

Deutsch



Fujitsu Software

openFT (Unix- und Windows-Systeme)

Installation und Betrieb

Systemverwalterhandbuch

Stand der Beschreibung:
openFT V12.1C60

November 2023

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

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

Sie können uns Ihre Kommentare per E-Mail an bs2000services@fujitsu.com senden.

Zertifizierte Dokumentation nach DIN EN ISO 9001:2015

Um eine gleichbleibend hohe Qualität und Anwenderfreundlichkeit zu gewährleisten, wurde diese Dokumentation nach den Vorgaben eines Qualitätsmanagementsystems erstellt, welches die Forderungen der DIN EN ISO 9001:2015 erfüllt.

Copyright und Handelsmarken

Copyright © 2023 Fujitsu Technology Solutions GmbH.

Alle Rechte vorbehalten.

Liefermöglichkeiten und technische Änderungen vorbehalten.

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

Inhaltsverzeichnis

Installation und Betrieb (Unix- und Windows-Systeme)	8
1 Einleitung	9
1.1 Kurzbeschreibung des Produkts	10
1.2 Zielsetzung und Zielgruppen des Handbuchs	11
1.3 Handbuchkonzept von openFT	12
1.4 Änderungen gegenüber der vorigen Version	14
1.4.1 Änderungen für alle Plattformen	15
1.4.2 Änderungen für Unix- und Windows-Plattformen	18
1.4.3 Änderungen für Unix-Plattformen	20
1.4.4 Änderungen für BS2000-Systeme und zOS	21
1.4.5 Änderungen für zOS	22
1.4.6 Neue Funktionen, die nur im openFT Explorer zur Verfügung stehen	23
1.5 Darstellungsmittel	24
1.6 Internet	25
2 Installation auf Unix-Systemen	26
2.1 Installation von openFT	27
2.1.1 Neuinstallation	29
2.1.2 Update-Installation von openFT	31
2.1.3 Installation einer Korrekturversion	33
2.1.4 Installation in ein alternatives root-Verzeichnis (Solaris)	34
2.1.5 Automatische Installation	36
2.1.6 Unterstützung von Openshift	37
2.1.7 Unterstützung von systemd	40
2.1.7.1 Einbenutzerbetrieb	41
2.1.7.2 Aktivierung von ftalarm	42
2.1.7.3 Änderung des umask Wertes	43
2.2 Wichtige Tätigkeiten nach der Installation	44
2.2.1 Standardeinstellungen überprüfen	45
2.2.2 Konfigurationsdaten importieren	47
2.2.3 Automatischen openFT-Start deaktivieren	48
2.2.4 ftalarm-Kommando aktivieren	49
2.2.5 Solaris SMF	50
2.2.6 openFT-FTAM auf HP-UX, AIX und Linux installieren oder deinstallieren	53
2.2.7 openFT-FTP auf HP-UX, AIX und Linux installieren oder deinstallieren	54
2.2.8 Authentifizierung über PAM	55
2.2.9 Partnerliste aus TNS erzeugen	57
3 Installation auf Windows-Systemen	58

3.1 Installation von openFT	59
3.1.1 Neuinstallation	61
3.1.2 Update-Installation von openFT	63
3.1.3 Installation einer Korrekturversion	65
3.1.4 Bedienerlose Installation	66
3.1.5 Installation des SNMP-Subagenten	70
3.1.6 Ändern und Reparieren von openFT	71
3.1.7 Deinstallation von openFT, openFT-CR und CMX	72
3.2 Wichtige Tätigkeiten nach der Installation	73
3.2.1 Standardeinstellungen überprüfen	74
3.2.2 Konfigurationsdaten importieren	76
3.2.3 Automatischen openFT-Start aktivieren und deaktivieren	77
3.2.4 Partnerliste aus TNS erzeugen	78
4 Betrieb	79
4.1 Betriebsparameter optimieren	81
4.2 Code-Tabellen verwalten	82
4.3 Asynchronen openFT-Server starten und beenden	86
4.4 Betriebsarten einstellen (Windows-Systeme)	87
4.4.1 Ablauf als Dienst unter Systemrechten	88
4.4.2 Ablauf als Dienst unter Benutzerrechten	89
4.5 SchutzbitEinstellung für neu angelegte Dateien (Unix-Systeme)	90
4.6 Dateizugriffsrechte für neu angelegte Dateien (Windows-Systeme)	91
4.7 Dateizugriff unter Benutzerrechten (Unix-Systeme)	92
4.8 Einbenutzerbetrieb (Unix-Systeme)	93
4.8.1 Umschalten auf Einbenutzerbetrieb	94
4.8.2 Rückkehr zum Mehrbenutzerbetrieb	96
4.8.3 Hinweise zur ftalarm-Funktion im Einbenutzerbetrieb	97
4.9 Sprachoberfläche wechseln	98
4.9.1 Sprachoberfläche auf Unix-Systemen wechseln	99
4.9.2 Sprachoberfläche auf Windows-Systemen wechseln	100
4.10 Aufträge administrieren	101
4.11 Partner administrieren	102
4.11.1 Partnerliste exportieren	104
4.12 Sicherheit im openFT-Betrieb	105
4.12.1 Authentifizierung	106
4.12.1.1 Eindeutige Instanzidentifikationen	107
4.12.1.2 Lokale RSA-Schlüsselpaare erzeugen und verwalten	108
4.12.1.3 Schlüssel importieren	110
4.12.1.4 Öffentliche Schlüssel exportieren	111
4.12.1.5 Schlüssel von Partnersystemen verwalten	112
4.12.1.6 Schlüssel an Partnersysteme verteilen	113

4.12.2	Erweiterte Absenderüberprüfung	114
4.12.3	Verschlüsselung bei der Dateiübertragung	115
4.13	FT-Betrieb überwachen und steuern	116
4.13.1	Logging von openFT	117
4.13.2	SNMP-Schnittstelle von openFT (Windows)	119
4.13.2.1	Tätigkeiten nach der Installation	120
4.13.2.2	openFT-Subagenten auf Windows starten	121
4.13.2.3	SNMP-Management für openFT (Windows)	122
4.13.3	Messdatenerfassung mit openFT	126
4.13.3.1	Messdatenerfassung konfigurieren	127
4.13.3.2	Messdaten anzeigen	128
4.14	FTAC-Umgebung verwalten	131
4.14.1	Berechtigungssätze verwalten	132
4.14.2	Berechtigungsprofile verwalten	134
4.14.3	FTAC-Umgebung sichern und übertragen	135
4.15	openFT-Instanzen und Cluster-Betrieb	136
4.16	Konfigurationsdaten sichern und wiederherstellen	138
4.17	FTAM-Besonderheiten auf Unix-/Windows-Systemen	139
4.17.1	Abbildung der Dateizugriffsrechte	140
4.17.1.1	Outbound-Aufträge	141
4.17.1.2	Inbound-Aufträge	142
4.17.2	Abbildung von FTAM-Attributen auf das reale Dateisystem	145
4.17.2.1	Inbound-Abbildung von FTAM-Attributen	146
4.17.2.2	Inbound-Abbildung des document type	149
4.17.2.3	Zugangs- und Zugriffsschutz	151
4.17.2.4	Outbound-Abbildung des document type	152
5	Zentrale Administration	155
5.1	Fernadministration	156
5.1.1	Fernadministrations-Server konfigurieren	157
5.1.1.1	ADM-Verwalter festlegen	158
5.1.1.2	openFT-Instanz als Fernadministrations-Server deklarieren	159
5.1.1.3	Berechtigungsprofile für den Zugang zum Fernadministrations-Server einrichten	160
5.1.1.4	Zu administrierende openFT-Instanzen in die Partnerliste eintragen	161
5.1.1.5	Konfigurationsdatei per Konfigurations-Editor erstellen	162
5.1.1.6	Konfigurationsdatei per Text- oder XML-Editor erstellen	165
5.1.1.7	Konfiguration importieren	177
5.1.1.8	Konfiguration exportieren und ändern	178
5.1.2	Zu administrierende openFT-Instanz konfigurieren	179
5.1.2.1	Berechtigungsprofil für openFT-Instanz ab V11.0 konfigurieren	180
5.1.2.2	Berechtigungsprofil für openFT-Instanz < V11.0 konfigurieren	181

5.1.3 Fernadministrations-Aufträge stellen	182
5.1.3.1 Fernadministration über Kommando-Schnittstelle	183
5.1.3.2 Fernadministration über openFT Explorer	185
5.1.4 Logging der Fernadministration	188
5.2 ADM-Traps	189
5.2.1 ADM-Trap-Server konfigurieren	190
5.2.2 ADM-Traps in der openFT-Instanz konfigurieren	191
5.2.3 ADM-Traps ansehen	192
5.3 Beispiel für eine XML-Konfigurationsdatei	194
6 Fehlerbehebung und Diagnose	198
6.1 Was tue ich, wenn	199
6.2 Diagnoseunterlagen erstellen	205
6.3 Trace-Funktion	206
6.3.1 Trace-Dateien	207
6.3.1.1 Trace-Funktion ein-/ausschalten	208
6.3.1.2 Trace-Dateien ansehen	210
6.3.1.3 Trace-Dateien aufbereiten mit fttrace	211
6.4 Weitere Diagnoseinformation	213
6.4.1 Diagnosesätze ausgeben	214
6.4.2 Meldungsdatei für Konsolkommandos	215
6.4.3 Diagnoseinformationen mit diaginfo ausgeben (Windows-Systeme)	216
6.5 Code-Tabellen	217
6.5.1 Code-Tabelle EBCDIC.DF.04	218
6.5.2 Code-Tabelle ISO 8859-1	219
7 Anhang	220
7.1 Wichtige CMX-Kommandos (Unix-Systeme)	221
7.1.1 tnsxcom - TS-Directory erzeugen	222
7.1.2 tnsxprop - Eigenschaften von TS-Anwendungen ausgeben	223
7.2 Transportsystem-Anwendungen in TNS eintragen	225
7.2.1 Automatisch erzeugte TNS-Einträge	227
7.2.2 Definition der lokalen TS-Anwendung für openFT-FTAM	229
7.2.3 Definition der fernen TS-Anwendungen für openFT	230
7.2.3.1 Beispieleinträge für openFT-Partner (Unix-Systeme)	231
7.2.3.2 Beispieleinträge für openFT-Partner (Windows-Systeme)	232
7.2.4 Definition der fernen TS-Anwendungen für openFT-FTAM	234
7.2.4.1 Beispieleinträge für FTAM-Partner (Unix-Systeme)	236
7.2.4.2 Beispieleinträge für FTAM-Partner (Windows-Systeme)	237
7.3 openFT im Cluster mit Unix-Systemen	239
7.3.1 Beispiel 1: eine ausfallsichere Instanz	240
7.3.2 Beispiel 2: Ausfallsicherheit für beide Rechner des Clusters	244
7.3.3 Hinweise zur Verwendung des TNS	247

7.4 openFT-Instanzenkonzept im Windows-Cluster	248
7.4.1 Beispiel	249
7.4.1.1 Installation von openFT	250
7.4.1.2 Konfiguration der ressourcen-spezifischen openFT-Eigenschaften des Clusters	251
7.4.1.3 Konfiguration von openFT	252
7.4.1.4 Arbeiten mit den einzelnen openFT-Instanzen	254
7.4.1.5 Arbeiten mit Windows-Cluster als openFT Server	255
7.4.2 Konfiguration der ressourcen-spezifischen openFT-Eigenschaften	256
7.5 FarSync X.25 Transportsystem unter Linux- und Windows- Systemen	264
7.5.1 Direkte Unterstützung von FarSync X.25 für Windows-Systeme	265
7.5.2 FarSync X.25 Unterstützung für Linux-Systeme	266
7.5.3 FarSync X.25 Transportsystem in openFT konfigurieren	267
7.6 Beispieldateien	268

Installation und Betrieb (Unix- und Windows-Systeme)

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 Rechnernetz. 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 bietet eine umfangreiche File-Transfer-Produktlinie, die openFT-Produktfamilie, für folgende Systemplattformen:

- BS2000®
- Linux® (Intel x86_64)
- Microsoft® Windows™ 10, Windows Server 2016 und 2019
- z/OS (IBM®)

1.1 Kurzbeschreibung des Produkts

Die openFT-Produktfamilie besteht aus folgenden Produkten:

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

FUJITSU Software openFT (Windows) ist das File-Transfer-Produkt für Rechner mit den Betriebssystemen Windows von Microsoft.

FUJITSU Software openFT (BS2000) ist das File-Transfer-Produkt für Rechner mit dem Betriebssystem BS2000.

FUJITSU Software openFT (z/OS) ist das File-Transfer-Produkt für Rechner mit dem Betriebssystem z/OS.

Dieses Handbuch gilt für die File-Transfer-Produkte openFT(Unix-Systeme) und openFT (Windows).

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

openFT erlaubt den Einsatz von folgenden Transportprotokollen:

- TCP/IP
- ISO TP0/2 (nicht auf z/OS)
- ISO TP4 (nicht auf z/OS)
- SNA (nur auf z/OS)

Der Funktionsumfang von openFT kann erweitert werden durch:

- FTAC:
FTAC bietet einen erweiterten Zugangs- und Zugriffsschutz. FTAC steht für **File Transfer Access Control**. FTAC wird auf BS2000-Systemen und auf z/OS durch das Zusatzprodukt openFT-AC realisiert. FTAC ist in Unix- und Windows-Systemen in openFT integriert.
- openFT-FTAM (nicht auf z/OS verfügbar):
openFT-FTAM unterstützt das in der ISO-Norm 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.
- openFT-FTP:
openFT-FTP unterstützt die FTP-Funktionalität. Damit ist eine Kopplung zu beliebigen FTP-Servern möglich.
- openFT-CR:
openFT-CR wird bis zur Version V12.1B benötigt, falls verschlüsselte Dateiübertragung gewünscht wird.

! Achtung

Ab openFT Version V12.1C wird openFT-CR nicht mehr ausgeliefert, da die Funktionalität in openFT integriert wurde.

Alle Bezugnahmen auf openFT-CR gelten daher nur für openFT-Versionen <= V12.1B.

1.2 Zielsetzung und Zielgruppen des Handbuchs

Dieses Handbuch wendet sich an den FT-Verwalter und den FTAC-Verwalter, der openFT auf einem Unix- oder Windows-System installieren und in Betrieb nehmen möchte.

Außerdem richtet sich das Handbuch an den Fernadministrator, der das openFT-System als Fernadministrations-Server einrichten und betreiben möchte.

Das Handbuch ist gültig für Linux-Systeme und Oracle Solaris-Systeme sowie für die Portierungen auf andere Unix-Plattformen wie z.B. AIX oder HP-UX.

i Ab openFT Version V12.1B10 erfolgt die Freigabe nur noch für Linux x86_64. Ab openFT Version V12.1C20 ist Solaris (Sparc) zusätzlich wieder in der Freigabe enthalten. Weitere Plattformen erhalten Sie auf Anfrage bei Ihrem vertrieblichen Fujitsu Ansprechpartner.

Die betriebssystemabhängigen Unterschiede werden ausführlich in der Freigabemitteilung beschrieben, die im Internet und auf der jeweiligen Produkt-CD mit ausgeliefert wird.

1.3 Handbuchkonzept von openFT

openFT - Konzepte und Funktionen

Dieses Handbuch richtet sich an alle, die den Leistungsumfang von openFT kennen lernen und die Funktionsweise verstehen möchten. Es beschreibt:

- das Konzept von openFT als Managed File Transfer
- den Leistungsumfang und die grundsätzlichen Funktionen der openFT-Produktfamilie
- die openFT-spezifischen Fachwörter

openFT (Unix- und Windows-Systeme) - Installation und Betrieb

Dieses Handbuch richtet sich an FT-, FTAC- und ADM-Verwalter auf Unix- und Windows-Systemen. Es beschreibt:

- die Installation von openFT und seinen optionalen Komponenten
- Betrieb, Steuerung und Überwachung des FT-Systems und der FTAC-Umgebung
- die Konfiguration und den Betrieb eines Fernadministrations-Servers und eines ADM-Trap-Servers

openFT (BS2000) - Installation und Betrieb

Dieses Handbuch richtet sich an FT- und FTAC-Verwalter auf BS2000-Systemen. Es beschreibt:

- die Installation von openFT und seinen optionalen Komponenten auf dem BS2000-System.
- Betrieb, Steuerung und Überwachung des FT-Systems und der FTAC-Umgebung
- die Abrechnungssätze

openFT (z/OS) - Installation und Betrieb

Dieses Handbuch richtet sich an FT- und FTAC-Verwalter auf dem z/OS. Es beschreibt:

- die Installation von openFT und seinen optionalen Komponenten, einschließlich der notwendigen Voraussetzungen für den Einsatz des Produkts.
- Betrieb, Steuerung und Überwachung des FT-Systems und der FTAC-Umgebung
- die Meldungen von openFT und openFT-AC für den FT-Verwalter
- weitere Informationsmöglichkeiten für den FT-Verwalter, z.B. die Abrechnungssätze und die Logging-Information

openFT (Unix- und Windows-Systeme) - Kommandoschnittstelle

Dieses Handbuch richtet sich an den openFT-Benutzer auf Unix- und Windows-Systemen und beschreibt:

- die Konventionen für den File Transfer zu Rechnern mit verschiedenen Betriebssystemen
- die openFT-Kommandos auf Unix- und Windows-Systemen
- Meldungen der verschiedenen Komponenten

Die Beschreibung der openFT-Kommandos gilt auch für die POSIX-Schnittstelle auf BS2000-Systemen.

openFT (BS2000) - Kommandoschnittstelle

Dieses Handbuch richtet sich an den openFT-Benutzer auf BS2000-Systemen und beschreibt:

- die Konventionen für den File Transfer zu Rechnern mit verschiedenen Betriebssystemen

-
- die openFT-Kommandos auf BS2000-Systemen
 - Meldungen der verschiedenen Komponenten

openFT (z/OS) - Kommandoschnittstelle

Dieses Handbuch richtet sich an openFT-Benutzer auf z/OS-Systemen und beschreibt:

- die Konventionen für den File Transfer zu Rechnern mit verschiedenen Betriebssystemen
- die openFT-Kommandos auf z/OS
- die Menüschnittstelle für den FT-Verwalter und den FT-Benutzer
- die Programmschnittstelle für den FT-Benutzer
- Meldungen der verschiedenen Komponenten

openFT (BS2000) - Programmschnittstelle

Dieses Handbuch richtet sich an den openFT-Programmierer und beschreibt die openFT- und openFT-AC-Programmschnittstellen auf BS2000-Systemen.

openFT (Unix- und Windows-Systeme) - C- und Java-Programmschnittstelle

Dieses Handbuch richtet sich an C- und Java-Programmierer auf Unix- und Windows-Systemen. Es beschreibt die C-Programmschnittstelle sowie die Grundzüge der Java-Schnittstelle.

openFT (Unix- und Windows-Systeme) - openFT-Script-Schnittstelle

Dieses Handbuch richtet sich an XML-Programmierer und beschreibt die XML-Anweisungen der openFT-Script-Schnittstelle.

i Viele der in den Handbüchern beschriebenen Funktionen können auch über die grafische Oberfläche von openFT, dem openFT Explorer, ausgeführt werden. Der openFT Explorer steht auf Unix- und Windows-Systemen zur Verfügung. Damit können Sie unabhängig vom lokalen System den Betrieb und die FTAC-Umgebung ferner openFT-Installationen auf beliebigen Plattformen bedienen, steuern und überwachen. 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 V12.1 gegenüber openFT V12.0A.

i Die funktionalen Erweiterungen der openFT-Kommandos, die entweder den Verwalter oder den Benutzer betreffen, stehen auch im openFT Explorer zur Verfügung, der auf Unix- und Windows-Systemen ausgeliefert wird. Details finden Sie in der zugehörigen Online-Hilfe unter dem Thema *Neue Funktionen*. Auf z/OS stehen die funktionalen Erweiterungen auch im Menüsystem (Panels) zur Verfügung.

1.4.1 Änderungen für alle Plattformen

- Erweiterte Unicode-Unterstützung

Auf allen Unicode-fähigen Systemen dürfen Dateinamen, FTAC-Zugangsberechtigungen und Folgeverarbeitungen auch Unicode-Zeichen enthalten. Dazu wurde die neue Funktion „Codierungsmodus“ eingeführt, um die Unicode-Namen auf den beteiligten Systemen korrekt darzustellen.

Die Kommandoschnittstellen wurden wie folgt erweitert:

- Alle Plattformen: Das neue Feld FNC-MODE bei der Langausgabe von Logging-Sätzen zeigt den Codierungsmodus für den Dateinamen an (Kommandos *ftshw*, SHOW-FT-LOGGING-RECORDS und FTSHWLOG). Auf BS2000-Systemen wurden die OPS-Variablen um die neuen Elemente FNC-MODE und FNCCS erweitert.
- BS2000- und z/OS-Systeme (ab openFT V12.1C): Die neue Option FILE-NAME-ENCODING zeigt den Codierungsmodus für die Angabe von Fernen Dateinamen sowie für Vor-, Nach- und Folgeverarbeitung bei Dateiübertragungsaufträgen bei folgenden Kommandos an:
 - TRANSFER-FILE-SYNCHRONOUS / FTSCOPY
 - TRANSFER-FILE / FTACOPY
 - CREATE-REMOTE-DIR / FTCREDIR
 - DELETE-REMOTE-DIR / FTDELDIR
 - MODIFY-REMOTE-DIR-ATTRIBUTES / FTMODDIR
 - MODIFY-REMOTE-FILE-ATTRIBUTES / FTMOD
 - SHOW-REMOTE-FILE-ATTRIBUTES / FTSHW
 - DELETE-REMOTE-FILE / FTDEL
 - EXECUTE-REMOTE-CMD / FTEXEC
 - EXECUTE-REMOTE-FTADM-CMD / FTADM
- Unix- und Windows-Systeme:
 - Neue Option *-fnc*, um den Codierungsmodus bei einem Dateiübertragungs-, Dateimanagement oder Administrationsauftrag festzulegen. Diese Option steht bei den Kommandos *ft*, *ftadm*, *ftcredir*, *ftdel*, *ftdeldir*, *ftexec*, *ftmod*, *ftmoddir*, *ftshw* und *nopy* zur Verfügung.
Der Codierungsmodus wird (zusätzlich zu *ftshw*) bei folgenden Kommandos angezeigt: *ftshw* und *ftshwr* (Feld FNC-MODE)
Mit *ftshw -sif* wird die Anzahl der nicht abbildbaren Dateinamen angezeigt.
 - Neues Attribut *CmdMode* in der Konfigurationsdatei eines Fernadministrations-Servers um den (empfohlenen) Codierungsmodus für administrierte openFT-Instanzen festzulegen. Der Codierungsmodus wird beim Kommando *ftshwc* im Feld MODE angezeigt.
Diese Funktion steht auch im Konfigurations-Editor des openFT Explorers zur Verfügung.
 - Auf Unix-Systemen lässt sich für Inbound-Aufträge zusätzlich der Zeichensatz einstellen, der im Zeichenmodus verwendet werden soll. Dazu wurde die neue Option *-fnccs* im Kommando *ftmodo* eingeführt.
Bei *ftshwo* wird im Feld FN-CCS-NAME der Zeichensatz angezeigt, der aktuell für Inbound-Aufträge im Zeichenmodus eingestellt ist.
 - Unicode für C und JAVA
- BS2000- und z/OS-Systeme: für Bibliothekselemente werden bei der Ausgabe von Logging-Sätzen zusätzlich zum Bibliotheksnamen auch Elementname, Typ und Version angezeigt.

-
- Bei Inbound-Aufträgen wird in der Langausgabe und der CSV-Ausgabe der Logging-Sätze im neuen Feld PTNR-ADDR die Adresse des Partnersystems angezeigt. Auf BS2000-Systemen wird die Partneradresse auch in der OPS-Variable PARTNER-ADDRESS angezeigt.

- Deaktivierung der Wiederanlauf-Funktion

Für asynchrone Dateiübertragungs-Aufträge über das openFT- und FTAM-Protokoll kann die Wiederanlauf-Funktion deaktiviert werden. Der Wiederanlauf kann partnerspezifisch für Outbound-Aufträge und global für Inbound- und Outbound-Aufträge eingestellt werden. Dazu wurden folgende Kommandos geändert:

Unix- und Windows-Systeme:

- *ftaddptn* und *ftmodptn*: Neue Option *-rco*
- *ftmodo*: Neue Optionen *-rco* und *-rci*

BS2000- und z/OS-Systeme:

- ADD-FT-PARTNER/MODIFY-FT-PARTNER bzw. FTADDPTN/FTMODPTN:
Neuer Operand RECOVERY-OUTBOUND
- MODIFY-FT-OPTIONS bzw. FTMODOPT:
Neue Operanden RECOVERY-OUTBOUND und RECOVERY-INBOUND

- RSA-Mindestschlüssellänge für das openFT Protokoll

Eine openFT Instanz kann eine RSA-Mindestschlüssellänge zur Verschlüsselung der openFT-Session verlangen. Die Mindestschlüssellänge kann in den Betriebsparametern festgelegt werden. Dazu wurden folgende Kommandos geändert:

Unix- und Windows-Systeme:

- *ftmodo*: Neue Option *-klmin*

BS2000- und z/OS-Systeme:

- MODIFY-FT-OPTIONS bzw. FTMODOPT: Neue Parameter RSA-PROPOSED und RSA-MINIMUM beim Operanden KEY-LENGTH

- AES-Mindestschlüssellänge für das openFT Protokoll

Eine openFT Instanz kann eine AES-Mindestschlüssellänge zur Verschlüsselung der openFT-Session verlangen. Die Mindestschlüssellänge kann in den Betriebsparametern festgelegt werden.

Dazu wurden folgende Kommandos geändert:

Unix- und Windows-Systeme:

- *ftmodo*: Neue Option *-aesmin*

BS2000- und z/OS-Systeme:

- MODIFY-FT-OPTIONS bzw. FTMODOPT: Neuer Parameter AES-MINIMUM beim Operanden KEY-LENGTH

- Verschlüsselung von Dateimanagementaufträgen

Bei Dateimanagement-Aufträgen können die Attribute der Dateien und Verzeichnisse verschlüsselt übertragen werden. Diese Eigenschaft kann auch in Berechtigungsprofilen eingestellt werden.

Dazu wurden folgende Kommandos erweitert:

Unix- und Windows-Systeme:

- *ftshw*: Neue Option *-c*
- *ftcrep* und *ftmodp*: Neue Option *-cm*
- *ftshwp*: Neuer Parameter FILE-AT-ENC in der Langausgabe und neuer Parameter *FileAtEnc* in der csv-Ausgabe.

BS2000- und z/OS-Systeme:

- SHOW-REMOTE-FILE-ATTRIBUTES bzw. FTSHW:
Neuer Operand FILE-ATTR-ENCRYPTION
- CREATE-FT-PROFILE und MODIFY-FT-PROFILE bzw. FTCREPF und FTMODPRF:
Neuer Operand FILE-ATTR-ENCRYPTION
- SHOW-FT-PROFILE bzw. FTSHWPRF:
neuer Parameter FILE-AT-ENC in der Langausgabe und neuer Parameter *FileAtEnc* in der csv-Ausgabe.

Beim Holen mehrerer Dateien aus fernen Systemen mit *ft_mget*, GET-REMOTE-FILES bzw. FTMGET gilt die Verschlüsselungs-Option (*-c* bzw. DATE-ENCRPTION) auch für Datei- und Verzeichnisattribute.

- Ab openFT V12.1C ist die CRYPT-Funktionalität in openFT integriert. Daher wird openFT-CR nicht mehr ausgeliefert.

Änderungen in openFT Version V12.1C10:

- Bei lokalen Outbound Aufträgen wird bei der Langausgabe und der CSV-Ausgabe von Protokollsätzen der entfernte Dateiname im neuen Feld REMOTE-FN angezeigt. Auf BS2000-Systemen wird der entfernte Dateiname auch in der OPS-Variablen F-REM-NAME angezeigt.

1.4.2 Änderungen für Unix- und Windows-Plattformen

- Übertragung von Dateiverzeichnissen:
 - Zwischen Unix- und Windows-Systemen können Dateiverzeichnisse übertragen werden. Dazu wurden die Kommandos *ft* und *ncopy* um die Option *-d* erweitert.
 - Das neue Feld PROGRESS in der Ausgabe von *ftshwr* zeigt den aktuellen Bearbeitungsstand bei der Übertragung von Verzeichnissen an.
 - Die neue Option *ftmodo -ltd* wurde eingeführt, um den Umfang des Logging bei der Verzeichnisübertragung einzustellen.
 - Der neue Wert *ftshwl -ff=T* selektiert Logging-Sätze von Aufträgen zur Verzeichnisübertragung. Zusätzlich wurde die Ausgabe von *ftshwl* erweitert um das Feld TRANSFILE (Langausgabe) sowie um die FT-Funktionen TD, SD, SF (Kurzausgabe) bzw. um den Wert FUNCTION=TRANSFER-DIR (Langausgabe).
- Übertragung mehrerer Dateien mit FTAM:

Zwischen Unix- und Windows-Systemen können über das FTAM-Protokoll mehrere Dateien synchron übertragen werden. Dies wird über eine spezielle Dateinamen-Syntax des Kommandos *ncopy* gesteuert.
- Erweiterung der openFT-Script-Kommandos
 - Der FT-Verwalter kann Grenzwerte für openFT-Script-Aufträge einstellen. Dazu wurde das Kommando *ftmodsuo* um die Optionen *-u*, *-thl* und *-ftl* erweitert.
 - Die aktuell eingestellten Grenzwerte werden bei *ftshwsuo* ausgegeben.
- Das Kommando *ftshwk* zeigt für öffentliche Schlüssel von Partnersystemen den Partnernamen an.
- Unterstützung von FarSync X.25

Auf Linux und Windows werden FarSync X.25-Karten vom Hersteller FarSite direkt durch openFT unterstützt. PCMX wird dafür nicht mehr benötigt.

Zusätzlich wird auf Linux durch den Einsatz der FarSync XOT-Runtime die Verbindungsmethode XOT (X.25 über TCP/IP) unterstützt.

Dazu wurden die Kommandos *ftaddptn*, *ftmodptn*, *ftmodo*, *ftshwptn* und *ftshwo* erweitert.
- Erweiterte Unterstützung des Application Entity Title

Der Application Entity Title (AET) kann jetzt auch für FTAM-Partner zur Absenderüberprüfung verwendet werden. Dazu wurde das Kommando *ftmodo* geändert, indem die Partner-Check-Option *-ptc* erweitert sowie die Option *-aet* zur Spezifizierung des AET hinzugefügt wurde. Das Kommando *ftshwo* wurde um die Option *-ae* erweitert.
- Die maximale Länge der Kommando-Angabe im Kommando *ftexec* wurde auf 8191 erhöht.
- Sonstige Änderungen
 - Geänderte Absenderüberprüfung für Partner, die über IPV6 mit Scope-ID oder X.25 mit Anschlussnummer adressiert werden. Damit ist immer eine eindeutige Identifizierung über die Partneradresse möglich.
 - Das Kommando *ft_mget* wurde um die Option *-case* erweitert, welche die Berücksichtigung der Groß- und Kleinschreibung in der Dateinamenstruktur steuert.
 - Der ADM-Verwalter kann seine Fernadministrations-Berechtigung jetzt auch zurückgeben (Kommando *ftmoda -admpriv=n*). Die Konfiguration des Fernadministrations-Servers bleibt erhalten.

Änderungen in openFT Version V12.1C20:

- Unterstützung von RSA-Schlüsseln mit Länge 3072 und 4096.

Änderungen in openFT Version V12.1C30:

-
- Die openFT-Administrator-Rechte können auf Windows an einen beliebigen Benutzer übertragen werden. Dazu wurde das Kommando *ftmodo* erweitert.

1.4.3 Änderungen für Unix-Plattformen

- Einbenutzerbetrieb

Auf Unix-Systemen kann der Administrator mit dem neuen Kommando *ftsetmode* vom standardmäßigen Mehrbenutzerbetrieb in den Einbenutzerbetrieb umschalten und umgekehrt. Im Einbenutzerbetrieb läuft openFT vollständig unter einer bestimmten Kennung, der sogenannten openFT-Kennung, die zugleich FT- und FTAC-Verwalter ist. Zum Anlegen und Verwalten weiterer openFT-Instanzen im Einbenutzerbetrieb wurden die Kommandos *ftcrei* und *ftmodi* um die Option *-ua* zur Angabe der Benutzerkennung einer neuen Instanz erweitert.

- openFT-Freigabe für 64-Bit-Linux
- SNMP wird auf Unix-Plattformen nicht mehr unterstützt.
- Unterstützung von systemd.

Änderungen in openFT Version V12.1C10:

- Unterstützung von Openshift.

Änderungen in openFT Version V12.1C30:

- Installation mit Lizenzschlüssel.

Änderungen in openFT Version V12.1C40:

- Die FT-Verwalterrechte können auf Unix-Systemen, wie bisher schon in Windows, an einen beliebigen Benutzer übertragen werden.
Dazu wurde das Kommando *ftmodo* erweitert.

Änderungen in openFT Version V12.1C60:

- Der FT-Verwalter kann nun eine Linux-Gruppe als FT-Verwaltergruppe zuweisen, jeder Benutzer in der Gruppe erhält FT-Verwalterrechte.
Dazu wurde das Kommando *ftmodo* erweitert.

1.4.4 Änderungen für BS2000-Systeme und zOS

- Neues Kommando GET-REMOTE-FILES (BS2000-Systeme) bzw. FTMGET (z/OS), um mehrere mit Wildcards spezifizierte Dateien synchron oder asynchron von einem fernen System zu holen.
- Neues Diagnose-Kommando FTPPING auf BS2000-POSIX und z/OS zum Testen einer openFT-Verbindung zu einem fernen Partner.

Änderungen in openFT Version V12.1C60:

- Unterstützung von RSA-Schlüsseln mit Länge 3072 und 4096 Bit.

1.4.5 Änderungen für zOS

- Das PARM-Element der z/OS Parameterdatei wurde wie folgt geändert:
 - Neues Schlüsselwort JOB_JOBCLASS für Folgeverarbeitungs-Jobs, Vorverarbeitungs- und Nachverarbeitungs-Jobs sowie Print-Jobs.
 - Neues Schlüsselwort LISTPARM für die Einstellung eines Standard-Druckers (LISTING=*STD in einem FT-Auftrag).
 - Das Schlüsselwort JOB_MSGCLASS gilt jetzt auch für Vorverarbeitungs- und Nachverarbeitungs-Jobs.
- In FTBATCH kann ab z/OS V2.1 der PARMDD-Parameter anstelle des Parameters PARM verwendet werden.
- NCOPY und FTACOPY: neuer Operandenwert LISTING=*STD bei LOCAL-PARAMETER, um den mit LISTPARM definierten Drucker zuzuordnen.
- openFT (z/OS) unterstützt jetzt Hostnamen mit einer Länge von bis zu 80 Zeichen. Dies gilt sowohl für die interne Kommunikation in z/OS als auch für die Verbindungen mit z/OS-Partnern.
- Das Element TNSTCPIP der z/OS-Parameterdatei wird nicht mehr unterstützt, die Beschreibung ist deshalb entfallen.

Änderungen in openFT Version V12.1C30:

- Das PARM-Element der z/OS Parameterdatei wurde wie folgt geändert:
 - Neues Schlüsselwort TZSTRING zur Zeitonenbehandlung, um fehlende Zeilen beim Lesen von Logging-Sätzen zu vermeiden, die während der Zeitumstellung von Sommer- auf Winterzeit geschrieben worden sind.

1.4.6 Neue Funktionen, die nur im openFT Explorer zur Verfügung stehen

Die folgenden neuen Funktionen stehen nur im openFT Explorer zur Verfügung:

- Öffentliche Schlüssel exportieren
Über das Menü *Administration*, Befehl *Schlüsselverwaltung - Öffentlichen Schlüssel exportieren...* kann der FT-Verwalter öffentliche Schlüssel der lokalen Instanz exportieren.
- Diagnoseinformationen und Konsolmeldungen löschen
Über das Menü *Administration*, Befehle *Diagnoseinformationen* und *Konsolmeldungen* kann der FT-Verwalter Diagnoseinformationen und Konsolmeldungen löschen.
- Das Logging steht auch im Objektbaum des openFT Explorers zur Verfügung.

Weitere Details finden Sie in der Online-Hilfe des openFT Explorers.

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.

i für Hinweistexte.

! für Warnhinweise.

1.6 Internet

Aktuelle Informationen im Internet

Aktuelle Informationen zur openFT-Produktfamilie finden Sie im Internet unter <http://www.fujitsu.com/de/openFT> (deutsch) bzw. <http://www.fujitsu.com/ts/openFT> (englisch).

2 Installation auf Unix-Systemen

In diesem Kapitel wird die Installation und die Konfiguration von openFT auf Unix-Systemen beschrieben.

i Mit openFT wird bis Version V12.1B 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).

Alle solche Referenzen gelten nur für openFT Versionen \leq V12.1B

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 < V11.0 auf Ihrem Rechner.
- Update-Installation
Es existiert openFT V11.0 oder V12.0 auf Ihrem Rechner.
- Installation einer Korrekturversion
Es existiert schon openFT V12.1 auf Ihrem Rechner.

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

- Ab openFT V12 wird der Betrieb ohne CMX unterstützt.
Für openFT-Versionen <= V12.1B gilt:
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“](#).
- Nur für openFT-Versionen <= V12.1B:
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 < V11.0 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 7.0 (JRE 7.0 mit Update 25) 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 eingerichtet 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.

i 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 < V11.0 installiert, dann handelt es sich um eine Neuinstallation.

Notwendige Arbeitsschritte des Systemverwalters

1. Falls schon ein openFT mit 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.
- Sichern die Partnerlisten-Einträge mit *ftshwptn* und ggf. auch die Betriebsparameter-Einstellungen mit *ftshwo* in eine externe Datei.
- Deinstallieren Sie openFT-CR, openFT und die Zusatzprodukte.

2. Installieren Sie die Produktsoftware zu openFT V12.1.

Dabei beachten Sie bitte Folgendes:

Ab openFT Version V12.1C30 können openFT-Lizenzschlüssel (einen für das openFT-Protokoll und optional je einen für das FTAM- und FTP-Protokoll) jederzeit nach der Installation mit dem openFT Explorer (*Administration - Lizenzverwaltung*) oder dem Kommando *ftaddlic* eingegeben werden.

Wenn Sie keinen Lizenzschlüssel angeben, dann läuft openFT mit allen Funktionen ohne Einschränkung für 30 Tage als Demoversion. Diese Demoversion darf ausschließlich zu Evaluierungszwecken verwendet werden!

3. Falls nötig importieren die gesicherten Konfigurationsdaten wie folgt:

- 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.
- Importieren Sie die gesicherten Partnerlisteneinträge und ggf. die Betriebsparameter-Einstellungen, indem Sie die Sicherungsdatei auf Kommandoebene aufrufen.

Nun ist openFT betriebsbereit und wird bei jedem Systemstart aktiviert.

¹ Ab openFT Version V12.1B10 erfolgt die Freigabe nur noch für Linux x86_64. Ab openFT Version V12.1C20 ist Solaris (Sparc) zusätzlich wieder in der Freigabe enthalten. Weitere Plattformen erhalten Sie auf Anfrage bei Ihrem vertrieblichen Fujitsu Ansprechpartner .

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“](#). Wenn CMX nachinstalliert wird, können Sie Standard-TNS-Einträge auch nachträglich per Tool erstellen, siehe [Abschnitt „Transportsystem-Anwendungen in TNS eintragen“](#).
- Das Instanzverzeichnis der Standard-Instanz wird eingerichtet, siehe [Abschnitt „Installation von openFT“](#). 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“](#). CMX-Betrieb, FTP-Server und die Verwendung des TNS sind deaktiviert.
- Als Prozessname 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 Standardberechtigungsatz erzeugt, mit dem alle File-Transfer-Funktionen erlaubt sind.
 - Es wird ein Schlüsselpaarsatz erzeugt (siehe [Abschnitt „Lokale RSA-Schlüsselpaare erzeugen und verwalten“](#)).
 - Für openFT Versionen <= V12.1B (ab Version V12.1C wird systemd verwendet):
Für die Plattformen Linux, HP-UX und AIX werden folgende Startup- und Shutdown-Dateien eingerichtet:
 - die instanzübergreifende 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“](#)).

i Für die Plattform Solaris wird ab openFT V12.0 SMF unterstützt, siehe [Abschnitt „Solaris SMF“](#). 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 in [Abschnitt „Installation von openFT“](#) beschrieben.

2.1.2 Update-Installation von openFT

Es wird eine Update-Installation ausgeführt, wenn bereits openFT V11.0 oder V12.0 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 Handbuch "openFT (Unix- und Windows-Systeme) - Kommandoschnittstelle").

Notwendige Arbeitsschritte des Systemverwalters

1. Installieren Sie openFT von dem Datenträger.
2. Während der Installation bei Systemen, bei denen die openFT-Installation im Dialog stattfindet, werden Sie 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. Diese Kommandos sind im Verzeichnis */opt/openft/bin/ftbin* zu finden, siehe auch Handbuch "openFT (Unix- und Windows-Systeme) - Kommandoschnittstelle".
3. Ab openFT Version V12.1C30 können openFT-Lizenzschlüssel (einen für das openFT-Protokoll und optional je einen für das FTAM- und FTP-Protokoll) jederzeit nach der Installation mit dem openFT Explorer (*Administration - Lizenzverwaltung*) oder dem Kommando *ftaddlic* eingegeben werden.
Wenn Sie keinen Lizenzschlüssel angeben, dann läuft openFT mit allen Funktionen ohne Einschränkung für 30 Tage als Demoversion. Diese Demoversion darf ausschließlich zu Evaluierungszwecken verwendet werden!
4. 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“](#).Siehe dazu auch [Abschnitt „openFT-Instanzen und Cluster-Betrieb“](#).

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“](#). 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.
- 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 in [Abschnitt „Installation von openFT“](#) beschrieben.

2.1.3 Installation einer Korrekturversion

Installation einer Korrekturversion heißt, dass schon openFT V12.1 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 V12.1 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.
3. Ab openFT Version V12.1C30 können openFT-Lizenzschlüssel (einen für das openFT-Protokoll und optional je einen für das FTAM- und FTP-Protokoll) jederzeit nach der Installation mit dem openFT Explorer (*Administration - Lizenzverwaltung*) oder dem Kommando *ftaddlic* eingegeben werden.
Wenn Sie keinen Lizenzschlüssel angeben, dann läuft openFT mit allen Funktionen ohne Einschränkung für 30 Tage als Demoversion. Diese Demoversion darf ausschließlich zu Evaluierungszwecken verwendet werden!

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 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 V11.0 oder V12.0, bei Installation einer Korrekturversion eine openFT Version V12.1.

Ab openFT Version V12.1C30 werden während der Installation die Lizenzschlüssel abgefragt:

- Wenn Sie einen gültigen Basislizenzschlüssel angeben, dann ist die Basisfunktionalität von openFT freigeschaltet (openFT-Protokoll, FTADM-Protokoll und FTAC-Funktionalität). In einem weiteren Schritt werden die optionalen Lizenzschlüssel für die Protokolle FTAM und FTP abgefragt. Wenn Sie einen gültigen Lizenzschlüssel für ein optionales Protokoll angeben, dann wird dieses Protokoll freigeschaltet. Sie können den Dialog überspringen, wenn keine gültigen Schlüssel für FTP und FTAM vorliegen.

i Wenn Sie einen gültigen Lizenzschlüssel für eine Sonderversion eingeben (z.B. CL- oder FTAM-CL-Version), dann werden keine Lizenzschlüssel für FTAM und/oder FTP abgefragt, da der unterstützte Funktionsumfang bereits in der Sonderversion enthalten ist.

- Wenn Sie keinen Lizenzschlüssel angeben, dann läuft openFT mit allen Funktionen ohne Einschränkung für 30 Tage als Demoversion. Diese Demoversion darf ausschließlich zu Evaluierungszwecken verwendet werden!

Sie können openFT-Lizenzschlüssel jederzeit nach der Installation mit dem openFT Explorer (*Administration - Lizenzverwaltung*) oder dem Kommando `ftaddlic` eingeben.

Gehen Sie wie folgt vor:

1. Installieren Sie die Produktsoftware zu openFT V12.1 in das alternative root-Verzeichnis.

Wechseln Sie in das gemountete Verzeichnis und starten Sie folgende Prozedur:

```
sh install.ft -r=<alternative root directory>
```

Beispiel:

Zur Installation von openFT in das Verzeichnis `/altroot` rufen Sie folgendes Kommando auf:

```
sh install.ft -r=/altroot
```

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 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 V12.1 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

i Ab Version openFT V12.1C30 werden während der Installation unter Solaris keine Eingabeaufforderungen mehr angezeigt, ob FTP und FTAM installiert werden sollen. Daher sind die Variablen "FTAM" und "FTP" in der response Datei nicht erforderlich, und wenn sie hinzugefügt werden, haben sie keine Auswirkungen.

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.

2.1.6 Unterstützung von Openshift

Ab Version 12.1C10 ist openFT für den Betrieb in einer eingeschränkten Umgebung, wie Openshift, vorbereitet. Aufgrund des fehlenden Zugriffs auf root nach dem Erzeugen des Docker-Images wird ein neuer Modus eingeführt, der als eingeschränkter Mehrbenutzermodus bezeichnet wird. Trotz des Namens ist er ähnlich wie der Einzelbenutzermodus. Der Hauptunterschied besteht darin, dass in diesem neuen Modus ein unprivilegierter Benutzer Instanzen erstellen darf. Der neue eingeschränkte Mehrbenutzermodus (limited multi user mode), aktiviert über das Kommando "ftsetmode -lm -ga=root:root", darf nur in einer containerbasierten Umgebung verwendet werden. Eine im Mehrbenutzermodus erstellte Instanz wird zum FT-Administrator und kann die üblichen Verwaltungsaufgaben ausführen.

Es ist erwähnenswert, dass die Instanz ohne systemd-Unterstützung erstellt wird, da systemd in einer containerisierten Umgebung nicht vorhanden ist und daher beim Erstellen, Installieren oder Aufrufen einiger Befehle entsprechende Warnungen erscheinen.

Ein beispielhaftes Dockerfile ist dem openFT-Paket im Docker/OpenShift-Speicherort beigefügt:

```
CD.ftv410.openFT12.1C10_F70.1_20201201.tgz
```

```
|-- docker
|   |-- OpenShift
|   |   |-- Dockerfile
|-- install.ft
|-- openFT-12.1C10-410.x86_64.rpm
```

Das Dockerfile befindet sich im Verzeichnis docker/OpenShift und kann folgendermaßen aussehen:

Dockerdatei:

```
# Example docker file for OpenShift
# Base system is Redhat8.
FROM registry.access.redhat.com/ubi8/ubi

# Install packages required
RUN yum install openssl procps net-tools tar -y; yum clean all

ENV PACKAGE_DIR /root/openFT_tmp

# switch to temporary directory for openFT package handling
RUN mkdir $PACKAGE_DIR
WORKDIR $PACKAGE_DIR

# Copy the openFT package the root dir. The desired package should be the only one in the
# directory.

COPY CD.ftv*.openFT*.tgz .

# Untar the openFT package to the root dir.
RUN tar -xvf CD.ftv*.openFT*.tgz

# Install openFT.
RUN rpm -i openFT-*.x86_64.rpm

# set workdir back to root's home
WORKDIR /root

# cleanup temporary directory
RUN rm -vfr $PACKAGE_DIR

# Switch to hidden limited multi user mode available under openshift environment.
RUN /opt/openFT/bin/ftbin/ftsetmode -lm -ga=root:root

# Expose basic port used by openFT.
EXPOSE 1100

# Set entry point to the exemplary start script.
ENTRYPOINT "/opt/openFT/bin/ftbin/openft_init"
```

Im Beispiel wird das standardmäßige `openft_init` (in der rpm-Datei vorhanden) ausgeführt. Das `openft_init`-Skript kann ähnlich wie das folgende aussehen:

openft_init:

```
# Export path to the openFT binaries.
export PATH=$PATH:/opt/openFT/bin

# Extract ip address of eth0 interface.
ip_addr=`ifconfig eth0 | grep "inet " | tr -s ' ' | cut -f3 -d ' '`

# Create instance a new user, with eth0 ip address.
ftcrei openft -addr=$ip_addr

# Switch to created instance, to allow usage of openFT for new user.
. ftseti openft

# Start openFT service.
ftstart

# Start /sbin/init as and long time running process.
exec /sbin/init
```

Der Zweck des Skripts ist es, eine eigene Instanz zu erstellen (die an die ipv4-Adresse der eth0-Schnittstelle auf Port 1100 gebunden wird) und den openFT-Dienst automatisch bei jedem Neustart des OpenShift-Containers zu starten. Im Beispiel wurde /sbin/init als lang laufender Prozess ausgewählt (Prozess, der im Falle eines Endes oder Absturzes den Neustart des Containers auslöst).

Mit der obigen Struktur kann man das Docker-Image erstellen, es auf den OpenShift-Cluster schieben und ausführen. Diese Schritte liegen außerhalb des Rahmens dieses Dokuments.

Zusätzliche Hinweise:

Falls andere Operationen durchgeführt werden müssen, die Root-Zugriff erfordern (wie die Installation von FTAM, FTP, JAVA oder anderen), muss das Dockerfile erweitert oder als Basis verwendet werden. Auch das Exportieren anderer erforderlicher Ports muss während der Image-Erstellung durchgeführt werden. Der Benutzer muss möglicherweise die Zugangsberechtigung der Dateiübertragung konfigurieren.

Im aktuellen openFT wurde die Verwendung von systemd eingeführt. Unter der Docker/Podman-Build-Umgebung ist systemd nicht verfügbar (unter Containern, die in der OpenShift-Umgebung laufen, ist das auch der Fall). Dies kann zu einigen Warnmeldungen während des Image-Erstellungsprozesses führen (und kann ignoriert werden).

Während des ftsetmode-Befehls wird ftstart aufgerufen, was unter podman-Build-Umgebung nicht funktioniert (es werden zusätzliche Meldungen ausgegeben). Dies ist kein Problem, wenn der Container danach funktioniert.

2.1.7 Unterstützung von systemd

Ab Version 12.1C von openFT wird SysV init nicht als Methode für den automatischen Start von openFT auf einer Linux-Plattform unterstützt. Stattdessen wird systemd verwendet. Während der Installation von openFT werden zwei neue systemd-Einheiten installiert :

1. openFT.service - ermöglicht den automatischen Start aller erstellten Instanzen von openFT
2. openFT@.service - ermöglicht eine selektive Steuerung einer openFT-Instanz

Darüber hinaus wird zum Anpassen der Einstellungen für Instanzen für jede Instanz eine Konfigurationsdatei `override.conf` erstellt.

Standardmäßig ist openFT.service aktiviert, d.h. es wird beim Systemstart gestartet. Während des Upgrades der vorhandenen Installation werden alte SysV-Init-Skripte deinstalliert, sodass alle daran vorgenommenen Änderungen verloren gehen.

Infolgedessen ist die Schnittstelle des Skripts `/etc/init.d/openFT` nicht mehr verfügbar und wird durch folgende Befehle ersetzt:

1. `systemctl start openFT.service` - startet alle openFT Instanzen
2. `systemctl stop openFT.service` - beendet alle openFT Instanzen
3. `systemctl restart openFT.service` - Neustart aller openFT Instanzen
4. `systemctl status openFT.service` - zeigt an, ob openFT seit dem letzten Systemstart mit "systemctl start" gestartet wurde
5. `systemctl enable openFT.service` - aktiviert den automatischen Start aller openFT-Instanzen (dies erfolgt standardmäßig bei Installation / Upgrade)
6. `systemctl disable openFT.service` - deaktiviert den automatischen Start aller openFT-Instanzen. Es ist jedoch möglich, einzelne Instanzen auszuwählen, die automatisch gestartet werden sollen
7. `systemctl start openFT@instancename.service` - startet eine openFT-Instanz, z.B. startet `systemctl start openFT@std` die Standardinstanz von openFT
8. `systemctl stop openFT@instancename.service` - beendet eine openFT Instanz.
9. `systemctl restart openFT@instancename.service` - Neustart einer openFT Instanz
10. `systemctl status openFT@instancename.service` - zeigt den Status einer openFT Instanz
11. `systemctl enable openFT@instancename.service` - aktiviert eine openFT Instanz. Beachten Sie, dass durch das Aktivieren von openFT service alle vorhandene Instanzen aktiviert werden, wenn dieser Befehl ausgeführt wurde
12. `systemctl disable openFT@instancename.service` - deaktiviert eine openFT-Instanz. Nach dem Aktivieren von openFT service und dem anschließenden Deaktivieren einer bestimmten Instanz werden alle Instanzen außer dieser deaktivierten Instanz beim Booten gestartet.
13. `systemctl status openFT@*` - zeigt den Status aller Instanzen.

Als Ergänzung zur obigen Liste wurden vorhandene openFT-Befehle übernommen, die wie folgt funktionieren:

1. `ftstart` behält das aktuelle Verhalten bei, startet jedoch zusätzlich `openFT@service` der Instanz in systemd
2. `ftstop` behält das aktuelle Verhalten bei, stoppt jedoch zusätzlich `openFT@service` der Instanz in systemd
3. `ftcrei` aktiviert zusätzlich `openFT@service` der Instanz in systemd
4. `ftdeli` deaktiviert zusätzlich `openFT@service` der Instanz in systemd

2.1.7.1 Einbenutzerbetrieb

Im Allgemeinen wird der Einbenutzerbetrieb von `systemd` nicht behandelt. Übliche `openFT`-Befehle können wie zuvor verwendet werden, z. `ftstart`, `ftstop`. Die einzige Ausnahme ist, dass während der Instanzerstellung mit dem Befehl `ftcrei` dieser automatisch in `systemd` aktiviert und beim Löschen mit `ftdeli` deaktiviert wird.

Remark

`OpenFT` startet nach der Neuinstallation im Mehrbenutzerbetrieb. Bei der Aktualisierung oder Korrektur der Installation bleibt der `openFT`-Modus erhalten. Wenn `openFT` im Mehrbenutzerbetrieb ausgeführt wurde, wird es nach der Update- oder Korrekturinstallation im Mehrbenutzerbetrieb ausgeführt. Wenn `openFT` im Einbenutzerbetrieb ausgeführt wurde, bleibt der Einbenutzerbetrieb erhalten, wenn `openFT` erneut installiert wird.

2.1.7.2 Aktivierung von ftalarm

Um den automatischen Start von ftalarm zu aktivieren, müssen Sie den systemd Unitfile mit dem Befehl "systemctl edit openFT@instancename" bearbeiten und die ExecStartPost-Aktion zum Starten von ftalarm auskommentieren. Im Einbenutzerbetrieb wird ftalarm wie zuvor aktiviert, indem das openFTinst-Skript bearbeitet wird.

2.1.7.3 Änderung des umask Wertes

Ähnlich wie bei ftalarm muss zum Ändern des Standard-umask-Werts den systemd Unitfile mit "systemctl edit openFT@instancename" bearbeitet, die Zeile zum Setzen des umask-Wert aktiviert und der gewünschte umask-Wert festgelegt werden.

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 [Abschnitt „Standardeinstellungen überprüfen“](#)
- 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 [Abschnitt „Konfigurationsdaten importieren“](#)
- automatischen openFT-Start deaktivieren; siehe [Abschnitt „Automatischen openFT-Start deaktivieren“](#)
- *ftalarm*-Funktion aktivieren, siehe [Abschnitt „ftalarm-Kommando aktivieren“](#)
- openFT-FTAM auf HP-UX, AIX und Linux installieren oder deinstallieren. siehe [Abschnitt „openFT-FTAM auf HP-UX, AIX und Linux installieren oder deinstallieren“](#)
- openFT-FTP auf HP-UX, AIX und Linux installieren oder deinstallieren, siehe [Abschnitt „openFT-FTP auf HP-UX, AIX und Linux installieren oder deinstallieren“](#)
- Authentifizierung über PAM (Pluggable Authentication Modules) aktivieren/deaktivieren, siehe [Abschnitt „Authentifizierung über PAM“](#)
- Partnerliste aus TNS erzeugen, siehe [Abschnitt „Partnerliste aus TNS erzeugen“](#)
- Fernadministrations-Server konfigurieren
Wenn Sie Ihr System als Fernadministrations-Server einsetzen möchten, müssen Sie diesen konfigurieren, siehe [Abschnitt „Fernadministrations-Server konfigurieren“](#).
- ADM-Trap-Server konfigurieren
Wenn Sie Ihr System als ADM-Trap-Server einsetzen möchten, müssen Sie diesen konfigurieren, siehe [Abschnitt „ADM-Trap-Server konfigurieren“](#).
- TNS-Einträge erstellen
Falls Sie den TNS verwenden, müssen Sie ggf. TNS-Einträge erstellen, siehe [Abschnitt „Transportsystem-Anwendungen in TNS eintragen“](#).

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 „Transportsystem-Anwendungen in TNS eintragen“](#).

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

i Ab openFT Version V12.1B erfolgt die Freigabe nur noch für Linux x86_64. Ab openFT Version V12.1C20 ist Solaris (Sparc) zusätzlich wieder in der Freigabe enthalten. Weitere Plattformen erhalten Sie auf Anfrage bei Ihrem vertrieblichen Fujitsu Ansprechpartner.

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 Standardberechtigungsatz ist so eingestellt, dass File Transfer uneingeschränkt möglich ist. Als FTAC-Verwalter sollten Sie daher den Standardberechtigungsatz umgehend dem Schutzbedürfnis des Rechners anpassen (siehe auch [Abschnitt „Berechtigungssätze verwalten“](#)).

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 CCS-NAME
YES NONE 16 8 2000 30 65535 ISO88591
PTN-CHK DYN-PART SEC-LEV FTAC-LOG FT-LOG FT-DIR-LOG ADM-LOG USE TNS USE CMX
STD ON B-P-ATTR ALL ALL NONE ALL NO NO
OPENFT-APPL FTAM-APPL FTP-PORT ADM-PORT ADM-CS
*STD *STD 21 11000 NO
ACTIVE ACTIVE ACTIVE ACTIVE
RSA-PROP RSA-MIN AES-MIN ENC-MAND
2048 0 NONE NO
HOST-NAME IDENTIFICATION / LOCAL SYSTEM NAME
*NONE mc011.mynet.local / $FJAM,MC011
FT-ADMIN FTAC-ADMIN
ROOT *STD
FN-CSS-NAME DEL-LOG ON AT RETPD RECOVERY ADM-TRAP-SERVER
ISO88591 OFF DAILY 00:00 14 IN+OUT *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 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 im Handbuch "openFT (Unix- und Windows-Systeme) - Kommandoschnittstelle".

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 „Eindeutige Instanzidentifikationen“](#).

- 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 -dp=f* auf OFF.

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

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 Handbuch "openFT (Unix- und Windows-Systeme) - Kommandoschnittstelle". 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 per 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 per Menü *Administration*, Befehl *Fernadministration - Konfiguration importieren*.

2.2.3 Automatischen openFT-Start deaktivieren

i Dieser Abschnitt gilt nur für openFT Versionen \leq V12.1C, da ab Version V12.1C systemd verwendet wird.

i Dieser Abschnitt gilt nicht für Solaris, da openFT V12.1 den automatischen Start von openFT auf Solaris ohne SMF nicht unterstützt. Für Solaris mit SMF wird ein anderer Mechanismus verwendet, siehe [Abschnitt „Solaris SMF“](#).

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“](#)).

Diese Dateien starten dann openFT in jeder 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 oder `/etc/rc.ft` auf AIX). 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“](#)). Diese Dateien beenden dann die jeweilige openFT-Instanz.

2.2.4 *ftalarm*-Kommando aktivieren

i Dieser Abschnitt gilt nicht für Solaris. Dort wird ein anderer Mechanismus verwendet, siehe [Abschnitt „Solaris SMF“](#).

Wenn Sie über eine Häufung fehlgeschlagener FT-Aufträge informiert werden wollen, empfiehlt es sich, das *ftalarm*-Kommando zu verwenden, siehe Handbuch "openFT (Unix- und Windows-Systeme) - Kommandoschnittstelle".

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 Solaris SMF

i Ab Version openFT V12.1B wird die Plattform Solaris nur noch auf Anfrage unterstützt,

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/etc/init/openFTinst* werden mit Solaris SMF **nicht** installiert. *ftalarm* wird per SMF aktiviert, siehe [Abschnitt „SolarisSMF“](#).
- 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 ab 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.

i Zur Einstellung der Schutzbits über SMF siehe [Abschnitt „Schutzbiteinstellung für neu angelegte Dateien \(Unix-Systeme\)“](#).

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.

i 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
online         16:32:14  svc:/application/ftalarm:inst001
#. ftseti inst001
# ftstart
ftstart: openFT 12.1A00 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. s

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 Einstellungen 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 Einstellungen anzeigen lassen mit:

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

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

i Ab openFT Version V12.1B erfolgt die Freigabe nur noch für Linux x86_64. Ab openFT Version V12.1C20 ist Solaris (Sparc) zusätzlich wieder in der Freigabe enthalten. Weitere Plattformen erhalten Sie auf Anfrage bei Ihrem vertrieblichen Fujitsu Ansprechpartner.

Ab der openFT-Version V12.1C30 existieren `install.ftam` und `install.ftp` nicht mehr, da sie durch das Lizenzsystem ersetzt werden. Das Ausführen von `install.ftp` und `install.ftam` auf openFT V12.1C30 oder höher hat keine Auswirkungen.

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 Handbuch "openFT (Unix- und Windows-Systeme) - Kommandoschnittstelle".

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.

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

i Ab openFT Version V12.1B erfolgt die Freigabe nur noch für Linux x86_64. Ab openFT Version V12.1C20 ist Solaris (Sparc) zusätzlich wieder in der Freigabe enthalten. Weitere Plattformen erhalten Sie auf Anfrage bei Ihrem vertrieblichen Fujitsu Ansprechpartner.

Ab der openFT-Version V12.1C30 existieren `install.ftam` und `install.ftp` nicht mehr, da sie durch das Lizenzsystem ersetzt werden. Das Ausführen von `install.ftp` und `install.ftam` auf openFT V12.1C30 oder höher hat keine Auswirkungen.

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 Handbuch "openFT (Unix- und Windows-Systeme) - Kommandoschnittstelle".

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.

2.2.8 Authentifizierung über PAM

i Ab openFT Version V12.1B erfolgt die Freigabe nur noch für Linux x86_64. Ab openFT Version V12.1C20 ist Solaris (Sparc) zusätzlich wieder in der Freigabe enthalten. Weitere Plattformen erhalten Sie auf Anfrage bei Ihrem vertrieblichen Fujitsu Ansprechpartner.

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 [Abschnitt „Authentifizierung über PAM“](#).

In manchen Fällen ist es notwendig, die Konfigurationsdateien zu überprüfen und die Einträge anzupassen, siehe [Abschnitt „Authentifizierung über PAM“](#).

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 Authentifizierungsverfahren 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
```

2.2.9 Partnerliste aus TNS erzeugen

i PCMX wird auf Unix-Systemen letztmalig mit openFT V12.1B unterstützt und ausgeliefert. Bitte stellen Sie alle TNS-Einträge, die openFT Partner betreffen, auf Partnerlisten-Einträge um.

openFT bietet durch die Partnerliste die Möglichkeit, ohne TNS zu arbeiten. 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 Installation auf Windows-Systemen

In diesem Kapitel wird die Installation und die Konfiguration von openFT auf Windows-Systemen beschrieben.

i Mit openFT wird auch ein Kommunikationsmanager ausgeliefert (PCMX). Dieser Kommunikationsmanager wird im Folgenden als CMX bezeichnet.

3.1 Installation von openFT

Die Installation von openFT müssen Sie unter einer Kennung mit Windows-Administratorrechten ausführen.

Die Installation von openFT V12.1 wird mit dem Windows Installer von Microsoft durchgeführt. Starten Sie die bedienergeführte Installation wie in Windows üblich durch Doppelklick auf das Programm *setup.exe*, das sich auf dem Datenträger mit der openFT-Software befindet. Sie können openFT auch "bedienerlos" installieren, siehe [Abschnitt „Bedienerlose Installation“](#).

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 < V11.0 auf Ihrem Rechner.
- **Update-Installation**
Es existiert openFT V11.0 oder V12.0 auf Ihrem Rechner.
- **Installation einer Korrekturversion**
Es existiert schon openFT V12.1 auf Ihrem Rechner.

Sie können eine vorhandene openFT-Installation über die Ändern-Funktion von Windows erweitern und den openFT SNMP-Agenten nachträglich installieren oder deinstallieren. Auf Windows 10 z.B. finden Sie die Funktion unter *Systemsteuerung - Programme und Funktionen - openFT - Ändern*. Mit *Systemsteuerung - Programme und Funktionen - openFT - Reparieren* können Sie eine vorhandene Installation ggf. auch reparieren.

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

- Ist im Betriebssystem *Deutsch* oder *Englisch* als Sprache eingestellt, wird diese bei der Installation verwendet und als Standardsprache für openFT voreingestellt. Für alle anderen Systemsprachen wird abgefragt, ob Deutsch oder Englisch bei der Installation und als Standardsprache verwendet werden soll (siehe dazu [Abschnitt „Sprachoberfläche wechseln“](#)).
- Ein Windowsbenutzer der mit dem openFT arbeiten können soll, benötigt das Recht „Log on locally“
- Für openFT Versionen <= V12.1B:
Wenn Sie die Verschlüsselung der Dateiinhalte nutzen wollen, müssen Sie zusätzlich openFT-CR V12.1 (Windows) installieren. Diese Software wird lizenzfrei gegen eine Schutzgebühr zur Verfügung gestellt. Wenn bereits ein openFT-CR mit Version < V11.0 installiert ist, dann müssen Sie diese Version vor der Installation von openFT deinstallieren. openFT-CR V12.1 dürfen Sie erst nach der Installation von openFT V12.1 installieren.



- Nach einer Neuinstallation von openFT V12.1 kann nur openFT-CR V12.1 verwendet werden. Ältere Version von openFT-CR aus V11.0 oder V12.0 können nach einer Neuinstallation von openFT V12.1 nicht mehr installiert werden.
- Bei einer Update-Installation von openFT V12.1 gilt:
War zuvor openFT-CR aus V11.0 oder V12.0 installiert, dann ist die openFT-CR Funktionalität bereits aktiviert und bleibt nach der Update-Installation erhalten. Wenn Sie anschließend die alte openFT-CR deinstallieren, dann kann das alte openFT-CR später nicht mehr installiert werden.

- Wenn Sie die openFT-Script-Schnittstelle oder das Java-API nutzen wollen, dann muss auf Ihrem System mindestens das J2SE™ Runtime Environment 7.0 (JRE 7.0 mit Update 25) installiert sein.

-
- Die Installation der SNMP-Unterstützung setzt einen installierten Microsoft SNMP-Server voraus, siehe [Abschnitt „Installation des SNMP-Subagenten“](#).

- Installationsverzeichnis

Der Pfad, unter dem openFT installiert wird, hängt von mehreren Faktoren ab und wird im Folgenden allgemein als *openFT-Installationsverzeichnis* bezeichnet.

Im Einzelnen gilt:

- Der Pfad ist abhängig von Ihrem Betriebssystem. Standardmäßig wird openFT in das Verzeichnis *%ProgramFiles%\openFT* installiert.
- Bei der Installation können Sie das Installationsverzeichnis frei vergeben, als Installationspfad darf jedoch kein Netzlaufwerk angegeben werden. Die maximale Pfadlänge beträgt 110 Zeichen.

Es wird empfohlen, den vorgeschlagenen Pfad zu verwenden.

- Instanzenverzeichnis

Das Instanzenverzeichnis wird beim Installieren eingerichtet und enthält

Unterverzeichnisse für anwendungsspezifische Daten der jeweiligen openFT-Instanz wie z.B. Logging-Datei, Schlüsselpaarsätze und Trace-Dateien. Bei Windows-Systemen lautet der Pfad standardmäßig *%ProgramData%\Fujitsu Technology Solutions\openFT\var\instanz*.

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

i 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.

3.1.1 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.
 - Sichern die Partnerlisten-Einträge mit *ftshwptn* und ggf. auch die Betriebsparameter-Einstellungen mit *ftshwo* in eine externe Datei.
 - Deinstallieren Sie openFT-CR, openFT und die Zusatzprodukte.
2. Installieren Sie die Produktsoftware zu openFT V12.1.

Während der Installation werden die Lizenzschlüssel abgefragt:

- Wenn Sie einen gültigen Basislizenzschlüssel angeben, dann ist die Basisfunktionalität von openFT freigeschaltet (openFT-Protokoll, FTADM-Protokoll und FTAC-Funktionalität). In einem weiteren Schritt werden die optionalen Lizenzschlüssel für die Protokolle FTAM und FTP abgefragt. Wenn Sie einen gültigen Lizenzschlüssel für ein optionales Protokoll angeben, dann wird dieses Protokoll freigeschaltet. Sie können den Dialog überspringen, wenn keine gültigen Schlüssel für FTP und FTAM vorliegen.

i Wenn Sie einen gültigen Lizenzschlüssel für eine Sonderversion eingeben (z.B. CL- oder FTAM-CL-Version), dann werden keine Lizenzschlüssel für FTAM und/oder FTP abgefragt, da der unterstützte Funktionsumfang bereits in der Sonderversion enthalten ist.

- Wenn Sie keinen Lizenzschlüssel angeben, dann läuft openFT mit allen Funktionen ohne Einschränkung für 30 Tage als Demoversion. Diese Demoversion darf ausschließlich zu Evaluierungszwecken verwendet werden!

Sie können openFT-Lizenzschlüssel jederzeit nach der Installation mit dem openFT Explorer (*Administration - Lizenzverwaltung*) oder dem Kommando *ftaddlic* eingeben.

Während der Installation wird automatisch die Identifikation (*ftmodo -id=*) gesetzt. Bitte überprüfen Sie, ob der Wert korrekt ist.

3. Falls nötig importieren die gesicherten Konfigurationsdaten wie folgt:
 - 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.
 - Importieren Sie die gesicherten Partnerlisteneinträge und ggf. die Betriebsparameter-Einstellungen, indem Sie die Sicherungsdatei auf Kommandoebene aufrufen.

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“](#).
Wenn CMX nachinstalliert wird, können Sie Standard-TNS-Einträge auch nachträglich per Tool erstellen, siehe [Abschnitt „Transportsystem-Anwendungen in TNS eintragen“](#).
 - Das Instanzverzeichnis der Standard-Instanz wird eingerichtet, siehe [Abschnitt „Installation von openFT“](#).
Die instanzenspezifischen Dateien befinden sich im Verzeichnis *%ProgramData%\Fujitsu Technology Solutions\openFT\var\std*.
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“](#).
CMX-Betrieb, FTP-Server und die Verwendung des TNS sind deaktiviert.
 - Als Prozessorname wird der Name des Rechners eingetragen.
 - 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 Standardberechtigungsatz erzeugt, mit dem alle File-Transfer-Funktionen erlaubt sind.
 - Es wird ein Schlüsselpaarsatz erzeugt (siehe [Abschnitt „Lokale RSA-Schlüsselpaare erzeugen und verwalten“](#)).
 - Der openFT-Dienst und der asynchrone openFT-Server werden gestartet.

3.1.2 Update-Installation von openFT

Es wird eine Update-Installation ausgeführt, wenn bereits openFT V10.0, V11.0 oder V12.0 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.
- Evtl. vorhandene Trace-Dateien und Diagnosedateien 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 Handbuch "openFT (Unix- und Windows-Systeme) - Kommandoschnittstelle").

Notwendige Arbeitsschritte des Systemverwalters

1. Installieren Sie openFT von dem Datenträger.
2. Während der Installation werden Sie aufgefordert, den Lizenzschlüssel einzugeben.

Nach einer Update-Installation wird der asynchrone openFT-Server für die Standard-Instanz automatisch gestartet, d.h. die Betriebsparameter-Option *Asynchronen Server automatisch starten* im openFT Explorer ist aktiviert. Diese Option finden Sie über das Menü *Administration*, Befehl *Betriebsparameter*, Registerblatt *Allgemein*. Für die anderen Instanzen ist diese Option deaktiviert. Daher müssen Sie diese Option in diesen Instanzen aktivieren, wenn der zugehörige asynchrone openFT-Server immer automatisch gestartet werden soll.

Automatisch ausgeführte Arbeitsschritte

Bei einer Update-Installation werden folgende Schritte automatisch ausgeführt:

- 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. Die Instanzverzeichnisse aktuell vorhandener Instanzen einschließlich der Standardinstanz werden aktualisiert, d.h.:
 - Die Logging-Datei wird gelöscht.
 - Es werden folgende Konfigurationsdaten übernommen:
 - Betriebsparameter (der Betrieb mit CMX bleibt eingeschaltet)
 - Instanzidentifikation
 - Einträge der Partnerliste
 - Berechtigungssätze und -profile
 - Schlüsselpaarsätze
 - Konfigurationsdaten für die zentrale Administration (bei Update von V11.0).

Ist bei der Update-Installation ein Neustart des Rechners notwendig, so wird der Instanzen-Update erst nach dem Neustart durchgeführt. Im Fehlerfall wird für jede Instanz eine Datei *ftupdi-Instanz.log* mit den entsprechenden Fehlermeldungen im Verzeichnis *%ProgramFiles%\openFT* angelegt. Bitte prüfen Sie nach jeder Update-Installation mit Neustart, ob im Verzeichnis *%ProgramFiles%\openFT* Dateien *ftupdi-Instanz.log* existieren. In diesem Fall müssen Sie den Update der Instanzen mit dem Kommando *ftupdi verzeichnis* manuell durchführen. Anschließend können Sie die zugehörige Datei *ftupdi-Instanz.log* löschen.

i Ab openFT Version 12.1C20 gibt es zwei zusätzliche Schlüsselpaare mit den Längen 3072 und 4096. Sie werden nach beendeter Update-Installation generiert, sobald die Instanz zum ersten mal läuft.

3.1.3 Installation einer Korrekturversion

Installation einer Korrekturversion heißt, dass schon openFT V12.1 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 V12.1 von dem Datenträger.

Alle Lizenzschlüssel werden ohne Rückfrage übernommen, der Installationsstatus des SNMP-Subagenten (installiert/nicht installiert) bleibt unverändert.

Automatisch ausgeführte Arbeitsschritte

Bei der Installation einer Korrekturversion werden folgende Schritte automatisch ausgeführt:

- Laufende openFT-Prozesse werden beendet, laufende openFT-Script-Aufträge werden abgebrochen.
- Die Berechtigungsprofile und -sätze, die Logging-Dateien, 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.

3.1.4 Bedienerlose Installation

CMX und openFT können auch bedienerlos mit Hilfe des Kommandos *msiexec* (Windows Installer) installiert werden. Bitte beachten Sie dabei Folgendes:

- Die Installation muss von einer Konsole mit Administratorberechtigung gestartet werden, d.h. entweder führt der Administrator die Installation durch oder die Konsole wurde bei eingeschalteter Benutzerkontensteuerung mit *Als Administrator ausführen* gestartet. Andernfalls fehlt die Berechtigung zur Installation!
- Wenn Sie im Betrieb mit CMX arbeiten möchten, sollten Sie CMX vor openFT installieren. Dadurch werden die Standard-TNS-Einträge für openFT automatisch erzeugt.

Mit *msiexec* installieren Sie die MSI-Installationspakete *openFT.msi* bzw. *PCMX-32.msi*. Beide befinden sich auf der Produkt-CD im Verzeichnis *openFT\Unattended_installation*.

Beim Aufrufe von *msiexec* geben Sie die jeweilige MSI-Datei als Argument an.

Mögliche weitere Windows Installer Parameter:

ADDLOCAL:

Mit ADDLOCAL wird bestimmt, welche optionalen Features installiert werden. Möglicher Wert für ADDLOCAL ist SNMP.

ADDLOCAL SNMP bedeutet, dass zusätzlich zu openFT auch der SNMP Subagent von openFT installiert wird. Dazu muss zuerst der SNMP-Dienst von Microsoft installiert werden, siehe [Abschnitt „Installation des SNMP-Subagenten“](#).

Wird ADDLOCAL nicht angegeben, dann wird nur das openFT-Protokoll installiert, die SNMP-Unterstützung wird nicht installiert.

openFT kann nur die Übertragungsprotokolle nutzen, für die ein gültiger Lizenzschlüssel vorhanden ist (siehe openFT Properties LICENSEKEY, FTAMLICENSEKEY und FTPLICENSEKEY).

TRANSFORMS:

Durch Angabe des Parameters kann die deutsche Sprachvariante von openFT eingestellt werden. Zur Spracheinstellung siehe [Abschnitt „Sprachoberflächewechseln“](#).

openFT Properties:

LICENSEKEY:

Für den Parameter LICENSEKEY ist ein gültiger openFT-Lizenzschlüssel anzugeben. Wenn Sie keinen Lizenzschlüssel angeben, läuft openFT mit allen Funktionen ohne Einschränkung für 30 Tage als Demoversion. Diese Demoversion darf ausschließlich zu Evaluierungszwecken verwendet werden!

Die Eingabe des openFT-Lizenzschlüssels ist auch jederzeit nach der Installation mit dem openFT Explorer (*Administration - Lizenzverwaltung*) oder dem Kommando *ftaddlic* möglich.

Der LICENSEKEY besteht aus fünf Teilschlüsseln, die durch das Minuszeichen getrennt sind und jeweils aus fünf Zeichen bestehen.

Beispiel:

12345-12345-12345-12345-12345

FTAMLICENSEKEY:

Die Angabe von FTAMLICENSEKEY ist optional.

Für FTAMLICENSEKEY ist ein gültiger Lizenzschlüssel für das FTAM-Protokoll anzugeben. Die Angabe von FTAMLICENSEKEY ist nur dann sinnvoll, wenn Sie bei LICENSEKEY einen Lizenzschlüssel für eine Server-Version von openFT angegeben haben.

Wenn Sie keine Lizenz für das FTAM-Protokoll erworben haben, müssen Sie FTAMLICENSEKEY nicht angeben. Das FTAM-Protokoll kann in diesem Fall nicht verwendet werden. Die Eingabe des Lizenzschlüssels für das FTAM-Protokoll ist auch jederzeit nach der Installation mit dem openFT Explorer (*Administration - Lizenzverwaltung*) oder dem Kommando *ftaddlic* möglich.

Der FTAMLICENSEKEY besteht aus fünf Teilschlüsseln, die durch das Minuszeichen getrennt sind und jeweils aus fünf Zeichen bestehen.

Beispiel:

54321-54321-54321-54321-54321

FTPLICENSEKEY:

Die Angabe von FTPLICENSEKEY ist optional.

Für FTPLICENSEKEY ist ein gültiger Lizenzschlüssel für das FTP-Protokoll anzugeben. Die Angabe von FTPLICENSEKEY ist nur dann sinnvoll, wenn Sie bei LICENSEKEY einen Lizenzschlüssel für eine Server-Version von openFT angegeben haben.

Wenn Sie keine Lizenz für das FTP-Protokoll erworben haben, müssen Sie FTPLICENSEKEY nicht angeben. Das FTP-Protokoll kann in diesem Fall nicht verwendet werden. Die Eingabe des Lizenzschlüssels für das FTP-Protokoll ist auch jederzeit nach der Installation mit dem openFT Explorer (*Administration - Lizenzverwaltung*) und dem Kommando *ftaddlic* möglich.

Der FTPLICENSEKEY besteht aus fünf Teilschlüsseln, die durch das Minuszeichen getrennt sind und jeweils aus fünf Zeichen bestehen.

Beispiel:

32154-32154-32154-32154-32154

INSTALLDIR:

Mit dem Parameter INSTALLDIR kann das Installationsverzeichnis von openFT angegeben werden, siehe auch [Abschnitt „Installation von openFT“](#).

Der Parameter INSTALLDIR kann auch beim *PCMX-32.msi* Paket für die bedienerlose CMX-Installation angegeben werden.

Standardmäßig wird openFT in das Verzeichnis *%ProgramFiles%\openFT* installiert.

Sie dürfen bei den Installationspfaden (INSTALLDIR) keine Netzlaufwerkpfade oder UNC-Pfade angeben!

openFT muss auf einer lokalen Festplatte installiert werden.

Die maximale Länge des auswählbaren Installationsverzeichnisses beträgt 110 Zeichen. Wenn Sie ein längeres Installationsverzeichnis angeben, wird die Installation abgelehnt.

Es wird empfohlen, den Parameter INSTALLDIR wegzulassen. Damit wird der Standard-Installationspfad verwendet.

Beispiele

1. Die bedienerlose Installation von CMX ohne Benutzerinteraktion starten Sie mit:

```
msiexec /i PCMX-32.msi /qn
```

2. Die bedienerlose Installation von openFT in deutscher Spracheinstellung in das Standardverzeichnis %
Program Files%\openFT ohne Benutzerinteraktion starten Sie mit

```
msiexec /i openFT.msi
```

3. Zur bedienerlosen Installation ohne Benutzerinteraktion von openFT inkl. SNMP in deutscher Sprache in das Standardverzeichnis geben Sie folgendes Kommando ein:

```
msiexec /i openFT.msi ADDLOCAL=SNMP
```

4. Zur bedienerlosen Installation ohne Benutzerinteraktion von openFT inkl. SNMP in deutscher Sprache in das Standardverzeichnis und Angabe des openFT- und optionalen FTAM-Lizenzschlüssels geben Sie folgendes Kommando ein:

```
msiexec /i openFT.msi ADDLOCAL=SNMP  
LICENSEKEY=12345-12345-12345-12345-12345  
FTAMLICENSEKEY=54321-54321-54321-54321-54321
```

i Bei einer bedienerlosen Installation (z.B. Schalter */qn* oder */qb*) wird der Rechner vom Windows Installer, falls notwendig, automatisch neu gestartet. Dies kann durch das Setzen der Option */norestart* (ab Windows Installer 3.0) bzw. des Parameters *REBOOT=ReallySuppress* verhindert werden.

Bei einer bedienerlosen Installation können Sie über den Exitcode von *msiexec.exe* feststellen, ob die Installation erfolgreich war oder nicht. Dazu starten Sie *msiexec* wie folgt:

```
start /wait msiexec /l*vx install.log /i openFT.msi
ADDLOCAL=SNMP
LICENSEKEY=12345-12345-12345-12345
FTAMLICENSE=54321-54321-54321-54321
/qn /norestart
```

Fragen Sie unmittelbar nach der Beendigung des *msiexec*-Kommandos mit *echo %ERRORLEVEL%* den Exitcode ab:

0

Installation erfolgreich, kein Neustart des Rechners erforderlich

3010

Installation erfolgreich, ein Neustart des Rechners ist zwingend erforderlich

Alle anderen Exitcodes (z.B. 1603) zeigen einen Fehler bei der Installation an, beispielsweise die Angabe eines ungültigen Lizenzschlüssels oder eines ungültigen Installationsverzeichnis.

Im Fehlerfall kann über das optionale Installationsprotokoll *install.log* die Ursache festgestellt werden.

Im obigen Beispiel wurde diese Protokollierung mit der Option */l*vx install.log* des *msiexec*-Kommandos beim Start der Installation eingeschaltet. Am Ende des protokollierten Installationsablaufs ist im Allgemeinen vor der abschließenden Auflistung der Properties die Fehlermeldung mit der Beschreibung des Fehlers zu finden, der zum Abbruch der Installation geführt hat.

Eine detaillierte Beschreibung des *msiexec*-Kommandos mit einer vollständigen Liste der möglichen Exitcodes finden Sie bei Microsoft im Internet.

3.1.5 Installation des SNMP-Subagenten

Um den SNMP-Subagenten von openFT auf Windows-Systemen zu installieren, muss zuerst der SNMP-Dienst von Microsoft installiert werden.

Anschließend können Sie den Subagenten von openFT installieren.

i Über SNMP kann nur eine openFT-Instanz verwaltet werden. Dabei handelt es sich jeweils um diejenige Instanz, die vor dem Start des SNMP-Dienstes mit der Systemumgebungsvariablen OPENFTINSTANCE eingestellt war. Diese Variable ist standardmäßig nicht gesetzt. In diesem Fall wird die Instanz *std* verwaltet.

SNMP-Dienst installieren/aktivieren

Im Folgenden wird die Installation am Beispiel Windows 10 beschrieben. Bei anderen Windows-Systemen kann es Abweichungen geben. Weitere Informationen entnehmen Sie bitte der Windows Dokumentation.

Unter Windows 10 gehen Sie wie folgt vor:

- In der Systemsteuerung den Eintrag *Programme und Funktionen* auswählen.
- Danach die Schaltfläche *Windows-Funktionen aktivieren/deaktivieren* drücken und im folgenden Dialog aus der Komponentenliste *Simple Network Management Protocol (SNMP)* auswählen.
- Nach der Installation muss der SNMP-Dienst konfiguriert werden. Dazu in der Systemsteuerung unter *Verwaltung* den Eintrag *Dienste* auswählen und hier doppelt auf *SNMP-Dienst* klicken. Auf der Karteikarte *Agent* kann unter *Kontakt* der eigene Name und unter *Standort* der Standort angegeben werden. Bei der Karteikarte *Traps* muss nichts eingetragen werden und auf der Karteikarte *Sicherheit* gibt man einen Community String an, der die Funktion eines Passwortes übernimmt. Außerdem müssen noch Zugriffsrechte vergeben werden. Falls später bei openFT nicht nur Einstellungen gelesen, sondern auch geändert werden sollen (beispielsweise um openFT zu starten oder zu beenden), muss als Recht *LESEN SCHREIBEN* ausgewählt werden. Andernfalls reicht *NUR LESEN* aus.

Subagent von openFT installieren

Gehen Sie wie folgt vor:

- In der Systemsteuerung den Eintrag *Software* bzw. *Programme und Funktionen* auswählen.
- Danach das Produkt *openFT V12.1A00* aus der Liste auswählen und auf die Schaltfläche *Ändern* drücken.
- Im Dialog *Anwendungsverwaltung* die Option *Ändern* wählen und auf die Schaltfläche *Weiter >* drücken.
- Im Dialog *Funktionen auswählen* die Funktion *SNMP Agent* auswählen und auf die Schaltfläche *Weiter >* drücken. Nach erneuter Bestätigung wird der SNMP-Subagent von openFT installiert.
Das Verzeichnis *openFT-Installationsverzeichnis\snmp* enthält eine Datei mit dem Namen *openFTMIB.txt*, welche die Management Information Base (MIB) enthält.
- Nach der Installation des SNMP-Subagenten muss der SNMP-Dienst neu gestartet werden.

3.1.6 Ändern und Reparieren von openFT

Eine installierte openFT-Version kann mit den üblichen Windows-Mitteln geändert und repariert werden.

Vor dem Ändern oder Reparieren sollte der openFT Explorer beendet werden. Andernfalls kann es vorkommen, dass der Rechner neu gestartet werden muss, weil bestimmte Dateien nicht ausgetauscht werden konnten.

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

Beim Ändern und Reparieren bleiben alle Einstellungen erhalten.

3.1.7 Deinstallation von openFT, openFT-CR und CMX

Bei der Deinstallation beachten Sie bitte Folgendes:

- Sie können die optionalen Produkte openFT-CR und CMX einzeln und unabhängig von openFT deinstallieren.
- Wenn Sie CMX deinstallieren, dann müssen Sie zuvor den Betrieb mit CMX deaktivieren, z.B. mit dem Kommando *ftmodo -cmx=n*.
- Wenn Sie openFT deinstallieren und außerdem openFT-CR auf dem Rechner installiert ist, dann müssen Sie zuerst openFT-CR deinstallieren.

Die jeweilige Software kann über die *Systemsteuerung* deinstalliert werden. Je nach Betriebssystem wählen Sie *Programme und Funktionen* oder *Programme - Programme und Funktionen*.

3.2 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:

- Benutzerkennwort eingeben (Kommando *ftsetpwd* oder über den openFT Explorer im Menü *Administration*, Befehl *Benutzerkennwort...*)
- Standardeinstellungen überprüfen, siehe [Abschnitt „Standardeinstellungen überprüfen“](#)
- 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 die zugehörige Datei *PCMX-32.msi* auf der Produkt-CD im Verzeichnis *openFT\Unattended_installation*.
- Konfigurationsdaten importieren, siehe [Abschnitt „Konfigurationsdaten importieren“](#)
- automatischen openFT-Start aktivieren/deaktivieren; siehe [Abschnitt „Automatischen openFT-Start aktivieren und deaktivieren“](#)
- Partnerliste aus TNS erzeugen, siehe [Abschnitt „Partnerliste aus TNS erzeugen“](#)
- Fernadministrations-Server konfigurieren
Wenn Sie Ihr System als Fernadministrations-Server einsetzen möchten, müssen Sie diesen konfigurieren, siehe [Abschnitt „Fernadministrations-Server konfigurieren“](#).
- ADM-Trap-Server konfigurieren
Wenn Sie Ihr System als ADM-Trap-Server einsetzen möchten, müssen Sie diesen konfigurieren, siehe [Abschnitt „ADM-Trap-Server konfigurieren“](#).
- TNS-Einträge erstellen
Falls Sie den TNS verwenden, müssen Sie ggf. TNS-Einträge erstellen, siehe [Abschnitt „Transportsystem-Anwendungen in TNS eintragen“](#).

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 „Transportsystem-Anwendungen in TNS eintragen“](#).

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

3.2.1 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 Standardberechtigungsatz ist so eingestellt, dass File Transfer uneingeschränkt möglich ist. Als FTAC-Verwalter sollten Sie daher den Standardberechtigungsatz umgehend dem Schutzbedürfnis des Rechners anpassen (siehe auch [Abschnitt „Berechtigungssätze verwalten“](#)).

Betriebsparameter-Einstellungen

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

```
ftshwo
STARTED PROC-LIM CONN-LIM ADM-CLIM RQ-LIM MAX-RQ-LIFE TU-SIZE CCS-NAME
  YES      2      16      8      2000      30      65535      CP1252
PTN-CHK DYN-PART SEC-LEV FTAC-LOG FT-LOG FT-DIR-LOGADM-LOG USE TNS USE CMX
  STD      ON      B-P-ATTR  ALL      ALL      NONE      ALL      NO      NO
OPENFT-APPL FTAM-APPL FTP-PORT ADM-PORT ADM-CS
*STD      *STD      21      11000      NO
ACTIVE      ACTIVE      ACTIVE      ACTIVE
RSA-PROP RSA-MIN AES-MIN ENC-MAND
2048      0      NONE      NO
HOST-NAME IDENTIFICATION / LOCAL SYSTEM NAME
*NONE      mc011.mynet.local / $FJAM,MC011
FT-ADMIN FTAC-ADMIN
SYSTEM *STD
DEL-LOG ON AT RETPD RECOVERY ADM-TRAP-SERVER
  OFF DAILY 00:00 14 IN+OUT *NONE
TRAP: SS-STATE FT-STATE PART-STATE PART-UNREA RQ-STATE TRANS-SUCC TRANS-FAIL
CONS OFF OFF OFF OFF OFF OFF OFF OFF
ADM OFF OFF 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 Handbuch "openFT (Unix- und Windows-Systeme) - Kommandoschnittstelle".

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 „Eindeutige Instanzidentifikationen“](#).

- 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 -dp=f* auf OFF.

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

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 Handbuch "openFT (Unix- und Windows-Systeme) - Kommandoschnittstelle". Alternativ können Sie auch den openFT Explorer benutzen, indem Sie im Objektfenster *Berechtigungssätze* den Berechtigungssatz *STD anpassen.

3.2.2 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 Eingabeaufforderung 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 Eingabeaufforderung 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*.

3.2.3 Automatischen openFT-Start aktivieren und deaktivieren

Für jede openFT-Instanz, die Sie manuell mit *ftcrei* erzeugen, ist der asynchrone openFT-Server so voreingestellt, dass er nicht automatisch beim Hochfahren des Systems gestartet wird.

Den automatischen Start des asynchronen openFT-Servers können Sie im openFT Explorer unter *Administration - Betriebsparameter - Allgemein* über die Option *Asynchronen Server automatisch starten* aktivieren bzw. deaktivieren.

3.2.4 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:

Rufen Sie das Programm *TNS User interface* auf, wählen im Menü *Datei* den Befehl *TNS-Einträge exportieren* und geben im Dialog TNS-Datei exportieren einen sprechenden Dateinamen an, z.B. *openft.tns*.

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:

```
openFT-Installationsverzeichnis\bin\ftbin\tns2ptn.exe openft.tns > ft_list.bat
```

ft_list.bat ist der frei wählbare Name der Ausgabedatei. *ft_list.bat* 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.bat*) als FT-Verwalter auf der Kommando-Ebene aus.

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.

4 Betrieb

- Betriebsparameter optimieren
- Code-Tabellen verwalten
- Asynchronen openFT-Server starten und beenden
- Betriebsarten einstellen (Windows-Systeme)
 - Ablauf als Dienst unter Systemrechten
 - Ablauf als Dienst unter Benutzerrechten
- Schutzbiteinstellung für neu angelegte Dateien (Unix-Systeme)
- Dateizugriffsrechte für neu angelegte Dateien (Windows- Systeme)
- Dateizugriff unter Benutzerrechten (Unix-Systeme)
- Einbenutzerbetrieb (Unix-Systeme)
 - Umschalten auf Einbenutzerbetrieb
 - Rückkehr zum Mehrbenutzerbetrieb
 - Hinweise zur ftalarm-Funktion im Einbenutzerbetrieb
- Sprachoberfläche wechseln
 - Sprachoberfläche auf Unix-Systemen wechseln
 - Sprachoberfläche auf Windows-Systemen wechseln
- Aufträge administrieren
- Partner administrieren
 - Partnerliste exportieren
- Sicherheit im openFT-Betrieb
 - Authentifizierung
 - Eindeutige Instanzidentifikationen
 - Lokale RSA-Schlüsselpaare erzeugen und verwalten
 - Schlüssel importieren
 - Öffentliche Schlüssel exportieren
 - Schlüssel von Partnersystemen verwalten
 - Schlüssel an Partnersysteme verteilen
 - Erweiterte Absenderüberprüfung
 - Verschlüsselung bei der Dateiübertragung

-
- FT-Betrieb überwachen und steuern
 - Logging von openFT
 - SNMP-Schnittstelle von openFT (Windows)
 - Tätigkeiten nach der Installation
 - openFT-Subagenten auf Windows starten
 - SNMP-Management für openFT (Windows)
 - Messdatenerfassung mit openFT
 - Messdatenerfassung konfigurieren
 - Messdaten anzeigen
 - FTAC-Umgebung verwalten
 - Berechtigungssätze verwalten
 - Berechtigungsprofile verwalten
 - FTAC-Umgebung sichern und übertragen
 - openFT-Instanzen und Cluster-Betrieb
 - Konfigurationsdaten sichern und wiederherstellen
 - FTAM-Besonderheiten auf Unix-/Windows-Systemen
 - Abbildung der Dateizugriffsrechte
 - Outbound-Aufträge
 - Inbound-Aufträge
 - Abbildung von FTAM-Attributen auf das reale Dateisystem
 - Inbound-Abbildung von FTAM-Attributen
 - Inbound-Abbildung des document type
 - Zugangs- und Zugriffsschutz
 - Outbound-Abbildung des document type

4.1 Betriebsparameter optimieren

Speziell für den FT-Verwalter sind die folgenden Vorschläge gedacht, den FT-Betrieb durch Anpassen der Betriebsparameter zu optimieren.

Zum Steuern des openFT-Betriebs gibt es folgende Parameter, die Sie über das Kommando *ftmodo* festlegen können:

- 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.
- Die maximale Verweildauer der Aufträge im Auftragsbuch

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

Die aktuellen Betriebsparameter können Sie auch über den openFT Explorer ansehen und verändern. Dazu öffnen Sie das Dialogfenster *Betriebsparameter* aus dem Menü *Administration*, Registerblätter *Allgemein* und *Optionen*. 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:

i *Unix-Systeme:* Sie können 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.

4.2 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
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
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.
In Unix-Systemen muss der Dateiname zwingend komplett klein geschrieben werden.
- 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
0000000100020003000400050006000700080009000A000B000C000D000E000F
0010001100120013001400150016001700180019001A001B001C001D001E001F
0020002100220023002400250026002700280029002A002B002C002D002E002F
0030003100320033003400350036003700380039003A003B003C003D003E003F
0040004100420043004400450046004700480049004A004B004C004D004E004F
0050005100520053005400550056005700580059005A005B005C005D005E005F
0060006100620063006400650066006700680069006A006B006C006D006E006F
0070007100720073007400750076007700780079007A007B007C007D007E007F
0080008100820083008400850086008700880089008A008B008C008D008E008F
0090009100920093009400950096009700980099009A009B009C009D009E009F
00A000A100A200A320AC00A5016000A7016100A900AA00AB00AC00AD00AE00AF
00B000B100B200B3017D00B500B600B7017E00B900BA00BB01520153017800BF
00C000C100C200C300C400C500C600C700C800C900CA00CB00CC00CD00CE00CF
00D000D100D200D300D400D500D600D700D800D900DA00DB00DC00DD00DE00DF
00E000E100E200E300E400E500E600E700E800E900EA00EB00EC00ED00EE00EF
00F000F100F200F300F400F500F600F700F800F900FA00FB00FC00FD00FE00FF
```

4.3 Asynchronen openFT-Server starten und beenden

Standardmäßig wird der asynchrone openFT-Server beim Systemstart automatisch gestartet (unter Windows-Systemen als Dienst).

Der asynchrone openFT-Server führt asynchrone Outbound-Aufträge aus, bearbeitet Inbound-Aufträge und ermöglicht (nur auf Windows-Systemen) die Nutzung von Berechtigungsprofilen. Ist der asynchrone openFT-Server nicht gestartet, können diese Funktionen nicht genutzt werden.

Asynchronen openFT-Server manuell starten und beenden

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*.

Einstellungen zum automatischen Starten ändern

- Unix-Systeme

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-Startdeaktivieren“](#)).

Hinweis: Auf Solaris erfolgt der automatische Start über SMF.

- Windows-Systeme

Über den openFT Explorer (*Administration/Betriebsparameter...*, Option *Asynchronen Server automatisch starten*) können Sie festlegen, ob beim Start des openFT-Dienstes automatisch auch der asynchrone openFT-Server gestartet werden soll. Bitte beachten Sie, dass standardmäßig die Option für das automatische Starten des asynchronen openFT-Servers nur bei der Instanz *std* aktiviert ist.

4.4 Betriebsarten einstellen (Windows-Systeme)

Der openFT-Dienst kann unter Benutzerrechten oder unter Systemrechten ablaufen. Standardmäßig wird der Dienst unter Systemrechten gestartet.

4.4.1 Ablauf als Dienst unter Systemrechten

Dieser Betriebsmodus ist die Standardeinstellung und empfiehlt sich, wenn auf einem System mehrere Benutzer arbeiten und ein echter Mehrbenutzerbetrieb erforderlich ist, z.B. auf einem zentralen Windows-Server. Die Beibehaltung dieser Standardeinstellung wird empfohlen.

Merkmale

- Der Dienst wird automatisch beim Start des Betriebssystems gestartet, sofern dies nicht explizit per Administration ausgeschaltet wurde.
- Der Zugriff auf das Dateisystem und auf Dateien im Netz erfolgt ausschließlich unter den Rechten des jeweiligen Benutzers, d.h.:
 - für Inbound-Aufträge (Aufträge mit Initiative im Partnersystem) ist dies der Eigentümer des FTAC-Profiles bzw. der Initiator des Auftrags, der sich durch *Kennung*, *Kennwort* ausgewiesen hat.
 - für Outbound-Aufträge ist dies der Benutzer, der den Auftrag lokal gestellt hat.

Dazu muss der Dienst bei bestimmten Aktionen in die Identität des Benutzers wechseln. Er benötigt dazu das Logon-Kennwort des jeweiligen Benutzers, das ihm im openFT Explorer über *Administration - Benutzerkennwort* bzw. mit Hilfe des Kommandos *ftsetpwd* mitgeteilt werden muss. Das Kennwort muss in folgenden Fällen hinterlegt werden:

- bei asynchronem Zugriff auf NTFS-Dateien oder UNC-Namen
- wenn bei Inbound-Aufträgen mit FTAC-Profilen gearbeitet werden soll
- bei lokaler und ferner Vor-, Nach- und Folgeverarbeitung
- bei Zugriff auf Dateien über UNC-Namen.
- Relative Pfadangaben bei Inbound-Aufträgen beziehen sich auf das benutzerspezifische Home-Verzeichnis. Dieses kann vom System- oder Domänen-Administrator in der Benutzerverwaltung von Windows festgelegt werden.
- Als Home-Verzeichnis für relativ angegebene Pfade gilt das im Benutzermanager für den entsprechenden Benutzer festgelegte Home-Verzeichnis. Falls keines angegeben ist, legt openFT das Home-Verzeichnis an, z.B. auf Windows 10 unter *Benutzer/Benutzerkennung.Rechnername* bzw. *Benutzerkennung.Domäne*.

4.4.2 Ablauf als Dienst unter Benutzerrechten

Beim Betrieb des openFT-Diensts unter Benutzerrechten wird der openFT-Dienst unter den Rechten eines definierten Benutzers gestartet. Der Benutzer **muss** jedoch Administrationsrechte besitzen. Beim Betrieb unter Benutzerrechten ist zu beachten, dass der asynchrone openFT-Server nur Aufträge für den Benutzer bearbeitet, unter dessen Rechten er gestartet wurde.

Dieser Betriebsmodus kann sinnvoll sein,

- wenn nur **ein** Benutzer auf dem System arbeitet und ein echter Mehrbenutzerbetrieb deshalb nicht erforderlich ist bzw.
- für automatisierte Verfahren, da dort in der Regel auch die Mehrbenutzerfunktionalität nicht benötigt wird.

Als Windows-Administrator stellen Sie den Benutzer wie folgt ein (Windows 10):

1. Wählen Sie *Systemsteuerung - Verwaltung - Dienste* und markieren den Dienst *openFT*.
2. Wählen Sie im Kontextmenü *Eigenschaften*.
Die Registerkarte *Anmelden* wird angezeigt.

In dem nun geöffneten Fenster wählen Sie *Anmelden als .. Dieses Konto*: und geben den Benutzernamen und das Kennwort des Benutzers ein, unter dessen Rechten der Dienst gestartet werden soll.

Soll der Dienst wieder unter Systemrechten laufen, so wählen Sie *Lokales Systemkonto*.

Merkmale

- Der Dienst wird automatisch beim Start des Betriebssystems gestartet, sofern dies nicht explizit per Administration ausgeschaltet wurde.
- Zugriff auf das Dateisystem mit den Rechten des jeweiligen Benutzers unter dem der Dienst läuft, d.h. der FT-Server kann ebenfalls nur auf die Dateien zugreifen, auf die auch der Benutzer selbst Zugriff hat. Somit ist ein Zugriff auf Dateien im Netz über UNC-Namen möglich, falls der Benutzer selbst darauf Zugriff hat.
- Als Zugangsberechtigung können alle FTAC-Profilen des Benutzers verwendet werden, unter dessen Rechten der Dienst läuft. Alternativ wird auch die Kombination *Kennung*,,*Kennwort* des Benutzers, unter dessen Rechten der Dienst läuft, als Zugangsberechtigung akzeptiert. Zugangsberechtigungen oder Kennungen anderer Benutzer werden nicht akzeptiert.
- Das Hinterlegen des Kennwortes über den openFT Explorer (*Administration - Benutzerkennwort*) ist nicht mehr nötig, damit FTAC-Profilen funktionieren, bei asynchronen Outbound-Aufträgen auf NTFS-Dateien zugegriffen werden kann und Folgeverarbeitung (lokale (outbound) oder ferne (inbound)) funktioniert.
Der Menüpunkt im openFT Explorer ist aber weiterhin vorhanden, um jederzeit in den anderen Betriebsmodus (Dienst läuft unter System-Rechten) wechseln zu können.
- Als Home-Verzeichnis für relativ angegebene Pfade gilt das im Benutzermanager für den entsprechenden Benutzer festgelegte Home-Verzeichnis. Falls keines angegeben ist, legt openFT z.B. unter Windows 10 unter *Benutzer* das Verzeichnis *Benutzerkennung.Rechnername* bzw. *Benutzerkennung.Domäne* an.

4.5 Schutzbiteinstellung für neu angelegte Dateien (Unix-Systeme)

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 Einstellungen mit dem Kommando:

```
svcadm refresh openFT:std
```

4. Starten Sie openFT mit dem Kommando *ftstart*.

5. Sie können sich die Einstellungen anzeigen lassen, indem Sie das Kommando *svccprop* eingeben (hier für die Standardinstanz):

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

Ausgabe:

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

i Ab Version openFT V12.1B wird die Plattform Solaris nur noch auf Anfrage unterstützt.

4.6 Dateizugriffsrechte für neu angelegte Dateien (Windows- Systeme)

Die Dateizugriffsrechte für neu angelegte Dateien legen Sie über den openFT Explorer fest. Dazu wählen Sie im Menü *Administration* den Befehl *Dateizugriffsrechte...* und legen im Dialogfenster *Dateizugriffsrechte* fest, ob eine empfangene Datei mit den Standardrechten des Verzeichnisses erstellt wird oder mit Vollzugriff für denjenigen, der die Datei erzeugt hat. Diese Angabe ist nur für NTFS-Dateisysteme relevant.

Im Inbound-Fall wird hier der Eigentümer des verwendeten Profils oder die vom Initiator explizit angegebene Benutzerkennung herangezogen.

Nach der Änderung müssen Sie den asynchronen openFT-Server neu starten.

4.7 Dateizugriff unter Benutzerrechten (Unix-Systeme)

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.

4.8 Einbenutzerbetrieb (Unix-Systeme)

openFT läuft auf Unix-Plattformen standardmäßig im Mehrbenutzerbetrieb unter privilegierter Kennung (*root*) und wechselt jeweils dann temporär in die Rolle eines Benutzers, wenn für diesen Benutzer openFT-Funktionen ausgeführt werden sollen.

Zum Umschalten vom Mehrbenutzer- in den Einbenutzerbetrieb und umgekehrt verwenden Sie das Kommando *ftsetmode*. *ftsetmode* sollten Sie nicht im laufenden Betrieb aufrufen, denn *ftsetmode* beendet die openFT-Aktivitäten in allen aktiven Instanzen (z.B. den openFT Explorer, *ftscript*-Aufträge oder *ftexec*- und *ncopy*-Kommandos).

i Ist bereits ein openFT V12.0 installiert und läuft openFT im Einbenutzerbetrieb, bleibt bei einer erneuten Installation von openFT V12.0 der Einbenutzerbetrieb erhalten.

4.8.1 Umschalten auf Einbenutzerbetrieb

Rufen Sie unter *root* folgendes Kommando auf (hier für die Kennung *user1*):

```
ftsetmode -s -ua=user1
```

openFT läuft danach vollständig unter dieser Kennung, der sogenannten openFT-Kennung. D.h. alle Instanzen (Standard-Instanz und alle weiteren aktiven Instanzen) werden der openFT-Kennung zugeordnet. Dabei gilt:

- Andere Kennungen als die openFT-Kennung haben keinen Zugriff auf Funktionen der entsprechenden openFT-Instanz (Ausnahmen: *ftcrei*, *ftdeli*, *ftmodi*). Aufrufe der openFT-Kommandos von nicht zugelassenen Kennungen aus werden abgewiesen.
- Auf Inbound-Seite kann nur über FTAC-Profile auf die openFT-Instanz zugegriffen werden, die der openFT-Kennung gehören und in denen kein explizites Benutzerkennwort spezifiziert ist.
- Berechtigungssätze und Berechtigungsprofile für fremde Kennungen sind unwirksam, bleiben aber bestehen.
- Zugriffe mit der Angabe von Benutzerkennung und Benutzerkennwort sind nicht möglich.

Administrationsrechte im Einbenutzerbetrieb

Nach dem Umschalten in den Einbenutzerbetrieb sind die Administrationsrechte (FT-, FTAC- und ADM-Verwalter) wie folgt zugeordnet:

- Die openFT-Kennung wird FT-Verwalter mit folgender Ausnahme: Das Einrichten, Löschen und Modifizieren von openFT-Instanzen ist in der openFT-Kennung nicht möglich.
- Die openFT-Kennung wird FTAC-Verwalter, d.h. bestehende Profile für andere Kennungen können gelöscht und auch modifiziert werden, sofern die Modifikation sich nicht auf die Benutzerkennung bezieht. Im Berechtigungssatz der openFT-Kennung werden die Grenzwerte für Administrator und Benutzer bei einem *ftmoda*-Aufruf simultan geändert.
- War die openFT-Kennung vor dem Umschalten ADM-Verwalter, dann bleibt sie ADM-Verwalter.
- War eine andere Kennung ADM-Verwalter, dann wird das Recht zurückgegeben (d.h. es ist kein ADM-Verwalter zugeordnet). Die openFT-Kennung kann sich dieses Recht anschließend selbst geben (*ftmoda -admpriv=y*), da sie FTAC-Verwalter ist. Dadurch kann die openFT-Instanz im Einbenutzerbetrieb als zentraler Administrationsserver arbeiten.

openFT-Instanzen im Einbenutzerbetrieb

Im Einbenutzerbetrieb gibt es folgende Besonderheiten:

- Die Instanzen-Kommandos *ftcrei* (Anlegen und Reaktivieren), *ftdeli* (Deaktivieren) und *ftmodi* (Modifizieren) sind nur unter *root* erlaubt. Das bedeutet im Einzelnen:
 - Beim Anlegen und beim Modifizieren muss immer eine Benutzerkennung angegeben werden. Damit kann *root* für beliebige Benutzerkennungen Instanzen anlegen oder vorhandene Instanzen beliebigen Kennungen zuordnen.
 - Wird eine openFT-Instanz einer anderen Benutzerkennung zugeordnet (per *ftmodi*), dann wird der neue Eigentümer der Instanz auch FTAC-Verwalter der Instanz. Wenn der bisherige Eigentümer der Instanz das ADM-Verwalterrecht besessen hat, so wird dieses auf den neuen Eigentümer übertragen.
- Die Instanzen-Kommandos *ftseti* (Einstellen) und *ftupdi* (Aktualisieren) sind nur dem Eigentümer der Instanz erlaubt.

Einbenutzerbetrieb unter Solaris

i Ab Version openFT V12.1B wird die Plattform Solaris nur noch auf Anfrage unterstützt.

Im Einbenutzerbetrieb werden die im SMF aktivierten (enabled) openFT-Instanzen „transient“ für die entsprechende openFT-Kennung gestartet. „Transient“ bedeutet, dass die openFT Instanzen im Einbenutzerbetrieb nicht von SMF überwacht werden.

Die openFT-Kennung kann im Einbenutzerbetrieb mit den Kommandos *ftstart* und *ftstop* die openFT Instanz nach Belieben starten oder stoppen. Die Einstellungen im SMF bleiben unverändert, siehe [Abschnitt „Solaris SMF“](#).

4.8.2 Rückkehr zum Mehrbenutzerbetrieb

Rufen Sie unter *root* folgendes Kommando auf:

```
ftsetmode -m
```

Für jede aktive Instanz einschließlich der Standardinstanz gilt:

- FT- und FTAC-Verwalter werden auf *root* gesetzt. Wenn die openFT-Kennung im Einbenutzerbetrieb ADM-Verwalter war, wird das ADM-Verwaltungsrecht zurückgegeben.
- Berechtigungssätze und Berechtigungsprofile für fremde Kennungen werden bei der Rückkehr in den Mehrbenutzerbetrieb erneut „aktiv“.
- Nach dem Umschalten wird openFT für die Instanzen wieder gestartet, für die er vor dem Umschalten gestartet war.

Reaktivieren einer benutzerspezifischen Instanz im Mehrbenutzerbetrieb

Benutzerspezifische Instanz bedeutet, dass eine Instanz im Einbenutzerbetrieb für eine Kennung ungleich *root* neu erzeugt oder einer anderen Kennung ungleich *root* zugeordnet wurde.

Wird eine benutzerspezifische Instanz im Mehrbenutzerbetrieb reaktiviert (*ftcrei*), dann wird *root* zum FT- und FTAC-Verwalter dieser Instanz gemacht. Falls der bisherige Eigentümer ADM-Verwalter war, dieses Recht auf *root* übertragen.

4.8.3 Hinweise zur *ftalarm*-Funktion im Einbenutzerbetrieb

Deaktivieren Sie die *ftalarm*-Funktion mit *ftalarm -t*, bevor Sie zwischen Einbenutzerbetrieb und Mehrbenutzerbetrieb wechseln oder im Einbenutzerbetrieb eine openFT-Instanz einer anderen Benutzerkennung zuweisen. Der Grund: Nach dem Wechsel wäre die *ftalarm*-Funktion zwar noch in der *cron*-Funktion eingehängt, aber nicht mehr wirksam.

ftalarm -t können Sie aus jeder beliebigen Benutzerkennung aufrufen. Dadurch ist es möglich, auch unwirksame oder unwirksam gewordene *ftalarm*-Einträge aus der *cron*-Funktion zu entfernen.

Mit *ftalarm -i* können Sie prüfen, ob für den aufrufenden Benutzer und die eingestellte openFT-Instanz die *ftalarm*-Funktion aktiviert ist.

4.9 Sprachoberfläche wechseln

Auf Unix- und Windows-Systemen kann die Spracheoberfläche zwischen Deutsch und Englisch gewechselt werden.

4.9.1 Sprachoberfläche auf Unix-Systemen 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. 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-Variablen).
- 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.

4.9.2 Sprachoberfläche auf Windows-Systemen wechseln

Die Standardsprache von openFT wird bei der Installation voreingestellt:

- Bei der bedienergeführten Installation: Ist im Betriebssystem *Deutsch* oder *Englisch* als Sprache eingestellt, wird diese Sprache bei der Installation als Standardsprache für openFT übernommen. Für alle anderen Systemsprachen wird abgefragt, ob *Deutsch* oder *Englisch* als Standardsprache für openFT voreingestellt werden soll.
- Bei der bedienerlosen Installation: openFT wird mit der Sprachoberfläche *Deutsch* installiert, wenn Sie für den Windows Installer den Parameter *TRANSFORMS=:de* angeben. Sonst wird openFT mit der Sprachoberfläche *Englisch* installiert.

Die Spracheinstellung lässt sich wie folgt ändern:

- Über die Systemsteuerung (bei Windows 10 z.B. Unterpunkt *Region und Sprache*) kann der Anwender die Spracheinstellung ändern. Diese Änderung gilt dann auch für andere Programme.
- Mit der Umgebungsvariable OPENFTLANG kann jeder Benutzer seine Spracheinstellung ändern.
 - > Rufen Sie dazu die Windows-Systemsteuerung auf.
 - > Wählen Sie *System und Sicherheit - System - Erweiterte Systemeinstellungen*.
 - > Klicken Sie im folgenden Dialog auf die Schaltfläche *Umgebungsvariablen*.
 - > Setzen Sie bei den Benutzervariablen die Variable OPENFTLANG auf *de* bzw. *en*.

Die folgende Tabelle zeigt, wie das Setzen bzw. Nichtsetzen von OPENFTLANG und die per Systemsteuerung gesetzte Spracheinstellung wirkt:

OPENFTLANG	Spracheinstellung	Resultat
nicht gesetzt, leer oder ungültiger Wert	nicht unterstützte Sprache	bei der Installation verwendete Sprache
nicht gesetzt, leer oder ungültiger Wert	unterstützte Sprache (<i>Deutsch</i> oder <i>Englisch</i>)	mit der Spracheinstellung gesetzte Sprache
gültiger Wert (<i>de</i> oder <i>en</i>)	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 Windows-Eingabeaufforderung neu aufgerufen wird. War ein Programm vor der Umstellung aktiv, müssen Sie es zuerst beenden und dann neu starten.

4.10 Aufträge administrieren

Im Auftragsbuch werden alle asynchronen Outbound-Aufträge sowie alle Inbound-Aufträge gespeichert.

Zur Administration von Aufträgen bietet openFT dem FT-Verwalter folgende Kommandos:

- *ftshwr*: sich über alle noch nicht abgeschlossenen asynchronen Aufträge auf Ihrem Rechner informieren. Dazu gehört auch das Recht, Informationen über Aufträge aller Benutzer abzufragen.
- *ftmodr*: die Bearbeitungsreihenfolge aller Aufträge Ihres Rechners *ändern*, auch von Aufträgen anderer Benutzer.
- *ftcanr*: asynchrone Aufträge Ihres Rechners *löschen*, auch die anderer Benutzer.

Sie können Aufträge auch über den openFT Explorer administrieren, indem Sie auf das Objektverzeichnis *Auftragsbuch* klicken. Dort können Sie asynchrone Aufträge löschen, das Auftragsbuch aktualisieren, Prioritäten für Aufträge verändern und 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.

4.11 Partner administrieren

Partnersysteme können nur dann administriert werden, wenn sie in der Partnerliste eingetragen sind. Dazu haben Sie zwei Möglichkeiten:

- Sie tragen den Partner mit Name und Adresse ein (benannter Partner).
- Sie tragen den Partner nur mit Adresse aber ohne Namen ein (eingetragener dynamische Partner). In diesem Fall sind einige Details zu beachten, siehe [Abschnitt „Partner administrieren“](#).

D.h. freie dynamische Partner (Partner, die nicht in der Partnerliste eingetragen sind) können nicht administriert werden. Mehr Informationen zum Partnerkonzept finden Sie im openFT-Handbuch "Konzepte und Funktionen".

Für Sonderfälle steht der **Transport Name Service** (TNS) zur Verfügung, siehe Abschnitt [Transport Name Service](#).

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.

Zur Administration von Partnern bietet openFT dem FT-Verwalter folgende Kommandos:

- *ftaddptn*: Neuen Partner in die Partnerliste eintragen und Eigenschaften des Partners festlegen.
- *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.
- *ftmodo*: Globale FTAC-Sicherheitsstufe festlegen (Option *-s*) und dynamische Partner aktivieren/deaktivieren (Option *-dp*).

Der Aufbau der Partneradressen ist im Handbuch "openFT (Unix- und Windows-Systeme) - Kommandoschnittstelle" erklärt.

Alternativ können Sie auch dem openFT Explorer verwenden, z.B.:

- 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 Kontextmenü-Befehle im Objektfenster *Partnerliste* können Sie neue Partner eintragen, Partner entfernen und die Eigenschaften von Partnern ändern.
- Globale Eigenschaften legen Sie fest mit dem Menü *Administration*, Befehl *Betriebsparameter*, Registerblatt *Optionen*.

i Zusätzlich gibt es im openFT Explorer das Objektverzeichnis *Partner*, in dem der jeweilige Benutzer seine bevorzugten Kopplungspartner einrichten kann.

Weitere Einzelheiten finden Sie in der Online-Hilfe.

Eingetragene dynamische Partner

Eingetragene dynamische Partner sind alle Partner, die nur mit Adresse, aber ohne Namen in der Partnerliste eingetragen sind. 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, dass *-s/=* ohne Parameter (Standardeinstellung des Kommandos *ftaddptn*) ein abweichendes Attribut ist, nicht aber *-s/=p* (Standardeinstellung für freie dynamische Partner).

Wenn Sie dynamische Partner aus der Partnerliste löschen möchten, müssen Sie alle Attribute des Partners mit *ftmodptn* auf die Standardwerte zurücksetzen.

Transport Name Service

Details sind im [Abschnitt „Transportsystem-Anwendungen in TNS eintragen“](#) beschrieben.

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

- CMX muss installiert sein da CMX den TNS und Funktionen für den Zugriff auf den TNS zur Verfügung stellt.
- Sie müssen CMX und TNS in den Betriebsparametern explizit aktivieren. Dazu geben Sie entweder das Kommando *ftmodo -cmx=y -tns=y* ein oder aktivieren beide Funktionen über den openFT Explorer (Betriebsparameter-Optionen *TNS benutzen* und *CMX benutzen*).

Auf Windows-Systemen ist TNS im openFT Explorer über *Administration - Partner TNS Adressen* erreichbar.

4.11.1 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 (Unix-Systeme)

- 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
```

Beispiele (Windows-Systeme)

- Sichern der Partnerliste im Format für Windows-Systeme in die Datei *ftpartner.bat*:

```
ftshwptn -pw > ftpartner.bat
```

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

```
cmd /c ftpartner.bat
```

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

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

4.12 Sicherheit im openFT-Betrieb

Weitergehenden Schutz beim File Transfer bieten die folgenden Funktionen:

- [Authentifizierung](#)
- [Erweiterte Absenderüberprüfung](#)
(falls z.B. nicht mit Authentifizierung gearbeitet werden kann)
- [Verschlüsselung bei der Dateiübertragung](#)

Hinweis

- Beim Übertragungsauftrag kann zusätzlich eine Integritätsprüfung angefordert werden, falls nicht mit Verschlüsselung gearbeitet wird (*ft/ncopy -di*).
- 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. Für die Verschlüsselung stellt der Secure-FTP-Server der openFT-Instanz seinen Schlüssel und das Zertifikat zur Verfügung. Eine gegenseitige Authentifizierung findet nicht statt.

4.12.1 Authentifizierung

Wenn mit Authentifizierung gearbeitet wird, spielen folgende Themen eine besondere Rolle:

- Eindeutige Instanzidentifikationen
- Lokale RSA-Schlüsselpaare erzeugen und verwalten
- Schlüssel importieren
- Öffentliche Schlüssel exportieren
- Schlüssel von Partnersystemen verwalten
- Schlüssel an Partnersysteme verteilen

4.12.1.1 Eindeutige Instanzidentifikationen

Für die Authentifizierung ist es notwendig, dass die Instanzidentifikation netzweit eindeutig ist.

Lokale Instanzidentifikation

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 mit dem Kommando *ftmodo -id* ändern. Im openFT Explorer verwenden Sie Menü *Administration*, Befehl *Betriebsparameter*, Registerblatt *Allgemein*, Parameter *Identifikation*.

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 *hosts*-Datei (an Unix-Systemen */etc/hosts*) oder im TNS vorzunehmen. Bei einem Eintrag im TNS muss der Globale Name dann mit der Instanzidentifikation des Partners übereinstimmen.

4.12.1.2 Lokale RSA-Schlüsselpaare erzeugen und verwalten

Bei der Neuinstallation von openFT wird ein RSA-Schlüsselpaarsatz erzeugt, bestehend aus privaten und öffentlichen Schlüsseln passender Länge.

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

- Mit *ftcrek* erzeugen Sie für die lokale openFT-Instanz einen RSA-Schlüsselpaarsatz.
- 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 Unix- oder Windows-System besteht aus fünf Schlüsselpaaren mit den Längen 768, 1024, 2048, 3072 und 4096 Bit. Bis einschließlich openFT Version 12.1C10 bestand ein RSA-Schlüsselpaarsatz im Unix- oder Windows-System nur aus drei Schlüsselpaaren mit den Längen 768, 1024 und 2048.

Private Schlüssel werden von openFT intern verwaltet. Öffentliche Schlüssel werden im Verzeichnis *config* des Instanzdateibaums (siehe [Abschnitt „Installation von openFT“](#) (Unix-Systeme) bzw. [Abschnitt „Installation von openFT“](#) (Windows-Systeme)) 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:

- 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.

4.12.1.3 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 [Abschnitt „Lokale RSA-Schlüsselpaare erzeugen und verwalten“](#). 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“](#).

Jedes importierte Schlüsselpaar erhält eine eindeutige Referenznummer. Importiert werden RSA-Schlüssel in den unterstützten Schlüssellängen (768, 1024, 2048, 3072 und 4096 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.

4.12.1.4 Öffentliche Schlüssel exportieren

Mit dem openFT Explorer können Sie öffentliche Schlüssel der lokalen Instanz exportieren und damit Partnern die zur Authentifizierung der eigenen Instanz erforderlichen Schlüssel zur Verfügung stellen (Menü *Administration - Schlüsselverwaltung*). Details siehe Online-Hilfe.

4.12.1.5 Schlüssel von Partnersystemen verwalten

Die öffentlichen Schlüssel der Partnersysteme müssen als Dateien im Verzeichnis *syskey* des Instanzdateibaums der lokalen openFT-Instanz hinterlegt werden, siehe [Abschnitt „Installation von openFT“](#) (Unix-Systeme) bzw. [Abschnitt „Installation von openFT“](#) (Windows-Systeme). 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.
An Unix-Systemen darf der Dateiname 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 [Abschnitt „FT-Betriebüberwachen und steuern“](#).

Schlüsseleigenschaften von Partnersystemen modifizieren

Sie können mit dem Kommando *ftmodk* die Schlüsseleigenschaften von Partnersystemen modifizieren, indem Sie ein Verfallsdatum (Option *-exp*) festlegen oder die Authentifizierungsstufe (1 oder 2, Option *-a*) 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.

4.12.1.6 Schlüssel an Partnersysteme verteilen

Öffentliche Schlüssel werden im Verzeichnis *config* des Instanzdateibaums der lokalen openFT-Instanz abgespeichert, siehe [Abschnitt „Installation von openFT“](#) (Unix-Systeme) bzw. [Abschnitt „Installation von openFT“](#) (Windows-Systeme).

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 anderem Betriebssystem (z.B. BS2000) übermitteln.

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

- Bei Partnern mit openFT (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 (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 (Windows) im Verzeichnis *syskey* des Instanzdateibaums. Bei der Standardinstanz lautet der Pfadname auf Windows 10 *%ProgramData%\Fujitsu Technology Solutions\openFT\var\std\syskey*. Als Dateiname muss die Instanzidentifikation Ihrer lokalen openFT-Instanz gewählt werden.
- Bei Partnern mit openFT (z/OS) 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.

4.12.2 Erweiterte Absenderüberprüfung

Erweiterte Absenderüberprüfung bedeutet:

- Für openFT-Partner, dass openFT nicht nur die Instanzidentifikation, sondern zusätzlich auch die Transportadresse überprüft.
- Für FTAM-Partner, dass der Calling Application Entity Title und die Transportadresse überprüft wird. Dazu muss sich der Partner mit einem Calling Application Entity Title identifizieren, der nicht dem nil AP-Title entspricht. FTAM-Partner werden standardmäßig über ihre Absenderadresse identifiziert.

Die erweiterte Absenderüberprüfung kann wie folgt gesteuert werden:

- global für openFT- und FTAM-Partner mit *ftmodo*, Option *-ptc* (siehe Tabelle) oder im openFT Explorer mit *Betriebsparameter - Allgemein, Partnerüberprüfung*

ftmodo	openFT-Partner	FTAM-Partner
<i>-ptc=i</i>	Instanzidentifikation	Transportadresse
<i>-ptc=a</i>	Instanzidentifikation + Transportadresse	Transportadresse
<i>-ptc=t</i>	Instanzidentifikation	AET
<i>-ptc=b</i>	Instanzidentifikation + Transportadresse	AET + Transportadresse

Für openFT-Partner gilt die globale Einstellung gilt für alle Partner, bei denen die Partnerüberprüfung auf Standard gesetzt ist (Ausgabe FTOPT bei *ftshwptn*) und die nicht mit Authentifizierung arbeiten.

- partnerspezifisch für openFT-Partner mit *ftaddptn / fmodptn -ptc=a* (ein) oder *-ptc=i* (aus) oder im openFT Explorer im Dialog *Partnerlisteneintrag* Abschnitt *Partnerüberprüfung*

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

4.12.3 Verschlüsselung bei der Dateiübertragung

Voraussetzungen für die Verschlüsselung von Dateiinhalten:

- Für openFT Versionen \leq V12.1B:
openFT-CR V12.0 muss sowohl lokal als auch auf dem Partnersystem installiert sein. openFT-CR ist aus rechtlichen Gründen nicht in allen Staaten verfügbar.
- Im lokalen System muss ein RSA-Schlüsselpaarsatz existieren und die Verschlüsselung darf nicht ausgeschaltet sein (durch Angabe von *ftmodo -kl=0* wird die Verschlüsselung ausgeschaltet).
Mit dem Kommando *ftshwo* können Sie dies überprüfen. Der Ausgabeparameter RSA-PROP zeigt die Länge des aktuell verwendeten RSA-Schlüssels in Bit an (0, 768, 1024, 2048, 3072 oder 4096). 0 bedeutet, dass die Verschlüsselung ausgeschaltet ist.

Sie können die gewünschte Länge des RSA-Schlüssels sowie der RSA-Mindestschlüssellänge per Betriebsparameter einstellen. Zusätzlich können Sie eine AES-Mindestschlüssellänge einstellen.

Verwenden Sie dazu folgende Optionen:

- Optionen *-kl* (gewünschte RSA-Schlüssellänge) und *-klmin* (Mindestlänge des RSA-Schlüssels) im Kommando *ftmodo* oder den openFT Explorer (Menü *Administration*, Befehl *Betriebsparameter*). Die Standardwerte nach Neuinstallation sind 2048 (*-kl*) und 0 (*-klmin*).
- Option *-aesmin* (Mindestlänge des AES-Schlüssels) im Kommando *ftmodo* oder den openFT Explorer (Menü *Administration*, Befehl *Betriebsparameter*). Der Standardwert nach Neuinstallation ist *-aesmin=* (keine minimale AES-Schlüssellänge festgelegt).

Weitere Details zu lokalen Schlüsseln finden Sie in [Abschnitt „Lokale RSA-Schlüsselpaareerzeugen und verwalten“](#).

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.

4.13 FT-Betrieb überwachen und steuern

Sie können den openFT-Betrieb überwachen und steuern durch:

- [Logging von openFT](#)
- [SNMP-Schnittstelle von openFT \(Windows\)](#)
- [Messdatenerfassung mit openFT](#)

4.13.1 Logging von openFT

Die Logging-Sätze werden in der Datei *syslog.Lyymmdd.Lhmmss* abgelegt, die sich im Verzeichnis *log* der jeweiligen openFT-Instanz befindet. *yymmdd* ist das Datum (Jahr, Monat, Tag) und *hmmss* ist die Uhrzeit Stunde, Minute, Sekunde für GMT), zu der die Datei angelegt wurde.

Logging-Sätze ansehen

Sie können sich mit dem Kommando *ftshwl* alle Logging-Sätze im System anschauen. Mit den Polling-Optionen *-po* und *-pnr* 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 entweder 0000 (positiver Bestätigung) oder die Ursache für die Ablehnung oder den Abbruch eines Auftrags steht. Die Bedeutung des Reason-Codes können Sie mit dem Kommando *ftshelp* ermitteln.

Alternative im openFT Explorer: Klicken Sie im Navigationsbereich unter *Administration* auf *Logging*.

Logging-Datei umschalten und Offline-Logging verwalten

Sie schalten die Logging-Datei um mit dem Kommando *ftmodo -lf=c* oder über den openFT Explorer im Registerblatt *Logging* unter *Administration - Betriebsparameter*.

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.

Mit dem *ftshwl -llf* können Sie sich die Namen aller Logging-Dateien anzeigen lassen (aktuelle Logging-Datei und Offline-Logging-Dateien).

Im openFT Explorer sehen Sie auch alle Offline-Logging-Dateien und deren Logging-Sätze (Teilbaum *Administration - Logging - Offline-Logging*).

Logging-Einstellungen ändern

Sie können folgende Logging-Einstellungen ändern:

- Den Umfang der Logging-Funktion (FT-, FTAC- und Administrationsfunktion sowie das Logging für die Verzeichnisübertragung). Dazu verwenden Sie das Kommando *ftmodo* (Optionen *-lt*, *-lc*, *-la* und *-ltd* (Verzeichniübertragung)).

Nach der Installation ist das Logging in vollem Umfang eingeschaltet.

- Die Intervalle für das automatische Löschen von Logging-Sätzen. Dazu verwenden Sie das Kommando *ftmodo* (Option *-ld*, *-lda*, *-ldd* und *-ldt*).

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.

Im openFT Explorer verwenden Sie das Registerblatt *Logging* unter *Administration - Betriebsparameter*.

Logging-Sätze löschen und Logging-Sätze in Datei sichern

Als FT-Verwalter, FTAC-Verwalter oder ADM-Verwalter dürfen Sie alle Logging-Sätze löschen. Dazu verwenden Sie das Kommando *ftdell*. oder den openFT Explorer (Logging-Objektfenster, Kontextmenü-Befehl *Logging-Sätze löschen*). Beim Löschen von Logging-Sätzen ändert sich die Größe der Datei, da der Speicherplatz beim Löschen sofort freigegeben wird.

Logging-Sätze sichern

Leiten Sie die Ausgabe von *ftshwl* wie folgt in eine Datei um:

- 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.

4.13.2 SNMP-Schnittstelle von openFT (Windows)

Voraussetzungen

An Windows-Systemen muss der SNMP-Dienst von Microsoft vorhanden sein. Den SNMP-Subagenten von openFT müssen Sie explizit installieren, siehe [Abschnitt „Installation desSNMP-Subagenten“](#).

i SNMP wird auf Unix-Systemen nicht mehr unterstützt.

4.13.2.1 Tätigkeiten nach der Installation

Nach der Installation von openFT sind folgende 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 NUR LESEN (Windows-Systeme) vergeben, können über SNMP nur Informationen ausgegeben werden. Das Ändern von Werten (auch Starten bzw. Stoppen) ist dann nicht möglich (siehe auch [Abschnitt „SNMP-Management für openFT \(Windows\)“](#)).
Näheres finden Sie im [Abschnitt „Installation des SNMP-Subagenten“](#).
2. Starten Sie den Agenten (siehe unten).

i Die Tätigkeiten des SNMP-Administrators müssen der Dokumentation der eingesetzten Management-Station entnommen werden.
Die Sicherheitsmechanismen entnehmen Sie bitte ebenfalls Ihrer SNMP-Dokumentation.

4.13.2.2 openFT-Subagenten auf Windows starten

Bei der Installation der openFT-SNMP-Funktion wird der openFT-Subagent beim SNMP-Dienst registriert. Um den openFT-Subagent zu starten, müssen Sie nach der Installation einmalig den SNMP-Dienst stoppen und neu starten. Danach wird der openFT-Subagent bei jedem Start des SNMP-Dienstes automatisch gestartet.

i 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“](#)).

4.13.2.3 SNMP-Management für openFT (Windows)

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:

- `openFT-installation-directory\snmp\openFTMIB.txt`

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

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	1	der asynchrone openFT-Server wird gestartet
stop	2	der asynchrone openFT-Server wird gestoppt

Ausgabe

Syntax	Integer	Bedeutung
on	3	der asynchrone openFT-Server ist gestartet
off	4	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").

Systemparameter

MIB-Definition

Objektname/ Objekt Identifier	Zugriff	Bedeutung	Kommando <i>ftmodo</i>
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	<i>-tu</i>
ftSysparMaxOSP/ 1.3.6.1.4.1.231.2.18.2.7.0	read-write	Max OSP ¹	<i>-cl</i>
ftSysparMaxISP/ 1.3.6.1.4.1.231.2.18.2.8.0	read-write	Max ISP ¹	<i>-cl</i>
ftSysparProcessorName/ 1.3.6.1.4.1.231.2.18.2.9.0	read-write	Processor Name	<i>-p</i>
ftSysparStationName/ 1.3.6.1.4.1.231.2.18.2.10.0	read-write	Station Name	<i>-l</i>
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)	<i>-ccs</i>
ftSysparMaxInboundReqs/ 1.3.6.1.4.1.231.2.18.2.12.0	read-write	Max Inbound Requests	<i>-rql</i>
ftSysparMaxLifeTime/ 1.3.6.1.4.1.231.2.18.2.13.0	read-write	Max Life Time	<i>-rqt</i>

¹Die 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 $Max\ OSP = Max\ ISP = Verbindungs\ limit * 2/3$ (auf ganzzahlige Werte gerundet).

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

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.

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).

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“](#).

4.13.3 Messdatenerfassung mit openFT

Um die Messdatenerfassung zu konfigurieren, müssen Sie FT-Verwalter sein. Wenn die Messdatenerfassung eingeschaltet und der asynchrone openFT-Server gestartet ist, kann jeder Benutzer die Messdaten abrufen.

4.13.3.1 Messdatenerfassung konfigurieren

Sie konfigurieren die Messdatenerfassung über das Kommando *ftmodo* 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.

4.13.3.2 Messdaten anzeigen

Sie folgende Möglichkeiten:

- Kommando *ftshwm*: lokale Messdaten anzeigen
- openFT Monitor: lokale oder entfernte Messdaten anzeigen

Sie starten den openFT Monitor entweder über den openFT Explorer (Menü *Extras* bzw. Kontextmenü eines Partnereintrags) oder über das Kommando *ftmonitor*.

Wenn Sie sich die Messdaten von openFT-Instanzen auf anderen Systemen anzeigen lassen möchten, geben Sie beim Aufruf des openFT Monitors den Partner und die Zugangsberechtigung an. 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.

- Vorverarbeitung: entfernte Messdaten anzeigen

Dazu definieren Sie auf dem fernen System für die Zugangsberechtigung ein Berechtigungsprofil, in dem Sie ein Dateinamen-Präfix mit dem Schlüsselwort **FTMONITOR* als Vorverarbeitungskommando angeben, siehe „[Berechtigungsprofil zum Anzeigen von Messdaten einrichten](#)“.

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.

- Windows-Leistungsüberwachung: lokale Messdaten anzeigen (nur auf Windows-Systemen), siehe [Abschnitt „Messdaten anzeigen“](#).

Berechtigungsprofil zum Anzeigen von Messdaten einrichten

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)
```

i 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
```

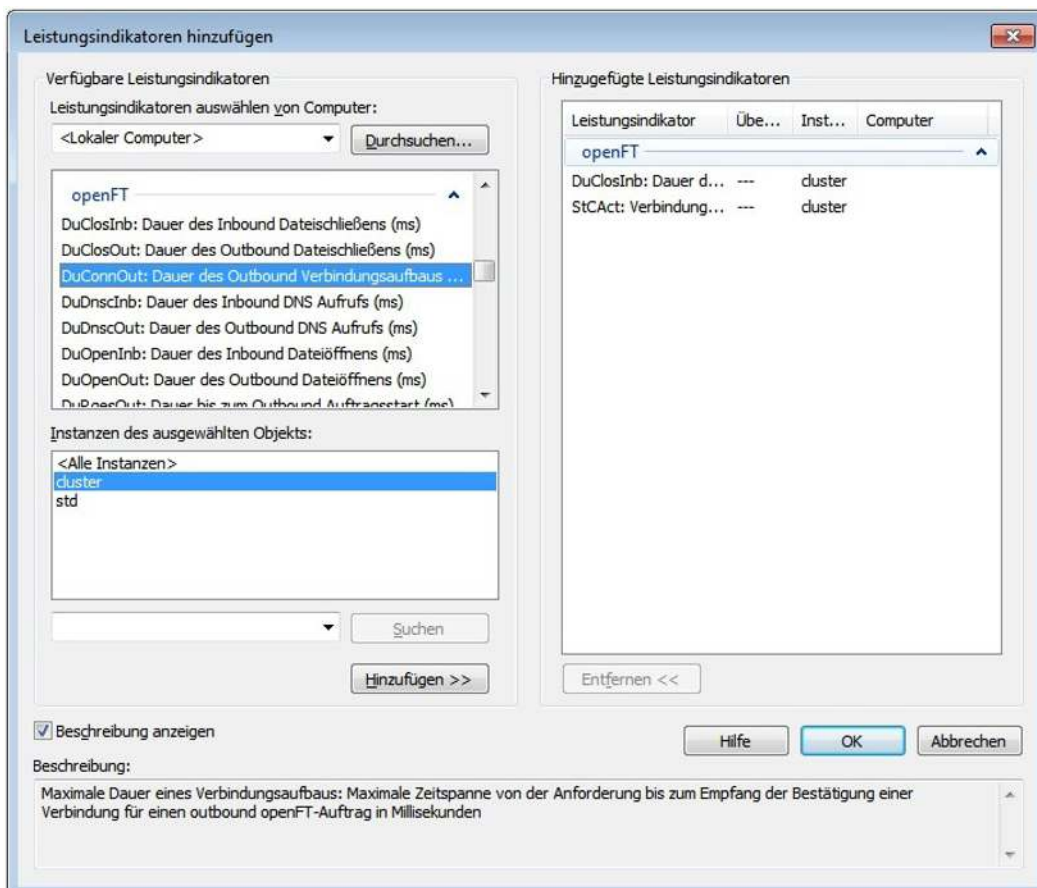
Die Messdaten werden in die Datei *partner1_data* ausgegeben. Innerhalb der Anführungszeichen können Sie als einzigen Parameter *-po=polling intervall* angeben. Wenn Sie das standardmäßige Polling-Intervall von 1 Sekunde verwenden wollen, schreiben Sie ein Leerzeichen zwischen die Anführungszeichen.

Messdaten über die Windows-Leistungsüberwachung anzeigen (nur an Windows-Systemen)

Dazu aktivieren Sie zuerst die gewünschten Messwerte über die Systemsteuerung. Gehen Sie wie folgt vor (die Beschreibung gilt für Windows 10):

- Starten Sie die Windows-Systemsteuerung und öffnen Sie über *System und Sicherheit - Verwaltung - Leistungsüberwachung* das Fenster *Leistungsüberwachung*.
- Klicken Sie in der Navigationsleiste auf *Überwachungstools - Leistungsüberwachung* und klicken Sie auf die Schaltfläche *+*.
- Im Fenster *Leistungsindikatoren hinzufügen* finden Sie unter *Verfügbare Leistungsindikatoren* die Rubrik *openFT*. Wählen Sie die gewünschten openFT-Messwerte und ggf. die openFT-Instanz aus und klicken Sie auf die Schaltfläche *Hinzufügen >>*. Die Messwerte werden rechts unter *Hinzugefügte Leistungsindikatoren* aufgelistet.
- Mit OK werden die Messwerte erfasst und angezeigt.

Sie können die openFT-Messwerte wieder aus der Windows-Leistungsüberwachung entfernen, indem Sie diese markieren und auf die Schaltfläche *Entfernen <<* klicken.



4.14 FTAC-Umgebung verwalten

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

4.14.1 Berechtigungssätze verwalten

Als FTAC-Verwalter haben Sie folgende Aufgaben:

- Sie legen den Standardberechtigungssatz mit dem Kommando *ftmoda @s* fest.
Nach einer Neuinstallation 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, siehe [Abschnitt „Berechtigungssätze verwalten“](#).
Über die Vorgaben des Standardberechtigungssatzes kann sich ein Benutzer nur dann hinwegsetzen, wenn Sie als FTAC-Verwalter seinen Berechtigungssatz entsprechend ändern oder wenn Sie ihm ein privilegiertes Berechtigungsprofil einrichten.
- Sie können Berechtigungssätze von allen Benutzern des Systems 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 für jeden Benutzer im System mit *ftmoda* einen individuellen Berechtigungssatz vergeben oder einen gegebenen Berechtigungssatz modifizieren.
- Sie legen erstmalig den ADM-Verwalter fest, indem Sie im Berechtigungssatz des ADM-Verwalters das ADM-Privileg setzen (siehe [Abschnitt „ADM-Verwalter festlegen“](#)).

Alternativ können Sie den openFT Explorer verwenden: Klicken Sie in der Navigationsleiste unter *Administration* auf *Berechtigungssätze*. Im Objektfenster *Berechtigungssätze* werden alle Berechtigungssätze aufgelistet. Der Standardberechtigungssatz hat den Namen *STD.

Berechtigungssätze sinnvoll einsetzen

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

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
- und openFT-Partner einer gesicherten Identitätsprüfung mit kryptografischen Mitteln zu unterziehen (siehe [Abschnitt „Authentifizierung“](#)).

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*, *fttp* nicht aktiv sein dürfen.

4.14.2 Berechtigungsprofile verwalten

Zur Administration von Berechtigungsprofilen bietet openFT dem FTAC-Verwalter folgende Kommandos:

- *ftcrep*: Berechtigungsprofile einrichten
- *ftdelp*: Berechtigungsprofile löschen
- *ftmodp*: Berechtigungsprofile ändern
- *ftshwp*: Berechtigungsprofile anzeigen

Sie können die Berechtigungsprofile auch über den openFT Explorer verwalten: Klicken Sie in der Navigationsleiste unter *Administration* auf das Objekt *Berechtigungsprofile*. Eine detaillierte Beschreibung zu den einzelnen Funktionen finden Sie in der Online-Hilfe.

Als FTAC-Verwalter haben Sie folgende Möglichkeiten, fremde Berechtigungsprofile zu bearbeiten:

- Sie können sie sich mit dem Kommando *ftshwp* ansehen. Die Zugangsberechtigung eines Berechtigungsprofils wird nicht mit ausgegeben. Das heißt, dass der FTAC-Verwalter durch seine Verwaltereigenschaft keine Zugriffsrechte auf die Dateien fremder Benutzerkennungen bekommt.
- Sie können sie mit dem Kommando *ftdelp* löschen. 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 sie mit dem Kommando *ftmodp* privilegieren (*-priv=y*) oder eine Privilegierung wieder zurücknehmen (*-priv=n*).
- Sie können auch andere Änderungen mit *ftmodp* vornehmen. Das Berechtigungsprofil wird dann so lange gesperrt, bis der Profileigentümer diese Änderungen quittiert, indem er z.B. mit *ftmodp ... -v=y* die Zugangsberechtigung wieder auf "gültig" setzt. Besitzen zusätzlich die FT-Verwalterrechte oder geben Sie im Profil explizit das Kennwort des Profileigentümers an, so werden die Profile nicht gesperrt.

Privilegierung von Berechtigungsprofilen

In begründeten Ausnahmefällen darf sich ein FT-Benutzer durch den Einsatz eines privilegierten Berechtigungsprofiles über die Vorgaben seines Berechtigungssatzes hinwegsetzen. Solche Ausnahmefälle können beispielsweise sein:

- es soll eine bestimmte Datei übertragen werden,
- es ist keine oder nur eine bestimmte Folgeverarbeitung erlaubt,
- ein Partnersystem mit einer hohen Sicherheitsstufe darf mit der Benutzerkennung File-Transfer betreiben, andere mit kleineren Sicherheitsstufen aber nicht.

Der Schutz für die Benutzerkennung wird in einem solchen Fall dadurch aufrecht erhalten, dass in dem Berechtigungsprofil nur sehr enge Zugriffsrechte erlaubt werden.

4.14.3 FTAC-Umgebung sichern und übertragen

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.

Zum Sichern und Übertragen der FTAC-Umgebung stehen Ihnen folgende Kommandos zur Verfügung:

- *ftexpe*: FTAC-Umgebung auf Datei ausgeben
- *ftimpe*: FTAC-Umgebung aus Datei übernehmen
- *ftshwe*: FTAC-Umgebung aus Exportdatei anzeigen

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

Gesicherte Berechtigungssätze und -profile können Sie sich auch über den openFT Explorer ansehen, indem Sie in der Navigationsleiste beim Objekt *Exportierte Berechtigungen* den Kontextmenü-Befehl *Exportdatei öffnen...* aufrufen.

Berechtigungssätze und -profile sichern und wieder einspielen

- Beim Sichern der FTAC-Umgebung 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.
- Beim Wiedereinspielen der gesicherten FTAC-Umgebung können Sie nach Sätzen, Profilen und Kennungen differenzieren, d.h. Sie müssen nicht den kompletten Sicherheitsstand 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 und müssen entsperrt werden (z.B. mit *ftmodp ... -v=y*).

4.15 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- bzw. Windows-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 [Abschnitt „openFT-Instanzen und Cluster-Betrieb“](#)).

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 sowie an Unix-Systemen die Startup- und Shutdown-Datei wie bei einer Neuinstallation initialisiert.

An Unix-Systemen wird beim Aktivieren einer vorhandenen Instanz 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 (Unix-Systeme)
- die Instanz aus der openFT-Instanzenverwaltung (Windows-Systeme)

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.

i 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.

- i**
- Wenn Sie an einem Unix-System mit mehreren Instanzen arbeiten, dann ist für jede der Instanzen im gegebenen Fall ein eigener Aufruf *ftalarm* erforderlich.
 - Bitte beachten Sie auch den [Abschnitt „Hinweise zur ftalarm-Funktion im Einbenutzerbetrieb“](#).
 - Eine detaillierte Beschreibung zu den Kommandos finden Sie im Handbuch "openFT (Unix- und Windows-Systeme) - Kommandoschnittstelle".

Startup- und Shutdown-Datei (Unix-Systeme)

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/Stop über Manifeste. Für jede Instanz wird automatisch ein Manifest erzeugt.

4.16 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 (Unix-Systeme)
ftshwptn -pw > partner_save.bat (Windows-Systeme)
```

Die Datei *partner_save* / *partner_save.bat* 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 (Unix-Systeme)
ftshwo -pw > option_save.bat (Windows-Systeme)
```

Die Datei *option_save* / *option_save.bat* 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
```

4.17 FTAM-Besonderheiten auf Unix-/Windows-Systemen

- Abbildung der Dateizugriffsrechte
 - Outbound-Aufträge
 - Inbound-Aufträge
- Abbildung von FTAM-Attributen auf das reale Dateisystem
 - Inbound-Abbildung von FTAM-Attributen
 - Inbound-Abbildung des document type
 - Zugangs- und Zugriffsschutz
 - Outbound-Abbildung des document type

4.17.1 Abbildung der Dateizugriffsrechte

In diesem Abschnitt wird die Abbildung der Unix-Dateischutzbits und der Zugriffsrechte von Windows-Dateien (FAT und NTFS) auf die Dateimanagement-Zugriffsrechte gemäß der openFT-Protokolle und in der ISO-Norm FTAM beschrieben. Er enthält Hinweise zur Änderung und Anzeige von Dateizugriffsrechten mit den Dateimanagement-Funktionen. Dabei wird zwischen Aufträgen mit Initiative im lokalen System (Outbound-Aufträge) und Aufträgen mit Initiative im fernen System (Inbound-Aufträge) differenziert.

4.17.1.1 Outbound-Aufträge

Sie können sich die Dateimanagement-Zugriffsrechte von Dateien, die im fernen Rechner vorliegen, ansehen sowie die Zugriffsrechte ändern.

Zugriffsrechte anzeigen

Die Zugriffsrechte von Dateien im fernen System lassen Sie sich mit dem FT-Kommando *ftshw* anzeigen. Angezeigt werden die folgenden Dateimanagement-Zugriffsrechte:

r (read)	Datei lesen
p (replace)	Datei überschreiben
x (extend)	Datei erweitern
e (erase)	Dateneinheit (File Access Data Unit FADU) löschen (nur bei FTAM-Partnern sinnvoll)
a (rdatt)	Dateiattribute lesen
c (chatt)	Dateiattribute ändern
d (delete)	Datei löschen

Hinweis für Unix-Systeme

Ist im fernen Unix-System openFT installiert, dann werden die Datei-Schutzbits *r*, *w* und *x* auf die Dateizugriffsrechte so abgebildet, wie im nächsten Abschnitt für die Inbound-Aufträge beschrieben ist.

Bei FTAM-Partnern wird von den veränderbaren (access control) und den unveränderbaren (permitted actions) Dateizugriffsrechten jeweils der restriktivere Wert angezeigt, weil er für mögliche Dateimanipulationen relevant ist.

Zugriffsrechte ändern

Dateizugriffsrechte ändern Sie mit Hilfe des FT-Kommandos *ftmod*. Darüber hinaus ist es möglich, bei Dateiübertragungsaufträgen über die FTAM-Funktionalität die Zugriffsrechte der Empfangsdatei zu setzen bzw. zu ändern. Welche Schutzbits und wie Schutzbits in einem fernen openFT (Unix-Systeme) oder openFT (Windows) gesetzt werden können, finden Sie bei den jeweiligen Kommandobeschreibungen. Nicht unterstützte Optionen oder Kombinationen von Optionen des Zugriffsmodus werden bei einem Dateimanagement-Auftrag abgewiesen, beim Dateiübertragungsauftrag ignoriert.

4.17.1.2 Inbound-Aufträge

Partner in fernen Systemen können sich die Dateimanagement-Zugriffsrechte von Ihren lokalen Dateien ansehen sowie die Zugriffsrechte ändern.

Das Zugriffsrecht *i* (insert - Dateneinheit (FADU) einfügen) ist in Unix- und Windows-Systemen nicht erlaubt.

Zugriffsrechte in Unix-Systemen anzeigen und ändern

Bei einem entsprechenden Auftrag von einem fernen System bildet openFT (Unix-Systeme) die lokalen Dateischutzbits *r*, *w* und *x* wie folgt auf die Dateimanagement-Zugriffsrechte ab:

angezeigte Zugriffsrechte	Unix-Dateischutzbits der Datei	Unix-Dateischutzbits der übergeordneten Dateiverzeichnisse
r (read) Datei lesen	r-Bit	x-Bit ¹
p (replace) Datei überschreiben	w-Bit	x-Bit
x (extend) Datei erweitern	w-Bit	x-Bit
e (erase) ² Dateneinheit löschen	w-Bit	x-Bit
a (rdatt) Dateiattribut lesen		x-Bit
c (chatt) Dateiattribut ändern	der Auftrag muss die Eigentümerberechtigung der Datei haben	x-Bit w-Bit für das direkt übergeordnete Verzeichnis
d (delete) Datei löschen	w-Bit	x-Bit w-Bit für das direkt übergeordnete Verzeichnis

¹Das r-Bit des darüberliegenden Dateiverzeichnisses ist ohne Bedeutung.

²Das Attribut ist nur für FTAM-Verbindungen sinnvoll.

Es werden die Zugriffsrechte von nur einer Benutzerklasse (owner, group, other) angezeigt. Es wird die Benutzerklasse entsprechend der Zugriffsrechte des Dateimanagement-Auftrags im Unix-System angezeigt. Bestehen Zugriffsrechte für mehrere Benutzerklassen, dann werden die Zugriffsrechte der höchsten Benutzerklasse angezeigt (z.B. Owner-Zugriffsrechte vor Group-Zugriffsrechten).

Im übrigen gelten für Dateizugriffe die lokalen Regeln des Unix-Systems. So muss zum Beispiel das x-Bit für alle darüberliegenden Dateiverzeichnisse gesetzt sein.

Zugriffsrechte ändern

Welche Möglichkeiten zur Änderung von Dateischutzbits sich im Unix-System ergeben, können Sie der folgenden Tabelle entnehmen:

Dateimanagement-Zugriffsrechte	Unix-Dateischutzbits	Funktion
rp x ead	rw ¹	read-write
rac	r- ¹	read-only
p x ead	-w ¹	write-only
ac	-- ¹	none

¹Vom Unix-System aus wird das x-Bit durch das jeweilige openFT-Kommando nicht verändert. Von Windows-PCs aus können auch die Attribute ferner Verzeichnisse geändert werden. In diesem Fall wird durch rp~~x~~ead (= @rw) auch das x-Bit gesetzt.

Die openFT-Protokolle und FTAM kennen bei Zugriffsrechten nur die Möglichkeit gesetzt oder nicht gesetzt. Das heißt, bei der Angabe von Zugriffsrechten muss explizit gesagt werden, ob ein Zugriffsrecht gesetzt oder nicht gesetzt werden soll. Die Möglichkeit, Zugriffsrechte unverändert zu lassen, gibt es bei den Protokollen nicht.

Damit Dateizugriffsrechte überhaupt modifiziert werden können, müssen die Dateimanagement-Zugriffsrechte *a* und *c* immer angegeben werden. Andernfalls wird der ferne Auftrag abgelehnt. Die Dateizugriffsrechte *pxed* müssen zusätzlich gesetzt werden, wenn für eine Datei das w-Schutzbit gesetzt werden soll, da alle diese Werte auf das w-Schutzbit einer Datei abgebildet werden. Alle anderen Kombinationen von Dateizugriffsrechten führen zur Ablehnung des fernen Auftrags.

Zugriffsrechte einer Datei ändern kann nur deren Eigentümer. Setzt der Eigentümer Zugriffsrechte, dann werden sie nur bei der Owner-Benutzerklasse gesetzt. Hingegen wird das Löschen von Zugriffsberechtigungen bei Owner-, Group- und Other-Benutzerklasse durchgeführt.

Zugriffsrechte in Windows-Systemen anzeigen

Bei einem entsprechenden Auftrag von einem fernen System bildet openFT (Windows) die lokalen Schutzattribute auf die Dateimanagement-Zugriffsrechte ab. Hierbei muss unterschieden werden, ob die Datei auf einem NTFS-Dateisystem oder einem anderen Dateisystem liegt.

Für die NTFS-Schutzattribute gelten folgende Abbildungen:

angezeigte Zugriffsrechte	Dateizugriffsrechte	Rechte im übergeordneten Verzeichnis
r (read) Datei lesen	Lesen	Lesen
p (replace) Datei überschreiben	Lesen und Schreiben	Lesen und Schreiben
x (extend) Datei erweitern	Lesen und Schreiben	Lesen
e (erase) ¹ Dateneinheit löschen	Lesen und Schreiben	Lesen
a (rdatt) Dateiattribut lesen	Lesen	Lesen

c (ch att) Dateiattribut ändern	Lesen und Schreiben	Lesen
d (d ele t e) Datei löschen	Löschen	Lesen und Schreiben

¹Das Attribut ist nur für FTAM-Verbindungen sinnvoll.

Die Zugriffsrechte gelten aus der Sicht des Benutzers, der beim Dateiübertragungsauftrag bzw. Dateimanagement-Auftrag (direkt, oder indirekt über ein FTAC-Profil) angegeben wurde. Für die Zuordnung der Zugriffsrechte zu einem Benutzer gelten die Regeln von Windows. Sollen die Attribute der Dateien eines Verzeichnisses aufgelistet werden und kann der aufrufende Benutzer für einige dieser Dateien die Schutzattribute nicht lesen, so werden für diese Dateien nur die Dateinamen ausgegeben.

Ist das - auch bei FAT-Dateien vorhandene - "Schreibgeschützt"-Attribut bei einer NTFS-Datei gesetzt, so hat dies die Wirkung, als wären die Zugriffsrechte "Schreiben" und "Löschen" nicht gesetzt.

Für die FAT-Schutzattribute gelten folgende Abbildungen:

angezeigte Zugriffsrechte	"Schreibgeschützt"-Attribut gesetzt
r (r ead) Datei lesen	ja oder nein
p (r eplac e) Datei überschreiben	nein
x (e xtend) Datei erweitern	nein
e (e rase) Dateneinheit löschen	nein
a (read a tttribute) Dateiattribut lesen	ja oder nein
c (c hange attribute) Dateiattribut ändern	nein
d (d ele t e) Datei löschen	nein

Die Rechte im übergeordneten Verzeichnis spielen bei FAT-Systemen keine Rolle.

i Das echte Ändern von Zugriffsrechten wird in Windows-Systemen nicht unterstützt.

4.17.2 Abbildung von FTAM-Attributen auf das reale Dateisystem

Der Abschnitt beschreibt die Realisierung des virtuellen Dateispeichers bei Nutzung der FTAM-Funktionalität und die Abbildungsmechanismen zwischen dem virtuellen und dem realen Dateispeicher des Unix-Systems oder Windows-Systems.

Die FTAM-Attribute werden teilweise auf die in Unix oder Windows-Systemen verfügbaren Attribute und teilweise auf den so genannten "FTAM-Katalog" (Unix-Systeme) oder die sogenannte "FTAM-Katalogerweiterung" (Windows-Systeme) abgebildet:

- Der FTAM-Katalog dient hierbei zur Erweiterung der in Unix-Systemen verfügbaren Dateiattribute. Er ist nur bei Zugriffen über FTAM von Bedeutung. Das heißt, eine Datei kann weiterhin mit dem Betriebssystem-Kommando *rm* gelöscht werden, auch wenn der Parameter *permitted actions* aus dem FTAM-Katalog dies einem FTAM-Partner nicht erlaubt. Dadurch kann es allerdings zu Inkonsistenzen zwischen dem FTAM-Katalog und dem realen Dateisystem kommen. Solche Inkonsistenzen werden automatisch beim Start von openFT (Unix-Systeme) entdeckt und die betreffenden Einträge im FTAM-Katalog gelöscht.

i Die im FTAM-Katalog gespeicherten FTAM-Attribute zu einer Datei sind für Verweise auf diese Datei (wie z.B. symbolische Links) nicht sichtbar.

- Die FTAM-Katalogerweiterung ist nur für NTFS-Dateien möglich und dient zur Erweiterung der in Windows verfügbaren Dateiattribute. Sie ist fester, aber für den gewöhnlichen Benutzer unsichtbarer Bestandteil einer lokalen NTFS-Datei. FAT-Dateien oder Dateien, auf die per Netzlaufwerk oder UNC-Name zugegriffen wird, können keine FTAM-Katalogerweiterung haben. Daher gehen die FTAM-spezifischen Attribute verloren, wenn z. B. eine NTFS-Datei in ein FAT-Dateisystem kopiert wird.

FTAM-Katalogerweiterungen können erzeugt werden durch:

- Dateiübertragungsaufträge mit FTAM (auf Empfangsdateien)
- Inbound-Dateimanagement-Aufträge
- Das Ändern der lokalen FTAM-Attribute

Die Attribute in der FTAM-Katalogerweiterung sind dann von Bedeutung, wenn über openFT (in der Regel mit FTAM) zugegriffen wird. Das heißt, eine Datei kann weiterhin über den Windows-Explorer oder mit dem Betriebssystem-Kommando *del* gelöscht werden, auch wenn der FTAM-Parameter *permitted actions* dies einem FTAM-Partner nicht erlaubt.

Einträge im FTAM-Katalog werden durch Inbound-Dateimanagement-Aufträge, durch Ändern der lokalen FTAM-Attribute oder durch einen Dateiübertragungsauftrag erzeugt. Durch Löschen der Datei vom fernen System aus wird auch der zugehörige Eintrag im FTAM-Katalog wieder entfernt.

Bitte beachten Sie, dass eine Datei, die im FTAM-Katalog bzw. in ihrer FTAM-Katalogerweiterung als Textdatei gekennzeichnet ist, nicht als Binärdatei übertragen oder durch Binärdaten erweitert werden darf.

4.17.2.1 Inbound-Abbildung von FTAM-Attributen

In folgenden Tabellen wird die Abbildung von FTAM-Attributen auf das reale Dateisystem dargestellt.

Unix-Systeme

Attributgruppe	FTAM-Attribute	Abbildung im Unix-System (inbound empfangen)	FTAM-Attribute ändern
Kernel group	permitted actions READ-FILE INSERT-DATA-UNIT REPLACE-FILE EXTEND-FILE ERASE-DATA-UNIT READ-ATTRIBUTES CHANGE-ATTRIBUTES DELETE-FILE	FTAM-Katalog	lokal erlaubt ¹
	universal class number GRAPHIC GENERAL IA5 VISIBLE	FTAM-Katalog	lokal erlaubt ¹
	string significance VARIABLE FIXED NOT-SIGNIFICANT	FTAM-Katalog	lokal erlaubt ¹
	maximum string length	FTAM-Katalog	lokal erlaubt ¹
	document type FTAM1 FTAM3	FTAM-Katalog	lokal erlaubt ¹
Storage group	file availability IMMEDIATE DEFERRED	FTAM-Katalog	inbound erlaubt
	future file size	wird ignoriert	nicht erlaubt
	storage account	wird ignoriert	nicht erlaubt
Security group	ActionList (of 1ACE):		
	READ-FILE	r	inbound erlaubt
	INSERT-DATA-UNIT	nicht erlaubt	nicht erlaubt
	REPLACE-FILE	w	inbound erlaubt
	EXTEND-FILE	w	inbound erlaubt

ERASE-DATA-UNIT	w	inbound erlaubt
READ-ATTRIBUTES	x dir	inbound erlaubt ²
CHANGE-ATTRIBUTES	w dir+owner	inbound erlaubt ²
DELETE-FILE	w + wdir	inbound erlaubt
LEGAL-QUALIFICATION	wird ignoriert	nicht erlaubt

¹Eine lokale Änderung der FTAM-Attribute ist mit dem Kommando *ftmodf* möglich.

²Der Wert muss immer mitgeschickt werden, darf aber nie geändert werden.

Windows-Systeme

Attributgruppe	FTAM-Attribute	Abbildung in Windows (inbound empfangen)	FTAM-Attribute ändern
Kernel group	permitted actions READ-FILE INSERT-DATA-UNIT REPLACE-FILE EXTEND-FILE ERASE-DATA-UNIT READ-ATTRIBUTES CHANGE-ATTRIBUTES DELETE-FILE	FTAM-Katalogerweiterung	lokal erlaubt ¹
	universal class number GRAPHIC GENERAL IA5 VISIBLE	FTAM-Katalogerweiterung	lokal erlaubt ¹
	string significance VARIABLE FIXED NOT-SIGNIFICANT	FTAM-Katalogerweiterung	lokal erlaubt ¹
	maximum string length	FTAM-Katalogerweiterung	lokal erlaubt ¹
	document type FTAM1 FTAM3	FTAM-Katalogerweiterung	lokal erlaubt ¹
Storage group	file availability IMMEDIATE DEFERRED	FTAM-Katalogerweiterung	inbound erlaubt

	future file size	wird ignoriert	nicht erlaubt
	storage account	wird ignoriert	nicht erlaubt
Security group	ActionList:		
	READ-FILE	Lesen ²	nicht erlaubt
	INSERT-DATA-UNIT	nicht erlaubt	nicht erlaubt
	REPLACE-FILE	Lesen + Schreiben ³	nicht erlaubt
	EXTEND-FILE	Lesen + Schreiben ²	nicht erlaubt
	ERASE-DATA-UNIT	Lesen + Schreiben ²	nicht erlaubt
	READ-ATTRIBUTES	Lesen ²	nicht erlaubt
	CHANGE-ATTRIBUTES	Lesen + Schreiben ²	nicht erlaubt
	DELETE-FILE	Löschen ³	nicht erlaubt
	LEGAL-QUALIFICATION	wird ignoriert	nicht erlaubt

¹Eine lokale Änderung der FTAM-Attribute ist mit dem Kommando *ftmodf* möglich.

²Zusätzlich Lesen im übergeordneten Verzeichnis erforderlich

³Zusätzlich Lesen + Schreiben im übergeordneten Verzeichnis erforderlich

Die folgenden Dateiattribute werden aus den aktuellen Unix- bzw. Windows-Dateiattributen abgeleitet:

- filename
- filesize
- identity-of-creator
- date-and-time-of-last-read-access
- date-and-time-of-creation
- date-and-time-of-last-modification
- access-control

Weitere Attribute werden von openFT nur "partiell" unterstützt. Als Responder liefert openFT für zu folgenden Dateiattributen keinen Wert (*no value available*):

- identity-of-last-modifier
- identity-of-last-reader
- identity-of-last-attribute-modifier
- storage-account
- legal-qualification

Der FTAM-Protokollparameter *filestore password* wird in Unix- und WindowsSystemen auf das Kennwort der betroffenen Benutzererkennung abgebildet.

4.17.2.2 Inbound-Abbildung des document type

Die folgenden Tabellen geben Auskunft über die Abbildung des *document type* bei der Dateiübertragung. Dabei wird zwischen openFT als Empfangssystem und openFT als Sendesystem unterschieden.

Abbildung des document type beim Inbound Empfangen (FTAM --> Lokales System)

FTAM (virtueller Dateispeicher des fernen Systems)			Lokale Empfangsdatei
document type	universal class	string significance	
FTAM-1	25 - GraphicString	variable/fix	Textdatei
FTAM-1	26 - VisibleString	variable/fix	Textdatei
FTAM-1	27 - GeneralString	not-significant	Textdatei
FTAM-1	22 - IA5String	not-significant	Textdatei
FTAM-3	----	not significant	unstrukturierte Binärdatei
FTAM-3	----	variable	satzstrukturierte Binärdatei
FTAM-3	----	fix	Binärdatei mit fester Satzlänge

Das Übertragen von FTAM-3 Dateien mit variabler und fixer *string significance* ist in der Funktionsnorm ENV 41204 nicht vorgesehen. openFT unterstützt diese Funktion zusätzlich, da dieses Dateiformat dem Benutzerformat in Unix- und Windows-Systemen entspricht.

Abbildung des document type beim Inbound Senden (FTAM <-- Lokales System)

FTAM (Anforderungen im Auftrag und/oder Einträge im FTAM-Katalog/-Katalogereiterung im lokalen System)			Lokale-Sendedatei
document type	universal class	string significance	
nicht angegeben	nicht angegeben	nicht angegeben	Textdatei
FTAM-1	nicht angegeben	nicht angegeben	Textdatei
FTAM-1	25 - GraphicString	variable/fix	Textdatei
FTAM-1	26 - VisibleString	variable/fix	Textdatei
FTAM-1	27 - GeneralString	not-significant	Textdatei
FTAM-1	22 - IA5String	not-significant	Textdatei
FTAM-3	----	nicht angegeben	unstrukturierte Binärdatei
FTAM-3	----	not significant	unstrukturierte Binärdatei
FTAM-3	----	variable	satzstrukturierte Binärdatei
FTAM-3	----	fix	Binärdatei mit fester Satzlänge

Existiert ein Eintrag zur Sendedatei im FTAM-Katalog/-Katalogerweiterung, so müssen die Dateiformat-Anforderungen im Auftrag mit diesem Eintrag übereinstimmen. Andernfalls können Dateiinkonsistenzen entstehen und infolgedessen Dateiübertragungsaufträge mit der betreffenden Datei abgebrochen werden.

Sind keine Anforderungen im Auftrag angegeben, so gelten die Angaben im FTAM-Katalog/ -Katalogerweiterung.

4.17.2.3 Zugangs- und Zugriffsschutz

openFT unterstützt die Security group des virtuellen Dateispeichers. Damit wird ein wirkungsvoller Zugriffsschutzmechanismus für Dateien zur Verfügung gestellt.

Um auf den virtuellen Dateispeicher eines Systems zugreifen zu können, werden die FTAM-Protokollparameter *initiator identity* und *filestore password* benötigt. Sie werden von openFT auf die Benutzerkennung und das Kennwort der Benutzerkennung im Unix- oder Windows-System abgebildet.

Auch beim File Transfer mit FTAM-Partnern können die FTAC-Funktionen für einen erweiterten Zugangs- und Zugriffsschutz genutzt werden. Wenn von einem FTAM-Partner aus ein Berechtigungsprofil im Unix- oder Windows-System angesprochen werden soll, muss die Zugangsberechtigung für dieses Berechtigungsprofil im Protokollparameter *initiator identity* geliefert werden. Die Parameter *filestore password* und *account* dürfen dann nicht angegeben werden. Ansonsten gelten die in diesem Handbuch zur FTAC-Funktionalität beschriebenen Regeln (z.B. Referenzieren einer im Berechtigungsprofil fest vorgegebenen Datei entweder über die Angabe *NOT-SPECIFIED für den Dateinamen oder durch Weglassen des Dateinamens usw.).

4.17.2.4 Outbound-Abbildung des document type

Wenn openFT als Initiator auftritt, kann der FT-Benutzer im Auftrag mit der Angabe zum Dateityp spezifizieren, ob Text- oder Binärdaten übertragen werden sollen (Optionen *-t*, *-u*, *-b* im *ft*- oder *ncopy*-Kommando). Im realen Dateispeicher des Unix- oder Windows-Systems existiert kein Attribut für Binär- oder Textdaten.

i In Windows-Systemen beachten Sie bitte, dass in nur NTFS-Dateien Einträge im FTAM-Katalog haben können. Daher kann man für Dateien auf gemounteten Netzlaufwerken oder UNC-Shares keine Einträge im FTAM-Katalog erzeugen oder bearbeiten, da gemountete Systeme und UNC-Shares wie FAT-Dateisysteme behandelt werden.

Die folgenden Tabellen geben Auskunft über die Abbildung des *document type* bei der Dateiübertragung. Dabei wird zwischen openFT als Empfangssystem und als Sendesystem unterschieden.

Outbound Senden (Lokales System --> FTAM)

Lokales System	FTAM-Attribute		
Dateityp	document type	universal class	string significance
Text (-t)	FTAM-1	25 - GraphicString	variable ¹
Benutzerformat (-u)	FTAM-3	----	variable ¹
Binär (-b)	FTAM-3	----	not-significant ¹
Binär + Satzlänge (-b -r=max-satzlänge)	FTAM-3	----	fixed

¹Wenn eine der Optionen *-t*, *-u* und *-b* angegeben wird und für Sendedatei auf dem lokalen System ein Eintrag im FTAM-Katalog/-Katalogerweiterung existiert, so muss dieser mit den Angaben in dieser Tabelle übereinstimmen.

Spezifiziert der FT-Benutzer im Auftrag keinen Dateityp, so werden die Angaben aus dem FTAM-Katalog übernommen. Fehlt ein Eintrag im FTAM-Katalog, so gilt FTAM1, GraphicString und variable.

Das Übertragen von FTAM-3 Dateien mit variabler oder fixer *string significance* ist in der Funktionsnorm ENV 41204 nicht vorgesehen. openFT unterstützt diese Funktion zusätzlich.

Outbound Empfangen (Lokales System <-- FTAM)

Beim Outbound Empfangen hängt der Typ der Empfangsdatei auch davon ab, ob und ggf. welchen Dateityp Sie beim Übertragungsauftrag angeben. Hier sind folgende Fälle zu unterscheiden.

1. Im Auftrag wird kein Dateityp angegeben

FTAM (virtueller Dateispeicher des fernen Systems)			Empfangsdatei auf dem lokalen System
document type	universal class	string significance	
FTAM-1	25 - GraphicString	variable/fix	Textdatei
FTAM-1	26 - VisibleString	variable/fix	Textdatei

FTAM-1	27 - GeneralString	not-significant	Textdatei
FTAM-1	22 - IA5String	not-significant	Textdatei
FTAM-3	----	not-significant	unstrukturierte Binärdatei
FTAM-3	----	variable	satzstrukturierte Binärdatei
FTAM-3	----	fix	Binärdatei mit fester Satzlänge

2. Im Auftrag wird *Text* bzw. der Schalter *-t* für den Dateityp angegeben

FTAM (virtueller Dateispeicher des fernen Systems)			Empfangsdatei auf dem lokalen System
document type	universal class	string significance	
FTAM-1	25 - GraphicString	variable/fix	Textdatei
FTAM-1	26 - VisibleString	variable/fix	Textdatei
FTAM-1	27 - GeneralString	not-significant	Textdatei
FTAM-1	22 - IA5String	not-significant	Textdatei

3. Im Auftrag wird *Benutzerformat* bzw. der Schalter *-u* für den Dateityp angegeben

FTAM (virtueller Dateispeicher des fernen Systems)			Empfangsdatei auf dem lokalen System
document type	universal class	string significance	
FTAM-3	----	variable	satzstrukturierte Binärdatei
FTAM-3	----	fix	Binärdatei mit fester Satzlänge

4. Im Auftrag wird *Binär* bzw. der Schalter *-b* für den Dateityp angegeben

FTAM (virtueller Dateispeicher des fernen Systems)			Empfangsdatei auf dem lokalen System
document type	universal class	string significance	
FTAM-3	----	not-significant	unstrukturierte Binärdatei

5. Im Auftrag wird *Binär + Satzlänge* bzw. die Schalter *-b* und *-r* (max. satzlänge) für den Dateityp angegeben

FTAM (virtueller Dateispeicher des fernen Systems)			Empfangsdatei auf dem lokalen System
document type	universal class	string significance	
FTAM-3	----	fix	Binärdatei mit fester Satzlänge

5 Zentrale Administration

Die zentrale Administration von openFT umfasst die Funktionen

- [Fernadministration](#)
- [ADM-Traps](#)

5.1 Fernadministration

- Fernadministrations-Server konfigurieren
 - ADM-Verwalter festlegen
 - openFT-Instanz als Fernadministrations-Server deklarieren
 - Berechtigungsprofile für den Zugang zum Fernadministrations-Server einrichten
 - Zu administrierende openFT-Instanzen in die Partnerliste eintragen
 - Konfigurationsdatei per Konfigurations-Editor erstellen
 - Konfigurationsdatei per Text- oder XML-Editor erstellen
 - Konfiguration importieren
 - Konfiguration exportieren und ändern
- Zu administrierende openFT-Instanz konfigurieren
 - Berechtigungsprofil für openFT-Instanz ab V11.0 konfigurieren
 - Berechtigungsprofil für openFT-Instanz < V11.0 konfigurieren
- Fernadministrations-Aufträge stellen
 - Fernadministration über Kommando-Schnittstelle
 - Fernadministration über openFT Explorer
- Logging der Fernadministration

5.1.1 Fernadministrations-Server konfigurieren

Der Fernadministrations-Server 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 V12.1.

Die folgende Tabelle zeigt, welche Schritte notwendig sind, um eine Konfiguration zu erstellen 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 (Konfigurationsdatei per Text- oder XML-Editor erstellen) oder Konfigurations-Editor (Konfigurationsdatei per Konfigurations-Editor erstellen) 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 [Abschnitt „Konfigurationexportieren und ändern“](#).

Jetzt müssen noch openFT-Instanzen auf den Partnersystemen für die Fernadministration konfiguriert werden, siehe [Abschnitt „Zu administrierende openFT-Instanz konfigurieren“](#).

5.1.1.1 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 oder die Berechtigung mit `ftmoda -admpriv=n` wieder zurückgeben. 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*.

5.1.1.2 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*.

- i** • 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 [Abschnitt „ADM-Trap-Server konfigurieren“](#).
- 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.

5.1.1.3 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 Profilenames. Diesen Namen müssen Sie in die Konfigurationsdatei eintragen, wenn Sie den Fernadministrator definieren, siehe [Abschnitt „Konfigurationsdatei per Text- oder XML-Editor erstellen“](#).

zugangsberechtigung

bezeichnet die FTAC-Zugangsberechtigung. Diese muss der Fernadministrator beim Fernadministrations-Auftrag angeben, siehe [Abschnitt „Fernadministration über Kommando-Schnittstelle“](#).

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*.

5.1.1.4 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*. 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.

i Der ADM-Verwalter muss für solche Partner in der Konfigurationsdatei zusätzlich das Attribut *Mode="Legacy"* angeben, siehe [Abschnitt „Konfigurationsdatei per Text- oder XML-Editor erstellen“](#).

5.1.1.5 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 „Konfigurationimportieren“](#).

Die Darstellung der Konfiguration entspricht dem, was Sie später auch unter *Fernadministration* im openFT Explorer sehen, siehe Beispiel im [Abschnitt „Konfigurationsdatei per Konfigurations-Editor erstellen“](#).

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.

i 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.

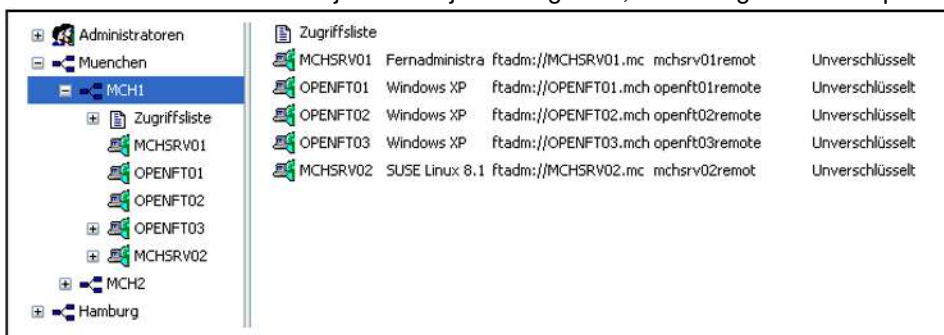
4. Sichern Sie am Schluss die gesamte Konfiguration mit dem Befehl

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.

5.1.1.6 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 [Abschnitt „Konfigurationsdatei per Text- oder XML-Editor erstellen“](#).

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 [Abschnitt „Konfigurationsdatei per Text- oder XML-Editor erstellen“](#),
- die Fernadministratoren, siehe [Abschnitt „Konfigurationsdatei per Text- oder XML-Editor erstellen“](#),
- die openFT-Instanzen und Gruppen von Instanzen, die von diesen Fernadministratoren verwaltet werden sollen, siehe [Abschnitt „Konfigurationsdatei per Text- oder XML-Editor erstellen“](#),
- die Fernadministrations-Rechte, welche die Fernadministratoren auf den jeweiligen openFT-Instanzen haben (die Zugriffsliste), siehe [Abschnitt „Konfigurationsdatei per Text- oder XML-Editor erstellen“](#).
- Den Codierungsmodus für *ftadm*-Kommandos, siehe [Abschnitt „Konfigurationsdatei per Text- oder XML-Editor erstellen“](#).

Die Konfigurationsdatei müssen Sie als ADM-Verwalter anschließend auf dem Fernadministrations-Server mit dem Kommando *ftimpc* importieren, siehe [Abschnitt „Konfiguration importieren“](#). Mit dem Kommando *ftexpc* 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“](#) zu finden.

XML-Vorlage und XML-Schema verwenden

Unter dem openFT-Installationsverzeichnis befindet sich im Verzeichnis *samples/ftadm* (Unix-Systeme) bzw. *samples\ftadm* (Windows-Systeme) die Datei *config.xml*, die eine einfache Beispielformatierung 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 V12.1 ist für die Version "1210" 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="1210"
  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 „Konfigurationsdatei per Text- oder XML-Editor erstellen“](#).
- 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 „Konfigurationsdatei per Text- oder XML-Editor erstellen“](#).
- 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 in [Abschnitt „Konfigurationsdatei per Text- oder XML-Editor erstellen“](#). Die detaillierte Beschreibung einer Gruppe entnehmen Sie dem [Abschnitt „Konfigurationsdatei per Text- oder XML-Editor erstellen“](#).
- 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 „Konfigurationsdatei per Text- oder XML-Editor erstellen“](#).

i 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 [Abschnitt „Fernadministration über Kommando-Schnittstelle“](#).

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-Profiles. 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“](#).

Beispiel:

```
<Configuration
  Version="1210">
  <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 „Konfigurationsdatei per Text- oder XML-Editorerstellen“](#).

- 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 in [Abschnitt „Konfigurationsdatei per Text-oder XML-Editor erstellen“](#).
- 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.

i 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 instanz, spezifische Zugriffsliste
- Ohne Gruppe:
Konfiguration
 - Fernadministrator(en)
 - optionale Zugriffsliste
 - Instanz**
 - optionale instanz, spezifische Zugriffsliste

Details zur Zugriffsliste finden Sie in [Abschnitt „Konfigurationsdatei per Text- oder XML-Editor erstellen“](#).

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“](#):

- openFT ab V11.0: REMOTE-ADMINISTRATION (entspricht *ftcrep ... -ff=a*)
- openFT < V11.0: TRANSFER-FILE + FILE-PROCESSING (entspricht *ftcrep ... -ff=tp*)

i 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 7"
      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.

Aufbau einer Zugriffsliste

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 [Abschnitt „Konfigurationsdatei per Text-oder XML-Editor erstellen“](#).

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 Attributes *AdministratorID* ist eine Zeichenfolge, die den Namen des Fernadministrators angibt. Dieser Fernadministrator muss am Anfang der Konfigurationsdatei mit einem Tag <AdministratorID> definiert sein, siehe [Abschnitt „Konfigurationsdatei per Text- oder XML-Editor erstellen“](#). 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 10"
    Address="HHWSRV11.hhw.mycompany.net"
    Admission="hhwsrv11remote"
    Mode="Legacy">
    <AccessList>
      <AccessEntry
        AdministratorID="Hugo"
        DenyFunction="FTAC"/>
    </AccessList>
  </Instance>
</Group>
```

Codierungsmodus definieren

Das Attribut *CmdMode* definiert im Fernadministrations-Server für jede administrierte Instanz eine Empfehlung, ob Zeichen- oder transparenter Modus verwendet werden soll. Der openFT-Desktop des Administrators kann sich nach einem *ftshwc*-Aufruf an den zentralen Server an diesen Angaben orientieren. *CmdMode* zwingt nicht zu einem bestimmten Modus, hilft aber, Fehler im Ablauf zu vermeiden und ein optimales Verhalten zu erreichen.

CmdMode kann auf einen der beiden folgenden Werte gesetzt werden:

- *Transparent*: Die zentrale Fernadministration empfiehlt die Verwendung des transparenten Modus (*ftadm -fnc=t*)
- *Char*: Die zentrale Fernadministration empfiehlt die Verwendung des Zeichenmodus (*ftadm -fnc=c*)

CmdMode kann in der XML-Konfiguration des Fernadministrations-Servers an drei verschiedenen Stellen angegeben werden:

- als Parameter in *<Configuration>*: Diese Angabe ist die Voreinstellung für alle Instanzen und Gruppen, sofern dort keine individuellen Einstellungen vorliegen.

-
- als Parameter in <Group>: Diese Angabe überschreibt Voreinstellungen aus <Configuration> oder aus darüber liegenden Gruppen und gilt für alle Gruppen und Instanzen innerhalb dieser Gruppe, sofern diese keine individuellen Einstellungen haben.
 - als Parameter in <Instance>: Diese Angabe hat Vorrang gegenüber allen Voreinstellungen. Wenn es sich um eine Instanz handelt, die im Legacy-Modus arbeitet, wird automatisch der Modus *Transparent* angenommen, auch wenn für diese Instanz nichts explizit angegeben ist. Findet sich zu einer Instanz, die nicht im Legacy-Modus arbeitet, weder in der Instanz selbst noch in einer der Gruppen, zu der die Instanz gehört, noch in der Konfiguration eine *CmdMode*-Festlegung, so gibt es keine Empfehlung für den Modus.

Wenn das Attribut *CmdMode* gesetzt ist, muss die Version in <Configuration> mindestens 1210 sein. openFT V12.1 kann XML-Konfigurationsdateien der Vorversionen (z.B. mit der Versionsangabe 1100) importieren; beim Exportieren muss die Version jedoch auf 1210 gesetzt werden.

5.1.1.7 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 [Abschnitt „Konfigurationsdatei per Text- oder XML-Editor erstellen“](#).

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.

5.1.1.8 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.

i 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.

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 [Abschnitt „Konfigurationsdatei per Text- oder XML-Editor erstellen“](#).

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“](#) oder [Abschnitt „Konfigurationsdatei per Text- oder XML-Editor erstellen“](#).
3. Importieren Sie die geänderte Datei, z.B. mit *ftimpc xml-datei*, siehe auch [Abschnitt „Konfiguration importieren“](#).

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.

5.1.2 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 [Abschnitt „Konfigurationsdatei per Text- oderXML-Editor erstellen“](#).

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.

5.1.2.1 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-System:

```
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-System und z/OS) an.

5.1.2.2 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 [Abschnitt „Berechtigungsprofil für openFT-Instanz ab V11.0 konfigurieren“](#)).

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-System:

```
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)
```

5.1.3 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 [Abschnitt „Fernadministration über openFTExplorer“](#)) 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 \(Fernadministration über Kommando-Schnittstelle\)](#)".

5.1.3.1 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 [Abschnitt „Berechtigungsprofile für den Zugang zum Fernadministrations-Server einrichten“](#)) und der Profilname muss in der Konfigurationsdatei einem Fernadministrator zugeordnet sein (siehe [Abschnitt „Konfigurationsdatei per Text- oder XML-Editor erstellen“](#)).

Beispiel für die Ausgabe

```
TYPE      = *INSTANCE      ACCESS = FT+FTOP+FTAC / *CHAR
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 und - falls konfiguriert - der Codierungsmodus, siehe auch Beschreibung von *ftshwc*.

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 „Konfigurationsdatei per Text- oder XML-Editor erstellen“](#).

Geben Sie das Kommando *ftadm* in folgender Form ein:

```
ftadm -ri=instanz "kommando"
```

- Kommando *ftadm* auf fernem Rechner eingeben

Melden Sie sich auf dem fernem 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 [Abschnitt „Fernadministration über Kommando-Schnittstelle“](#).

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.

zugangsberechtigung

Nur auf fernem Rechner: FTAC-Zugangsberechtigung für den Zugang zum Fernadministrations-Server. Das zugehörige Profil muss die Eigenschaft ACCESS-TO-ADMINISTRATION besitzen (siehe [Abschnitt „Berechtigungsprofile für den \(Berechtigungsprofile für den Zugang zum Fernadministrations-Server einrichten\)](#)

[Zugang zum Fernadministrations-Server einrichten“](#) (Berechtigungsprofile für den Zugang zum Fernadministrations-Server einrichten)) und der Profilname muss in der Konfigurationsdatei einem Fernadministrator zugeordnet sein (siehe [Abschnitt „Konfigurationsdatei per Text- oder XML-Editor erstellen“](#)).

5.1.3.2 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 [Abschnitt „Berechtigungsprofile für den Zugang zum Fernadministrations-Server einrichten“](#)) und der Profilname muss in der Konfigurationsdatei einem Fernadministrator zugeordnet sein (siehe [Abschnitt „Konfigurationsdatei per Text- oder XML-Editor erstellen“](#)).

Wenn Sie auch die Option *Zugangsberechtigung abspeichern* aktivieren, dann hat dies den Vorteil, dass Sie die Zugangsberechtigung bei künftigen 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 [Abschnitt „Fernadministration über openFT Explorer“](#)) 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.

5.1.4 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,
- und mit dem Kommando *ftdell* löschen, sofern Sie die Berechtigung dazu haben.

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-Trap-Server konfigurieren](#)
- [ADM-Traps in der openFT-Instanz konfigurieren](#)
- [ADM-Traps ansehen](#)

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 [Abschnitt „ADM-Traps ansehen“](#).

- 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` (Unix-Systeme)
- `%ProgramData%\Fujitsu Technology Solutions\openFT\var\std\log\sysatpf` (Windows-Systeme)

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- und z/OS-Systeme finden Sie im openFT-Handbuch "openFT (BS2000) - Installation und Betrieb" und im Handbuch "openFT (z/OS) - Installation und Betrieb"

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 [Abschnitt „ADM-Trap-Server konfigurieren“](#).
- 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

i Aus Performancegründen 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.).
 - 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 „Fernadministration über Kommando-Schnittstelle“](#). 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. 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 [Abschnitt „Berechtigungsprofile für den Zugang zum Fernadministrations-Server einrichten“](#)) und der Profilname muss in der Konfigurationsdatei einem Fernadministrator zugeordnet sein (siehe [Abschnitt „Konfigurationsdatei per Text- oder XML-Editor erstellen“](#)).

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.

```
<Configuration
  Version="1210"
  Description="Konfiguration fuer zentralen Server MCHSRV01">
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  ;Nur an Unix-Systemen
  xsi:noNamespaceSchemaLocation="/opt/openFT/include/config.xsd">
  ;Nur an Windows-Systemen
  xsi:noNamespaceSchemaLocation="<openFT-installationsverzeichnis>/include/
  config.xsd"s
  <AdministratorID
    Name="Hans"
    Description="Verwalter der Domaenen Controller"
```

```
    UserID="rz\hans"
    Profile="Profil01"/>
  <AdministratorID
    Name="Fritz"
```

1.
2.

```

    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 10"
        Address="ftadm: //OPENFT01.mch.mycompany.net"
        Admission="openft01remote"/>
      <Instance
        Name="OPENFT02" 4.
        Description="Windows 10"
        Address="ftadm: //OPENFT02.mch.mycompany.net"
        Admission="openft02remote"/>
      <Instance
        Name="OPENFT03" 4.
        Description="Windows 10"
        Address="ftadm: //OPENFT03.mch.mycompany.net"
        Admission="openft03remote">
        <AccessList> 5.
          <AccessEntry
            AdministratorID="Hans"
            DenyFunction="FTMOD"/>
          </AccessList>
      </Instance>
      <Instance
        Name="MCHSRV02" 4.
        Description="SUSE SLES 11, 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>
        <AccessEntry
            AdministratorID="Hans"
            AllowFunction="FT FTAC"/>
        </AccessList>
    <Instance
        Name="MCHSRV03"
        Description="Windows Server 2016 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>
            <AccessEntry
                AdministratorID="Emil"
                AllowFunction="FT FTAC"/>
            <AccessEntry
                AdministratorID="Hugo"
                AllowFunction="FT FTAC"/>
        </AccessList>
        <Instance
            Name="HHWSRV01"
            Description="Solaris 10"
            Address="ftadm: //HHWSRV01.hhw.mycompany.net"
            CmdMode="Char"
            Admission="hhwsrv01remote"/>
        <Instance
            Name="HHWSRV02"
            Description="HP-11"
            Address="ftadm: //HHWSRV02.hhw.mycompany.net"
            Admission="hhwsrv02remote"/>
        <Instance
            Name="HHWSRV11"
            Description="Solaris 10"
            Address="HHWSRV11.hhw.mycompany.net"
            Admission="hhwsrv11remote"
            Mode="Legacy">
        <AccessList>
            <AccessEntry
                AdministratorID="Hugo"
                DenyFunction="FTAC"/>
        </AccessList>
    </Instance>
</Group>

```

```

<Group
  Name="HH2"
  Description="Personalabteilung">
  <AccessList>
    <AccessEntry
      AdministratorID="Emil"
      AllowFunction="FT FTAC"/>
    <AccessEntry
      AdministratorID="Hugo"
      AllowFunction="FTOP"/>
  </AccessList>
  <Instance
    Name="HHWSRV99"
    Description="Mainframe-System (BS2000) "
    Address="ftadm: //HHWSRV99.hhw.mycompany.net"
    Admission="hhwsrv99remote"/>
  </Group>
</Group>
</Configuration>

```

Erläuterung

1. Benutzererkennung, die auf dem Fernadministrations-Server die angegebenen Administratorrechte hat. Damit kann Fernadministration direkt am Fernadministrations-Server betrieben werden. Wenn hier keine Benutzererkennung 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*). Zusätzlich kann mittels *CmdMode* der Codierungsmodes festgelegt werden.
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 Fehlerbehebung und Diagnose

Dieses Kapitel enthält folgende Informationen:

- [Was tue ich, wenn ...](#)
- [Diagnoseunterlagen erstellen](#)
- [Trace-Funktion](#)
- [Weitere Diagnoseinformation](#)
- [Code-Tabellen](#)

6.1 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-Systeme automatisch erstellt).
- im Partnersystem der asynchrone openFT-Server nicht gestartet ist.
- eine Firewall im Partnersystem keine Verbindung zulässt.

i 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?
- Wenn Sie an einem Windows-System den TNS verwenden:
 - wurde für die lokale Adresse ein RFC1006-Eintrag mit TSEL \$FJAM gemacht?
 - wurde der lokalen Anwendung \$FJAM die Portnummer 1100 zugeordnet? Die Portnummer 102 sollte grundsätzlich nicht verwendet werden, da es zu Kollisionen mit anderen Anwendungspaketen kommen kann.
- 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 hosts-Datei (an Unix-Systemen */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 während Logging-Sätze geschrieben werden.
2. Volles Dateisystem beim Schreiben auf die Logging-Datei.
3. An Unix-Systemen: *kill* auf den openFT-Prozess während Logging-Sätze geschrieben werden.

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.

An Windows-Systemen können Sie zum Löschen der Logging-Datei z.B. den Windows-Explorer verwenden.

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.

Unix-System:

Bei der Standardinstanz lautet der Pfadname dieser Dateien:

`/var/openFT/std/config/sysfsa.dat`

und

`/var/openFT/std/config/sysfsa.idx`

2. Systemabsturz bei geöffneten `sysfsa`. *
3. An Unix-Systemen: `kill` auf den openFT-Prozess bei geöffneten `sysfsa`. *
4. An Unix-Systemen: volles Dateisystem bei ISAM-Zugriff

An Unix-Systemen hinterlässt ISAM bei Fall 2, 3 und 4 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.

Beispiel mit der Standardinstanz auf Unix-Systemen:

```
/opt/openFT/bin/ftbin/dcheck -b /var/openFT/std/config/sysfsa
```

Beispiel mit der Standardinstanz auf Windows 10-Systemen):

```
dcheck -b "C:\ProgramData\Fujitsu Technology  
Solutions\openFT\var\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:

Unix-System:

```
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
```

Windows-System:

```
cd C:\ProgramData\Fujitsu Technology Solutions\var\std\config  
ftstop  
move sysfsa.dat sav.sysfsa.dat  
del sysfsa.idx  
ftshwa  
del sysfsa.dat  
move sav.sysfsa.dat sysfsa.dat  
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

- An Windows-Systemen kann dies bei Kopplung zu Nicht-TCP/IP-Netzen vorkommen (z.B. X.25): Überprüfen Sie die Konfigurationseinstellungen für das jeweilige Transportsystem.
- 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 *ftshwa* 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.

... in Unix-Systemen 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.

... auf einem Windows-Terminalserver oder Windows-Server beim Start eines openFT Kommandos durch einen Benutzer die Meldung "Can't create termination event (error x). Command aborted." ausgegeben wird.

Das bedeutet, dass das entsprechende openFT Kommando wegen fehlender Rechte des Aufrufers bestimmte interne Objekte nicht einrichten kann und deshalb das Kommando nicht ausgeführt werden kann. Dieses Problem kann auf Windows-Terminalservern oder Windows-Servern auftreten, wenn der Gruppe der *Benutzer* das Recht zum *Erstellen globaler Objekte* fehlt. Um das Problem zu beheben, muss der Systemverwalter in der Rechteverwaltung des Betriebssystems der Gruppe *Benutzer* das Recht zum *Erstellen globaler Objekte* gewähren.

... sich in Windows-Systemen der openFT-Dienst nur beim Reboot des Systems starten lässt, nicht aber manuell, und der Benutzer die benötigten Verwalter-Rechte hat?

Im vorliegenden Fall erhalten Sie von Windows eine Fehlermeldung über eine fehlgeschlagene Initialisierung mit der Nummer 0xC0000022. Dies wird dadurch ausgelöst, dass in der Systemumgebungsvariablen PATH vor dem openFT-Installationspfad ein Pfad mit einem Netzlaufwerk bzw. ein UNC-Name oder ein Pfad mit Leerzeichen eingetragen ist. Falls der Dienst automatisch beim Booten des Systems gestartet wird, dann sind diese Einträge noch nicht aktiv und der Dienst startet normal. Später sind sie dann aktiviert und für SYSTEM mangels fehlender Rechte nicht zugreifbar.

Lösung:

Pfad bereinigen.

... es unter Windows zu Initialisierungsfehlern in user32.dll oder kernel32.dll kommt, wenn eine Folgeverarbeitung gestartet wird?

Ursache:

Die System-Umgebungsvariable PATH enthält nicht zugreifbare UNC-Pfade/Netzlaufwerke.

Lösung:

Pfad bereinigen und nur lokale zugreifbare Pfade verwenden.

Performance-Hinweis

Wenn Sie im Betrieb mit CMX den TNS verwenden (*ftmodo -tns=y*), dann sollten Sie bei den TNS-Einträgen 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.

6.2 Diagnoseunterlagen erstellen

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.
- Diagnoseinformation, siehe [Abschnitt „Weitere Diagnoseinformation“](#).
- 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 'BLANK'profilname'BLANK'-l*) und einen Ausdruck der Berechtigungssätze (*ftshwa'BLANK'@a*).
- Die Version und die Variante des Betriebssystems.
- Die Version des Kommunikationssystems (CMX, ...).
- Gegebenenfalls Prozesstabelle (*ps*-Kommando in Unix-Systemen).

An Unix-Systemen können Sie außerdem 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.

Auf Windows-Systemen steht zu diesem Zweck das Programm *diaginfo.exe* zur Verfügung.

6.3 Trace-Funktion

Dieser Abschnitt beschreibt, wie Sie Trace-Dateien erstellen und auswerten können.

6.3.1 Trace-Dateien

Zur Unterstützung der Fehlerdiagnose können Sie einen Überwachungszustand ein- und ausschalten.

6.3.1.1 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 [Abschnitt „Trace-Funktion ein-/ausschalten“](#).

Bei eingeschaltetem Überwachungszustand werden die Diagnosedaten in Trace-Dateien geschrieben. Die Trace-Dateien befinden sich im Dateiverzeichnis *traces* der jeweiligen openFT-Instanz.

Bei der Standardinstanz lautet der Pfadname wie folgt:

- auf an Unix-Systemen */var/openFT/std/traces*
- Auf Windows-Systemen
C:\ProgramData\Fujitsu Technology Solutions\openFT\var\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*.

Schnittstellen-Trace ein- und ausschalten (Windows-Systeme)

Sie können über den openFT Explorer zusätzlich den Schnittstellen-Trace einschalten. Dazu gehen Sie wie folgt vor:

1. Aktivieren Sie in *Administration - Betriebsparameter - Überwachung* die Option *Schnittstellentrace*.
2. Beenden Sie den openFT-Dienst über die Systemsteuerung und starten Sie ihn neu.

Das Ausschalten geht analog:

1. Deaktivieren Sie die Option *Schnittstellentrace* in *Administration - Betriebsparameter - Überwachung*.

2. Beenden Sie den openFT-Dienst über die Systemsteuerung und starten Sie ihn neu.

i Bitte beachten Sie, dass der Schnittstellen-Trace sehr umfangreich ist und den Ablauf von openFT verlangsamen kann. Daher sollten Sie den Schnittstellen-Trace nur dann einschalten, wenn dies zu Diagnosezwecken notwendig ist.

6.3.1.2 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. Die Trace-Dateien befinden sich im Dateiverzeichnis *traces* der jeweiligen openFT-Instanz.

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*. In Windows-Systemen sind Dateien mit der Endung *.PPE* Schnittstellen-Trace-Dateien.

Die Namen der Trace-Dateien haben folgendes Format:

- *Yoddhhmm.Sssccc.Pppppp.fttf*
Protokolltrace-Dateien von synchronen Outbound-Aufträgen.
- *Soddhhmm.Sssccc.I000.fttf*
Protokolltrace-Dateien des Kontrollprozesses.
- *Soddhhmm.Sssccc.Iiii.fttf*
Protokolltrace-Dateien der Serverprozesse, die asynchrone Outbound-Aufträge sowie Inbound-Aufträge abwickeln.
- *prozess-pid-thid-zeit.PPE* (Windows-Systeme)
Schnittstellen-Trace-Dateien. Dabei bedeuten *prozess* der Name des Prozesses, der das Kommando ausgeführt hat, *pid* die Prozess-Id in Hexadezimalzahlen, *thid* die Thread-Id in Hexadezimalzahlen und *zeit* die Zeit in Millisekunden seit Systemstart.

Erläuterung zu den Protokolltrace-Dateien

oddhhmm.Sssccc

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 *.Liii* geschrieben, z.B.:
S8101010.S33222.I001.fttf (erste Trace-Datei)
S8101010.S33222.I001.L001.fttf (Folgedatei)

6.3.1.3 Trace-Dateien aufbereiten mit `fttrace`

Einsatzhinweis

Funktion: Trace-Dateien aufbereiten

Benutzergruppe: FT-Benutzer und FT-Verwalter

Funktionsbeschreibung

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 der Optionen

-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 Folgeverarbeitungs-kommandos werden mit XXX überschrieben.
Standardwert, wenn `-s/` nicht angegeben wird.

h (high)

Passwörter, Benutzerkennungen, Zugangsberechtigungen,
Abrechnungsnummern, Folgeverarbeitungs-kommandos und Dateinamen werden mit XXX überschrieben.

i Bei der Ausgabe im Dumpformat (-d) gilt unabhängig von der Angabe in -s/ immer die niedrigste Sicherheitsstufe (-s/=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.

6.4 Weitere Diagnoseinformation

- Diagnosesätze ausgeben
- Meldungsdatei für Konsolkommandos
- Diagnoseinformationen mit diaginfo ausgeben (Windows-Systeme)

6.4.1 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.

6.4.2 Meldungsdatei für Konsolkommandos

Unix-Systeme

Konsolenausgaben kommen auf die Unix-Konsole. Zur Verfolgung über einen längeren Zeitraum werden diese von openFT erzeugten Konsolenausgaben zusätzlich auch in die *conslog*-Datei geschrieben. *conslog* liegt im Verzeichnis *log* der jeweiligen openFT-Instanz. 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.

Windows-Systeme

Zur diagnostischen Verfolgung von Konsolenausgaben werden diese auch in die Datei *conslog* ausgegeben. *conslog* liegt im Verzeichnis *log* der jeweiligen openFT-Instanz.

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

6.4.3 Diagnoseinformationen mit `diaginfo` ausgeben (Windows-Systeme)

Mit dem Kommando `diaginfo` können Sie weitere Diagnoseinformationen erstellen lassen. Starten Sie dazu `diaginfo` mit der Option `-a` und leiten Sie die Ausgabe in eine Datei um.

Beispiel: `diaginfo -a > diag.txt`

Diese Diagnosedatei können Sie dann dem Kundendienst zur Verfügung stellen.

6.5 Code-Tabellen

Die Codetabellen sind nützlich, um Umcodierungsfehler diagnostizieren zu können.

6.5.1 Code-Tabelle EBCDIC.DF.04

		oberes Halbbyte															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
unteres Halbbyte	0					SP	&	-	ø	Ø	°	μ	ϕ	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	¼	G	P	X	7
	8					ç	ì	Ç	Ì	h	q	y	½	H	Q	Y	8
	9					ñ	ß	Ñ	”	i	r	z	¾	I	R	Z	9
	A					·	! ^	:	«	ª	¡	¬	SHY	1	2	3	
	B					.	\$,	#	»	º	¿	[ô	ú	Ô	{	
	C					<	* %	@	ø	æ	Ð	\	ö	ü	Ö	Ü	
	D					()	_ '	´	´	¸	¸]	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)

6.5.2 Code-Tabelle ISO 8859-1

		oberes Halbbyte															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
unteres Halbbyte	0			SP	0	@	P	`	p			NBSP	°	À	Ð	à	ð
	1			!	1	A	Q	a	q			ı	±	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	Ê	Ú	ê	ú
	B			+	;	K	[k	{			«	»	Ë	Û	ë	û
	C			,	<	L	\	l				¬	¼	Ì	Ü	ì	ü
	D			-	=	M]	m	}			SHY	½	Í	Ý	í	ý
	E			.	>	N	^	n	~			®	¾	Î	Þ	î	þ
	F			/	?	O	_	o				¯	¿	Ï	ß	ï	ÿ

Code-Tabelle ISO 8859-1

7 Anhang

Dieses Kapitel enthält folgende Informationen:

- [Wichtige CMX-Kommandos \(Unix-Systeme\)](#)
- [Transportsystem-Anwendungen in TNS eintragen](#)
- [openFT im Cluster mit Unix-Systemen](#)
- [openFT-Instanzenkonzept im Windows-Cluster](#)
- [FarSync X.25 Transportsystem unter Linux- und Windows-Systemen](#)
- [Beispieldateien](#)

7.1 Wichtige CMX-Kommandos (Unix-Systeme)

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.

7.1.1 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`

7.1.2 *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 Für *datei* ist der Name einer Datei anzugeben, die die GLOBALEN NAMEN der TS-datei 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
```

7.2 Transportsystem-Anwendungen in TNS eintragen

Die Verwendung des Transport Name Service (TNS) für Kopplung über TCP/IP ist nicht 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“](#)).

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:

Unix-Systeme:

Rufen Sie das Skript */opt/openFT/bin/ftbin/ftgentns* auf.

Windows-Systeme:

Rufen Sie das Programm *createtns.exe* auf. *createtns.exe* befindet sich im Unterverzeichnis *bin\ftbin* des openFT-Installationsverzeichnis.

TNS-Einträge manuell erzeugen

Unix-Systeme:

Die Einträge in den TNS können mit Hilfe des TNS-Compilers *tnsxc* erfolgen. Dazu tragen Sie die TS-Anwendungen in eine Datei ein, die Sie mit Hilfe des TNS-Compilers *tnsxc* übersetzen (siehe [Abschnitt „tnsxc - TS-Directory erzeugen“](#)).

Einige Unix-Systeme 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.

Windows-Systeme:

TNS-Einträge erstellen Sie über die grafische Oberfläche *TNS User Interface*, die über die Programmleiste aufgerufen werden kann (*Start - Programme - PCMX-32 - TNS User Interface*).

Weiterhin kann es sinnvoll sein, die fernen TS-Anwendungen der Partnersysteme einzutragen, die Aufträge an das lokale System stellen. Es ist darauf zu achten, dass der Name, unter dem Aufträge mit diesem Partner abgewickelt werden, der

Instanzenidentifikation 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 in [Abschnitt „Definition der fernen TS-Anwendungen für openFT“](#) beschrieben.

TNS-Einträge bei Cluster-Konfiguration

i Beim Betrieb von Clustern mit openFT wird empfohlen, TNS und CMX nicht zu verwenden.

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). Beispiele hierzu finden Sie in [Abschnitt „Beispiel“](#) (Windows Systeme) bzw. in [Abschnitt „Beispiel 1: eine ausfallsichere Instanz“](#) und [Abschnitt „Beispiel 2: Ausfallsicherheit für beide Rechner des Clusters“](#) (Unix-Systeme).

7.2.1 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:

Unix-Systeme (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'
```

Windows-Systeme (Darstellung nach Export in eine Textdatei)

```

$FJAM\
    TSEL          OSITYPE T' $FJAM'
    TSEL          WANSBKA T' $FJAM'
    TSEL          WANFAR  T' $FJAM'
    TSEL          RFC1006 T' $FJAM'
    TSEL          LANINET A' 1100'
    APPTYPE       openFT
$FJAMOUT\
    TSEL          OSITYPE T' $FJAMOUT'
    TSEL          WANSBKA T' $FJAMOUT'
    TSEL          WANFAR  T' $FJAMOUT'
    TSEL          RFC1006 T' $FJAMOUT'
    TSEL          LANINET A' 1101'
    APPTYPE       openFT
$FTAM\
    TSEL          OSITYPE T' $FTAM'
    TSEL          WANSBKA T' $FTAM'
    TSEL          WANFAR  T' $FTAM'
    TSEL          RFC1006 T' $FTAM'
    TSEL          LANINET A' 4800'
    SSEL          V' '
    PSEL          V' '
    APPTYPE       openFT
TranSON\
    TA            RFC1006 127.0.0.1 PORT 4444 A' SOCKS4'
    APPTYPE       PROXY

```

*) Der Eintrag TranSON wird von PCMX-32 erzeugt.

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.

i *Windows-Systeme:* Ab openFT V11 wurde der Transport-Selektor der Anwendung \$FTAM von SNI-FTAM auf \$FTAM geändert.

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 *ftstdiscn* existieren, dann werden diese gelöscht.
- Alle anderen schon vorhandenen Einträge außer \$FJAM_OUTBOUND, *ftstd* oder *ftstdiscn* bleiben unverändert.

7.2.2 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.

Unix-Systeme:

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.

Windows-Systeme:

Sie nehmen die Einträge über die grafische Oberfläche des *TNS User Interface* vor.

Weitere Information dazu können Sie der Online-Hilfe zum *TNS User Interface* entnehmen.

Der GLOBALE NAME \$FTAM ist vorgegeben. Für den Transport-Selektor wird T'\$FTAM' empfohlen. P-Selektor und S-Selektor sind frei wählbar. Es wird empfohlen, das Leerformat zu verwenden, sofern es die Partner nicht anders verlangen.

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
```

7.2.3 Definition der fernen TS-Anwendungen für openFT

Es 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

- im TNS User Interface (Windows-Systeme)
- in der Datei, die mit dem TNS-Compiler *tnsxc* übersetzt wird oder (falls vorhanden) über die grafische Oberfläche (Unix-Systeme)

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.

7.2.3.1 Beispieleinträge für openFT-Partner (Unix-Systeme)

Die nachfolgend aufgeführten Beispiele setzen voraus, dass das entsprechende Transportsystem auf Ihrem Unix-Rechner unterstützt wird.

i Bitte beachten Sie, dass auf Unix-Systemen standardmäßig nur TCP/IP-RFC1006 vorhanden ist.

- Eintrag einer Partneradresse (für einen openFT (BS2000) 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 CMX- oder Windows-Partner:

```
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
```

7.2.3.2 Beispieleinträge für openFT-Partner (Windows-Systeme)

Die folgenden Beispiele werden mit dem *TNS User Interface* erstellt. *Kursiv* dargestellte Werte dürfen verändert werden.

- Eintrag einer Partneradresse für openFT (Windows) bei Transfer über TCP/IP-RFC1006:

Globaler Name ***ftwin***
Anwendungstyp openFT
P-Selektor <keiner>
S-Selektor <keiner>
T-Selektor TRANSDATA \$FJAM
Portnummer ***1100***
Proxy <keiner>
Rechnername ***transportsystemabhängig***

- Eintrag einer Partneradresse für openFT (BS2000) bei Transfer über TCP/IP-RFC1006:

Globaler Name ***ftbs2***
Anwendungstyp openFT
P-Selektor <keiner>
S-Selektor <keiner>
T-Selektor TRANSDATA \$FJAM
Portnummer ***102***
Proxy <keiner>
Rechnername ***transportsystemabhängig***

- Eintrag einer Partneradresse bei Transfer über TranSON:

Globaler Name ***fttranson***
Anwendungstyp openFT
P-Selektor <keiner>
S-Selektor <keiner>
T-Selektor TRANSDATA \$FJAM
Portnummer ***1100***
Proxy TranSON
Rechnername ***transportsystemabhängig***

Die globale Anwendung TranSON mit der Adresse des Proxy wird bei der Installation von PCMX-32 eingetragen.

-
- Eintrag einer Partneradresse bei Transfer über X.25:

Globaler Name	ftiso
Anwendungstyp	openFT
P-Selektor	<keiner>
S-Selektor	<keiner>
T-Selektor	TRANSDATA \$FJAM
Transportprotokoll-	
Identifikation	<leer> 1100
Subnetz	X.121
Transportprotokoll-	
klasse	Klasse2 (0 möglich)
X25-DTE-Adresse	transportsystemabhängig

7.2.4 Definition der fernen TS-Anwendungen für openFT-FTAM

i 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 oder X.25 erreichbaren Partnersysteme sind keine TNS-Einträge 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 an Unix-Systemen die Angabe `PSEL V ' '` oder `SSEL V ' '` und an Windows-Systemen die Angabe von *Leerformat* unbedingt erforderlich. Bei den Transportadressen für FTAM-Partner darf an Unix-Systemen 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 (Unix-Systeme)

Die Einträge der mit *tnsxcom* zu übersetzenden Datei müssen im Prinzip so aussehen, wie in den folgenden Beispielen in [Abschnitt „Beispieleinträge für FTAM-Partner \(Unix-Systeme\)“](#). 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 LAN Address	_____		
b)	called TSEL	_____	Code:	_____
c)	called SSEL	_____	Code:	_____
d)	called PSEL	_____	Code:	_____
e)	Protocol Identifier (Layer 3 CUD)	_____		
f)	called APT	_nein _____NILAPTtitle __ 1)		
g)	called AEQ	_nein _____ 1)		
h)	calling APT	_nein _____NILAPTtitle __ 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 LAN Address	_____		
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.

7.2.4.1 Beispieleinträge für FTAM-Partner (Unix-Systeme)

Die nachfolgend aufgeführten Beispiele setzen voraus, dass das entsprechende Transportsystem auf Ihrem Unix-Rechner unterstützt wird.

- 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 (Windows)

<= V10.0 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
```

7.2.4.2 Beispieleinträge für FTAM-Partner (Windows-Systeme)

Kursiv dargestellte Werte dürfen verändert werden.

- Eintrag einer FTAM-Partneradresse für openFT (Windows) ab V11 sbei Transfer über TCP/IP-RFC1006:

Globaler Name	<i>ftamwin</i>
P-Selektor	LEERFORMAT
S-Selektor	LEERFORMAT
T-Selektor	TRANSDATA \$FTAM
Portnummer	4800
Proxy	<keiner>
Rechnername	<i>transportsystemabhängig</i>

- Eintrag einer FTAM-Partneradresse für openFT(Windows) < V11 bei Transfer über TCP/IP-RFC1006:

Globaler Name	<i>ftamwina</i>
P-Selektor	LEERFORMAT
S-Selektor	LEERFORMAT
T-Selektor	ASCII SNI-FTAM
Portnummer	4800
Proxy	<keiner>
Rechnername	<i>transportsystemabhängig</i>

- Eintrag einer FTAM-Partneradresse für openFT (Unix-Systeme) bei Transfer über TCP/IP-RFC1006, wenn auf dem Unix-System CMX oder PCMX ab V4.0 im Einsatz ist:

Globaler Name	<i>ftamunix</i>
P-Selektor	LEERFORMAT
S-Selektor	LEERFORMAT
T-Selektor	TRANSDATA \$FTAM
Portnummer	4800
Proxy	<keiner>
Rechnername	<i>transportsystemabhängig</i>

- Eintrag einer Partneradresse für openFT-FTAM (BS2000) bei Transfer über TCP/IP-RFC1006:

Globaler Name	<i>ftambs2</i>
P-Selektor	LEERFORMAT
S-Selektor	LEERFORMAT
T-Selektor	TRANSDATA \$FTAM
Portnummer	102
Proxy	<keiner>
Rechnername	<i>transportsystemabhängig</i>

-
- Eintrag einer Partneradresse bei Transfer über TranSON:

Globaler Name	ftamtranson
P-Selektor	LEERFORMAT
S-Selektor	LEERFORMAT
T-Selektor	TRANSDATA \$FTAM
Portnummer	102
Proxy	TranSON
Rechnername	transportsystemabhängig

Die globale Anwendung TranSON mit der Adresse des Proxy wird bei der Installation von PCMX-32 eingetragen.

- Beispiel für eine Kopplung mit dem Rechner DEX

Der Partner verlangt die Selektoren im ASCII-Format, sendet aber selbst leere Selektoren in seiner Absenderadresse, wenn er die Initiative hat.

Globaler Name	dex
Namensteil 5	
P-Selektor	ASCII TS
S-Selektor	ASCII TS-SSAP
T-Selektor	ASCII TS-TSAPEAF
Rechnername	transportsystemabhängig

Der folgende Eintrag ist notwendig, wenn beim Rechner DEX die Initiative ist. Er dient ausschließlich zur Identifizierung eines Initiators.

Globaler Name	dex#01
Namensteil 5	
P-Selektor	<keiner>
S-Selektor	<keiner>
T-Selektor	ASCII TS-TSAPEAF
Rechnername	transportsystemabhängig

7.3 openFT im Cluster mit Unix-Systemen

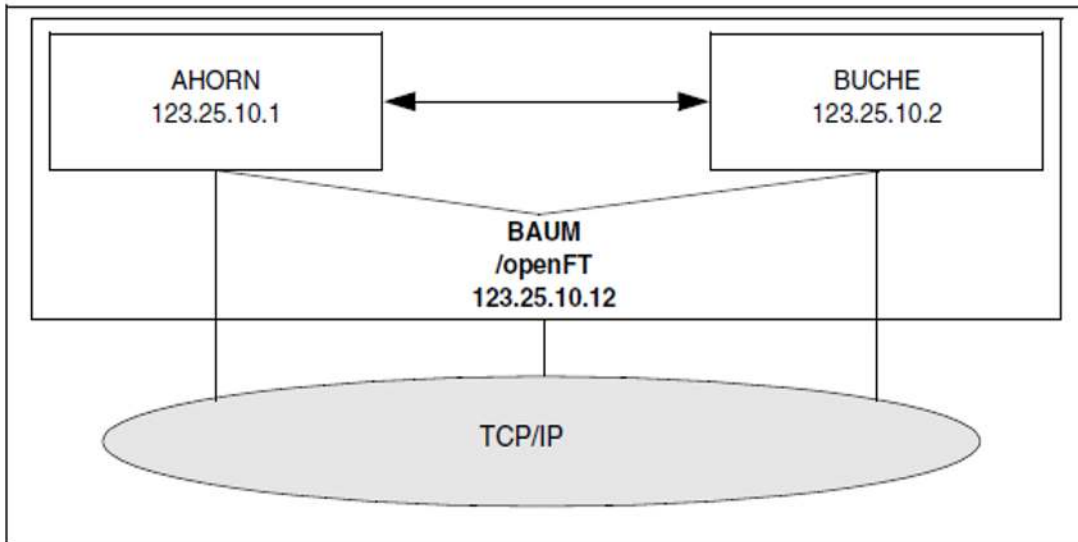
Software-Voraussetzungen

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“](#).

Es wird empfohlen, ohne CMX und TNS zu arbeiten.

7.3.1 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

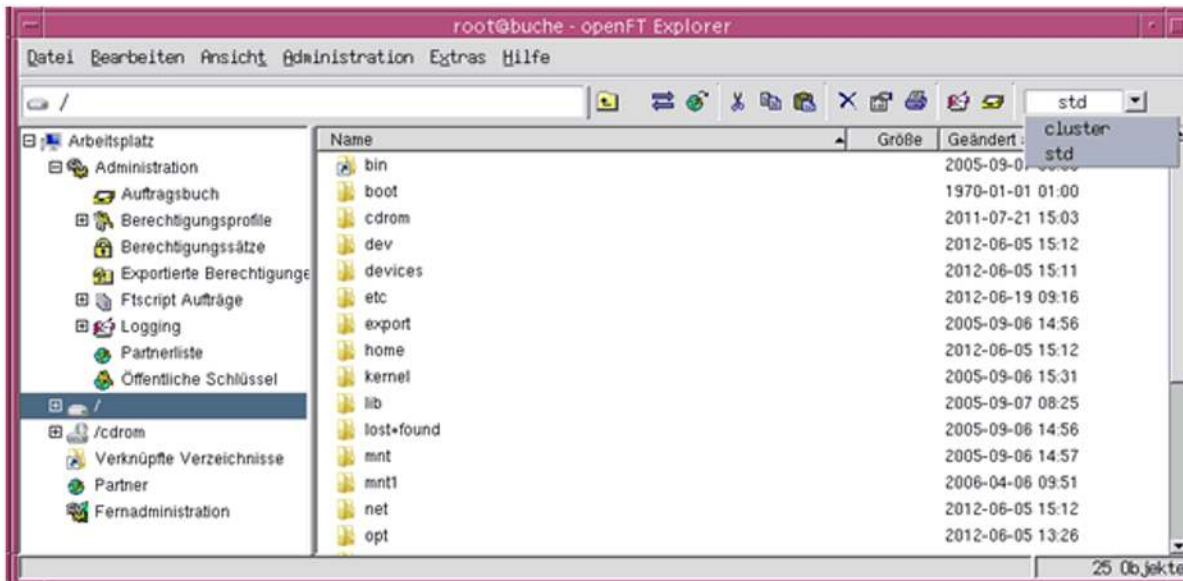
```

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 `. fseti 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

`. fseti 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.

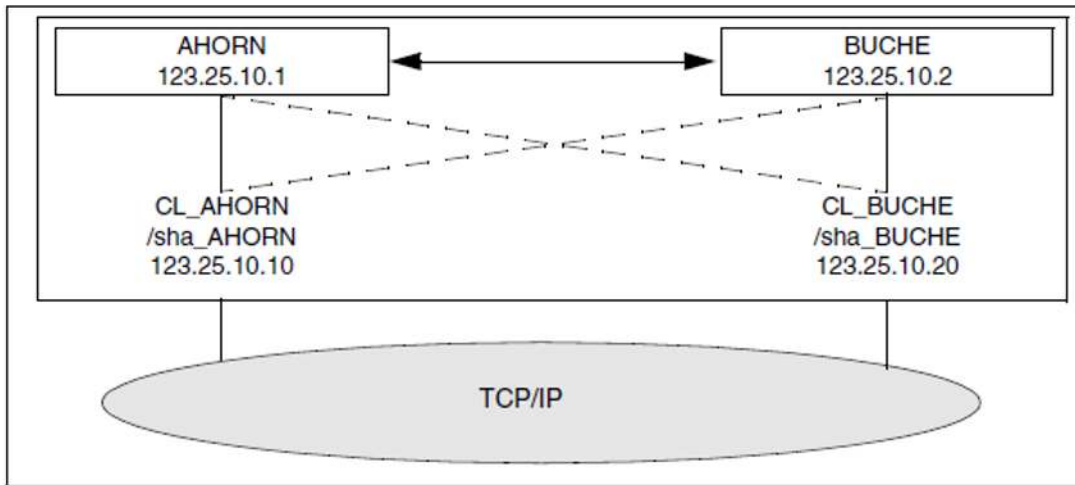


Instanz im Cluster auswählen

7.3.2 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 $? in
        0)exit 0;;
        1)exit 1;;
    esac;;
check) VALUE=`$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.

7.3.3 Hinweise zur Verwendung des TNS

Auf Solaris dürfen die TNS-Einträge nur TCP/IP-Bestandteile enthalten. Eine Eingabedatei für das Kommando *tnsxcn* 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 *tnsxcn* überschrieben.

7.4 openFT-Instanzenkonzept im Windows-Cluster

Software-Voraussetzungen

openFT (Windows) V12.1 (auf allen Knoten des Clusters muss die gleiche openFT-Version installiert werden).

Wenn Sie den TNS verwenden, dann muss CMX installiert sein der Betrieb mit CMX und TNS muss explizit per Betriebsparameter eingeschaltet sein, z.B. mit dem Kommando *ftmodo -tns=y -cmx=y*.

7.4.1 Beispiel

Es handelt sich um einen Windows-Cluster *OPENFT* mit der IP-Adresse 192.168.90.30, der aus zwei Knoten *P870_DDM* (Adresse 192.168.90.10) und *PN70_DDM* (Adresse 192.168.90.20) besteht. Es gilt:

- Auf jedem Knoten gibt es eine *std*-Instanz.
- Es gibt für beide Clusterknoten eine *cluster*-Instanz, die zu einem Zeitpunkt nur einem Knoten zugeordnet ist, da sie sich auf dem umschaltbaren Cluster-Laufwerk befindet.

Das bedeutet, dass es drei ansprechbare openFT's auf den beiden Knoten des Clusters gibt.

Das Ausfallkonzept besteht darin, dass die ausfallgesicherte *cluster*-Instanz (Hostname OPENFT) auf dem Rechner läuft, der aus Sicht des Clusters online ist (entweder *P870_DDM* oder *PN70_DDM*). Bei Verwendung der *std*-Instanzen auf den einzelnen Knoten ist zu beachten, dass diese nicht ausfallgesichert sind.

Der Windows-Cluster ist so zu konfigurieren, dass eine Platte immer verfügbar ist, die vom Cluster verwaltet wird (Physical Disk z.B. S:\openFT).

7.4.1.1 Installation von openFT

Installation auf dem ersten Knoten

openFT lokal installieren (ggf. inkl. Zusatzprodukt openFT-CR):

- Wählen Sie für alle Pfade immer eine lokale Platte (z.B. C:) aus.
- Starten Sie den Rechner neu. Hinterlegen Sie das Benutzerkennwort für openFT (*ftsetpwd* oder openFT Explorer, Menü *Administration*, Befehl *Benutzerkennwort*).
- Prüfen Sie, ob die Identifikation richtig gesetzt ist (*ftshwo* oder openFT Explorer) und korrigieren Sie sie ggf. (*ftmodo -id=* oder openFT Explorer).

Installation auf dem zweiten Knoten

openFT lokal installieren (ggf. inkl. Zusatzprodukt openFT-CR): siehe erster Knoten.

7.4.1.2 Konfiguration der ressourcen-spezifischen openFT-Eigenschaften des Clusters

Der Cluster muss so konfiguriert werden, dass ein Laufwerk, auf dem sich die umzuschaltenden openFT-Daten befinden, immer verfügbar ist (hier S:\).

Ein Beispiel zur Konfiguration der ressourcen-spezifischen openFT-Eigenschaften ist im [Abschnitt „Konfiguration der ressourcen-spezifischen openFT-Eigenschaften“](#) enthalten.

7.4.1.3 Konfiguration von openFT

Es wird empfohlen, ohne CMX und TNS zu arbeiten (*ftmodo -tns=n -cmx=n*, Standardeinstellung nach Neuinstallation).

Wird mit TNS gearbeitet, so muss dafür gesorgt werden, dass auf beiden Knoten des Clusters die TNS-Einträge identisch sind, bzw. die TNS-Einträge mit umgeschaltet werden.

Der asynchrone Server ist kein eigenständiger Dienst. Die Dienste *openFT* und *openFT Security Server* müssen immer gestartet sein.

Konfiguration auf dem ersten Knoten (P870_DDM)

- Asynchronen openFT-Server beenden: über *Administration - Asynchronen Server beenden* oder per Kommando *ftstop*
- Falls Sie im Betrieb mit CMX den TNS verwenden, müssen Sie die TNS-Einträge \$FJAM, \$FJAMOUT und ggf. \$FTAM anpassen (es dürfen nur TCP/IP Einträge enthalten sein).

- Adresse der *std*-Instanz setzen:

```
ftmodi std -addr=P870_DDM
```

- Asynchronen openFT-Server auf Instanz *std* starten: Instanz *std* auswählen und im openFT Explorer *Administration - Asynchronen Server starten* auswählen oder Kommando *ftstart* eingeben.
- Ersten Knoten online bringen (per Move Group).
- Neue Instanz

cluster erzeugen und überprüfen (*OPENFT* ist der Hostname des Clusters, *OPENFT.XYZ.NET* der zugehörige DNS-Name; das Verzeichnis *S:\openFT* muss existieren, das Verzeichnis *S:\openFT\cluster* darf nicht existieren):

```
ftcrei cluster S:\openFT\cluster -addr=OPENFT.XYZ.NET
ftshwi @a -l
Instance  Address          Directory
-----
cluster   OPENFT.XYZ.NET   S:\openFT\cluster
std       P870_DDM         C:\ProgramData\Fujitsu Technology Solutions\
openFT\var\std
```

ftcrei erzeugt einen neuen Dienst *openFT - cluster*. Dieser muss von der Cluster-Software bei Bedarf umgeschaltet werden.

- openFT Explorer neu starten, Instanz *cluster* in der Drop-Down-Liste des openFT Explorers auswählen und asynchronen openFT-Server automatisch starten: Im openFT Explorer unter *Administration - Betriebsparameter* die Option *Asynchronen Server automatisch starten* aktivieren.
Beim Start des Dienstes *openFT - cluster* wird automatisch der asynchrone openFT-Server gestartet.
- Benutzerkennwort der neu erzeugten Instanz über den openFT Explorer oder das Kommando *ftsetpwd* setzen.
- Falls in der Instanz *cluster* mit Authentifizierung gearbeitet werden soll, müssen Public Keys von Partnerrechnern im Verzeichnis *S:\openFT\cluster\syskey* hinterlegt bzw. der Public Key aus dem Verzeichnis *S:\openFT\cluster\config* den Partnerrechnern zur Verfügung gestellt werden.

Konfiguration auf dem zweiten Knoten (PN70_DDM)

- Asynchronen openFT-Server beenden (s. o.)

-
- Falls *TNS benutzen* aktiv: Anpassen der TNS-Einträge \$FJAM, \$FJAMOUT und ggf. \$FTAM (es dürfen nur TCP /IP Einträge enthalten sein)

- Adresse der *std*-Instanz setzen:

```
ftmodi std -addr=PN70_DDM
```

- Asynchronen openFT-Server auf Instanz *std* starten (s.o.)

- Zweiten Knoten online bringen

- Instanz

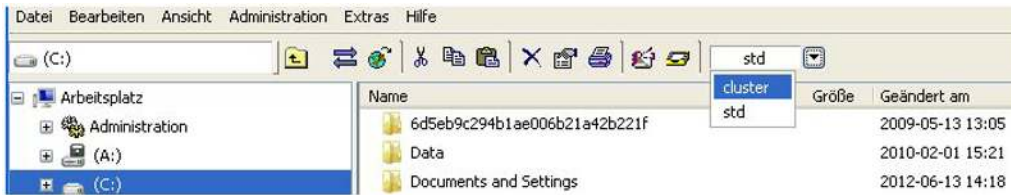
cluster aktivieren und überprüfen (es darf keine Adresse angegeben werden, da die Instanz schon existiert):

```
ftcrei cluster S:\openFT\cluster
ftshwi @a -l
Instanz      Adresse                Verzeichnis
-----
cluster      OPENFT.XYZ.NET         S:\openFT\cluster
std          PN70_DDM                C:\ProgramData\Fujitsu Technology Solutions\
openFT\var\std
```

7.4.1.4 Arbeiten mit den einzelnen openFT-Instanzen

1. Möglichkeit (openFT Explorer)

Setzen Sie die Instanz im openFT Explorer im Listenfeld oben rechts.



Instanz im Cluster auswählen

2. Möglichkeit (Kommandozeilen)

- Cluster *OPENFT* (ausfallgesichert) auf *P870_DDM* oder *PN70_DDM*, je nachdem, wo die Platte S:\ online ist:

```
ftseti cluster
```

... beliebiges openFT Kommando

```
ftcrep cluster1 FromOPENFT ...
```

```
ftshwl @a -nb=10
```

- Rechner *P870_DDM* (nicht ausfallgesichert):

```
ftseti std
```

... beliebiges openFT Kommando

```
ftcrep ahorn SendToP870_DDM ...
```

```
ftshwl -rc=@f
```

- Rechner *PN70_DDM* (nicht ausfallgesichert):

siehe Rechner *P870_DDM*

7.4.1.5 Arbeiten mit Windows-Cluster als openFT Server

- Bei Transfers mit dem ausfallgesicherten Windows-Cluster *OPENFT* muss der Hostname *OPENFT* bzw. die IP-Adresse 192.168.90.30 angesprochen werden, z.B.

```
ftshw OPENFT!. FromOPENFT -d
```

- Bei Transfers direkt zum Rechner *P870_DDM* (nicht ausfallgesichert) muss der Hostname *P870_DDM* bzw. die IP-Adresse 192.168.90.10 angesprochen werden, z.B.

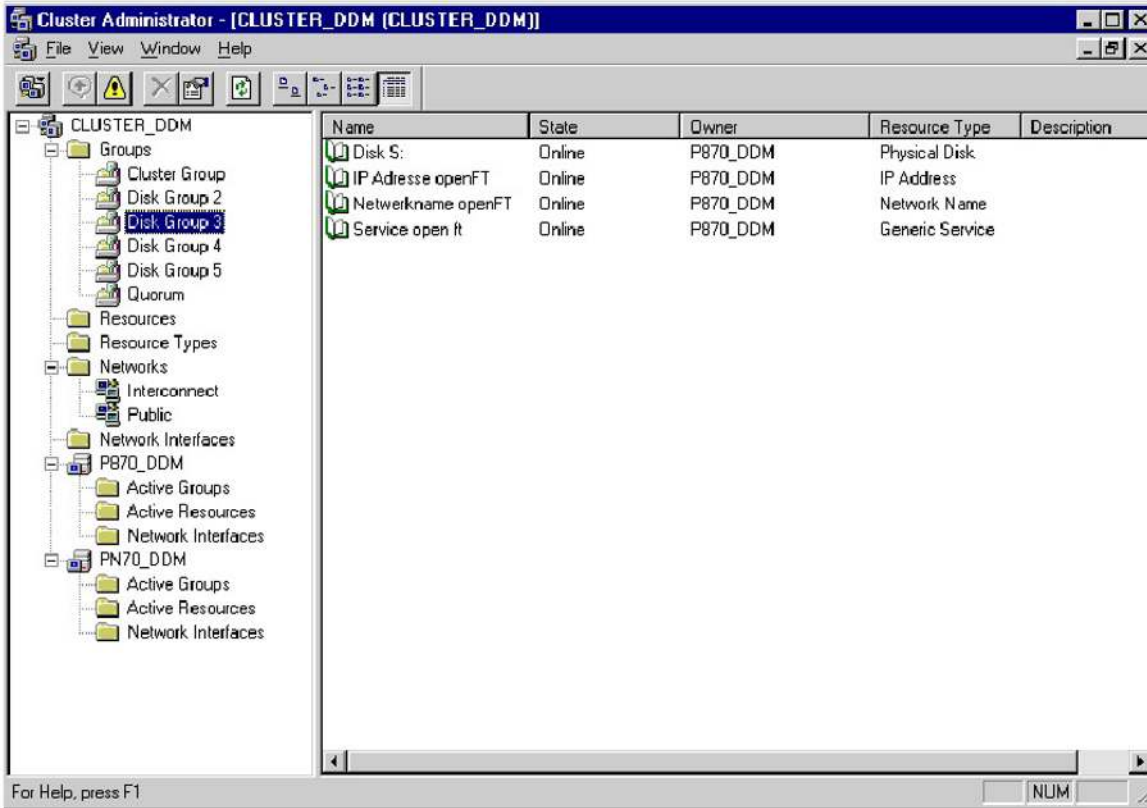
```
ncopy LocFile P870_DDM!RemFile SendToP870_DDM
```

- Bei Transfers direkt zum Rechner *PN70_DDM* (nicht ausfallgesichert) muss der Hostname *PN70_DDM* bzw. die IP-Adresse 192.168.90.20 angesprochen werden, z.B.

```
ncopy PN70_DDM!RemFile LocFile GetFromPN70_DDM
```

7.4.2 Konfiguration der ressourcen-spezifischen openFT-Eigenschaften

Über das Cluster-Administrator-Tool, das ein Bestandteil des Windows Servers ist, wird auf einem der beiden Knoten unter *Programs - Administrative Tools - Cluster Configuration* nun openFT im Cluster konfiguriert.

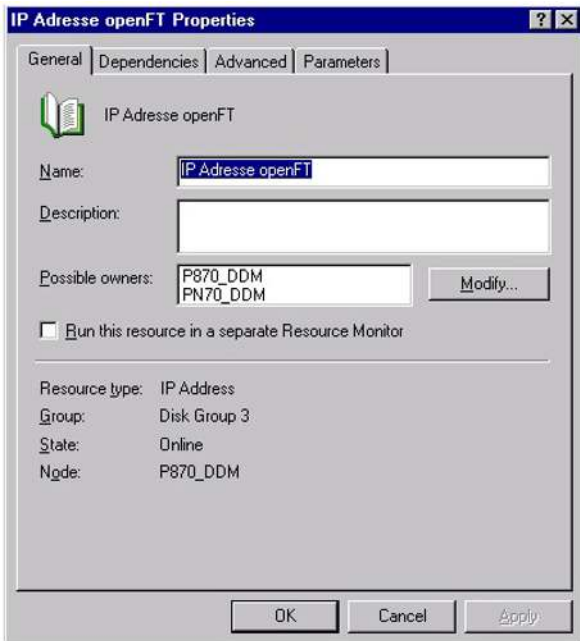


openFT im Cluster konfigurieren

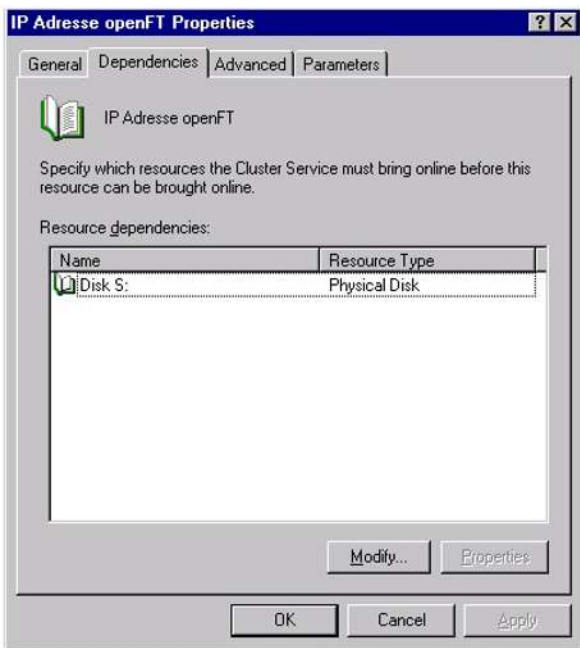
Die einzelnen Ressourcen sind mit folgenden Eigenschaften einzurichten:

1.	Name	z.B. IP Adresse openFT
	Resource Type	IP Adresse
	Dependencies	Physical Disk (hier Disk S:)
	Advanced	Standard oder anpassen
	Parameters	IP Adresse (und zwar diejenige, die ein openFT-Client benötigt, um den Cluster zu adressieren)

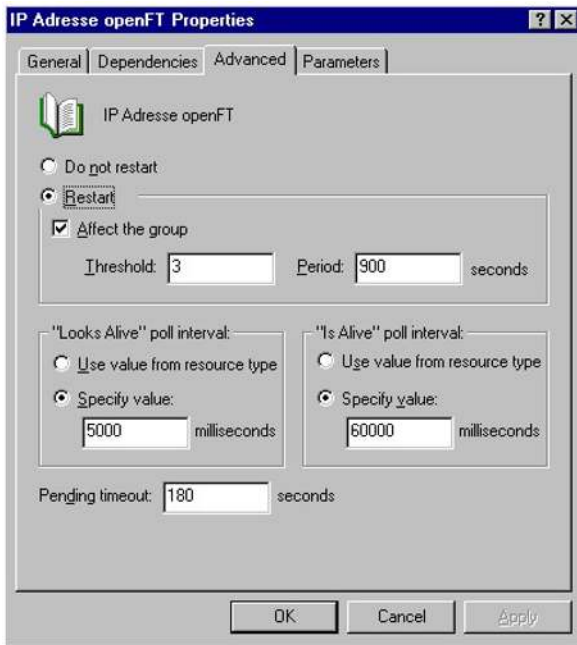
Mit *Apply* wird die Ressource erstellt und anschließend auf Online gesetzt (rechte Maustaste – *Bring Online*).



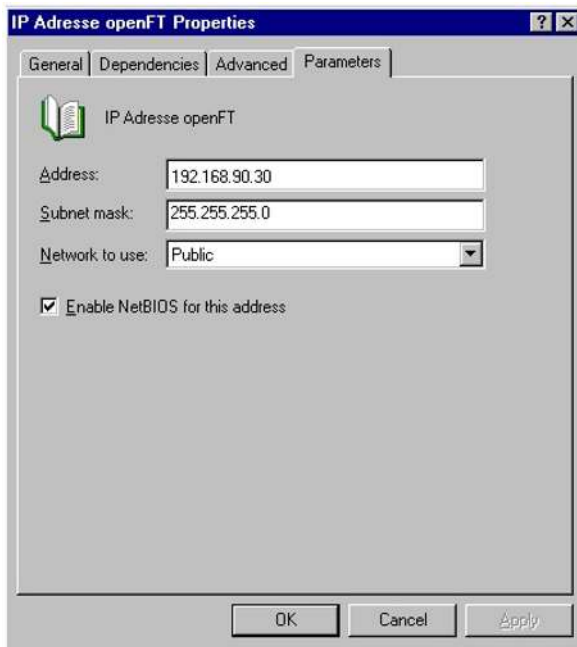
openFT im Cluster konfigurieren: IP Address - General



openFT im Cluster konfigurieren: IP Address - Dependencies



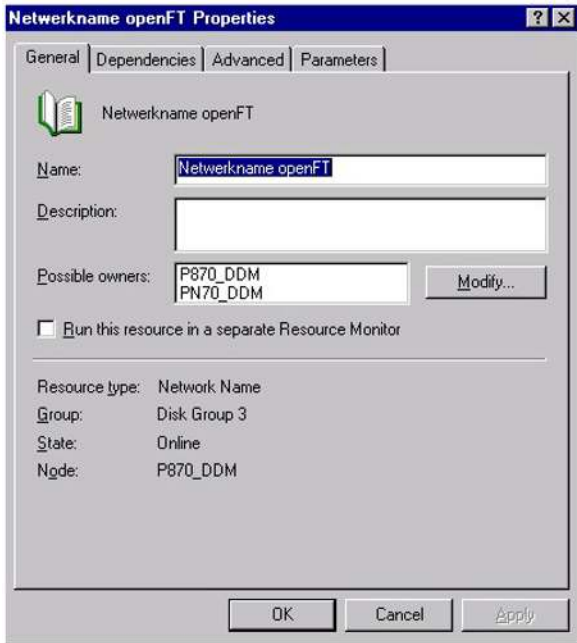
openFT im Cluster konfigurieren: IP Address - Advanced



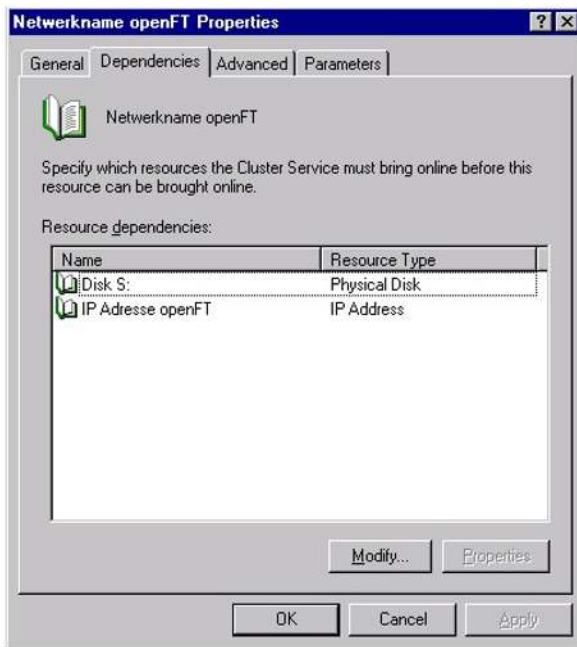
openFT im Cluster konfigurieren: IP Address - Parameters

2.	Name	z.B. Netzwerkname openFT
	Resource Type	Network Name
	Dependencies	Physical Disk (hier Disk S:) IP Adresse openFT
	Advanced	Standard oder anpassen
	Parameters	Name z.B. OPENFT

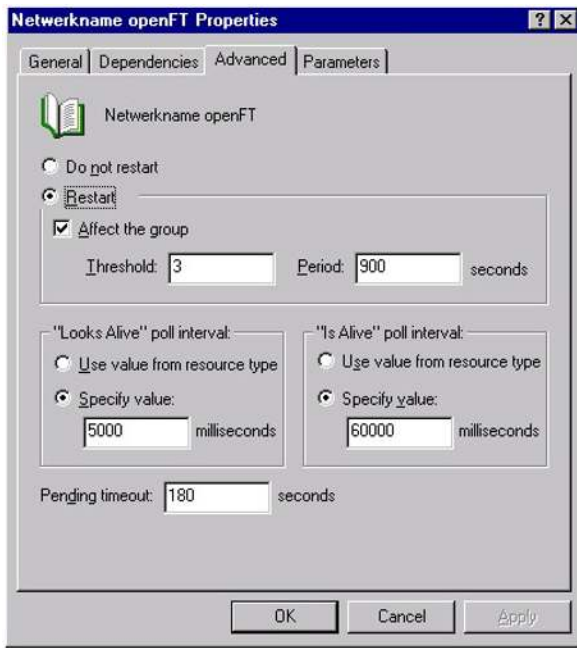
Mit *Apply* wird die Ressource erstellt und anschließend auf Online gesetzt (rechte Maustaste – *Bring Online*).



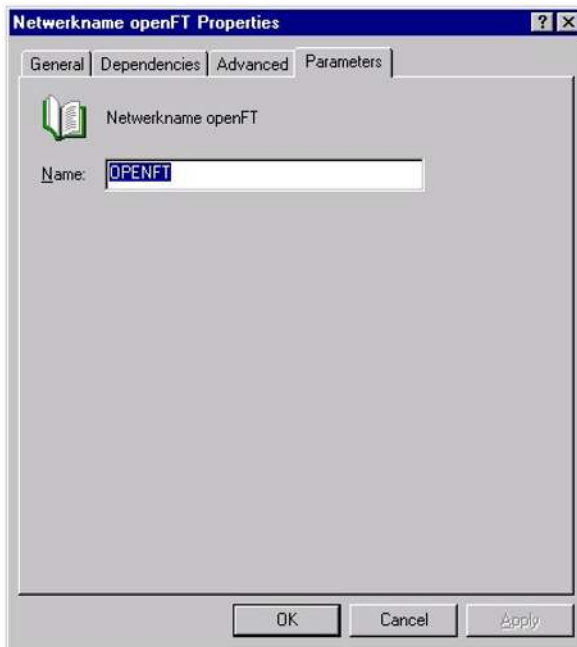
openFT im Cluster konfigurieren: Network Name - General



openFT im Cluster konfigurieren: Network Name - Dependencies



openFT im Cluster konfigurieren: Network Name - Advanced



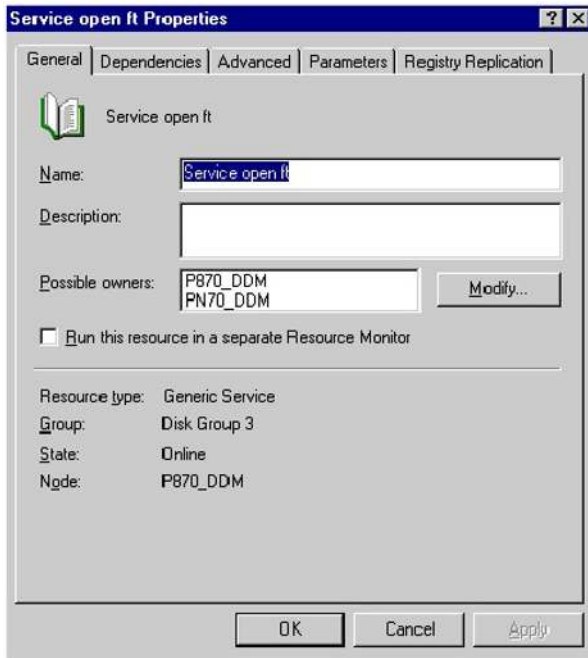
openFT im Cluster konfigurieren: Network Name - Parameters

Konfiguration des openFT Dienstes

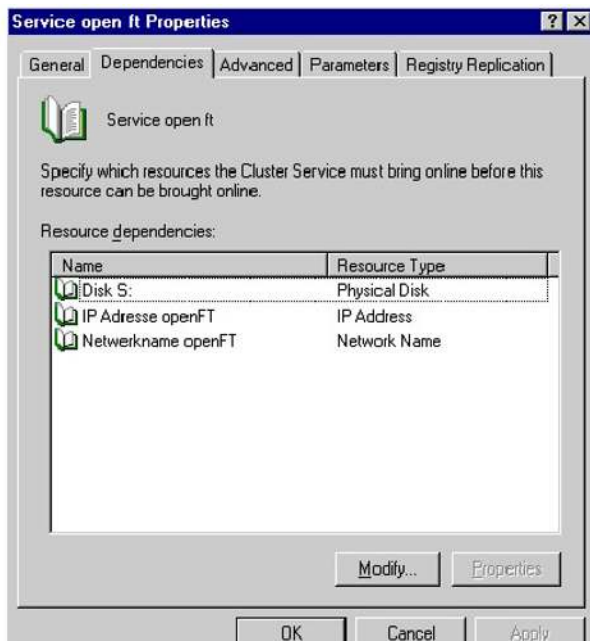
3.	Name	z.B. Service openFT
	Resource Type	Generic Service
	Dependencies	Physical Disk (hier Disk S:) IP Adresse openFT Netzwerkname openFT

Advanced	Standard oder anpassen
Parameters	Service name: openFT - cluster
Registry Replication	SOFTWARE\Classes\SNI\WINTNS (nur notwendig, wenn TNS verwendet wird)

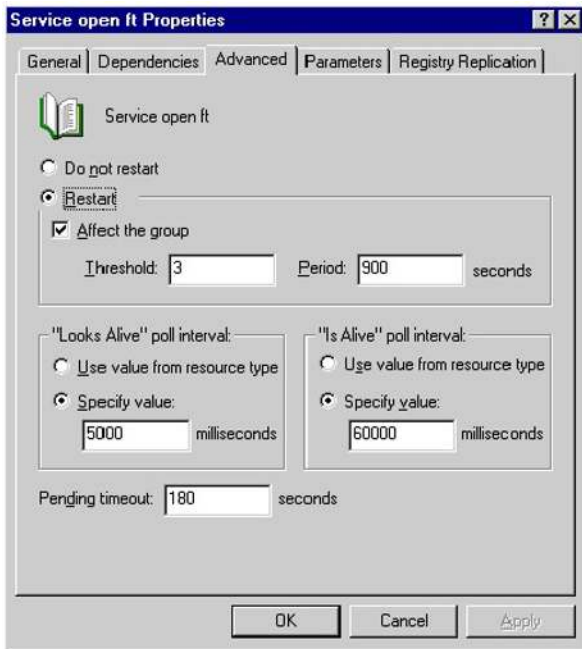
Mit *Apply* wird die Ressource erstellt und anschließend auf Online gesetzt (rechte Maustaste - *Bring Online*).



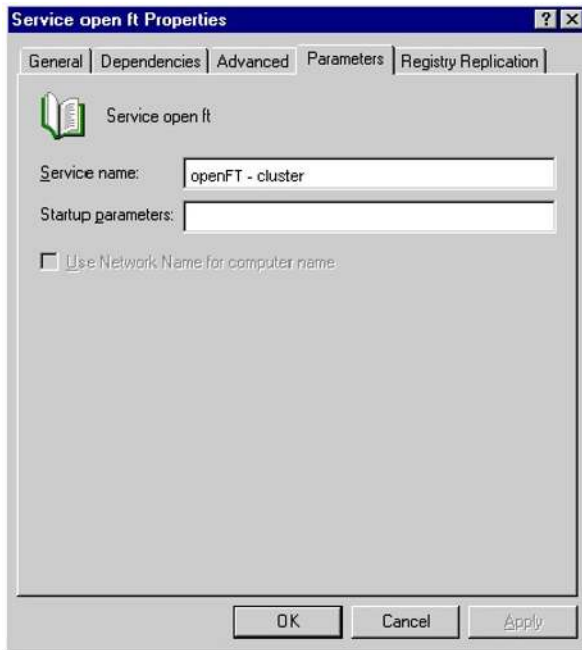
openFT im Cluster konfigurieren: Generic Service - General



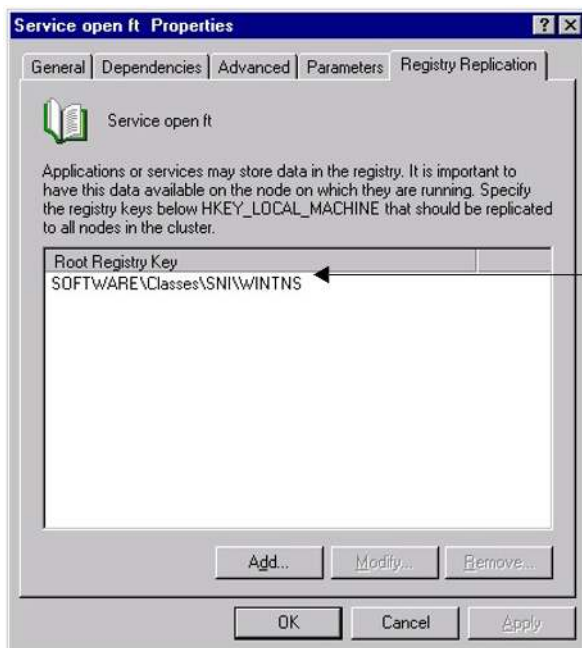
openFT im Cluster konfigurieren: Generic Service - Dependencies



openFT im Cluster konfigurieren: Generic Service - Advanced



openFT im Cluster konfigurieren: Generic Service - Parameters



Nur bei Betrieb mit CMX und TNS notwendig

openFT im Cluster konfigurieren: Generic Service - Registry Replication

Beim Betrieb ohne CMX und TNS muss keine Registry Replication durchgeführt werden.

7.5 FarSync X.25 Transportsystem unter Linux- und Windows- Systemen

Unter Linux- und Windows-Systemen werden FarSync X.25 Karten vom Hersteller FarSite direkt durch openFT unterstützt, d.h. die Konfigurationsdaten werden vollständig in openFT angegeben, PCMX wird dafür nicht (mehr) benötigt. Der CMX-lose Betrieb muss eingeschaltet sein (*ftmodo -cmx=n*).

Zusätzlich wird unter Linux durch den Einsatz der FarSync XOT-Runtime die Kopplungsmethode XOT (X.25 über TCP/IP) unterstützt.

Das Transportsystem X.25 kann vom openFT- und vom FTAM-Protokoll verwendet werden.

7.5.1 Direkte Unterstützung von FarSync X.25 für Windows-Systeme

Unter Windows-Systemen werden maximal 4 FarSync X.25 Karten (Adapter) mit jeweils maximal 4 Anschlüssen (Line) unterstützt. Insgesamt werden also 16 Anschlüsse unterstützt. Adapter und Anschlüsse werden von 0 – 3 durchnummeriert. Jeder Anschluss wird somit durch eine Kombination von Adapternummer und Anschlussnummer eindeutig indentifiziert (0-3).

Für den Einsatz mit openFT wird die jeweils aktuellste Version der FarSync X.25 Software für Windows-Systeme empfohlen. Diese ist derzeit:

- 4.2.0 ab Windows 7

7.5.2 FarSync X.25 Unterstützung für Linux-Systeme

Unter Linux wird für jeden Anschluss ein eigenes Gerät eingerichtet. Es werden maximal 16 Anschlüsse unterstützt. Die Anschlüsse werden von 0 – 15 durchnummeriert. Jeder Anschluss wird somit durch eine eigene Nummer eindeutig identifiziert.

Die mindestens benötigte Version der FarSync X.25 Software für Linux ist 3.2.9.

Die benötigte X.25 Software kann von folgender Seite heruntergeladen werden:

http://www.farsite.com/custsupp/Download_X.25_software.htm

XOT-Unterstützung

Für die Unterstützung von XOT (X.25 über TCP/IP) wird unter Linux mindestens die FarSync XOT-Runtime Version 3.2 benötigt. Damit ist über XOT eine Kopplung zum FarSync X.25 Gateway oder einem anderen Gerät eines beliebigen Herstellers, welches XOT unterstützt, möglich.

Die FarSync XOT-Runtime stellt unter Linux eine virtuelle X.25-Schnittstelle zur Verfügung. Die Konfiguration von openFT für die Nutzung der FarSync XOT-Runtime ist identisch mit der Konfiguration für die Nutzung der FarSync X.25-Karten. Um die XOT-Runtime anzusprechen, muss nur die Adapternummer (Standardwert: Adapter 0) des XOT-Adapters (der virtuellen X.25-Schnittstelle) angegeben werden. Zusätzlich ist im FarSync Konfigurationsprogramm ein Eintrag für das XOT-Routing zu erstellen, d.h. für abgehende Verbindungen muss eine Zuordnung zwischen einer DTE-Zieladresse und der IP-Zieladresse des XOT-Partners erstellt werden.

i Durch manuelle Änderungen in den Konfigurationsdateien der XOT-Runtime ist es möglich, mehrere XOT-Adapter zu nutzen. Aber wegen Problemen in der XOT-Runtime wird für openFT nicht empfohlen, mehrere XOT-Adapter zu nutzen.

7.5.3 FarSync X.25 Transportsystem in openFT konfigurieren

Das FarSync X.25 Transportsystem konfigurieren Sie über das Kommando *ftmodo*.

Jedem X.25-Anschluss auf der FarSync X.25-Karte können Sie dabei eine eigene DTE-Adresse zugeordnen, die bei abgehenden Verbindungen als DTE-Adresse des Absenders (Calling DTE Address) im X.25-Verbindungsaufbau gesendet wird. Die Zuordnung einer DTE-Adresse zu einem Anschluss ist optional. Wird einem Anschluss keine DTE-Adresse zugeordnet, dann wird im X.25-Verbindungsaufbau keine DTE-Absenderadresse mitgeschickt.

7.6 Beispieldateien

Mit openFT wird eine Reihe von Beispieldateien ausgeliefert, die Sie für unterschiedliche Zwecke einsetzen können. Sie finden diese Dateien nach der Installation von openFT im Verzeichnis

- */opt/openFT/samples* (Unix-Systeme)
- *openFT-installationsverzeichnis\samples* (Windows-Systeme)

ftadm

Die Datei *config.xml* enthält eine einfache Beispielkonfiguration zur Fernadministration. Dieses Beispiel können Sie als Vorlage verwenden und entsprechend Ihren Wünschen anpassen.

ftscript

Das Verzeichnis enthält Beispiele für die openFT-Script-Schnittstelle. Die Beschreibung der Schnittstelle finden Sie im Handbuch "openFT (Unix- und Windows-Systeme) - openFT-Script-Schnittstelle".

filedist.ftsc

Mehrere Dateien an verschiedene Partnersysteme verteilen.

transsuc.ftsc

Eine Datei an ein Partnersystem übertragen mit Folgeverarbeitung.

treecopy.ftsc

Einen kompletten Verzeichnisbaum an ein Partnersystem übertragen.

ftacct.xlt (Unix-Systeme)

Das Excel-Template demonstriert, wie Sie das CSV-Ausgabeformat der Logging-Kommandos auswerten und für Buchführungszwecke in Excel nutzen können.

ftapi

Umfasst die Dateien *sample1.c*, *sample2.c*, *sample3.c*, *sample4.c*, *sample5.c*, *sample6.c* und *sample7.c*.

Diese Beispiele zeigen verschiedene Einsatzmöglichkeiten für die C-Programmschnittstelle von openFT. Die Beschreibung der Beispiele finden Sie im Handbuch "openFT (Unix- und Windows-Systeme) - Programmschnittstelle".

sample1.c

Eine Datei asynchron übertragen.

sample2.c

Mehrere Dateien übertragen mit Folgeverarbeitung.

sample3.c

Den Inhalt eines fernen Verzeichnisses anzeigen.

sample4.c

Einen Befehl auf dem Partnersystem ausführen.

sample5.c

Die Dateiattribute aller Dateien eines fernen Verzeichnisses jeweils in Puffergröße in einer Schleife einlesen.

sample6.c

Verzeichnis im fernen System erzeugen.

sample7.c

Leeres Verzeichnis im fernen System löschen.

java

Umfasst die Dateien *Sample1.java*, *Sample2.java*, *Sample3.java*, *Sample4.java*, *Sample5.java*, *Sample6.java* und *Sample7.java*.

Diese Beispiele zeigen die Java-Programmschnittstelle von openFT. Wie Sie die Beispiele übersetzen und ablaufen lassen, ist im Handbuch "openFT (Unix- und Windows-Systeme) - Programmschnittstelle" beschrieben.

Sample1.java

Eine Datei asynchron übertragen.

Sample2.java

Mehrere Dateien übertragen mit Folgeverarbeitung.

Sample3.java

Den Inhalt eines fernen Verzeichnisses anzeigen.

Sample4.java

Einen Befehl auf dem Partnersystem ausführen.

Sample5.java

Die Dateiattribute aller Dateien eines fernen Verzeichnisses jeweils in Puffergröße in einer Schleife einlesen.

Sample6.java

Neues Verzeichnis im fernen System erzeugen.

Sample7.java

Leeres Verzeichnis im fernen System löschen.

treecopy-get, treecopy-send, treecopy-send-unique (Unix-Systeme)

Diese Shell-Skripte zeigen verschiedene Möglichkeiten zur Übertragung eines kompletten Verzeichnisses an Unix- oder Windows-Partnersysteme.

treecopy-get

alle Dateien eines Verzeichnisses per Vorverarbeitung aus einem Partner-System holen. Hier wird im fernen System Vorverarbeitung ohne explizite Angabe einer Zwischendatei verwendet.

treecopy-send

alle Dateien eines Verzeichnisses per Vorverarbeitung in ein tar-Archiv packen, an ein Partner-System übertragen und dort per Nachverarbeitung entpacken.

treecopy-send-unique

alle Dateien eines Verzeichnisses per Vorverarbeitung in ein tar-Archiv packen, an ein Partner-System übertragen und dort per Folgeverarbeitung entpacken.

Durch die Verwendung von %UNIQUE im Empfangsdateinamen können mehrere Skripte parallel ausgeführt werden.

msexcel (Windows-Systeme)

Das Verzeichnis enthält die Microsoft Excel-Dateien *ftaccnt.xlt* und *openft32.xls*.

ftaccnt.xlt

Microsoft Excel-Template (Microsoft Excel 2003 und 2007). Das Template demonstriert, wie Sie das CSV-Ausgabeformat der Logging-Kommandos auswerten und für Buchführungszwecke in Microsoft Excel nutzen können.

openft32.xls

fügt das Menü *openFT* mit den Befehlen *Transfer this File* und *Cancel Transmission* in die Menüleiste von Microsoft Excel ein. Die Datei enthält die zugehörigen Microsoft Visual Basic-Makros. Die Beschreibung der Makros wird eingeblendet, wenn Sie die Datei öffnen.

msword (Windows-Systeme)

Die Datei *openFT32.dot* ist eine Microsoft Word-Vorlage (Microsoft Word 2003 und 2007). Dokumente, die mit dieser Vorlage erstellt wurden, können sich selbst zu einem Partnersystem übertragen und ggf. dort ausdrucken. Die Vorlage muss dazu lokal auf Ihrem Rechner und auf dem Partnersystem im Verzeichnis für die Microsoft Word Vorlagen installiert werden.

openFT32.dot fügt das Menü *openFT* mit den Befehlen *Transfer Document*, *Cancel Transfer* und *Send Clipboard* in die Menüleiste von Microsoft Word ein. Die Datei enthält die zugehörigen Microsoft Visual Basic-Makros. Die Beschreibung der Makros wird eingeblendet, wenn Sie die Datei öffnen.

ocxdemo (Windows-Systeme)

Das Beispiel zeigt die Verwendung des OCX Control *fttrans.ocx*. Das Verzeichnis enthält die entsprechende Microsoft Visual Basic-Anwendung und den zugehörigen Source-Code. Die Beschreibung der OCX-Steuerung in openFT finden Sie in der Datei *Liesmich bzw. Readme* im Verzeichnis *ocxdemo* sowie im Handbuch "openFT (Unix- und Windows-Systeme) - Programmschnittstelle".

Durch den Aufruf von *ocxdemo.exe* wird die Microsoft Visual Basic Anwendung gestartet und das OCX-Control von openFT geladen.

shellext (Windows-Systeme)

Das Verzeichnis enthält die Programmbibliothek sowie die Installations- bzw. Deinstallationsdatei für die openFT Shell-Erweiterung. Mit der openFT Shell-Erweiterung können Sie auf dem Desktop vordefinierte Sendevorlagen erzeugen, um eine Dateiübertragung zu einem definierten Partner zu starten, indem Sie mit Drag and Drop die Datei aus dem Windows-Explorer auf die Sendevorlage ziehen.

Nach der Installation legen Sie eine neue Sendevorlage wie folgt an:

- Wählen Sie im Desktop-Kontextmenü unter *Neu* den Eintrag *openFT Sendevorlage*.

Auf dem Desktop wird ein neues Icon erzeugt, dessen Name verändert werden kann. Die Dateierweiterung *.openFTst* darf nicht vom Namen gelöscht werden. Anschließend können Sie die openFT-spezifischen Parameter konfigurieren.

- Klicken Sie mit der rechten Maustaste auf das Icon der Sendevorlage und wählen das Menü *Eigenschaften* aus. Das Dialogfenster *Eigenschaften* wird angezeigt.

Es enthält die folgenden zusätzlichen openFT-spezifischen Registerkarten:

openFT Allgemein

Angaben zum Partnersystem

openFT Optionen

Angaben zu den Optionen des Sendeauftrags

simple (Windows-Systeme)

Die Datei *ncopy.c* zeigt an Hand des Kommandos *ncopy*, wie Sie Kommandos aus einem Programm über die zugehörigen DLLs aufrufen.

www (Windows-Systeme)

Die Beispielprogramme in diesem Verzeichnis zeigen, wie Sie openFT für den Download im Internet oder einem Intranet nutzen können. Das Beispiel verwendet ein Windows-System als Client und ein Unix-System als Server-Plattform. Die ausführliche Beschreibung von Konzept und Realisierung finden Sie in der Datei *Liesmich* bzw. *Readme* im Verzeichnis *www*.