben, ob ein Auftrag nach der Zugangsprüfung angenommen wurde oder warum er abgelehnt wurde.

In ADM-Logging-Sätzen gibt der Reason-Code an, warum ein Fernadministrations-Auftrag nicht durchgeführt wurde.

Sie können sich den zur Code-Nummer gehörenden Meldungstext mit dem Kommando *fthelp* (siehe Seite 219) ausgeben lassen:

`fthelp` *code-nummer*

Bei zahlreichen Codes entsprechen die letzten drei Ziffern des Codes der Nummer der zugehörigen Meldung von openFT.

Zusätzlich können noch einige Codes auftreten, die nicht zu openFT-Meldungen (siehe openFT-Benutzerhandbuch) gehören und in folgenden Tabellen aufgelistet sind:

RC	Grund
0000	Auftrag akzeptiert
1001	Auftrag zurückgewiesen. Ungültige Transfer-Admission
1003	Auftrag zurückgewiesen. Transfer-Direction unzulässig
1004	Auftrag zurückgewiesen. Partner-Name unzulässig
1006	Auftrag zurückgewiesen. Verstoß gegen File-Name Beschränkung
100f	Auftrag zurückgewiesen. Verstoß gegen Success-Processing Beschränkung
1010	Auftrag zurückgewiesen. Verstoß gegen Failure-Processing Beschränkung
1011	Auftrag zurückgewiesen. Verstoß gegen Write-Mode Beschränkung
1012	Auftrag zurückgewiesen. Verstoß gegen FT-Function Beschränkung
1014	Auftrag zurückgewiesen. Verstoß gegen Data-Encryption Beschränkung
2001	Auftrag zurückgewiesen. Syntaxfehler bei der File-Name Expansion

RC	Grund
2004	Auftrag zurückgewiesen. Gesamtlänge der Folgeverarbeitung größer als 1000 Zeichen
3001	Auftrag zurückgewiesen. User-Identification ungültig
3003	Auftrag zurückgewiesen. Password ungültig
3004	Auftrag zurückgewiesen. Transfer-Admission gesperrt
3011	Auftrag zurückgewiesen. Verstoß gegen User Outbound Send Level
3012	Auftrag zurückgewiesen. Verstoß gegen User Outbound Receive Level
3013	Auftrag zurückgewiesen. Verstoß gegen User Inbound Send Level
3014	Auftrag zurückgewiesen. Verstoß gegen User Inbound Receive Level
3015	Auftrag zurückgewiesen. Verstoß gegen User Inbound Processing Level
3016	Auftrag zurückgewiesen. Verstoß gegen User Inbound File Management Level
3021	Auftrag zurückgewiesen. Verstoß gegen ADM Outbound Send Level
3022	Auftrag zurückgewiesen. Verstoß gegen ADM Outbound Receive Level
3023	Auftrag zurückgewiesen. Verstoß gegen ADM Inbound Send Level
3024	Auftrag zurückgewiesen. Verstoß gegen ADM Inbound Receive Level
3025	Auftrag zurückgewiesen. Verstoß gegen ADM Inbound Processing Level
3026	Auftrag zurückgewiesen. Verstoß gegen ADM Inbound File Management Level

RC	Grund
7001	Die Administrator-Id ist ungültig. In den Konfigurationsdaten des Fernadministrations-Servers konnte aus der User-Id oder dem Profilnamen keine gültige Administrator-Id ermittelt werden.
7002	Die Routing-Info ist ungültig. In den Konfigurationsdaten des Fernadministrations-Servers wurde die in der Routing-Info angegebene openFT-Instanz nicht gefunden.
7003	Das angegebene Fernadministrations-Kommando ist ungültig. Der Fernadministrations-Server weist das angegebene Kommando zurück, da es sich nicht um ein unterstütztes Fernadministrations-Kommando handelt.
7101	Verstoß gegen die Zugriffsrechteliste. Bei der Prüfung der Zugriffsrechte wurde festgestellt, dass der Administrator-Id in den Konfigurationsdaten des Fernadministrations-Servers nicht die benötigten Rechte zugeordnet sind, um das gültige Fernadministrations-Kommando auf der angegebenen openFT-Instanz auszuführen.
7201	Verstoß gegen die maximale Kommandolänge. Der Fernadministrations-Server ersetzt - insbesondere bei BS2000 Kommandos - die vom Benutzer angegebenen und von openFT garantierten kürzesten Kommandonamen durch den vollen Kommandonamen. Wird durch die Ersetzung des Kommandonamens das gesamte Fernadministrations-Kommando länger als die maximale Kommandolänge von 8192 Zeichen, dann wird das Kommando abgelehnt.

6.39 ftshwm - Messwerte des openFT-Betriebs ausgeben

Mit dem Kommando *ftshwm* können Sie sich die aktuellen Messwerte des openFT-Betriebs ausgeben lassen. Voraussetzung ist, dass der FT-Verwalter die Messdatenermittlung eingeschaltet hat (Kommando *ftmodo -mon=n*) und dass der asynchrone openFT-Server läuft.

Format

ftshwm -h |
[-ty]
[-raw]
[-po=<Polling Intervall 1..600> [-pnr=<Polling Anzahl 1..3600>]]
[-csv]
[<Name 1..12> [... <Name(100) 1..12>]| @a]

Beschreibung

-h gibt die Kommandosyntax am Bildschirm aus. Weitere Angaben nach *-h* werden ignoriert.

-ty Anstelle der Messwerte und Metadaten sollen deren Typen und Skalierungsfaktoren ausgegeben werden.

Der Typ der Metadaten entspricht *TIME (Zeitstempel) bzw. *STRING (Textausgabe der gewählten Selektion).

Der Typ eines Messwertes entspricht einem der Werte INT, BOOL oder PERCENT (Zahl, Ein/Aus-Wert oder Prozentsatz). Bei Int-Werten ist ggf. der Skalierungsfaktor in Klammern angegeben: INT(<Skalierungsfaktor>).

Der Skalierungsfaktor eines Messwertes hat nur bei der Ausgabe im CSV-Format Bedeutung. Dort ist er die Zahl, durch die der dargestellte Wert dividiert werden muss, um die echte Größe des Wertes zu erhalten.

Eine gleichzeitige Angabe von *-raw* ist nicht erlaubt.

-raw Die Messwerte sollen als unaufbereitete Rohdaten ausgegeben werden. Diese Option ist für weiterverarbeitende Programme gedacht. Diese Option darf nicht zusammen mit *-ty* angegeben werden. Messwerte des Objekts *Dauer* werden nicht ausgegeben.

Ohne diese Angabe werden die Daten aufbereitet ausgegeben.

Im folgenden Abschnitt „Beschreibung der Messwerte“ auf Seite 335 ist eine Tabelle mit Erläuterungen enthalten, der zu entnehmen ist, welche Werte bei Angabe bzw. Nicht-Angabe der Option *-raw* ausgegeben werden und wie sie in Abhängigkeit von dieser Option zu interpretieren sind.

-po=Polling Intervall
: Die Ausgabe soll nach der angegebenen Pollingzeit in Sekunden erstmals erfolgen und im entsprechenden Intervall wiederholt werden.

  Mit der gleichzeitigen Angabe von *-pnr* können Sie die Anzahl der Ausgaben begrenzen. Wenn Sie *-po* ohne *-pnr* angeben, dann wird die Ausgabe beliebig oft wiederholt.

  Eine über die Option *-po* angestoßene wiederholte Ausgabe (mit oder ohne *-pnr*) kann durch ein Unterbrechungssignal abgebrochen werden. Außerdem wird sie im Fehlerfall, bei Beendigung des asynchronen openFT oder bei Beendigung der Messdatenerfassung abgebrochen.

  Mögliche Werte: 1 bis 600.

-po nicht angegeben
: Die Messwerte werden sofort und nur einmal ausgegeben.

-pnr=Polling Anzahl
: Mit *-pnr* geben Sie die Anzahl der Ausgaben an. *-pnr* kann nur zusammen mit *-po* angegeben werden.

  Mögliche Werte: 1 bis 3600.

-csv Die Informationen sollen im CSV-Format ausgegeben werden. Zunächst werden in einer Zeile als Feldnamen die Kurznamen der Messwerte ausgegeben, dann folgt eine Zeile mit den Messwerten bzw. deren Typen und Skalierungsfaktoren als Dezimalzahl.

  Sie können den Umfang der Ausgabe durch Angabe einzelner für Sie wichtiger Messwerte eingrenzen.

Name [Name ...] | **@a**
: Der genannte Messwert soll ausgegeben werden bzw., wenn *-ty* spezifiziert ist, der zu dem genannten Namen gehörende Typ und Skalierungsfaktor.

  Name muss einer der Kurznamen der Messwerte sein, die als CSV-Überschrift ausgegeben werden. Sie können bis zu 100 durch Leerzeichen getrennte Namen angeben.

  @a für *Name*
  : Alle openFT-Messwerte bzw. die Typen und Skalierungsfaktoren aller openFT-Messwerte sollen ausgegeben werden.

  Name nicht angegeben
  : Es wird eine vordefinierte Standardmenge von Messwerten ausgegeben (siehe Abschnitt „Beschreibung der Messwerte“ auf Seite 335).

6.39.1 Beschreibung der Messwerte

Die unten stehende Tabelle zeigt alle Messwerte, die mit der Option *@a* ausgegeben werden. Sie können stattdessen auch eine beliebige Liste aus den in der Tabelle aufgeführten Messwerten angeben.

Zum Anzeigen der Messwerte des openFT-Betriebs steht Ihnen der openFT Monitor zur Verfügung. Verwenden Sie das Kommando *ftmonitor*, um den openFT Monitor aufzurufen, siehe openFT-Benutzerhandbuch

Aus den ersten beiden Buchstaben des Namens geht hervor, zu welchem Datenobjekt der Messwert gehört:

- Th = Durchsatz (Throughput)
- Du = Dauer (Duration)
- St = Status (State)

Der zweite Bestandteil des Namens kennzeichnet den Leistungsindikator, z.B. *Netb* für Netzbytes. Aus den letzten 3 Buchstaben des Namens geht bei Messwerten des Datenobjekts *Durchsatz* oder *Dauer* hervor, aus welchen Auftragstypen der Messwert gespeist wird, z.B.

- Ttl = FT Total
- Snd = FT Sendeaufträge
- Rcv = FT Empfangsaufträge
- Txt = Übertragung von Textdateien
- Bin = Übertragung von Binärdateien
- Out = FT Outbound
- Inb = FT Inbound

Ist die Messdatenerfassung für alle Partner ausgeschaltet (*ftmodo -monp=*), dann werden nur folgende Werte versorgt:

Status: StCLim, StCAct, StRqLim, StRqAct, StOftr, StFtmr, StFtpr, StTrcr

Alle anderen Werte sind 0.

Name	Bedeutung	Ausgabe aufbereitet (formatted)	Ausgabe nicht aufbereitet (raw)
ThNetbTtl	Durchsatz Netzbytes: Anzahl der Bytes, die übertragen wurden	Anzahl Bytes pro Sekunde	Bytes kumuliert
ThNetbSnd	Durchsatz Netzbytes (Sendeaufträge): Anzahl der Bytes, die bei Sendeaufträgen übertragen wurden	Anzahl Bytes pro Sekunde	Bytes kumuliert
ThNetbRcv	Durchsatz Netzbytes (Empfangsaufträge): Anzahl der Bytes, die bei Empfangsaufträgen übertragen wurden	Anzahl Bytes pro Sekunde	Bytes kumuliert
ThNetbTxt [1)]	Durchsatz Netzbytes (Textdateien): Anzahl der Bytes, die bei der Übertragung von Textdateien übertragen wurden	Anzahl Bytes pro Sekunde	Bytes kumuliert
ThNetbBin [1)]	Durchsatz Netzbytes (Binärdateien): Anzahl der Bytes, die bei der Übertragung von Binärdateien übertragen wurden	Anzahl Bytes pro Sekunde	Bytes kumuliert
ThDiskTtl	Durchsatz Plattenbytes: Anzahl der Bytes, die bei Übertragungsaufträgen aus Dateien gelesen oder in Dateien geschrieben wurden	Anzahl Bytes pro Sekunde	Bytes kumuliert
ThDiskSnd	Durchsatz Plattenbytes (Sendeaufträge): Anzahl der Bytes, die bei Sendeaufträgen aus Dateien gelesen wurden	Anzahl Bytes pro Sekunde	Bytes kumuliert
ThDiskRcv	Durchsatz Plattenbytes (Empfangsaufträge): Anzahl der Bytes, die bei Empfangsaufträgen in Dateien geschrieben wurden	Anzahl Bytes pro Sekunde	Bytes kumuliert
ThDiskTxt [1)]	Durchsatz Plattenbytes (Textdateien): Anzahl der Bytes, die bei Übertragungsaufträgen aus Textdateien gelesen oder in Textdateien geschrieben wurden	Anzahl Bytes pro Sekunde	Bytes kumuliert
ThDiskBin [1)]	Durchsatz Plattenbytes(Binärdateien): Anzahl der Bytes, die bei Übertragungsaufträgen aus Binärdateien gelesen oder in Binärdateien geschrieben wurden	Anzahl Bytes pro Sekunde	Bytes kumuliert
ThRqto	openFT-Aufträge: Anzahl der eingegangenen openFT-Aufträge	Anzahl pro Sekunde	Anzahl kumuliert
ThRqft [1)]	Dateiübertragungs-Aufträge: Anzahl der eingegangenen Dateiübertragungs-Aufträge	Anzahl pro Sekunde	Anzahl kumuliert

Name	Bedeutung	Ausgabe aufbereitet (formatted)	Ausgabe nicht aufbereitet (raw)
ThRqfm [1)]	Dateimanagement-Aufträge: Anzahl der eingegangenen Dateimanagement-Aufträge	Anzahl pro Sekunde	Anzahl kumuliert
ThSuct	erfolgreiche Aufträge: Anzahl der erfolgreich beendeten openFT-Aufträge	Anzahl pro Sekunde	Anzahl kumuliert
ThAbrt	Auftragsabbrüche: Anzahl der Auftragsabbrüche von openFT-Aufträgen	Anzahl pro Sekunde	Anzahl kumuliert
ThIntr	Auftragsunterbrechungen: Anzahl der Auftragsunterbrechungen von openFT-Aufträgen	Anzahl pro Sekunde	Anzahl kumuliert
ThUsrf	Aufträge von nichtberechtigten Benutzern: Anzahl der openFT-Aufträge, bei denen die Benutzerprüfung mit Fehler beendet wurde	Anzahl pro Sekunde	Anzahl kumuliert
ThFoll [1)]	gestartete Folgeverarbeitungen: Anzahl der gestarteten Folgeverarbeitungen	Anzahl pro Sekunde	Anzahl kumuliert
ThCosu [1)]	aufgebaute Verbindungen: Anzahl der erfolgreich aufgebauten Verbindungen	Anzahl pro Sekunde	Anzahl kumuliert
ThCofl	abgebrochene Verbindungsaufbau-Versuche: Anzahl der mit Fehler abgebrochenen Verbindungsaufbau-Versuche	Anzahl pro Sekunde	Anzahl kumuliert
ThCobr	Verbindungsabbrüche: Anzahl der wegen Verbindungsfehler erfolgten Verbindungsabbrüche	Anzahl pro Sekunde	Anzahl kumuliert
DuRqtlOut [1)]	Maximale Auftragsdauer outbound: Maximale Auftragsdauer eines outbound-Auftrags	Millisekunden [2)]	-
DuRqtlInb [1)]	Maximale Auftragsdauer inbound: Maximale Auftragsdauer eines inbound-Auftrags	Millisekunden [2)]	-
DuRqftOut [1)]	Maximale Auftragsdauer outbound Transfer: Maximale Dauer eines outbound Dateiübertragungs-Auftrags	Millisekunden [2)]	-
DuRqftInb [1)]	Maximale Auftragsdauer inbound Transfer: Maximale Dauer eines inbound Dateiübertragungs-Auftrags	Millisekunden [2)]	-
DuRqfmOut [1)]	Maximale Auftragsdauer outbound Dateimanagement: Maximale Dauer eines outbound Dateimanagement-Auftrags	Millisekunden [2)]	-

Name	Bedeutung	Ausgabe aufbereitet (formatted)	Ausgabe nicht aufbereitet (raw)
DuRqfmInb [1)]	Maximale Auftragsdauer inbound Dateimanagement: Maximale Dauer eines inbound Dateimanagement-Auftrags	Millisekunden [2)]	-
DuRqesOut [1)]	Maximale Auftragswartezeit outbound: Maximale Wartezeit bis zur outbound Auftragsbearbeitung (für Aufträge ohne spezifizierte Startzeit)	Millisekunden [2)]	-
DuDnscOut [1)]	Maximale Dauer eines outbound DNS-Auftrags: Maximale Zeitspanne, die ein outbound openFT-Auftrag in der Partnerprüfung verweilte	Millisekunden [2)]	-
DuDnscInb [1)]	Maximale Dauer eines inbound DNS-Auftrags: Maximale Zeitspanne, die ein inbound openFT-Auftrag in der Partnerprüfung verweilte	Millisekunden [2)]	-
DuConnOut [1)]	Maximale Dauer eines Verbindungsaufbaus: Maximale Zeitspanne von der Anforderung bis zum Empfang der Bestätigung einer Verbindung für einen outbound openFT-Auftrag	Millisekunden [2)]	-
DuOpenOut [1)]	Maximale Dateiöffnungszeit (outbound): Maximale Zeitspanne, die ein outbound openFT-Auftrag zum Öffnen der lokalen Datei benötigte	Millisekunden [2)]	-
DuOpenInb [1)]	Maximale Dateiöffnungszeit (inbound): Maximale Zeitspanne, die ein inbound openFT-Auftrag zum Öffnen der lokalen Datei benötigte	Millisekunden [2)]	-
DuClosOut [1)]	Maximale Dauer des Dateischließens (outbound): Maximale Zeitspanne, die ein outbound openFT-Auftrag zum Schließen der lokalen Datei benötigte	Millisekunden [2)]	-
DuClosInb [1)]	Maximale Dauer des Dateischließens (inbound): Maximale Zeitspanne, die ein inbound openFT-Auftrag zum Schließen der lokalen Datei benötigte	Millisekunden [2)]	-
DuUsrcOut [1)]	Maximale Dauer der Benutzerprüfung (outbound): Maximale Dauer, die ein outbound openFT-Auftrag zur Überprüfung der Benutzerkennung und Zugangsberechtigung benötigte	Millisekunden [2)]	-
DuUsrcInb [1)]	Maximale Dauer der Benutzerprüfung (inbound): Maximale Dauer, die ein inbound openFT-Auftrag zur Überprüfung der Benutzerkennung und Zugangsberechtigung benötigte	Millisekunden [2)]	-
StRqas	Anzahl der synchronen Aufträge im Zustand ACTIVE	Mittelwert [3)]	aktuelle Anzahl
StRqaa	Anzahl der asynchronen Aufträge im Zustand ACTIVE	Mittelwert [3)]	aktuelle Anzahl

Name	Bedeutung	Ausgabe aufbereitet (formatted)	Ausgabe nicht aufbereitet (raw)
StRqwt	Anzahl der Aufträge im Zustand WAIT	Mittelwert [3]	aktuelle Anzahl
StRqhd	Anzahl der Aufträge im Zustand HOLD	Mittelwert [3]	aktuelle Anzahl
StRqsp	Anzahl der Aufträge im Zustand SUSPEND	Mittelwert [3]	aktuelle Anzahl
StRqlk	Anzahl der Aufträge im Zustand LOCKED	Mittelwert [3]	aktuelle Anzahl
StRqfi [1]	Anzahl der Aufträge im Zustand FINISHED	Mittelwert [3]	aktuelle Anzahl
StCLim	Maximale Verbindungsanzahl: Obergrenze für die Anzahl der Verbindungen, die für asynchrone Aufträge aufgebaut werden	aktuell eingestellter Wert	
StCAct	Anzahl belegter Verbindungen für asynchrone Aufträge	Anteil in % von StCLim [4]	aktuelle Anzahl
StRqLim	Maximale Auftragszahl: Maximale Anzahl asynchroner Aufträge in der Auftragsverwaltung	aktuell eingestellter Wert	
StRqAct	Belegte Einträge der Auftragsverwaltung	Anteil in % von StRqLim [4]	aktuelle Anzahl
StOftr	openFT Protokoll aktiviert/deaktiviert	ON (aktiviert), OFF (deaktiviert)	
StFtmr	FTAM Protokoll aktiviert/deaktiviert	ON (aktiviert), OFF (deaktiviert)	
StFtpr	FTP Protokoll aktiviert/deaktiviert	ON (aktiviert), OFF (deaktiviert)	
StTrcr [1]	Trace eingeschaltet/ausgeschaltet	ON (aktiviert), OFF (deaktiviert)	

[1] Ausgabe nur mit @a

[2] Maximalwert des Messintervalls (= Zeit, die seit der letzten Abfrage der Messwerte bzw. dem Start der Erfassung vergangen ist).

[3] Mittelwert des Messintervalls (= Zeit, die seit der letzten Abfrage der Messwerte bzw. dem Start der Erfassung vergangen ist). Format n.mm, n ist eine ganze Zahl und mm sind als Nachkommastellen zu interpretieren (z.B. 1.75 entspricht 1,75).

[4] Wenn der Bezugswert im laufenden Betrieb gesenkt wird, dann kann die Ausgabe vorübergehend über 100 (%) liegen.

Beispiel

```
ftshwm

openFT(std)   Monitoring (formatted)
MonOn=2012-02-17 15:36:12 PartnerSel=OPENFT  RequestSel=ONLY-ASYNC,ONLY-LOCAL
2012-02-17 15:40:01

 Name      Value
 ----------------
 ThNetbTtl 38728
 ThNetbSnd 38728
 ThNetbRcv 0
 ThDiskTtl 16384
 ThDiskSnd 16384
 ThDiskRcv 0
 ThRqto    1
 ThSuct    0
 ThAbrt    0
 ThIntr    0
 ThUsrf    0
 ThCofl    0
 ThCobr    0
 StRqas    0.00
 StRqaa    8.66
 StRqwt    1.66
 StRqhd    0.00
 StRqsp    0.00
 StRqlk    0.00
 StCLim    16
 StCAct    37
 StRqLim   1000
 StRqAct   1
 StOftr    ON
 StFtmr    OFF
 StFtpr    OFF
```

Erläuterung der Ausgabe:

Das Standardausgabeformat beginnt mit einem Header mit den Angaben:
- Name der openFT-Instanz und ausgewähltes Datenformat (*raw* oder *formatted*)
- Startzeitpunkt der Messdatenerfassung sowie die Partner- und Auftragsselektion
- Aktueller Zeitstempel

Danach folgt die Liste mit den Standardwerten, siehe auch Seite 335.

6.40 ftshwo - Betriebsparameter anzeigen

Das Kommando *ftshwo* gibt die Betriebsparameter des lokalen openFT-Systems aus. Die Ausgabe kann neben der Standardausgabe und der Ausgabe im CSV-Format auch in Form einer plattformspezifischen Kommandofolge gewählt werden. Dadurch lassen sich die Einstellungen sichern und auf einem anderen Rechner mit dem ausgewählten Betriebssystem wieder einlesen.

Die Betriebsparameter kann der FT-Verwalter mit dem Kommando *ftmodo* setzen oder ändern.

Die Zugangsberechtigung des ADM-Trap-Servers wird bei der Standardausgabe und der CSV-Ausgabe nicht ausgegeben. Sie erscheint nur in der Ausgabe als Kommandofolge (*-px*, *-pw*, *-p2*, *-pz*).

Format

ftshwo -h |
[-csv | -px | -pw | -p2 | -pz]

Beschreibung

-h gibt die Kommandosyntax am Bildschirm aus. Weitere Angaben nach *-h* werden ignoriert.

-csv Die Betriebsparameter werden im CSV-Format ausgegeben. Die einzelnen Werte sind dabei durch Strichpunkte getrennt.

-px Die Betriebsparameter werden als Kommandofolge ausgegeben. Diese kann als Shell-Prozedur auf Unix-Systemen aufgerufen werden, um die Betriebsparameter wieder identisch zu erzeugen.

-pw Die Betriebsparameter werden als Kommandofolge ausgegeben. Diese kann als Batch-Prozedur auf Windows-Systemen aufgerufen werden, um die Betriebsparameter wieder identisch zu erzeugen.

-p2 Die Betriebsparameter werden als Kommandofolge ausgegeben. Diese kann als SDF-Prozedur auf BS2000/OSD-Systemen aufgerufen werden, um die Betriebsparameter wieder identisch zu erzeugen.

-pz Die Betriebsparameter werden als Kommandofolge ausgegeben. Diese kann als Clist-Prozedur auf z/OS-Systemen aufgerufen werden, um die Betriebsparameter wieder identisch zu erzeugen.

keine Option angegeben
Die Betriebsparameter werden im Standardformat ausgegeben.

6.40.1 Ausgabeformat von ftshwo

Beispiel

```
ftshwo
STARTED PROC-LIM CONN-LIM ADM-CLIM RQ-LIM MAX-RQ-LIFE TU-SIZE KEY-LEN CCS-NAME
  YES     NONE       16        8     2000      30       65535    2048  ISO8859-1
PTN-CHK DYN-PART SEC-LEV  FTAC-LOG FT-LOG ADM-LOG     USE TNS USE CMX ENC-MAND
  STD       ON   B-P-ATTR    ALL    ALL    ALL          NO      NO       NO
OPENFT-APPL      FTAM-APPL          FTP-PORT           ADM-PORT         ADM-CS
*STD             *STD               21                 11000              NO
ACTIVE           ACTIVE             ACTIVE             ACTIVE
HOST-NAME        IDENTIFICATION / LOCAL SYSTEM NAME
*NONE            mc011.mynet.local / $FJAM,MC011

DEL-LOG  ON  AT     RETPD    ADM-TRAP-SERVER
 OFF   DAILY 00:00    14     *NONE

TRAP: SS-STATE FT-STATE PART-STATE PART-UNREA RQ-STATE TRANS-SUCC TRANS-FAIL
CONS    OFF      OFF       OFF        OFF       OFF       OFF        OFF
ADM              OFF       OFF        OFF       OFF       OFF        OFF

FUNCT:  SWITCH PARTNER-SELECTION    REQUEST-SELECTION    OPTIONS    OPTIONS-LL
MONITOR  OFF   ALL                  ALL
TRACE    OFF   ALL                  ALL                  NONE       OFF
```

Bedeutung der Ausgaben mit zugehöriger Kommando-Option:

Feldname	Bedeutung und Werte	Kommando/ -Option
STARTED	gibt an, ob der asynchrone openFT-Server gestartet ist (YES) oder nicht (NO).	*ftstart* *ftstop*
PROC-LIM	maximale Anzahl der openFT-Server, die für die Bearbeitung asynchroner Aufträge zur Verfügung stehen.	*ftmodo -pl=*
CONN-LIM	maximale Anzahl asynchroner Aufträge, die simultan bearbeitet werden können.	*ftmodo -cl=*
ADM-CLIM	maximale Anzahl asynchroner Administrations-Aufträge einschließlich ADM-Traps, die simultan bearbeitet werden können.	*ftmodo -admcl=*
RQ-LIM	maximale Anzahl von Dateiübertragungsaufträgen, die sich gleichzeitig im Auftragsbuch des lokalen Systems befinden können.	*ftmodo -rql=*
MAX-RQ-LIFE	maximale Lebensdauer von Aufträgen im Auftragsbuch (in Tagen).	*ftmodo -rqt=*

Feldname	**Bedeutung und Werte**	**Kommando/ -Option**
TU-SIZE	Obergrenze für die Nachrichtenlänge auf Transportebene (in Byte)	*ftmodo -tu=*
KEY-LEN	Länge des RSA-Schlüssels, der aktuell zum Verschlüsseln des AES-/DES-Schlüssels verwendet wird.	*ftmodo -kl=*
CCS-NAME	Name des Zeichensatzes, der als Standard bei Dateiübertragungsaufträgen verwendet wird, siehe Seite 249.	*ftmodo -ccs=*
PTN-CHK	Einstellung für die Absenderüberprüfung: ADDR: Adresse STD: Identifikation	*ftmodo -ptc=*
DYN-PART	Einstellung für dynamische Partnereinträge: ON (eingeschaltet) OFF (ausgeschaltet)	*ftmodo -dp=*
SEC-LEV	Standard-Sicherheitsstufe für Partner in der Partnerliste, für die keine Sicherheitsstufe festgelegt wurde: 1..100: feste Sicherheitsstufe, 1 bedeutet niedrig, 100 bedeutet hoch. B-P-ATTR: Die Standard-Sicherheitsstufe hängt von den Attributen des Partners ab: 10, wenn der Partner authentifiziert ist. 90, wenn der Partner im Transportsystem bekannt ist. 100 sonst, d.h. wenn der Partner nur über seine Adresse identifiziert wird.	*ftmodo -sl=* *ftmodo -sl=p*
FTAC-LOG	Umfang des FTAC-Loggings: ALL: alle FTAC-Zugriffsprüfungen MODIFY: modifizierende Dateimanagement-Aufträge und abgelehnte FTAC-Zugriffsprüfungen REJECTED: nur abgelehnte FTAC-Zugriffsprüfungen	*ftmodo -lc=*

Feldname	Bedeutung und Werte	Kommando/ -Option
FT-LOG	Umfang des FT-Loggings: ALL: alle Aufträge FAIL: nur fehlerhafte FT-Aufträge NONE: FT-Logging ausgeschaltet	*ftmodo -lt=*
ADM-LOG	Umfang des ADM-Loggings: ALL: alle Aufträge FAIL: nur fehlerhafte ADM-Aufträge MODIFY: nur modifizierende ADM-Aufträge NONE: ADM-Logging ausgeschaltet	*ftmodo -la=*
USE TNS	gibt an, ob im Betrieb mit CMX der TNS verwendet werden soll (YES) oder nicht (NO)	*ftmodo -tns=*
USE CMX	gibt an, ob der Betrieb mit CMX eingeschaltet ist (YES) oder nicht (NO)	*ftmodo -cmx=*
ENC-MAND	gibt an, ob die Inbound- und/oder Outbound-Verschlüsselung eingeschaltet ist	*ftmodo -c=*
OPENFT-APPL	Portnummer des lokalen openFT-Servers, ggf. ergänzt durch den Transport-Selektor. *STD bedeutet, dass der Standardwert verwendet wird, d.h. 1100 und $FJAM im Transdata-Format (EBCDIC, 8 Zeichen lang, mit Leerzeichen aufgefüllt). Zeile 2: ACTIVE: openFT-Protokoll aktiviert DISABLED: openFT-Protokoll (inbound) deaktiviert INACT: openFT-Protokoll (inbound) nicht verfügbar	*ftmodo -openft=* *ftmodo -acta=*
FTAM-APPL	Portnummer des lokalen FTAM-Servers, ggf. ergänzt durch den Transport-, den Session- und den Presentation-Selektor. *STD bedeutet, dass der Standardwert verwendet wird, d.h. 4800 und $FTAM im Transdata-Format (EBCDIC, 8 Zeichen lang, mit Leerzeichen aufgefüllt). Zeile 2: ACTIVE: FTAM-Protokoll aktiviert DISABLED: FTAM-Protokoll (inbound) deaktiviert INACT: FTAM-Protokoll (inbound) nicht verfügbar NAVAIL: FTAM nicht installiert	*ftmodo -ftam=* *ftmodo -acta=*

Feldname	**Bedeutung und Werte**	**Kommando/ -Option**
FTP-PORT	Portnummer des lokalen FTP-Servers. Standardport: 21 Zeile 2: ACTIVE: FTP-Protokoll aktiviert DISABLED: FTP-Protokoll (inbound) deaktiviert INACT: FTP-Protokoll (inbound) nicht verfügbar NAVAIL: FTP nicht installiert	*ftmodo -ftp=* *ftmodo -acta=*
ADM-PORT	Portnummer, die für die Fernadministration verwendet wird. Standardport: 11000 Zeile 2: ACTIVE: Fernadministration aktiviert DISABLED: Fernadministration (inbound) deaktiviert INACT: Fernadministration (inbound) nicht verfügbar	*ftmodo -adm=* *ftmodo -acta=*
ADM-CS	gibt an, ob die lokale openFT-Instanz als Fernadministrations-Server gekennzeichnet ist (YES) oder nicht (NO).	*ftmodo -admcs=*
HOST-NAME	Hostname des lokalen Rechners, *NONE bedeutet, dass kein Hostname vergeben wurde.	*ftcrei -addr=* *ftmodi -addr=*
IDENTIFICATION	Instanzidentifikation der lokalen openFT-Instanz	*ftmodo -id=*
LOCAL-SYSTEM-NAME	Name des lokalen Systems	*ftmodo -p= -l=*
DEL-LOG	automatisches Löschen von Logging-Sätzen eingeschaltet (ON) oder ausgeschaltet (OFF)	*ftmodo -ld=*
ON	Tag, an dem die Logging-Sätze gelöscht werden sollen: MON, TUE, ... SUN (Wochentag) oder 1...31 (Tag des Monats) oder DAILY (täglich)	*ftmodo -ldd=*
AT	Uhrzeit, zu der die Logging-Sätze gelöscht werden sollen (hh:mm)	*ftmodo -ldt=*
RETPD	Mindestalter der zu löschenden Logging-Sätze in Tagen. 0 bedeutet aktueller Tag.	*ftmodo -lda=*
ADM-TRAP-SERVER	Name oder Adresse des Partners, an den die ADM-Traps gesendet werden. *NONE bedeutet, dass das Senden der ADM-Traps ausgeschaltet ist.	*ftmodo -atpsv=*

Feldname	Bedeutung und Werte	Kommando/ -Option
TRAP	In diesem Bereich werden die TRAP-Einstellungen ausgegeben, mögliche Werte sind ON und OFF. Die Zeile CONS bezeichnet die Konsolen-Traps, die Zeile ADM die ADM-Traps. Die Spalten bezeichnen die Ereignisse, bei denen ggf. Traps erzeugt werden: SS-STATE: Statuswechsel des openFT-Subsystems (nur Zeile CONS) FT-STATE: Statuswechsel des asynchronen Servers PART-STATE: Statuswechsel von Partnersystemen PART-UNREA: Nichterreichbarkeit von Partnersystemen RQ-STATE: Statuswechsel der Auftragsverwaltung TRANS-SUCC: Erfolgreich abgeschlossene Aufträge TRANS-FAIL: Fehlgeschlagene Aufträge	*ftmodo* *-tpc=* *-atp=*
FUNCT	In diesem Bereich werden die Einstellungen zur Messdatenerfassung (Zeile MONITOR) und zur Überwachung (Zeile TRACE) ausgegeben. Die einzelnen Spalten bedeuten: SWITCH: Funktion (Messdatenerfassung bzw. Überwachung) ist eingeschaltet (ON) oder ausgeschaltet (OFF) PARTNER-SELECTION: Auswahl nach Protokolltyp des Partnersystems. Mögliche Protokolltypen: OPENFT, FTP, FTAM. Bei TRACE kann zusätzlich ADM (Administrationspartner) ausgegeben werden. ALL bedeutet alle Protokolltypen ausgewählt, d.h. Überwachung / Messdatenerfassung für alle Partnersysteme möglich. NONE bedeutet kein Protokolltyp ausgewählt.	*ftmodo* *-mon=* *-tr=* *ftmodo* *-monp=* *-trp=*

Feldname	**Bedeutung und Werte**	**Kommando/ -Option**
FUNCT (Forts.)	REQUEST-SELECTION: Auswahl nach Art des Auftrags. Möglich sind: ONLY-SYNC/ONLY-ASYNC (nur synchrone oder nur asynchrone Aufträge) ONLY-LOCAL/ONLY-REMOTE (nur lokal gestellte oder nur entfernt gestellte Aufträge). ALL bedeutet keine Einschränkung, d.h. alle Aufträge.	*ftmodo* *-monr=* *-trr=*
	OPTIONS (nur bei TRACE): NONE bedeutet keine Options (Trace im Standardformat) NO-BULK-DATA bedeutet Minimal-Trace, d.h. Massendaten (Dateiinhalte) werden nicht protokolliert. Es werden auch keine Wiederholungen von Datenprotokoll-Elementen protokolliert.	*ftmodo -tro=*
	OPTIONS-LL Umfang der Überwachung für untere Protokollschichten: OFF: Ausgeschaltet STD: Standard DETAIL: Details	*ftmodo -troll=*

6.41 ftshwp - Berechtigungsprofile anzeigen

ftshwp steht für "show profile", also Zeigen eines Berechtigungsprofils. Mit *ftshwp* können Sie sich über Berechtigungsprofile informieren. In der Kurzform erhalten Sie die Namen der ausgewählten Berechtigungsprofile und die Information, ob

– das Berechtigungsprofil privilegiert ist: Stern (*) vor dem Profilnamen
– die Zugangsberechtigung gesperrt ist: Ausrufezeichen (!) vor dem Profilnamen

Als ADM-Verwalter dürfen Sie sich auch über ADM-Profile informieren (d.h. Profile mit der Eigenschaft "Zugang zum Fernadministrations-Server").

Als FTAC-Verwalter dürfen Sie sich über alle Berechtigungsprofile in Ihrem System informieren.

Format

```
ftshwp  -h  |
        [ <Profilname 1..8> | @s ]
        [ -s=[<Zugangsberechtigung 8..32> | @a | @n]
             [,<Benutzerkennung 1..32> | @a | @adm] ]
        [ -l ][ -csv ]
```

Beschreibung

-h gibt die Kommandosyntax am Bildschirm aus. Weitere Angaben nach *-h* werden ignoriert.

Profilname | **@s**
: Hier können Sie den Namen des Berechtigungsprofils angeben, über das Sie sich informieren wollen.

  @s für *Profilname*
  : Informiert über das Standard-Berechtigungsprofil der Benutzerkennung, sofern es eingerichtet ist. Andernfalls erhalten Sie eine entsprechende Meldung.

Profilname nicht angegeben
: Sie benutzen den Namen des Berechtigungsprofils nicht als Auswahlkriterium. Wenn Sie nicht mit *-s* (siehe unten) ein Berechtigungsprofil auswählen, erhalten Sie Informationen über alle Ihre Berechtigungsprofile ausgegeben.

-s=[Zugangsberechtigung | **@a** | **@n**][**,**Benutzerkennung | **@a** | **@adm**]

Mit *-s* können Sie Auswahlkriterien angeben, welche Berechtigungsprofile Sie sich ansehen wollen.

Wenn Sie sich ein Standard-Berechtigungsprofil ansehen möchten, dann dürfen Sie nur *@n* oder *@a* angeben.

Zugangsberechtigung
: Sie wollen sich über das Berechtigungsprofil mit dieser Zugangsberechtigung informieren. Eine binäre Zugangsberechtigung müssen Sie sedezimal in der Form x\'...\' oder X\'...\' angeben.

@a für *Zugangsberechtigung*
: Wenn Sie hier *@a* angeben, erhalten Sie entweder Informationen über das mit *Profilname* (siehe oben) angesprochene Berechtigungsprofil oder (falls kein Profilname angegeben wurde) über alle Berechtigungsprofile.

  @a können Sie als FTAC-Verwalter angeben, wenn Sie sich über Berechtigungsprofile fremder Benutzerkennungen informieren wollen. Die Zugangsberechtigung sollen Sie nämlich gar nicht kennen.

@n für *Zugangsberechtigung*
: Wenn Sie hier *@n* angeben, erhalten Sie Informationen über Berechtigungsprofile, die keine definierte Zugangsberechtigung haben.

  @n können Sie als FTAC-Verwalter angeben, wenn Sie sich über Berechtigungsprofile fremder Benutzerkennungen informieren wollen, die keine definierte Zugangsberechtigung haben.

Zugangsberechtigung nicht angegeben
: Die Zugangsberechtigung wird nach der Kommandoabgabe am Bildschirm abgefragt. Sie bleibt unsichtbar, um zu verhindern, dass Unbefugte die Zugangsberechtigung sehen. Um Eingabefehler zu vermeiden, wird eine Kontrolleingabe verlangt. Wenn Sie die Eingabeanforderungen nur durch Drücken der Returntaste beantworten, wirkt das wie die Angabe von *@a* im Kommando.

,Benutzerkennung
: Als FTAC-Verwalter dürfen Sie hier jede beliebige Benutzerkennung angeben.

@a für *Benutzerkennung*
: Als FTAC-Verwalter erhalten Sie Informationen über die Berechtigungsprofile aller Benutzerkennungen.

  Als ADM-Verwalter erhalten Sie Informationen über die eigenen Berechtigungsprofile sowie über ADM-Profile.

@adm für *Benutzerkennung*
Als FTAC- oder ADM-Verwalter erhalten Sie Informationen über ADM-Profile.

Benutzerkennung nicht angegeben
Es werden (unabhängig davon, wer das Kommando absetzt) nur Informationen über Profile der eigenen Benutzerkennung ausgegeben.

-s nicht angegeben
Falls kein Profilname angegeben wurde, werden Informationen über alle Berechtigungsprofile unter der Kennung ausgegeben, von der aus das *ftshwp* abgesetzt wird. Sonst wird über das Berechtigungsprofil mit dem angegebenen Namen informiert.

-l Mit dieser Option geben Sie an, dass Sie den Inhalt der ausgewählten Berechtigungsprofile sehen wollen.

In der ausführlichen Form erhalten Sie den gesamten Inhalt der ausgewählten Berechtigungsprofile. Dem Parameter USER-ADM können Sie entnehmen,
– für welche Kennung ein Berechtigungsprofil gültig ist oder ob es sich um ein ADM-Profil handelt,
– ob es nur für ein bestimmtes Kennwort der Kennung gültig ist,
– ob es für alle beliebigen Kennwörter der Kennung gültig ist,
– ob es kein definiertes Kennwort hat und damit gesperrt ist.

Bitte beachten Sie, dass ADM-Profile immer mit *ADM im Parameter USER-ADM gekennzeichnet werden.

USER-ADM=	**Bedeutung**
(kennung,,OWN)	Das Profil gilt für alle Kennwörter der Kennung.
(kennung,,YES)	Das Profil gilt nur für ein bestimmtes Kennwort der Kennung (nach einem *ftcrep* oder *ftmodp* mit der Angabe *-ua=Benutzerkennung,kennwort*). Wenn das Kennwort anschließend geändert wird, ist damit das Profil nicht mehr verwendbar (nicht gesperrt!). Sie können es zum Beispiel wieder aktivieren, indem Sie das Kennwort zurücksetzen.
(kennung,, NOT-SPECIFIED)	Der FTAC-Verwalter hat das Berechtigungsprofil nur mit Kenntnis der Kennung angelegt oder geändert. Dadurch wurde das Profil gesperrt. Sie müssen das Profil mit *ftmodp* und dem Parameter *-v=y* "entsperren".

Falls ein Berechtigungsprofil gesperrt ist, zeigt zusätzlich der Parameter *TRANS-ADM* die Ursache für die Sperrung an. Die möglichen Werte des Parameters und die Bedeutung können Sie der folgenden Tabelle entnehmen:

TRANS-ADM=	**mögliche Ursache und Maßnahme**
NOT-SPECIFIED	Der FTAC-Verwalter hat das Berechtigungsprofil ohne Zugangsberechtigung angelegt, oder Sie haben keine Zugangsberechtigung vergeben. Gegenmaßnahme: Zugangsberechtigung vergeben
DUPLICATED	Jemand wollte ein Berechtigungsprofil mit der selben Zugangsberechtigung erzeugen. Gegenmaßnahme: Neue Zugangsberechtigung vergeben
LOCKED (by_adm)	Der FTAC-Verwalter hat das Berechtigungsprofil nur mit Kenntnis der Kennung geändert. Damit blieb zwar die Zugangsberechtigung unverändert, aber sie wurde gesperrt. Gegenmaßnahme: Profil mit dem Kommando *ftmodp* und dem Parameter *-v=y* "entsperren"
LOCKED (by_import)	Das Berechtigungsprofil wurde mit dem Kommando *ftimpe* angelegt. Die Zugangsberechtigung bleibt unverändert, ist aber als gesperrt markiert. Gegenmaßnahme: Profil mit dem Kommando *ftmodp* und dem Parameter *-v=y* "entsperren"
LOCKED (by_user)	Sie haben Ihr Berechtigungsprofil gesperrt. Gegenmaßnahme: Profil mit dem Kommando *ftmodp* und dem Parameter *-v=y* "entsperren"
EXPIRED	Die Frist, bis zu der die Zugangsberechtigung verwendet werden darf, ist abgelaufen. Gegenmaßnahme: Profil mit dem Kommando *ftmodp* und dem Parameter *-d* "entsperren", indem die zeitliche Einschränkung mit der Angabe *-d=* aufgehoben oder eine neue Frist mit *-d=datum* festgelegt wird

Es gibt keine Möglichkeit, mit *ftshwp* eine Zugangsberechtigung anzuschauen. Wenn Sie eine Zugangsberechtigung vergessen haben, müssen Sie mit *ftmodp* eine neue definieren.

-l nicht angegeben

Sie erhalten nur die Namen Ihrer Berechtigungsprofile ausgegeben. Zusätzlich erhalten Sie durch entsprechende Markierungen Information darüber, ob ein Berechtigungsprofil privilegiert (∗) und ob es gesperrt (!) ist.

-csv Mit *-csv* geben Sie an, dass die FT-Berechtigungsprofile im CSV-Format ausgegeben werden sollen. Die Werte der Ausgabe werden durch Strichpunkte getrennt ausgegeben. Die Angabe von *-csv* bewirkt stets die Ausgabe in der ausführlichen Form (analog zu *-l*), gleichgültig, ob *-l* gleichzeitig angegeben wurde oder nicht.

-csv nicht angegeben
Sie bekommen die FT-Berechtigungsprofile im Standardformat ausgegeben, d.h. ohne Angabe von *-l* in Kurzform und mit Angabe von *-l* in ausführlicher Form.

Beispiele

1. Sie möchten sich als FTAC-Verwalter alle Standard-Berechtigungsprofile auf Ihrem System ansehen.

   ```
   ftshwp @s -s=@n,@a -l
   ```

   Die Ausgabe hat folgende Form:

   ```
   *STD
    TRANS-ADM   = (NOT-SPECIFIED)
    USER-ADM    = (hugo,,OWN)
    FT-FUNCTION = (TRANSFER-FILE, MODIFY-FILE-ATTRIBUTES, READ-FILE-
   DIRECTORY)
    LAST-MODIF  = 2012-03-23 17:12:25
   *STD
    TRANS-ADM   = (NOT-SPECIFIED)
    WRITE       = NEW-FILE
    USER-ADM    = (dagobert,,OWN)
    FT-FUNCTION = (TRANSFER-FILE)
    LAST-MODIF  = 2012-03-22 16:06:55
   ```

2. Sie möchten sich als FT-Verwalter das Profil *acctrap1* auf dem ADM-Trap-Server ansehen.

   ```
   ftshwp acctrap1 -l
   ```

   Die Ausgabe hat folgende Form:

   ```
   acctrap1
    USER-ADM    = (ADMIN002,,OWN)
    FT-FUNCTION = (ADM-TRAP-LOG)
    LAST-MODIF  = 2012-01-23 18:24:42
   ```

   Der Wert ADM-TRAP-LOG bei FT-FUNCTION im Profil *acctrap1* bedeutet, dass der Fernadministrations-Server über dieses Profil ADM-Traps empfangen kann.

3. Sie möchten sich als ADM-Verwalter die ADM-Profile auf dem Fernadministrations-Server ansehen.

   ```
   ftshwp -s=@a,@adm  -l
   ```

   Die Ausgabe hat folgende Form:

   ```
   acccentr
    USER-ADM    = (*ADM,,OWN)
    FT-FUNCTION = (ACCESS-TO-ADMINISTRATION)
    LAST-MODIF  = 2012-01-23 18:21:08
   ```

   Das Profil *acccentr* ist ein ADM-Profil. Dies erkennt man am Wert ACCESS-TO-ADMINISTRATION bei FT-FUNCTION. Bei USER-ADM wird als Kennung *ADM ausgegeben.

4. Sie sind FT-Verwalter und möchten sich das Profil *remadmin* ansehen, das für die Fernadministration eingerichtet wurde.

   ```
   ftshwp remadmin -l
   ```

   Die Ausgabe hat folgende Form:

   ```
   remadmin
    USER-ADM    = (ADMIN001,,OWN)
    FT-FUNCTION = (REMOTE-ADMINISTRATION)
    LAST-MODIF  = 2012-02-27 16:20:38
   ```

6.42 ftshwptn - Eigenschaften von Partnern anzeigen

Mit dem Kommando *ftshwptn* können Sie folgende Informationen über die in der Partnerliste eingetragenen Partnersysteme anfordern:

- Den Namen des Partnersystems
- Den Zustand des Partnersystems (aktiviert, deaktiviert)
- Die Sicherheitsstufe, die dem Partnersystem zugewiesen wurde
- Die Priorität, die dem Partnersystem zugewiesen wurde
- Die Einstellung der openFT-Überwachungsfunktion (Trace) für das Partnersystem
- Die Anzahl der im lokalen System erteilten, noch nicht abgeschlossenen Dateiübertragungsaufträge an das Partnersystem
- Die Anzahl der im Partnersystem erteilten Dateiübertragungsaufträge für das lokale System
- Den Modus für Absenderüberprüfung und Authentifizierung
- Die Transportadresse des Partnersystems, ggf. mit Portnummer, wenn diese vom Standardwert abweicht
- Die Identifikation des Partnersystems
- Die Routing-Information, wenn das Partnersystem nur über eine Zwischeninstanz erreichbar ist

Außerdem können Sie die Partner in der Partnerliste als plattformspezifische Kommandofolge ausgeben. Dadurch lässt sich die Partnerliste sichern und kann auf einem anderen Rechner mit ggf. anderem Betriebssystem wieder eingelesen werden.

Format

```
ftshwptn  -h |
        [ <Partner 1..200> | @a ]
        [ -st=a | -st=na | -st=d | -st=ie | -st=nc | -st=ad | -st=da ]
        [ -l | -csv | -px | -pw | -p2 | -pz ]
```

Beschreibung

-h gibt die Kommandosyntax am Bildschirm aus. Weitere Angaben nach *-h* werden ignoriert.

Partner | **@a**
gibt den Partner an, dessen Eigenschaften Sie anzeigen möchten. Sie können den Namen des Partners in der Partnerliste oder die Adresse des Partnersystems angeben. Einzelheiten zur Adressangabe finden Sie auf Seite 68.

@a für *Partner*
Es werden die Eigenschaften aller Partner in der Partnerliste angezeigt.

Partner nicht angegeben
Es werden die Eigenschaften aller Partner in der Partnerliste angezeigt.

-st=a | **-st=na** | **-st=d** | **-st=ie** | **-st=nc** | **-st=ad** | **-st=da**
Mit diesem Operanden können Sie die Eigenschaften von Partnersystemen anzeigen, die einen bestimmten Zustand haben. Sie können bei *-st* folgende Werte angeben:

a (active)
Es werden alle Partnersysteme angezeigt, die im Zustand ACTIVE sind.

na (not active)
Es werden alle Partnersysteme angezeigt, die **nicht** im Zustand ACTIVE sind.

d (deactivated)
Es werden alle Partnersysteme angezeigt, die im Zustand DEACTIVE sind.

ie (installation error)
Es werden alle Partnersysteme angezeigt, die im Zustand LUNK, RUNK, LAUTH, RAUTH, NOKEY oder IDREJ sind.

nc (not connected)
Es werden alle Partnersysteme angezeigt, die im Zustand NOCON oder DIERR sind.

ad (active + automatic deactivation)
Es werden alle Partnersysteme angezeigt, die mit der Option AUTOMATIC-DEACTIVATION versehen sind (siehe Option *-ad* bei den Kommandos *ftaddptn* und *ftmodptn*), aber noch aktiv sind.

da (deactivated + automatic deactivation)
Es werden alle Partnersysteme angezeigt, die aufgrund der Option AUTOMATIC-DEACTIVATION tatsächlich deaktiviert wurden.

-st nicht angegeben

Die Ausgabe wird nicht auf Partnersysteme mit einem bestimmten Zustand eingeschränkt.

-l | **-csv** | **-px** | **-pw** | **-p2** | **-pz**

Diese Optionen bestimmen den Umfang und das Format der Ausgabe.

-l Die Eigenschaften der Partnersysteme werden in der ausführlichen Form als Tabelle ausgegeben.

-csv Die Eigenschaften der Partnersysteme werden im CSV-Format ausgegeben. Die einzelnen Werte sind dabei durch Strichpunkte getrennt.

-px Die Eigenschaften der Partnersysteme werden als Kommandofolge ausgegeben. Diese kann in Unix-Systemen als Shell-Prozedur aufgerufen werden, um Partnereinträge mit identischen Eigenschaften zu erzeugen.

-pw Die Eigenschaften der Partnersysteme werden als Kommandofolge ausgegeben. Diese kann in Windows-Systemen als Batch-Prozedur aufgerufen werden, um Partnereinträge mit identischen Eigenschaften zu erzeugen.

-p2 Die Eigenschaften der Partnersysteme werden als Kommandofolge ausgegeben. Diese kann in BS2000-Systemen als SDF-Prozedur aufgerufen werden, um Partnereinträge mit identischen Eigenschaften zu erzeugen.

-pz Die Eigenschaften der Partnersysteme werden als Kommandofolge ausgegeben. Diese kann in z/OS-Systemen als CLIST-Prozedur aufgerufen werden, um Partnereinträge mit identischen Eigenschaften zu erzeugen.

-l, *-csv*, *-px*, *-pw*, *-p2*, *-pz* nicht angegeben

Wenn Sie keine dieser Optionen angeben, dann werden die Eigenschaften der Partner in der Kurzform aufgelistet.

6.42.1 Ausgabeformat von ftshwptn

Beispiel für eine Ausgabe in Kurzform und in Langform:

```
$ftshwptn

NAME     STATE SECLEV   PRI  TRACE  LOC  REM P-CHK ADDRESS
pingftam ACT   50       NORM FTOPT    0    0       ftam://PING.homenet.de
PINGO    ACT   STD      NORM FTOPT    0    0 FTOPT PINGPONG.homenet.de:1234
rout0001 ACT   STD      HIGH FTOPT    0    0 FTOPT INCOGNITO
servftp  ACT   B-P-ATTR LOW  ON       0    0       ftp://ftp.homenet.de

ftshwptn -l

NAME     STATE SECLEV   PRI  TRACE  LOC  REM P-CHK ADDRESS
         INBND REQU-P                             ROUTING  IDENTIFICATION
pingftam ACT    50      NORM FTOPT    0    0       ftam://PING.homenet.de
         DEACT STD
PINGO    ACT   STD      NORM FTOPT    0    0 FTOPT PINGPONG.homenet.de:1234
         ACT   SERIAL                                       PINGPONG.homenet.de
rout0001 ACT   STD      HIGH FTOPT    0    0 FTOPT INCOGNITO
         ACT   STD                                ROUT01   INCOGNITO.id.new
servftp  ACT   B-P-ATTR LOW  ON       0    0       ftp://ftp.homenet.de
         ACT   STD
```

Erläuterung

NAME

Name, mit dem das Partnersystem in die Partnerliste eingetragen ist.

Wenn hier kein Name eingetragen ist, handelt es sich um einen dynamischen Partner.

STATE

gibt an, wie lokal gestellte Dateiübertragungsaufträge an das angegebene Partnersystem bearbeitet werden.

ACT Lokal gestellte Dateiübertragungsaufträge an dieses Partnersystem werden nach *ftstart* bearbeitet.

DEACT

Lokal gestellte Dateiübertragungsaufträge an dieses Partnersystem werden zunächst nicht bearbeitet, sondern nur im Auftragsbuch abgelegt.

ADEAC

Fehlgeschlagene Verbindungsaufbauversuche zu diesem Partnersystem führen zu dessen Deaktivierung. Die maximale Anzahl von direkt aufeinander folgenden Fehlversuchen beträgt 5. Um wieder File Transfer mit diesem Partnersystem betreiben zu können, muss es explizit mit *ftmodptn -st=a* aktiviert werden.

NOCON
: Aufbau einer Transportverbindung ist misslungen.

LUNK
: Lokales System ist dem fernen FT-System unbekannt.

RUNK
: Partnersystem ist im lokalen Transportsystem unbekannt.

AINAC
: Partnersystem wurde nach mehreren erfolglosen Verbindungsaufbauversuchen deaktiviert.

LAUTH
: Das lokale System konnte im Partnersystem nicht authentifiziert werden. Dem Partnersystem muss ein aktueller öffentlicher Schlüssel der lokalen openFT-Instanz zur Verfügung gestellt werden.

RAUTH
: Das Partnersystem konnte im lokalen System nicht authentifiziert werden. Es muss ein aktueller öffentlicher Schlüssel des Partnersystems in das Verzeichnis *syskey* der openFT-Instanz eingebracht werden, siehe auch „Instanzenverzeichnis“ auf Seite 26. Bei der Standardinstanz liegt *syskey* im Verzeichnis */var/openFT/std*

DIERR
: Auf der Verbindung zum Partnersystem wurde ein Datenintegritätsfehler entdeckt. Das kann entweder durch Manipulationsversuche auf der Übertragungsstrecke oder einen Fehler im Transportsystem bedingt sein. Die Verbindung wurde abgebrochen, der betroffene Auftrag aber nicht (falls er wiederanlauffähig ist).

NOKEY
: Der Partner akzeptiert keine Verbindung ohne Verschlüsselung, aber im lokalen System ist kein Schlüssel vorhanden. Es muss ein neuer Schlüssel erzeugt werden.

IDREJ
: Der Partner oder eine Zwischeninstanz akzeptiert die vom lokalen System geschickte Instanzidentifikation nicht. Es muss geprüft werden, ob die lokale Instanzidentifikation mit dem Eintrag in der Partnerliste des Partners konsistent ist.

SHORT
: Beim Partner ist ein Betriebsmittelengpass aufgetreten.

SECLEV
: Sicherheitsstufe, die dem Partnersystem zugeordnet wurde.

  1..100
  : Dem Partner ist eine feste Sicherheitsstufe zugeordnet:
    1 bedeutet die niedrigste Sicherheitsstufe (Partner ist sehr vertrauenswürdig) und 100 die höchste Sicherheitsstufe (Partner ist wenig vertrauenswürdig).

  STD Es gilt die globale Einstellung für die Sicherheitsstufe.

  B-P-ATTR
  : Die Sicherheitsstufe wird dem Partner anhand seiner Attribute zugeordnet, d.h.:
    - Sicherheitsstufe 10, wenn der Partner authentifiziert ist.
    - Sicherheitsstufe 90, wenn der Partner im Transportsystem bekannt ist und über den im Transportsystem bekannten Namen identifiziert wird.
    - Sicherheitsstufe 100 sonst, d.h. wenn der Partner nur über seine Adresse identifiziert wird.

PRI Priorität eines Partners bzgl. der Abarbeitung von Aufträgen:

  NORM
  : Normale Priorität.

  LOW Niedrige Priorität.

  HIGH Hohe Priorität.

TRACE
: globale Einstellungen für die Partner-Selektion der openFT-Überwachungsfunktion:

  FTOPT
  : Es gilt die globale Einstellung für die Partner-Selektion der openFT-Überwachungsfunktion.

  ON Die Überwachungsfunktion ist für diesen Partner eingeschaltet. Es wird jedoch nur dann ein Trace geschrieben, wenn auch die globale openFT-Überwachungsfunktion eingeschaltet ist. Details siehe Abschnitt „Partnerspezifischen Trace einschalten“ auf Seite 392.

  OFF Die Überwachungsfunktion ist für diesen Partner ausgeschaltet.

LOC gibt die Anzahl der Dateiübertragungsaufträge an, die im lokalen System eingegeben wurden und an das Partnersystem gerichtet sind.

REM gibt die Anzahl der Dateiübertragungsaufträge an, die im fernen FT-System erteilt wurden und an das lokale FT-System gerichtet sind.

P-CHK
: gibt Einstellungen für die Absenderüberprüfung und Authentifizierung an.

  FTOPT
  : Es gilt die globale Einstellung für die Absenderüberprüfung.

  STD
  : Die Überprüfung der Transportadresse ist ausgeschaltet. Es wird ausschließlich die Identifikation des Partners geprüft. Die Transportadresse des Partners wird auch dann nicht überprüft, wenn die erweiterte Absenderüberprüfung global eingeschaltet ist.

  T-A
  : Die Überprüfung der Transportadresse ist eingeschaltet. Die Transportadresse des Partners wird auch dann überprüft, wenn die Überprüfung der Transportadresse global ausgeschaltet ist. Stimmt die Transportadresse, unter der sich der Partner anmeldet, nicht mit dem Eintrag in der Partnerliste überein, dann wird der Auftrag abgelehnt.

  AUTH
  : Der Partner wird anhand seines öffentlichen Schlüssels im Verzeichnis *syskey* einer Identitätsprüfung mit kryptografischen Mitteln unterzogen („authentifiziert“). Der Partner unterstützt die Authentifizierungsstufe 2.

  !AUTH
  : Der Partner wird anhand seines öffentlichen Schlüssels im Verzeichnis *syskey* einer Identitätsprüfung mit kryptografischen Mitteln unterzogen („authentifiziert“). Der Partner unterstützt die Authentifizierungsstufe 1.

  AUTHM
  : Es muss mit Authentifizierung gearbeitet werden.

  NOKEY
  : Es liegt kein gültiger Schlüssel vom Partnersystem vor, obwohl eine Authentifizierung erforderlich ist.

ADDRESS
: Adresse des Partnersystems.

ROUTING
: Routing-Info des Partnersystems falls definiert, wird nur bei *ftshwptn -l* ausgegeben.

IDENTIFICATION
: Identifikation des Partnersystems falls definiert, wird nur bei *ftshwptn -l* ausgegeben.

INBND Zustand des Partners für Inbound-Aufträge:

ACT Inbound-Funktion ist aktiviert, d.h. fern gestellte Aufträge werden bearbeitet.

DEACT
Inbound-Funktion ist deaktiviert, d.h. fern gestellte Aufträge werden abgelehnt.

REQU-P Bearbeitungsmodus für asynchrone Outbound-Aufträge:

STD Aufträge zu diesem Partner können parallel bearbeitet werden.

SERIAL
Aufträge zu diesem Partner werden immer seriell bearbeitet.

6.43 ftshwr - Eigenschaften und Zustand von Aufträgen anzeigen

Mit dem Kommando *ftshwr* ("show request") können Sie Informationen über Dateiübertragungsaufträge anfordern. Dabei können Sie Auswahlkriterien für die Sie interessierenden FT-Aufträge angeben.

Als FT-Verwalter können Sie sich über Aufträge beliebiger Eigentümer informieren.

Format

ftshwr -h |
[-ua=<Benutzerkennung 1..32> | -ua=@a]
[-ini=l | -ini=r | -ini=lr | -ini=rl]
[-st=a | -st=w | -st=l | -st=c | -st=f | -st=h | -st=s]
[-pn=<Partner 1..200>]
[-fn=<Dateiname 1..512>]
[-gid=<globale Auftrags-Id 1..4294967295>]
[-s | -l][-csv]
[<Auftrags-Id 1..2147483647>]

Beschreibung

-h gibt die Kommandosyntax am Bildschirm aus. Weitere Angaben nach *-h* werden ignoriert.

-ua=Benutzerkennung | **-ua=@a**
Mit *-ua* legt man fest, für welche Benutzerkennung Aufträge angezeigt werden sollen.

Benutzerkennung
Sie können als Benutzer nur Ihre eigene Benutzerkennung angeben.
Als FT-Verwalter dürfen Sie hier jede beliebige Benutzerkennung angeben.

@a Als FT-Verwalter können Sie sich durch Angabe von @a Aufträge aller Benutzerkennungen anzeigen lassen.

-ua nicht angegeben
Die eigene Benutzerkennung ist das Auswahlkriterium.
Ausnahme:
Der FT-Verwalter hat das Kommando aufgerufen und dabei auch eine Auftrags-Id angegeben. In diesem Fall ist die Voreinstellung *@a*.

-ini=l | **-ini=r** | **-ini=lr** | **-ini=rl**
Mit *-ini* legen Sie fest, für welchen Initiator Sie Aufträge anzeigen wollen. Folgende Angaben sind möglich:

l (local) Nur lokal gestellte Aufträge werden angezeigt.

r (remote) Nur fern gestellte Aufträge werden angezeigt.

lr, rl (local + remote) Sowohl lokale als auch fern gestellte Aufträge werden angezeigt.

-ini nicht angegeben
Der Initiator ist nicht Auswahlkriterium (entspricht *lr* bzw. *rl*).

-st=a | **-st=w** | **-st=l** | **-st=c** | **-st=f** | **-st=h** | **-st=s**
Mit *-st* werden nur Informationen zu den Aufträgen mit dem angegebenen Status ausgegeben. Folgende Angaben sind möglich:

a (active)
Der Auftrag wird gerade ausgeführt.

w (wait)
Der Auftrag wartet auf die Ausführung.

l (locked)
Der Auftrag ist gesperrt.

c (cancelled)
Der Auftrag wurde gelöscht.

f (finished)
Der Auftrag wurde bereits ausgeführt.

h (hold)
Der bei der Auftragserteilung angegebene Startzeitpunkt ist noch nicht erreicht.

s (suspend)
Der Auftrag wurde unterbrochen, d.h. er befindet sich im Zustand SUSPEND.

-pn=Partner
Mit *-pn* können Sie einen Namen oder eine Adresse für das Partnersystem angeben, für das Sie Aufträge anzeigen wollen. Der Partner sollte so angegeben werden, wie er bei der Auftragseingabe angegeben wurde oder wie er beim Kommando *ftshwr* ohne Option *-s*, *-l* oder *-csv* ausgegeben wird. Wenn openFT zu einer angegebenen Partneradresse einen Partner in der Partnerliste findet, so zeigt *ftshwr* den Namen des Partners an, selbst wenn bei der Auftragseingabe eine Partneradresse angegeben wurde.

-fn=Dateiname

Mit *-fn* legen Sie fest, für welchen Dateinamen Aufträge angezeigt werden sollen. Es werden Aufträge angezeigt, die im lokalen System auf diese Datei zugreifen.

Es muss der Dateiname angegeben werden, der auch bei der Auftragserstellung verwendet wurde. Dieser Dateiname wird auch beim Kommando *ftshwr* ohne Option *-fn* ausgegeben.

Wildcards im Dateinamen sind nicht erlaubt.

-gid=globale Auftrags-Id

Mit *-gid* geben Sie die globale Auftrags-Identifikation eines bestimmten Auftrags an, der angezeigt werden soll. Die globale Auftrags-Identifikation ist nur für Inbound-Aufträge von openFT- und FTAM-Partnern relevant. Sie wird vom Initiator des Auftrags vergeben (Transfer-Id) und an das lokale System übermittelt.

-gid= nicht angegeben

Die globale Auftrags-Identifikation ist nicht Auswahlkriterium.

-s (sum) gibt an, dass eine Summenübersicht der Aufträge ausgegeben wird. Diese Übersicht enthält für jeden möglichen Auftragszustand (siehe Option *-st*) die Anzahl der Aufträge, die sich in diesem Zustand befinden.

-l (long) gibt an, dass die Eigenschaften der Aufträge in der ausführlichen Form ausgegeben werden.

-csv gibt an, dass die Eigenschaften der Aufträge im CSV-Format ausgegeben werden sollen. Wenn zusätzlich *-s* angegeben ist, wird die Summenübersicht im CSV-Format ausgegeben. Die Werte der Ausgabe werden durch Strichpunkte getrennt aufgelistet.

-s, *-l* und *-csv* nicht angegeben

Es werden die Attribute der Aufträge in der Standardform ausgegeben.

Auftrags-Id

Mit *Auftrags-Id* geben Sie die Identifikation eines bestimmten Auftrags an, der angezeigt werden soll. Die Auftrags-Id wird bei der Bestätigung der Auftragsannahme am Bildschirm ausgegeben, Sie können sie sich z.B. auch über das Kommando *ftshwr -l* anzeigen lassen.

Wenn Sie eine Auftrags-Id angegeben haben und die übrigen angegebenen Auswahlkriterien nicht zu dem Auftrag passen, dann wird der Auftrag nicht angezeigt und folgende Fehlermeldung ausgegeben:

```
ftshwr: Auftrag Auftrags-Id nicht gefunden
```

6.43.1 Ausgabeformat von ftshwr

6.43.1.1 Standardausgabe von ftshwr

```
$ftshwr
TRANS-ID   INI STATE PARTNER  DIR  BYTE-COUNT  FILE-NAME
65558      LOC WAIT  *PINGO   TO   0           /home1/september.pdf
196610     LOC WAIT  servus.* FROM 0           /home2/mails/memo02.txt
262146     LOC WAIT  servus.* TO   0           /home3/pic/picture10.gif
```

Beschreibung der Ausgabe

TRANS-ID
: Die Spalte TRANS-ID (Transfer Identification) enthält die Auftragsnummer, mit der openFT die Dateiübertragungsaufträge kennzeichnet. Über die Nummer TRANS-ID können Aufträge mit dem Kommando *ftcanr* gelöscht werden.

INI
: Die Spalte INI gibt den Initiator an:
LOC: Der Auftrag wurde im lokalen System gestellt.
REM: Der Auftrag wurde im fernen System gestellt.

STATE
: Die Spalte STATE gibt den Zustand und die Priorität des Auftrags an.

  Die Priorität wird hinter dem Zustandskennzeichen angezeigt. Als Anzeige ist nur *l* für "low" möglich, hat der Auftrag die Priorität *normal*, erfolgt keine Anzeige.

  Folgende Zustände sind möglich:

  ACT (active)
  : Der Auftrag wird gerade bearbeitet.

  WAIT (wait)
  : Der Auftrag wartet. In diesem Fall kann das Partnersystem (PARTNER) zusätzlich gekennzeichnet sein. Aus dieser Kennzeichnung können Sie die Ursache für den *WAIT*-Zustand entnehmen.

  LOCK (locked)
  : Der Auftrag ist für einen gewissen Zeitraum von der Bearbeitung ausgeschlossen. Dieser Zustand kann sowohl bei openFT- als auch bei FTAM-Partnern auftreten.
  Bei openFT-Partnern, z.B. wenn ein Betriebsmittelengpass vorliegt oder wenn externe Datenträger erst noch verfügbar gemacht werden müssen.
  Bei FTAM-Partnern, wenn einer der Partner über das FTAM-Protokoll eine Wartezeit bis zum nächsten Start- oder Recovery-Versuch vorschlägt, die über der normalerweise vorgesehenen Verzögerung liegt.

In diesem Fall kann das Partnersystem (PARTNER) zusätzlich gekennzeichnet sein. Aus dieser Kennzeichnung können Sie die Ursache für den *LOCKED*-Zustand entnehmen.

CANC (cancelled)
: Der Auftrag wurde im lokalen System gelöscht. Er ist aber im fernen System schon bekannt, weil z.B. der Auftrag schon einmal aktiv war. Deshalb kann der Auftrag erst nach erneutem Verbindungsaufbau zum Partner aus dem Auftragsbuch entfernt werden.

FIN (finished)
: Dieser Zustand kommt bei Aufträgen mit FTAM-Partnern vor, wenn der Auftrag beendet oder abgebrochen wurde, aber der Benutzer noch nicht über das Ende des Auftrags informiert wurde.

HOLD (hold)
: Der bei der Auftragserteilung angegebene Startzeitpunkt ist noch nicht erreicht.

SUSP (suspend)
: Der Auftrag wurde unterbrochen.

PARTNER
: Name oder Adresse des Partners, siehe auch Seite 68. Ist die Partneradresse länger als 8 Zeichen, dann wird sie auf 7 Zeichen gekürzt und durch einen Stern (*) am Ende gekennzeichnet.

  Liegt ein *WAIT*- oder *LOCKED*-Zustand vor, so finden Sie vor PARTNER folgende zusätzliche Kennzeichnungen im Auftragsbuch:

  ␣ Momentan sind keine Betriebsmittel (z.B. kein Speicher) frei.

  * Der FT-Verwalter hat die Betriebsmittel gesperrt, zum Beispiel hat er den Partner deaktiviert.

  ! Der Verbindungsaufbau zum Partnersystem ist fehlgeschlagen, der Partner ist derzeit nicht aktiv oder er kann derzeit keine weiteren Verbindungen annehmen oder ein Netzknoten ist ausgefallen. Auch möglich: Die Verbindung zum Partnersystem ist ausgefallen oder ein Datenintegritätsfehler wurde festgestellt.

  ? Es liegt ein Installations- oder Konfigurationsfehler vor (zum Beispiel ist das lokale System dem Partner nicht bekannt), die Authentifizierung eines der Partner ist fehlgeschlagen oder die Verschlüsselung ist lokal oder im Partnersystem nicht verfügbar.

DIR Die Spalte DIR gibt die Übertragungsrichtung an

TO Senden in das ferne System.

FROM
Holen aus dem fernen System.

BYTE-COUNT
Die Spalte BYTE-COUNT gibt die Anzahl der bereits gesichert übertragenen Bytes an. Der Zähler wird in regelmäßigen Abständen aktualisiert.

FILE-NAME
Name der Datei im lokalen System.

6.43.1.2 Summenausgabe von ftshwr

Bei der Summenausgabe wird eine Tabelle mit den Aufträgen in den einzelnen Auftragszuständen ausgegeben (Bedeutung siehe Spalte *Status* in der Standardausgabe):

```
ftshwr -s
 ACT   WAIT   LOCK   SUSP   HOLD    FIN      TOTAL
   3      2      0      0      0      0          5
```

6.43.1.3 Ausführliche Ausgabe von ftshwr

Beispiel für Ausgabe des Auftrags mit der Auftrags-Id 131074 in ausführlicher Form:

```
ftshwr -l 131074

TRANSFER-ID =131074      STORE  =12-05-29 11:45:27  FILESIZE=514610
   STATE    =WAIT        BYTECNT=0
   INITIATOR=LOCAL       TRANS  =TO                 PRIO    =NORM
   WRITE    =REPLACE     START  =SOON               CANCEL  =NO
   COMPRESS =NONE        DATA   =CHAR
   TRANSP   =NO          ENCRYPT=NO
   TARGFORM =BLOCK       TRECFRM=STD
   OWNER    =maier       DICHECK=NO                 RECFORM =VARIABLE
   PARTNER  =ftserv01.mycompany.net
   PARTNER-STATE = ACT
   PARTNER-PRIO  = NORM
   LOC: FILE     =/home2/memo02.txt
        TRANS-ADM=(maier)
        CCSN     =ISO8859-1
   REM: FILE     =/home/save/memo02.txt
        TRANS-ADM=(servelog)
```

Beispiel für Ausgabe des Inbound-Auftrags mit der Auftrags-Id 524410 in ausführlicher Form:

```
ftshwr -l 524410

TRANSFER-ID =524410      STORE  =12-06-14 14:33:24  FILESIZE=10485760
   STATE    =ACTIVE      BYTECNT=0                  RECSIZE =1024
   INITIATOR=REMOTE      TRANS  =FROM               PRIO    =
   WRITE    =REPLACE     START  =SOON               CANCEL  =NO
   COMPRESS =NONE        DATA   =CHAR               GLOB-ID =852520
   TRANSP   =NO          ENCRYPT=NO                 TABEXP  =NO
   OWNER    =user1       DICHECK=NO                 RECFORM =VARIABLE
   PARTNER  =ftserv.mycompany.net
   PARTNER-STATE =ACT
   PARTNER-PRIO  =NORM
   FILE     =par.file.S3.C31
   TRANS-ADM=(serv,)
```

Beschreibung der Ausgabe

TRANSFER-ID
: Auftrags-Id, mit der openFT die Dateiübertragungsaufträge kennzeichnet. Über diese Auftrags-Id können Aufträge mit dem Kommando *ftcanr* gelöscht werden.

STATE
: Zustand des Auftrags. Folgende Zustände sind möglich:

  ACTIVE
  : Der Auftrag wird gerade bearbeitet.

  WAIT
  : Der Auftrag wartet. Falls die Ursache für den WAIT-Zustand bekannt ist, können Sie weitere Informationen dazu dem Feld PARTNER-STATE entnehmen.

  LOCKED
  : Der Auftrag ist für einen gewissen Zeitraum von der Bearbeitung ausgeschlossen. Dieser Zustand kann sowohl bei openFT- als auch bei FTAM-Partnern auftreten.
  Bei openFT-Partnern, z.B. wenn ein Betriebsmittelengpass vorliegt oder wenn externe Datenträger erst noch verfügbar gemacht werden müssen.
  Bei FTAM-Partnern, wenn einer der Partner über das FTAM-Protokoll eine Wartezeit bis zum nächsten Start- oder Recovery-Versuch vorschlägt, die über der normalerweise vorgesehenen Verzögerung liegt.
  Falls die Ursache für den LOCKED-Zustand bekannt ist, können Sie weitere Informationen dazu dem Feld PARTNER-STATE entnehmen.

CANCELLED
: Der Auftrag wurde im lokalen System gelöscht. Er ist aber im fernen System schon bekannt, weil z.B. der Auftrag schon einmal aktiv war. Deshalb kann der Auftrag erst nach erneutem Verbindungsaufbau zum Partner aus dem Auftragsbuch entfernt werden.

FINISHED
: Dieser Zustand kommt bei Aufträgen mit FTAM-Partnern vor, wenn der Auftrag beendet oder abgebrochen wurde, aber der Benutzer noch nicht über das Ende des Auftrags informiert wurde.

HOLD
: Der bei der Auftragserteilung angegebene Startzeitpunkt ist noch nicht erreicht.

SUSPENDED
: Der Auftrag wurde unterbrochen.

INITIATOR
: gibt an, wo der Auftrag gestellt wurde. Folgende Ausgaben sind möglich:

LOCAL
: Der Auftrag wurde im lokalen System gestellt.

REMOTE
: Der Auftrag wurde im fernen System gestellt.

WRITE
: gibt an, ob die Zieldatei neu erzeugt, überschrieben oder erweitert wird. Folgende Werte sind möglich:

OVERWRITE (Standardwert)
: Eine bereits vorhandene Zieldatei wird überschrieben. War die Zieldatei noch nicht vorhanden, wird sie neu eingerichtet.

EXTEND
: Die übertragene Datei wird an das Ende einer bereits vorhandenen Zieldatei angehängt. War die Zieldatei noch nicht vorhanden, wird sie neu eingerichtet.

NEW
: Die Zieldatei wird neu erzeugt und beschrieben.

COMPRESS
: Angabe, ob die Datei komprimiert übertragen werden soll.

Mögliche Werte: BYTE, ZIP, NONE

TRANSP
: Angabe, ob die Datei im transparenten Dateiformat übertragen werden soll. Mögliche Werte: YES, NO

TARGFORM
: Format der Datei im Zielsystem.

  Mögliche Werte:

  STD (Standardwert)
  : Die Datei wird im gleichen Format wie im Sendesystem gespeichert.

  BLOCK
  : Die Datei wird im Blockformat gespeichert.

  SEQ
  : Die Datei wird als sequenzielle Datei gespeichert.

OWNER
: lokale Benutzerkennung

PARTNER
: Name oder Adresse des Partners, siehe auch Seite 68.

PARTNER-STATE
: Status des Partners. Mögliche Werte:

  ACT aktiviert

  DEACT
  : deaktiviert

  NOCON
  : keine Verbindung, z.B. weil der openFT-Server im fernen System nicht gestartet ist.

  INSTERR
  : Es liegt ein Installations- oder Konfigurationsfehler vor (zum Beispiel ist das lokale System dem Partner nicht bekannt), die Authentifizierung eines der Partner ist fehlgeschlagen oder die Verschlüsselung ist lokal oder im Partnersystem nicht verfügbar.

  SHORT
  : Beim Partner ist ein Betriebsmittelengpass aufgetreten.

PARTNER-PRIO
: Priorisierung des Partners bei der Abarbeitung von Aufträgen.
Mögliche Werte:

  LOW der Partner hat niedrige Priorität.

  NORM
  : der Partner hat normale Priorität.

  HIGH
  : der Partner hat hohe Priorität.

LOC Eigenschaften im lokalen System:

  FILE Dateiname im lokalen System

  TRANS-ADM
  : Zugangsberechtigung für das lokale System

  CCSN
  : CCS-Name, der im lokalen System verwendet wird. Der CCSN wird nur bei Textdateien ausgegeben.

  SUCC-PROC
  : lokale Folgeverarbeitungskommandos im Erfolgsfall
  (falls im Auftrag angegeben)

  FAIL-PROC
  : lokale Folgeverarbeitungskommandos im Fehlerfall
  (falls im Auftrag angegeben)

REM Eigenschaften im fernen System:

  FILE Dateiname im fernen System

  TRANS-ADM
  : Zugangsberechtigung im fernen System. Mögliche Werte sind:

    REMOTE-PROFILE
    : bei einem Auftrag mit FTAC-Zugangsberechtigung

    TRANS-ADM=(*Kennung*)
    : bei einem Auftrag mit *Kennung,,Kennwort*

  CCSN
  : CCS-Name, der im fernen System verwendet wird

  SUCC-PROC
  : ferne Folgeverarbeitungskommandos im Erfolgsfall
  (falls im Auftrag angegeben)

FAIL-PROC
: ferne Folgeverarbeitungskommandos im Fehlerfall
(falls im Auftrag angegeben)

STORE
: Angabe, zu welcher Zeit der Auftrag ins Auftragsbuch eingetragen wurde

BYTECNT
: Dieser Wert wird nur ausgegeben, wenn der Auftrag gerade aktiv ist oder wenn er schon einmal aktiv war und die Übertragung zur Zeit unterbrochen ist. BYTECNT gibt die Anzahl der bereits gesichert übertragenen Bytes an. Der Zähler wird regelmäßig aktualisiert.

TRANS
: gibt die Übertragungsrichtung an. Mögliche Werte sind:

  TO Das Dokument wird gesendet.

  FROM Das Dokument wird empfangen.

START
: Angabe, zu welcher Zeit der Auftrag gestartet werden soll. Folgende Angaben sind möglich:

  Datum / Uhrzeit
  : Es wird das Datum und die Uhrzeit ausgegeben, zu der der Auftrag gestartet werden soll.

  SOON
  : Der Auftrag wird so bald wie möglich gestartet.

  keine Angabe
  : Der Auftrag wurde im fernen System gestellt.

DATA Angaben zum Dateityp. Folgende Werte sind möglich:

  CHAR (Standardwert bei openFT-Partnern)
  : Die Datei enthält Text mit variablen Satzlängen.

  BIN Die Datei enthält eine unstrukturierte Folge von Binärdaten.

  USER Die Datei enthält strukturierte Binärdaten mit variabler Satzlänge.

ENCRYPT
: gibt an, ob Verschlüsselung angegeben war.
Mögliche Werte: NO / YES.

TRECFRM
: Satzformat der Datei im Zielsystem.

  Mögliche Werte:

  STD (Standardwert)
  : Die Datei wird im gleichen Satzformat wie im Sendesystem gespeichert.

  UNDEFINED
  : Die Datei wird in undefiniertem Satzformat gespeichert.

DICHECK
: gibt an, ob die Datenintegrität geprüft werden soll.
  Mögliche Werte: NO / YES.

FILESIZE
: Größe der Datei in Bytes. Ist die Ausgabe rechts mit einem "K" gekennzeichnet, so erfolgt die Ausgabe in Kilobyte. Ist diese Ausgabe mit einem "M" gekennzeichnet, so erfolgt die Ausgabe in Megabyte. Die Größe wird hier nur dann angezeigt, wenn der Auftrag bereits aktiv war. Bei Empfangs-Aufträgen wird hier nur dann ein Wert angezeigt, wenn der Partner ihn mitschickt.

PRIO Priorität des Auftrags. Folgende Ausgaben sind möglich:

  NORM
  : der Auftrag hat normale Priorität

  LOW der Auftrag hat niedrige Priorität

  keine Angabe
  : der Auftrag wurde im fernen System eingegeben

CANCEL
: Wenn bei der Auftragserteilung der "Cancel-Timer" gesetzt wurde, steht hier der Zeitpunkt, an dem der Auftrag aus dem Auftragsbuch gelöscht wird. Wurde im Auftrag keine Löschzeit angegeben, steht hier NO.

GLOB-ID
: globale Auftrags-Identifikation, wird nur bei Inbound-Aufträgen von openFT- und FTAM-Partnern angezeigt (INITIATOR=REMOTE). Sie stimmt mit der Auftrags-Identifikation (=TRANSFER-ID) auf der Initiator-Seite überein.

RECFORM
: Satzformat.
  Mögliche Werte: UNDEFINED, VARIABLE, FIX

RECSIZE
: maximale Satzlänge, falls angegeben.

DIAGCODE

Diese Zeile ist normalerweise leer.
Andernfalls liefert sie weitere Diagnoseinformationen zu Betriebszuständen und enthält dann einen CMX-Returncode oder einen FTAM- bzw. openFT-Diagnosecode. Die Formate für openFT-Diagnosecodes sind `NEBFnnnn` (NEABF) bzw. `NEBDnnnn` (NEABD). Die folgenden openFT-Diagnosecodes sind definiert:

Wert	Bedeutung
0	Keine Ursache angegeben.
1	Es kommt zu einem normalen Verbindungsaufbau.
2	Es herrscht ein Betriebsmittelengpass.
3	Es herrscht ein Betriebsmittelengpass, die Verbindung wird später von der ablehnenden Instanz aufgebaut.
4	Die Initialisierung ist nicht abgeschlossen.
5	Es ist ein SHUTDOWN in Durchführung.
6	Die anfordernde Instanz ist unbekannt.
7	Es ist ein Protokollfehler aufgetreten.
8	Es ist ein Transportfehler aufgetreten.
9	Es ist ein Systemfehler aufgetreten.
10	Dieser Code ist reserviert für SN77309 Teil 5.
11	Die Verbindung wird ohne Verschlüsselung nicht akzeptiert.

Das Format für FTAM-Diagnosecodes ist `FTAMnnnn`. Als FTAM-Diagnosecodes sind die Werte aus der ISO-Norm 8571-3 möglich. Einen Auszug der möglichen Diagnosecodes aus der Norm finden Sie im gleichlautenden Abschnitt im Benutzerhandbuch.

Folgende Werte werden nur bei FTAM-Partnern ausgegeben:

STOR-ACCOUNT

Abrechnungsnummer

Wird nur ausgegeben, wenn sie vom Benutzer angegeben wurde.

AVAILABILITY

Verfügbarkeit

Folgende Werte sind möglich: IMMEDIATE, DEFERRED

Wird nur ausgegeben, wenn sie vom Benutzer angegeben wurde.

ACCESS-RIGHTS
: Zugriffsmodus

  Als Werte sind Kombinationen aus r, i, p, x, e, a, c, d möglich. Wird nur ausgegeben, wenn sie vom Benutzer angegeben wurde.

LEGAL-QUAL
: Rechtliche Bestimmung

  Wird nur ausgegeben, wenn das lokale System Initiator ist und sie vom Benutzer angegeben wurde.

6.44 ftstart - Asynchronen openFT-Server starten

Mit diesem Kommando wird der asynchrone openFT-Server gestartet. Dieser bearbeitet alle im Auftragsbuch gespeicherten Aufträge sowie alle Inbound-Aufträge.

Mit dem Start des asynchronen openFT-Servers werden implizit die Schutzbiteinstellungen für Dateien festgelegt, die bei Inbound-Aufträgen neu angelegt werden. Es gelten die Einstellungen der Shell, unter der Sie *ftstart* eingegeben haben. Näheres siehe Abschnitt „Schutzbiteinstellung für neu angelegte Dateien“ auf Seite 59.

Ein Beenden mit Neustart des asynchronen openFT-Servers ist z.B. dann notwendig, wenn Sie zwischen dem Betrieb mit CMX und ohne CMX umschalten möchten.

Für openFT auf Solaris beachten Sie bitte den Abschnitt „Solaris SMF“ auf Seite 41.

Format

ftstart [-h]

Beschreibung

-h gibt die Kommandosyntax am Bildschirm aus.

6.45 ftstop - Asynchronen openFT-Server stoppen

Mit diesem Kommando wird der asynchrone openFT-Server beendet. Danach werden keine Inbound-Aufträge und keine lokal gestellten Asynchronaufträge mehr bearbeitet, d.h.:

– Inbound-Aufträge werden zurückgewiesen

– lokal gestellte Asynchronaufträge werden im Auftragsbuch gespeichert.

Nach Erteilung des Kommandos *ftstop* wird der asynchrone openFT-Server erst dann beendet, wenn sich alle Server-Prozesse beendet haben. Dies kann einige Minuten dauern, wenn zum Beispiel der Verbindungsabbau durch Leitungsprobleme verzögert wird.

Nach erneutem Start des asynchronen openFT-Servers werden die Aufträge, die im Auftragsbuch stehen, normal bearbeitet. Für Aufträge, die durch die Beendigung des asynchronen openFT-Servers abgebrochen wurden, wird ein Wiederanlauf durchgeführt, wenn der Partner diese Funktion unterstützt.

Für openFT auf Solaris beachten Sie bitte den Abschnitt „Solaris SMF“ auf Seite 41.

Format

ftstop [-h]

Beschreibung

-h gibt die Kommandosyntax am Bildschirm aus.

6.46 ftupdi - Instanzenverzeichnis aktualisieren

Mit *ftupdi* können Sie einen Instanzdateibaum, der mit openFT V10.0 oder V11.0 erstellt wurde, so aktualisieren, dass er mit openFT V12.0 weiter verwendet werden kann. Die Einstellungen der Betriebsparameter, FTAC-Berechtigungssätze und FTAC-Berechtigungsprofile sowie die Logging-Sätze bleiben erhalten.

Eventuell noch vorhandene Aufträge für diese Instanz gehen verloren.

Format

ftupdi -h | <Verzeichnis 1..128>

Beschreibung

-h gibt die Kommandosyntax am Bildschirm aus. Weitere Angaben nach *-h* werden ignoriert.

Verzeichnis
: Hier geben Sie das Verzeichnis an, in dem sich der Instanzdateibaum der zu aktualisierenden Instanz befindet.

Meldungen des ftupdi-Kommandos

Konnte *ftupdi* nicht ordnungsgemäß ausgeführt werden, dann wird eine selbsterklärende Meldung ausgegeben; der Exitcode ist dann ungleich 0.

Beispiel

Der FT-Verwalter will das Verzeichnis der Instanz *hugo* aktualisieren.

```
ftupdi /var/openFT/.hugo
```

6.47 ftupdk - Öffentliche Schlüssel aktualisieren

Mit *ftupdk* können Sie die öffentlichen Schlüsseldateien bestehender Schlüsselpaarsätze aktualisieren.

Dadurch können Sie beispielsweise aktualisierte Kommentare aus der Datei *syspkf.comment* in bestehende öffentliche Schlüsseldateien übernehmen oder versehentlich gelöschte öffentliche Schlüsseldateien eines Schlüsselpaarsatzes ersetzen.

Format

ftupdk [-h]

Beschreibung

-h gibt die Kommandosyntax am Bildschirm aus.

Beispiel

Der Name des FT-Verwalters soll in die öffentlichen Schlüsseldateien übernommen werden. Zunächst wird mit einem Editor die Datei *syspkf.comment* bearbeitet. Diese Datei liegt im Unterverzeichnis *config* des Instanzenverzeichnisses, siehe Kommando *ftcrei* auf Seite 190.

Die Datei könnte z.B. nur folgende Zeile enthalten:

```
FT-Verwalter: Werner Wernersen, Tel. 12345
```

Das Kommando lautet:

```
ftupdk
```

Das Kommando wird ohne Fehlermeldung ausgeführt. Anschließend steht die Information als Kommentarzeile am Anfang aller öffentlichen Schlüsseldateien *syspkf...* .

6.48 install.ftam - Installation von openFT-FTAM

Mit dem Kommando *install.ftam* können Sie openFT-FTAM installieren und deinstallieren. Die Installation ist nur erlaubt, wenn eine openFT-FTAM-Lizenz vorliegt.

Das Kommando *install.ftam* steht in dem Verzeichnis */opt/openFT/bin/ftbin*.

Format

install.ftam -h | -i | -d

Beschreibung

-h gibt die Kommandosyntax am Bildschirm aus. Weitere Angaben nach *-h* werden ignoriert.

-i openFT-FTAM wird installiert.

-d openFT-FTAM wird deinstalliert.

6.49 install.ftp - Installation von openFT-FTP

Mit dem Kommando *install.ftp* können Sie openFT-FTP installieren und deinstallieren. Die Installation ist nur erlaubt, wenn eine openFT-FTP-Lizenz vorliegt.

Das Kommando *install.ftp* steht in dem Verzeichnis */opt/openFT/bin/ftbin*.

Format

install.ftp -h | -i | -d

Beschreibung

-h gibt die Kommandosyntax am Bildschirm aus. Weitere Angaben nach *-h* werden ignoriert.

-i openFT-FTP wird installiert.

-d openFT-FTP wird deinstalliert.

7 Was tue ich, wenn ...

... die Meldung „Lokale Datei inkonsistent“ ausgegeben wird.

Das kann bedeuten, dass

– eine Binärdatei versehentlich als Textdatei übertragen wurde (Option *-b* verwenden!)

– eine Textdatei zu lange Sätze enthält (Option *-r* verwenden!)

... die Meldung „Fernes System nicht verfügbar“ ausgegeben wird.

Das kann bedeuten, dass

– die in der Partnerliste, dem TNS oder dem Hosts-Eintrag angegebene Partneradresse nicht stimmt. Bei BS2000-Kopplungen sollte überprüft werden, ob ein BCMAP-Eintrag für $FJAM mit der Portnummer 1100 im BS2000-Partner gemacht wurde (dieser wird ab openFT V9.0 für BS2000/OSD automatisch erstellt).

– im Partnersystem der asynchrone openFT-Server nicht gestartet ist.

– eine Firewall im Partnersystem keine Verbindung zulässt.

Sie können versuchen, ob Sie mit dem Kommando *ftping <partneradresse>* eine Rückmeldung vom fernen openFT-System erhalten.

Bitte beachten Sie, dass *ftping* nur für den internen Einsatz vorgesehen ist und keine garantierte Schnittstelle darstellt.

... das eigene System von Partnersystemen nicht erreichbar ist.

Es sollten folgende Fehlerquellen überprüft werden:

– wurde der asynchrone openFT-Server gestartet?

– entspricht die lokale Adresse den Standardeinstellungen (*ftmodo -openft=@s*) oder wurde sie verändert?

– wurde im Partnersystem die Portnummer 1100 adressiert ? Im BS2000 wird automatisch von openFT ein BCMAP erstellt. Damit dies erfolgreich ist, dürfen keine alten BCMAP-Einträge vorhanden sein.

– ist die Firewall für die Anwendung openFT freigeschaltet?

... die Meldung „Lokales System im fernen System unbekannt“ ausgegeben wird.

Das bedeutet, dass Ihr Partnersystem Ihr lokales System nicht als Partner akzeptiert. Dazu sollten Sie auf dem Partnersystem prüfen:

– Sind dynamische Partner ausgeschlossen und es existiert kein oder kein passender Eintrag in der Partnerliste für Ihr lokales System?

  Lösungsmöglichkeiten:
  – Im Partnersystem Ihr lokales System in die Partnerliste eintragen oder
  – im fernen System den Partnerlisteneintrag überprüfen, z.B. ob die gesendete Instanzidentifikation mit der eingetragenen Instanzidentifikation übereinstimmt, oder
  – dynamische Partner zulassen

– Schlägt die Partneradressüberprüfung für Ihr lokales System fehl?

Auf dem lokalen System sollten Sie die Einstellungen der Betriebsparameter *Identifikation* und *Prozessorname* überprüfen.

... die Meldung „Fernes System xy unbekannt“ ausgegeben wird.

Das kann bedeuten, dass

– Sie für das Partnersystem den Eintrag in der Partnerliste, die TNS-Einträge oder die Einträge in der Hosts-Datei ändern müssen,

– ein TNS-Eintrag verwendet wird, obwohl die TNS-Nutzung deaktiviert ist,

– dynamische Partner deaktiviert sind und der Partner nicht in der Partnerliste eingetragen ist.

... das BS2000 nicht erreicht werden kann

Wenn Ihr lokales System im BS2000 unbekannt ist, geben Sie im BS2000 das Kommando *add-ft-partner* ein.

Wenn Sie die Meldung "Fernes System nicht verfügbar" erhalten, prüfen Sie ob eine der folgenden Ursachen vorliegt:

– Betriebsmittelengpass im fernen System
– Fernes FT-System nicht gestartet
– BCIN fehlt
– Keine Netzverbindung (z.B. bei TCP/IP-Kopplung Überprüfung mit dem Kommando *ping*)
– Nameserver-Eintrag fehlt oder ist fehlerhaft

... der Name des Partners in den Logging-Sätzen fehlt

Tragen Sie den Partner in die Partnerliste, in den DNS, in die */etc/hosts* oder in den TNS ein.

... die Logging-Funktion sich nicht aufrufen lässt, also die Logging-Datei nicht mehr lesbar bzw. inkonsistent ist

Gründe hierfür können sein:

1. Systemabsturz oder *kill* auf den openFT-Prozess, während Logging-Sätze geschrieben werden.
2. Volles Dateisystem beim Schreiben auf die Logging-Datei.

Die einzige Möglichkeit besteht darin, openFT zu beenden (*ftstop*) und die betroffene Logging-Datei zu löschen.

Sie können den vollen Pfadnamen der betroffenen Logging-Datei kann mit dem Kommando *ftshwl -llf -plf=0* ermitteln, vorausgesetzt, die Logging-Datei wurde nach Auftreten des Problems noch nicht gewechselt.

Dabei gehen alle Logging-Sätze der betroffenen Datei verloren.

Das explizite Anlegen einer leeren Logging-Datei ist nicht sinnvoll, da diese wegen fehlender Headerinformationen ebenfalls inkonsistent ist.

Um Platzproblemen zuvor zu kommen, sollten Sie

– regelmäßig die Logging-Datei wechseln (*ftmodo -lf=c*),
– alte Offline-Logging-Dateien auf einem anderen Rechner/Speichermedium sichern
– und anschließend die alten Offline-Logging-Dateien auf dem openFT-Rechner löschen.

Alternative: Aktivieren Sie das automatische Löschen von Logging-Sätzen (*ftmodo*, Optionen *-ld, -lda, -ldd* und *-ldt*).

... der Zugriff auf die Berechtigungssatz- und Berechtigungsprofildatei Fehler bringt oder wenn diese Datei defekt ist

Gründe hierfür können sein:

1. Manueller Zugriff auf die Dateien *sysfsa.dat* und *sysfsa.idx*. Diese Dateien befinden sich im Verzeichnis *config* der jeweiligen openFT-Instanz, siehe „Instanzenverzeichnis“ auf Seite 26. Bei der Standardinstanz lautet der Pfadname dieser Dateien:

   /var/openFT/std/config/sysfsa.dat

   und

   /var/openFT/std/config/sysfsa.idx.
2. Systemabsturz oder *kill* auf den openFT-Prozess bei geöffneten *sysfsa.**

3. Volles Dateisystem bei ISAM-Zugriff

Bei Fall 2 und 3 hinterlässt ISAM i.d.R. eine unbrauchbare Indexdatei.

Lösungsmöglichkeiten:

– Versuch mit Export/Import:
  Exportieren Sie mit *ftexpe* die Daten in eine Sicherungsdatei.
  Beenden Sie dann den openFT-Server mit *ftstop*, löschen Sie *sysfsa.dat* und *sysfsa.idx* und starten Sie openFT wieder mit *ftstart*. Importieren Sie die Daten mit *ftimpe* aus der Sicherungsdatei.

– Versuchen Sie, die ISAM-Indexdatei per *dcheck* wieder herzustellen (hier im Beispiel mit der Standardinstanz):

  ```
  /opt/openFT/bin/ftbin/dcheck -b /var/openFT/std/config/sysfsa
  ```

  Eventuell muss die Indexdatei zuvor explizit gelöscht werden:

  – Bei leerer Datendatei *sysfsa.dat* gehen keine Daten verloren, somit können beide ISAM-Dateien bei gestopptem openFT gelöscht und vor *ftstart* per *ftshwa* initialisiert werden.

  – Enthält die Datendatei bereits Änderungen der Berechtigungssätze und/oder -profile, dann geben Sie folgende Kommandos ein:

    ```
    cd /var/openFT/std/config
    ftstop
    mv sysfsa.dat sav.sysfsa.dat && rm sysfsa.idx
    ftshwa >/dev/null
    rm sysfsa.dat && mv sav.sysfsa.dat sysfsa.dat
    /opt/openFT/bin/ftbin/dcheck -b sysfsa
    ftstart
    ```

    Erläuterung:
    Eine defekte *sysfsa.idx* muss neu erzeugt werden. Hierzu wird die zu erhaltende *sysfsa.dat* zuerst gesichert. Per *ftshwa* wird eine neue *sysfsa.dat* erzeugt, sofort wieder gelöscht und durch die gesicherte *sysfsa.dat* ersetzt, wodurch ein wieder verwendbares Paar von Dateien existiert.

– Wenn auch dieser Versuch nicht zum Erfolg führt, müssen Sie die Berechtigungssatz- und Berechtigungsprofildatei löschen und mit neuen Einträgen einen konsistenten Stand erzeugen.

... ich bei einem ncopy-Auftrag keine freie Transportverbindung bekomme

– Prüfen Sie die Partneradresse im Partnereintrag oder in der Partnerliste.

– Wenn Sie mit TNS arbeiten: prüfen Sie Ihre TNS-Einträge und prüfen Sie, ob die TNS-Nutzung und der Betrieb mit CMX aktiviert sind: Bei *ftshwo* muss bei USE TNS und USE CMX jeweils der Wert YES angezeigt werden. Andernfalls aktivieren Sie die TNS-Nutzung und den Betrieb mit CMX mit *ftmodo -tns=y -cmx-y*.

– Prüfen Sie die Adresseinstellungen der Betriebsparameter.

... die openFT-Meldung „Ferne Zugangsberechtigung ungültig“ erscheint

Aus Datenschutzgründen unterscheidet diese Meldung auf der Initiatorseite nicht zwischen den verschiedenen möglichen Gründen für die Ablehnung. Diese Informationen sind nur über das openFT-Logging des Responder-Systems verfügbar.

... Aufträge im Zustand „WAIT“ stehen bleiben?

– prüfen Sie, ob der asynchrone openFT-Server im lokalen System gestartet ist

– prüfen Sie, ob der openFT bzw. der asynchrone openFT-Server im fernen System gestartet ist

Mit *ftshwr -l* können Sie weitere Ursachen ermitteln.

... das Löschen eines Auftrages im openFT Explorer auffällig lange dauert (ca. 1 Minute)

Das kann bedeuten,

– dass für den Auftrag, der gelöscht werden soll, eine Mail bei Beendigung des Auftrages angefordert wurde
– und dass es wegen eines Konfigurationsproblems der Mailfunktion des Unix-Systems ca. 1 Minute dauert, um eine Mail abzusenden.

Lösung:

Auf eine Mail bei Beendigung des Auftrages verzichten, d.h. beim *ft*-Kommando die Option *-m=n* angeben (oder *-m* weglassen da Standardwert ab V10.0). Aufträge, die aus dem openFT Explorer gestartet werden, fordern nie eine Beendigungsmail an.

... in Linux-Systemen im openFT Explorer die linke Maustaste nicht wie gewünscht funktioniert

Dies kann daran liegen, dass die Funktion der NumLock-Taste mit Xfree und KDE (auf größeren SuSE-Linux-Systemen) per Generierung anders eingestellt wurde.

Dies führt zu Problemen, wenn die NumLock-Taste als Alt-Feststelltaste fungiert: aus Klick wird Alt-Klick, aus Doppelklick wird Alt-Doppelklick.

Das Problem kann der Systemverwalter durch Umschalten der NumLock-Taste beheben, ggf. ist im BIOS die NumLock-Funktionalität einstellbar. Mit dem Kommando *xmodmap* können die Tastenbelegungen überprüft und geändert werden.

Performance-Hinweis

Wenn Sie im Betrieb mit CMX den TNS verwenden (*ftmodo -tns=y*), dann sollten Sie bei den TNS-Einträgen in Unix-Systemen das Protokoll RFC1006 einstellen, da das RFC1006-Protokoll deutlich performanter ist als die Kommunikation über LANINET. Im BS2000 sollte ohne BCMAP Einträge gearbeitet werden. Werden trotzdem BCMAP Einträge benötigt, so gilt: Ist der PTSEL-I-Eintrag vorhanden, so wird RFC1006 verwendet.

Beim Betrieb ohne CMX wird immer das RFC1006-Protokoll verwendet.

7.1 Verhalten im Fehlerfall

Sollte trotz aller Sorgfalt einmal ein Fehler auftreten, den weder der FTAC-Verwalter noch der Systemverwalter beheben kann, wenden Sie sich bitte an den Kundendienst von Fujitsu Technology Solutions. Um die Fehlersuche zu erleichtern, erstellen Sie bitte die folgenden Unterlagen:

- Genaue Beschreibung der Fehlersituation und Angabe, ob der Fehler reproduzierbar ist.
- Versionsangabe des File-Transfer-Produkts im eigenen System.
- Versionsangabe des File-Transfer-Produkts im Partnersystem, sowie das Betriebssystem des Partnersystems.
- Diagnose-Information (diese wird mit dem openFT-Kommando *ftshwd* erzeugt).
- Gegebenenfalls die FTAC-, FT- und ADM-Logging-Sätze (diese werden mit dem FT-Kommando *ftshwl* zur Verfügung gestellt).
- Gegebenenfalls die openFT-Trace-Datei.
- Bei Fehlern im Zusammenhang mit einem bestimmten Berechtigungsprofil: einen Ausdruck des Profils (*ftshwp␣profilname␣-l*) und einen Ausdruck der Berechtigungssätze (*ftshwa␣@a*).
- Die Version und die Variante des Betriebssystems.
- Die Version des Kommunikationssystems (CMX, ...).
- Gegebenenfalls Prozesstabelle (*ps*-Kommando).

Außerdem können Sie durch Aufruf der Prozedur */opt/openFT/bin/ftbin/ftdiaginfo* die Aufsammlung diverser Diagnosedaten starten. Diese Prozedur erzeugt die Datei *ftdiaginfo.tgz* (komprimierte tar-Datei) und legt sie im aktuellen Verzeichnis ab. Schicken Sie diese Datei dann mit der Fehlerbeschreibung an den zuständigen Ansprechpartner.

8 Diagnose

Dieses Kapitel beschreibt, wie Sie Trace-Dateien erstellen und auswerten können. Weitere Diagnoseinformationen erhalten Sie mit Hilfe des Kommandos „ftshwd - Diagnoseinformation ausgeben“ auf Seite 301.

Am Schluss dieses Kapitels finden Sie Codetabellen, um Umcodierungsfehler diagnostizieren zu können.

8.1 Trace-Dateien

Zur Unterstützung der Fehlerdiagnose können Sie einen Überwachungszustand ein- und ausschalten.

8.1.1 Trace-Funktion ein-/ausschalten

Die Trace-Funktion können Sie wie folgt steuern:

– mit dem Kommando *ftmodo -tr=n/f* schalten Sie die Trace-Funktion generell ein oder aus.

– mit dem Kommando *ftmodo -trp -trr* können Sie bei eingeschaltetem Trace nach Protokoll-Typ und Auftragsart selektieren.

– mit dem Kommando *ftmodo -tro=b* wird nur ein Minimal-Trace erstellt.

– mit dem Kommando *ftmodo -troll* steuern Sie den Trace-Umfang für die unteren Protokollschichten.

  Damit ist es möglich, im Betrieb mit CMX auch CMX-Trace-Dateien im Verzeichnis der Instanz abzuspeichern. Diese können z.B. mit dem openFT Explorer wie die Trace-Dateien von openFT ausgewählt und angezeigt werden.

Diese Einstellungen können Sie auch im openFT Explorer vornehmen (*Administration - Betriebsparameter - Überwachung*).

Zusätzlich können Sie einen partnerspezifischen Trace erstellen, siehe Seite 392.

Bei eingeschaltetem Überwachungszustand werden die Diagnosedaten in Trace-Dateien geschrieben. Die Trace-Dateien befinden sich im Dateiverzeichnis *traces* der jeweiligen openFT-Instanz, siehe „Instanzenverzeichnis“ auf Seite 26. Bei der Standardinstanz lautet der Pfadname */var/openFT/std/traces*.

Nach Beendigung der Diagnose sollten Sie aus Performancegründen den Überwachungszustand wieder ausschalten. Die Trace-Dateien können beliebig groß werden, da sie nicht zyklisch überschrieben werden. Es ist jedoch möglich, die Trace-Dateien mit dem Kommando *ftmodo -tr=c* zu schließen und neue Trace-Dateien zu öffnen. Diese Funktion steht auch im openFT Explorer zur Verfügung (Schaltfläche *Datei wechseln* auf dem Registerblatt *Überwachung*).

Partnerspezifischen Trace einschalten

Wenn Sie nur Traces zu einem speziellen Partner aufzeichnen möchten, dann gehen Sie wie folgt vor:

1. Schalten Sie die Trace-Funktion für den gewünschten Partner ein, z.B. mit *ftmodptn partner1 -tr=n*.
2. Schalten Sie den Trace für die Partnertypen aus, z.B. mit *ftmodo -trp=*.
3. Schalten Sie die allgemeine Trace-Funktion ein, z.B. mit *ftmodo -tr=n*.

8.1.2 Trace-Dateien ansehen

Trace-Dateien können Sie entweder direkt über den openFT Explorer ansehen oder nach Aufbereiten mit dem Kommando *fttrace* mit einem Editor öffnen.

Dateien mit der Endung *.fttf* werden direkt aufbereitet und im openFT Editor angezeigt, wenn Sie im openFT Explorer auf eine solche Datei doppelklicken.

Dateien mit der Endung *.fttf* sind Protokolltrace-Dateien. Ihre Namen beginnen mit *Y* oder *S*. Die Namen der Trace-Dateien haben folgendes Format:

– Y*oddhhmm*.S*ssccc*.P*ppppp*.fttf
Protokolltrace-Dateien von synchronen Outbound-Aufträgen.

– S*oddhhmm*.S*ssccc*.I000.fttf
Protokolltrace-Dateien des Kontrollprozesses.

– S*oddhhmm*.S*ssccc*.I*iii*.fttf
Protokolltrace-Dateien der Serverprozesse, die asynchrone Outbound-Aufträge sowie Inbound-Aufträge abwickeln.

Erläuterung zu den Protokolltrace-Dateien

oddhhmm.S*ssccc*
: gibt den Erzeugungszeitpunkt der Protokolltrace-Datei an.
Dabei bezeichnet *o* den Monat (1 = Januar, 2 = Februar, ... A = Oktober, B = November, C = Dezember), *dd* den Tag, *hhmm* die Uhrzeit in Stunden (hh) und Minuten (mm), *ssccc* die Uhrzeit in Sekunden (*ss*) und Millisekunden (*ccc*).

ppppp
: gibt die Prozess-Id der Protokolltrace-Datei beim Typ=Y an.

iii
: ist der Index des Serverprozesses (Typ S), beginnend mit 001.

Trace-Dateien bei Fehlern

– Kann eine Trace-Datei wegen Speicherengpass nicht fehlerfrei geschrieben werden, dann wird eine Meldung ausgegeben.

– Kann ein Satz einer Serverprozess-Trace-Datei wegen Verstoßes gegen die maximale Satzlänge nicht geschrieben werden, dann wird die Trace-Datei geschlossen und die nachfolgenden Sätze werden in eine neue Folgedatei mit dem Zusatz-Suffix .L*iii* geschrieben, z.B.:
S8101010.S33222.I001.fttf (erste Trace-Datei)
S8101010.S33222.I001.L001.fttf (Folgedatei)

8.1.3 Trace-Dateien aufbereiten mit fttrace

Mit dem Kommando *fttrace* können Sie openFT-Trace-Dateien für alle Protokolle auswerten (openFT-, FTAM- und FTP-Protokoll).

Format

```
fttrace -h |
        [ -d ]
        [ -sl=n | -sl=l | -sl=m | -sl=h ]
        [ -cxid=<context id> ]
        [ -f=hh:mm:ss ]
        [ -t=hh:mm:ss ]
          <tracefile>  [<tracefile> ... ]
```

Beschreibung

-h gibt die Kommandosyntax am Bildschirm aus. Weitere Angaben nach *-h* werden ignoriert.

-d gibt an, dass die Trace-Dateien im sedezimalen Format (Dumpformat) ausgegeben werden sollen. Dies wirkt jedoch nicht beim FTP-Protokoll.

Wenn Sie *-d* nicht angeben, werden die Dateien in abdruckbarer Form ausgegeben, Standardwert.

-sl=n | **-sl=l** | **-sl=m** | **-sl=h**
legt die Sicherheitsstufe für die Ausgabe fest, wenn die Dateien in abdruckbarer Form ausgegeben werden (siehe auch Hinweis):

n (no) keine Sicherheitsanforderung, d.h. es werden alle Daten ausgegeben, auch Kennungen, Zugangsberechtigungen, Passwörter, Dateinamen usw.

l (low) Passwörter werden mit XXX überschrieben.

m (medium)
Passwörter, Benutzerkennungen, Zugangsberechtigungen, Abrechnungsnummern und Folgeverarbeitungskommandos werden mit XXX überschrieben. Standardwert, wenn *-sl* nicht angegeben wird.

h (high)
Passwörter, Benutzerkennungen, Zugangsberechtigungen, Abrechnungsnummern, Folgeverarbeitungskommandos und Dateinamen werden mit XXX überschrieben.

Bei der Ausgabe im Dumpformat (*-d*) gilt unabhängig von der Angabe in *-sl* immer die niedrigste Sicherheitsstufe (*-sl=n*), da die Trace-Daten ohne weitere Interpretation und Auswertung ausgegeben werden und diese deshalb auch Benutzerkennungen und Kennworte im Klartext enthalten können.

-cxid=context id
: Selektiert die Trace-Einträge nach der Context-Id. Wenn Sie *-cxid* weglassen oder nur *-cxid=* ohne Context-Id angeben, dann werden alle Trace-Einträge ausgegeben.

-f=hh**:**mm**:**ss (from)
: Gibt den Zeitpunkt an, von dem an Trace-Einträge in der Trace-Datei ausgewertet werden sollen.
Sie geben den Zeitpunkt im Format Stunden:Minuten:Sekunden an (jeweils 2-stellig).

  Wenn Sie keinen Startzeitpunkt festlegen, werden Trace-Einträge von Anfang an ausgegeben.

-t=hh**:**mm**:**ss (to)
: Gibt den Zeitpunkt an, bis zu dem Trace-Einträge in der Trace-Datei ausgewertet werden sollen.
Sie geben den Zeitpunkt im Format Stunden:Minuten:Sekunden an (jeweils 2-stellig).

  Wenn Sie keinen Endzeitpunkt festlegen, werden die Trace-Einträge bis zum Ende ausgegeben.

tracefile
: Name(n) der Trace-Datei(en), die Sie auswerten möchten. Sie können mehrere Trace-Dateien angeben, die Benutzung von Wildcards ist erlaubt.

8.2 Code-Tabellen

8.2.1 Code-Tabelle EBCDIC.DF.04

unteres Halbbyte \ oberes Halbbyte	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0					SP	&	-	ø	Ø	°	µ	¢	ù	¦	Ù	0
1					NBSP	é	/	É	a	j	¯	£	A	J	÷	1
2					â	ê	Â	Ê	b	k	s	¥	B	K	S	2
3					ä	ë	Ä	Ë	c	l	t	•	C	L	T	3
4					à	è	À	È	d	m	u	©	D	M	U	4
5					á	í	Á	Í	e	n	v	§	E	N	V	5
6					ã	î	Ã	Î	f	o	w	¶	F	O	W	6
7					å	ï	Å	Ï	g	p	x	1/4	G	P	X	7
8					ç	ì	Ç	Ì	h	q	y	1/2	H	Q	Y	8
9					ñ	ß	Ñ	¨	i	r	z	3/4	I	R	Z	9
A					`	!	^	:	«	ª	¡	¬	SHY	1	2	3
B					.	$	,	#	»	º	¿	[	ô	û	Ô	{
C					<	*	%	@	ð	æ	Ð	\	ö	ü	Ö	Ü
D					(	)	_	'	ý	¸	Ý	]	ò	Û	Ò	}
E					+	;	>	=	þ	Æ	Þ	´	ó	ú	Ó	Ú
F					|		?	“	±	¤	®	×	õ	ÿ	Õ	~

Code-Tabelle EBCDIC.DF.04 (Zeichensatz entsprechend ISO-8859-1)

8.2.2 Code-Tabelle ISO 8859-1

unteres Halbbyte \ oberes Halbbyte	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0			SP	0	@	P	`	p			NBSP	°	À	Ð	à	ð
1			!	1	A	Q	a	q			¡	±	Á	Ñ	á	ñ
2			"	2	B	R	b	r			¢	²	Â	Ò	â	ò
3			#	3	C	S	c	s			£	³	Ã	Ó	ã	ó
4			$	4	D	T	d	t			¤	´	Ä	Ô	ä	ô
5			%	5	E	U	e	u			¥	µ	Å	Õ	å	õ
6			&	6	F	V	f	v			¦	¶	Æ	Ö	æ	ö
7			'	7	G	W	g	w			§	•	Ç	×	ç	÷
8			(	8	H	X	h	x			¨	¸	È	Ø	è	ø
9			)	9	I	Y	i	y			©	¹	É	Ù	é	ù
A			*	:	J	Z	j	z			ª	º	Ë	Ú	ê	ú
B			+	;	K	[	k	{			«	»	Ê	Û	ë	û
C			,	<	L	\	l	|			¬	1/4	Ì	Ü	ì	ü
D			-	=	M	]	m	}			SHY	1/2	Í	Ý	í	ý
E			.	>	N	^	n	~			®	3/4	Î	Þ	î	þ
F			/	?	O	_	o				¯	¿	Ï	ß	ï	ÿ

Code-Tabelle ISO 8859-1

9 Anhang

Dieses Kapitel enthält Informationen zu

- CSV-Ausgaben der Administrationskommandos
- CMX-Kommandos
- TNS-Einträgen
- Einsatz von openFT im Cluster
- Exitcodes zu Administrationskommandos

9.1 Struktur der CSV-Ausgaben

9.1.1 Ausgabeformat

Die Form der Ausgabe entspricht bei allen Kommandos folgenden Regeln:

– Jeder Datensatz wird als eigene Zeile ausgegeben. Ein Datensatz enthält alle Informationen über ein Objekt, das angezeigt werden soll.

– Die erste Zeile ist eine Überschrift und enthält die Feldnamen der jeweiligen Spalten. **Garantiert werden nur die Feldnamen, nicht die Reihenfolge der Felder in einem Datensatz.** Die Reihenfolge der Spalten wird also durch die Reihenfolge der Feldnamen in der Überschriftenzeile bestimmt.

– Beim Kommando *ftshwe* werden nacheinander zwei Tabellen jeweils mit eigener Überschrift ausgegeben. Ist eine der Tabellen leer, so entfällt auch die entsprechende Überschrift.

– Innerhalb einer Ausgabezeile werden Felder durch Semikolon ";" voneinander getrennt.

Folgende Datentypen werden in der Ausgabe unterschieden:

– Number

  Ganze Zahl

– String

  Da das Zeichen ";" in der CSV-Ausgabe ein Metazeichen ist, wird Text – für den Fall, dass ";" darin vorkommt – in Anführungszeichen (") eingeschlossen. Anführungszeichen innerhalb eines Textfeldes werden verdoppelt, um sie von Textbegrenzern unterscheiden zu können. Beim Importieren in ein Programm werden diese Verdopplungen automatisch wieder rückgängig gemacht und die Textbegrenzer entfernt. Schlüsselworte werden in Großbuchstaben mit einem Stern (*) beginnend ausgegeben und nicht in Anführungszeichen eingeschlossen.

– Date

  Datum und Zeit werden in der Form yyyy-mm-dd hh:mm:ss ausgegeben. In einigen Fällen wird nur die Kurzform yyyy-mm-dd ausgegeben, d.h. das Datum alleine.

– Time

  Die Uhrzeit wird in der Form hh:mm:ss oder nur hh:mm ausgegeben.

9.1.2 ftshwa

Die folgende Tabelle zeigt das CSV-Ausgabeformat eines Berechtigungssatzes.

In der Spalte **Parameter** finden Sie den Namen des Ausgabeparameters bei der Normalausgabe, siehe Seite 289.

Spalte	Typ	Werte und Bedeutung	Parameter
UserId	String	Benutzerkennung, eingeschlossen in Anführungszeichen / *STD *STD bedeutet Standardberechtigungssatz	USER-ID
UserMaxObs	Number	0 ... 100 Benutzer-Grenzwert für OUTBOUND-SEND	MAX. USER LEVELS OBS
UserMaxObsStd	String	*YES / *NO *YES bedeutet Wert wie Standardberechtigungssatz [1]	
UserMaxObr	Number	0 ... 100 Benutzer-Grenzwert für OUTBOUND-RECEIVE	MAX. USER LEVELS OBR
UserMaxObrStd	String	*YES / *NO *YES bedeutet Wert wie Standardberechtigungssatz [1]	
UserMaxIbs	Number	0 ... 100 Benutzer-Grenzwert für INBOUND-SEND	MAX. USER LEVELS IBS
UserMaxIbsStd	String	*YES / *NO *YES bedeutet Wert wie Standardberechtigungssatz [1]	
UserMaxIbr	Number	0 ... 100 Benutzer-Grenzwert für INBOUND-RECEIVE	MAX. USER LEVELS IBR
UserMaxIbrStd	String	*YES / *NO *YES bedeutet Wert wie Standardberechtigungssatz [1]	
UserMaxIbp	Number	0 ... 100 Benutzer-Grenzwert für INBOUND-PROCESSING	MAX. USER LEVELS IBP
UserMaxIbpStd	String	*YES / *NO *YES bedeutet Wert wie Standardberechtigungssatz [1]	
UserMaxIbf	Number	0 ... 100 Benutzer-Grenzwert für INBOUND-FILE-MANAGEMENT	MAX. USER LEVELS IBF
UserMaxIbfStd	String	*YES / *NO *YES bedeutet Wert wie Standardberechtigungssatz [1]	
AdmMaxObs	Number	0 ... 100 Grenzwert des FTAC-Verwalters für OUTBOUND-SEND	MAX. ADM LEVELS OBS
AdmMaxObsStd	String	*YES / *NO *YES bedeutet Wert wie Standardberechtigungssatz [1]	

Spalte	Typ	Werte und Bedeutung	Parameter
AdmMaxObr	Number	0 ... 100 Grenzwert des FTAC-Verwalters für OUTBOUND-RECEIVE	MAX. ADM LEVELS OBR
AdmMaxObrStd	String	*YES / *NO *YES bedeutet Wert wie Standardberechtigungssatz [1]	
AdmMaxIbs	Number	0 ... 100 Grenzwert des FTAC-Verwalters für INBOUND-SEND	MAX. ADM LEVELS IBS
AdmMaxIbsStd	String	*YES / *NO *YES bedeutet Wert wie Standardberechtigungssatz [1]	
AdmMaxIbr	Number	0 ... 100 Grenzwert des FTAC-Verwalters für INBOUND-RECEIVE	MAX. ADM LEVELS IBR
AdmMaxIbrStd	String	*YES / *NO *YES bedeutet Wert wie Standardberechtigungssatz [1]	
AdmMaxIbp	Number	0 ... 100 Grenzwert des FTAC-Verwalters für INBOUND-PROCESSING	MAX. ADM LEVELS IBP
AdmMaxIbpStd	String	*YES / *NO *YES bedeutet Wert wie Standardberechtigungssatz [1]	
AdmMaxIbf	Number	0 ... 100 Grenzwert des FTAC-Verwalters für INBOUND-FILE-MANAGEMENT	MAX. ADM LEVELS IBF
AdmMaxIbfStd	String	*YES / *NO *YES bedeutet Wert wie Standardberechtigungssatz [1]	
Priv	String	*YES / *NO *YES bedeutet Berechtigungssatz des FTAC-Verwalters	ATTR
Password	String	*NO	ATTR
AdmPriv	String	*YES / *NO *YES bedeutet Berechtigungssatz des ADM-Verwalters	ATTR

[1] nur relevant wenn UserId ungleich *STD, beim Standardberechtigungssatz wird immer *NO ausgegeben. *YES entspricht in Normalausgabe einem Stern (*) hinter dem Wert.

9.1.3 ftshwatp

Die folgende Tabelle zeigt das CSV-Format eines ADM-Traps.

In der Spalte **Parameter** finden Sie den Namen des Ausgabeparameters bei der Langausgabe von *ftshwatp*, siehe Seite 296.

Spalte	Typ	Werte und Bedeutung	Parameter
TrapId	Number	Nummer des ADM-TRAPs, 1 bis 18-stellig	TRAP-ID
Source	String	Name des Partners, auf dem der Trap aufgetreten ist, eingeschlossen in Anführungszeichen	SOURCE
TrapTime	Date	Zeitpunkt, an dem der Trap aufgetreten ist	DATE, TIME
TrapType	String	Typ des Traps	TYPE
PartnerState	String	Zustand des Trap auslösenden Partners	PTN-STATE
TransId	Number	Transfer-Id [1]	TRANS-ID
RqInitiator	String	Benutzerkennung bzw. Ort [1] eingeschlossen in Anführungszeichen / *REM	INITIATOR
PartnerName	String	Partnername [1] eingeschlossen in Anführungszeichen	PARTNER
FileName	String	Dateiname [1] eingeschlossen in Anführungszeichen	FILENAME
RqError	String	Reason-Code [1] eingeschlossen in Anführungszeichen	RC
RqErrorMsg	String	Meldungstext [1] eingeschlossen in Anführungszeichen	ERROR-MSG

[1] des Trap auslösenden Transfers

9.1.4 ftshwc

Die folgende Tabelle zeigt das CSV-Format für die Ausgabe der fernadministrierbaren openFT-Instanzen.

In der Spalte **Parameter** finden Sie den Namen des Ausgabeparameters bei der Normalausgabe von *ftshwc*, siehe Seite 299.

Spalte	Typ	Werte und Bedeutung	Parameter
Name	String	Name eingeschlossen in Anführungszeichen	NAME
Description	String	Beschreibung eingeschlossen in Anführungszeichen	DESCRIPTION
Type	String	*GROUP / *INSTANCE Typ (Gruppe oder openFT-Instanz)	TYPE
AccessFtAdm	String	*YES / *NO / *NONE Lesende und modifizierende FT-Zugriffe sind erlaubt (entspricht den Rechten des FT-Verwalters) / nicht erlaubt / nicht relevant (bei Type = *GROUP)	ACCESS
AccessFtacAdm	String	*YES / *NO / *NONE Lesende und modifizierende FTAC-Zugriffe sind erlaubt (entspricht den Rechten des FTAC-Verwalters) / nicht erlaubt / nicht relevant (bei Type = *GROUP)	ACCESS
AccessFtOp	String	*YES / *NO / *NONE Lesende FT-Zugriffe sind erlaubt / nicht erlaubt / nicht relevant (bei Type = *GROUP)	ACCESS
Mode	String	*FTADM / *LEGACY / *NONE Die Instanz wird über das FTADM-Protokoll administriert / über ftexec administriert / nicht relevant (bei Type = *GROUP)	MODE

Beispiel

```
ftshwc -csv
Name;Description;Type;AccessFtAdm;AccessFtacAdm;AccessFtOp;Mode
"Hamburg";"Rechenzentrum Nord in Hamburg Wandsbek";*GROUP;*NONE;*NONE;*NONE;
"Hamburg/HH1";"QA Rechenzentrum";*GROUP;*NONE;*NONE;*NONE;
"Hamburg/HH1/HHWSRV01";"Solaris 10";*INSTANCE;*YES;*YES;*YES;*FTADM
"Hamburg/HH1/HHWSRV02";"HP-11";*INSTANCE;*YES;*YES;*YES;*FTADM
"Hamburg/HH1/HHWSRV11";"Solaris 9";*INSTANCE;*YES;*NO;*YES;*LEGACY
"Hamburg/HH2";"Personalabteilung";*GROUP;*NONE;*NONE;*NONE;
"Hamburg/HH2/HHWSRV99";"Mainframe-System
(BS2000/OSD)";*INSTANCE;*NO;*NO;*YES;*FTADM
```

9.1.5 ftshwe

Das Kommando *ftshwe* gibt nacheinander die in einer FTAC-Auslagerungsdatei enthaltenen Objekte in einem Format aus, das der Ausgabe der Kommandos *ftshwa* (Seite 401) und *ftshwp* (Seite 420) entspricht.

9.1.6 ftshwk

Die folgende Tabelle zeigt das CSV-Format für die Ausgabe der Eigenschaften von RSA-Schlüsseln.

In der Spalte **Parameter** finden Sie den Namen des Ausgabeparameters bei der Normalausgabe, siehe Seite 305.

Spalte	Typ	Werte und Bedeutung	Parameter
Reference	Number	Schlüsselreferenz	KEY-REF
Identification	String	Identifikation des Partners eingeschlossen in Anführungszeichen / *OWN *OWN bedeutet privater Schlüssel für die eigene Instanz	IDENTIFICATION
CreDate	Date	Datum, an dem der Schlüssel erzeugt wurde	CRE-DATE
ExpDate	String	Datum, an dem der Schlüssel abläuft / *NONE	EXP-DATE
Expired	String	*YES / *NO Schlüssel ist abgelaufen / nicht abgelaufen	EXP-DATE (EXPIRED)
KeyLen	Number	768 / 1024 / 2048 Schlüssellänge in Bit	KEY-LEN
AuthLev	Number	1 / 2 Authentifizierungsstufe	AUTHL

9.1.7 ftshwl

Die folgende Tabelle zeigt das CSV-Ausgabeformat eines Logging-Satzes, wenn die Option *-llf* nicht angegeben wurde. Bei Angabe der Option -llf hat die Ausgabe ein anderes Format, siehe Seite 409.

Als Beispiel für eine mögliche Auswerteprozedur steht Ihnen eine Formatvorlage im Microsoft-Excel-Format in folgender Datei zur Verfügung:

/opt/openFT/samples/ftaccnt.xlt

In der Spalte **Parameter** finden Sie den Namen des Ausgabeparameters bei der Langausgabe, siehe Seite 317 ff.

Spalte	Typ	Werte und Bedeutung	Parameter
LogId	Number	Nummer des Logging-Satzes, maximal 12-stellig	LOGGING-ID
ReasonCode	String	Reason-Code eingeschlossen in Anführungszeichen, um nicht als Zahl interpretiert zu werden. FTAC-Reason-Codes werden als sedezimaler String ausgegeben	RC
LogTime	Date	Zeitpunkt, an dem der Logging-Satz geschrieben wurde	TIME
InitUserId	String	Initiator des Auftrags eingeschlossen in Anführungszeichen / *REM	INITIATOR
InitTsn	String	*NONE	---
PartnerName	String	Partnername eingeschlossen in Anführungszeichen (Name oder Adresse)	PARTNER
TransDir	String	*TO / *FROM / *NSPEC Übertragungsrichtung	TRANS
RecType	String	*FT / *FTAC / *ADM Typ des Logging-Satzes	REC-TYPE
Func	String	*TRANS-FILE / *READ-FILE-ATTR / *DEL-FILE / *CRE-FILE / *MOD-FILE-ATTR / *READ-DIR / *MOVE-FILE / *CRE-FILE-DIR / *DEL-FILE-DIR / *LOGIN / *MOD-FILE-DIR / *REM-ADMIN / *REM-ADMIN-ROUT FT-Funktion	FUNCTION
UserAdmisId	String	Benutzerkennung, auf die sich die Aufträge im lokalen System beziehen, eingeschlossen in Anführungszeichen	USER-ADM
FileName	String	lokaler Dateiname eingeschlossen in Anführungszeichen	FILENAME
Priv	String	*YES / *NO / *NONE Profil ist privilegiert / nicht privilegiert / nicht relevant da kein Profil verwendet wurde oder kein FTAC-Logging-Satz vorliegt	PRIV

Spalte	Typ	Werte und Bedeutung	Parameter
ProfName	String	Name des FTAC-Profils eingeschlossen in Anführungszeichen / *NONE	PROFILE
ResultProcess	String	*STARTED / *NOT-STARTED / *NONE Zustand der Folgeverarbeitung	PCMD
StartTime	Date	Startzeitpunkt der Übertragung	STARTTIME
TransId	Number	Nummer des Übertragungsauftrags	TRANS-ID
Write	String	*REPL / *EXT / *NEW / *NONE Schreibmodus	WRITE
StoreTime	Date	Zeitpunkt der Auftragsannahme: – Bei Initiative im lokalen System der Zeitpunkt der Auftragserteilung – Bei Initiative im fernen System der Zeitpunkt des Eintrags im Auftragsbuch	 REQUESTED STORETIME
ByteNum	Number	Anzahl der übertragenen Bytes	TRANSFER
DiagInf	String	Diagnoseinformation / *NONE	---
ErrInfo	String	Zusatzinformation zur Fehlermeldung, eingeschlossen in Anführungszeichen / *NONE	ERRINFO
Protection	String	*SAME / *STD Schutzattribute werden übertragen / nicht übertragen	PROTECTION ---
ChangeDate	String	*SAME / *STD Änderungsdatum der Sendedatei für die Empfangsdatei übernehmen / nicht übernehmen	CHG-DATE
SecEncr	String	*YES / *NO Verschlüsselung der Auftragsbeschreibung eingeschaltet / ausgeschaltet	SEC-OPTS
SecDichk	String	*YES / *NO Datenintegritätsprüfung der Auftragsbeschreibung eingeschaltet / ausgeschaltet	SEC-OPTS
SecDencr	String	*YES / *NO Verschlüsselung des übertragenen Dateiinhalts eingeschaltet / ausgeschaltet	SEC-OPTS
SecDdichk	String	*YES / *NO Datenintegritätsprüfung des übertragenen Dateiinhalts eingeschaltet / ausgeschaltet	SEC-OPTS
SecLauth	String	*YES / *NO Authentifizierung des lokalen Systems im fernen System eingeschaltet / ausgeschaltet	SEC-OPTS
SecRauth	String	*YES / *NO Authentifizierung des fernen Systems im lokalen System eingeschaltet / ausgeschaltet	SEC-OPTS

Spalte	Typ	Werte und Bedeutung	Parameter
RsaKeyLen	Number	768 / 1024 / 2048 / leer Länge des für die Verschlüsselung verwendeten RSA-Schlüssels in Bit oder leer, wenn SecEncr nicht den Wert *YES hat	SEC-OPTS
SymEncrAlg	String	*DES / *AES-128 / *AES-256 / leer Verwendeter Verschlüsselungsalgorithmus oder leer, wenn SecEncr nicht den Wert *YES hat	SEC-OPTS
CcsName	String	Name des Zeichensatzes eingeschlossen in Anführungszeichen / leer	CCS-NAME
AdminId	String	Administrator-Id auf dem Fernadministrations-Server, eingeschlossen in Anführungszeichen / leer	ADMIN-ID
Routing	String	Routinginformation eingeschlossen in Anführungszeichen / leer	ROUTING
AdmCmd	String	Administrationskommando eingeschlossen in Anführungszeichen / leer	ADM-CMD
As3Type	String	leer (interne Funktion)	---
As3MsgTid	String	leer (interne Funktion)	---
As3RcpStat	String	leer (interne Funktion)	---
AuthLev	Number	1 / 2 / leer Authentifizierungsstufe	SEC-OPTS
GlobReqId	Number	Globale Auftragsidentifikation (fern gestellte Aufträge) / leer (lokal gestellte Aufträge)	GLOB-ID

CSV-Ausgabe bei ftshwl -llf

Bei der Option *-llf* werden nur die beiden folgenden Spalten ausgegeben:

Spalte	Typ	Werte und Bedeutung	Parameter
TimeStamp	Date	Erstellungszeitpunkt der Logging-Datei	---
LoggingFileName	String	Vollqualifizierter Name der Logging-Datei	(Dateiname)

9.1.8 ftshwm

Die folgende Tabelle zeigt das CSV-Ausgabeformat für die Messwerte des openFT-Betriebs, wenn alle Messwerte ausgegeben werden (*ftshwm -csv @a*).

Bei Option *-raw* werden die Werte für die Dauer nicht ausgegeben (*Duxxx*, siehe Fußnote).

In der Spalte **Std** sind die Standardwerte durch „x“ gekennzeichnet. Diese werden bei *ftshwm -csv* ohne *@a* und ohne explizite Namensangabe ausgegeben.

Die ausführliche Beschreibung der Messwerte entnehmen Sie dem Abschnitt „Beschreibung der Messwerte“ auf Seite 335. Die einzelnen Messgrößen (ThNetbTtl ... StTrcr) haben in allen Ausgabeformaten (Normalausgabe, Langausgabe und CSV-Ausgabe) die gleichen Namen.

Spalte	Typ	Werte aufbereitet	Werte nicht aufbereitet	Bedeutung	Std
CurrTime	Date	Zeitpunkt	Zeitpunkt	aktuelle Zeit	x
MonOn	Date	Zeitpunkt	Zeitpunkt	Startzeitpunkt der Überwachung bzw. letzte Änderung der Konfiguration. Eine Änderung von PartnerSel/ReqSel gilt als Neustart.	x
PartnerSel	String6	*ALL / *NONE / OPENFT / FTAM / FTP		Ausgewählter Partnertyp	x
ReqSel	String	*ALL / ONLY-SYNC / ONLY-ASYNC / ONLY-LOCAL / ONLY-REMOTE		Ausgewählter Auftragstyp	x
Data	String	FORM	RAW	Ausgabeformat (aufbereitet/nicht aufbereitet)	x
ThNetbTtl	Number	Anzahl Bytes pro Sekunde	Bytes kumuliert	Durchsatz Netzbytes	x
ThNetbSnd	Number	Anzahl Bytes pro Sekunde	Bytes kumuliert	Durchsatz Netzbytes Sendeaufträge	x
ThNetbRcv	Number	Anzahl Bytes pro Sekunde	Bytes kumuliert	Durchsatz Netzbytes Empfangsaufträge	x
ThNetbTxt	Number	Anzahl Bytes pro Sekunde	Bytes kumuliert	Durchsatz Netzbytes Textdateien	
ThNetbBin	Number	Anzahl Bytes pro Sekunde	Bytes kumuliert	Durchsatz Netzbytes Binärdateien	
ThDiskTtl	Number	Anzahl Bytes pro Sekunde	Bytes kumuliert	Durchsatz Plattenbytes	x
ThDiskSnd	Number	Anzahl Bytes pro Sekunde	Bytes kumuliert	Durchsatz Plattenbytes Sendeaufträge	x

Spalte	Typ	Werte aufbereitet	Werte nicht aufbereitet	Bedeutung	Std
ThDiskRcv	Number	Anzahl Bytes pro Sekunde	Bytes kumuliert	Durchsatz Plattenbytes Empfangsaufträge	x
ThDiskTxt	Number	Anzahl Bytes pro Sekunde	Bytes kumuliert	Durchsatz Plattenbytes Textdateien	
ThDiskBin	Number	Anzahl Bytes pro Sekunde	Bytes kumuliert	Durchsatz Plattenbytes Binärdateien	
ThRqto	Number	Anzahl pro Sekunde	Anzahl kumuliert	Eingegangene openFT-Aufträge	x
ThRqft	Number	Anzahl pro Sekunde	Anzahl kumuliert	Eingegangene Dateiübertragungsaufträge	
ThRqfm	Number	Anzahl pro Sekunde	Anzahl kumuliert	Eingegangene Dateimanagement-Aufträge	
ThSuct	Number	Anzahl pro Sekunde	Anzahl kumuliert	Erfolgreich beendete openFT-Aufträge	x
ThAbrt	Number	Anzahl pro Sekunde	Anzahl kumuliert	Abgebrochene openFT-Aufträge	x
ThIntr	Number	Anzahl pro Sekunde	Anzahl kumuliert	Unterbrochene openFT-Aufträge	x
ThUsrf	Number	Anzahl pro Sekunde	Anzahl kumuliert	Aufträge von nichtberechtigten Benutzern	x
ThFoll	Number	Anzahl pro Sekunde	Anzahl kumuliert	Gestartete Folgeverarbeitungen	
ThCosu	Number	Anzahl pro Sekunde	Anzahl kumuliert	Aufgebaute Verbindungen	
ThCofl	Number	Anzahl pro Sekunde	Anzahl kumuliert	Abgebrochene Verbindungsaufbau-Versuche	x
ThCobr	Number	Anzahl pro Sekunde	Anzahl kumuliert	Verbindungsabbrüche wegen Verbindungsfehler	x
DuRqtlOut[1]	Number	Millisekunden	---	Maximale Auftragsdauer outbound	
DuRqtlInb[1]	Number	Millisekunden	---	Maximale Auftragsdauer inbound	
DuRqftOut[1]	Number	Millisekunden	---	Maximale Auftragsdauer outbound Transfer	
DuRqftInb[1]	Number	Millisekunden	---	Maximale Auftragsdauer inbound Transfer	
DuRqfmOut[1]	Number	Millisekunden	---	Maximale Auftragsdauer outbound Dateimanagement	

Spalte	Typ	Werte aufbereitet	Werte nicht aufbereitet	Bedeutung	Std
DuRqfmInb[1]	Number	Millisekunden	---	Maximale Auftragsdauer inbound Dateimanagement	
DuRqesOut[1]	Number	Millisekunden	---	Maximale Auftragswartezeit outbound	
DuDnscOut[1]	Number	Millisekunden	---	Maximale Dauer der Partnerprüfung für einen outbound openFT-Auftrag	
DuDnscInb[1]	Number	Millisekunden	---	Maximale Dauer der Partnerprüfung für einen inbound openFT-Auftrag	
DuConnOut[1]	Number	Millisekunden	---	Maximale Dauer eines Verbindungsaufbaus für einen outbound openFT-Auftrag	
DuOpenOut[1]	Number	Millisekunden	---	Maximale Dateiöffnungszeit (outbound)	
DuOpenInb[1]	Number	Millisekunden	---	Maximale Dateiöffnungszeit (inbound)	
DuClosOut[1]	Number	Millisekunden	---	Maximale Dauer des Dateischließens (outbound)	
DuClosInb[1]	Number	Millisekunden	---	Maximale Dauer des Dateischließens (inbound)	
DuUsrcOut[1]	Number	Millisekunden	---	Maximale Dauer der Benutzerprüfung (outbound)	
DuUsrcInb[1]	Number	Millisekunden	---	Maximale Dauer der Benutzerprüfung (inbound)	
StRqas	Number (100)[2]	Mittelwert	aktuelle Anzahl	Anzahl der synchronen Aufträge im Zustand ACTIVE	x
StRqaa	Number (100)[2]	Mittelwert	aktuelle Anzahl	Anzahl der asynchronen Aufträge im Zustand ACTIVE	x
StRqwt	Number (100)[2]	Mittelwert	aktuelle Anzahl	Anzahl der Aufträge im Zustand WAIT	x
StRqhd	Number (100)[2]	Mittelwert	aktuelle Anzahl	Anzahl der Aufträge im Zustand HOLD	x
StRqsp	Number (100)[2]	Mittelwert	aktuelle Anzahl	Anzahl der Aufträge im Zustand SUSPEND	x
StRqlk	Number (100)[2]	Mittelwert	aktuelle Anzahl	Anzahl der Aufträge im Zustand LOCK	x

Spalte	Typ	Werte aufbereitet	Werte nicht aufbereitet	Bedeutung	Std
StRqfi	Number (100)[2]	Mittelwert	aktuelle Anzahl	Anzahl der Aufträge im Zustand FINISHED	
StCLim	Number	aktuell eingestellter Wert		Maximale Anzahl der Verbindungen, die für asynchrone Aufträge aufgebaut werden	x
StCAct	Prozent	Anteil in % von StCLim	aktuelle Anzahl	Anzahl belegter Verbindungen für asynchrone Aufträge	x
StRqLim	Number	aktuell eingestellter Wert		Maximale Anzahl asynchroner Aufträge in der Auftragsverwaltung	x
StRqAct	Prozent	Anteil in % von StRqLim	aktuelle Anzahl	Belegte Einträge der Auftragsverwaltung	x
StOftr	BOOL	1 / 0		openFT-Protokoll aktiv / nicht aktiv	x
StFtmr	BOOL	1 / 0		FTAM-Protokoll aktiv / nicht aktiv	x
StFtpr	BOOL	1 / 0		FTP-Protokoll aktiv / nicht aktiv	x
StTrcr	BOOL	1 / 0		Trace eingeschaltet / ausgeschaltet	

[1] wird bei Option *-raw* nicht ausgegeben

[2] Number (100) ist der Messwert multipliziert mit 100 (z.B. entspricht Ausgabe 225 dem Messwert 2.25)

Beispiele

```
ftshwm -ty -csv @a
```

```
CurrTime;MonOn;PartnerSel;ReqSel;Data;ThNetbTtl;ThNetbSnd;ThNetbRcv;ThNetbTxt
;ThNetbBin;ThDiskTtl;ThDiskSnd;ThDiskRcv;ThDiskTxt;ThDiskBin;ThRqto;ThRqft;Th
Rqfm;ThSuct;ThAbrt;ThIntr;ThUsrf;ThFoll;ThCosu;ThCofl;ThCobr;DuRqtlOut;DuRqtl
Inb;DuRqftOut;DuRqftInb;DuRqfmOut;DuRqfmInb;DuRqesOut;DuDnscOut;DuDnscInb;DuC
onnOut;DuOpenOut;DuOpenInb;DuClosOut;DuClosInb;DuUsrcOut;DuUsrcInb;StRqas;StR
qaa;StRqwt;StRqhd;StRqsp;StRqlk;StRqfi;StCLim;StCAct;StRqLim;StRqAct;StOftr;S
tFtmr;StFtpr;StTrcr
*TIME;*TIME;*STRING;*STRING;*STRING;*INT;*INT;*INT;*INT;*INT;*INT;*INT;*INT;*
INT;*INT;*INT;*INT;*INT;*INT;*INT;*INT;*INT;*INT;*INT;*INT;*INT;*INT;*INT;*IN
T;*INT;*INT;*INT;*INT;*INT;*INT;*INT;*INT;*INT;*INT;*INT;*INT;*INT;*INT;*INT(100);
*INT(100);*INT(100);*INT(100);*INT(100);*INT(100);*INT(100);*INT;*PERCENT;*IN
T;*PERCENT;*BOOL;*BOOL;*BOOL;*BOOL
```

```
ftshwm -csv ThNetbTtl ThDiskTtl
```

```
CurrTime;MonOn;PartnerSel;ReqSel;Data;ThNetbTtl;ThDiskTtl
2008-02-28 15:40:01;2008-02-28 15:36:12;OPENFT,FTAM;ONLY-ASYNC,ONLY-
REMOTE;FORM;2681262;524064
```

9.1.9 ftshwo

Die folgende Tabelle zeigt das CSV-Ausgabeformat der Betriebsparameter.

In der Spalte **Parameter** finden Sie den Namen des Ausgabeparameters bei der Normalausgabe, siehe Seite 342 ff. Einige Parameter haben feste Werte, da sie nur aus Kompatibilitätsgründen unterstützt werden oder durch andere Parameter abgelöst wurden.

Spalte	Typ	Werte und Bedeutung	Parameter
PartnerLim	Number	0	---
ReqLim	Number	maximale Anzahl Aufträge	RQ-LIM
TaskLim	Number	maximale Anzahl Prozesse	PROC-LIM
ConnLim	Number	maximale Anzahl Transportverbindungen	CONN-LIM
ReqWaitLev	Number	1	---
TransportUnitSize	Number	Maximale Länge einer Transporteinheit	TU-SIZE
PartnerCheck	String	*STD / *TRANSP-ADDR Partnerüberprüfung	PTN-CHK
SecLev	Number	0... 100 / *B-P-ATTR Standardwert für die Sicherheitsstufe von Partnern	SEC-LEV
TraceOpenft	String	*STD / *OFF Tracefunktion für openFT-Partner eingeschaltet / ausgeschaltet	FUNCT, Zeile TRACE PARTNER-SELECTION
TraceOut	String	*FILE / leer Tracefunktion eingeschaltet / ausgeschaltet	FUNCT, Zeile TRACE SWITCH
TraceSession	String	*OFF	---
TraceFtam	String	*STD / *OFF Tracefunktion für FTAM-Partner eingeschaltet / ausgeschaltet	FUNCT, Zeile TRACE PARTNER-SELECTION
LogTransFile	String	*ON / *OFF FT-Logging eingeschaltet / ausgeschaltet	FT-LOG
MaxInboundReq	Number	maximale Anzahl Aufträge	(wie RQ-LIM)
MaxReqLifetime	String	maximale Verweildauer von Aufträgen im Auftragsbuch / *UNLIMITED	MAX-RQ-LIFE
SnmpTrapsSubsystemState	String	*ON / *OFF SNMP-Traps bei Statuswechsel des Subsystems eingeschaltet / ausgeschaltet	TRAP, Zeile SNMP SS-STATE
SnmpTrapsFtState	String	*ON / *OFF SNMP-Traps bei Statuswechsel des asynchronen Servers eingeschaltet / ausgeschaltet	TRAP, Zeile SNMP FT-STATE

Spalte	Typ	Werte und Bedeutung	Parameter
SnmpTrapsPartnerState	String	*ON / *OFF SNMP-Traps bei Statuswechsel der Partner eingeschaltet / ausgeschaltet	TRAP, Zeile SNMP PART-STATE
SnmpTrapsPartnerUnreach	String	*ON / *OFF SNMP-Traps bei Nichterreichbarkeit von Partnersystemen eingeschaltet / ausgeschaltet	TRAP, Zeile SNMP PART-UNREA
SnmpTrapsReqQueueState	String	*ON / *OFF SNMP-Traps bei Statuswechsel der Auftragsverwaltung eingeschaltet / ausgeschaltet	TRAP, Zeile SNMP RQ-STATE
SnmpTrapsTransSucc	String	*ON / *OFF SNMP-Traps bei erfolgreich abgeschlossenen Aufträgen eingeschaltet / ausgeschaltet	TRAP, Zeile SNMP TRANS-SUCC
SnmpTrapsTransFail	String	*ON / *OFF SNMP-Traps bei fehlerhaften Aufträgen eingeschaltet / ausgeschaltet	TRAP, Zeile SNMP TRANS-FAIL
ConsoleTraps	String	*ON / *OFF Konsolen-Traps (für mindestens ein Kriterium) eingeschaltet / ausgeschaltet.	TRAP, Zeile CONS
TeleService	String	leer	
HostName	String	Hostname des lokalen Rechners / *NONE	HOST-NAME
Identification	String	Instanz-Identifikation eingeschlossen in Anführungszeichen	IDENTIFICATION
UseTns	String	*YES / *NO TNS im Betrieb mit CMX verwenden / nicht verwenden	USE TNS
ConsTrapsSubsystemState	String	*ON / *OFF Konsolen-Traps bei Statuswechsel des Subsystems eingeschaltet / ausgeschaltet	TRAP, Zeile CONS SS-STATE
ConsTrapsFtState	String	*ON / *OFF Konsolen-Traps bei Statuswechsel des asynchronen Servers eingeschaltet / ausgeschaltet	TRAP, Zeile CONS FT-STATE
ConsTrapsPartnerState	String	*ON / *OFF Konsolen-Traps bei Statuswechsel der Partner eingeschaltet / ausgeschaltet	TRAP, Zeile CONS PART-STATE
ConsTrapsPartnerUnreach	String	*ON / *OFF Konsolen-Traps bei Nichterreichbarkeit von Partnersystemen eingeschaltet / ausgeschaltet	TRAP, Zeile CONS PART-UNREA

Spalte	Typ	Werte und Bedeutung	Parameter
ConsTrapsReqQueueState	String	*ON / *OFF Konsolen-Traps bei Statuswechsel der Auftragsverwaltung eingeschaltet / ausgeschaltet	TRAP, Zeile CONS RQ-STATE
ConsTrapsTransSucc	String	*ON / *OFF Konsolen-Traps bei erfolgreich abgeschlossenen Aufträgen eingeschaltet / ausgeschaltet	TRAP, Zeile CONS TRANS-SUCC
ConsTrapsTransFail	String	*ON / *OFF Konsolen-Traps bei fehlerhaften Aufträgen eingeschaltet / ausgeschaltet	TRAP, Zeile CONS TRANS-FAIL
FtLog	String	*ALL / *FAIL / *NONE Umfang des FT-Loggings	FT-LOG
FtacLog	String	*ALL / *FAIL / *NONE Umfang des FTAC-Loggings	FTAC-LOG
Trace	String	*ON / *OFF Tracefunktion eingeschaltet / ausgeschaltet	FUNCT, Zeile TRACE SWITCH
TraceSelp	String	*ALL / OPENFT / FTP / FTAM / ADM / leer [1] Trace-Auswahl nach Typ des Partners	FUNCT, Zeile TRACE PARTNER-SELECTION
TraceSelr	String	*ALL / ONLY-SYNC / ONLY-ASYNC / ONLY-LOCAL / ONLY-REMOTE [1] Trace-Auswahl nach Typ des Auftrags	FUNCT, Zeile TRACE REQUEST-SELECTION
TraceOpt	String	*NO-BULK-DATA / *NONE Minimal-Trace / keine Trace-Optionen	FUNCT, Zeile TRACE OPTIONS
KeyLen	Number	768 / 1024 / 2048 RSA-Schlüssellänge in Bit	KEY-LEN
CcsName	String	Zeichensatz eingeschlossen in Anführungszeichen	CCS-NAME
AppEntTitle	String	*YES / *NO Bei FTAM wird der "nil-Application Entity Title" geschickt / nicht geschickt	---
StatName	String	Name der lokalen openFT-Anwendung$FJAM	LOCAL-SYSTEM-NAME
SysName	String	Name des lokalen Systems / leer	LOCAL-SYSTEM-NAME
FtStarted	String	*YES / *NO Asynchroner openFT-Server gestartet / nicht gestartet	STARTED
openftAppl	String	*STD / Portnummer Portnummer des lokalen openFT-Servers	OPENFT-APPL
ftamAppl	String	*STD / Portnummer Portnummer des lokalen FTAM-Servers	FTAM-APPL

Spalte	Typ	Werte und Bedeutung	Parameter
FtpPort	Number	Portnummer Portnummer des lokalen FTP-Servers	FTP-PORT
ftpDPort	Number	Wert / leer (interne Funktion)	---
ftstdPort	String	*STD / Portnummer Standardport für dynamische Partner	---
DynPartner	String	*ON / *OFF Dynamische Partnereinträge eingeschaltet / ausgeschaltet	DYN-PART
ConTimeout	Number	Wert (interne Funktion)	---
ChkpTime	Number	Wert (interne Funktion)	---
Monitoring	String	*ON / *OFF Messdatenerfassung eingeschaltet / ausgeschaltet	FUNCT, Zeile MONITOR SWITCH
MonSelp	String	*ALL / OPENFT / FTP / FTAM / leer [1] Auswahl nach Typ des Partnersystems	FUNCT, Zeile MONITOR PARTNER-SELECTION
MonSelr	String	*ALL / ONLY-SYNC / ONLY-ASYNC / ONLY-LOCAL / ONLY-REMOTE [1] Auswahl nach Art des Auftrags	FUNCT, Zeile MONITOR REQUEST-SELECTION
AdmTrapServer	String	Name des ADM-TRAP-Servers / *NONE	ADM-TRAP-SERVER
AdmTrapsFtState	String	*ON / *OFF ADM-Traps bei Statuswechsel des asynchronen Servers eingeschaltet / ausgeschaltet	TRAP, Zeile ADM FT-STATE
AdmTrapsPartnerState	String	*ON / *OFF ADM-Traps bei Statuswechsel der Partner eingeschaltet / ausgeschaltet	TRAP, Zeile ADM PART-STATE
AdmTrapsPartnerUnreach	String	*ON / *OFF ADM-Traps bei Nichterreichbarkeit von Partnersystemen eingeschaltet / ausgeschaltet	TRAP, Zeile ADM PART-UNREA
AdmTrapsReqQueueState	String	*ON / *OFF ADM-Traps bei Statuswechsel der Auftragsverwaltung eingeschaltet / ausgeschaltet	TRAP, Zeile ADM RQ-STATE
AdmTrapsTransSucc	String	*ON / *OFF ADM-Traps bei erfolgreich abgeschlossenen Aufträgen eingeschaltet / ausgeschaltet	TRAP, Zeile ADM TRANS-SUCC
AdmTrapsTransFail	String	*ON / *OFF ADM-Traps bei fehlerhaften Aufträgen eingeschaltet / ausgeschaltet	TRAP, Zeile ADM TRANS-FAIL
AdminConnLim	String	maximale Anzahl Administrationsverbindungen	ADM-CLIM

Spalte	Typ	Werte und Bedeutung	Parameter
AdmPort	String	Portnummer / *NONE Portnummer für Fernadministration	ADM-PORT
OpenftApplState	String	*ACTIVE / *INACT / *DISABLED / *NAVAIL Status des openFT-Servers	OPENFT-APPL, 2. Zeile
FtamApplState	String	*ACTIVE / *INACT / *DISABLED / *NAVAIL Status des FTAM-Servers	FTAM-APPL, 2. Zeile
FtpState	String	*ACTIVE / *INACT / *DISABLED / *NAVAIL Status des FTP-Servers	FTP-PORT, 2. Zeile
AdmState	String	*ACTIVE / *INACT / *DISABLED Status für Inbound-Fernadministration, auf dem ADM-Trap-Server auch Status für das Empfangen von ADM-Traps	ADM-PORT, 2. Zeile
AdminLog	String	*ALL / *FAIL / *MODIFY / *NONE Umfang des ADM-Loggings	ADM-LOG
CentralAdminServer	String	*YES / *NO Lokaler Rechner ist Fernadministrations-Server / kein Fernadministrations-Server	ADM-CS
ActiveAppl	String	*ALL / *NONE / OPENFT / FTAM / FTP / ADM [1] aktive Server	siehe 2. Zeile bei OPENFT-APPL, FTAM-APPL, FTP-PORT, ADM-PORT
UseCmx	String	*YES / *NO Betrieb mit CMX / ohne CMX	USE CMX
TraceOptLowerLayers	String	*DETAIL / *STD / *OFF Überwachungsumfang für untere Protokollschichten	OPTIONS-LL
EncMandIn	String	*YES / *NO Inbound-Verschlüsselung eingeschaltet / ausgeschaltet	ENC-MAND (IN)
EncMandOut	String	*YES / *NO Outbound-Verschlüsselung eingeschaltet / ausgeschaltet	ENC-MAND (OUT)
DelLog	String	*ON / *OFF Automatisches Löschen von Logging-Sätzen eingeschaltet / ausgeschaltet	DEL-LOG
DelLogRetpd	Number	Mindestalter der zu löschenden Logging-Sätze in Tagen. 0 bedeutet aktueller Tag.	RETPD
DelLogRepeat	String	*MONTHLY / *WEEKLY / *DAILY Wiederholungsintervall für das Löschen der Logging-Sätze.	DEL-LOG ON

Spalte	Typ	Werte und Bedeutung	Parameter
DelLogDay	Number	1..31 / 1..7 / 0 Tag, an dem das Löschen wiederholt werden soll. Bei DelLogRepeat = *MONTHLY ist das der Tag im Monat, bei DelLogRepeat = *WEEKLY der Wochentag (1 = Montag), bei DelLogRepeat = *DAILY wird 0 ausgegeben	DEL-LOG ON
DelLogTime	Time	Uhrzeit des Löschens	DEL-LOG AT

[1] Es sind auch Kombinationen mehrerer Werte möglich (nicht mit *ALL oder *NONE)

9.1.10 ftshwp

Die folgende Tabelle zeigt das CSV-Ausgabeformat eines Berechtigungsprofils.

In der Spalte **Parameter** finden Sie den Namen des Ausgabeparameters bei der Langausgabe, siehe auch Seite 350f und Seite 352f.

Spalte	Typ	Werte und Bedeutung	Parameter
ProfName	String	Name des Profils eingeschlossen in Anführungszeichen	(Profilname)
Priv	String	*YES / *NO Profil ist privilegiert / nicht privilegiert	PRIVILEGED
TransAdm	String	*SECRET / *NSPEC Zugangsberechtigung wurde vergeben / nicht vergeben	TRANS-ADM NOT-SPECIFIED
Duplicated	String	*YES / *NO *YES bedeutet: Profil ist gesperrt wegen des Versuchs, die Zugangsberechtigung doppelt zu vergeben	TRANS-ADM DUPLICATED
LockedByImport	String	*YES / *NO *YES bedeutet: Profil ist gesperrt da es importiert wurde	TRANS-ADM LOCKED (by_import)
LockedByAdm	String	*YES / *NO *YES bedeutet: Profil ist gesperrt durch FTAC-Verwalter	TRANS-ADM LOCKED (by_adm)
LockedByUser	String	*YES / *NO *YES bedeutet: Profil ist durch Benutzer gesperrt	TRANS-ADM LOCKED (by_user)
Expired	String	*YES / *NO *YES bedeutet: Profil ist gesperrt da Frist abgelaufen	TRANS-ADM EXPIRED
ExpDate	String	Ablaufdatum in der Kurzform yyyy-mm-dd / *NRES (kein Ablaufdatum)	EXP-DATE
Usage	String	*PUBLIC / *PRIVATE / *NSPEC Nutzung	USAGE
IgnObs	String	*YES / *NO Vorgabe für Outbound Send ignorieren / nicht ignorieren	IGN-MAX-LEVELS OBS
IgnObr	String	*YES / *NO Vorgabe für Outbound Receive ignorieren / nicht ignorieren	IGN-MAX-LEVELS OBR

Spalte	Typ	Werte und Bedeutung	Parameter
IgnIbs	String	*YES / *NO Vorgabe für Inbound Send ignorieren / nicht ignorieren	IGN-MAX-LEVELS IBS
IgnIbr	String	*YES / *NO Vorgabe für Inbound Receive ignorieren / nicht ignorieren	IGN-MAX-LEVELS IBR
IgnIbp	String	*YES / *NO Vorgabe für Inbound Processing ignorieren / nicht ignorieren	IGN-MAX-LEVELS IBP
IgnIbf	String	*YES / *NO Vorgabe für Inbound File Management ignorieren / nicht ignorieren	IGN-MAX-LEVELS IBF
Initiator	String	*LOC / *REM / *NRES Initiator nur lokal / nur fern / nicht eingeschränkt	INITIATOR
TransDir	String	*FROM / *TO / *NRES Erlaubte Übertragungsrichtung vom Partner / zum Partner / nicht eingeschränkt	TRANS-DIR
MaxPartLev	Number	0... 100 / *NRES Maximale Sicherheitsstufe / Sicherheitsstufe nicht eingeschränkt	MAX-PART-LEV
Partners	String	ein oder mehrere FT-Partner getrennt durch Kommas, eingeschlossen in Anführungszeichen / *NRES (keine Einschränkung)	PARTNER
FileName	String	Dateiname oder Dateinamen-Präfix eingeschlossen in Anführungszeichen / *NRES Schränkt den Zugriff auf diese Datei oder Dateien mit diesem Präfix ein. *NRES bedeutet keine Einschränkung	FILE-NAME
Library	String	*NRES auf Unix-Systemen nicht relevant	LIBRARY
FileNamePrefix	String	*YES / *NO Der Dateiname in FileName ist ein Präfix / ist kein Präfix	FILE-NAME = (PREFIX=..)
ElemName	String	*NRES	---
ElemPrefix	String	*NO	---
ElemVersion	String	*NRES	---
ElemType	String	*NRES	---
FilePass	String	*NRES	---

Spalte	Typ	Werte und Bedeutung	Parameter
Write	String	*NEW / *EXT / *REPL / *NRES Schreibregel	WRITE
UserAdmId	String	Benutzerkennung eingeschlossen in Anführungszeichen	USER-ADM (user-id,...)
UserAdmAcc	String	Abrechnungsnummereingeschlossen in Anführungszeichen / *NRES	USER-ADM (..,account,...)
UserAdmPass	String	*OWN / *YES / *NSPEC / *NONE Passwort wird übernommen / wurde angegeben / wurde nicht angegeben / wird nicht benötigt	USER-ADM (...,...,password)
ProcAdmId	String	*NRES	---
ProcAdmAcc	String	*NRES	---
ProcAdmPass	String	*NRES	---
SuccProc	String	Folgeverarbeitung bei Erfolg, eingeschlossen in Anführungszeichen / *NONE / *NRES / *EXPANSION	SUCC-PROC
SuccPrefix	String	Folgeverarbeitungspräfix bei Erfolg, eingeschlossen in Anführungszeichen / *NONE	SUCC-PREFIX
SuccSuffix	String	Folgeverarbeitungssuffix bei Erfolg, eingeschlossen in Anführungszeichen / *NONE	SUCC-SUFFIX
FailProc	String	Folgeverarbeitung bei Fehler, eingeschlossen in Anführungszeichen / *NONE / *NRES / *EXPANSION	FAIL-PROC
FailPrefix	String	Folgeverarbeitungspräfix bei Fehler, eingeschlossen in Anführungszeichen / *NONE	FAIL-PREFIX
FailSuffix	String	Folgeverarbeitungssuffix bei Fehler, eingeschlossen in Anführungszeichen / *NONE	FAIL-SUFFIX
TransFile	String	*ALLOWED / *NOT-ALLOWED Dateien übertragen und löschen erlaubt / nicht erlaubt	FT-FUNCTION = (TRANSFER-FILE)
ModFileAttr	String	*ALLOWED / *NOT-ALLOWED Dateiattribute modifizieren erlaubt / nicht erlaubt	FT-FUNCTION = (MODIFY-FILE-ATTRIBUTES)
ReadDir	String	*ALLOWED / *NOT-ALLOWED Dateiverzeichnisse ansehen erlaubt / nicht erlaubt	FT-FUNCTION = (READ-DIRECTORY)
FileProc	String	*ALLOWED / *NOT-ALLOWED Vor-/Nachverarbeitung erlaubt / nicht erlaubt	FT-FUNCTION = (FILE-PROCESSING)
AccAdm	String	*ALLOWED / *NOT-ALLOWED Zugang zum Fernadministrations-Server erlaubt / nicht erlaubt	FT-FUNCTION = (ACCESS-TO-ADMINISTRATION)

Spalte	Typ	Werte und Bedeutung	Parameter
RemAdm	String	*ALLOWED / *NOT-ALLOWED Fernadministration durch Fernadministrations-Server erlaubt / nicht erlaubt	FT-FUNCTION = (REMOTE-ADMINISTRATION)
Text	String	Text eingeschlossen in Anführungszeichen / *NONE	TEXT
DataEnc	String	*YES / *NO / *NRES Datenverschlüsselung ist vorgeschrieben / verboten / weder vorgeschrieben noch verboten	DATA-ENC
ModDate	Date	Zeitpunkt der letzten Änderung	LAST-MODIF
AdmTrapLog	String	*ALLOWED / *NOT-ALLOWED ADM-Traps empfangen erlaubt / nicht erlaubt	FT-FUNCTION = (ADM-TRAP-LOG)

9.1.11 ftshwptn

Die folgende Tabelle zeigt das CSV-Ausgabeformat eines Partners in der Partnerliste.

In der Spalte **Parameter** finden Sie den Namen des Ausgabeparameters bei der Langausgabe, siehe Seite 357.

Spalte	Typ	Werte und Bedeutung	Parameter
PartnerName	String	Partnername eingeschlossen in Anführungszeichen	NAME
Sta	String	*ACT / *DEACT / *NOCON / *LUNK / *RUNK / *ADEAC / *AINAC / *LAUTH / *RAUTH / *NOKEY / *DIERR / *IDREJ Status des Partners	STATE
SecLev	String	*STD / *B-P-ATTR / 1...100 globale Sicherheitsstufe / attributspezifische Sicherheitsstufe / feste Sicherheitsstufe	SECLEV
Trace	String	*FTOPT / *STD / *ON / *OFF Trace-Einstellung	TRACE
Loc	Number	Anzahl der lokal gestellten Dateiübertragungsaufträge an diesen Partner	LOC
Rem	Number	Anzahl der von diesem Partner gestellten Dateiübertragungsaufträge	REM
Processor	String	Prozessorname eingeschlossen in Anführungszeichen / leer	ADDRESS
Entity	String	Entityname eingeschlossen in Anführungszeichen / leer	ADDRESS
NetworkAddr	String	Partneradresse (Netzadresse ohne Portnummer/Selektoren) eingeschlossen in Anführungszeichen	ADDRESS
Port	Number	Portnummer	ADDRESS (Portnummer)
PartnerCheck	String	*FTOPT / *STD / *TRANSP-ADDR / *AUTH / *AUTHM / *NOKEY Absenderüberprüfung	P-CHK
TransportSel	String	Transport-Selektor eingeschlossen in Anführungszeichen / leer	ADDRESS (Transport-Selektor)
LastAccessDate	Date	Zeitpunkt des letzten Zugriffs in der Kurzform yyyy-mm-dd	---
SessionSel	String	Session-Selektor eingeschlossen in Anführungszeichen / leer	ADDRESS (Session-Selektor)

Spalte	Typ	Werte und Bedeutung	Parameter
PresentationSel	String	Presentation-Selektor eingeschlossen in Anführungszeichen / leer	ADDRESS (Presentation-Selektor)
Identification	String	Identifikation eingeschlossen in Anführungszeichen	IDENTIFICATION
SessRout	String	Routing-Information eingeschlossen in Anführungszeichen / *ID / leer *ID bedeutet Routing-Info gleich Identifikation	ROUTING
PartnerAddr	String	Partneradresse (mit Portnummer und Selektoren) eingeschlossen in Anführungszeichen	ADDRESS
Check	String	*FTOPT / *STD / *TRANSP-ADDR Partnerüberprüfung	P-CHK
AuthMand	String	*YES / *NO Authentifizierung erforderlich / nicht erforderlich	P-CHK
Priority	String	*LOW / *NORM / *HIGH Priorität	PRI
AS3	String	*NO (interne Funktion)	---
AuthLev	Number	1 / 2 / leer Authentifizierungsstufe	P-CHK
InboundSta	String	*ACT / *DEACT Inbound-Funktion aktiviert / deaktiviert	INBND
RequProc	String	*STD / *SERIAL Der Bearbeitungsmodus für asynchrone Outbound-Aufträge ist parallel / ist seriell	REQU-P

9.1.12 ftshwr

Die folgende Tabelle zeigt das CSV-Ausgabeformat eines Auftrags.

Für *ftshwr* ist auch die Kurzausgabe möglich, siehe Seite 430.

In der Spalte **Parameter** finden Sie den Namen des Ausgabeparameters bei der Langausgabe, siehe Seite 365.

Spalte	Typ	Werte und Bedeutung	Parameter
TransId	Number	Auftrags-Id	TRANSFER-ID
Initiator	String	*LOC / *REM Initiator lokal / fern	INITIATOR
State	String	*LOCK / *WAIT / *HOLD / *FIN / *ACT / *CANC / *SUSP Zustand des Auftrags	STATE
PartnerName	String	Name oder Adresse des Partners eingeschlossen in Anführungszeichen	PARTNER
PartnerState	String	*ACT / *INACT / *NOCON / *INSTERR Status des Partners	PARTNER-STATE
TransDir	String	*TO / *FROM Übertragungsrichtung	TRANS
ByteNum	Number	Anzahl der übertragenen Bytes / leer	BYTECNT
LocFileName	String	Dateiname im lokalen System eingeschlossen in Anführungszeichen	LOC: FILE
LocElemName	String	leer	---
LocElemType	String	leer	---
LocElemVersion	String	leer	---
Prio	String	*NORM / *LOW Priorität des Auftrags	PRIO
Compress	String	*NONE / *BYTE / *ZIP Komprimierte Übertragung	COMPRESS
DataEnc	String	*YES / *NO Benutzerdaten werden verschlüsselt übertragen / nicht verschlüsselt übertragen	ENCRYPT
DiCheck	String	*YES / *NO Datenintegrität wird überprüft / nicht überprüft	DICHECK
Write	String	*REPL / *EXT / *NEW Schreibmodus	WRITE

Spalte	Typ	Werte und Bedeutung	Parameter
StartTime	String	Zeitpunkt, an dem der Auftrag gestartet wird (Format yy-mm-dd hh:mm:ss) / *SOON (Auftrag wird so bald wie möglich gestartet)	START
CancelTime	String	Zeitpunkt an dem der Auftrag aus dem Auftragsbuch gelöscht wird (Format yy-mm-dd hh:mm:ss) / *NO (kein Löschzeitpunkt)	CANCEL
Owner	String	lokale Benutzerkennung eingeschlossen in Anführungszeichen	OWNER
DataType	String	*CHAR / *BIN / *USER Dateityp	DATA
Transp	String	*YES / *NO Übertragung transparent / nicht transparent	TRANSP
LocTransAdmId	String	Benutzerkennung für den Zugang zum lokalen System, eingeschlossen in Anführungszeichen / *NONE	LOC: TRANS-ADM (USER)
LocTransAdmAcc	String	leer	---
LocProfile	String	leer	---
LocProcAdmId	String	leer	---
LocProcAdmAcc	String	leer	---
LocSuccProc	String	Lokale Folgeverarbeitung bei Erfolg, eingeschlossen in Anführungszeichen / *NONE / leer	LOC: SUCC-PROC
LocFailProc	String	Lokale Folgeverarbeitung bei Fehler, eingeschlossen in Anführungszeichen / *NONE / leer	LOC: FAIL-PROC
LocListing	String	leer	---
LocMonjv	String	leer	---
LocCcsn	String	Name des Zeichensatzes im lokalen System eingeschlossen in Anführungszeichen / *STD	LOC: CCSN
RemFileName	String	Dateiname im fernen System eingeschlossen in Anführungszeichen / *NSPEC / *NONE / leer	REM: FILE
RemElemName	String	leer	---
RemElemType	String	leer	---
RemElemVersion	String	leer	---

Spalte	Typ	Werte und Bedeutung	Parameter
RemTransAdmId	String	Kennung im fernen System eingeschlossen in Anführungszeichen / *NONE	REM: TRANS-ADM=(user-id,...)
RemTransAdmAcc	String	Abrechnungsnummer im fernen System eingeschlossen in Anführungszeichen / leer	REM: TRANS-ADM=(...,account)
RemTransAdmAccount [1]	String	Abrechnungsnummer im fernen System eingeschlossen in Anführungszeichen / leer	REM: TRANS-ADM=(...,account)
RemProfile	String	*YES / *NONE *YES bedeutet Zugang über FTAC-Berechtigungsprofil	REM: TRANS-ADM=REMOTE-PROFILE
RemProcAdmId	String	leer	---
RemProcAdmAcc	String	leer	---
RemSuccProc	String	Ferne Folgeverarbeitung bei Erfolg, eingeschlossen in Anführungszeichen / *NONE / leer	REM: SUCC-PROC
RemFailProc	String	Ferne Folgeverarbeitung bei Fehler, eingeschlossen in Anführungszeichen / *NONE / leer	REM: FAIL-PROC
RemCcsn	String	Name des Zeichensatzes, der im fernen System verwendet wird, eingeschlossen in Anführungszeichen / *STD	REM: CCSN
FileSize	Number	Größe der Datei in Bytes / leer	FILESIZE
RecSize	Number	Maximale Satzlänge in Bytes / leer	RECSIZE
RecFormat	String	*STD / *VARIABLE / *FIX / *UNDEFINED Satzformat	RECFORM
StoreTime	Date	Zeitpunkt, an dem der Auftrag ins Auftragsbuch eingetragen wurde	STORE
ExpEndTime	Date	leer	---
TranspMode	String	*YES / *NO Übertragung transparent / nicht transparent	TRANSP
DataEncrypt	String	*YES / *NO Benutzerdaten verschlüsselt / nicht verschlüsselt übertragen	ENCRYPT
TabExp	String	*AUTO / *YES / *NO Tabulatorexpansion	TABEXP

Spalte	Typ	Werte und Bedeutung	Parameter
Mail	String	*ALL / *FAIL / *NO Ergebnismitteilung	LOC: MAIL
DiagCode	String	Diagnoseinformationen / leer	DIAGCODE
FileAvail	String	*IMMEDIATE / *DEFERRED / *NSPEC Verfügbarkeit (nur bei FTAM)	AVAILABILITY
StorageAccount	String	Abrechnungsnummer (nur bei FTAM) / leer	STOR-ACCOUNT
AccessRights	String	FTAM-Zugriffsrechte / leer Mögliche Werte sind @r, @w oder eine Kombination aus r, i, p, x, e, a, c, d	ACCESS-RIGHTS
LegalQualif	String	Rechtliche Bestimmung (nur bei FTAM) / leer	LEGAL-QUAL
PartnerPrio	String	*LOW / *NORM / *HIGH Partnerpriorität	PARTNER-PRIO
TargetFileForm	String	*STD / *BLOCK / *SEQ Dateiformat im Zielsystem	TARGFORM
TargetRecForm	String	*STD / *UNDEFINED Satzformat im Zielsystem	TRECFRM
Protection	String	*STD / *SAME Übertragung von Schutzattributen	PROTECT
GlobReqId	Number	Globale Auftragsidentifikation Bei lokal gestellten Aufträgen gleich der Auftrags-Id, bei fern gestellten Aufträgen gleich der Auftrags-Id auf der Initiator-seite	TRANSFER-ID oder GLOB-ID

[1] RemTransAdmAcc und RemTransAdmAccount haben dieselbe Bedeutung und denselben Inhalt. Aus Kompatibilitätsgründen sind beide Parameter in der CSV-Ausgabe enthalten.

Kurzausgabe von ftshwr im CSV-Format

Mit *ftshwr -s -csv* wird eine zweizeilige Tabelle mit der Anzahl der Aufträge im jeweiligen Status ausgegeben, siehe auch Seite 365.

Spalte	Typ	Werte
Act	Number	Anzahl der Aufträge im Zustand ACTIVE
Wait	Number	Anzahl der Aufträge im Zustand WAIT
Lock	Number	Anzahl der Aufträge im Zustand LOCK
Susp	Number	Anzahl der Aufträge im Zustand SUSPEND
Hold	Number	Anzahl der Aufträge im Zustand HOLD
Fin	Number	Anzahl der Aufträge im Zustand FINISHED
Total	Number	Gesamtanzahl aller Aufträge

Beispiel

```
ftshwr -s -csv

Act;Wait;Lock;Susp;Hold;Fin;Total
0;1;0;0;2;0;3
```

9.2 Wichtige CMX-Kommandos

Dieser Abschnitt enthält eine kurze Beschreibung der wichtigsten CMX-Kommandos, die für die Konfiguration von openFT benötigt werden, wenn openFT mit CMX betrieben wird. Detailliertere Informationen können Sie dem Handbuch „CMX - Betrieb und Administration“ entnehmen.

tnsxcom - TS-Directory erzeugen

Mit dem Kommando *tnsxcom* können Sie Dateien des Formates *tnsxfrm* in TS-Directories überführen. Dabei können Sie verschiedene Modi einstellen für Funktionen wie Syntaxprüfung, Aktualisierung oder Neuerstellung des TS-Directories.

Das Kommando hat folgende Syntax (gekürzt):

tnsxcom [**-l -s -S -u -i**] [datei]

Die Optionen haben die folgende Bedeutung:

-l LOAD-Modus
tnsxcom nimmt die Einträge einzeln aus der Datei *datei* und füllt das (bisher leere) TS-Directory mit den syntaktisch korrekten Einträgen.

-s CHECK-Modus
tnsxcom wendet nur die Syntaxprüfung auf die Datei *datei* an und protokolliert mögliche Syntaxfehler. Das TS-Directory wird nicht verändert.

-S CHECK-UPD-Modus
Wie bei der Option *-s* erfolgt in einem ersten Lauf zuerst die Syntaxprüfung auf die gesamte Datei *datei*. Treten dabei keine Syntaxfehler auf, so aktualisiert *tnsxcom* das TS-Directory in einem zweiten Lauf.

-u UPDATE-Modus
tnsxcom nimmt die Einträge einzeln aus der Datei *datei* und mischt die syntaktisch korrekten Einträge in das TS-Directory. Nicht vorhandene Einträge werden dabei erzeugt, vorhandene aktualisiert.

-i INTERAKTIV-Modus
tnsxcom liest Einträge im Format *tnsxfrm* von stdin, nachdem er durch Ausgabe eines Promptzeichens seine Eingabebereitschaft angezeigt hat und mischt diese in das TS-Directory. Nicht vorhandene Einträge werden dabei erzeugt, vorhandene aktualisiert.

datei Name der Datei mit Einträgen im Format *tnsxfrm*, die bei den Schaltern *-l*, *-s*, *-S* oder *-u* ausgewertet werden soll. Es können mehrere Dateien angegeben werden.

Beispiele

– Der folgende Aufruf überführt die Einträge aus der Datei *input.dir* in das aktuelle TS-Directory:
```
tnsxcom -S input.dir
```

– Sie möchten den Eintrag $FJAM aus dem TS-Directory löschen. Die Input-Datei *upd.dir* muss dazu folgenden Eintrag enthalten:
```
$FJAM DEL
```
Der Aufruf lautet: `tnsxcom -u upd.dir`

tnsxprop - Eigenschaften von TS-Anwendungen ausgeben

tnsxprop gibt die Werte aller Eigenschaften in einem abdruckbaren Format auf stdout aus, die in einem TS-Directory für die angegebene TS-Anwendungen enthalten sind.

Mit Hilfe des ersten Parameters kann man festlegen, in welchem Format die Eigenschaften ausgegeben werden sollen.

Die TS-Anwendungen werden durch die Parameterwerte von *name* bestimmt. Die Parameterwerte für *name* können auch aus der Datei *datei* an *tnsxprop* übergeben werden. Wird weder für *name* noch für *datei* eine Angabe gemacht, so bereitet *tnsxprop* die Eigenschaften aller TS-Anwendungen des TS-Directory im angegebenen Format auf.

Das Kommando hat folgende Syntax (gekürzt):

tnsxprop [**-S** | **-h**] [**-f** datei] [name ...]

-S Diese Angabe ist die Standardeinstellung. Mit diesem Schalter erfolgt die Ausgabe der Eigenschaften in symbolischer Darstellung im Format *tnsxfrm*.

-h Mit diesem Schalter erfolgt die Aufbereitung der Eigenschaften in sedezimaler Darstellung. Die Ausgabe erfolgt als Zeichenkette von Sedezimal-Ziffern, zusammen mit der entsprechenden Bitdarstellung, wobei das niederwertigste Bit ganz rechts steht.

-f datei

Für *datei* ist der Name einer Datei anzugeben, die die GLOBALEN NAMEN der TS-Anwendungen enthält, deren Eigenschaften abgefragt werden sollen. Die GLOBALEN NAMEN sind wie unter *name* beschrieben anzugeben.

name Für *name* ist der GLOBALE NAME der TS-Anwendung im TS-Directory wie folgt anzugeben:

NP5.NP4,NP3.NP2.NP1

Die einzelnen NP*i* sind die Namensteile des GLOBALEN NAMENS.

Dabei ist NP5 der Namensteil[5], also der Namensteil der untersten Hierarchiestufe. NP1 ist der Namensteil[1], also der in der Hierarchie höchste Namensteil. Die Namensteile sind in von links nach rechts aufsteigender hierarchischer Reihenfolge anzugeben.

Ist bei einem GLOBALEN NAMEN einer der Namensteile nicht belegt (z.B. NP4) und folgt diesem Namensteil noch ein Namensteil höherer Hierarchie (z.B. NP3), so ist von dem nicht belegten Namensteil nur das Trennzeichen (.) anzugeben. Eine Folge von Trennzeichen am Ende des Wertes von *name* kann weggelassen werden.

Enthalten die Namensteile Sonderzeichen, deren Sonderbedeutung eine Mehrdeutigkeit der Syntax verursachen würde, so müssen diese Sonderzeichen mit dem Gegenschrägstrich (\) entwertet werden. Im Zweifelsfall sollten Sie jedes Sonderzeichen entwerten; überflüssige Entwertungen werden von *tnsxprop* ignoriert.

Gibt man für einen Namensteil einen Stern (*) an, so liefert *tnsxprop* die Eigenschaften aller TS-Anwendungen die in allen anderen angegebenen Namensteilen mit der Angabe in *name* übereinstimmen (Filtermodus TS_RESTRICTED).

Beispiele

1. Die Eigenschaften der TS-Anwendung, die nur den Namensteil[5] mit dem Wert *Beispiel_1* hat, sollen in sedezimaler Darstellung ausgegeben werden:

   ```
   tnsxprop -h Beispiel_1
   ```

2. Die Eigenschaften der TS-Anwendung, die nur den Namensteil[5] mit dem Wert *Beispiel_1* hat, sollen in symbolischer Darstellung ausgegeben werden:

   ```
   tnsxprop Beispiel_1
   ```

3. Die Eigenschaften aller TS-Anwendung sollen in eine Datei *tns* ausgegeben werden:

   ```
   tnsxprop > tns
   ```

9.3 Transportsystem-Anwendungen in TNS eintragen

Ab openFT V10 ist die Verwendung des Transport Name Service (TNS) für Kopplung über TCP/IP nicht mehr notwendig. Wenn Sie den TNS dennoch nutzen, z.B. weil Sie mit anderen Transportsystemen als TCP/IP koppeln oder vorhandene TNS-Einträge nutzen möchten, muss CMX installiert sein und der Betrieb mit CMX und TNS muss explizit per Betriebsparameter eingeschaltet sein, z.B. mit dem Kommando *ftmodo -tns=y -cmx=y*. Alternativ dazu können Sie im openFT Explorer über das Menü *Administration*, Befehl *Betriebsparameter*, Registerblatt *Protokolle* die Optionen *TNS benutzen* und *CMX benutzen* aktivieren.

Der TNS identifiziert eine Transportsystem-Anwendung (TS-Anwendung) über einen symbolischen Namen, den sogenannten GLOBALEN NAMEN. Der symbolische Name kann allgemein aus bis zu fünf Namensteilen bestehen.

Diesen symbolischen Namen werden Adressinformationen zugeordnet. Die notwendigen Angaben wie Stationsnamen, Anwendungsnamen, Portnummern usw. erfahren Sie von Ihrem Netzverwalter.

Je nach Installationsvariante (Neuinstallation, Update-Installation) und Kopplungsart werden bestimmte Einträge schon bei der Installation von openFT gemacht, sofern vor der Installation von openFT auf dem System ein CMX installiert wurde (siehe Abschnitt „Automatisch erzeugte TNS-Einträge“ auf Seite 436).

Standard-TNS-Einträge per Skript erzeugen

Wird CMX erst nach openFT installiert oder sind keine aktuellen TNS-Einträge für openFT vorhanden, können Sie die Standard-TNS-Einträge für openFT wie folgt erstellen:

Rufen Sie das Skript */opt/openFT/bin/ftbin/ftgentns* auf.

TNS-Einträge manuell erzeugen

Die Einträge in den TNS können mit Hilfe des TNS-Compilers *tnsxcom* erfolgen. Dazu tragen Sie die TS-Anwendungen in eine Datei ein, die Sie mit Hilfe des TNS-Compilers *tnsxcom* übersetzen (siehe Abschnitt „tnsxcom - TS-Directory erzeugen“ auf Seite 432).
Einige Unix-System bieten auch eine grafische Oberfläche (Menüsystem oder Web-Interface), über die Sie die Partnersysteme eintragen können. Weitere Informationen dazu entnehmen Sie bitte dem CMX-Handbuch.

Weiterhin kann es sinnvoll sein, die fernen TS-Anwendungen der Partnersysteme einzutragen, die Aufträge an das lokale System stellen. Bei openFT-Partnern ab V8.1 ist darauf zu achten, dass der Name, unter dem Aufträge mit diesem Partner abgewickelt werden, der Instanzidentifikation des fernen Systems entspricht. Im Zweifelsfall ist hierfür ein TNS-Eintrag nötig.

Im Fall von WAN-Partnern lässt sich bei Aufträgen, die im fernen System erteilt werden, der Partner leichter identifizieren. Zum Beispiel wird der Name, mit dem der Partner im TNS eingetragen ist, in den Logging-Sätzen festgehalten. Bei FTAM-Partnern, die nicht über TCP/IP gekoppelt sind, ist ein Eintrag im TNS Voraussetzung.

Welche Einträge bei welcher Installationsvariante und bei welcher Kopplungsart automatisch bei der Installation angelegt bzw. modifiziert werden, können Sie dem Abschnitt „Automatisch erzeugte TNS-Einträge“ entnehmen.

Die Vorgehensweise beim Eintragen von fernen TS-Anwendungen wird ab Seite 439 beschrieben.

TNS-Einträge bei Cluster-Konfiguration

Beachten Sie bitte, dass eine Cluster-Konfiguration nur für TCP/IP unterstützt wird. Für Cluster-Konfigurationen müssen Sie daher alle openFT-spezifischen TNS-Einträge überprüfen und diejenigen Transportsystem-Einträge löschen, die nicht TCP/IP betreffen (d.h. alles außer RFC1006 und LANINET). Zwei Beispiele dazu finden Sie auf Seite 444 und Seite 449.

9.3.1 Automatisch erzeugte TNS-Einträge

Wenn auf dem System CMX installiert ist, werden bei der Installation von openFT je nach Installationsvariante bestimmte FT-Anwendungen automatisch in den TNS eingetragen bzw. bestehende Einträge entsprechend modifiziert.

Es wird empfohlen, die bei der Installation eingetragenen Anwendungen nicht zu modifizieren. Ist dies dennoch erforderlich, muss beachtet werden, dass die Portnummer des $FJAM-Eintrags durch 100 teilbar und die Portnummer des $FJAMOUT-Eintrags gleich Portnummer des $FJAM-Eintrags + 1 sein muss. Wenn Ihr System durch eine Firewall geschützt ist und von außen erreichbar sein soll, muss der Port des $FJAM-Eintrags in der Firewall freigeschaltet sein.

TNS-Einträge bei Neuinstallation

Bei einer Neuinstallation werden abhängig von der Plattform maximal folgende Einträge gemacht (siehe auch Datei */opt/openFT/config/tnsstd*):

```
$FJAM\
        TSEL    WANNEA T'$FJAM'
        TSEL    LANSBKA T'$FJAM'
        TSEL    WANSBKA T'$FJAM'
        TSEL    OSITYPE T'$FJAM'
        TSEL    RFC1006 T'$FJAM'
        TSEL    LANINET A'1100'
```

```
$FJAMOUT\
        TSEL    WANNEA T'$FJAMOUT'
        TSEL    LANSBKA T'$FJAMOUT'
        TSEL    WANSBKA T'$FJAMOUT'
        TSEL    OSITYPE T'$FJAMOUT'
        TSEL    RFC1006 T'$FJAMOUT'
        TSEL    LANINET A'1101'

$FTAM\
        PSEL    V''
        SSEL    V''
        TSEL    LANSBKA T'$FTAM'
        TSEL    WANSBKA T'$FTAM'
        TSEL    OSITYPE T'$FTAM'
        TSEL    RFC1006 T'$FTAM'
        TSEL    LANINET A'4800'
```

Die lokale TS-Anwendung $FJAM ist Ansprechpartner für Inbound-Aufträge von openFT-Partnern, $FJAMOUT für Outbound-Aufträge zu openFT-Partnern.

Die lokale TS-Anwendung $FTAM ist Ansprechpartner für alle Inbound- und Outbound-Aufträge mit FTAM-Partnern.

TNS-Einträge bei Update-Installation

Bei einer Update-Installation gilt:

- Es werden maximal die TNS-Einträge erzeugt, die auch bei einer Neuinstallation erzeugt werden.
- Wenn Einträge der Form $FJAM_OUTBOUND, *ftstd* oder *ftstdisdn* existieren, dann werden diese gelöscht.
- Alle anderen schon vorhandenen Einträge außer $FJAM_OUTBOUND, *ftstd* oder *ftstdisdn* bleiben unverändert.

Entsprechendes gilt auch, wenn auf Ihrem System vorher eine openFT-Version < V10.0 installiert war, da TNS-Einträge bei der Deinstallation nicht gelöscht werden.

9.3.2 Definition der lokalen TS-Anwendung für openFT-FTAM

Möchten Sie openFT-FTAM im Betrieb mit TNS nutzen, so muss die lokale Anwendung $FTAM definiert sein. Dies geschieht bei einer Neuinstallation bzw. Update-Installation automatisch, falls CMX installiert ist und falls kein $FTAM-Eintrag existiert. Die lokale Anwendung $FTAM wird für alle Aufträge mit FTAM-Partnern (outbound und inbound) verwendet.

Besonderheiten

Beim TCP/IP-LAN-Transportsystem sind zwei Einträge zum symbolischen Namen zu machen:

- ein Eintrag RFC1006 mit dem Transport-Selektor. Als Transport-Selektor geben Sie den symbolischen Namen $FTAM an. Die Angabe muss im TRANSDATA-Format (Indikator *T*) erfolgen.
- ein Eintrag LANINET mit der Portnummer. Die Portnummer wird im ASCII-Format angegeben.

Sie müssen den Eintrag in einem festgelegten Format (siehe Beispiele) machen.

Weitere Information dazu können Sie dem Handbuch zu CMX entnehmen.

Der GLOBALE NAME $FTAM ist vorgegeben. Für den Transport-Selektor wird `T'$FTAM'` empfohlen. Die Angaben `PSEL V''` und `SSEL V''` sind unbedingt erforderlich.

Beispieleinträge für openFT-FTAM auf Solaris Sparc

```
$FTAM\
   PSEL    V''                ; leerer Presentation Selektor
   SSEL    V''                ; leerer Session Selektor
   TSEL    WANSBKA T'$FTAM'   ; Eintrag für WAN-CONS, ISDN-CONS
   TSEL    LANSBKA T'$FTAM'   ; Eintrag für ETHN-CLNS/passiv
                              ; bei Koppl. zu CMX V3.0
                              ; notwendig
   TSEL    OSITYPE T'$FTAM'   ; Eintrag für ETHN-CLNS/active
   TSEL    RFC1006 T'$FTAM'   ; Eintrag für TCP/IP-RFC1006
   TSEL    LANINET A‘4800‘    ; Eintrag für TCP/IP
```

9.3.3 Definition der fernen TS-Anwendungen für openFT

Bei openFT-Partnern ab V8.1 ist darauf zu achten, dass der Name, unter dem Aufträge mit diesem Partner abgewickelt werden, der Instanzidentifikation des fernen Systems entspricht. Im Zweifelsfall ist hierfür ein TNS-Eintrag nötig, bei dem der GLOBALE NAME die Instanzidentifikation ist.

Für jedes weitere Partnersystem, das für lokal gestellte Aufträge erreichbar sein soll, muss ein TNS-Eintrag vorgenommen werden. In beiden oben angeführten Fällen können Sie für die Partnersysteme zusätzlich TNS-Einträge vornehmen und somit eigene Namen für die Partnersysteme vergeben. Die Einträge erfolgen in der Datei, die mit dem TNS-Compiler *tnsxcom* übersetzt wird oder über die grafische Oberfläche (falls vorhanden).

Als symbolischer Name (GLOBALER NAME) ist ein maximal 78 Zeichen langer alphanumerischer Name zu verwenden. Er darf keine Sonderzeichen enthalten, außer:

- "." als Separator
- "#" . Die Angabe hinter dem Zeichen "#" dient nur zur Unterscheidung bei gleichem Präfix. Damit haben Sie die Möglichkeit, einen Partner, der mehrere Adressen hat, mehrmals unter dem gleichen Namen (Präfix) einzutragen. Das ist nur sinnvoll bei Inbound-Aufträgen. So wird das Partnersystem immer mit der gleichen Partneradresse (entspricht dem Präfix) angezeigt.

Den symbolischen Namen können Sie beim Eintragen der Partneranwendung frei wählen. Er muss aber im lokalen System eindeutig sein. Welche weiteren Werte einzutragen sind, hängt davon ab, wie das ferne System an das Netz angeschlossen ist. Die Eingabe muss im TRANSDATA-Format (Indikator *T*) erfolgen. Die für die Einträge nötigen Informationen erhalten Sie von Ihrem Netzverwalter.

9.3.3.1 Beispieleinträge für openFT-Partner

Die nachfolgend aufgeführten Beispiele setzen voraus, dass das entsprechende Transportsystem auf Ihrem Unix-Rechner unterstützt wird.

Bitte beachten Sie, dass auf Unix-Systemen standardmäßig nur TCP/IP-RFC1006 vorhanden ist.

- Eintrag einer Partneradresse (für openFT für BS2000/OSD-Partner) bei Transfer über TCP/IP-RFC1006 (Port 102):

```
ftbs2\
        TA      RFC1006 123.4.5.68     T'$FJAM'
;                       Internet-Adr.  T-Selektor
```

- Eintrag einer PCMX-Partneradresse bei Transfer über TCP/IP-RFC1006 und einem PCMX-, CMX-V4.0- oder Windows-Partner (ab FT-PCD V2.6):

```
ftrfc\
        TA      RFC1006 123.4.5.67     PORT 1100 T'$FJAM'
;                       Internet-Adr.  Portnr    T-Selektor
```

- Eintrag variabler Internet-Adressen für ein- und denselben Partner (z.B. ein Notebook mit verschiedenen Einsatzorten und damit verbundenen verschiedenen Internet-Adressen) mit dem Namen *mobile*:

```
mobile\
        TA      RFC1006 100.22.33.45     PORT 1100 T'$FJAM'
;                       Internet-Adr1.  Portnr    T-Selektor
mobile#1\
        TA      RFC1006 101.20.30.40     PORT 1100 T'$FJAM'
;                       Internet-Adr2.  Portnr    T-Selektor
mobile#2\
        TA      RFC1006 102.21.31.41     PORT 1100 T'$FJAM'
;                       Internet-Adr3.  Portnr    T-Selektor
```

- Eintrag einer Partneradresse bei Transfer über ETHN-CLNS/active:

```
ftethna\
        TA      OSITYPE 49+006C080015304050FE T'$FJAM'
 ;                      OSI-Netzadresse       T-Selektor
```

(OSI-Netzadresse gemäß der Norm ISO 8348/Add.2, der Aufbau ist im Handbuch zu CMX beschrieben.)

- Eintrag einer Partneradresse bei Transfer über ETHN-CLNS/passive:

```
ftethnp\
        TA      LANSBKA 080014110960  T'$FJAM'
 ;                      Ethernet-Adr. T-Selektor
```

- Eintrag einer Partneradresse bei Transfer über WAN-NEA, WAN-NX25, ISDN-NEA, ISDN-NX25

```
ftwannea\
        TA      WANNEA T'$FJAM'    1/18            WAN 2
;                     T-Selektor  Rechner/Region  WAN CC
```

- Eintrag einer Partneradresse bei Transfer über WAN-CONS, ISDN-CONS

```
ftcons\
        TA     WANSBKA X.121 45890012233 T'$FJAM'  WAN 3
 ;                      SNPA-Info       T-Sel.    WAN CC
```

9.3.4 Definition der fernen TS-Anwendungen für openFT-FTAM

Für FTAM-Partner sind nur dann TNS-Einträge notwendig, wenn diese Partner nicht über TCP/IP gekoppelt werden. Um den Transport Name Service nutzen zu können, muss CMX installiert sein und der Betrieb mit CMX und TNS muss explizit per Betriebsparameter eingeschaltet sein, z.B. mit dem Kommando *ftmodo -tns=y -cmx=y*. Alternativ dazu können Sie im openFT Explorer über das Menü *Administration*, Befehl *Betriebsparameter*, Registerblatt *Protokolle* die Optionen *TNS benutzen* und *CMX benutzen* aktivieren.

Für alle über TCP/IP erreichbaren Partnersysteme sind ab openFT V10 keine TNS-Einträge mehr notwendig, da Sie die Partneradresse direkt angeben oder in der Partnerliste eintragen können.

Die Angaben für Presentation-/Session- und Transport-Selektoren sind in ASCII (A'...'), EBCDIC (E'...'), TRANSDATA-Format (T'...') oder sedezimal (X'...') möglich. Presentation- und Session-Selektoren dürfen 0 bis 16 Byte lang sein. Bei fehlendem Presentation- oder Session-Selektor ist die Angabe `PSEL V''` oder `SSEL V''` unbedingt erforderlich. Bei den Transportadressen für FTAM-Partner darf keine CC-Liste angegeben werden.

Wenn ein Partner unterschiedliche Adressen für In- und Outboundaufträge hat, kann zur Administrationserleichterung ein dummy-Eintrag mit der inboundseitig ankommenden Absenderadresse erfolgen. Dies ist durch die Angabe eines "#" Zeichens, gefolgt von einer Nummer im Namensteil 5 des "Globalen Namens" möglich.

Besonderheiten

Die Einträge der mit *tnsxcom* zu übersetzenden Datei müssen im Prinzip so aussehen, wie in den folgenden Beispielen auf Seite 443. Die folgende Checkliste können Sie dabei zu Hilfe nehmen.

Checkliste

Die folgende Checkliste soll Ihnen helfen, die notwendigen Daten für den TNS-Eintrag eines FTAM-Partners zu erheben. Die Fragen müssen vom FTAM-Partner beantwortet werden.

1. openFT-FTAM baut die Verbindung auf.

   Welche Werte haben folgende Parameter (mit Angabe der Kodierung):

a)	called X121/ LAN Address/ NSAP/X.31	_____		
b)	called TSEL	_____	Code:	_____
c)	called SSEL	_____	Code:	_____
d)	called PSEL	_____	Code:	_____
e)	Protocol Identifier (Layer 3 CUD)	_____		
f)	called APT	_nein _____NILAPTitle __ [1)]		
g)	called AEQ	_nein _____ [1)]		
h)	calling APT	_nein _____NILAPTitle __ [1)]		

[1)] APT (Application Process Title) und AEQ (Application Entity Qualifier) werden nicht in den TNS-Einträgen, sondern in openFT-Kommandos angegeben. Manche FTAM-Partner erwarten APTs und evtl. AEQs, manche erwarten, dass keine APTs/AEQs angegeben werden.

2. Der Partner baut die Verbindung auf.

   Welche Werte haben folgende Parameter (mit Angabe der Kodierung):

a)	calling X121/ LAN Address/ NSAP/X.31	_____		
b)	calling TSEL	_____	Code:	_____
c)	calling SSEL	_____	Code:	_____
d)	calling PSEL	_____	Code:	_____

Sie müssen auf eine korrekte Groß- und Kleinschreibung achten und daran denken, dass Leerzeichen und X‘00‘ in den Angaben für die Selektoren korrekt angegeben werden.

9.3.4.1 Beispieleinträge für FTAM-Partner

Die nachfolgend aufgeführten Beispiele setzen voraus, dass das entsprechende Transportsystem auf Ihrem Unix-Rechner unterstützt wird.

Bitte beachten Sie, dass auf Unix-Systemen standardmäßig nur TCP/IP-RFC1006 vorhanden ist.

- Eintrag einer Partneradresse bei Transfer über TCP/IP-RFC1006. Der Partner unterstützt die von RFC1006 standardisierte Portnummer 102.

```
ftamrfc\
     PSEL    V''
     SSEL    V''
     TA      RFC1006  123.4.5.67      T'$FTAM'
;                     Internet-Adr.   T-Selektor
```

- Eintrag einer Partneradresse (openFT ≤ V10.0 für Windows mit FTAM-Funktionalität) bei Transfer über TCP/IP-RFC1006 (Port 4800):

```
ftamwnt\
    PSEL    V''
    SSEL    V''
    TA      RFC1006  123.4.5.68     PORT 4800    A'SNI-FTAM'
;                    Internet-Adr.  Portnr       T-Selektor
```

- Eintrag einer Partneradresse bei Transfer über ETHN-CLNS/active:

```
ftametha\
    PSEL    V''
    SSEL    V''
    TA      OSITYPE 49+006C080015304050FE T'$FTAM'
 ;                      OSI-Netzadresse   T-Selektor
```

(OSI-Netzadresse gemäß der Norm ISO 8348/Add.2, der Aufbau ist im Handbuch zu CMX beschrieben.)

- Eintrag einer Partneradresse bei Transfer über ETHN-CLNS/passive:

```
ftamethp\
    PSEL    V''
    SSEL    V''
    TA      LANSBKA 080014110960  T'$FTAM'
 ;                 Ethernet-Adr. T-Selektor
```

- Eintrag einer Partneradresse bei Transfer über WAN-CONS, ISDN-CONS

```
ftamcons\
    PSEL    V''
    SSEL    V''
    TA      WANSBKA X.121 45890040034 T'$FTAM' X'D5000002'
 ;                        SNPA-Info    T-Sel.   TPI
```

9.4 openFT im Cluster mit Unix-Systemen

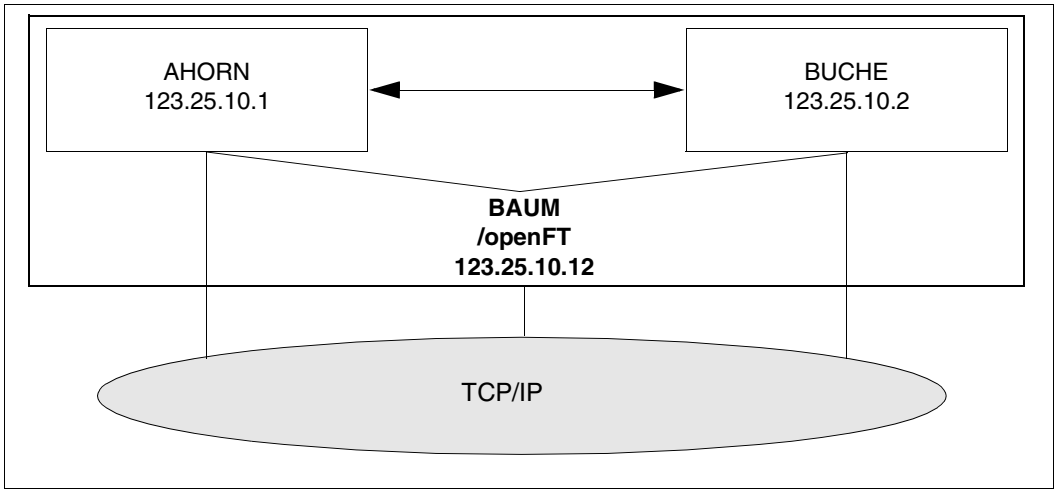
Software-Voraussetzungen

Auf allen Knoten des Clusters muss dieselbe openFT-Version installiert werden. Wenn Sie im Betrieb mit CMX den TNS verwenden, beachten Sie bitte Abschnitt „Hinweise zur Verwendung des TNS“ auf Seite 452.

Es wird empfohlen, ohne CMX und TNS zu arbeiten.

9.4.1 Beispiel 1: eine ausfallsichere Instanz

Der Cluster BAUM (Unix-Systeme, IP-Adresse 123.25.10.12) besteht aus den beiden Rechnern AHORN (IP-Adresse 123.25.10.1) und BUCHE (IP-Adresse 123.25.10.2) . Das Ausfallkonzept besteht darin, dass BAUM entweder auf Rechner AHORN oder BUCHE läuft. Ausfallgesichert ist in diesem Fall nur eine openFT-Instanz.



openFT im Cluster - eine ausfallsichere Instanz

Konfigurieren Sie den Cluster so, dass eine Platte immer verfügbar ist. In diesem Beispiel ist es das Verzeichnis */openFT*.

Erforderliche Schritte auf dem Rechner AHORN

1. openFT installieren (ggf. inkl. Zusatzprodukte openFT-CR, openFT-FTAM und openFT-FTP)
2. openFT deaktivieren:

   ```
   ftstop
   ```

3. Im Betrieb mit CMX und TNS müssen Sie die TNS-Einträge $FJAM, $FJAMOUT und ggf. $FTAM auf dem System anpassen, es dürfen nur RFC1006 und LANINET Einträge enthalten sein, s.o..
4. Adresse der Instanz *std* setzen:

   ```
   ftmodi std -addr=AHORN
   ```

   Die Instanz *std* meldet sich ausschließlich bei der Adresse AHORN an. Alle weiteren Adressen auf dem Rechner stehen für andere Instanzen zur Verfügung.
5. openFT auf Instanz *std* aktivieren und Identifikation setzen, falls dies nicht schon bei der Installation automatisch geschehen ist:

   ```
   . ftseti std
   [ftmodo -id=AHORN.WALD.NET]
   ftstart
   ```

6. Platte */openFT* auf AHORN mounten.
7. Neue Instanz *cluster* erzeugen und überprüfen; das Verzeichnis */openFT* muss vorhanden sein, das Verzeichnis */openFT/cluster* darf nicht vorhanden sein:

   ```
   ftcrei cluster /openFT/cluster -addr=BAUM.WALD.NET
   ftshwi @a -l

   Instanz  Adresse         Verzeichnis
   -------  -----------     --------------------
   cluster  BAUM.WALD.NET   /openFT/cluster
   std      AHORN           /var/openFT/std
   ```

8. Falls in der Instanz *cluster* mit Authentifizierung gearbeitet werden soll, dann müssen Public Keys von Partnerrechnern im Verzeichnis */openFT/cluster/syskey* hinterlegt, bzw. der Public Key aus dem Verzeichnis */openFT/cluster/config* den Partnerrechnern zur Verfügung gestellt werden.
9. Instanz *cluster* deaktivieren:

   ```
   ftseti std; ftdeli cluster
   ```

Erforderliche Schritte auf dem Rechner BUCHE

1. openFT installieren (ggf. inkl. Zusatzprodukte openFT-CR, openFT-FTAM und openFT-FTP)
2. openFT deaktivieren:

   ```
   ftstop
   ```

3. Im Betrieb mit CMX und TNS müssen Sie die TNS-Einträge $FJAM, $FJAMOUT und ggf. $FTAM auf dem System anpassen, falls vorhanden, es dürfen nur RFC1006 und LANINET Einträge enthalten sein, s.o.
4. Adresse der Instanz *std* setzen:

   ```
   ftmodi std -addr=BUCHE
   ```

   Die Instanz *std* meldet sich ausschließlich bei der Adresse BUCHE an. Alle weiteren Adressen auf dem Rechner stehen für andere Instanzen zur Verfügung.
5. openFT auf Instanz *std* aktivieren und Identifikation setzen, falls dies nicht schon bei der Installation automatisch geschehen ist:

   ```
   . ftseti std
   [ftmodo -id=BUCHE.WALD.NET]
   ftstart
   ```

6. Erstellen Sie anschließend ein Shell-Skript zur Verwaltung der Instanzen, das die Fälle *start*, *stop* und *check* behandelt. Das Skript muss auf den Rechnern AHORN und BUCHE verfügbar und konfiguriert sein und könnte bei Einsatz von RMS (Reliant Monitor Services) so aussehen:

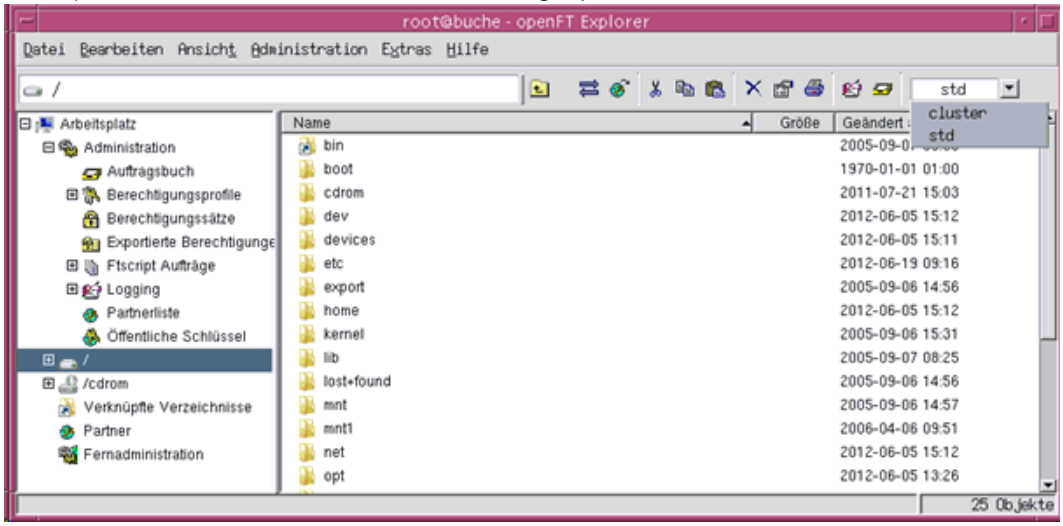
   ```
   PAR=$1
   BIN=/opt/bin; export BIN
   INST=cluster
   OPENFTINSTANCE=$INST; export OPENFTINSTANCE
   case $PAR in
   start) OPENFTINSTANCE=std; export OPENFTINSTANCE
      $BIN/ftcrei $INST /openFT/$INST
      case $? in
         0|5) continue;;
         *) exit 1;;
      esac
      OPENFTINSTANCE=$INST; export OPENFTINSTANCE
      $BIN/ftstart 2>/dev/null
      case $? in
         0|180) exit 0;;
         *) exit 1;;
      esac;;
   ```

```
stop) $BIN/ftstop 2>/dev/null
   case $? in
      0|181) continue;;
      *) exit 1;;
   esac
   OPENFTINSTANCE=std; export OPENFTINSTANCE
   $BIN/ftdeli cluster
   case $? in
      0) exit 0;;
      *) exit 1;;
   esac;;
check) VALUE=`$BIN/ftshwo -csv 2>/dev/null |fgrep FtStarted\
               |sed s/";"/" "/g`
   [ -z $VALUE ] && exit 1
   set $VALUE
   i=1
   FTROW=1
   while [ "$1" != "FtStarted" ]
   do shift
   FTROW=`expr $FTROW + 1`
   done
   FTSTART=`$BIN/ftshwo -csv|fgrep -v FtStarted|cut \
           -f$FTROW -d\;`
   if [ $FTSTART = '*NO'  ]
   then # openFT server not active
   exit 1
   else # openFT server active
   exit 0
   fi
   ;;
esac
```

Arbeiten mit den einzelnen Instanzen

Wenn alles erledigt ist, gibt es auf den Rechnern AHORN und BUCHE jeweils eine Standardinstanz, die nicht ausfallgesichert ist. Durch Auswahl im openFT Explorer oder durch das Kommando . *ftseti std* arbeiten Sie mit der jeweiligen Standardinstanz. Sie können in den Standardinstanzen alle openFT-Funktionen nutzen (z.B. Berechtigungsprofile einrichten, Logging-Sätze ansehen usw.). Von außen können die Standardinstanzen auf AHORN und BUCHE ganz normal über die Adressen dieser Rechner (123.25.10.1 oder 123.25.10.2) angesprochen werden.

Die ausfallgesicherte Instanz *cluster* steht auf demjenigen der beiden Rechner zur Verfügung, auf dem die Platte */openFT* aktuell gemountet ist. Auf diesem Rechner können Sie über den openFT Explorer oder durch das Kommando
. *ftseti cluster* mit der Instanz arbeiten und dort alle openFT-Funktionen nutzen. Hier ist es nicht notwendig zu wissen, auf welchem Rechner die Platte */openFT* gemountet ist. Als Partner müssen Sie BAUM auswählen. Von außen wird der Cluster BAUM (openFT-Instanz *cluster*) unter der IP-Adresse 123.25.10.12 angesprochen.

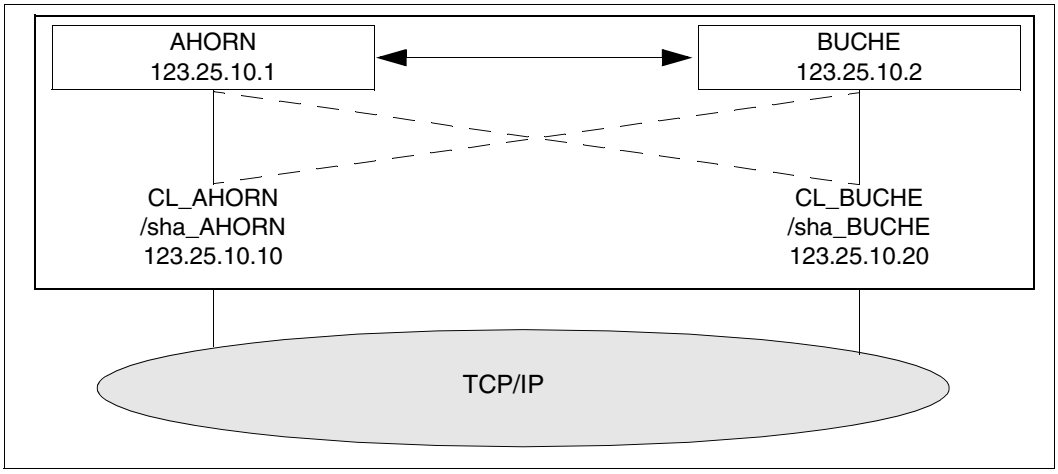


Instanz im Cluster auswählen

9.4.2 Beispiel 2: Ausfallsicherheit für beide Rechner des Clusters

Der Cluster mit Unix-Systemen besteht wiederum aus zwei Rechnern AHORN (IP-Adresse 123.25.10.1) und BUCHE (IP-Adresse 123.25.10.2).

In diesem Beispiel soll aber auf beiden Rechnern je eine ausfallgesicherte openFT-Instanz zur Verfügung stehen. Dazu wird der Rechner AHORN durch CL_AHORN (IP-Adresse 123.25.10.10) und der Rechner BUCHE durch CL_BUCHE (IP-Adresse 123.25.10.20) überlagert. Fällt der Rechner AHORN aus, so wird CL_AHORN auf den Rechner BUCHE umgeschaltet. Fällt der Rechner BUCHE aus, dann wird CL_BUCHE auf den Rechner AHORN umgeschaltet.



openFT im Cluster - ausfallsichere Instanzen auf zwei Rechnern

Konfigurieren Sie den Cluster so, dass für jeden Rechner eine Platte immer verfügbar ist, beispielsweise */sha_AHORN* und */sha_BUCHE*.

Erforderliche Schritte auf dem Rechner AHORN

1. Standardinstanz konfigurieren wie im Beispiel 1.
2. Platten */sha_AHORN* und */sha_BUCHE* auf AHORN mounten.
3. Instanzen *ahorn* und *buche* erzeugen und überprüfen:

```
ftcrei ahorn /sha_AHORN/FTCL -addr=CL_AHORN.WALD.NET
ftcrei buche /sha_BUCHE/FTCL -addr=CL_BUCHE.WALD.NET
ftshwi @a -l

Instanz    Adresse            Verzeichnis
---------- ----------         --------------------
ahorn      CL_AHORN.WALD.NET  /sha_AHORN/FTCL
buche      CL_BUCHE.WALD.NET  /sha_BUCHE/FTCL
std        AHORN              /var/openFT/std
```

4. Instanzen *ahorn* und *buche* deaktivieren:

```
ftdeli ahorn
ftdeli buche
```

Erforderliche Schritte auf dem Rechner BUCHE

1. Standardinstanz konfigurieren wie im Beispiel 1.
2. Erstellen Sie anschließend jeweils ein Shell-Skript zur Steuerung von openFT auf den Rechnern AHORN und BUCHE, das die Fälle *start, stop und check* behandelt. Beide Skripts müssen jeweils auf beiden Rechnern verfügbar sein. Das Shell-Skript könnte beim Einsatz von RMS beispielsweise so aussehen (im Skript für BUCHE muss im Folgenden *ahorn* durch *buche* ersetzt werden):

```
PAR=$1
BIN=/opt/bin; export BIN
INST=ahorn
OPENFTINSTANCE=$INST; export OPENFTINSTANCE
case $PAR in
start) OPENFTINSTANCE=std; export OPENFTINSTANCE
   $BIN/ftcrei $INST /sha_AHORN/FTCL
   case $? in
      0|5) continue;;
      *) exit 1;;
   esac
   OPENFTINSTANCE=$INST; export OPENFTINSTANCE
   $BIN/ftstart 2>/dev/null
   case $? in
      0|180) exit 0;;
      *) exit 1;;
   esac;;
stop) $BIN/ftstop 2>/dev/null
   case $? in
      0|181) exit 0;;
      *) exit 1;;
   esac
   OPENFTINSTANCE=std; export OPENFTINSTANCE
   $BIN/ftdeli $INST
   case $? in
      0)exit 0;;
      1)exit1;;
   esac;;
check) VALUE=`$BIN/ftshwo -csv|fgrep FtStarted \
              |sed s/";"/" "/g`
   set $VALUE
   i=1
   FTROW=1
   while [ "$1" != "FtStarted" ]
   do shift
      FTROW=`expr $FTROW + 1`
   done
   FTSTART=`$BIN/ftshwo -csv|fgrep -v FtStarted \
            |cut -f$FTROW -d\;`
   if [ $FTSTART = '*NO' ]
   then # openFT server not active
      exit 1
   else # openFT server active
      exit 0
   fi;;
esac
```

Arbeiten mit den einzelnen Instanzen

Wenn alles erledigt ist, gibt es auf den Rechnern AHORN und BUCHE jeweils eine Standardinstanz, die nicht ausfallgesichert ist. Durch Auswahl im openFT Explorer oder durch das Kommando . *ftseti std* arbeiten Sie mit der jeweiligen Standardinstanz. Sie können in den Standardinstanzen alle openFT-Funktionen nutzen (z.B. Berechtigungsprofile einrichten, Logging-Sätze ansehen usw.). Von außen können die Standardinstanzen auf AHORN und BUCHE ganz normal über die Adressen dieser Rechner (123.25.10.1 oder 123.25.10.2) angesprochen werden.

Die openFT-Instanzen *ahorn* und *buche* stehen jeweils auf dem Rechner zur Verfügung, auf dem die entsprechende Platte gemountet ist. Sie können wie gewohnt über den openFT Explorer oder die Kommandoschnittstelle genutzt werden.

Um Dateien zu diesen Instanzen zu übertragen, müssen die IP-Adressen von CL_AHORN.WALD.NET bzw. CL_BUCHE.WALD.NET (123.25.10.10 bzw. 123.25.10.20) angesprochen werden.

9.4.3 Hinweise zur Verwendung des TNS

Auf Solaris dürfen die TNS-Einträge nur TCP/IP-Bestandteile enthalten. Eine Eingabedatei für das Kommando *tnsxcom* könnte wie folgt aussehen:

```
$FJAM      DEL

$FJAM\
   TSEL    RFC1006  T'$FJAM'   ; Eintrag für TCP/IP-RFC1006
   TSEL    LANINET  A'1100'    ; Eintrag für TCP/IP

$FJAMOUT DEL

$FJAMOUT\
   TSEL    RFC1006  T'$FJAMOUT' ; Eintrag für TCP/IP-RFC1006
   TSEL    LANINET  A'1101'     ; Eintrag für TCP/IP

$FTAM      DEL

$FTAM
   PSEL    V''                  ; leerer Presentation Selektor
   SSEL    V''                  ; leerer Session Selektor
   TSEL    RFC1006  T'$FTAM'    ; Eintrag für TCP/IP-RFC1006
   TSEL    LANINET  A'4800'     ; Eintrag für TCP/IP
```

Damit werden die im TNS vorhandenen Einträge beim *tnsxcom* überschrieben.

9.5 Exitcodes und Meldungen zu Administrationskommandos

Nachfolgend finden Sie die von openFT ausgegebenen Fehlermeldungen, ihre Exit-Codes sowie Bedeutung und Maßnahme. Bitte beachten Sie, dass Umlaute auf manchen Systemen nicht korrekt dargestellt werden können. In diesem Fall wird der Meldungstext mit Doppelvokalschreibweise ausgegeben, z.B. ae statt ä.

Die Beschreibung ist folgendermaßen aufgebaut:

Exitcode Meldungstext
ggf. Bedeutung und Maßnahme

9.5.1 Meldungen bei allen Kommandos

0 Das Kommando wurde erfolgreich ausgeführt

3 Das Kommando wurde entsprechend der Antwort auf eine Rückfrage abgebrochen

4 Bei der Bearbeitung eines Kommandos trat ein Syntaxfehler auf

225 Informationsausgabe abgebrochen

Bedeutung:
Es wurde z.B. ein show-Kommando unterbrochen.

Maßnahme:
Kommando wiederholen

226 Inhalt der Monitordatei inkonsistent

Bedeutung:
Das Kommando kann nicht angenommen werden, weil der Inhalt der angegebenen Monitordatei nicht konsistent ist.
Mögliche Fehlerursache: Der Benutzer hat auf die Monitordatei anders als lesend zugegriffen, während sie einen FT-Auftrag überwachte.
Der Inhalt der Monitordatei ist damit nicht mehr verwendbar.

227 Monitordatei wird nicht von openFT verwendet

Maßnahme:
Namen der Monitordatei korrigieren und Kommando wiederholen.

228 Monitordatei nicht vorhanden

Maßnahme:
Namen der Monitordatei korrigieren und Kommando wiederholen.

236 Eingestellte Instanz '<Instanz>' nicht mehr gefunden

Bedeutung:
Das Kommando wurde abgewiesen, die Instanz '<Instanz>' ist nicht mehr vorhanden.

250 Bei der Bearbeitung eines Kommandos trat ein interner Fehler auf

251 Kommando mit Core Dump abgebrochen

253 Die eingestellte openFT Instanz ist ungültig

Bedeutung:
Bei der Bearbeitung eines Kommandos wurde festgestellt, dass die eingestellte Instanz ungültig ist.

255 ftexec/ftadm Kommando fehlgeschlagen

Bedeutung:
Die entfernte Ausführung eines Kommandos mit Hilfe von ftexec oder ftadm schlug fehl.

9.5.2 Meldungen zu Administrationskommandos und Messdatenerfassung

Für die nachfolgend aufgeführten Meldungen muss der Exitcode bei *fthelp* um 1000 erhöht werden, z.B. 1034 statt 34.

20 openFT bereits gestartet

Bedeutung:
openFT kann in jeder Instanz nur einmal gestartet werden.

Maßnahme:
openFT ggf. beenden.

21 Auftrag muss zuerst ohne FORCE Option gelöscht werden

Bedeutung:
Vor der Verwendung der FORCE Option muss das Kommando ohne FORCE Option aufgerufen werden.

Maßnahme:
Kommando zunächst ohne FORCE Option absetzen.

29 Maximale Anzahl Schlüsselpaarsätze überschritten

Maßnahme:
Vor dem Anlegen eines neuen Schlüsselpaarsatzes muss zuerst ein älterer Schlüsselpaarsatz gelöscht werden.

30 Warnung: Letzter Schlüsselpaarsatz gelöscht

Bedeutung:
Der letzte Schlüsselpaarsatz wurde gelöscht.
Ohne Schlüsselpaarsatz ist keine verschlüsselte Übertragung, Authentifizierung und Datenintegritätsprüfung möglich.

Maßnahme:
Erzeugen Sie einen neuen Schlüsselpaarsatz.

31 Kein Schlüsselpaarsatz vorhanden

Bedeutung:
Alle Übertragungen werden ohne Verschlüsselung durchgeführt.

Maßnahme:
Erzeugen Sie bei Bedarf einen Schlüsselpaarsatz.

32 Letzter Schlüsselpaarsatz darf nicht gelöscht werden

33 Die öffentlichen Schlüsseldateien konnten nicht aktualisiert werden

Bedeutung:
Der Inhalt der Datei *syspkf* konnte nicht vollständig aktualisiert werden.

Als Fehlerursache kommen in Betracht:
– Die Datei *syspkf* ist gesperrt,
– Speicherplatz für die Einrichtung der Datei *syspkf* reicht nicht aus.

Maßnahme:
Je nach Fehlerursache geeignete Maßnahmen treffen.
– Dateisperre aufheben.
– Speicherplatz zuweisen bzw. den Systemverwalter darum bitten.

Aktualisieren Sie den Schlüssel mit *ftupdk*.

34 Kommando nur für FT-, FTAC- oder ADM-Verwalter erlaubt

Bedeutung:
Das Kommando ist nur für den FT-, FTAC- oder ADM-Verwalter erlaubt.

Maßnahme:
Das Kommando ggf. durch den FT-, FTAC- oder ADM-Verwalter ausführen lassen.

35 Kommando nur für FT-Verwalter erlaubt

Bedeutung:
Das Kommando ist nur für den FT-Verwalter erlaubt.

Maßnahme:
Das Kommando ggf. durch den FT-Verwalter ausführen lassen.

36 Benutzer nicht für andere Kennungen berechtigt

Bedeutung:
Der Benutzer ist nicht berechtigt, im Kommando eine andere, fremde Benutzerkennung anzugeben.

Maßnahme:
Eigene Kennung angeben oder Kommando vom FT- bzw. FTAC-Verwalter ausführen lassen.

37 Schlüsselreferenz unbekannt

Bedeutung:
Die angegebene Schlüsselreferenz ist unbekannt.

Maßnahme:
Das Kommando mit einer existierenden Schlüsselreferenz wiederholen.

38 Auftrag <Auftrags-Id> ist in der Beendigungsphase und kann nicht mehr gelöscht werden

39 openFT nicht aktiv

Bedeutung:
Der openFT ist nicht gestartet.

Maßnahme:
openFT ggf. starten.

40 Config-Userid nicht bekannt oder Speicherplatz nicht ausreichend

Bedeutung:
Die Config-Userid der aktuellen Instanz ist entweder nicht bekannt oder der ihr zugewiesene Speicherplatz reicht nicht aus für die Einrichtung des Auftragsbuchs, der Datei zur Speicherung der Überwachungsdaten oder der Schlüsseldateien.

Maßnahme:
Die Config-Userid entweder einrichten oder ihr mehr Speicherplatz zuweisen bzw. den Systemverwalter darum bitten.

41 Angegebene Datei ist keine gültige Überwachungsdatei

42 openFT konnte nicht gestartet werden

43 Partner mit gleichem Attribut '<1>' bereits in der Partnerliste

Bedeutung:
In der Partnerliste existiert bereits ein Partnereintrag mit dem gleichen Attribut <Attribut>.

Maßnahme:
Das Attribut <Attribut> bei Partnereinträgen muss eindeutig sein.
Kommando entsprechend korrigieren und wiederholen.

44 Maximale Partneranzahl überschritten

Bedeutung:
Die Partnerliste enthält bereits die maximal zulässige Anzahl von Partnereinträgen.

Maßnahme:
Nicht mehr benötigten Partner löschen.

45 Kein Partner in Partnerliste gefunden

Bedeutung:
Es wurde kein Partner zur angegebenen Selektion in der Partnerliste gefunden.

Maßnahme:
Prüfen, ob der angegebene Partnername bzw. die angegebene Partneradresse richtig war.
Gegebenenfalls Kommando mit korrekten Angaben wiederholen.

46 Protokolltyp des Partners kann nicht geändert werden

Bedeutung:
Der Protokolltyp des Partnereintrags kann nachträglich nicht geändert werden.

Maßnahme:
Ggf. den Partner aus der Partnerliste löschen und mit neuem Protokolltyp wieder eintragen.

47 Auftrag <Auftrags-Id> nicht gefunden

Bedeutung:
Der Auftrag mit der Transfer-Id <Auftrags-Id> wurde nicht gefunden.

Maßnahme:
Vorhandene Transfer-Id angeben und Kommando wiederholen.

48 Aktive Aufträge konnten noch nicht gelöscht werden

49 CCS Name '<1>' unbekannt

50 ftscript Prozess konnte nicht gestartet werden

51 Fehler beim Ausgeben eines ftscript Benutzers

52 Maximale ftscript-Benutzer-Anzahl überschritten

53 ftscript-Kapitel nicht gefunden

54 ftscript-Id nicht gefunden

55 ftscript-Datei nicht gefunden

56 ftscript-Auftrag ist nicht beendet

57 Inbound Aufträge können nicht modifiziert werden

58 Die Konfiguration des ADM-Trap-Servers ist unstimmig

59 Monitoring ist nicht aktiv

Bedeutung:
Das Kommando wird nur bei eingeschalteter Messdatenerfassung unterstützt.

Maßnahme:
Aktivieren Sie die Messdatenerfassung in den Betriebsparametern und wiederholen Sie das Kommando.

60 Datei konnte nicht erzeugt werden <2>

Bedeutung:
Das Kommando wurde nicht ausgeführt, da die lokale Datei nicht erzeugt werden konnte.

Maßnahme:
Verzeichnis und Zugriffsrechte überprüfen. Kommando wiederholen.

61 Übergeordnetes Verzeichnis nicht gefunden

Bedeutung:
Beim Exportieren der Konfigurationsdaten konnte die lokale Datei nicht angelegt werden, weil der angegebene Pfad nicht existiert.

Maßnahme:
Pfad für Konfigurationsdatei anlegen bzw. korrigieren und Kommando wiederholen.

62 Datei existiert bereits

Bedeutung:
Das Kommando wurde nicht ausgeführt, da die angegebene Datei bereits existiert.

Maßnahme:
Entweder existierende Konfigurationsdatei löschen bzw. einen anderen Namen wählen und Kommando wiederholen.

63 Resultierender Dateiname zu lang

Bedeutung:
Der Dateiname ist syntaktisch falsch bzw. zu lang. Als Fehlerursache kommt die Angabe eines teilqualifizierten Dateinamens in Betracht.

Maßnahme:
Kommando mit richtiger Syntax wiederholen.

64 Datei gegen Mehrfachzugriff gesperrt

Bedeutung:
Das Kommando wurde nicht ausgeführt, da die Datei bereits durch einen anderen Prozess gesperrt ist.

Maßnahme:
Kommando später wiederholen.

65 Datei nicht gefunden

Bedeutung:
Das Kommando wurde nicht ausgeführt, da die angegebene Datei nicht gefunden wurde.

Maßnahme:
Dateinamen korrigieren und Kommando wiederholen.

66 Zu wenig Speicherplatz für Datei

Bedeutung:
Das Kommando wurde nicht ausgeführt, weil der zulässige Speicherplatz auf dem lokalen Datenträger erschöpft ist.

Maßnahme:
Je nach Fehlerursache geeignete Maßnahmen treffen.

- Nicht mehr benötigte Dateien löschen, oder
- Systemverwalter bitten, mehr Speicherplatz zuzuweisen.

67 Syntaxfehler im resultierenden Dateinamen

Bedeutung:
Der Zugriff auf die Datei kann nicht erfolgen, da z.B. der absolute Dateiname zu lang wird.

Maßnahme:
Pfad oder Dateiname verkürzen. Kommando wiederholen.

68 Zugriff auf Datei ist unzulässig <2>

Bedeutung:
Das Kommando wurde nicht ausgeführt, da die Datei nur bestimmte Zugriffsmodi zulässt (z.B. nur lesen).

Maßnahme:
Dateinamen oder Dateischutzmerkmale korrigieren.
Kommando wiederholen.

69 Fehler beim Zugriff auf Datei <2>

Bedeutung:
<2>: DVS-Fehler

Maßnahme:
Geeignete Maßnahmen treffen gemäß Fehlercode.

70 Konfigurationsdaten fehlerhaft

Bedeutung:
Die Konfigurationsdaten sind syntaktisch oder semantisch falsch und können daher nicht importiert werden.

Maßnahme:
Den Fehler anhand der zusätzlichen Diagnoseausgaben korrigieren und danach das Importieren der Konfigurationsdaten wiederholen.

71 Importieren der Konfigurationsdaten bei gestartetem Fernadministrations-Server nicht möglich

Bedeutung:
Die Änderungen in den Konfigurationsdaten sind so umfangreich, dass sie nur bei beendetem Fernadministrations-Server importiert werden können.

Maßnahme:
openFT mit dem Kommando *ftstop* beenden und danach das Importieren der Konfigurationsdaten wiederholen.

73 Kommando abgebrochen

Bedeutung:
Der Anwender hat das Kommando abgebrochen.

74 Kommando nur für ADM-Verwalter auf einem Fernadministrations-Server erlaubt

Bedeutung:
Das Kommando ist nur für den ADM-Verwalter erlaubt.

Maßnahme:
Das Kommando ggf. durch den ADM-Verwalter ausführen lassen.

77 Wechseln des Transportzugriffsystems nicht möglich. Ursache: <1>

Bedeutung:
Der Betriebsmodus mit oder ohne CMX konnte mit dem *ftmodo*-Kommando nicht geändert werden. Als mögliche Ursachen kommen in Betracht:

openFT ist gestartet

CMX ist nicht installiert

78 Zu kurze Zeit nach letztem Logging-Datei-Wechsel

Bedeutung:
Logging-Datei kann momentan noch nicht gewechselt werden, da der zeitstempelabhängige Dateinamensteil sich nicht vom Namensteil der aktuellen Logging-Datei unterscheidet.

Maßnahme:
Wiederholen Sie das Kommando nach einiger Wartezeit (falls nötig).

9.5.3 Meldungen zur Fernadministration

Für die nachfolgend aufgeführten Meldungen muss der Exitcode bei *fthelp* um 2000 erhöht werden, z.B. 2052 statt 52.

52 Administrationsauftrag vom Fernadministrations-Server zurückgewiesen

Bedeutung:
Der Administrationsauftrag wurde vom Fernadministrations-Server zurückgewiesen, weil er im Widerspruch zu den Einstellungen in der Konfigurationsdatei des Fernadministrations-Servers steht.

Der genaue Ablehnungsgrund kann durch den ADM-Verwalter im zugehörigen ADM-Logging-Satz auf dem Fernadministrations-Server festgestellt werden.

Mögliche Reason-Codes:

7001 Die AdministratorID ist ungültig. In den Konfigurationsdaten des Fernadministrations-Servers konnte aus der UserID oder dem Profilnamen keine gültige AdministratorID abgeleitet werden.

7002 Die Routing-Info ist ungültig. In den Konfigurationsdaten des Fernadministrations-Servers wurde die in der Routing-Info angegebene openFT-Instanz nicht gefunden.

7003 Das angegebene Fernadministrations-Kommando ist ungültig. Der Fernadministrations-Server weist das angegebene Kommando zurück, da es sich nicht um ein unterstütztes Fernadministrations-Kommando handelt.

7101 Verstoß gegen die Zugriffsrechteliste. Bei der Prüfung der Zugriffsrechte wurde festgestellt, dass der AdministratorID in den Konfigurationsdaten des Fernadministrations-Servers nicht die benötigten Rechte zugeordnet sind, um das gültige Fernadministrations-Kommando auf der angegebenen openFT-Instanz auszuführen.

7201 Verstoß gegen die maximale Kommandolänge. Der Fernadministrations-Server führt insbesondere bei BS2000-Kommandos eine Ersetzung des vom Benutzer angegebenen und von openFT garantierten kürzesten Kommandonamens durch den vollen Kommandonamen durch. Wird durch die Ersetzung des Kommandonamens das gesamte Fernadministrations-Kommando länger als die maximale Kommandolänge von 8192 Zeichen, dann wird das Kommando abgelehnt.

Maßnahme:
Die benötigten Anpassungen an den Konfigurationsdaten durch den ADM-Verwalter durchführen lassen bzw. Kommando überprüfen. Geändertes Kommando eventuell wiederholen.

54 Kommando ungültig

Bedeutung:
Beim angegebenen Kommando handelt es sich nicht um ein zulässiges Kommando, das per Fernadministration auf dem angegebenen System ausgeführt werden darf.

Maßnahme:
Zulässiges Kommando angeben bzw. fehlende Routing-Information ergänzen. Kommando wiederholen.

57 openFT hat keine Berechtigung Administrations-Aufträge zu bearbeiten

Bedeutung:
openFT ist nicht (mehr) berechtigt Administrationsaufträge zu bearbeiten. Dies ist zum Beispiel dann der Fall, wenn ein Fernadministrations-Server zu einem normalen Server zurückgestuft wurde
(*ftmodo -admcs=n*) bzw. wenn Kommandos, die nur auf einem Fernadministrations-Server ausgeführt werden dürfen, von einer openFT-Instanz bearbeitet werden, die nicht als Fernadministrations-Server konfiguriert wurde.

Fachwörter

Mit *Kursivschrift* wird auf weitere Fachwörter verwiesen.

absoluter Pfadname
: Gesamtweg von der Wurzel des Dateisystems bis zur Datei.

access control
: Dateiattribut im *virtuellen Dateispeicher*, gehört zur *security group*, legt *Zugriffsrechte* fest.

action list
: Element des Dateiattributs *access control* (gehört zur *security group*) im *virtuellen Dateispeicher*, legt *Zugriffsrechte* fest.

ADM-Partner
: Partnersystem einer openFT-Instanz, mit dem über das *FTADM-Protokoll* kommuniziert wird, um *Fernadministration* durchzuführen.

ADM-Traps
: Kurze Meldungen, die bei bestimmten Ereignissen, die während des openFT-Betriebs auftreten, an den *ADM-Trap-Server* gesendet werden.

ADM-Trap-Server
: Server, der die *ADM-Traps* empfängt und dauerhaft speichert. Er muss als *Fernadministrations-Server* konfiguriert sein.

ADM-Verwalter
: Verwalter des *Fernadministrations-Servers*. Er darf als einzige Person die Konfigurationsdaten des Fernadministrations-Servers ändern.

Administrierte openFT-Instanzen
: openFT-Instanzen, die durch *Fernadministratoren* im laufenden Betrieb administriert werden können.

AES (Advanced Encryption Standard)
Aktueller symmetrischer Verschlüsselungsstandard, festgelegt vom NIST (National Institute of Standards and Technology), basierend auf dem an der Universität Leuven (B) entwickelten Rijndael-Algorithmus. Das AES-Verfahren wird von der openFT-Produktfamilie zur Verschlüsselung der Auftragsbeschreibungsdaten und ggf. der Dateiinhalte verwendet.

ANSI-Code
Normierter 8-Bit-Zeichensatz für den Nachrichtenaustausch. Das Akronym steht für „American National Standards Institute“.

API (Application Programming Interface)
Ein Interface, das Anwendungsprogrammierern zur freien Verfügung steht. Es bietet eine auf eine bestimmte Funktionalität ausgelegte Menge von Schnittstellenmechanismen an.

Application Entity Title (AET)
Der Application Entity Title ist eine Schicht 7-Adress-Information des *ISO-Referenzmodells*. Er ist nur für *FTAM-Partner* von Bedeutung.

asynchroner Auftrag
Der *FT-Auftrag* wird nach der Auftragsabgabe entkoppelt vom Benutzer durchgeführt. Der Benutzer kann weiterarbeiten, nachdem das System die Annahme des Auftrags bestätigt hat. (vgl. *synchroner Auftrag*)

Auftrag
Siehe *FT-Auftrag*

Auftragsbuch
Datei, die *asynchrone Aufträge* und ihre Bearbeitungszustände enthält.

Auftrags-Identifikation
Vom lokalen System vergebene Nummer zur Identifikation eines *FT-Auftrags*.

Auftragsspeicherung
FT-Funktion, die *FT-Aufträge* bis zu ihrer Erledigung bzw. Beendigung speichert.

Auftragsverwaltung
FT-Funktion, die *FT-Aufträge* verwaltet und dafür sorgt, dass sie von der Abgabe des Auftrags bis zur Erledigung bzw. Beendigung bearbeitet werden.

Authentifizierung
Verfahren, mit dem openFT die eindeutige Identität des Auftragspartners überprüft.

Benannter Partner
Partnersystem, das mit Namen in der *Partnerliste* eingetragen ist.

Berechtigungsprofil
Mittel zur Festlegung der Schutzfunktionen von *FTAC*. Berechtigungsprofile definieren eine *Zugangsberechtigung*, die in *FT-Aufträgen* statt der *LOGIN-* oder *LOGON-Berechtigung* angegeben werden muss. Im Berechtigungsprofil werden die *Zugriffsrechte* auf eine Benutzerkennung festgelegt, indem die Verwendung von Parametern in *FT-Aufträgen* eingeschränkt wird.

Berechtigungsprofil, privilegiertes
Siehe *privilegiertes Berechtigungsprofil*

Berechtigungssatz
Im Berechtigungssatz wird bei Einsatz von *FTAC* für eine Benutzerkennung festgelegt mit welchen *Partnersystemen* diese Kennung welche FT-Funktionen nutzen darf.

Berechtigungssatz, privilegierter
Siehe *privilegierter Berechtigungssatz*

Betriebsmittel
Hardware- und Software-Objekte, die das *FT-System* zur Ausführung eines *FT-Auftrags* benötigt (Prozesse, Verbindungen, Leitungen). Diese Betriebsmittel werden durch die *Betriebsparameter* gesteuert.

Betriebsparameter
Parameter, die *Betriebsmittel* steuern (z.B. mögliche Anzahl von Verbindungen).

Bibliothek
Datei mit interner Struktur (Elemente)

Bibliothekselement
Teil einer Bibliothek. Ein Bibliothekselement kann seinerseits wieder in Sätze strukturiert sein.

character repertoire
Zeichenvorrat einer Datei im *virtuellen Dateispeicher*.
Für Dateien die mit *FTAM-Partnern* übertragen werden, kann man wählen zwischen: *GeneralString*, *GraphicString*, *IA5String* und *VisibleString*.

Character Separated Values (CSV)
Dieses Ausgabeformat ist ein speziell im PC Umfeld weit verbreitetes, tabellenartiges Format, bei dem die einzelnen Felder durch ein Separatorenzeichen getrennt sind (häufig Semikolon ";"). Es erlaubt die Weiterverarbeitung der Ausgaben für die wichtigsten openFT-Kommandos mit eigenen Tools.

Client
- Begriff aus der Client/Server-Architektur: derjenige Partner, der die Dienste eines *Servers* in Anspruch nimmt.
- Logische Instanz, welche einem *Server* Aufträge erteilt.

Cluster
Eine Anzahl von Rechnern, die über ein schnelles Netzwerk verbunden sind und die von außen in vielen Fällen als ein Rechner gesehen werden können. Ziel des „Clustering" besteht meistens in der Erhöhung der Rechenkapazität oder der Verfügbarkeit gegenüber einem einzelnen Rechner.

Comma Separated Values
siehe *Character Separated Values.*

Communication Controller
Datenkommunikationsrechner

concurrency control
Element des FTAM-Dateiattributs *access control* (gehört zur *security group*) im *virtuellen Dateispeicher.* Steuert konkurrierende Zugriffe.

constraint set
Element des *document type*.

contents type
Dateiattribut im *virtuellen Dateispeicher,* gehört zur *kernel group*, beschreibt die Dateistruktur und die Form des Dateiinhalts.

Data Encryption Standard (DES)
Internationale Norm zur Verschlüsselung von Daten zur Erhöhung der Sicherheit. Das DES-Verfahren wird von den openFT-Produkten zur Verschlüsselung der Auftragsbeschreibungsdaten und ggf. der Auftragsdaten verwendet, falls mit älteren openFT-Versionen gekoppelt wird, die noch kein *AES* unterstützen.

Dateiattribute
Eigenschaften einer Datei, beispielsweise Größe der Datei, Zugriffsrechte auf die Datei oder Satzstruktur der Datei.

Dateimanagement

Möglichkeit im fernen System Dateien zu „managen“. Es gibt folgende Möglichkeiten:

- Dateiverzeichnisse anlegen
- Dateiverzeichnisse anzeigen und ändern
- Dateiverzeichnisse löschen
- Dateiattribute anzeigen und ändern
- Dateien umbenennen
- Dateien löschen

Dateispeicher, virtueller

Siehe *virtueller Dateispeicher*

Dateiübertragungsauftrag

Siehe *FT-Auftrag*

Dateiverzeichnis

Dateiverzeichnisse sind Ordner im hierarchischen Dateisystem eines Unix-Systems (einschließlich POSIX) oder eines Windows-Systems, welche Dateien und/oder andere Dateiverzeichnisse enthalten.

Datencodierung

Art und Weise, in der ein *FT-System* die Zeichen intern darstellt.

Datenkommunikationssystem

Summe der Hardware- und Software-Einrichtungen, die es zwei oder mehreren Kommunikationspartnern ermöglicht, unter Beachtung bestimmter Regeln Daten auszutauschen.

Datenkomprimierung

Reduktion von Daten durch eine verdichtete Darstellung.

Datenschutz

- Im engeren Sinne gemäß Bundesdatenschutzgesetz die Aufgabe, durch den Schutz der personenbezogenen Daten vor Missbrauch bei der Datenverarbeitung der Beeinträchtigung schutzwürdiger Belange der Betroffenen entgegenzuwirken.
- Im weiteren Sinne die Aufgabe, durch den Schutz der Daten vor Missbrauch in ihren Verarbeitungsphasen der Beeinträchtigung fremder und eigener schutzwürdiger Belange zu begegnen.

Datensicherheit

Technisch-organisatorische Aufgabe, die Sicherheit von Datenbeständen und Datenverarbeitungsabläufen zu gewährleisten; d.h. insbesondere zu erreichen, dass

- der Zugriff zu Daten nur Berechtigten möglich ist,
- keine unerwünschte bzw. unberechtigte Verarbeitung von Daten erfolgt,
- die Daten bei der Verarbeitung nicht verfälscht werden,
- die Daten reproduzierbar sind.

DHCP

Dienst in TCP/IP-Netzen, der Clients auf Anforderung automatisch IP-Adressen und TCP/IP-Parameter zuteilt.

Dienst

- Begriff der OSI-Architektur: Ein Dienst (Service) ist die Menge von Funktionen, die ein Diensterbringer (Service Provider) an einem Dienstzugangspunkt (Service Access Point) zur Verfügung stellt.
- Begriff der Client-Server-Architektur: Eine Menge von Funktionen, die ein Server den Clients zur Verfügung stellt.
- Begriff in Unix- und Windows-Systemen: Ein Programm, eine Routine oder ein Prozess zur Durchführung einer bestimmten Systemfunktion, die der Unterstützung anderer Programme dient, insbesondere auf einer niedrigen (hardwarenahen) Ebene.

document type

Wert des Dateiattributs *contents type* (gehört zur *kernel group*). Beschreibt die Form des Dateiinhalts im *virtuellen Dateispeicher*.

- *document type* für Textdateien: **FTAM-1**
- *document type* für Binärdateien: **FTAM-3**

Dynamischer Partner

Partnersystem, das entweder gar nicht (*freier dynamischer Partner*) oder nur mit Adresse und ohne Namen (*eingetragener dynamischer Partner*) in der Partnerliste eingetragen ist.

EBCDIC

Normierter Standardcode für den Nachrichtenaustausch, wie er z.B. im BS2000/OSD vorkommt. Das Akronym steht für „Extended Binary Coded Decimal Interchange Code“.

Eigentümer eines FT-Auftrags

Benutzerkennung im *lokalen System* bzw. *fernen System*, mit der dieser *FT-Auftrag* durchgeführt wird. Eigentümer ist immer die Kennung, unter der der Auftrag abgesetzt wurde, nicht diejenige unter der der Auftrag durchgeführt wird.

Eingetragener dynamischer Partner
: Partnersystem, das nur mit Adresse und ohne Namen in der Partnerliste eingetragen ist.

Empfangsdatei
: Datei im *Empfangssystem*, in der die Daten einer *Sendedatei* abgespeichert werden.

Empfangssystem
: System, an das eine Datei gesendet wird. Dies kann das *lokale* oder *ferne System* sein.

Emulation
: Komponente, die die Eigenschaften eines anderen Geräts nachbildet.

Entity
: Siehe *Instanz*

Explorer
: Programm von Microsoft, das zusammen mit Windows-Betriebssystemen ausgeliefert wird und eine einfache Art der Navigation im Dateisystem ermöglicht.

Fernadministration
: Administration von openFT-Instanzen von fernen Rechnern aus.

Fernadministrations-Server
: Zentrale Komponente, die für die *Fernadministration* und für *ADM-Traps* benötigt wird. Ein Fernadministrations-Server läuft auf einem Unix- oder Windows-System mit openFT ab V11.0. Wenn er für die *Fernadministration* eingesetzt wird, dann enthält er sämtliche dafür notwendigen Konfigurationsdaten.

Fernadministrator
: Rolle, die im *Fernadministrations-Server* konfiguriert wird und dazu berechtigt, bestimmte Administrationsfunktionen auf bestimmten openFT-Instanzen auszuführen.

Fernes System
: Siehe *Partnersystem*

File Transfer
: Dateiübertragung

Firewall-Rechner
Rechner, der zwei Netze miteinander verbindet. Die möglichen Zugriffe können genau geregelt und auch protokolliert werden.

Folgeverarbeitung
FT-Funktion, die nach Abschluss des *FT-Auftrages* die vom Benutzer spezifizierten Kommandos oder Anweisungen im *lokalen* und/oder *fernen System* zur Ausführung bringt. Für positiven und negativen Abschluss können unterschiedliche Folgeverarbeitungen definiert werden, siehe auch *Vor- und Nachverarbeitung*.

Folgeverarbeitungsauftrag
Anweisungen innerhalb eines *FT-Auftrages*, die nach der Dateiübertragung *Folgeverarbeitung(en)* durchführen.

Freier dynamischer Partner
Partnersystem, das nicht in der Partnerliste eingetragen ist.

FTAC (File Transfer Access Control)
Erweiterter Zugangsschutz bei Dateiübertragung und Dateimanagement. Für BS2000 und z/OS realisiert im Produkt openFT-AC, für andere Betriebssysteme Bestandteil des openFT-Produkts, z.B. bei openFT für Unix-Systeme und openFT für Windows-Systeme.

FTAC-Verwalter
Verwalter der FTAC-Funktionen, sollte mit demjenigen identisch sein, der für den Datenschutz verantwortlich ist.

FTAC-Logging-Funktion
Funktion, mit der FTAC jeden Zugriff über File Transfer auf das geschützte System protokolliert.

FTADM-Protokoll
Protokoll, das bei der Kommunikation zwischen zwei openFT-Instanzen verwendet wird, um *Fernadministration* zu betreiben oder *ADM-Traps* zu übertragen.

FTAM-1
document type für Textdateien

FTAM-3
document type für Binärdateien

FTAM-Dateiattribute

Jedes System, das den File Transfer über FTAM-Protokolle ermöglicht, muss seine Dateien dem Partner in einer normgemäßen Beschreibung (ISO 8571) zur Verfügung stellen. Zu diesem Zweck werden die Attribute einer Datei vom realen Dateispeicher auf einen *virtuellen Dateispeicher* abgebildet und umgekehrt. Dazu werden im Wesentlichen drei Gruppen von Dateiattributen unterschieden:

– kernel group: beschreibt die wesentlichen Attribute der Dateien.
– storage group: umfasst die Speicherattribute von Dateien.
– security group: definiert Sicherheitsattribute bzgl. Zugang und Zugriff.

FTAM-Katalog

Der FTAM-Katalog dient zur Erweiterung der verfügbaren Dateiattribute. Die Erweiterung ist nur bei Zugriffen über FTAM von Bedeutung. Zum Beispiel kann eine Datei auf einem Unix-System mit dem Kommando *rm* gelöscht werden, auch wenn der Parameter *permitted actions* das nicht erlaubt.

FTAM-Partner

Partnersystem, mit dem über *FTAM-Protokolle* kommuniziert wird.

FTAM-Protokoll (File Transfer, Access and Management)

Von der ISO (International Organization for Standardization) genormtes *Protokoll* für die Dateiübertragung (ISO 8571, FTAM).

FTP-Partner

Partnersystem, mit dem über das *FTP-Protokoll* kommuniziert wird.

FTP-Protokoll

Herstellerunabhängiges Protokoll zur Dateiübertragung in TCP/IP-Netzen.

FT-Auftrag

Auftrag an ein *FT-System*, eine Datei von einem *Sendesystem* zu einem *Empfangssystem* zu übertragen und gegebenenfalls *Folgeverarbeitungsaufträge* zu starten.

FT-System

System zur Dateiübertragung, bestehend aus einem Rechner und der zur Dateiübertragung nötigen Software.

FT-Trace

Diagnosefunktion, die den Ablauf des FT-Betriebs protokolliert.

FT-Verwalter

Person, die das openFT-Produkt auf einem Rechner verwaltet. openFT kann von allen Benutzerkennungen mit UID=0 verwaltet werden.

Funktionsnorm

Empfehlung, wann und wie bestimmte ISO-/OSI-Normen eingesetzt werden sollen (äquivalenter Begriff: *Profil*). Für die Übertragung unstrukturierter Dateien ist die europäische Vornorm CEN/CENELEC ENV 41 204 erstellt worden, für das Dateimanagement die europäische Vornorm CEN/CENELEC ENV 41205.

Gateway

Im allgemeinen Sprachgebrauch ein System, das zwei oder mehr Netze miteinander verknüpft und nicht als Bridge arbeitet. Varianten: Gateway auf Netzebene (= Router oder OSI-Relais), Transport- und Anwendungsgateway.

Gateway-Rechner

Kommunikationsrechner, die ein Rechnernetz mit einem anderen Rechnernetz verbinden. In Gateway-Rechnern werden die unterschiedlichen Protokolle der unterschiedlichen Rechnernetze aufeinander abgebildet.

GeneralString

Zeichenvorrat für Dateien, die mit *FTAM-Partnern* übertragen werden

GraphicString

Zeichenvorrat für Dateien, die mit *FTAM-Partnern* übertragen werden

Globale Auftrags-Identifikation

Auftragsnummer, die der *Initiator* bei einem openFT- oder FTAM-Auftrag an den *Responder* übermittelt. D.h. die globale Auftrags-Identifikation im Responder ist identisch zur *Auftrags-Identifikation* im Initiator. Der Responder erzeugt für den Auftrag eine eigene (lokale) Auftrags-Identifikation. Damit lassen sich vor allem für den Wiederanlauf-Fall die im Initiator und im Responder gespeicherten Informationen eindeutig einem Auftrag zuordnen.

Grundfunktionen

Die wichtigsten File-Transfer-Funktionen. Im *Berechtigungssatz* wird die Menge der Grundfunktionen festgelegt, die von einer Benutzerkennung genutzt werden können. Die sechs Grundfunktionen sind:

- Inbound Empfangen
- Inbound Senden
- Inbound Folgeverarbeitung
- Inbound Dateimanagement
- Outbound Empfangen
- Outbound Senden

heterogenes Netz
Ein Netz, das aus mehreren Teilnetzen aufgebaut ist, die nach unterschiedlichen technischen Prinzipien arbeiten.

Hintergrundprozess
Ein Prozess, der unabhängig vom Benutzerprozess abläuft. Man erzeugt einen Hintergrundprozess, indem man das Kommando mit dem Sonderzeichen & abschließt. Anschließend ist der Prozess, der den Hintergrundprozess abschickt, sofort für neue Aufgaben frei und braucht sich um den Hintergrundprozess nicht mehr zu kümmern, der nun simultan zu ihm selbst abläuft.

homogenes Netz
Ein technisch nach einem einzigen Prinzip aufgebautes Netz.

HOSTS-Datei
Netzverwaltungsdatei, die alle erreichbaren Rechner mit Internet-Adresse, Rechnername und Alias-Name enthält.

IA5String
Zeichenvorrat für Dateien, die mit *FTAM-Partnern* übertragen werden.

Identifizierung
Verfahren zur Erkennung einer Person oder eines Objekts.

inbound-Auftrag
Auftrag, der in einem anderen System gestellt wurde.

inbound Dateimanagement
In einem *fernen System* gestellter *Auftrag*, bei dem Dateiverzeichnisse oder Dateiattribute des *lokalen Systems* angesehen, Dateiattribute geändert sowie lokale Dateien gelöscht werden können.

inbound empfangen
In *fernem System* gestellter *Auftrag*, bei dem im *lokalen System* eine Datei empfangen wird.

inbound Folgeverarbeitung
In einem *fernen System* gestellter *Auftrag* mit *Folgeverarbeitung* im *lokalen System*.

inbound senden
In *fernem System* gestellter *Auftrag*, bei dem eine Datei aus dem *lokalen System* in das ferne System gesendet wird.

Initiator
Hier: *FT-System*, in dem ein *FT-Auftrag* gestellt wurde.

Instanz / Entity
Begriff der OSI-Architektur: aktives Element in einer Schicht. Siehe auch *openFT-Instanz*

Instanzidentifikation
Netzweit eindeutige Adresse einer *openFT-Instanz*.

Integrität
Unverfälschtheit und Korrektheit von verarbeiteten, übertragenen und gespeicherten Daten.

interoperability
Fähigkeit zweier *FT-Systeme*, zusammenarbeiten zu können.

ISO-/OSI-Referenzmodell
Das ISO-/OSI-Referenzmodell stellt einen Rahmen für die Normung der Kommunikation offener Systeme dar (ISO=International Organization for Standardization).

Job
Folge von Kommandos, Anweisungen und Daten.

Jobübertragung
Übertragung einer Datei, die im *Empfangssystem* einen *Job* darstellt und dort als solcher angestoßen wird.

Kennwort / Passwort
Folge von Zeichen, die der Benutzer eingeben muss, um den Zugriff zu einer Benutzerkennung, einer Datei, einer Jobvariablen, einem Netzknoten oder einer Anwendung zu erhalten. Das Kennwort einer Benutzerkennung dient zur *Authentifizierung* des Benutzers. Es dient dem Zugangsschutz. Das Datei-Kennwort dient zur Überprüfung der Zugriffsberechtigung beim Zugriff auf eine Datei (Jobvariable). Es dient dem Zugriffsschutz.

Kernel group
Gruppe von Dateiattributen im *virtuellen Dateispeicher*, umfasst die Kernattribute einer Datei.

Komprimierung
Bedeutet, dass mehrere aufeinanderfolgende identische Zeichen auf ein Zeichen verkürzt werden und die Zeichenanzahl hinzugefügt wird. Damit verkürzen sich Übertragungszeiten.

Konnektivität
Allgemein die Möglichkeit der Kommunikation zwischen Systemen und Partnern, gelegentlich auch nur auf die Kommunikationsmöglichkeiten von Transportsystemen bezogen.

Local Area Network (LAN)
Ursprünglich ein mit hoher Geschwindigkeit arbeitendes Netz geringer Reichweite. Heute jedes Netz auch großer Reichweite, das gemäß CSMA/CD, Token Ring oder FDDI arbeitet **(**vgl. *WAN Wide Area Network*).

Logging-Funktion
Funktion, mit der *openFT* jeden Zugriff über File Transfer auf das geschützte System protokolliert.

Logging-Satz
Enthält Informationen über eine von openFT durchgeführte Zugangsprüfung (FTAC-Logging-Satz) oder über einen Übertragungs- oder Fernadministrations-Auftrag, der nach positiver Zugangsprüfung gestartet wurde (FT-Logging-Satz bzw. ADM-Logging-Satz).

Logical Unit (LU)
Schnittstelle zwischen einem Anwendungsprogramm und dem Datenkommunikationsnetz SNA. Der Typ einer LU beschreibt die Charakteristika der Kommunikation.

Login-Berechtigung
Zugangsberechtigung zu einem Rechner, die (in der Regel) aus Benutzerkennung und Kennwort besteht, berechtigt zum Dialogbetrieb, siehe auch *LOGON-Berechtigung*.

LOGON-Berechtigung
Zugangsberechtigung zu einem Rechner, die (in der Regel) aus Benutzerkennung, Abrechnungsnummer und Kennwort besteht, berechtigt zum Dialogbetrieb.

Lokales System
Das *FT-System*, an dem der Benutzer arbeitet.

maximum-string-length
Bezeichnet im *virtuellen FTAM-Dateispeicher* die maximale Länge von *Strings* innerhalb einer Datei.

Nachverarbeitung
openFT bietet die Möglichkeit, im Empfangssystem die empfangenen Daten durch eine Folge von Betriebssystemkommandos bearbeiten zu lassen. Die Nachverarbeitung läuft dabei (im Gegensatz zur *Folgeverarbeitung*) unter der Prozesskontrolle von openFT.

Network Control Program (NCP)
Betriebssystem des Front-End-Prozessors für einen SNA-Host.

Netzbeschreibungsbuch
Datei, die bis openFT V9 verwendet wurde und die Angaben über *ferne Systeme* (*FT-Systeme*) enthält.

Offenes Rechnernetz
Rechnernetz, in dem nach den Regeln von ISO/OSI kommuniziert wird. Durch festgelegte *Protokolle* wird das Zusammenwirken unterschiedlicher Rechner verschiedener Hersteller möglich.

Offline Logging
Die Logging-Datei kann im laufenden Betrieb gewechselt werden. Nach dem Umschalten bleibt die bisherige Logging-Datei als Offline-Logging-Datei bestehen; neue Logging-Sätze werden in eine neue Logging-Datei geschrieben. Die Logging-Sätze einer Offline-Logging-Datei können weiterhin mit openFT-Mitteln angesehen werden.

openFT Explorer
Programm von openFT, das eine grafische Oberfläche zur Verfügung stellt, über die Dateiübertragungs- und Administrations-Funktionen von openFT durchgeführt werden können.

openFT Monitor
Programm, mit dem die Messdaten des openFT-Betriebs in Diagrammform angezeigt werden können. Der openFT Monitor benötigt ein grafikfähiges Terminal.

openFT-FTAM
Zusatzprodukt zu openFT (für BS2000, Unix-Systeme und Windows-Systeme) zur Unterstützung der Dateiübertragung mit FTAM-Protokollen. FTAM steht für File Transfer, Access and Management (ISO 8571).

openFT-Instanz
: Auf einem einzelnen Rechner oder einem Cluster im TCP/IP-Netz können mehrere openFT-Systeme gleichzeitig ablaufen, sogenannte openFT-Instanzen. Jede Instanz hat eine eigene Adresse (Instanzidentifikation) und besteht aus dem geladenen Code der openFT-Produkte (inklusive der Zusatzprodukte sofern vorhanden) und den variablen Dateien wie Logging-Dateien, Auftragsbuch usw.

openFT-Partner
: *Partnersystem*, mit dem über *openFT-Protokolle* kommuniziert wird.

openFT-Protokolle
: Genormte *Protokolle* für die Dateiübertragung (SN77309, SN77312).

openFT-Script
: Schnittstelle von openFT, die eine XML-basierte Skript-Sprache für Dateiübertragungs- und Dateimanagement-Funktionen zur Verfügung stellt. Diese Schnittstelle ermöglicht es, mehrere Dateiübertragungs- oder Dateimanagementaufträge zu einem openFT-Script-Auftrag zusammen zu fassen.

openFT-Script-Kommandos
: Kommandos zur Verwaltung von openFT-Script-Aufträgen.

Outbound-Auftrag
: Auftrag, der im eigenen Rechner gestellt wurde.

outbound empfangen
: Lokal gestellter Auftrag bei dem im *lokalen System* eine Datei empfangen wird.

outbound senden
: Lokal gestellter Auftrag, bei dem aus dem *lokalen System* eine Datei gesendet wird.

Owner
: Siehe *Eigentümer eines FT-Auftrags*

Partner
: siehe *Partnersystem*

Partnerliste
: Datei, die Angaben über *ferne Systeme* (*FT-Systeme*) enthält.

Partnersystem
: Hier: *FT-System*, das zusammen mit dem *lokalen System FT-Aufträge* durchführt.

permitted actions
Dateiattribut im *virtuellen Dateispeicher,* gehört zur *kernel group*, legt grundsätzlich erlaubte Aktionen fest.

Portnummer
Nummer, die eine TCP/IP-Anwendung bzw. den Endpunkt einer TCP/IP-Verbindung innerhalb eines Rechners eindeutig identifiziert.

POSIX (Portable Open System Interface)
Gremium und von ihm geschaffene Normen für auf verschiedene Systemplattformen portable Schnittstellen.

Postkorb
Der Postkorb ist eine Datei, die mit dem Kommando mail gelesen werden kann. Jeder Benutzer hat einen Postkorb, um darin Nachrichten zu empfangen.

Presentation
Instanz zur Realisierung der Darstellungsschicht (Schicht 6) des *ISO/OSI-Referenzmodells* in einem *FT-System*, das z.B. mit *FTAM-Protokollen* arbeitet.

Presentation-Selektor
Subadresse, mit der eine *Presentation-Anwendung* angesprochen wird.

Private key
Geheimer Dechiffrierschlüssel, mit dem der Empfänger eine mit einem *public key* verschlüsselte Nachricht entschlüsseln kann. Wird von verschiedenen Verschlüsselungsverfahren verwendet, u.a. dem *RSA-Verfahren*.

privilegiertes Berechtigungsprofil
Berechtigungsprofil, mit dem ein Benutzer die Vorgaben des *FTAC-Verwalters* im *Berechtigungssatz* überschreiten kann. Dazu bedarf es der Genehmigung des *FTAC-Verwalters*. Nur er kann Berechtigungsprofile privilegieren.

privilegierter Berechtigungssatz
Berechtigungssatz des *FTAC-Verwalters*.

Profil
Bei OSI eine Norm, die für einen bestimmten Zweck festschreibt, welche Protokolle einzusetzen sind und Vorschriften über die Werte der Parameter und Optionen enthält.
Hier: Ein einer Benutzerkennung zugeordneter Kommando-Vorrat, dessen Zulässigkeit über Syntax-Dateien sichergestellt wird.
Siehe auch *Berechtigungsprofil*, *privilegiertes Berechtigungsprofil*.

Prompting in Prozeduren
: Funktion, die den Datenstationsbenutzer auffordert, zum Ablauf der Prozedur benötigte Daten einzugeben.

Protokoll
: Summe der Regeln und Verfahren zwischen zwei oder mehr gleichrangigen Partnern, um einen festgelegten Zweck zu erreichen, meist in Form der Definition der auszutauschenden Nachrichten und der korrekten Abläufe von Nachrichtenfolgen inklusive der Behandlung von Fehlerfällen und sonstigen Ausnahmefällen.

Public key
: Veröffentlichter Chiffrierschlüssel; wird vom Empfänger einer Nachricht festgelegt und veröffentlicht bzw. dem Absender der Nachricht mitgeteilt, damit dieser an den Empfänger gerichtete Nachrichten damit verschlüsseln kann. Wird von verschiedenen Verschlüsselungsverfahren verwendet, u.a. dem Rivest-Shamir-Adleman-Verfahren (*RSA-Verfahren)*; muss zu dem nur dem Empfänger bekannten *private key* passen.

RAS
: Remote Access Service; ein Dienst von Windows, der die Kommunikation mit fernen Rechnern ermöglicht.

relativer Pfadname
: Weg vom gerade aktuellen *Dateiverzeichnis* bis zur Datei.

Responder
: Hier: *FT-System*, welches vom *Initiator* angesprochen wird.

RFC (Request for Comments)
: Verfahren im Internet zur Kommentierung von vorgeschlagenen Normen, Festlegungen oder auch Berichten. Auch Bezeichnung für ein auf diese Weise verabschiedetes Dokument.

RFC1006
: Zusatzprotokoll zur Realisierung der ISO-Transportdienste (Transportklasse 0) auf TCP/IP-Basis.

Rivest-Shamir-Adleman-Verfahren (RSA-Verfahren)
: Nach seinen Erfindern benanntes Verschlüsselungsverfahren, das mit einem aus *public key* und *private key* bestehenden Schlüsselpaar arbeitet. Wird von der openFT-Produktfamilie benutzt, um die Identität des Partnersystems eindeutig zu überprüfen und dem Partnersystem den AES-Schlüssel für die Verschlüsselung der Dateiinhalte zu übermitteln.

Router

Element in einem Netz, das zwischen Netzen residiert und Nachrichtenströme durch die Netze lenkt und dazu Wegewahl, Adressierung und andere Funktionen behandelt. Arbeitet auf Schicht 3 des OSI-Modells.

Satz

Eine Zusammenfassung von Daten, die als eine logische Einheit behandelt werden.

Satz fester Länge

Ein Satz in einer Datei, in der alle Sätze nach Vereinbarung dieselbe Länge haben; innerhalb der Datei ist keine Anzeige der Länge erforderlich.

Satz variabler Länge

Satz in einer Datei, in der die Sätze unterschiedlich lang sein können. Die Satzlänge muss entweder durch ein Satzlängenfeld am Anfang des Satzes angegeben werden, oder implizit durch einen Begrenzer (z.B. Carriage Return - Line Feed) zum nächsten Satz ermittelbar sein.

Schutzattribute

Sicherheitsrelevante Eigenschaften eines Objekts, die Art und potenzielle Möglichkeit des Zugriffs auf dieses Objekt festlegen.

Secure FTP

Verfahren, mit dem eine Verbindung über das *FTP-Protokoll* getunnelt wird, so dass sichere Verbindungen mit Verschlüsselung und *Authentifizierung* möglich sind.

Security group

Gruppe von Dateiattributen des *virtuellen Dateispeichers*, umfasst die Sicherheitsattribute einer Datei.

Sendedatei

Datei im *Sendesystem*, aus der Daten in die *Empfangsdatei* gesendet werden.

Sendesystem

Hier: *FT-System*, das eine Datei sendet. Dies kann das *lokale* oder das *ferne System* sein.

Server

Logische Instanz bzw. Anwendungskomponente, welche Aufträge eines Clients ausführt und die (koordinierte) Nutzung allgemein verfügbarer Dienste (File, Print, Datenbank, Kommunikation, etc.) bereitstellt. Kann selbst bezüglich eines anderen Servers Client sein.

Service Class
Parameter, mit dem *FTAM-Partner* aushandeln, welche Funktionalität sie verwenden.

Session
- In OSI die Bezeichnung für eine Schicht-5-Verbindung.
- In SNA eine allgemeine Bezeichnung für eine Verbindung zwischen Kommunikationspartnern (Applikationen, Geräten oder Benutzern).

Session-Selektor
Subadresse, mit der eine *Session-Anwendung* angesprochen wird.

Shell-Metazeichen
Folgende Metazeichen haben eine besondere Bedeutung für die Shell: *, [ ], ?, <, >, |, &, &&, ( ), { }

Sicherheitsstufe
Bei Einsatz der *FTAC-Funktionen* ist die Sicherheitsstufe ein Maß für das Schutzbedürfnis gegenüber einem *Partnersystem*.

SNA-Netz
Datenkommunikationssystem, das sich entsprechend der Systems Network Architecture (SNA) von IBM verhält.

SNMP (Simple Network Management Protocol)
Von der Internet Engineering Task Force (IETF) für TCP/IP-Netze definiertes Protokoll zur Übertragung von Managementinformationen.

Sonderzeichen
Siehe *Shell-Metazeichen*

Standardausgabe (stdout)
Standardausgabe ist voreingestellt auf den Bildschirm.

Standardberechtigungssatz
Der Standardberechtigungssatz ist die Vorgabe für alle Benutzerkennungen. Der Benutzer darf diese Vorgabe für seinen Berechtigungssatz weiter einschränken.

Standardeingabe (stdin)
Standardeingabe ist voreingestellt auf die Tastatur.

Standardfehlerausgabe (stderr)
Standardfehlerausgabe ist voreingestellt auf den Bildschirm.

Storage group
Dateiattribut im *virtuellen Dateispeicher*, umfasst die Speicherattribute von Dateien.

String
Zeichenkette

string-significance
Beschreibt für die Übertragung mit *FTAM-Protokollen* das Format der *Strings* in den Dateien.

Synchroner Auftrag
Der Benutzerprozess, von dem der *FT-Auftrag* abgegeben wurde, wartet auf das Ende der Übertragung. Der Benutzer kann nicht weiterarbeiten (vgl. *asynchroner Auftrag*).

System
Siehe *FT-System*

System, fernes
Siehe *fernes System*

System, lokales
Siehe *lokales System*

TCP/IP (Transmission Control Protocol / Internet Protocol)
Verbreitetes Protokoll zur Datenübertragung (entspricht etwa den Schichten 3 und 4 des *ISO/OSI-Referenzmodells*, d.h. Netzwerk- und Transportschicht). Wurde ursprünglich für das ARPANET (Rechnernetz des US-Verteidigungsministeriums) entwickelt, inzwischen de-facto-Standard.

Transfer-Identification
Siehe *Auftrags-Identifikation*

TranSON
TranSON ist ein Software Produkt, das einen gesicherten Zugang zu einem Server ermöglicht. Der Einsatz von TranSON ist für die Anwendung transparent. Die Verbindung zum fernen Partner wird vom Arbeitsplatz über einen Client Proxy und Server Proxy zum fernen Partner geleitet. Der Client Proxy befindet sich auf dem Arbeitsplatz, der Server Proxy beim fernen Partner. Die Übertragung zwischen Client Proxy und Server Proxy ist verschlüsselt.

Transport Name Service (TNS)
Dienst zur Verwaltung transportsystemspezifischer Eigenschaften. Einträge für *Partnersysteme* enthalten die Informationen zum jeweils verwendeten *Transportsystem*.

Transportprotokoll
Protokoll der *Transportschicht*

Transportschicht
Schicht 4 des *ISO/OSI-Referenzmodells,* wickelt die Protokolle für den Datentransport ab.

Transport-Selektor (T-Selektor)
Subadresse, mit der eine ISO-8072-Anwendung in der *Transportschicht* angesprochen wird.

Transportsystem
- Teil eines Systems oder einer Architektur, der ungefähr die Funktionen der unteren vier OSI-Schichten erbringt, also den Transport der Nachrichten von einem Partner zum anderen Partner einer Kommunikationsbeziehung.
- Summe von Hardware- und Softwareeinrichtungen, die für den Datentransport in Rechnernetzen sorgt.

Transportverbindung
Logische Verbindung zwischen zwei Benutzern des Transportsystems (Datenstationen oder Anwendungen).

Übertragungseinheit
In einer FTAM-Übertragung die kleinste Dateneinheit zum Transport von Dateiinhalten. Für *FTAM-1* und *FTAM-3* sind dies *Strings*. Eine Übertragungseinheit kann, muss aber nicht einem Satz der Datei entsprechen.

Unicode
Universelle Zeichencodierung, wird vom Unicode-Konsortium überwacht und gepflegt. Dieser Codierungs-Standard liefert die Grundlage, um Textdaten in beliebigen Sprachen mit moderner Software und IT-Protokollen zu verarbeiten, zu speichern und auszutauschen. Der Unicode-Standard definiert die drei Unicode Varianten UTF-8, UTF-16 und UTF-32.

universal-class-number
Zeichenvorrat einer Datei im *virtuellen Dateispeicher*

UNIX®

Eingetragenes Warenzeichen der Open Group für ein weit verbreitetes Mehrbenutzer-Betriebssystem. Ein System darf nur den Namen UNIX führen, wenn es von der Open Group zertifiziert ist.

Unix-System

Allgemein übliche Bezeichnung für ein Betriebssystem, welches UNIX®-typische Funktionen implementiert und entsprechende Schnittstellen anbietet. Auch POSIX und Linux werden zu den Unix-Systemen gerechnet.

Virtueller Dateispeicher

Im virtuellen FTAM-Dateispeicher stellt ein *FT-System* in der Rolle des *Responders* seine Dateien für *Partnersysteme* zur Verfügung. Die Darstellung einer Datei im virtuellen Dateispeicher ist durch die FTAM-Norm vorgegeben, siehe *Dateiattribute*.

VisibleString

character repertoire für Dateien, die mit *FTAM-Partnern* übertragen werden.

Vorverarbeitung

Über die Vorverarbeitung erlaubt openFT das Abschicken eines Empfangsauftrags, bei dem nicht eine ferne Datei, sondern die Ausgaben eines fernen Kommandos bzw. Programms übertragen werden. Mit Hilfe der Vorverarbeitung sind z.B. Datenbankabfragen im fernen System möglich. Die Vorverarbeitung ist auch lokal möglich.

WAN (Wide Area Network)

Öffentliches oder privates Netz, das große Entfernungen überbrücken kann und dabei - im Gegensatz zu *LAN*s - relativ langsam mit höherer Fehlerrate arbeitet. Heutzutage sind diese Definitionen nur noch eingeschränkt gültig, Beispiel: bei ATM-Netzen.

Wiederanlauf

Automatische Fortsetzung eines *FT-Auftrags* nach einer Unterbrechung.

Wiederanlaufpunkt

Stelle, bis zu der die Daten der *Sendedatei* bei einer Unterbrechung der Dateiübertragung in der *Empfangsdatei* gesichert abgespeichert sind und ab der die Daten nach einem *Wiederanlauf* weiter übertragen werden.

X-Terminal

Ein Bildschirm oder eine Softwarekomponente zur Darstellung der grafischen X Window-Oberfläche von Unix-Systemen. Ein X-Terminal oder eine entsprechende Software-Emulation ist Voraussetzung für den Einsatz der grafischen Oberfläche von openFT, dem openFT Explorer.

Zentrale Administration

Die zentrale Administration von openFT umfasst die Funktionen *Fernadministration* und *ADM-Traps* und setzt den Einsatz eines *Fernadministrations-Servers* voraus.

Zugangsberechtigung

Berechtigung für die Dateiübertragung und das Dateimanagement bei Einsatz von FTAC. Die Zugangsberechtigung ersetzt die *LOGIN-Berechtigung* bzw. die *LOGON-Berechtigung*.

Zugangsschutz

Beinhaltet alle Methoden zum Schutz eines Datenverarbeitungssystems vor unberechtigtem Systemzugang.

Zugriffsrecht

Leitet sich von der *Zugangsberechtigung* ab. Das Zugriffsrecht legt fest, worauf ein Benutzer, der die Zugangsberechtigung angegeben hat, Zugriff hat.

Abkürzungen

ACSE	Association Control Service Element
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
ASCII	American Standard Code for Information Interchange
BCAM	Basic Communication Access Method
CAE	Common Application Environment
CCP	Communication Control Programm
CCS	Coded Character Set
CEN	Comité Européen de Normalisation
CENELEC	Comité Européen de Normalisation Électrotechnique
CMX	Communication Manager Unix Systems
CSV	Character Separated Values
DCAM	Data Communication Access Method
DCM	Data Communication Method
DES	Data Encryption Standard
DIN	Deutsches Institut für Normung
DNS	Domain Name Service
EBCDIC	Extended Binary-Coded Decimal Interchange Code
ENV	Europäischer Normen-Vorschlag
FADU	File Access Data Unit
FJAM	File Job Access Method
FMLI	Form and Menu Language Interpreter
FSB	Forwarding Support Information Base
FSS	Forwarding Support Service
FT	File Transfer
FTAC	File Transfer Access Control
FTAM	File Transfer, Access and Management (ISO 8571)
FTP	File Transfer Protocol

FTPS	FTP über SSL / TLS
GPL	Gnu Public License
GSM	Global System for Mobile Communication
ISAM	Index Sequential Access Method
ISO	International Organization for Standardization
LAN	Local Area Network
LMS	Library Maintenance System
MIB	Management Information Base
MSV	Mittelschnelles Synchron Verfahren
NDMS	Network Data Management System
NIS	Network Information Service
OSI	Open Systems Interconnection
OSS	OSI Session Service
PAM	Pluggable Authentication Modules
PEM	Privacy Enhanced Mail
PICS	Protocol Implementation Conformance Statement
PKCS	Public Key Cryptography Standards
PLAM	Primary Library Access Method
RFC1006	Request for Comments 1006
RMS	Reliant Monitor Services
SAM	Sequential Access Method
SDF	System Dialog Facility
SNA	Systems Network Architecture
SNMP	Simple Network Management Protocol
SNPA	Subnetwork Point of Attachment
SSL	Secure Socket Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
TID	Transport Identification
TLS	Transport Layer Security
TNSX	Transport Name Service in Unix systems
TPI	Transport Protocol Identifier
TS	Transport System
WAN	Wide Area Network

Literatur

Die Handbücher sind online unter *http://manuals.ts.fujitsu.com* zu finden.

openFT für Unix-Systeme
Managed File Transfer in der offenen Welt
Benutzerhandbuch

openFT für Windows-Systeme
Installation und Administration
Systemverwalterhandbuch

openFT für Windows-Systeme
Managed File Transfer in der offenen Welt
Benutzerhandbuch

openFT für Unix- und Windows-Systeme
Programmschnittstelle
Programmierhandbuch

openFT für Unix- und Windows-Systeme
openFT-Script-Schnittstelle
Programmierhandbuch

openFT für BS2000/OSD
Managed File Transfer in der offenen Welt
Benutzerhandbuch

openFT für BS2000/OSD
Installation und Administration
Systemverwalterhandbuch

openFT für BS2000/OSD
Programmschnittstellen
Programmierhandbuch

openFT für z/OS
Managed File Transfer in der offenen Welt
Benutzerhandbuch

openFT für z/OS
Installation und Administration
Systemverwalterhandbuch

CMX
Betrieb und Administration
Benutzerhandbuch

CMX
Anwendungen programmieren
Programmierhandbuch

OSS(SINIX)
OSI Session Service
User's Guide

Stichwörter

B

R

T