IBM Financial Transaction Manager for SWIFT Services for Multiplatforms
Version 3.2.4

Migration Guide

BBMP-0324-00

This edition applies to Version 3.2.4 Fix Pack 1 of IBM® Financial Transaction Manager for SWIFT Services for Multiplatforms (5725-X92).

Reference key: 20200930-1437

© Copyright International Business Machines Corporation 2020.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

About this publication v
Summary of changes v
Conventions and terminology used in this publication v

Part 1. Overview 1

Part 2. Planning FTM SWIFT 324 5

Part 3. Preparing to migrate to FTM SWIFT 324 7

Chapter 1. Installing FTM SWIFT 324 9
Granting access permissions to FTM SWIFT 324 users 9
Creating directory structures 9
Allocating and mounting file systems 9
Configuring the instance for runtime file system mount point 10
Creating the customization directory structure 10
Creating the runtime directory structure for the broker 11

Chapter 2. Preparing the customization environment 13
Preparing a CDP initialization file 13
Preparing a customization profile 13
Provide FTM SWIFT 300 customization meta data 14
Running the customization profile 14

Chapter 3. Preparing a runtime system on which a broker runs 15
Preparing a user profile for each runtime system on which a broker runs 15

Chapter 4. Collect grants of Db2 resources 17

Chapter 5. Prepare software integrity 19

Chapter 6. Prepare the data integrity framework 21

Chapter 7. Collect role assignments 23

Chapter 8. Prepare MER templates 25

Chapter 9. Creating deployment data for migration 27

Chapter 10. Modifying broker resources 29

Chapter 11. Backing up application server profiles 31

Chapter 12. Prepare update of FTM SWIFT 300 configuration entities 33

Part 4. Switching to FTM SWIFT 324 35

Chapter 13. Stopping message and file processing 37

Chapter 14. Backing up runtime database 39

Chapter 15. Deploying..... 41

Chapter 16. Update FTM SWIFT 300 configuration and security entities..... 43

Part 5. Verifying FTM SWIFT 324..... 47

Part 6. Cleaning up obsolete resources..... 51

Part 7. Migrating SAG Add-On..... 53

Chapter 17. Preparing..... 55

Chapter 18. Switching..... 57

Part 8. Handling migration problems..... 59

Chapter 19. Falling back to FTM SWIFT 300..... 61

Chapter 20. Re-migrating after falling back to FTM SWIFT 300..... 65

Chapter 21. Falling back SAG Add-On..... 67

Appendix A. Notices..... 69

Trademarks..... 70

Index..... 71

About this publication

This publication applies to the IBM Financial Transaction Manager for SWIFT Services Version 3.2.4 Fix Pack 1 (abbreviated to FTM SWIFT 324).

It describes how to migrate from IBM Financial Transaction Manager for SWIFT Services 3.0.0 Fix Pack 13 or Fix Pack 14 (abbreviated to FTM SWIFT 300) to FTM SWIFT 324.

Summary of changes

For a detailed description of changes and enhancements done with FTM SWIFT 324 refer to IBM Financial Transaction Manager for SWIFT Services 3.2.4 (Multiplatform) - Release Information.

Conventions and terminology used in this publication

The following variables are used in this publication:

old_inst_dir
The installation directory used for FTM SWIFT 300.
The default is `/opt/IBM/ftm/swift/v300`.

inst_dir
The installation directory used for FTM SWIFT 324.
The default is `/opt/IBM/ftm/swift/v324`.

old_cust_dir
The customization directory used by FTM SWIFT 300.
The default is `/var/ftmswift_v300/cus`.

cust_dir
The customization directory used by FTM SWIFT 324.
The default is `/var/ftmswift_v324/cus`.

old_run_dir
The runtime directory used by FTM SWIFT 300.
The default is `/var/ftmswift_v300/run`.

run_dir
The runtime directory used by FTM SWIFT 324.
The default is `/var/ftmswift_v324/run`.

deployment_dir
The directory in which deployment data and instructions are written by the CDP. It is specified in the CDP initialization file element `DeploymentDirectory`.
The default is `/var/ftmswift_v324/cus/depdata`.

DNIvDB01

The name of the FTM SWIFT 324 runtime database.

DNIvINST
The name of an FTM SWIFT instance.

DNIvOU
The name of a business OU.

DNIvSN
The schema name of the Db2® tables in the FTM SWIFT runtime database.

© Copyright IBM Corp. 2020

Part 1. Overview

If you used FTM SWIFT 300 and want to migrate to FTM SWIFT 324, you must migrate your software to more recent levels, then activate the new capabilities offered by the new software. An In-place (IP) migration is used to migrate an FTM SWIFT instance within its current customization and runtime environments, that is, within an environment that:

- Runs on the same operating system image
- Uses the same Db2 database subsystem
- Uses the same IBM MQ queue manager cluster
- Uses the same IBM Integration Bus message brokers
- Uses the same SAG workstations with an unchanged SAG version.
- Keeps the values of all existing variables and parameters. If a value can be changed it is explicitly described in this document.

Phases of an In-place migration

Figure 1 on page 1 illustrates the phases of an In-place migration.

Figure 1. In-place (IP) migration

It comprises the following phases:

Planning
Before you begin installing and migrating to FTM SWIFT 324, check which software levels are required, which steps and decisions you must take.

Preparing
Carry out all tasks that can be done in advance. The FTM SWIFT 300 environment is still used for processing and is not affected by this preparation activities.

Switching
Stop all processing in the FTM SWIFT 300 environment, execute deployment instructions, scripts and other executable files created during the preparation phase. In this phase your system can not process business messages.

Verifying
Determine whether the FTM SWIFT 324 environment was installed correctly and switching was successful. During this phase your system can not process business messages. However, at the end of this phase, after you successfully verified the migrated environment, you will restart your applications and resume processing.

Cleaning up
After you have verified that migration to FTM SWIFT 324 was successful, remove obsolete resources from your system.

Figure 2 on page 2 shows the phases in case of problems.

© Copyright IBM Corp. 2020

Figure 2. Handling problems

Falling back
If migration turns out to be unsuccessful, you can return to a state in which you can continue to use your FTM SWIFT 300 environment, if you have not yet begun to clean up the migration environment. In this phase your system can not process business messages.

Re-migrating
After falling back and solving whatever problems occurred, you can reattempt to migrate to FTM SWIFT 324.

Overview of the steps of an In-place migration

The overall migration consists of the following tasks:

1. Check the FTM SWIFT 300 PTF level of your current system.
2. Install the required FTM SWIFT 300 PTFs.
3. Check the software requirements for FTM SWIFT 324.
4. Install and upgrade products that do not cover the software requirements for FTM SWIFT 324. For example, upgrade your IBM Integration Bus V9 to IBM Integration Bus V10.
5. Migrate FTM SWIFT 300 to FTM SWIFT 324.
6. Check the software requirements for FTM SWIFT 324 SAG Add-On.
7. Install and upgrade products that did not cover the software requirements for FTM SWIFT 324 SAG Add-On. For example, upgrade your SAG.
8. Install the SAG Add-On.
9. Migrate your FTM SWIFT 300 SAG Add-On to the new FTM SWIFT 324 SAG Add-On.

Resources adapted in the preparation phase

After you installed FTM SWIFT 324, the following resources are prepared:

Customization definition document (CDD)
A new CDD is created from the existing FTM SWIFT 300 CDD.

Customization initialization file (ini-file)
A new ini-file is prepared.

Customization profile
A new customization profile is prepared.

Deployment data

The following resources are customized:

- Message flows
- WAS applications
- Database objects

Runtime profile
A new dniprofile is created.

Broker profile
A new broker profile (dniczbrk.sh) is created.

Changes applied in the switching phase

In the switching phase the following changes are applied to the existing system:

1. Db2: Implement changes to database objects.
2. Message Broker: The new FTM SWIFT 324 flows are deployed
3. WebSphere Application Server (WAS): The FTM SWIFT 324 applications are installed.
4. SAG Add-On: After you finished the FTM SWIFT 324 migration, the SAG Add-On has to be migrated. For details refer to Part 7, “Migrating SAG Add-On,” on page 53). Until you start to migrate the SAG Add-On, the SAG Add-On continues to work with FTM SWIFT 324.

IBM MQ resources are not changed.

Part 2. Planning FTM SWIFT 324

Before you begin installing and migrating to FTM SWIFT 324, you need to make decisions that will affect your setup. The tasks described in this section can be carried out at any time, and do not require any product code.

Before beginning the migration process:

1. Ensure that the software level of the FTM SWIFT 300 instance that is to be migrated is on Version 3.0.0, fix pack 13 or fix pack 14.

   One option to verify the installed level is to issue the following IBM Installation Manager command:

   ```
   ./imcl listInstalledPackages
   ```

   The command output contains information for all packages installed with IBM Installation Manager. The FTM SWIFT 300 related package name starts with *com.ibm.ftmswift*. The installed fix pack level is printed in italics in the example below. If you don't find the fix pack *13* or *14*, you are not on the correct fix pack level to perform the migration.

   ```
   com.ibm.ftmswift.mp.v300_3.0.13.20200729_1104
   ```

2. Ensure that your FTM SWIFT 300 uses software levels on customization and runtime systems that are supported by FTM SWIFT 324 as well. For details refer to Detailed hardware and software requirements for IBM Financial Transaction Manager offerings.
3. To become acquainted with the migration procedure, it is best to migrate to FTM SWIFT 324 on a test system before attempting to migrate on a production system.
4. Ensure that the persons with the following roles are available during customization and configuration:
   - IBM Integration Bus application developer
   - IBM Integration Bus administrator
   - Db2 administrator
   - Customizer
   - System configuration administrators
   - Security administrators
   - Data integrity administrator
   - WebSphere® Application Server operator (if the AO, MER, or RMA Facility is used)
   - WebSphere Application Server administrator (if the AO, MER, or RMA Facility is used)
5. Ensure that:
   - All system configuration and security administration changes are completed, that is, there are no outstanding commit, approve or deploy actions for those changes. For details refer to Ensure that no configuration or security administration change is pending.
   - No re-customization actions are outstanding. For details refer to Ensure that no customization operation is pending.
   - No PTF migration actions are outstanding.
6. If you use FTM SWIFT 324 nodes or message sets in your own message flows, or if you use modified FTM SWIFT sample message flows, you must plan to update your Toolkit environment and re-deploy your compiled message flows.
7. The default installation directory of FTM SWIFT 324 is `/opt/IBM/ftm/swift/v324`. However, you can choose any directory you like. This manual uses the abbreviation *inst_dir* to indicate this directory.

© Copyright IBM Corp. 2020

Part 3. Preparing to migrate to FTM SWIFT 324

Preparation steps are steps that can be performed while FTM SWIFT 300 is still running, namely:

- Installation of FTM SWIFT 324 programs
- Preparation of the customization environment
- Generation of customization deployment data for migration

Note: After the customization definitions are prepared, FTM SWIFT 300 must not be changed before the migration is completed.

© Copyright IBM Corp. 2020

Chapter 1. Installing FTM SWIFT 324

Migration fromFTM SWIFT 300 to FTM SWIFT 324is only possible by installing the FTM SWIFT 324 fix pack 1 (3.2.4.1) code. To install FTM SWIFT 324, refer to Installing FTM SWIFT.

Granting access permissions to FTM SWIFT 324 users

This description assumes that you continue to use all existing users and groups from FTM SWIFT 300.

To ease access for these groups, issue the following commands:

```
chgrp -R dniadmin inst_dir/admin
chgrp -R dnilpp inst_dir/run
chmod 755 inst_dir
chmod 750 inst_dir/admin
chmod 750 inst_dir/run
```

This gives the users in each of the specified groups access to the specified directories and all their subdirectories.

Table 1. Required access permissions to the customization programs, runtime programs, and data

Directory	Owner permissions	Owner group permissions	Other permissions	Owner group
inst_dir	r w x	r - x	r - x	Primary group of installer
inst_dir/admin	r w x	r - x	- - -	dniadmin
inst_dir/run	r w x	r - x	- - -	dnilpp
inst_dir/iFix	r w x	r - x	r - x	Primary group of installer

Creating directory structures

FTM SWIFT 324 requires various directories in a file system for customization and runtime data. It is recommended that you allocate separate file systems exclusively used by FTM SWIFT 324.

Allocating and mounting file systems

Table 2 on page 9 lists the file systems required by an FTM SWIFT instance.

Table 2. Default mount points and space requirements for file systems

File system	Applicable on	Default mount point name	Space requirements
customization file system	the customization system	cust_dir	At least 50 MB per instance.

© Copyright IBM Corp. 2020

Table 2. Default mount points and space requirements for file systems (continued)			
File system	**Applicable on**	**Default mount point name**	**Space requirements**
runtime file systems	each runtime system	`run_dir`	At least 50 MB for each file system for generic runtime data, plus the space you plan for storing traces. **Note:** If the file system becomes full and no trace information can be written, FTM SWIFT 324 stops processing messages.

The mount points are base directories in which you create subdirectories for certain FTM SWIFT 324 functions:

- You can choose your own mount point names.
- If your customization system and a runtime system are identical, you can use a common mount point for both.
- If more than one FTM SWIFT 324 instance is running in the same system, either each can have its own customization and runtime file systems, or they can share customization and runtime file systems. If they share file systems, instance segregation is ensured by the naming conventions.

Allocate and mount the file systems that FTM SWIFT 324 is to use.

Configuring the instance for runtime file system mount point

If you used a `dni.conf` file in FTM SWIFT 300 to configure the runtime file system mount point, you might want to adapt it for new FTM SWIFT 324 environment:

1. On the runtime system, log on as a system configuration administrator (sa1 or sa2).
2. Make a copy of your FTM SWIFT 300 `dni.conf` file to a location you note for later use during the migration procedure.
3. Ensure read access to group dnilpp.
4. Edit the copied file according to your needs. For example you might want to change the variables dnitrace or dniruntime.

Note: You will later on specify your runtime file system mount point in the directory names used in:

- The Broker Administration Program (BAP) directory in the environment variable `DNI_BAP_PATH` when you create the user profile in "Preparing a user profile for each runtime system on which a broker runs" on page 15
- The FSM instance directory when you configure the attribute `FSMInstanceDir` of the configuration objects of type `DnfLT`

Creating the customization directory structure

By default, FTM SWIFT 324 stores customization data in the directories shown in Table 3 on page 10.

Table 3. Directory structure for customization	
Description	**Default directory**
Customization definition document (CDD) directory used to store your CDDs.	`cust_dir/cdd`

Table 3. Directory structure for customization (continued)	
Description	**Default directory**
Customization definition directory used to store customization definition data.	`cust_dir/defs`
Deployment data directory used to store customization deployment data like instructions and vehicles you create.	`cust_dir/depdata`

To create the required customization directories and give read and write access to the group dnicusgr, ask the root user to issue the following commands:

```
mkdir cus_mount_point/cdd
mkdir cus_mount_point/defs
mkdir cus_mount_point/depdata
chgrp -R dnicusgr cus_mount_point
chmod -R 770 cus_mount_point
```

where *cus_mount_point* represents the name of the customization file system mount point you chose. The default is `cust_dir`.

Creating the runtime directory structure for the broker

Table 4 on page 11 lists the directories required on each runtime system, their default values and how you can customize them.

Table 4. Directory structure for the broker			
Directory Name	**Default directory**	**Customization possibility**	**Description**
cache directory	`run_dir/cache`	Set by the **dniruntime** variable in dni.conf with the appended subdirectory `/cache`.	Used to store temporary files.
trace directory	`run_dir/trace`	Set by the **dnitrace** variable in dni.conf.	Used to store trace files.
xfsm directory	`run_dir/trace/xfsm`	Set by the **dnitrace** variable in dni.conf with the appended subdirectory `/xfsm`.	Used to store trace files written by external SFD functions.
fsm instance directory	`run_dir/fsm`	Set by the `FSMInstanceDir` attribute of the `DnfLT` CO of the LT. **Note:** If more than one FTM SWIFT 324 instance runs on the same system, make sure each uses a different FSM instance directory.	Used to store temporary files, such as shared memory handles and trace files, written by internal SFD functions.

Table 4. Directory structure for the broker (continued)			
Directory Name	**Default directory**	**Customization possibility**	**Description**
bap directory	`run_dir/bap`	The directory specified by the **DNI_BAP_PATH** environment variable in the user profile (for example dniprofile) with the appended subdirectory `/bap`.	Used by the Broker Administration Program (BAP) to store information about deployed message flows for being able to maintain them later.

To create the required runtime directories and give read and write access to the group dnilpp, ask the root user to issue the following commands:

```
mkdir run_mount_point/cache
mkdir run_mount_point/bap
mkdir run_mount_point/trace
mkdir run_mount_point/trace/xfsm
mkdir run_mount_point/fsm
chgrp -R dnilpp run_mount_point
chmod -R 770 run_mount_point
```

where:

run_mount_point
The name of the runtime file system mount point you chose. The default is `run_dir`.

Chapter 2. Preparing the customization environment

Before the customization environment on the customization system can be used, you must prepare it.

Preparing a CDP initialization file

To create a separate Customization Definition Program (CDP) initialization file for each FTM SWIFT 324 instance:

1. On the customization system, log on as a customizer (ucust1).
2. Copy the initialization file template that is delivered with FTM SWIFT 324 to the directory `cust_dir` by issuing the following command:

   ```
   cp inst_dir/admin/samples/dniczcdp.ini cust_dir/DNIvINST.ini
   ```

3. Adapt the copy of the initialization file to your needs.

   Note: Do not change the order of the tags in the initialization file.

   - If you have used other directory names than those proposed in "Creating the customization directory structure" on page 10, change the value of the `dir` attributes of the `TraceFile`, `CustomizationDefinitionDirectory` and `DeploymentDirectory` elements.

   The elements and attributes contained in the file are described in Table 5 on page 13.

Table 5. Initialization file contents

Element	Attribute	Description
TraceFile	dir	Directory into which the CDP trace file and action log file are to be written.
	name	Name of the trace file.
CustomizationDefinitionDirectory	dir	Directory that contains proprietary files used by the CDP to regulate its internal processing. Do not edit these files.
DeploymentDirectory	dir	Directory in which deployment data and deployment instructions are to be written.
ServiceBundleSetFile This element occurs several times.	ccsid	The CCSID of the code page used by the service bundle files. Do not change this value.
	name	The name of the definition file for the service-bundle set. Do not change this value.

Preparing a customization profile

To create a separate customization profile for each FTM SWIFT 324 instance:

1. On the customization system, log on as a customizer (ucust1).
2. Copy the sample profile delivered with FTM SWIFT 324 to the directory `cust_dir` and give it a name that associates it with your instance by issuing the following command:

   ```
   cp inst_dir/admin/samples/dniczcus.prf cust_dir/dnicus_DNIvINST
   ```

3. Specify the access rights that allow another user (for example, the Db2 administrator) to access this file:

   ```
   chmod 775 cust_dir/dnicus_DNIvINST
   ```

© Copyright IBM Corp. 2020

4. Adapt the profile to your needs:
   - Modify the setting of environment variable DNICINIFILE to point to the initialization file specified in step “2” on page 13 in “Preparing a CDP initialization file” on page 13.
   - If you installed FTM SWIFT 324 in a directory other than `inst_dir`, adapt the setting of environment variable DNI_PATH.
   - Ensure that environment variable DNI_JAVA is set to the Java™ home directory for 64-bit, for example:

     ```
     DNI_JAVA=/usr/java8_64/jre
     ```

Provide FTM SWIFT 300 customization meta data

Copy the FTM SWIFT 300 CDP metadata to FTM SWIFT 324, for example:

```
cp -p -r old_cust_dir/defs cust_dir/defs
```

Running the customization profile

To run the customization profile of an instance:

1. On the customization system, log on to the system as a customizer (ucust1).
2. Change to the directory `cust_dir`
3. Run the profile by entering the following command:

   ```
   . ./dnicus_DNIvINST
   ```

Now you are able to perform customization tasks.

Note: To cause the profile to be run automatically each time you log on, add it to your .profile or other startup file.

Chapter 3. Preparing a runtime system on which a broker runs

Before a runtime system on which a broker runs can be used, you must prepare it.

Preparing a user profile for each runtime system on which a broker runs

To prepare a new profile for each runtime system on which a broker runs:

1. On each runtime system, log on as an FTM SWIFT security administrator (ua1 or ua2) or system configuration administrator (sa1 or sa2).
2. Copy the sample profile to the directory `run_dir`. To do this, issue the following command:

   ```
   cp inst_dir/run/samples/dniczpro.prf run_dir/dniprofile
   ```

   Note: The name `dniprofile` is used throughout this manual. If you chose a different name for this profile, use that instead.
3. For most of the environment variables in the `dniprofile` file you **must** reuse the values from your FTM SWIFT 300 dniprofile, except for DNI_PATH and DNI_BAP_PATH:

Environment variable	Value to be used	Description
DNI_I	Your current instance	Default instance used by the CLI.
DNI_OU	Your OU	Default OU used by the CLI.
DNI_S	Your service	Default service used by the CLI.
DNI_QM_$DNI_I	Your current queue manager	Queue manager of the broker to which this profile applies.
DNI_SN	Your current Db2 schema name	Schema name of the FTM SWIFT 300 runtime database tables.
DNI_DSN	Your current Db2 location	Location of the FTM SWIFT 300 runtime database.
DNI_PATH	*inst_dir*	Installation directory of FTM SWIFT 324.
DNI_CONFPATH	Your current directory, for example `/etc`	Directory that contains the FTM SWIFT 300 configuration file (`dni.conf`) that defines the runtime directories that are to be used. This environment variable needs to be set only if runtime directories other than the default runtime directories are used. Ensure that the variable is not preceded by a hash character (#). For more information, refer to “Configuring the instance for runtime file system mount point” on page 10.
DNI_BAP_PATH	*run_dir*	Directory that contains the **/bap** subdirectory in which files that are generated during use of the BAP are stored. Use the value from “Creating the runtime directory structure for the broker” on page 11.

© Copyright IBM Corp. 2020

Environment variable	Value to be used	Description
DB2_PATH	Your current Db2 path, for example `/opt/IBM/db2/V11.1`	DB2 installation directory. The value is used to extend the environment variables LIBPATH and CLASSPATH.
DNI_JAVA_PATH	Your current Java path, for example `/usr/java8_64/jre`	Java installation directory.
DNI_WMQ_PATH	Your current IBM MQ path, for example `/usr/mqm`	Installation directory of IBM MQ.
DNI_WMB_PATH	Your current IBM Integration Bus path, for example `/opt/IBM/mqsi/10.0.0.15`	Installation directory of IBM Integration Bus.

4. Specify the access rights that allow other users to access this file:

```
chgrp dnilpp run_dir/dniprofile
chmod 750 run_dir/dniprofile
```

Chapter 4. Collect grants of Db2 resources

If you added own permissions to any of the following Db2 views you should note them now. It is required to GRANT them again later in the migration procedure.

Permissions needed during deployment sequence

- DNIvSN.DNF_MWHFN_DNIvOU
- DNIvSN.DNIV_A_US_DNIvOU

© Copyright IBM Corp. 2020

Chapter 5. Prepare software integrity

FTM SWIFT 324 uses a new code signing certificate for its Software Integrity Checker.

To enable the FTM SWIFT 324 Software Integrity Checker to use the new signing certificate, the following steps are required.

1. On the runtime system, log on as data integrity administrator.
2. Run the FTM SWIFT 300 profile `dniprofile` by entering the following command:

   ```
   . old_run_dir/dniprofile
   ```

3. Copy the certificate keystore files used by FTM SWIFT 300:
   - Copy the certificate keystore files to the FTM SWIFT 324 installation or runtime system, for example:

     ```
     cp -p old_run_dir/ftmswift_keystore.jks run_dir/
     ```

   - If the customization system is separated, copy the certificate keystore files to the FTM SWIFT 324 customization system, for example:

     ```
     cp -p old_cust_dir/ftmswift_keystore.jks cust_dir/
     ```

4. Delete the signing certificate used by FTM SWIFT 300 from the copied certificate keystore files:

   ```
   keytool -delete -alias ftmswift -keystore ftmswift_keystore.jks -storepass password
   ```

   where:

   keystore
   The file name of the new keystore.

   password
   The keystore password when importing the signing certificate to FTM SWIFT 300

   For example:

   ```
   keytool -delete -alias ftmswift -keystore /var/ftmswift_v324/run/ftmswift_keystore.jks
                   -storepass password
   ```

5. Import the FTM SWIFT 324 signing certificate into the copied certificate keystore files:

   ```
   keytool -import -alias ftmswift -file inst_dir/sub_dir/cert/FTMSWIFT.cer
           -keystore ftmswift_keystore.jks -storepass password
   ```

   where:

   inst_dir
   The directory where FTM SWIFT 324 is installed

   sub_dir
   The subdirectory that includes the certificate directory. Possible values:

   run
   Specify this value if you create the keystore file on the installation or runtime system

   admin
   Specify this value if you create the keystore file on the customization system

   keystore
   The file name of the keystore to be created

   password
   The keystore password when importing the signing certificate to FTM SWIFT 300

© Copyright IBM Corp. 2020

For example:

```
keytool -import -alias ftmswift
        -file inst_dir/run/cert/FTMSWIFT.cer
        -keystore /var/ftmswift_v324/run/ftmswift_keystore.jks -storepass password
```

6. Copy and adapt Java policy files used by FTM SWIFT 300:
   a. Copy your Java policy file for the installation or runtime system, for example:

      ```
      cp -p old_run_dir/ftmswift.policy run_dir/
      ```

   b. If the customization system is separated, copy your Java policy file for the FTM SWIFT 324 customization system, for example:

      ```
      cp -p old_cust_dir/ftmswift.policy cust_dir/
      ```

   c. Change the *keystore* entry in the copied Java policy files to point to the FTM SWIFT 324 keystore file.

      For example:

      ```
      keystore "file:old_run_dir/ftmswift_keystore.jks", "jks";
      ```

      is changed to

      ```
      keystore "file:run_dir/ftmswift_keystore.jks", "jks";
      ```

Chapter 6. Prepare the data integrity framework

If you have activated the data integrity framework in FTM SWIFT 300, the vault must be made available to FTM SWIFT 324.

Copy the vault file used by FTM SWIFT 300, for example:

```
cp -p old_run_dir/ftmswift_vault.jceks run_dir/
```

© Copyright IBM Corp. 2020

Chapter 7. Collect role assignments

If you assigned users to FTM SWIFT 324 security role *DnfVerifAdmin*, you must note them now because you must recreate these assignments later on in the migration procedure. The assignments to security roles *SWIFTNetInterActSender* and *SWIFTNetInterActSnFOperator* must be noted to enable deletion of these roles during the cleanup sequence.

1. Log on to your runtime system as a security administrator (ua1 or ua2)
2. Enter the following commands for all of your OUs:

```
dnicli -i DNIvINST -ou OneOfYourOUs -s DNI_SECADM -c "list -user % -lo nb" | grep
DnfVerifAdmin
dnicli -i DNIvINST -ou OneOfYourOUs -s DNI_SECADM -c "list -user % -lo nb" | grep
SWIFTNetInterActSender
dnicli -i DNIvINST -ou OneOfYourOUs -s DNI_SECADM -c "list -user % -lo nb" | grep
SWIFTNetInterActSnFOperator
```

3. Note the role assignments for each of the business OUs

© Copyright IBM Corp. 2020

Chapter 8. Prepare MER templates

This section applies only if you started migration from IBM Financial Transaction Manager for SWIFT Services 3.0.0 Fix Pack 13, and if you use the MER facility.

1. On the runtime system, log on as a user with access rights as described in migtpl.
2. Run the FTM SWIFT 300 profile `dniprofile` by entering the following command:

   ```
   . old_run_dir/dniprofile
   ```

3. Run the following command to migrate templates. If it finds, for example, templates using the fin2017 message definition set, they are migrated to use the fin2018 message definition set.

   ```
   dnpadm.sh migtpl -outputfile migrated.csv
   ```

For more information, see MER administration utility migtpl command.

© Copyright IBM Corp. 2020

Chapter 9. Creating deployment data for migration

The FTM SWIFT 324 Customization Definition Program (CDP) generates the deployment data you use to migrate your instance. There is a separate set of deployment data for each server.

To use the CDP to generate deployment data, you need, as a starting point, a customization definition document (CDD) that reflects the current layout of the FTM SWIFT 300 instance to be migrated.

Note: Ensure that your latest CDD changes were marked as **implemented**.

To create an intial CDD and generate the deployment data:

1. Log on to to the customization system as a customizer (ucust1).
2. Change to the FTM SWIFT 300 customization directory (for example, *old_cust_dir*) by issuing the following command:

   ```
   cd old_cust_dir
   ```

3. Run your FTM SWIFT 300 customization profile, for example:

   ```
   . ./dnicus_DNIvINST
   ```

4. Start the CDP and export your current FTM SWIFT 300 CDD, for example:

   ```
   dnicdp -i DNIvINST
   export cdd/DNIvINST.cdd
   quit
   ```

5. Copy your exported FTM SWIFT 300 CDD to the new CDD directory *cust_dir*/cdd, for example:

   ```
   cp old_cust_dir/cdd/DNIvINST.cdd cust_dir/cdd/DNIvINST.cdd
   ```

6. Change to the customization directory by issuing the following command:

   ```
   cd cust_dir
   ```

7. Edit the CDD *cust_dir*/cdd/*DNIvINST*.cdd.

   Change the values of the following placeholders:

   DNIvPATH
   Specify the new installation directory, for example:

   ```
   inst_dir
   ```

8. Run your FTM SWIFT 324 customization profile, for example:

   ```
   . ./dnicus_DNIvINST
   ```

9. Make the modified CDD known to CDP:

   Start the CDP in **customization mode** and implement your CDD, for example:

   ```
   dnicdp -i DNIvINST
   import cdd/DNIvINST.cdd
   prepare -full
   implement
   quit
   ```

   A message *DNIZ9386I: The value for placeholder '**DNIvPATH**' related to object...was changed...* can be ignored.

   Note down the name of the directory in which the deployment data is placed for later use during the switching phase.

© Copyright IBM Corp. 2020

10. Edit the CDD *cust_dir*/cdd/*DNIvINST*.cdd. Remove the following placeholders if they exist:
    - **DNIvDBRMDIR**
    - **DNIvPKGOWNER**
    - **DNFvMWO** (for each OU where it has been assigned to)
11. Use the CDP to generate the deployment data needed to migrate your instance:

    Start the CDP in **migration mode**, for example:

    ```
    dnicdpm -i DNIvINST
    import cdd/DNIvINST.cdd
    prepare
    implement
    quit
    ```

    The generated deployment instructions are stored in the file:

    ```
    deployment_dir/DNIvINST/timestamp/instructions.txt
    ```

Attention: The migration of your customization data to FTM SWIFT 324 is now complete. However, do not deploy this data now. This data will be deployed later, during the switching phase.

If your customization and runtime systems are different, share the deployment data between those systems.

Chapter 10. Modifying broker resources

To prepare your broker to work with the FTM SWIFT 324 services, create a new FTM SWIFT 324 broker profile:

1. On the runtime system, log on as IBM Integration Bus administrator (uwmba1).
2. Make a backup copy of your current FTM SWIFT 300 broker profile and prepare a broker profile for the new FTM SWIFT 324 environment.
   a. Issue the following commands:

   ```
   cp -p work_path/common/profiles/dniczbrk.sh /home/uwmba1/dniczbrk_300.sh
   cp -p work_path/common/profiles/dniczbrk.sh /home/uwmba1/dniczbrk_324.sh
   ```

   where *work_path* represents the work-path directory of the message broker, for example, `/var/mqsi`.
   b. Edit the file `/home/uwmba1/dniczbrk_324.sh` to match the FTM SWIFT 324 environment. You must replace any references to the FTM SWIFT 300 installation directory *old_inst_dir* with the reference to the FTM SWIFT 324 installation directory.
3. If you extended the message broker startup as described in Software Integrity Checker to integrate software integrity checking do the following:
   a. Create a backup copy of the broker startup script *work_path*`/config/`*broker_name*`/profiles/ftmswift_startup.sh` where:

   work_path
   The machine-wide IBM Integration Bus working directory (that is, the value of environment variable `MQSI_WORKPATH`)

   broker_name
   The name of your message broker

   You can use for example the following command:

```
cp -p work_path/config/broker_name/profiles/ftmswift_startup.sh /home/uwmba1/ftmswift_startup.sh
```

   b. Edit file *work_path*`/config/`*broker_name*`/profiles/ftmswift_startup.sh` to match the FTM SWIFT 324 environment. You must change any references to the FTM SWIFT 300 installation directory *old_inst_dir* to the FTM SWIFT 324 installation directory *inst_dir* and any references to the FTM SWIFT 300 customization directory *old_cust_dir* to the FTM SWIFT 324 installation directory *cust_dir*.

© Copyright IBM Corp. 2020

Chapter 11. Backing up application server profiles

If you have installed the Administration and Operation (AO) Facility, the Message Entry and Repair (MER) Facility, or Relationship Management Application (RMA) perform the following steps to backup your application server profiles.

Which resources you need to back up depends on whether you use a clustered application server environment or a single server:

- If you have a clustered application server environment, back up your deployment manager profile and all other profiles on all nodes that belong to the cluster.
- If you have a single application server environment, back up the application server profile.

As the WebSphere Application Server operator (UWASO1):

1. Ensure the complete application server environment including all application servers and deployment manager is stopped. If you cannot stop your application server, perform the backup in the switching phase.
2. Issue the following command for each profile that must be backed up:

```
was_home/bin/manageprofiles.sh -backupProfile -profileName profile_name -backupFile backup_file
```

where:

was_home
Installation directory of the IBM WebSphere Application Server

profile_name
Profile name, for example AppSrv01

backup_file
Absolute path and name of the backup file to create. For example:

```
/backup/20151228/WasBackup.zip
```

© Copyright IBM Corp. 2020

Chapter 12. Prepare update of FTM SWIFT 300 configuration entities

Generate CLI scripts needed for the migration of configuration entities. For details refer to Prepare the migration of configuration entities .

Note: Make sure to use the dniprofile of FTM SWIFT 324.

© Copyright IBM Corp. 2020

Part 4. Switching to FTM SWIFT 324

After all preparation steps have been carried out for an FTM SWIFT 300 instance, carry out the following steps to switch it to FTM SWIFT 324.

Warning: After you begin the steps described in this section, your current runtime environment will remain inoperable until all of them are completed. If, for any reason, you encounter problems that prevent you from concluding the switch from an FTM SWIFT 300 to FTM SWIFT 324, re-create your current runtime environment as described in Part 8, “Handling migration problems,” on page 59.

© Copyright IBM Corp. 2020

Chapter 13. Stopping message and file processing

Stop all FTM SWIFT 300 message and file processing:

1. Stop SIPN FIN and FMT FIN processing:
   a. Stop all applications that use the SIPN FIN or FMT FIN services to send FIN messages.
   b. Stop MERVA ESA from sending messages to FTM SWIFT 300. To do this, identify which of the MERVA functions listed in the DSLKPROC TYPE=SEND section (ALLSENDQ) are relevant to FTM SWIFT 300, and stop each one by issuing the following MERVA command:

      ```
      HF function
      ```

      For example, to stop the function DSLMRSTS, enter:

      ```
      HF DSLMRSTS
      ```

   c. Stop the sending and receiving of FMT FIN messages by issuing the fmtstop command to the DNF_PF_CMD service for each LT in the appropriate business OU. For more information about the fmtstop command, see FMT FIN operation commands.
   d. Stop all LT sessions. To do this, log on as a SWIFTNet FIN operator and issue a quit command and a logout command for each LT:

      ```
      DNIvINST.DNIvOU.DNF_ILC_CMD>quit -lt ltname
      DNIvINST.DNIvOU.DNF_ILC_CMD>logout -lt ltname
      ```

2. For MSIF scenarios, before migrating, the following conditions must be met:
   - All SendMsg, SendFile, and RespondDownload scenarios must be complete, that is, for each scenario the transfer condition must be **finished**, **waitForReplication** or **stopped**. The SWIFTNet notifications (that is, Y-Copy authorisation notifications, non-delivery warnings, and delivery notifications) that correspond to a scenario are processed in a separate phase, and can be processed after migration.
   - All ReceiveMsg, ReceiveFile, and DownloadFile scenarios must be complete, that is, for each scenario the transfer condition must be **finished**.

   A ProvideFileForDownload scenario can remain in the transfer state **Downloadable** and the transfer condition **running**. After migration, the MSIF transfer service will continue to accept, from counterparts, download requests for such scenarios.

   Stop the processing of the MSIF transfer service, and ensure that the transfer condition of each scenario is compatible with migration:

   a. Stop all applications that use the MSIF transfer service.
   b. Stop all open SnF queue sessions by issuing the **release** command to the DNF_O_CMD service for each SnF queue for which you acquired a session.
   c. Stop all open SnF input and output channels by issuing the **close** command to the DNF_O_CMD service.
   d. Ensure that no further transfers are sent out by stopping the MSIF transfer service for each OU, where MSIF is running. Stop the MSIF transfer service by issuing, for each business OU, the **stop** command to the DNF_O_CMD service.

   For more information about the MSIF commands of service DNF_O_CMD refer to MSIF transfer service operation and administration commands.
3. Stop the SAGs and SAG Add-Ons as described in Stopping an SAG and Operating an SAG Add-On and .
4. Stop the FTM SWIFT 300 WAS applications.
5. Stop all FTM SWIFT related message flows.

© Copyright IBM Corp. 2020

Chapter 14. Backing up runtime database

Back up the FTM SWIFT 300 runtime database. This database can be restored provided that the target tables have not been altered or replaced in the meantime. If you need to restore your runtime system, any changes made to your runtime system after these image copies were created will not be reflected. Therefore, carry out this backup procedure as close as possible to the time at which switching to FTM SWIFT 324 is to begin.

To back up the FTM SWIFT 300 runtime database (for example, DNIDBRUN), log on as a Db2 administrator and issue the following commands:

1. Issue the list command to get all application handles of the applications still connecting to the FTM SWIFT 300 runtime database. For example:

   ```
   db2 list application for db DNIDBRUN
   ```

2. If list command returns the following warning, the next step “3” on page 39 can be skipped.

   ```
   SQL1611W No data was returned by Database System Monitor
   ```

3. If the list command returns results like this

   ```
   Auth ID  Application    Appl.    Application Id               DB     # of
            Name           Handle                                Name     Agents
   -------- -------------- -------- ---------------------------- ------   ------
   DB2INST1 db2jcc_applica 4341     127.0.0.1.39281.110624235945 DNIDBRUN 1
   DB2INST1 db2jcc_applica 4339     127.0.0.1.39280.110624235943 DNIDBRUN 1
   ```

   note the application handles and issue a force application command to ensure that all connections to the FTM SWIFT 300 database are terminated. For example:

   ```
   db2 "force application (4339, 4341)"
   ```

4. Back up the runtime database. For example:

   ```
   db2 backup db DNIDBRUN to ~/backup
   ```

© Copyright IBM Corp. 2020

Chapter 15. Deploying

The final steps of the switching phase involve deploying the necessary changes:

1. On the runtime system, log on as a Db2 administrator (udb2adm1).
2. Stop all Db2 applications and the database system.
3. Log on as an IBM Integration Bus administrator (for example, uwmba1).
4. Copy the prepared FTM SWIFT 324 broker profile (see “2” on page 29) to the work-path directory of the IBM Integration Bus. For this, issue the following commands:

   ```
   cp -p /home/uwmba1/dniczbrk_324.sh work_path/common/profiles/dniczbrk.sh
   ```

   where *work_path* represents the work-path directory of the IBM Integration Bus, for example `/var/mqsi`. This profile is processed when the broker starts.
5. To enable the broker to load FTM SWIFT 324 LIL files, enter the following command on a single line:

   ```
   mqsichangebroker broker -l inst_dir/run/lil64:inst_dir/run/jplugin
   ```
6. Log out your IBM Integration Bus administrator.
7. If you did not backup your application server profiles in Chapter 11, “Backing up application server profiles,” on page 31, perform it now.
8. Ensure that all existing FTM SWIFT 300 and future FTM SWIFT 324 system configuration administrators and security administrators switch to the updated user profile version that was created in “Preparing a user profile for each runtime system on which a broker runs” on page 15. If your installation does not use a centrally maintained version of dniprofile, assure all administrators will use an updated version of their profile too.
9. If you have activated the data integrity framework in FTM SWIFT 300 update the vault used by the data integrity framework by issuing the `dnpdic -update` command as described in Data Integrity Checker Utility commands .

   For example, to update the data integrity framework to use the copied vault `ftmswift_vault.jceks`, issue the following command as data integrity administrator:

   ```
   dnpdic -update
          -Djava.security.policy=cust_dir/ftmswift.policy
          -keystore cust_dir/ftmswift_vault.jceks
          -dsn DNIDBRUN -schema DNIvSN -uid helen -pw helens_password
   ```
10. On the runtime system, log on as a FTM SWIFT 300 security administrator (ua1 or ua2) or system configuration administrator (sa1 or sa2).
11. Rename the FTM SWIFT 300 runtime file system. For example, issue the following commands:

    ```
    mv old_run_dir old_run_dir/run_old
    ```

    If you used mounted directories, change the shown commands accordingly.
12. If you used a dni.conf file in FTM SWIFT 300:
    a. Backup your currently used FTM SWIFT 300 dni.conf file. Note the location of the backup file if it might be needed during a fallback situation.
    b. Replace the currently used dni.conf file with the one prepared in “2” on page 10.
13. The deployment data that you will use to migrate your instance was generated when you carried out the steps described in “11” on page 28. The deployment instructions were generated to a file with a name of the form:

    ```
    deployment_dir/DNIvINST/timestamp/instructions.txt
    ```

© Copyright IBM Corp. 2020

Carry out the deployment instructions for the following resource classes:

- DB (migrate database)
- DBGNT (grant database privileges)
- DBBND (bind FIN FSM for 324)
- CFGPF (install WAS applications)

14. Reapply customer specific Db2 permissions.

    If you noted Db2 permissions as described in Chapter 4, “Collect grants of Db2 resources,” on page 17, reapply those permissions.

15. Stop and restart your IBM Integration Bus.
16. Update IBM Integration Bus to use FTM SWIFT 324 message flows

    a. On a runtime system, log on as a IBM Integration Bus administrator (uwmba1).

    b. Run the profile for your FTM SWIFT 324 runtime environment by entering:

    ```
    . run_dir/dniprofile
    ```

    c. Execute BAP to deploy the FTM SWIFT 324 BAR files

    ```
    dniczbap -cmd prepare -btdd deployment_dir/DNIvINST/timestamp/BTDD.xml -deploy -broker
    DNIvBRK
    ```

    where *deployment_dir* is the directory created during preparation step “9” on page 27.

    d. Execute BAP to start all message flows provided by FTM SWIFT 324 on the current broker:

    ```
    dniczbap -cmd start
    ```

    e. To activate FTM SWIFT 324 accounting:

    - If the SIPN FIN or FMT FIN services are to be used, the broker administrator must enter the following commands:

```
mqsichangeflowstats broker -s -e eg -f "DNF_ILS_FIN" -c active -n basic -o "xml"
mqsichangeflowstats broker -s -e eg -f "DNF_ILS_ACK" -c active -n basic -o "xml"
```

    where:

    broker
    The name of your FTM SWIFT 300 broker

    eg
    The name of the execution group

    If you deployed the above mentioned bar files to multiple execution groups, repeat the steps for each execution group in which the bar files are deployed.

17. Start the SAGs and SAG Add-Ons as described in Starting an SAG and Operating an SAG Add-On.
18. If you have installed FTM SWIFT 324 WAS applications, ask the WebSphere Application Server operator (root) to start these applications.
19. If you use FTM SWIFT nodes or message sets in your own message flows, or if you modified FTM SWIFT sample message flows, you must update your Toolkit environment:

    a. Backup the broker archive (BAR) files that include FTM SWIFT 300 resources.

    b. Install the nodes or sample message flows provided by FTM SWIFT 324 and prepare the IBM Integration Toolkit workstation. See the section "IBM Integration Toolkit" in Preparing the IBM Integration Toolkit workstation for details how to update the com.ibm.dni.api.jar and com.ibm.dnq.api.jar plug-ins.

    c. Rebuild the BAR files.

    d. Deploy the BAR files.

Chapter 16. Update FTM SWIFT 300 configuration and security entities

Changes to certain configuration entities (COs) are necessary to ensure that FTM SWIFT 324 continues to run correctly. The entities that are affected depend on your installation.

To update the configuration entities:

1. On the runtime system, log on as a system configuration administrator (sa1 or sa2).
2. Adapt the message files directory to your FTM SWIFT 324 installation directory:
   a. Update the value. Enter the installation directory you specified in placeholder DNIvPATH. For this, issue the following commands:

      ```
      add -ou SYSOU -ct DniFileDir -co DniMessageFiles -attr Path -val
      DNIvPATH/run/msg
      com -ou SYSOU
      ```

      where

      - *DNIvPATH* is the new installation path, for example *inst_dir*.

      To complete the update, issue the following commands:

      ```
      app -ou SYSOU
      dep -ou SYSOU
      ```

      If dual authorization is enabled, another user with the appropriate access rights must approve the changes before they can be deployed. If dual authorization is disabled, you can skip approving the changes and immediately deploy them.

   b. End the CLI session:

      ```
      .quit
      ```

3. If you activated the data integrity framework:
   a. Update the value. Enter the runtime directory you have stored the data integrity vault. For this, issue the following commands:

      ```
      add -ou SYSOU -ct DniFileDir -co DniVault -attr Path -val run_dir
      com -ou SYSOU
      ```

      To complete the update, issue the following commands:

      ```
      app -ou SYSOU
      dep -ou SYSOU
      ```

      If dual authorization is enabled, another user with the appropriate access rights must approve the changes before they can be deployed. If dual authorization is disabled, you can skip approving the changes and immediately deploy them.

   b. End the CLI session:

      ```
      .quit
      ```

4. If you customized the FIN service:
   a. For each OU, verify your FSM instance directory:

      Issue, for each LT, the following commands:

© Copyright IBM Corp. 2020

```
add -ou DNIvOU -ct DnfLT -co ltname -attr FSMInstanceDir -val fsm_inst_dir
com -ou DNIvOU
```

where

- *DNIvOU* is the business OU to which the LT belongs
- *ltname* is the listed Logical Terminal.
- *fsm_inst_dir* is the FSM instance directory that you specified in Table 4 on page 11. For example:

```
run_dir/fsm
```

To complete the configuration, issue the following commands:

```
app -ou DNIvOU
dep -ou DNIvOU
```

If dual authorization is enabled, another user with the appropriate access rights must approve the changes before they can be deployed. If dual authorization is disabled, you can skip approving the changes and immediately deploy them.

b. Adapt the message files directory for FIN to your new installation directory *inst_dir*:

Update the value according to the value specified in placeholder DNIvPATH:

```
add -ou SYSOU -ct DniFileDir -co DnfMessageFilesFin -attr Path -val
DNIvPATH/run/msg
com -ou SYSOU
app -ou SYSOU
dep -ou SYSOU
```

If dual authorization is enabled, another user with the appropriate access rights must approve the changes before they can be deployed. If dual authorization is disabled, you can skip approving the changes and immediately deploy them.

c. End the CLI session:

```
.quit
```

5. If you customized the MSIF service:

a. Adapt the message files directory for MSIF to your new installation directory *inst_dir*:

Update the value according to the value specified in placeholder DNIvPATH:

```
add -ou SYSOU -ct DniFileDir -co DnfMessageFilesMsif -attr Path -val
DNIvPATH/run/msg
com -ou SYSOU
app -ou SYSOU
dep -ou SYSOU
```

If dual authorization is enabled, another user with the appropriate access rights must approve the changes before they can be deployed. If dual authorization is disabled, you can skip approving the changes and immediately deploy them.

b. End the CLI session:

```
.quit
```

6. If you customized the MER service:

a. Adapt the message files directory for MER to your new installation directory *inst_dir*:

Update the value according to the value specified in placeholder DNIvPATH:

```
add -ou SYSOU -ct DniFileDir -co DnqMessageFiles -attr Path -val
DNIvPATH/run/msg
com -ou SYSOU
```

```
app -ou SYSOU
dep -ou SYSOU
```

If dual authorization is enabled, another user with the appropriate access rights must approve the changes before they can be deployed. If dual authorization is disabled, you can skip approving the changes and immediately deploy them.

b. End the CLI session:

```
.quit
```

7. To run the automated update of FTM SWIFT 300 configuration data prepared at Chapter 12, “Prepare update of FTM SWIFT 300 configuration entities,” on page 33 use the instructions at Migrate the configuration entities.
8. Reapply customer specific role assignments.

   If you noted users having assigned FTM SWIFT 300 security role *DnfVerifAdmin* as described in Chapter 7, “Collect role assignments,” on page 23, reapply those assignments for the *DnfSignatureAdmin* role that replaces *DnfVerifAdmin*. You can use the following command sequence which must be issued for all noted assignments:

   ```
   dnicli -s DNI_SECADM -ou OneOfYourOUs
   add -ro DnfSignatureAdmin -user OneOfYourNotedUsers -ou OneOfYourOUs
   com -user OneOfYourNotedUsers
   app -user OneOfYourNotedUsers
   ```

   If dual authorization is enabled, another user with the appropriate access rights must approve the changes. If dual authorization is disabled, you can approve them directly. The changes are immediately active.

Part 5. Verifying FTM SWIFT 324

The following sections describe how to verify that the installation and migration of the FTM SWIFT 324 was successful.

1. To verify your BAR file deployment, complete the following task:
   a. On the runtime system, log on as IBM Integration Bus administrator (uwmba1).
   b. List the version of the system administration flow deployed on your broker (for example, MQM1BRK):

```
. run_dir/dniprofile
dniczbap -cmd list -broker MQM1BRK | grep DNI_SYSADM
```

   The list output must include the version information and looks similar to the following line:

```
DNIZ1466I:     Flow name:       DNI_SYSADM,  version: 3.2.4.1.20200908-1634
```

2. To verify the installation of Db2 stored procedures follow the instruction in Verifying the installation of the database routines.
3. To verify the cryptographic services used by the CLI:
   a. On the runtime system, log on as FTM SWIFT 324 system configuration administrator (sa1 or sa2).
   b. Enter the following commands:

```
dnicli -s DNI_SYSADM -ou SYSOU
add -ou DNFSYSOU -ct DnfLAUKeyRM -co TestLAUKeyFP -attr hk1 -secval
0123456789ABCDEF
rem -ou DNFSYSOU -ct DnfLAUKeyRM -co TestLAUKeyFP
com -ou DNFSYSOU
```

   All commands must end without an error.

```
app -ou DNFSYSOU
dep -ou DNFSYSOU
.quit
```

   If dual authorization is enabled, another user with the appropriate access rights must approve the changes before they can be deployed. If dual authorization is disabled, you can skip approving the changes and immediately deploy them.
4. To verify that the SIPN FIN service works:
   a. On the runtime system, log on as a user who has the role SWIFTNetFINOperator for any one OU.
   b. In your business OU (for example, BANKA) log in to an LT (for example, XXXXUSNYA) and then stop the connection to the LT:

```
dnicli -s DNF_ILC_CMD -ou BANKA
login -lt XXXXUSNYA
logout -lt XXXXUSNYA
.quit
```

   If the login was successful, the FIN service is ready to be used.
5. If you are using the SAG Add-On, you can verify the connection as follows:
   a. On the runtime system, log on as a user who has the role SagAdmin for OU DNFSYSOU.
   b. Issue the following commands:

```
dnicli -s DNFSAGCFG -ou DNFSYSOU
llk
.quit
```

© Copyright IBM Corp. 2020

Then, all LAU keys that were already created must be listed.

6. To verify the MSIF services:
   a. On the runtime system, log on as FTM SWIFT 324 security administrator (ua1 or ua2).
   b. Run dniprofile by entering the following command:

```
. run_dir/dniprofile
```

   c. Issue the following command for your business OU (for example, BANKA):

```
dnicli -ou BANKA -s DNF_O_FT -c "SendMsg"
```

   The command must produce the following result:

```
DNFO0001I Reference is '<48 chars reference_number>'.
DNFO0004E Processing failed.
DNFO3149E No value specified for mandatory option 'LocalDN' of 'TransferOptions'
          option set used to process the request; OU='BANKA'.
```

   d. Issue the list command to the MSIF command service for your business OU (for example, BANKA):

```
dnicli -ou BANKA -s DNF_O_CMD -c "list"
```

   This command must show the following result:

```
DNFO0091E You are not authorized to issue the command you just issued.
```

7. To verify that the enterprise applications are installed and correctly configured:
   a. Choose a user:
      - For the Message Entry and Repair (MER) Facility, choose a user who has the role DnqERMsgAdmin for any one OU.
      - For the Relationship Management Application (RMA) or Administration and Operation (AO) Facility, choose a user who has the role DniSA in SYSOU.
   b. Allow the chosen user to log in to the application server and to use the corresponding enterprise application.
   c. In a browser, open the URL of each enterprise application that is to be tested, for example:

```
https://http_hostname/context_root/
```

   where

   http_hostname
   The host name or IP address of the HTTP server.

   context_root
   The context root that is used for the enterprise application:

Enterprise application	Context root
WebHome	**/ftm-swift/**
MER Facility	**/dnqmer/**
RMA	The value of the DNFvRMACONTROOT customization placeholder. The default is **/rma/**.
AO Facility	The value of the DNPvAOCONTROOT customization placeholder. The default is **/ao/**.

   d. After you opened the URL:

- For the MER Facility, the list of all OUs for which the role DnqERMsgAdmin was assigned to a user, is displayed.
- For the RMA, the relationship list is displayed.
- For the AO Facility, the Console entry is listed in the navigation pane and no error messages are shown in the content pane.

Note: Now it is the time to start your applications and services (for example, the FIN, or MSIF service).

Part 6. Cleaning up obsolete resources

Attention: After this step, you will no longer be able to fall back to FTM SWIFT 300.

After you have ensured that the migration to FTM SWIFT 324 was successful, carry out the following steps to remove obsolete resources from your system:

1. Remove FTM SWIFT 300 security roles that are no longer used on FTM SWIFT 324.
   a. Log on to your runtime system as a security administrator (ua1 or ua2)
   b. Before security roles can be removed they must be removed from any user assignment.

      If you noted users to FTM SWIFT 324 security role assignments as described in Chapter 7, “Collect role assignments,” on page 23, remove those assignments now. You can use the following command sequence which must be issued for all noted assignments for the roles DnfVerifAdmin, SWIFTNetInterActSender and SWIFTNetInterActSnFOperator:

      ```
      dnicli -s DNI_SECADM -ou OneOfYourOUs
      rem -user OneOfYourNotedUsers -ro DnfVerifAdmin -ou OneOfYourOUs
      com -user OneOfYourNotedUsers
      app -user OneOfYourNotedUsers
      ```

   c. Enter the following commands to delete the obsolete security roles:

      ```
      dnicli -s DNI_SECADM -ou SYSOU
      del -ro DnfVerifAdmin
      com -ro DnfVerifAdmin
      app -ro DnfVerifAdmin

      del -ro SWIFTNetInterActSender
      com -ro SWIFTNetInterActSender
      app -ro SWIFTNetInterActSender

      del -ro SWIFTNetInterActSnFOperator
      com -ro SWIFTNetInterActSnFOperator
      app -ro SWIFTNetInterActSnFOperator
      ```

      If dual authorization is enabled, another user with the appropriate access rights must approve the changes. If dual authorization is disabled, you can approve them directly. The changes are immediately active.
2. Remove the FTM SWIFT 300 customization and runtime environment, for example:

   ```
   rm -R /var/ftmswift_v300
   ```

3. Remove all FTM SWIFT 300 customization and runtime profiles.
4. While preparing for migration, a backup from your FTM SWIFT 300 runtime database was taken to save your current data. Delete the backup file only if you are sure that you no longer need these database backup file.
5. Delete the backup copy of the IBM Integration Bus administrator profile (dniczbrk_300.sh). If you are using the extended broker startup script delete the backup copy of the extended broker startup script (ftmswift_startup.sh).
6. Delete the prepared new copy of the IBM Integration Bus administrator profile (dniczbrk_324.sh).
7. Remove the backup copy of your application server profile.
8. Remove the backup copy of your BAR-files.
9. To uninstall FTM SWIFT 300 refer to Installation.

© Copyright IBM Corp. 2020

Part 7. Migrating SAG Add-On

This part describes how to migrate your FTM SWIFT 300 SAG Add-On to the level of FTM SWIFT 324.

Attention: After SAG Add-On is migrated, you will no longer be able to fall back to FTM SWIFT 300.

© Copyright IBM Corp. 2020

Chapter 17. Preparing

To prepare your SAG workstation, carry out the following steps:

1. Optionally, you can setup a **new** SAG workstation with the required software levels. If you choose this option, prepare your SAG Add-On profile.
2. If you choose to use your current SAG workstation:
   a. Make a backup copy of your SAG workstation.
   b. Save your current SAG Add-On profile (dnfcssao.cfg) to a temporary directory.
3. For installation purposes you need the following information. Please note your values for:
   - The Remote Application (RA) owner.
   - On Windows: The password of the Remote Application (RA) owner.
   - The instance name of the SAG Remote API.
   - The installation directory of the SAG Remote API.
4. Download all files included in directory *inst_dir*/admin/SAGAddOn73 or *inst_dir*/admin/SAGAddOn74 from your FTM SWIFT 324 installation.

   Transfer the following files:
   a. The file SAGAddOnRepository.zip in binary format.
   b. The readme in text format.
   c. All sample response files suitable for the operating system in text format.
5. If you plan to use the unattended installation mode, modify the installation response file according to your needs.

© Copyright IBM Corp. 2020

Chapter 18. Switching

For each SAG used by your instance, migrate your SAG Add-On.

1. If you only have one SAG workstation connected to FTM SWIFT 300:
   a. Stop message and file processing as documented in Chapter 13, “Stopping message and file processing,” on page 37.
   b. Log out your corresponding FIN LTs or stop the InterAct or FileAct processing of transfers that use this SAG.
2. Stop the SAG Add-On on your SAG workstation. For details refer to Operating an SAG Add-On .
3. Uninstall the current FTM SWIFT 300 SAG Add-On. For details refer to Uninstalling the SAG Add-On .
4. Delete the installation directory of the current level of the SAG Add-On with all its remaining content.
5. Install the new FTM SWIFT 324 SAG Add-On. For details refer to Installing the SAG Add-On .
6. Copy your SAG Add-On profile (dnfcssao.cfg) saved in “2.b” on page 55 to the FTM SWIFT 324 SAG Add-On runtime directory. This defaults to: `/var/ftmswift_v324/sao` (AIX® and RHEL x86) or `%PROGRAMDATA%\ftmswift_v324\sao` (on Windows).
7. Edit your SAG Add-On profile. Update the XML elements:

   <TraceDirectory>
   The directory to which trace files are written. It defaults to: `/var/ftmswift_v324/sao/log` (AIX and RHEL x86) or `%PROGRAMDATA%\ftmswift_v324\sao\log` (on Windows).
8. Make the Remote Application (RA) user the owner of the profile and grant read and write permission.
9. Start the SAG Add-On on your SAG workstation. For details refer to Operating an SAG Add-On .

© Copyright IBM Corp. 2020

Part 8. Handling migration problems

This part describes how to handle problems during migration.

© Copyright IBM Corp. 2020

Chapter 19. Falling back to FTM SWIFT 300

Falling back means returning to FTM SWIFT 300. This might be necessary if, after migration, you encounter severe problems that can best be resolved by reverting to your former environment.

Attention: After switching from FTM SWIFT 300 to FTM SWIFT 324, falling back is possible only if:

- You have not carried out the steps described in Part 6, “Cleaning up obsolete resources,” on page 51.
- You have not recustomized the instance, that is, you have not made changes to the CDD and run the resulting deployment vehicles in FTM SWIFT 324 after the Switching phase.
- No PTFs were applied in FTM SWIFT 324 after the Switching phase.
- You have not migrated your SAG Add-On.

To fall back from FTM SWIFT 324 to FTM SWIFT 300, carry out the following steps for each instance on the runtime systems on which the brokers run:

1. Stop all message and file processing as described in Chapter 13, “Stopping message and file processing,” on page 37.
2. If you used a dni.conf file in FTM SWIFT 300, ask your root system administrator to restore the dni.conf file (see step “12.a” on page 41).
3. Ask your FTM SWIFT 300 system configuration administrator to retrieve the FTM SWIFT 300 runtime file system (see “11” on page 41), for example issue the following command:

   ```
   mv old_run_dir/run_old old_run_dir/run
   ```

4. Ask your IBM Integration Bus administrator (uwmba1) to restore your FTM SWIFT 300 broker files.
   a. Restore your FTM SWIFT 300 broker profile that you saved in step “2” on page 29. Issue the following commands:

      ```
      cp -p /home/uwmba1/dniczbrk_300.sh work_path/common/profiles/dniczbrk.sh
      ```

      where *work_path* represents the work-path directory of the message broker, for example, `/var/mqsi`
   b. If you extended the message broker startup, restore your FTM SWIFT 300 broker startup script that you saved in step “3” on page 29. Issue the following commands:

```
cp -p /home/uwmba1/ftmswift_startup.sh work_path/config/broker_name/profiles/ftmswift_startup.sh
rm /home/uwmba1/ftmswift_startup.sh
```

work_path
The machine-wide IBM Integration Bus working directory (that is, the value of environment variable `MQSI_WORKPATH`)

broker_name
The name of your message broker

5. Instruct all FTM SWIFT 300 system configuration administrators and security administrators to revert to using the runtime profile file that correspond to FTM SWIFT 300, for example:

   ```
   old_run_dir/dniprofile
   ```

6. On the runtime system, log on as a Db2 administrator (udb2adm1).
7. Restore the FTM SWIFT 300 runtime data from the backup copy (see Chapter 14, “Backing up runtime database,” on page 39).
   a. Issue the following commands:

© Copyright IBM Corp. 2020

```
db2 drop db DNIvDSN
db2 restore db DNIvDSN from ~/backup
```

8. Undo changes of Db2 objects modified during migration. For this, first issue the following command to connect to your runtime database:

   ```
   db2 connect to DNIvDSN
   ```

   Then restore existing JAR files in the local Db2catalog. Edit the file

   ```
   deployment_dir/DNIvINST/admin/dnicommon_inst_sp_fb01.ddl
   ```

   and replace all occurrences of **DNIvOLDINSTPATH** with the installation directory of FTM SWIFT 300. Then issue the following command:

   ```
   db2 +c -td# -z fallback.log -svf DNIvINST/admin/dnicommon_inst_sp_fb01.ddl
   ```

   If the SIPN FIN or FMT FIN services are used, then restore existing JAR files in the local Db2catalog. Edit the file

   ```
   deployment_dir/DNIvINST/admin/dnffin_inst_sp_fb01.ddl
   ```

   and replace all occurrences of **DNIvOLDINSTPATH** with the installation directory of FTM SWIFT 300. Then issue the following command:

   ```
   db2 +c -td# -z fallback.log -svf deployment_dir/DNIvINST/admin/dnffin_inst_sp_fb01.ddl
   ```

   Issue the following command to reset the connection to your runtime database:

   ```
   db2 connect reset
   ```

9. On the runtime system, log on as a IBM Integration Bus administrator (uwmba1).
10. Issue the following mqsichangebroker command on a single line:

```
mqsichangebroker broker -l old_inst_dir/run/lil64:old_inst_dir/run/jplugin
```

    where *old_inst_dir* represents the FTM SWIFT 300 installation directory.

11. Re-start all brokers that are associated with the FTM SWIFT 300 instance.
12. Use the BAP tool to deploy FTM SWIFT 300 message flows again.
    a. Run the profile for your runtime environment by entering:

       ```
       . old_run_dir/dniprofile
       ```

    b. Prepare and deploy the BAR-files by entering:

       ```
       dniczbap -cmd prepare -all -deploy
       ```

13. Execute BAP to start all message flows provided by FTM SWIFT 300:

    ```
    dniczbap -cmd start
    ```

14. After all message flows were deployed, reactivate the collection of FTM SWIFT 300 accounting data. If the SIPN FIN or FMT FIN services are used, you must enter the following commands:

```
mqsichangeflowstats broker -s -e eg -f "DNF_ILS_FIN" -c active -n basic -o "xml"
mqsichangeflowstats broker -s -e eg -f "DNF_ILS_ACK" -c active -n basic -o "xml"
```

    where:

    broker
    The name of your FTM SWIFT 300 broker

eg
The name of the FIN execution group

If you deployed the above mentioned bar files to multiple execution groups, repeat the steps for each execution group in which the bar files are deployed.

15. If you use FTM SWIFT 324 nodes or message sets in your own message flows, or if you modified FTM SWIFT 324 sample message flows, deploy your saved BAR files. After this, re-establish your Toolkit environment. See the sectionPreparing the IBM Integration Toolkit workstation and for details.
16. If you have installed the Administration and Operation (AO) Facility, the Message Entry and Repair (MER) Facility, or Relationship Management Application (RMA) perform the following steps to restore the application server configuration.
    a. Stop all application servers for which the configuration is to be restored.
    b. As a WebSphere Application Server operator (UWASO1), issue the following commands:
        1) To delete the FTM SWIFT 324 profiles and to remove the profile directory:

```
was_home/bin/manageprofiles.sh -delete -profileName profile_name
rm -r was_home/profiles/profile_name
```

where:

was_home
Installation directory of the application server

profile_name
Profile name, for example AppSrv01

        2) To restore the FTM SWIFT 300 profiles:

```
was_home/bin/manageprofiles.sh -restoreProfile -backupFile backup_file
```

where:

backup_file
Path and name of the backup file to create

    c. If you have a clustered application server environment, perform a full resynchronization between all your nodes belonging to the cell.
17. Start the SAGs and SAG Add-Ons as described in Starting an SAG and Operating an SAG Add-On.
18. As a customizer, remove the customization definitions of FTM SWIFT 324. Issue the following commands:

```
cd cust_dir/defs
rm -R *
```

19. As a customizer, switch back to your previous customization environment. For this:
    a. Reuse your FTM SWIFT 300 customization profile dnicus_*DNIvINST*, for example located in *old_cust_dir*
    b. Reuse your FTM SWIFT 300 CDD *DNIvINST*.cdd, for example located in *old_cust_dir*/cdd.
    c. Reuse your FTM SWIFT 300 ini-file *DNIvINST*.ini, for example located in *old_cust_dir*/cus.
20. If you have installed FTM SWIFT 324 WAS applications, ask the WebSphere Application Server operator (root) to start these applications.
21. Your FTM SWIFT 300 runtime and customization system is now restored.

Note: The concept for falling back and remigrating after falling back assumes that the same software level is used for all steps. If you think the reason causing you to fall back to FTM SWIFT 300 is fixed by an FTM SWIFT PTF or a fix for this problem is part of an APAR package which can be retrieved from the FTM SWIFT 324 support page, contact IBM service before you continue. Do not apply any new software level without confirmation by the IBM support team.

Chapter 20. Re-migrating after falling back to FTM SWIFT 300

If problems occurred during your initial attempt to migrate to FTM SWIFT 324 and if you fell back to the previous software level, plan for re-migration only after you have identified the reason for the fallback and have resolved the problem.

© Copyright IBM Corp. 2020

Chapter 21. Falling back SAG Add-On

Falling back means returning to the use of FTM SWIFT 300 SAG Add-On. To fall back:

1. If you only have one SAG workstation connected to FTM SWIFT 324, stop message and file processing as documented in Chapter 13, “Stopping message and file processing,” on page 37.
2. If you have more than one SAG workstation connected to FTM SWIFT 324, log out your corresponding FIN LT or stop the InterAct or FileAct processing of transfers that are send over this SAG.
3. Stop your SAG.
4. Stop the SAG Add-On.
5. Restore your SAG workstation backup copy that you created in step “2.a” on page 55.

© Copyright IBM Corp. 2020

Appendix A. Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information about the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which was exchanged, should contact:

IBM Deutschland GmbH
Dept. M358
IBM-Allee 1
71139 Ehningen
Germany

© Copyright IBM Corp. 2020

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements might have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements might have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This document contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information”:

```
www.ibm.com/legal/copytrade.shtml
```

Adobe is either a registered trademark or a trademark of Adobe Systems Incorporated in the United States, and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linux® is a registered trademark of Linus Torvalds in the United States, other countries or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Index

A

access permissions, granting to users 9
accounting, activating 42, 62
application server profile, backing up 31

B

broker profile 41
broker, modifying 17, 19, 21, 25, 29

C

CDP initialization file 13
CDP profile 13
CDP trace file
    directory 13
cleaning up 1
Configuration Data Provider node, data and cache 11
cryptographic archive 41
Custom mountpoints, configuring 10
customization definition directory 13
customization directory structure, creating 10
customization environment, deleting 51
customization environment, preparing 13
customization profile 13

D

default installation directory 5
deploy message flows 62
deploying resources 41
deployment data directory 10
deployment data, preparing 27
directory structure, creating the customization 10
directory structure, creating the runtime 11
directory, trace 11
DNI_BAP_PATH 15
DNI_PATH 15
dni.conf 10, 11, 41, 61
dniczbrk.sh 41, 61
dniprofile 15
dniruntime 10
dnitrace 10
DNIvDBRMLIB 27
DNIvPATH 27, 43
dnizbrk.sh 29

E

environment variables 15

F

falling back 1
file system, allocating 9
file system, mounting 9
FSM instance directory 10, 43
FSMInstanceDir 10
ftmswift_startup.sh 29

G

granting access permissions to users 9

H

hierarchical file system
    customization directory structure 10

I

In-place 1
initialization file, CDP 13
inst_dir 5
installing
    FTM SWIFT 324 9

M

message files directory 43
migrating, message broker 1
migrating, SAG Add-On 1
Migrating, SAG Add-On 53
migration phase 1

N

Notices 69

P

permissions, granting users access 9
planning 5
preparing 1
profile, customization 13

R

re-migrating 1
resource class CFGPF 42
resource class DB 42
resource class DBBND 42
resource class DBGNT 42
rights, granting users access 9
roles 23
routine-instance directory 41
run DDL admin modules 62
runtime directory structure, creating 11
runtime environment, deleting 51

S

SAG Add-On, falling back 67
SAG Add-On, preparing 55
SAG Add-On, switching 57
software level 5
switching 1

T

Toolkit 63
Toolkit environment 42
trace data 11
trace directory 11

V

verifying 1

W

WAS application, uninstalling 51

Product Number: 5725-X92

BBMP-0324-00