IBM Financial Transaction Manager for SWIFT Services for Multiplatforms

Version 3.0.0

Migration Guide

BBMP-0300-03

IBM Financial Transaction Manager for SWIFT Services for Multiplatforms

Version 3.0.0

Migration Guide

BBMP-0300-03

This edition applies to Version 3.0.0 of IBM Financial Transaction Manager for SWIFT Services for Multiplatforms (5725-X92) and to all subsequent releases and modifications until otherwise indicated in new editions.

Reference key: 20170403-0645

Contents

About this publication

This publication applies to the IBM® Financial Transaction Manager for SWIFT Services (abbreviated to FTM SWIFT). It describes how to migrate from IBM WebSphere® Business Integration for Financial Networks (abbreviated to WebSphere BI for FN) to FTM SWIFT.

Migration Guide Replacement Notice

This edition of the Migration Guide (*BBMP-0300-03*) replaces the previous book edition (*BBMP-0300-02*).

Now, it describes how to migrate from WebSphere BI for FN latest PTF levels (as of December 2016) to FTM SWIFT latest Fix Pack level (as of December 2016).

Terminology used in this publication

Feature

The term *feature* is used to summarize services that belongs together. FTM SWIFT consists of the following features:

Support for SWIFTNet FIN

This feature comprises the following services, which are used to transfer FIN messages via the SIPN:

- SIPN FIN service
- SIPN FIN LT session operation service

Financial Message Transfer (FMT)

This feature comprises the following services, which are used to transfer FIN messages internally:

- FMT FIN service
- FMT FIN session operation service

Messaging Services for SWIFTNet InterAct and FileAct (MSIF)

This feature comprises the following services, which are used to transfer business messages via SWIFTNet InterAct and files via SWIFTNet FileAct:

- MSIF transfer services
- MSIF command service

Message Management (MM)

This feature comprises the services and facilities that help you to manage financial message traffic:

- Sequential Data Facility (SDF) import and export services
- Message printing service
- Message Entry and Repair (MER) Facility
- Message routing service

Message Broker

The term *message broker* comprises the following products:

- WebSphere Message Broker V7 and V8
- IBM Integration Bus V9

FTM SWIFT uses the WebSphere Message Broker terminology. For an overview of the differences refer to "Name changes in IBM Integration Bus Version 9.0".

Multi-platform

The term *multi-platform* comprises the following operating system:

- AIX®

Part 1. Overview

If you used WebSphere BI for FN Version 3.1. and want to migrate to FTM SWIFT Version 3.0.0, you must migrate your software to more recent levels, then activate the new capabilities offered by the new software. This is called *migration*. The In-place (IP) migration is used to migrate a WebSphere BI for FN 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 WebSphere MQ queue manager cluster
- Uses the same WebSphere Message Broker brokers
- Keeps their values of all existing variables and parameters. If an value can be changed it is explicitly described in this document.

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

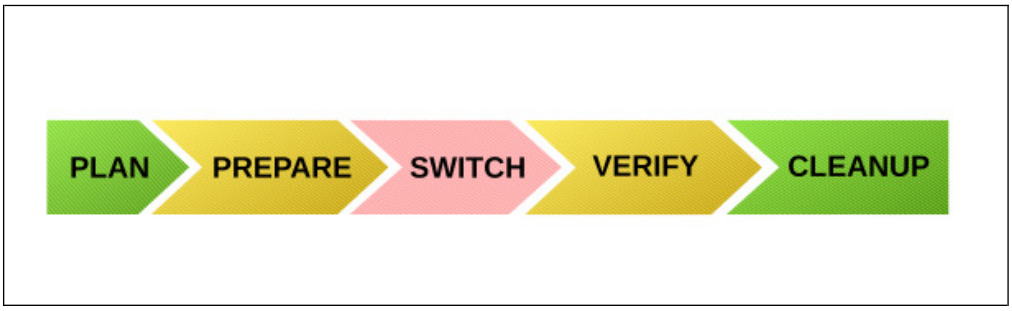

Figure 1. In-place (IP) migration

It comprises the following phases:

Planning
Before you begin installing and migrating to the FTM SWIFT, 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 WebSphere BI for FN environment is still used for processing and is not affected by this preparation activities.

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

Verifying
Determine whether the FTM SWIFT environment was installed correctly and switching was successful. In this phase your system can not process business messages.

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

Figure 2 shows the phases in case of problems.

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 WebSphere BI for FN 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.

The overall migration consists of the following tasks:

1. Check the WebSphere BI for FN PTF level of your current system.
2. Install the required WebSphere BI for FN PTFs.
3. Check the software requirements for FTM SWIFT.
4. Install and upgrade products that did not cover the software requirements for FTM SWIFT. For example, upgrade your Message Broker V8 to IBM Integration Bus V9.
5. Migrate WebSphere BI for FN to FTM SWIFT.
6. Check the software requirements for FTM SWIFT SAG Add-On.
7. Install and upgrade products that did not cover the software requirements for FTM SWIFT SAG Add-On. For example, upgrade your SAG.
8. Install the SAG Add-On.
9. Migrate your WebSphere BI for FN SAG Add-On to the new FTM SWIFT SAG Add-On.

Figure 3 on page 3 illustrates which resources are involved in the preparation phase and which steps are performed in the switching phase. After you installed FTM SWIFT, following resources are prepared:

`Customization definition document (CDD)`
A new CDD is created from the existing WebSphere BI for FN CDD.

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

`Deployment data`
Following resources are customized:

- Message Broker flows
- WAS applications
- FIN bind (dnfcwdbs)

`Runtime profile`
A new dniprofile is created.

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

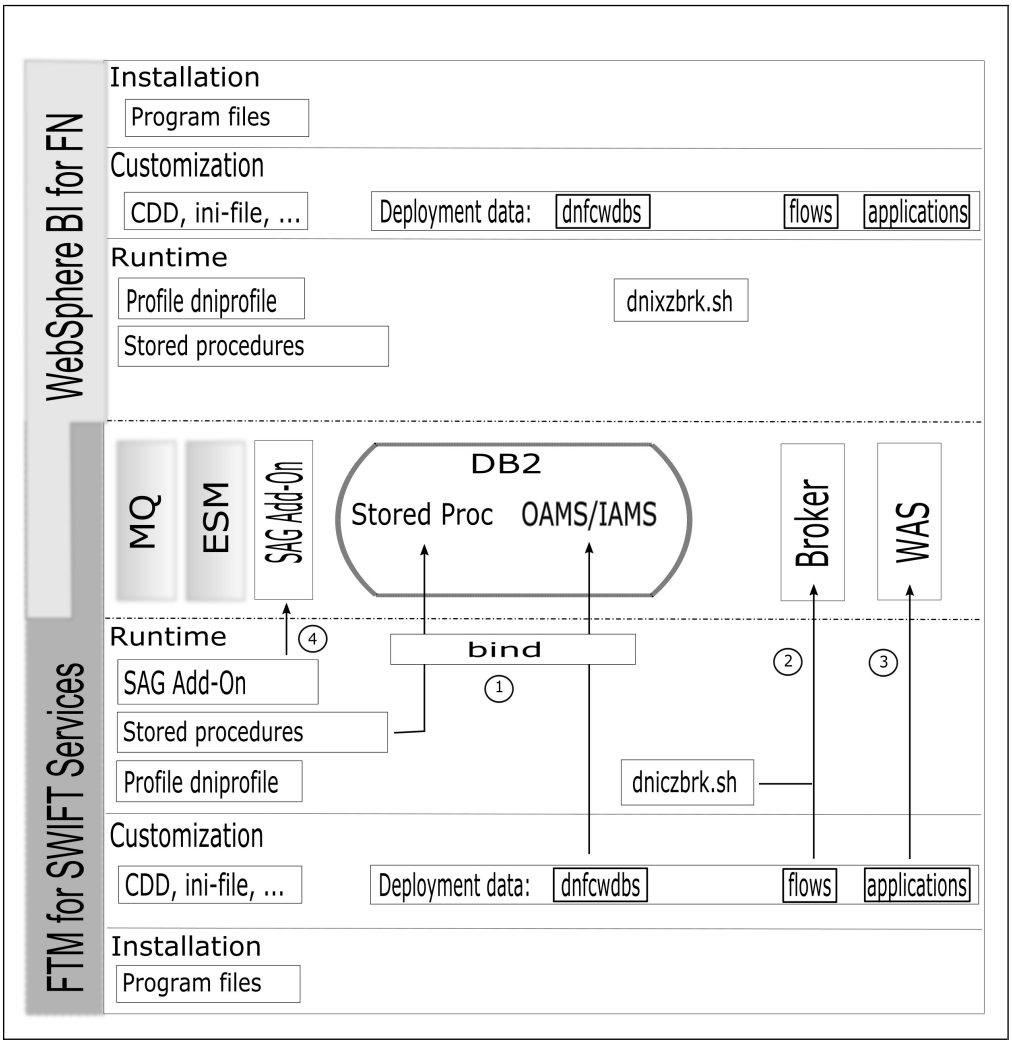

Figure 3. Involved resources and switching steps in FTM SWIFT

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

1. DB2: The stored procedures are extracted and bound. If you use the FIN service, the FSM plan is bound too. The definition of the DNI_RDU_HISTORY table is updated.
2. Message Broker: The new FTM SWIFT flows are deployed
3. WebSphere Application Server (WAS): The new FTM SWIFT applications are installed.
4. SAG Add-On: After you finished the FTM SWIFT migration, the SAG Add-On and with this the SWIFT Alliance Gateway (SAG) has to be migrated (see Part 7, “Migrating SAG Add-On,” on page 49). Until you start to migrate the SAG Add-On, the WebSphere BI for FN SAG Add-On continues to work with FTM SWIFT.

The WebSphere MQ and external security manager (ESM) resources are not changed.

Part 2. Planning FTM SWIFT

Before you begin installing and migrating to the IBM Financial Transaction Manager for SWIFT Services, 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 WebSphere BI for FN instance that is to be migrated is Version 3.1.1, and that the following PTFs were installed:
   - UI42655 (Base, product level 3.1.1.29)
   - UI41572 (Message Management, product level 3.1.1.21)
   - UI38427 (Support for SWIFTNet FIN, product level 3.1.1.13)
   - UI41762 (Messaging Services for SWIFTNet InterAct and FileAct, product level 3.1.1.19)
   - UI42571 (SAG AddOn, product level 3.1.1.5)

   One option to verify that these PTFs are applied on the runtime system is to issue following command:

   ```
   lslpp -l | grep wbifn
   ```

   The listed product levels must be at least:

   ```
   ibm.wbifn311.dnf          3.1.1.13  COMMITTED  WebSphere Business Integration
   ibm.wbifn311.dni          3.1.1.29  COMMITTED  WebSphere Business Integration
   ibm.wbifn311.mm           3.1.1.21  COMMITTED  WebSphere Business Integration
   ibm.wbifn311.msif         3.1.1.19  COMMITTED  WebSphere Business Integration
   ```
2. Ensure that your WebSphere BI for FN customization and runtime systems meet the hardware and software requirements for FTM SWIFT. Use the following software versions for WebSphere BI for FN:
   - AIX Version 6.1 or Version 7.1
   - IBM Integration Bus Version 9.0.0.6

     How to migrate your Message Broker Version 8 to IBM Integration Bus Version 9.0.0.6 is described in Appendix A, “Migrating from WebSphere Message Broker V8 to IBM Integration Bus Version 9.0.0.6,” on page 69.

     How to migrate your Message Broker Version 7 to IBM Integration Bus Version 9.0.0.6, and the additional requirements for this migration, is described in Appendix B, “Migrating from WebSphere Message Broker V7 to IBM Integration Bus Version 9.0.0.6,” on page 77.
   - WebSphere MQ Version 8.0.0.3
   - IBM WebSphere Application Server Version 8.5.5.6
   - DB2 Version 10.1.0.4
   - xlC (IBM C/C++ compiler) Version 10.1
   - Java™ 7.0 SR9 FP1 (7.0.9.1)
3. Ensure that IBM Installation Manager Version 1.8.3 is installed.
4. To become acquainted with the migration procedure, it is best to migrate to FTM SWIFT on a test system before attempting to migrate on a production system.
5. Ensure that the persons with the following roles are available during customization and configuration:
   - WebSphere MQ administrator

- WebSphere Message Broker application developer
- WebSphere Message Broker administrator
- DB2 administrator
- WebSphere BI for FN customizer
- WebSphere BI for FN system configuration administrators
- WebSphere BI for FN security administrators
- 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)

6. 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.
   - No re-customization actions are outstanding.
   - No PTF migration actions are outstanding.
7. If you use WebSphere BI for FN nodes or message sets in your own message flows, or if you use modified WebSphere BI for FN sample message flows, you must plan to update your Toolkit environment and re-deploy your compiled message flows.
8. Ensure that the service bundle DNFEIAS is removed from all OUs in your CDD. If it is assigned to an OU, remove this DNFEIAS service bundle from this OU and recustomize your instance as described in *WebSphere BI for FN: Planning, Installation, and Customization* before any migration activities.
9. Ensure that the service bundles DNFIASNF and DNFINTERACT are removed from all OUs in your CDD. If they are assigned to an OU, remove this DNFIASNF and DNFINTERACT service bundles from this OU and recustomize your instance as described in *WebSphere BI for FN: Planning, Installation, and Customization* before any migration activities.
10. The default installation directory of FTM SWIFT is `/opt/IBM/ftm/swift/v300`. However, you can choose any directory you like. This manual uses the abbreviation *inst_dir* to indicate this directory.

Part 3. Preparing to migrate to FTM SWIFT

Preparation steps are those that can be carried out while WebSphere BI for FN system continues to run. It includes:

- Installation of FTM SWIFT programs
- Preparation of the customization environment
- Generation of the customization definitions

Chapter 1. Installing FTM SWIFT

To install FTM SWIFT V3.0.0.3 (fix pack 3), refer to http://www.ibm.com/support/knowledgecenter/SSRH46_3.0.0_SWS/installing.html

Granting access permissions to FTM SWIFT users

This description assumes that you use the existing groups from WebSphere BI for FN:

dniadmin
Runs administration tasks for FTM SWIFT.

dnilpp
Runs the FTM SWIFT services.

dnicusgr
Creates customization and deployment data for FTM SWIFT.

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

Creating directory structures

FTM SWIFT 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.

Allocating and mounting file systems

Table 2 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	/var/ftmswift_v300/cus	At least 50 MB per instance.

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	/var/ftmswift_v300/run	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 stops processing messages.

The mount points are base directories in which you create subdirectories for certain FTM SWIFT 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 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 is to use.

Configuring the instance for runtime file system mount point

If you chose not to use the default runtime file system mount point, configure your instance to be able to use the customized mount point:

1. On the runtime system, log on as a system configuration administrator (sa1 or sa2).
2. Copy the sample **dni.conf** file to your home directory, and give read access to group dnilpp. For example:

   ```
   cp inst_dir/run/samples/dni.conf ~/dni.conf
   chmod 750 ~/dni.conf
   chgrp dnilpp ~/dni.conf
   ```

3. In the copy of dni.conf, set the variables dnitrace, and dniruntime to the appropriate directories.

   For example, if you choose /tmp/ftmswift_v300/run as a mount point, edit the corresponding lines so that it looks like this:

   ```
   # Set the directory to store trace information
   dnitrace /tmp/ftmswift_v300/run/trace

   # Set the directory to store runtime and cache data
   dniruntime /tmp/ftmswift_v300/run
   ```

   Note:

   - The dnftrace variable used in WebSphere BI for FN has been removed in FTM SWIFT.
   - If an FTM SWIFT component cannot read or parse the dni.conf file, it stores runtime and trace data in default subdirectories of the following directory:

     /var/ftmswift_v300/run
   - If the component cannot access a directory specified in the dni.conf file, the syslog contains messages related to the problem.

- If **dniruntime** is set incorrectly, FTM SWIFT cannot work properly.
- If **dnitrace** is set incorrectly, FTM SWIFT writes trace information to the directory `/var/tmp`.

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 17
- 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 stores customization data in the directories shown in Table 3.

Table 3. Directory structure for customization

Description	Default directory
Customization definition document (CDD) directory used to store your CDDs.	`/var/ftmswift_v300/cus/cdd`
Customization definition directory used to store customization definition data.	`/var/ftmswift_v300/cus/defs`
Deployment data directory used to store customization deployment data like instructions and vehicles you create.	`/var/ftmswift_v300/cus/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 `/var/ftmswift_v300/cus`.

Creating the runtime directory structure for the broker

Table 4 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	`/var/ftmswift_v300/run/cache`	Set by the **dniruntime** variable in dni.conf with the appended subdirectory `/cache`.	Used to store temporary files.
trace directory	`/var/ftmswift_v300/run/trace`	Set by the **dnitrace** variable in dni.conf.	Used to store trace files.

Table 4. Directory structure for the broker (continued)

Directory Name	Default directory	Customization possibility	Description
xfsm directory	`/var/ftmswift_v300/run/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. Needed only if the **Support for SWIFTNet FIN** feature is used.
fsm instance directory	`/var/ftmswift_v300/run/fsm`	Set by the `FSMInstanceDir` attribute of the `DnfLT` CO of the LT. **Note:** If more than one FTM SWIFT 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. Needed only if the **Support for SWIFTNet FIN** feature is used.
bap directory	`/var/ftmswift_v300/run/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 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 `/var/ftmswift_v300/run`.

Creating the runtime directory structure for the Java database routines

By default, FTM SWIFT stores runtime information for the database routines in the directories shown in Table 5.

Table 5. Directory structure for the Java database routines

Directory Name	Default directory	Description
routines directory	`/var/ftmswift_v300/run/routines`	Highest-level directory for code used to install and run FTM SWIFT Java database routines.
routines-instance directory	`/var/ftmswift_v300/run/routines/DNIvINST`	The instance subdirectory which contains Java database routines that applies to a particular FTM SWIFT instance.

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

```
mkdir -p run_mount_point/routines/DNIvINST
chgrp -R dnilpp run_mount_point
chmod -R 770 run_mount_point
```

where *run_mount_point* represents the name of the runtime file system mount point you chose. The default is `/var/ftmswift_v300/run`.

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 instance:

1. On the customization system, log on as a customizer (ucust1).
2. Copy the initialization file template that is delivered with FTM SWIFT to the directory `/var/ftmswift_v300/cus` by issuing the following command:
   `cp inst_dir/admin/samples/dniczcdp.ini /var/ftmswift_v300/cus/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 11, 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 6.

Table 6. 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 instance:

1. On the customization system, log on as a customizer (ucust1).
2. Copy the sample profile delivered with FTM SWIFT to the directory `/var/ftmswift_v300/cus` and give it a name that associates it with your instance by issuing the following command:
   `cp inst_dir/admin/samples/dniczcus.prf /var/ftmswift_v300/cus/dnicus_DNIvINST`
3. Specify the access rights that allow another user (for example, the DB2 administrator) to access this file:
   `chmod 775 /var/ftmswift_v300/cus/dnicus_DNIvINST`

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 15 in "Preparing a CDP initialization file" on page 15.
   - If you installed FTM SWIFT in a directory other than `/opt/IBM/ftm/swift/v300`, 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/java7_64/jre
     ```

Authorizing users to perform customization tasks

To authorize users to act as customizers (ucust1) that is, to use the CDP to perform customization tasks:

1. Add their user IDs to the group dniadmin.
2. Add their user IDs to the group dnicusgr.

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 `/var/ftmswift_v300/cus`
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 `/var/ftmswift_v300/run`. To do this, issue the following command:

   ```
   cp inst_dir/run/samples/dniczpro.prf /var/ftmswift_v300/run/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 WebSphere BI for FN 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 WebSphere BI for FN runtime database tables.
DNI_DSN	Your current DB2 location	Location of the WebSphere BI for FN runtime database.
DNI_PATH	`/opt/IBM/ftm/swift/v300`	Installation directory of FTM SWIFT.
DNI_CONFPATH	Your current directory, for example `/etc`	Directory that contains the WebSphere BI for FN 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	`/var/ftmswift_v300/run`	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.

Environment variable	Value to be used	Description
DB2_PATH	Your current DB2 path, for example `/opt/IBM/db2/V10.1`	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/java7_64/jre`	Java installation directory.
DNI_WMQ_PATH	Your current WebSphere MQ path, for example `/usr/mqm`	Installation directory of WebSphere MQ.
DNI_WMB_PATH	Your current WebSphere Message Broker path, for example `/opt/IBM/mqsi/9.0.0.5`	Installation directory of WebSphere Message Broker.

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

```
chgrp dnilpp /var/ftmswift_v300/run/dniprofile
chmod 750 /var/ftmswift_v300/run/dniprofile
```

Chapter 4. Preparing the runtime system on which the database is located

This section describes steps you must take before you begin customizing the runtime system on which the database is located.

Extracting the class files

To extract the class files from the FTM SWIFT Java archives (files `.jar`):

1. Log on as a DB2 administrator (udb2adm1).
2. Run the customization profile contained in the following directory:

   `. /var/ftmswift_v300/cus/dnicus_`*`DNIvINST`*

   This customization profile was created during the procedure described "Preparing a customization profile" on page 15.
3. Enter the following command:

   `dnfxdrtn [-jar `*`jar_file_dir`*`] -t /var/ftmswift_v300/run/routines/`*`DNIvINST`*

   where:

   jar_file_dir
   : The directory that contains the `dnfcdrtn.jar` file. The default is `$DNI_PATH/run/classes`.

   DNIvINST
   : The name of the FTM SWIFT instance.

   This command extracts the class file from the `.jar` file and stores it into following directory:

   `/var/ftmswift_v300/run/routines/`*`DNIvINST`*`/com/ibm/dnf/dbm/rtn`

   If the return code is not 0, check the log file dnfrundb.log and trace file dnfrundb.trc. These files are located in the current directory.

Chapter 5. Creating deployment data for migration

The FTM SWIFT 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 WebSphere BI for FN layout of the V3.1.1 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 AIX on the customization system as a customizer (ucust1).
2. Change to the WebSphere BI for FN customization directory (for example, `/var/dni_03_01/cus`) by issuing the following command:
   ```
   cd /var/dni_03_01/cus
   ```
3. Run your WebSphere BI for FN customization profile, for example:
   ```
   . ./dnicus_DNIvINST
   ```
4. Start the CDP and restore (export) your current WebSphere BI for FN CDD, for example:
   ```
   dnicdp -i DNIvINST
   export cdd/DNIvINST.cdd
   quit
   ```
5. Copy your restored WebSphere BI for FN CDD to the new CDD directory `/var/ftmswift_v300/cus/cdd`, for example:
   ```
   cp /var/dni_03_01/cus/cdd/DNIvINST.cdd /var/ftmswift_v300/cus/cdd/DNIvINST.cdd
   ```
6. Change to the customization directory by issuing the following command:
   ```
   cd /var/ftmswift_v300/cus
   ```
7. Edit the CDD `/var/ftmswift_v300/cus/cdd/DNIvINST.cdd`. Change the values of following placeholders:

   DNIvPATH
   Specify the new installation directory, for example:
   ```
   /opt/IBM/ftm/swift/v300
   ```
8. Remove following placeholders, if they exist:
   - DNFvMWE (for each OU where it has been assigned to)
   - DNFvPATH
   - DNFvSG05
   - DNQvPATH
9. Run your FTM SWIFT customization profile, for example:
   ```
   . ./dnicus_DNIvINST
   ```
10. Use the CDP to generate the deployment data needed to migrate your instance:
    a. Start the CDP in **customization mode**, for example:
       ```
       dnicdp -i DNIvINST
       ```
    b. Enter the command to import your CDD, for example:
       ```
       import cdd/DNIvINST.cdd
       ```

If the import command issues following error message:

```
DNIZ9383E: The CDD contains incorrect Broker section.
           Run supplement command.
```

stop here and check that the required WebSphere BI for FN PTFs are installed. If they are not installed, install it now and then continue.

c. Issue the prepare command for the target CDD, for example:

   ```
   prepare
   ```

   The generated deployment instructions are stored in the file:

   deployment_dir/*DNIvINST*/*timestamp*/instructions.txt

d. To quit the CDP session, enter:

   ```
   quit
   ```

Attention: The migration of your customization data to FTM SWIFT 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 6. Modifying broker resources

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

1. On the runtime system, log on to AIX as a broker administrator (uwmba1).
2. Create the new FTM SWIFT broker profile by copying the sample profile to your home directory. For example:

   ```
   cp /opt/IBM/ftm/swift/v300/run/samples/dniczbrk.sh /home/uwmba1/dniczbrk.sh
   ```
3. Edit the FTM SWIFT broker profile:
   a. Set the DB2INSTANCE variable to the value you are currently using in WebSphere BI for FN.
   b. Check the DNI_WMQ_PATH environment variable. Its value must correspond to the IBM MQ installation path, for example, `/usr/mqm`.
   c. Check the DNI_JAVA_LIBPATH environment variable. Its value must correspond to the Java 64-bit library path, for example:

      ```
      /usr/java7_64/jre/lib/ppc64/j9vm
      ```
   d. Check the DNI_INSTALLATION_PATH environment variable. Its value must correspond to the FTM SWIFT installation path, for example: /opt/IBM/ftm/swift/v300.
   e. Check the ODBCINI environment variable. Its value must correspond to the file you created when you set up ODBC for your broker.
   f. Check the ODBCSYSINI environment variable. Its value must correspond to the file you created when you set up ODBC for your broker.
   g. If the MSIF services are to be used, remove the hash character (#) from the following statement:

      ```
      #export MQSI_THREAD_STACK_SIZE=3000000
      ```
   h. If runtime directories other than the defaults are to be used and you do not use the system wide dni.conf in the `/etc` directory, remove the hash character (#) from the following statements:

      ```
      #DNI_CONF=dni_conf_dir
      #export DNI_CONFPATH=$DNI_CONF
      ```

      where *dni_conf_dir* represents the directory that contains the FTM SWIFT configuration file that defines the runtime directories that are to be used.
4. Make a backup copy of your current WebSphere BI for FN broker profile. Issue the following command:

   ```
   cp work_path/common/profiles/dnixzbrk.sh /home/uwmba1/dnixzbrk.sh
   ```

   where *work_path* represents the work-path directory of the message broker, for example, `/var/mqsi`.

Chapter 7. 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
```

Part 4. Switching to FTM SWIFT

After all preparation steps have been carried out for a WebSphere BI for FN instance, carry out the following steps to switch it to FTM SWIFT.

Note: 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 WebSphere BI for FN V3.1.1 to FTM SWIFT Version 3.0.0, re-create your current runtime environment as described in Part 8, “Handling migration problems,” on page 57.

Chapter 8. Stopping message and file processing

Stop all WebSphere BI for FN 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 WebSphere BI for FN. To do this, identify which of the MERVA functions listed in the DSLKPROC TYPE=SEND section (ALLSENDQ) are relevant to WebSphere BI for FN, 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 *WebSphere BI for FN: System Administration*.
   d. Stop the sending of FIN messages by stopping these message flows:
      - DNF_ILC_FIN
      - DNF_PF_IS

      You can do this in one of the following ways:
      - By using the Message Broker Toolkit
      - By issuing the mqsistopmsgflow command
   e. 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 *WebSphere BI for FN: System Administration*.

3. Stop the RM transfer service message flow (DNF_L_TR).
4. Stop the message printing service. To do this, log on as a message print administrator and issue a stop command for each print queue:

```
dnicli -s DNQ_P_CMD -ou <ou>
stop -qname %
.quit
```

5. Stop the SAGs and SAG Add-Ons as described in *WebSphere BI for FN: System Administration*.
6. Stop the WebSphere BI for FN WAS applications.
7. Disable the automatic starting of the WebSphere BI for FN WAS applications.

Chapter 9. Removing WebSphere BI for FN message flows

Remove all WebSphere BI for FN message flows in one of the following ways:

- Delete the WebSphere BI for FN message flows from the corresponding execution groups.

  To do this, either:

  – Use a Message Broker Toolkit

  – Issue the **mqsideploy** command.

  Note: If you have defined execution group specific values, it avoids that all special settings for this group will be removed.
- Delete all WebSphere BI for FN execution groups, if all WebSphere BI for FN message flows are contained in execution groups that contain **only** WebSphere BI for FN message flows.

  To do this, either:

  – Use a Message Broker Toolkit

  – Issue the **mqsideleteexectutiongroup** command.

Regardless of which method you use to delete execution groups or to remove the flows:

1. Wait for the response from the corresponding job or command.
2. Ask the broker operator to stop the brokers of the WebSphere BI for FN instance that is being migrated.

Chapter 10. Backing up runtime database

Back up the WebSphere BI for FN V3.1.1 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 is to begin.

To back up the WebSphere BI for FN V3.1.1 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 WebSphere BI for FN runtime database. For example:

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

2. If list command returns the following warning, the next step 3 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 WebSphere BI for FN database are terminated. For example:

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

4. Back up the runtime database. For example:

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

Chapter 11. 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. Make a backup copy of your DB2 administrator profile.

   ```
   cp .profile .profile.bak
   ```
4. Update the CLASSPATH in your DB2 administrator profile:

   Replace the old routine-instance directory by the new directory:

   ```
   /var/dni_03_01/run/routines/DNIvINST
   by
   /var/ftmswift_v300/run/routines/DNIvINST
   ```

   Remove the WebSphere BI for FN cryptographic archive from the profile:

   ```
   wbifn_inst_dir/dniv311/run/classes/dnicrypto.jar
   ```

   where *wbifn_inst_dir* is your current WebSphere BI for FN installation directory.
5. Check the PATH environment variable. Its value must include the Java 7 path, for example:

   ```
   export PATH=/usr/java7_64/bin:$PATH
   ```
6. Copy the FTM SWIFT cryptographic archives into the DB2 function folder and set the access rights:

   ```
   cp inst_dir/run/classes/dnicsl.* db2_instance_dir/sqllib/function/jar/
   chmod 750 db2_instance_dir/sqllib/function/jar/dnicsl.*
   chgrp dnilpp db2_instance_dir/sqllib/function/jar/dnicsl.*
   ```
7. Run your DB2 administrator profile and restart the database system.
8. Run your customization profile:

   ```
   . /var/ftmswift_v300/cus/dnicus_DNIvINST
   ```
9. Migrate the stored procedures and bind packages. For this, issue the following command in one line:

   ```
   dnixdcsp -sn DNIvSN -d DNIvDSN
    -port db2_port -user db2_admin -pwd db2_admin_pwd
    -f deployment_dir/DNIvINST/admin/dnixzmsp.ddl
    -t /var/ftmswift_v300/run/routines/DNIvINST -m
   ```

   where

   DNIvSN
   : The existing name of the DB2 schema used in WebSphere BI for FN.

   DNIvDSN
   : The existing name of the DB2 location of the WebSphere BI for FN runtime database.

   DNIvINST
   : The existing name of your WebSphere BI for FN instance.

   db2_port
   : DB2 port if your database is located on a remote system.

   db2_admin
   : DB2 administrator id, for example db2inst1.

db2_admin_pwd
Password of your DB2 administrator.

deployment_dir
Your **new** deployment data directory of FTM SWIFT.

10. If you have configured the SIPN FIN service, bind the FSM. For this, issue the following commands:

```
db2 connect to DNIvDSN
db2 bind inst_dir/run/data/dnfcwdbs.bnd collection DNFvCOLLID qualifier DNIvSN grant public
db2 connect reset
```

where

DNIvDSN
The existing name of the DB2 location of the WebSphere BI for FN runtime database.

DNIvSN
The existing name of the DB2 schema used in WebSphere BI for FN.

DNFvCOLLID
The existing collection ID of the SIPN FIN services.

inst_dir
The FTM SWIFT installation directory.

11. To migrate the RDU history table, select the file *deployment_dir*/*DNIvINST*/admin/dnicdmig.ddl. If you want to keep the content of the RDU history table, remove the comment symbols from the insert statement. Execute following commands:

```
db2 connect to DNIvDSN
db2 -t -v -n -s -f deployment_dir/DNIvINST/admin/dnicdmig.ddl
db2 connect reset
```

12. Log on as a WebSphere Message Broker administrator (for example, uwmba1).
13. Copy the prepared FTM SWIFT broker profile (see 2 on page 23) to the work-path directory of the WebSphere Message Broker. For this, issue the following commands:

```
cp /home/uwmba1/dniczbrk.sh work_path/common/profiles/dniczbrk.sh
chmod +x work_path/common/profiles/dniczbrk.sh
```

where *work_path* represents the mqsi work-path directory of the WebSphere Message Broker, for example /var/mqsi. This profile is processed when the broker starts.

14. Remove the old WebSphere BI for FN broker profile. For this, issue the following command:

```
rm work_path/common/profiles/dnixzbrk.sh
```

15. To enable the broker to load FTM SWIFT LIL files, enter the following command on a single line:

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

16. Log out your WebSphere Message Broker administrator.
17. If you did not backup your application server profiles in Chapter 7, “Backing up application server profiles,” on page 25, perform it now.
18. Ensure that all existing WebSphere BI for FN and future FTM SWIFT 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 17. If your installation

does not use a centrally maintained version of dniprofile, assure all administrators will use an updated version of their profile too.

19. On the runtime system, log on as a WebSphere BI for FN security administrator (ua1 or ua2) or system configuration administrator (sa1 or sa2).
20. Rename the WebSphere BI for FN runtime file system, for example issue the following commands:

    ```
    mv /var/dni_03_01/run /var/dni_03_01/run_old
    mv /var/dnf_03_01/run /var/dnf_03_01/run_old
    ```

21. If you used a dni.conf file in WebSphere BI for FN, ask your root system administrator to backup your WebSphere BI for FN dni.conf file. For example:
    - To backup the file if the default configuration directory was used, issue the following command:

      ```
      cp /etc/dni.conf /home/sa1/dni.conf.old
      ```

    - To backup the file if an instance-specific configuration directory was used, issue the following command:

      ```
      cp /var/dni/DNIvINST/dni.conf /home/sa1/dni.conf.old
      ```

      where /var/dni/*DNIvINST* is a directory you created to serve as instance configuration directory.

22. If you used a dni.conf file in WebSphere BI for FN, ask your root system administrator to copy the prepared FTM SWIFT dni.conf file (see "Configuring the instance for runtime file system mount point" on page 10) to a directory to which the group DNILPP has read access. For example:
    - To copy the file to the default configuration directory that applies to all instances, issue the following command:

      ```
      cp /home/sa1/dni.conf /etc/dni.conf
      ```

    - To copy the file to an instance-specific configuration directory, issue the following commands:

      ```
      cp /home/sa1/dni.conf /var/dni/DNIvINST/dni.conf
      chgrp dnilpp /var/dni/DNIvINST/dni.conf
      chmod 750 /var/dni/DNIvINST/dni.conf
      ```

      where /var/dni/*DNIvINST* is a directory you created to serve as instance configuration directory.

23. The deployment data that you will use to migrate your instance was generated when you carried out the steps described in Chapter 5, "Creating deployment data for migration," on page 21. The deployment instructions were generated to a file with a name of the form:

    deployment_dir/DNIvINST/*timestamp*/instructions.txt

    Carry out the deployment instructions for following resource classes:
    - MBRK (deploy all message flows)
    - CFGPF (install WAS applications)

    Note: During installation of WAS applications you get following warning messages that can be ignored:

```
WARNING: J2C authentication alias instance_Runtime_AuthAlias already configured.
WARNING: J2C authentication alias instance_RefData_AuthAlias already configured.
WARNING: JDBC Provider instance_JDBC_Provider already configured.
WARNING: Data source instance_Runtime_DS already configured.
WARNING: Data source instance_RefData_DS already configured.
WARNING: Queue instance_RCP_Queue already configured.
WARNING: Queue instance_RSP_Queue already configured.
WARNING: Queue instance_Remote_Event_Queue already configured.
```

24. To activate FTM SWIFT 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 WebSphere BI for FN 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.
25. If you deleted the WebSphere BI for FN execution groups in Chapter 9, “Removing WebSphere BI for FN message flows,” on page 31 add your specific settings to the created FTM SWIFT execution groups.
26. Start the SAGs and SAG Add-Ons as described in *WebSphere BI for FN: System Administration*.
27. If you have installed FTM SWIFT WAS applications, ask the WebSphere Application Server operator (root) to start these applications.
28. If you use WebSphere BI for FN nodes or message sets in your own message flows, or if you modified WebSphere BI for FN sample message flows, you must update your Toolkit environment:
    a. Backup the broker archive (BAR) files that include WebSphere BI for FN resources.
    b. Install the nodes or sample message flows provided by FTM SWIFT and prepare the WebSphere Message Broker Toolkit workstation. See the section "Preparing the WebSphere Message Broker Toolkit workstation" in http://www.ibm.com/support/knowledgecenter/SSRH46_3.0.0_SWS/preparing_toolkit_ws.html 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 12. Update WebSphere BI for FN configuration entities

Changes to certain configuration entities (COs) are necessary to ensure that FTM SWIFT 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 new installation directory /opt/IBM/ftm/swift/v300:
   a. Make a note of your current value so that it is available if you need to fall back:

      ```
      dnicli -s DNI_SYSADM -ou SYSOU
      list -ou SYSOU -ct DniFileDir -co DniMessageFiles -attr Path -lo V
      ```

      The list command returns your current value, for example:

      ```
      DNIP3301I /opt/IBM/dniv311/run/msg
      ```

   b. Update the value. Enter the installation directory you specified in placeholder DNIvPATH. For this, issue 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 /opt/IBM/ftm/swift/v300.

      To complete the update, issue 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.

   c. End the CLI session:

      ```
      .quit
      ```

3. If you customized the SIPN FIN or FMT FIN service:
   a. For each OU, verify your FSM instance directory:

      Issue the following list command to the DNI_SYSADM service for SYSOU.

      ```
      dnicli -s DNI_SYSADM -ou SYSOU
      list -ou DNIvOU -ct DnfLT -co % -attr FSMInstanceDir -lo OV
      ```

      If the list command returns

      ```
      DNIP3301I ltname /var/dnf_03_01/run/fsm
      or
      DNIP3301I ltname /var/dni_03_01/run/fsm
      ```

      make a note of these values.

      Issue for each LT following commands:

```
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:

  ```
  /var/ftmswift_v300/run/fsm
  ```

To complete the configuration, issue 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 /opt/IBM/ftm/swift/v300:

   Backup your current value so that it is available if you need to fall back:

   ```
   list -ou SYSOU -ct DniFileDir -co DnfMessageFilesFin -attr Path -lo V
   ```

   The list command returns your current value, for example:

   ```
   DNIP3301I /opt/IBM/dnfv311/run/msg
   ```

   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
   ```

4. If you customized the MSIF service:

   a. Adapt the message files directory for MSIF to your new installation directory /opt/IBM/ftm/swift/v300:

      Backup your current value so that it is available if you need to fall back:

      ```
      dnicli -s DNI_SYSADM -ou SYSOU
      list -ou SYSOU -ct DniFileDir -co DnfMessageFilesMsif -attr Path -lo V
      ```

      The list command returns your current value, for example:

      ```
      DNIP3301I /opt/IBM/dnfv311/run/msg
      ```

      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
```

5. If you customized the MER service:

a. Adapt the message files directory for MER to your new installation directory /opt/IBM/ftm/swift/v300:

Backup your current value so that it is available if you need to fall back:

```
dnicli -s DNI_SYSADM -ou SYSOU
list -ou SYSOU -ct DniFileDir -co DnqMessageFiles -attr Path -lo V
```

The list command returns your current value, for example:

```
DNIP3301I /opt/IBM/dnqv311/run/msg
```

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
```

Part 5. Verifying FTM SWIFT

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

To verify your BAR file deployment, complete the following task:

1. On the runtime system, log on to AIX as a broker administrator (uwmba1).
2. List the version of the system administration flow deployed on your broker (for example, MQM1BRK):

   ```
   . /var/ftmswift_v300/run/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: 3.0.0.3.20161202-1634
   ```

To verify the cryptographic services used by the CLI:

1. On the runtime system, log on to AIX as an FTM SWIFT system configuration administrator (sa1 or sa2).
2. Enter 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.

To verify that the SIPN FIN service works:

1. On the runtime system, log on to AIX as a user who has the role SWIFTNetFINOperator for any one OU.
2. 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.

To verify that the SAG AddOn can be connected and works:

1. On the runtime system, log on to AIX as a SagAdmin.
2. Issue following commands:

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

all LAU keys that were already created must be listed.

To verify the MSIF services:

1. On the runtime system, log on as a FTM SWIFT security administrator (ua1 or ua2).
2. Run dniprofile by entering the following command:

   ```
   . /var/ftmswift_v300/run/dniprofile
   ```

3. 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'.
   ```

4. 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.
   ```

To verify that the enterprise applications are installed and correctly configured:

1. 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.
2. Allow the chosen user to log in to the application server and to use the corresponding enterprise application.
3. 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/**.

4. 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.

After all verification steps are successfully done, confirm that the deployment of the FTM SWIFT CDD is complete. To do this:

1. Log in as a customizer (ucust1).
2. Change to the customization directory by issuing the following command:
   ```
   cd /var/ftmswift_v300/cus
   ```
3. Run your FTM SWIFT customization profile, for example:
   ```
   . ./dnicus_DNIvINST
   ```
4. Start the CDP in customization mode, for example:
   ```
   dnicdp -i DNIvINST
   ```
5. Import your current CDD, for example:
   ```
   import cdd/DNIvINST.cdd
   ```
6. Implement your current CDD, for example:
   ```
   implement
   ```
7. To quit the CDP session, enter:
   ```
   quit
   ```

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 your system is cleaned, you will no longer be able to fall back to WebSphere BI for FN V3.1.1.

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

1. Remove the WebSphere BI for FN customization and runtime environment, for example:
   ```
   rm -R /var/dni_03_01
   rm -R /var/dnf_03_01
   ```
2. Remove all WebSphere BI for FN customization and runtime profiles.
3. While preparing for migration, a backup from your WebSphere BI for FN 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.
4. Delete the backup copy of the WebSphere Message Broker administrator profile (dnixzbrk.sh).
5. Uninstall the WebSphere BI for FN WAS applications using the WAS administration console.
6. Remove the backup copy of your application server profile.
7. Remove the backup copy of your BAR-files.
8. Drop the obsolete DB2 table DNI_RDU_HISTORY_BAK.
9. Uninstall WebSphere BI for FN V3.1.1. For example, as root user issue following command:
   ```
   wbifn_inst_dir/dniv311/_uninst/uninstaller
   ```

   Note: The broker must be stopped before you can uninstall the product.
10. Skip this step if you have not customized the SIPN FIN or FMT FIN service. With the SIPN FIN and FMT FIN service some EIAS resources have been created. To remove these obsolete resources:
    a. On the runtime system, log on as a system configuration administrator (sa1 or sa2) and run the profile for your runtime environment by entering:
       ```
       . /var/ftmswift_v300/run/dniprofile
       ```
       Create a temporary directory where dnfczmlc stores the CLI command files which will contain the configuration remove statements.
       Switch to this directory and enter the following command:
       ```
       dnfczmlc -i instance [-dual YES|NO] [-to timeout]
       ```
       where

       -i instance
       The name of the instance.

       -dual YES|NO
       Specifies whether files are to be created for a system that uses dual authorization for SYSOU. The default is -dual YES. Specify -dual NO only if dual authorization is to be turned off for both DNI_SYSADM and DNI_SECADM in SYSOU at the time when the created files are executed. Whether dual authorization is switched on or off for other OUs is irrelevant.

-to timeout

The number of milliseconds that the CLI waits for a response to this command before it issues an error message. The default is 100000 (100 seconds). It must be a whole number between 20000 and 9999999.

The program dnfczmlc creates the following CLI command files:

- If dual authorization is not used (-dual NO):

  1. dnfczmlc_1_ua_rem_ro_all.cli
  2. dnfczmlc_2_sa_ent_all.cli

- If dual authorization is used (-dual YES):

  1. dnfczmlc_1_ua_rem_ro_com.cli
  2. dnfczmlc_1_ua_rem_ro_app.cli
  3. dnfczmlc_2_sa_rem_cos_com.cli
  4. dnfczmlc_2_sa_rem_cos_dep.cli
  5. dnfczmlc_3_sa_rem_co_com.cli
  6. dnfczmlc_3_sa_rem_co_dep.cli
  7. dnfczmlc_4_sa_rem_ct_com.cli
  8. dnfczmlc_4_sa_rem_ct_dep.cli

Execute the CLI command files in the following sequence and using the following user authorization:

- If dual authorization is not used (-dual NO):

```
Any security administrator
dnicli -s DNI_SECADM -ou SYSOU -cft dnfczmlc_1_ua_rem_ro_all.cli | tee -a dniconfig.log

Any system configuration administrator
dnicli -s DNI_SYSADM -ou SYSOU -cft dnfczmlc_2_sa_ent_all.cli | tee -a dniconfig.log
```

- If dual authorization is used (-dual YES):

```
A first security administrator
dnicli -s DNI_SECADM -ou SYSOU -cft dnfczmlc_1_ua_rem_ro_com.cli | tee -a dniconfig.log

A second security administrator
dnicli -s DNI_SECADM -ou SYSOU -cft dnfczmlc_1_ua_rem_ro_app.cli | tee -a dniconfig.log

A first system configuration administrator
dnicli -s DNI_SYSADM -ou SYSOU -cft dnfczmlc_2_sa_rem_cos_com.cli | tee -a dniconfig.log
dnicli -s DNI_SYSADM -ou SYSOU -cft dnfczmlc_3_sa_rem_co_com.cli | tee -a dniconfig.log
dnicli -s DNI_SYSADM -ou SYSOU -cft dnfczmlc_4_sa_rem_ct_com.cli | tee -a dniconfig.log

A second system configuration administrator
dnicli -s DNI_SYSADM -ou SYSOU -cft dnfczmlc_2_sa_rem_cos_dep.cli | tee -a dniconfig.log
dnicli -s DNI_SYSADM -ou SYSOU -cft dnfczmlc_3_sa_rem_co_dep.cli | tee -a dniconfig.log
dnicli -s DNI_SYSADM -ou SYSOU -cft dnfczmlc_4_sa_rem_ct_dep.cli | tee -a dniconfig.log
```

Part 7. Migrating SAG Add-On

This part describes how to migrate your WebSphere BI for FN SAG Add-On to the level of FTM SWIFT.

Chapter 13. Planning

This chapter discusses the prerequisite products that you need to install on your SAG workstation before you can install and use the SAG Add-On delivered with FTM SWIFT. These include:

- Determine the software level of your operating system, the installed SAG and of the installed MQ Client. Check against the software requirements which are described on the following website:

  `http://www.ibm.com/software/industry/financial-transaction-manager/requirements`
- Ensure that the required Java version is installed.
- Ensure that the IBM Installation Manager is installed.
- Decide if you want to prepare a new environment. With this, plan for a new SAG workstation.

Chapter 14. 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 system:
   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 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/SAGAddOn from your FTM SWIFT installation.

   Transfer:

   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.
6. Install IBM Installation Manager if it is not already installed.

Chapter 15. 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, stop message and file processing as documented in Chapter 8, “Stopping message and file processing,” on page 29.
2. If you have more than one SAG workstation connected to FTM SWIFT, 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 on your SAG workstation.
   - For AIX, issue the stopsrc command.
   - For Solaris, issue the dnfsssub command.
   - For Windows, open the Windows Services Management Console, click Start→ Settings→ Control Panel→ Administrative Tools→ Services, select **WBI for FN - SAG Add-On** from the list of services and click **Stop** in the action menu.

   For more information, see chapter 'Operating an SAG Add-On' in *WebSphere BI for FN: System Administration*.
5. If needed, upgrade your operating system.
6. Upgrade your SAG to SAG 7.0.50.
7. Upgrade your WebSphere MQ Client to 7.5.0.2.
8. Install the required Java version.
9. Uninstall your current SAG Add-On by running the following program:
   - On AIX or Solaris:

     `sao_inst_dir/_uninst/uninstaller`
   - On Windows:

     `sao_inst_dir\_uninst\uninstaller.exe`

   where *sao_inst_dir* represents the installation directory of the SAG Add-On.
10. Delete the installation directory of the current level of the SAG Add-On with all its remaining content.
11. Install the SAG Add-On from FTM SWIFT. For this, you need following information:
    - The name of the installation directory. The default directory is `/opt/IBM/ftm/SAGAddOn`
    - The SWIFT Remote API Host Adapter (RAHA) information and the Java (JRE) installation directory. For more information, see step 3 on page 53.

    How to install the SAG Add-On is described in http://www.ibm.com/support/knowledgecenter/SSRH46_3.0.0_SWS/installing_sao.html
12. Copy your saved SAG Add-On profile (dnfcssao.cfg) from your temporary directory to the directory in which the SAG Add-On is installed.
13. Edit your SAG Add-On profile. Update the XML element <ResourceBundleDirectory>. Specify the path to the directory that holds the SAG Add-On resource bundle, for example, on AIX or Solaris: *sao_inst_dir*/res, on Windows: *sao_inst_dir*\res, where *sao_inst_dir* represents the directory in which the SAG Add-On is installed.

14. Make the Remote Application (RA) user the owner of the profile and grant read and write permission.

Part 8. Handling migration problems

This part describes how to handle problems during migration.

Chapter 16. Falling back to WebSphere BI for FN

Falling back means returning to WebSphere BI for FN V3.1.1. 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 WebSphere BI for FN V3.1.1 to FTM SWIFT, falling back is possible only if:

- You have not carried out the steps described in Part 6, "Cleaning up obsolete resources," on page 47.
- 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 after the Switching phase.
- No PTFs were applied in FTM SWIFT after the Switching phase. If PTFs were applied and you still need to fall back, contact your IBM service representative.
- You have not migrated your SAG Add-On.

To fall back from FTM SWIFT to WebSphere BI for FN, 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 8, "Stopping message and file processing," on page 29.
2. If you have already deployed flows in FTM SWIFT in step 23 on page 37, remove them in the way described in Chapter 9, "Removing WebSphere BI for FN message flows," on page 31.
3. If you have installed the Administration and Operation (AO) Facility, the Message Entry and Repair (MER) Facility, or Relationship Management Application (RMA) log on as a root system administrator to:
   a. Stop and uninstall all FTM SWIFT applications.
   b. Start all WebSphere BI for FN applications.
   c. Enable the automatic starting of the WebSphere BI for FN WAS applications.
4. If you used a dni.conf file in WebSphere BI for FN, ask your root system administrator to restore the dni.conf file (see step 21 on page 37). For example:
   - To copy the file to the default configuration directory that applies to all instances, issue the following command:
     ```
     cp /home/sa1/dni.conf.old /etc/dni.conf
     ```
   - To copy the file to an instance-specific configuration directory, issue the following command:
     ```
     cp /home/sa1/dni.conf.old /var/dni/DNIvINST/dni.conf
     ```
     where `/var/dni/DNIvINST` is a directory you created to serve as instance configuration directory.
5. Ask your WebSphere BI for FN system configuration administrator to retrieve the WebSphere BI for FN runtime file system (see 20 on page 37), for example issue the following command:
   ```
   mv /var/dni_03_01/run_old /var/dni_03_01/run
   mv /var/dnf_03_01/run_old /var/dnf_03_01/run
   ```

6. Ask your broker administrator (uwmba1) to restore your WebSphere BI for FN broker profile that you saved in step 4 on page 23. Issue the following commands:

   ```
   cp /home/uwmba1/dnixzbrk.sh work_path/common/profiles/dnixzbrk.sh
   rm work_path/common/profiles/dniczbrk.sh
   ```

   where *work_path* represents the work-path directory of the message broker, for example, /var/mqsi.
7. Instruct all WebSphere BI for FN system configuration administrators and security administrators to revert to using the runtime profile file that correspond to WebSphere BI for FN, for example:

   ```
   /var/dni_03_01/run/dniprofile
   ```
8. On the runtime system, log on as a DB2 administrator (udb2adm1).
9. Stop all DB2 applications and the database system.
10. Update the CLASSPATH in your DB2 administrator profile:

    Add the following line to the profile:

    ```
    export CLASSPATH=wbifn_inst_dir/dniv311/run/classes/dnicrypto.jar:$CLASSPATH
    ```

    where *wbifn_inst_dir* is your WebSphere BI for FN installation directory.

    Replace the FTM SWIFT routine-directory by the WebSphere BI for FN routine-directory:

    ```
    /var/ftmswift_v300/run/routines/DNIvINST
    by
    /var/dni_03_01/run/routines/DNIvINST
    ```
11. Remove the FTM SWIFT cryptographic archives from the DB2 function folder:

    ```
    rm db2_instance_dir/sqllib/function/jar/dnicsl.*
    ```
12. Run your DB2 administrator profile and restart the database system.
13. Restore the WebSphere BI for FN runtime data from the backup copy (see Chapter 10, “Backing up runtime database,” on page 33).
    a. Issue the following commands:

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

       DNIvDSN
       The existing name of the DB2 location of the WebSphere BI for FN runtime database (for example, DNIDBRUN).
14. Run the WebSphere BI for FN customization profile:

    ```
    . /var/dni_03_01/cus/dnicus_DNIvINST
    ```
15. Restore the stored procedures and bind packages. For this, issue the following command in one line:

    ```
    dnixdcsp -sn DNIvSN -d DNIvDSN
     -port db2_port -user db2_admin -pwd db2_admin_pwd
     -f wbifn_deployment_dir/DNIvINST/admin/dnixzrst.ddl
     -t /var/dni_03_01/run/routines/DNIvINST -m
    ```

    where

    DNIvSN
    The existing name of the DB2 schema used in WebSphere BI for FN.

    DNIvDSN
    The existing name of the DB2 location of the WebSphere BI for FN runtime database.

DNIvINST
The name of your WebSphere BI for FN instance.

db2_port
DB2 port if your database is located on a remote system.

db2_admin
DB2 administrator id, for example db2inst1.

db2_admin_pwd
Password of your DB2 administrator.

wbifn_deployment_dir
The deployment directory of WebSphere BI for FN.

16. If you have configured the SIPN FIN service, bind the FSM. For this, issue the following commands:

```
db2 connect to DNIvDSN
db2 bind wbifn_inst_dir/dnfv311/run/data/dnfcwdbs.bnd collection DNFvCOLLID qualifier DNIvSN grant public
db2 connect reset
```

where

DNIvDSN
The existing name of the DB2 location of the WebSphere BI for FN runtime database.

DNIvSN
The existing name of the DB2 schema used in WebSphere BI for FN.

DNFvCOLLID
The existing collection ID of the SIPN FIN services.

wbifn_inst_dir
The WebSphere BI for FN installation directory, for example, /opt/IBM.

17. On the runtime system, log on to AIX as a WebSphere Message Broker administrator (uwmba1).
18. Issue the following mqsichangebroker command on a single line:

```
mqsichangebroker broker -l wbifn_inst_dir/dniv311/run/lil64:
wbifn_inst_dir/dnfv311/run/lil64:
wbifn_inst_dir/dniv311/run/jplugin:
wbifn_inst_dir/dnfv311/run/jplugin:
wbifn_inst_dir/dnqv311/run/jplugin
```

where *wbifn_inst_dir* represents the WebSphere BI for FN installation directory.

Note:

- Include *wbifn_inst_dir*/dnfv311/run/jplugin only if the MSIF feature is used.
- Include *wbifn_inst_dir*/dnqv311/run/jplugin only if the MM feature is used.

19. Re-start all brokers that are associated with the WebSphere BI for FN instance.
20. Use the BAP tool to deploy WebSphere BI for FN V3.1.1 message flows again.
    a. Run the profile for your runtime environment by entering:
       ```
       . /var/dni_03_01/run/dniprofile
       ```
    b. Prepare and deploy the BAR-files by entering:
       ```
       dniczbap -cmd prepare -all -deploy
       ```
21. After all message flows were deployed, reactivate the collection of WebSphere BI for FN 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_level" -c active -n basic -o "xml"
mqsichangeflowstats broker -s -e eg -f "DNF_ILS_ACK_level" -c active -n basic -o "xml"
```

where:

broker
The name of your WebSphere BI for FN broker

eg The name of the FIN execution group

level The level of the message flow, for example 4480. To determine the level of a deployed message flow, enter the following command:

```
dniczbap -cmd list
```

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.

22. If you use WebSphere BI for FN nodes or message sets in your own message flows, or if you modified WebSphere BI for FN sample message flows, deploy your saved BAR files. After this, re-establish your Toolkit environment. See the section "Preparing the WebSphere Message Broker Toolkit workstation" in the *WebSphere BI for FN: Application Programming* for details.
23. Start the SAG Add-Ons and SAGs as described in *WebSphere BI for FN: System Administration*.
24. As a customizer, remove the customization definitions of FTM SWIFT. Issue following commands:

    ```
    cd /var/ftmswift_v300/cus/defs
    rm -R *
    ```

25. As a customizer, switch back to your previous customization environment. For this:
    a. Reuse your WebSphere BI for FN V3.1.1 customization profile dnicus_*DNIvINST*, for example located in /var/dni_03_01/cus.
    b. Reuse your WebSphere BI for FN V3.1.1 CDD *DNIvINST*.cdd, for example located in /var/dni_03_01/cus/cdd.
    c. Reuse your WebSphere BI for FN V3.1.1 ini-file *DNIvINST*.ini, for example located in /var/dni_03_01/cus.
26. Your WebSphere BI for FN V3.1.1 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 WebSphere BI for FN V3.1.1 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 support page, contact IBM service before you continue. Do not apply any new software level without confirmation by the IBM support team.

Chapter 17. Re-migrating after falling back to WebSphere BI for FN

If problems occurred during your initial attempt to migrate to FTM SWIFT 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.

To repeat the migration, follow the procedure described in this Migration Guide.

Chapter 18. Falling back SAG Add-On

Falling back means returning to the use of WebSphere BI for FN SAG Add-On. To fall back:

1. If you only have one SAG workstation connected to FTM SWIFT, stop message and file processing as documented in Chapter 8, “Stopping message and file processing,” on page 29.
2. If you have more than one SAG workstation connected to FTM SWIFT, 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 2a on page 53.

Part 9. Appendixes

Appendix A. Migrating from WebSphere Message Broker V8 to IBM Integration Bus Version 9.0.0.6

A WebSphere BI for FN V3.1.1 instance uses message brokers and toolkit provided by WebSphere Message Broker. This procedure describes how to migrate a WebSphere BI for FN V3.1.1 instance from WebSphere Message Broker V8 to IBM Integration Bus Version 9.0.0.6. The migration described by this procedure takes place within the same environment (that is, it is an in-place migration); it does not create a new environment for the migrated instance.

Preparing

To prepare your IBM Integration Bus V9, carry out the following steps:

1. Install IBM Integration Bus V9 software for both the broker and toolkit, including any required PTFs on the runtime system in parallel to your WebSphere Message Broker V8. However, after you install the software, do not modify your current broker or create a new broker, because that will be covered later in this procedure.
2. Install the following WebSphere BI for FN PTFs and carry out the migration steps:
   - UI42655 (Base, product level 3.1.1.29)
   - UI41572 (Message Management, product level 3.1.1.21)
   - UI38427 (Support for SWIFTNet FIN, product level 3.1.1.13)
   - UI41762 (Messaging Services for SWIFTNet InterAct and FileAct, product level 3.1.1.19)
3. To prepare your WebSphere BI for FN environment, on the runtime system, log on as a **WebSphere BI for FN system configuration or security administrator**:
   a. Make a backup copy of your dniprofile, for example:
      ```
      cp /var/dni_03_01/run/dniprofile /var/dni_03_01/run/dniprofile_old
      ```
   b. Make a copy of your dniprofile, for example:
      ```
      cp /var/dni_03_01/run/dniprofile /var/dni_03_01/run/dniprofile_new
      ```
   c. Edit this copy. Adapt the environment variable DNI_WMB_PATH. It requires IBM Integration Bus V9. For example:
      ```
      /opt/IBM/mqsi/9.0.0.6
      ```
4. To prepare your broker, on the runtime system, log on as a **WebSphere Message Broker administrator** (uwmba1):
   a. Back up WebSphere Message Broker V8 resources. For more information, see the "Backing up WebSphere Message Broker Version 8 resources" topic of the IBM Integration Bus V9 Knowledge Center.
   b. Use the odbc initialization file as a template to create the file */var/mqsi/odbc/odbc9.ini*. For example, issue the following command:
      ```
      cp /opt/IBM/mqsi/9.0.0.6/ODBC/unixodbc/odbc.ini /var/mqsi/odbc/odbc9.ini
      ```
      To give the broker access permission to this file, enter the following command:
      ```
      chgrp mqbrkrs /var/mqsi/odbc/odbc9.ini
      ```
   c. Update the following lines in the /var/mqsi/odbc/odbc9.ini file:

```
[ODBC Data Sources]
runtime_dsn=IBM DB2 ODBC Driver
...
[runtime_dsn]
Driver=Your_DB2_install_directory/lib64/db2o.o
Description=WBIFN DB2 ODBC Database
Database=runtime_dsn
...
[ODBC]
...
InstallDir=Your_Broker_install_directory/ODBC/V7.0
```

where:

runtime_dsn
: Data source name of the runtime database.

Your_DB2_install_directory
: The DB2 installation directory (for example, /opt/IBM/db2/V10.1).

Your_Broker_install_directory
: The IBM Integration Bus installation directory (for example, /opt/IBM/mqsi/9.0.0.6).

d. Use the odbcinst initialization file as a template to create the file */var/mqsi/odbc/odbcinst.ini*. For example, issue the following command:

```
cp /opt/IBM/mqsi/9.0.0.6/ODBC/unixodbc/odbcinst.ini /var/mqsi/odbc/odbcinst.ini
```

To give the broker access permission to this file, enter the following command:

```
chgrp mqbrkrs /var/mqsi/odbc/odbcinst.ini
```

e. Update and verify the following line in the /var/mqsi/odbc/odbcinst.ini file:

```
[ODBC]
...
TraceFile=trace_dir/odbctrace.out
Threading=2
```

where:

trace_dir
: A directory with plenty of free space to hold trace output (for example, /tmp).

Verify that following line is included:

```
Threading=2
```

f. Backup your current profile by issuing the following command:

```
cp homedir/.profile homedir/.profile_old
```

where *homedir* represents the home directory of the WebSphere Message Broker administrator (uwmba1).

g. Prepare a new profile by issuing the following command:

```
cp homedir/.profile homedir/.profile_new
```

Edit this profile. Update the broker profile statement so that it looks like this:

```
. /opt/IBM/mqsi/9.0.0.6/bin/mqsiprofile
```

5. If you installed the WebSphere BI for FN Eclipse plug-ins in your V8 Toolkit, do this also in your V9 Toolkit. For more information about preparing the

toolkit workstation, see *WebSphere BI for FN: Application Programming*. To test any services that use nodes that are provided by WebSphere BI for FN, recreate your BAR files.

Switching

To switch from WebSphere Message Broker V8 to IBM Integration Bus V9, carry out the following steps:

1. Stop all sessions and services, for example:
   a. Stop all applications that send requests to WebSphere BI for FN.
   b. Log out SIPN FIN LTs.
   c. Close MSIF SnF input and output channels.
   d. Release SWIFTNet SnF queues.
   e. Stop the MSIF Message Transfer service.
   f. Stop the RM transfer service message flow (DNF_L_TR).
   g. Stop the message printing service.
   h. Close all dnicli sessions.
   i. Stop the SAGs and SAG Add-Ons.
   j. Stop the WebSphere BI for FN WAS applications.

   For more information about stopping sessions and services, see *WebSphere BI for FN: System Administration*.
2. On the runtime system, log on as a **WebSphere Message Broker administrator** (uwmba1):
   a. Stop all WebSphere MQ channels that are connected to the Version 8 broker.
   b. Stop the broker.
   c. Edit the WebSphere BI for FN broker profile dnixzbrk.sh. It is located in *work_path*/common/profiles/dnixzbrk.sh, where *work_path* represents the mqsi work-path directory of the WebSphere Message Broker, for example /var/mqsi.
      - Check the ODBCINI environment variable. It must correspond to 4b on page 69.
      - Check the ODBCSYSINI environment variable. It must correspond to 4d on page 70.
   d. Replace the profile of **WebSphere Message Broker administrator** (uwmba1). Issue the following command:

      ```
      cp home_dir/.profile_new home_dir/.profile
      ```
   e. Log out your **WebSphere Message Broker administrator** (uwmba1).
   f. Log on as a **WebSphere Message Broker administrator** (uwmba1). The new version of .profile is activated.
   g. Migrate the broker to the new target level by issuing the following command:

      ```
      mqsimigratecomponents brokername -t 9.0.0.6
      ```

      where *brokername* represents the name of your broker. Ensure that the following parameters are specified:

      -t The target level (for example, 9.0.0.6 for V9 Fix Pack 6).

      If the command ends with the BIP6123E error message, issue the MQ command dltmqlnk to resolve the problem and repeat this step.

h. Start the migrated broker. The verification program checks the configuration of the broker.

3. On the runtime system, log on as a **WebSphere BI for FN system configuration or security administrator**.
   a. Replace your dniprofile with the copy you modified in step 3 on page 69, for example:
      ```
      cp /var/dni_03_01/run/dniprofile_new /var/dni_03_01/run/dniprofile
      ```
   b. Ensure that all dnicli users use this profile.
4. To verify that the switching was successful, on the runtime system, log on as a **user with the monitoring (DniMonitor) role** in the system OU SYSOU:
   a. Run the new version of dniprofile that was created in step 3a by entering the following command:
      ```
      . /var/dni_03_01/run/dniprofile
      ```
   b. Test whether the WebSphere Message Broker subscription mechanism works for WebSphere BI for FN. To do this, depending on whether you have registered to receive WebSphere BI for FN events in the syslog (that is, depending on whether you use the event notification service DNI_N_EVENT), issue one of the following sets of commands:
      - If you have already registered to receive WebSphere BI for FN events in the syslog:
        ```
        dnicli -ou SYSOU -s DNI_MONITOR
        reg -ou DNIAAA
        .quit
        ```
      - If you have not registered to receive WebSphere BI for FN events in the syslog:
        ```
        dnicli -ou SYSOU -s DNI_MONITOR
        reg -sq prefix.DNI_N_EVENT
        reg -ou DNIAAA
        dreg -sq prefix.DNI_N_EVENT
        .quit
        ```

        where *prefix* represents the queue prefix set by the DNIvQPFX placeholder during customization.

      These commands register to receive events for an OU with the name DNIAAA. However, because an OU with this name does not exist, WebSphere BI for FN returns an error response and issues an error event. The error response on the console is similar to this one:
      ```
      DNIM5006E Access denied for user 'sa1'; command: 'reg'; OU: 'DNIAAA'.
      ```

      The switching was successful if your syslog contains an error event similar to this one:
      ```
      DNIM5007E 2015-12-03 13:12:27 SYSOU DNI_MONITOR
                Access denied for user 'sa1'; command: 'reg'; OU: 'DNIAAA'.
      ```
5. Migrate your WebSphere Message Broker Toolkit workspace to V9 as described in the IBM Integration Bus V9 Knowledge Center.
6. If you created BAR files in step 5 on page 70, deploy your message flows.

Cleaning up obsolete resources

After you have verified that the migration to IBM Integration Bus V9 was successful, carry out the following steps to remove obsolete resources from your system:

1. Remove the saved WebSphere Message Broker V8 resources.

2. Remove the saved WebSphere Message Broker Toolkit resources.
3. Uninstall WebSphere Message Broker V8.
4. Delete the following copies of dniprofile:

   ```
   /var/dni_03_01/run/dniprofile_old
   /var/dni_03_01/run/dniprofile_new
   ```

Falling back to Message Broker V8

Falling back means returning to the use of WebSphere Message Broker V8. Changes that you made to brokers, the WebSphere Message Broker Toolkit, and development resources after migration to V9 are not retained.

To fall back from IBM Integration Bus V9 to WebSphere Message Broker V8, carry out the following steps for each instance on the runtime system on which the broker runs:

1. Stop all sessions and services, for example:
   a. Stop all applications that send requests to WebSphere BI for FN.
   b. Log out SIPN FIN LTs.
   c. Close MSIF SnF input and output channels.
   d. Release SWIFTNet SnF queues.
   e. Stop the MSIF transfer service.
   f. Stop the RM transfer service message flow (DNF_L_TR).
   g. Stop the message printing service.
   h. Close all dnicli sessions.
   i. Stop the SAGs and SAG Add-Ons.
   j. Stop the WebSphere BI for FN WAS applications.

   For more information about stopping sessions and services, see *WebSphere BI for FN: System Administration*.
2. Restore the WebSphere Message Broker Toolkit to V8:
   a. Close all IBM Integration Bus Toolkit Version 9 sessions.
   b. Restore the Version 8 workspace from the backup that you took before migration.
   c. Restart WebSphere Message Broker Toolkit Version 8.
3. On the runtime system, log on as a **WebSphere Message Broker administrator** (uwmba1):
   a. Stop the V9 broker.
   b. Restore the broker to Version 8 by issuing the following command:

      ```
      mqsimigratecomponents brokername -s 9.0.0.6 -t 8.0.0.6
      ```

      where *brokername* represents the name of your broker. Ensure that the following parameters are specified:

      -s The source level (for example, 9.0.0.6 for V9 Fix Pack 6).

      -t The target level (for example, 8.0.0.6 for V8 Fix Pack 6).
   c. Restore your previous profile by issuing the following command:

      ```
      cp homedir/.profile_old homedir/.profile
      ```

      where *homedir* represents the home directory of the WebSphere Message Broker administrator (uwmba1).

d. Log off and login again as a WebSphere Message Broker administrator (uwmba1).

e. Issue the following command to start the broker:

```
mqsistart brokername
```

4. On the runtime system, log on as a **WebSphere BI for FN system configuration or security administrator**. Replace `/var/dni_03_01/run/dniprofile` with the backup copy created in step 3a on page 69 by issuing the following command:

```
cp /var/dni_03_01/run/dniprofile_old  /var/dni_03_01/run/dniprofile
```

5. To verify that the fallback was successful, on the runtime system, log on as a **user with the monitoring (DniMonitor) role** in the system OU SYSOU:

a. Run the dniprofile by entering the following command:

```
. /var/dni_03_01/run/dniprofile
```

b. Test whether the WebSphere Message Broker subscription mechanism works for WebSphere BI for FN. To do this, depending on whether you have registered to receive WebSphere BI for FN events in the syslog (that is, depending on whether you use the event notification service DNI_N_EVENT), issue one of the following sets of commands:

- If you have already registered to receive WebSphere BI for FN events in the syslog:

```
dnicli -ou SYSOU -s DNI_MONITOR
reg -ou DNIAAA
.quit
```

- If you have not registered to receive WebSphere BI for FN events in the syslog:

```
dnicli -ou SYSOU -s DNI_MONITOR
reg -sq prefix.DNI_N_EVENT
reg -ou DNIAAA
dreg -sq prefix.DNI_N_EVENT
.quit
```

  where *prefix* represents the queue prefix set by the DNIvQPFX placeholder during customization.

These commands register to receive events for an OU with the name DNIAAA. However, because an OU with this name does not exist, WebSphere BI for FN returns an error response and issues an error event. The error response on the console is similar to this one:

```
DNIM5006E Access denied for user 'sa1'; command: 'reg'; OU: 'DNIAAA'.
```

The fallback was successful if your syslog contains an error event similar to this one:

```
DNIM5007E 2015-12-03 13:12:27 SYSOU DNI_MONITOR
          Access denied for user 'sa1'; command: 'reg'; OU: 'DNIAAA'.
```

Re-migrating

If problems occurred during your initial attempt to migrate to IBM Integration Bus V9 and if you fell back to the previous software level and resolved these problems, you might want to re-attempt to migrate to V9. When you re-migrate, the procedure you follow is slightly different from the procedure you followed when you migrated the first time. To re-migrate:

1. Follow the procedure described in "Preparing" on page 69 but do not carry out the following steps:

- Step 1 on page 69
- Step 2 on page 69

2. Follow the procedure described in "Switching" on page 71.

Appendix B. Migrating from WebSphere Message Broker V7 to IBM Integration Bus Version 9.0.0.6

A WebSphere BI for FN V3.1.1 instance uses message brokers and toolkit provided by WebSphere Message Broker. This procedure describes how to migrate a WebSphere BI for FN V3.1.1 instance from WebSphere Message Broker V7 to IBM Integration Bus Version 9.0.0.6. The migration described by this procedure takes place within the same environment (that is, it is an in-place migration); it does not create a new environment for the migrated instance.

Note:
- WebSphere Message Broker Version 7 only supports DB2 V10.1 with Fix Pack 6. Therefore, WebSphere Message Broker Version 7 needs to be at least at level 7.0.0.6.
- WebSphere Message Broker Version 7 does not support WebSphere MQ Version 8. Therefore, WebSphere MQ needs to be at Version 7.1, at least at level 7.1.0.4.

Preparing

To prepare your IBM Integration Bus V9, carry out the following steps:

1. Install IBM Integration Bus V9 software for both the broker and toolkit, including any required PTFs on the runtime system in parallel to your WebSphere Message Broker V7. However, after you install the software, do not modify your current broker or create a new broker, because that will be covered later in this procedure.
2. Install the following WebSphere BI for FN PTFs and carry out the migration steps:
   - UI42655 (Base, product level 3.1.1.29)
   - UI41572 (Message Management, product level 3.1.1.21)
   - UI38427 (Support for SWIFTNet FIN, product level 3.1.1.13)
   - UI41762 (Messaging Services for SWIFTNet InterAct and FileAct, product level 3.1.1.19)
3. To prepare your WebSphere BI for FN environment, on the runtime system, log on as a **WebSphere BI for FN system configuration or security administrator**:
   a. Make a backup copy of your dniprofile, for example:
      ```
      cp /var/dni_03_01/run/dniprofile /var/dni_03_01/run/dniprofile_old
      ```
   b. Make a copy of your dniprofile, for example:
      ```
      cp /var/dni_03_01/run/dniprofile /var/dni_03_01/run/dniprofile_new
      ```
   c. Edit this copy. Adapt the environment variable DNI_WMB_PATH. It requires IBM Integration Bus V9. For example:
      ```
      /opt/IBM/mqsi/9.0.0.6
      ```
4. To prepare your broker, on the runtime system, log on as a **WebSphere Message Broker administrator** (uwmba1):
   a. Back up WebSphere Message Broker V7 resources. For more information, see the "Backing up WebSphere Message Broker Version 7 resources" topic of the IBM Integration Bus V9 Knowledge Center.
   b. Use the odbc initialization file as a template to create the file */var/mqsi/odbc/odbc9.ini*. For example, issue the following command:
      ```
      cp /opt/IBM/mqsi/9.0.0.6/ODBC/unixodbc/odbc.ini /var/mqsi/odbc/odbc9.ini
      ```

To give the broker access permission to this file, enter the following command:

```
chgrp mqbrkrs /var/mqsi/odbc/odbc9.ini
```

c. Update the following lines in the /var/mqsi/odbc/odbc9.ini file:

```
[ODBC Data Sources]
runtime_dsn=IBM DB2 ODBC Driver
...
[runtime_dsn]
Driver=Your_DB2_install_directory/lib64/db2o.o
Description=WBIFN DB2 ODBC Database
Database=runtime_dsn
...
[ODBC]
...
InstallDir=Your_Broker_install_directory/ODBC/V7.0
```

where:

runtime_dsn
: Data source name of the runtime database.

Your_DB2_install_directory
: The DB2 installation directory (for example, /opt/IBM/db2/V10.1).

Your_Broker_install_directory
: The IBM Integration Bus installation directory (for example, /opt/IBM/mqsi/9.0.0.6).

d. Use the odbcinst initialization file as a template to create the file */var/mqsi/odbc/odbcinst.ini*. For example, issue the following command:

```
cp /opt/IBM/mqsi/9.0.0.6/ODBC/unixodbc/odbcinst.ini /var/mqsi/odbc/odbcinst.ini
```

To give the broker access permission to this file, enter the following command:

```
chgrp mqbrkrs /var/mqsi/odbc/odbcinst.ini
```

e. Update and verify the following line in the /var/mqsi/odbc/odbcinst.ini file:

```
[ODBC]
...
TraceFile=trace_dir/odbctrace.out
Threading=2
```

where:

trace_dir
: A directory with plenty of free space to hold trace output (for example, /tmp).

Verify that following line is included:

```
Threading=2
```

f. Backup your current profile by issuing the following command:

```
cp homedir/.profile homedir/.profile_old
```

where *homedir* represents the home directory of the WebSphere Message Broker administrator (uwmba1).

g. Prepare a new profile by issuing the following commands:

```
echo ". /opt/IBM/mqsi/9.0.0.6/bin/mqsiprofile" > homedir/.profile_new
```

where *homedir* represents the home directory of the WebSphere Message Broker administrator (uwmba1).

h. Add a new WebSphere BI for FN broker profile. For this, issue the following commands:

```
cp wbifn_inst_dir/dniv311/run/samples/dnixzbrk.sh work_path/common/profiles/dnixzbrk.sh
chmod +x work_path/common/profiles/dnixzbrk.sh
```

where *work_path* represents the mqsi work-path directory of the WebSphere Message Broker, for example /var/mqsi.

This profile is processed when the broker starts.

i. Edit the WebSphere BI for FN broker profile:

- Set the DB2INSTANCE variable. Change the sample value *db2inst1* to your needs.
- Set the DNI_WMQ_PATH variable. Change the sample value */usr/mqm* to your needs.
- Set the WebSphere BI for FN installation path. Change the sample value */opt/IBM* to your needs.
- Check the ODBCINI environment variable. It must correspond to 4b on page 77.
- Check the ODBCSYSINI environment variable. It must correspond to 4d on page 78.
- If the MSIF services are to be used, remove the hash character (#) from the following statement:

  ```
  #export MQSI_THREAD_STACK_SIZE=3000000
  ```

- If runtime directories other than the defaults are to be used, remove the hash character (#) from the following statements:

  ```
  #DNI_CONF=dni_conf_dir
  #export DNI_CONFPATH=$DNI_CONF
  ```

  where *dni_conf_dir* represents the directory that contains the WebSphere BI for FN configuration file that defines the runtime directories that are to be used.

5. If you installed the WebSphere BI for FN Eclipse plug-ins in your V7 Toolkit, do this also in your V9 Toolkit. For more information about preparing the toolkit workstation, see *WebSphere BI for FN: Application Programming*. To test any services that use nodes that are provided by WebSphere BI for FN, recreate your BAR files.

Switching

To switch from WebSphere Message Broker V7 to IBM Integration Bus V9, carry out the following steps:

1. Stop all sessions and services, for example:
   a. Stop all applications that send requests to WebSphere BI for FN.
   b. Log out SIPN FIN LTs.
   c. Close MSIF SnF input and output channels.
   d. Release SWIFTNet SnF queues.
   e. Stop the MSIF Message Transfer service.
   f. Stop the RM transfer service message flow (DNF_L_TR).
   g. Stop the message printing service.
   h. Close all dnicli sessions.

i. Stop the SAGs and SAG Add-Ons.

j. Stop the WebSphere BI for FN WAS applications.

For more information about stopping sessions and services, see *WebSphere BI for FN: System Administration*.

2. On the runtime system, log on as a **WebSphere Message Broker administrator** (uwmba1):
   a. Stop all WebSphere MQ channels that are connected to the Version 7 broker.
   b. Stop the broker.
   c. Edit the WebSphere BI for FN broker profile dnixzbrk.sh. It is located in *work_path*/common/profiles/dnixzbrk.sh, where *work_path* represents the mqsi work-path directory of the WebSphere Message Broker, for example /var/mqsi.
      - Check the ODBCINI environment variable. It must correspond to 4b on page 77.
      - Check the ODBCSYSINI environment variable. It must correspond to 4d on page 78.
   d. Replace the profile of **WebSphere Message Broker administrator** (uwmba1). Issue the following command:

      ```
      cp home_dir/.profile_new home_dir/.profile
      ```

   e. Log out your **WebSphere Message Broker administrator** (uwmba1).
   f. Log on as a **WebSphere Message Broker administrator** (uwmba1). The new version of .profile is activated.
   g. Migrate the broker to the new target level by issuing the following command:

      ```
      mqsimigratecomponents brokername -t 9.0.0.6
      ```

      where *brokername* represents the name of your broker. Ensure that the following parameters are specified:

      -t The target level (for example, 9.0.0.6 for V9 Fix Pack 6).

      If the command ends with the BIP6123E error message, issue the MQ command dltmqlnk to resolve the problem and repeat this step.
   h. Start the migrated broker. The verification program checks the configuration of the broker.
3. On the runtime system, log on as a **WebSphere BI for FN system configuration or security administrator**.
   a. Replace your dniprofile with the copy you modified in step 3 on page 77, for example:

      ```
      cp /var/dni_03_01/run/dniprofile_new /var/dni_03_01/run/dniprofile
      ```

   b. Ensure that all dnicli users use this profile.
4. To verify that the switching was successful, on the runtime system, log on as a **user with the monitoring (DniMonitor) role** in the system OU SYSOU:
   a. Run the new version of dniprofile that was created in step 3a by entering the following command:

      ```
      . /var/dni_03_01/run/dniprofile
      ```

   b. Test whether the WebSphere Message Broker subscription mechanism works for WebSphere BI for FN. To do this, depending on whether you have registered to receive WebSphere BI for FN events in the syslog (that is, depending on whether you use the event notification service DNI_N_EVENT), issue one of the following sets of commands:

- If you have already registered to receive WebSphere BI for FN events in the syslog:

  ```
  dnicli -ou SYSOU -s DNI_MONITOR
  reg -ou DNIAAA
  .quit
  ```

- If you have not registered to receive WebSphere BI for FN events in the syslog:

  ```
  dnicli -ou SYSOU -s DNI_MONITOR
  reg -sq prefix.DNI_N_EVENT
  reg -ou DNIAAA
  dreg -sq prefix.DNI_N_EVENT
  .quit
  ```

  where *prefix* represents the queue prefix set by the DNIvQPFX placeholder during customization.

These commands register to receive events for an OU with the name DNIAAA. However, because an OU with this name does not exist, WebSphere BI for FN returns an error response and issues an error event. The error response on the console is similar to this one:

```
DNIM5006E Access denied for user 'sa1'; command: 'reg'; OU: 'DNIAAA'.
```

The switching was successful if your syslog contains an error event similar to this one:

```
DNIM5007E 2015-12-03 13:12:27 SYSOU DNI_MONITOR
          Access denied for user 'sa1'; command: 'reg'; OU: 'DNIAAA'.
```

5. Migrate your WebSphere Message Broker Toolkit workspace to V9 as described in the IBM Integration Bus V9 Knowledge Center.
6. If you created BAR files in step 5 on page 79, deploy your message flows.

Cleaning up obsolete resources

After you have verified that the migration to IBM Integration Bus V9 was successful, carry out the following steps to remove obsolete resources from your system:

1. Remove the saved WebSphere Message Broker V7 resources.
2. Remove the saved WebSphere Message Broker Toolkit resources.
3. Uninstall WebSphere Message Broker V7.
4. Delete the following copies of dniprofile:

   ```
   /var/dni_03_01/run/dniprofile_old
   /var/dni_03_01/run/dniprofile_new
   ```

Falling back to Message Broker V7

Falling back means returning to the use of WebSphere Message Broker V7. Changes that you made to brokers, the WebSphere Message Broker Toolkit, and development resources after migration to V9 are not retained.

To fall back from IBM Integration Bus V9 to WebSphere Message Broker V7, carry out the following steps for each instance on the runtime system on which the broker runs:

1. Stop all sessions and services, for example:
   a. Stop all applications that send requests to WebSphere BI for FN.
   b. Log out SIPN FIN LTs.

c. Close MSIF SnF input and output channels.
d. Release SWIFTNet SnF queues.
e. Stop the MSIF transfer service.
f. Stop the RM transfer service message flow (DNF_L_TR).
g. Stop the message printing service.
h. Close all dnicli sessions.
i. Stop the SAGs and SAG Add-Ons.
j. Stop the WebSphere BI for FN WAS applications.

For more information about stopping sessions and services, see *WebSphere BI for FN: System Administration*.

2. Restore the WebSphere Message Broker Toolkit to V7:
   a. Close all IBM Integration Bus Toolkit Version 9 sessions.
   b. Restore the Version 7 workspace from the backup that you took before migration.
   c. Restart WebSphere Message Broker Toolkit Version 7.
3. On the runtime system, log on as a **WebSphere Message Broker administrator** (uwmba1):
   a. Stop the V9 broker.
   b. Restore the broker to Version 7 by issuing the following command:
      ```
      mqsimigratecomponents brokername -s 9.0.0.6 -t 7.0.0.6
      ```
      where *brokername* represents the name of your broker. Ensure that the following parameters are specified:

      -s The source level (for example, 9.0.0.6 for V9 Fix Pack 6).

      -t The target level (for example, 7.0.0.6 for V7 Fix Pack 6).
   c. Restore your previous profile by issuing the following command:
      ```
      cp homedir/.profile_old homedir/.profile
      ```
      where *homedir* represents the home directory of the WebSphere Message Broker administrator (uwmba1).
   d. Log off and login again as a WebSphere Message Broker administrator (uwmba1).
   e. Issue the following command to start the broker:
      ```
      mqsistart brokername
      ```
4. On the runtime system, log on as a **WebSphere BI for FN system configuration or security administrator**. Replace `/var/dni_03_01/run/dniprofile` with the backup copy created in step 3a on page 77 by issuing the following command:
   ```
   cp /var/dni_03_01/run/dniprofile_old  /var/dni_03_01/run/dniprofile
   ```
5. To verify that the fallback was successful, on the runtime system, log on as a **user with the monitoring (DniMonitor) role** in the system OU SYSOU:
   a. Run the dniprofile by entering the following command:
      ```
      . /var/dni_03_01/run/dniprofile
      ```
   b. Test whether the WebSphere Message Broker subscription mechanism works for WebSphere BI for FN. To do this, depending on whether you have registered to receive WebSphere BI for FN events in the syslog (that is, depending on whether you use the event notification service DNI_N_EVENT), issue one of the following sets of commands:

- If you have already registered to receive WebSphere BI for FN events in the syslog:

  ```
  dnicli -ou SYSOU -s DNI_MONITOR
  reg -ou DNIAAA
  .quit
  ```

- If you have not registered to receive WebSphere BI for FN events in the syslog:

  ```
  dnicli -ou SYSOU -s DNI_MONITOR
  reg -sq prefix.DNI_N_EVENT
  reg -ou DNIAAA
  dreg -sq prefix.DNI_N_EVENT
  .quit
  ```

  where *prefix* represents the queue prefix set by the DNIvQPFX placeholder during customization.

These commands register to receive events for an OU with the name DNIAAA. However, because an OU with this name does not exist, WebSphere BI for FN returns an error response and issues an error event. The error response on the console is similar to this one:

```
DNIM5006E Access denied for user 'sa1'; command: 'reg'; OU: 'DNIAAA'.
```

The fallback was successful if your syslog contains an error event similar to this one:

```
DNIM5007E 2015-12-03 13:12:27 SYSOU DNI_MONITOR
          Access denied for user 'sa1'; command: 'reg'; OU: 'DNIAAA'.
```

Re-migrating

If problems occurred during your initial attempt to migrate to IBM Integration Bus V9 and if you fell back to the previous software level and resolved these problems, you might want to re-attempt to migrate to V9. When you re-migrate, the procedure you follow is slightly different from the procedure you followed when you migrated the first time. To re-migrate:

1. Follow the procedure described in “Preparing” on page 77 but do not carry out the following steps:
   - Step 1 on page 77
   - Step 2 on page 77
2. Follow the procedure described in “Switching” on page 79.

Appendix C. Summary of changes

Following changes, and enhancements are done with FTM SWIFT:

- The IBM Installation Manager is used to install the product.
- The default installation path has been changed.
- The default customization and runtime file system mount point has been changed.
- All programs are running in 64-bit mode.
- The broker profile dnixzbrk.sh is replaced by dniczbrk.sh
- The script dnfczmlc.sh is renamed to dnfczmlc.
- Profile dniprofile has been changed:
  - Variables DNF_PATH and DNQ_PATH removed
  - Variable IBM_JAVA_OPTIONS added
  - Alias for program dnfcaoma added
- Profile dnicus_*DNIvINST* has been changed:
  - Variables DNF_PATH and DNQ_PATH removed
- The definition of the RDU history table has been adjusted.
- The FTM SWIFT WAS applications names have been changed.
- The context root of the Home application is now **ftm-swift**.
- The EIAS and DIAS services are no longer included.
- The dnftrace parameter is removed from file dni.conf.
- Some obsolete placeholders have been removed. For more information, see step 8 on page 21

Appendix D. 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

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

Product Number: 5725-X92

Printed in USA

BBMP-0300-03