Separate system upgrade and data migration

Migrating IBM Tivoli Identity Manager 5.1 to IBM Security Identity Manager 6.0.2

IBM Security Identity Manager

Last updated: 12 August 2020

Revision history

Date	Description	Author
12 Aug 2020	Fixed minor typo in ‘Introduction’.	Mrunmayee Khedkar
05 June 2020	Initial.	Mrunmayee Khedkar

Contents

Introduction

Use these tasks to migrate database and directory data from an existing IBM® Tivoli® Identity Manager to a separate environment that runs IBM Security Identity Manager Version 6.0.2

These tasks require the installation of middleware and the upgrade and installation of IBM Security Identity Manager Version 6.0.2. The topics include best practices for the upgrade and migration from production environments.

Supported upgrade paths:

From	To
IBM Tivoli Identity Manager Version 5.1 that is deployed on WebSphere Application Server 6.1 or WebSphere Application Server 7.0	IBM Security Identity Manager Version 6.0.2 that is deployed on WebSphere Application Server 9.0.5

Table 1. Upgrade paths to IBM Security Identity Manager Version 6.0.2

Note These upgrade paths do not support the migration of Tivoli Identity Manager Version 5.1 that run with either a Microsoft SQL Server database or a Sun One Oracle directory server. Contact the database and directory server provider team, if you want to migrate data from Microsoft SQL Server or Sun One Directory server to the supported version for IBM Security Identity Manager Version 6.0.2

IBM Security Identity Manager supports data migration for both UNIX systems and Windows systems. IBM Security Identity Manager Version supports data migration among supported UNIX based operating systems. Data that resides in HP_UX environments can be migrated to any of the supported UNIX environments. However, data cannot be migrated from UNIX environments to Windows environments or from Windows environments to UNIX environments.

To migrate data, previous versions of IBM Tivoli Identity Manager must have the latest fix packs and interim fixes installed.

See the IBM Security Identity Manager product documentation to review:

- The supported release levels and fix pack specifications for the supported operating systems.
- Instructions for migrating adapters.

For known issues about migrating data, see Post-migration troubleshooting and known issues

- Migration process overview

  The data migration can be done either for a single-server environment or a cluster environment that consists of multiple computers. The middleware can be installed on one or more computers in either environment. The data migration consists of a collection of activities.

- Database Migration

IBM Security Identity Manager Version supports data migration from most databases supported on IBM Tivoli Identity Manager Version 5.1.

- Directory Server Migration

Security Identity Manager Version 6.0.2 supports data migration from most directory servers supported on Tivoli Identity Manager Version 5.1.

- Upgrade to IBM Security Identity Manager 6.0.2

The following sections provide information about how to upgrade to IBM Security Identity Manager Version 6.0.2 both for single-server and cluster environments.

- Post-Upgrade production cutover

Use this information to conduct a post-upgrade production cutover.

- Post Migration troubleshooting and known issues

Post migration troubleshooting provides information about known issues when the migration is completed and provides tips for troubleshooting.

Migration process overview

The data migration can be done either for a single-server environment or a cluster environment that consists of multiple computers. The middleware can be installed on one or more computers in either environment. The data migration consists of a collection of activities.

The major steps to migrate Tivoli® Identity Manager and related prerequisite middleware servers are:

In the Tivoli Identity Manager Version 5.1 server environment:

1. Stop WebSphere® Application Server and any connections to the Tivoli Identity Manager database if necessary.
2. Back up and export the following data from middleware servers to a temporary file directory:
    - Database server components
    - Directory server components

Note : After the backup and export are completed, you can bring the Tivoli Identity Manager Version 5.1 server environment back into production. You can load production data into the new Security Identity Manager Version 6.0.2 system at a later date. You can migrate data to a test environment before a production cutover to the new system. Any changes you make to Security Identity Manager data on the new system are overwritten when you reimport the Tivoli Identity Manager Version 5.1 production data during the final cutover.

- In the Security Identity Manager Version 6.0.2 server environment:
    1. Install the required middleware (at the required release and fix pack level).
    2. Configure DB2 Universal Database™ and IBM® Security Directory Server. See Database installation and configuration and Installation and configuration of IBM Tivoli Directory Server.

Database migration

IBM® Security Identity Manager Version supports data migration from most databases supported on IBM Tivoli® Identity Manager Version 5.1.

DB2 Universal Database migration

Use these scenarios to migrate DB2 Universal Database data to a version that Security Identity Manager Version 6.0.2 supports.

DB2 data migration to a system that has a different endian format than the source system

Typically, data migration is performed between operating systems that use the same endian format. Use these procedures if you must migrate your data to an operating system that uses a different endian format.

Endian is the convention that is used to interpret the bytes in a data word when stored in computer memory. Systems that use big endian store or transmit binary data in which the most significant value is placed first. Systems that use little endian store or transmit binary data in which the least significant value is placed first.

These procedures document the steps to migrate a DB2 database from a Linux for System z to an X86Linux system. To migrate other combinations of systems that use big endian and small endian, the procedures are similar, however, changes to the commands might be required. For the exact syntax and details of the DB2 commands, see the IBM Knowledge Center:

http://www.ibm.com/support/knowledgecenter/SSEPGG/welcome.

Because the number of reporting tables can vary depending upon the entity mapping that you defined, the procedures give no instructions to export reporting tables. After the migration to Security Identity Manager, you must run a full data synchronization to create and populate the reporting tables in the database.

Exporting DB2 Universal Database data

DB2 Universal Database provides a DB2MOVE utility. Use the export options provided with this utility to move data from a 5.1 system to a 6.0.2 system before the upgrade.

This procedure shows how to export the data from a Linux for System z operating system. The system uses the **big endian** format. The procedure is similar for systems that use the **little endian** format.

Perform these steps on a Linux for System z DB2 setup. Run the commands in sequence.

These variables are required for the commands:

Variable	Value
source database name	Name of the database that is configured for IBM Tivoli Identity Manager, such as ITIMDB.
database user name	Name of the database user who is configured for the IBM Tivoli Identity Manager database, such as itimuser.
database user password	The password of the database user.

Table 1. Export command values

Each command creates these files:

File name	Description
EXPORT.out	The summarized result of the EXPORT action.
db2move.lst	The list of original table names, their corresponding PC/IXF file names (tab*nnn*.ixf), and message file names tab*nnn*.ixf). This list, the exported PC/IXF files, and LOB files (tab*nnn*c.*yyy*) are used as input to the **db2move IMPORT** or **LOAD** action.
tab*nnn*.ixf	The exported PC/IXF file of a specific table. "*nnn*" is the table number.
tab*nnn*.msg	The export messages file of the corresponding table. "*nnn*" is the table number.
tab*nnnc*.*yyy*.lob	The exported LOB files of a specific table. "*nnn*" is the table number. "*c*" is a letter of the alphabet. "*yyy*" is a number that ranges 001 - 999. These files are created only if the table that is being exported contains LOB data.

Table 2. Export command output files

Procedure

1. Log in as the root user to the system on which the DB2 database is installed.
2. Go to *DB2 installation directory*/bin directory.

   Ensure that the /bin directory does not
   Contain tabnn.msg, tabnn.ixf, db2move.lst, IMPORT/EXPORT.out, or tab*.lob files that are generated as part of any previous import or export activity. If such files are present, you can move them to different directory.
3. Type and run the command on one line.

```
./db2move source database name export –u database user name -p database user password
-tn RESOURCE_PROVIDERS,LCR_INPROGRESS_TABLE,PO_TOPIC_TABLE,SCHEDULED_MESSAGE,NEXTVALUE,
PROCESS,SYNCH_POINT,PASSWORD_TRANSACTION,LISTDATA,REPORT,ENTITY_COLUMN,COLUMN_REPORT,
AUTHORIZATION_OWNERS,ACI,ACI_ROLEDNS,ACI_PRINCIPALS,ACI_PERMISSION_ATTRIBUTERIGHT,
ACI_PERMISSION_CLASSRIGHT,ENTITLEMENT,ENTITLEMENT_PROVISIONINGPARAMS,
SYNCHRONIZATION_HISTORY,SYNCHRONIZATION_LOCK,RESOURCES_SYNCHRONIZATIONS,CHANGELOG,
```

```
SERVICE_ACCOUNT_MAPPING,RECONCILIATION,AUTH_KEY,POLICY_ANALYSIS,COMPLIANCE_ALERT,
AUDIT_EVENT,I18NMESSAGES,BULK_DATA_SERVICE,MIGRATION_STATUS,
RECERTIFICATIONLOG,SCRIPT,MANUAL_SERVICE_RECON_ACCOUNTS,VIEW_DEFINITION,COMMON_TASKS,
SUMMARY_ORDER,PASSWORD_SYNCH,ROLE_INHERITANCE,SOD_POLICY,SOD_VIOLATION_HISTORY,
SOD_VIOLATION_STATUS,RECERTIFIER_DETAILS_INFO
```

The output files are created in the *DB2 installation directory*/bin directory.

4. Move these files into a separate folder, such as /parent_export.
5. Type and run the command on one line.

```
./db2move source database name export -u database user name -p database user password
                                    -tn ACTIVITY, USERRECERT_HISTORY
```

The output files are created in the *DB2 installation directory*/bin directory.

6. Move these files into a separate folder, such as /child1_export.
7. Type and run the command on one line.

```
./db2move source database name export -u database user name -p database user password -tn
REMOTE_RESOURCES_RECONS,PO_NOTIFICATION_TABLE,WORKITEM,ACCT_CHANGE,BULK_DATA_STORE,
SOD_RULE,USERRECERT_ACCOUNT
```

The output files are created in the *DB2 installation directory*/bin directory.

8. Move these files into a separate folder, such as /child2_export.
9. Run one of these commands on one line.
   Type and run this command if the IBM Tivoli Identity Manager 51 setup from where the DB2 data is being exported is at any maintenance level lower than or equal to FP13.

```
./db2move source database name export –u database user name -p database user password
-tn REMOTE_SERVICES_REQUESTS,REMOTE_RESOURCES_RECON_QUERIES,
PO_NOTIFICATION_HTMLBODY_TABLE,PROCESSDATA,PROCESSLOG,WI_PARTICIPANT,
ACTIVITY_LOCK,PENDING,RECONCILIATION_INFO,WORKFLOW_CALLBACK,ATTR_CHANGE,
POLICY_ANALYSIS_ERROR,AUDIT_MGMT_TARGET,AUDIT_MGMT_PROVISIONING,
AUDIT_MGMT_DELEGATE,BULK_DATA_INDEX,TASKS_VIEWABLE,SOD_OWNER,SOD_RULE_ROLE,
SOD_VIOLATION_ROLE_MAP,USERRECERT_ROLE,USERRECERT_GROUP
```

   If the IBM Tivoli Identity Manager 51 setup from where the DB2 data is being exported is at any maintenance level higher than FP13 IF46, type and run this command.

```
./db2move source database name export –u database user name -p database user password
-tn REMOTE_SERVICES_REQUESTS,REMOTE_RESOURCES_RECON_QUERIES,
PO_NOTIFICATION_HTMLBODY_TABLE,PROCESSDATA,PROCESSLOG, WI_PARTICIPANT,
ACTIVITY_LOCK,PENDING,RECONCILIATION_INFO,WORKFLOW_CALLBACK,ATTR_CHANGE,
POLICY_ANALYSIS_ERROR, AUDIT_MGMT_TARGET,AUDIT_MGMT_PROVISIONING,
AUDIT_MGMT_DELEGATE,BULK_DATA_INDEX,TASKS_VIEWABLE, SOD_OWNER,SOD_RULE_ROLE,
SOD_VIOLATION_ROLE_MAP, USERRECERT_ROLE,USERRECERT_GROUP,PENDING_REQUESTS
```

10. The output files are created in the *DB2 installation directory*/bin directory.
11. Move these files into a separate folder, such as /child3_export.
12. Go to ITIM_HOME/config/rdbms/db2 directory and copy enrole_admin.sql, enrole.ddl, and itim_sib.ddl to a directory, such as /DDL_Files.

Note: For clustered environments, ITIM_HOME is the directory on the deployment manager where IBM Tivoli Identity Manager is installed.

Installing DB2 Universal Database and copying data to the target server environment

After you export your data, you must update the system to the required level of the DB2 database.

Before you begin

Ensure that you have the correct level of administrative authority. On Windows systems, the login user ID must be in the Administrators Group. On UNIX or Linux systems, the login user ID must be root. Ensure that you completed the previous export data procedure.

About this task

These variables are required for the commands. The Security Identity Manager 6.0 system it the target system.

Variable	Value
database name	Name of the database that you create with this procedure.
database administrator	Name of the database administrator on the target system
database administrator password	The password of the database administrator on the target system
database user name	Name of the database user who is configured for the IBM Security Identity Manager database, such as itimuser.
database user password	The password of the database user.

Table 1. Command values

Procedure

1. On the target database server, install the new version of DB2 Universal Database.

   See Database installation and configuration. Because this operation is a migration, ensure that you create the same 5.1 database system user, for example, itimuser. The user must have the same rights and privileges it had on the old system.
2. Create DB2 instance and configure database on the target database server. Use the same database user name and the password that is used in Tivoli Identity Manager Version 5.1. This name is the schema name and the password is already saved in properties files in the *OLD_ITIM_HOME*\data directory. These values cannot be changed during the upgrade. Refer Database installation and configuration
3. Copy the DDL and SQL files from the /DDL_Files directory that you created in the Exporting DB2 Universal Database data procedure. Put them in any directory on the target computer.

   In this case, the X86Linux system, which uses the little endian format.
4. Go to the DB2 installation directory/bin directory and connect to the database that you created.

   Run the command

   ```
   db2 connect to database name user database administrator using database administrator password
   ```
5. Run the enrole_admin.sql and itim_sib.dll files that you copied in step 3.

   Run these commands:

   ```
   db2 -tf directory path/enrole_admin.sql
   db2 -tf directory path/itim_sib.dll
   ```
6. Disconnect from the database.

Run the command:

```
db2 disconnect all
```

7. Go to the DB2 installation directory/bin directory and connect to the database that you created.

   Run the command

   ```
   db2 connect to database name user database user name using database user password
   ```

8. Run the enrole.dll file that you copied in step 3.

   Run the command:

   ```
   db2 -tf directory path/enrole.dl
   ```

9. Disconnect from the database.

   Run the command:

   ```
   db2 disconnect all
   ```

Importing the data to X86Linux DB2 setup from the linux on z system platform

After you export the data from a big endian system, you can use this procedure to transfer the data to your system in the little endian format.

Before you begin

Ensure that the DB2 instance profile on which the target database resides is properly sourced.

About this task

Use the procedure to import the data from the directories that you created on your Linux for System z operating system for Exporting DB2 Universal Database data. The commands correspond to the export commands that you ran in that procedure. Run the commands in sequence. Perform these steps on the X86Linux system DB2 setup.

These variables are required for the commands:

Variable	Value
target database name	Name of the database that is configured for IBM Security Identity Manager, such as ITIMDB.
database user name	Name of the database user who is configured for the IBM Security Identity Manager database, such as itimuser.
database user password	The password of the database user.

Table 1. Import command values

Each command creates these files:

File name	Description
IMPORT.out	The summarized result of the IMPORT action.

File name	Description
tab*nnn*.msg	The import messages file of the corresponding table.

Table 2. Import command output files

Procedure

1. Log in as the root user to the X86Linux system on which the new DB2 database is installed.
2. Go to the *DB2 installation directory*/bin directory.

   All the actions must be done in this directory.
3. Copy the data from the /parent_export directory that you created into the *DB2 installation directory*/bin directory.
   a. Type and run the command on one line.
   ```
   ./db2move <target database name> import –u <database user name>
   –p <database user password> -io insert
   ```
   The output files are created in the *DB2 installation directory*/bin directory.
   b. Move these files into a separate folder, such as /parent_import.
   c. Remove tabnn.ixf and db2move.lst files from the *DB2 installation directory*/bin directory.
4. Copy the data from the /child1_export directory that you created into the *DB2 installation directory*/bin directory.
   a. Type and run the command on one line.
   ```
   ./db2move <target database name> import –u <database user name>
   –p <database user password> -io insert
   ```
   The output files are created in the *DB2 installation directory*/bin directory.
   b. Move these files into a separate folder, such as /child1_import.
   c. Remove tabnn.ixf and db2move.lst files from the *DB2 installation directory*/bin directory.
5. Copy the data from the /child2_export directory that you created into the *DB2 installation directory*/bin directory.

   Type and run the command on one line.
   ```
   ./db2move <target database name> import –u <database user name>
   –p <database user password> -io insert
   ```

   a. Type and run the command on one line.
   ```
   ./db2move <target database name> import –u <database user name>
   –p <database user password> -io insert
   ```
   The output files are created in the *DB2 installation directory*/bin directory.
   b. Move these files into a separate folder, such as /child2_import.
   c. Remove tabnn.ixf and db2move.lst files from the *DB2 installation directory*/bin directory.
6. Copy the data from the /child3_export directory that you created into the *DB2 installation directory*/bin directory.

   Type and run the command on one line.
   ```
   ./db2move <target database name> import –u <database user name>
   –p <database user password> -io insert
   ```

Type and run the command on one line.

```
./db2move <target database name> import –u <database user name>
    –p <database user password> -io insert
```

The output files are created in the *DB2 installation directory*/bin directory.

a. Move these files into a separate folder, such as /child3_import.
b. Remove tabnn.ixf and db2move.lst files from the *DB2 installation directory*/bin directory.

7. Verify that the data was imported correctly
   a. Verify that all the tables that were present in the source database are created in the target database.
   b. Verify that all the tables in ITIMUSER schema contain the same number of rows that were in the source database.
   c. Verify that all the indexes present in the ITIMUSER schema of the source database are created in the ITIMUSER schema of the target database
   d. Verify that all the views present in the ITIMUSER schema of the source database are created in the ITIMUSER schema of the target database
   e. Verify that the database permissions of the source database user, such as itimuser, are the same as the permissions of the target database user.

DB2 data migration to a system that has a same endian format than the source system

Use these tasks to migrate DB2 Universal Database data to a version that Security Identity Manager Version 6.0.2 supports.

Backing up DB2 Universal Database data

DB2 Universal Database provides backup and restore commands. Use these commands to move data from the 5.1 system to the 6.0.2 system before the upgrade.

Before you begin

Ensure that the free disk space and virtual memory requirements are met. Additionally, ensure that adequate free disk space exists in the system temp directory. The target system must meet the hardware and software requirements described on the Security Identity Manager product documentation site.

Ensure that you have the needed administrative authority. On Windows systems, the login user ID must be in the Administrators Group. On UNIX and Linux systems, the login user ID must be root.

Procedure

1. Open a DB2® command window.

UNIX and Linux systems

Log on as the DB2 instance owner and enter db2 to open a DB2 command window.

Windows systems

Click **Start** > **Run**, and enter db2cmd. When the DB2 command window opens, enter db2.

2. Close all connections to the Tivoli® Identity Manager database. Stop WebSphere® and any other tools.
   - When you upgrade on a WebSphere single server, stop the Tivoli Identity Manager application and the WebSphere server on which the Tivoli Identity Manager application is running.
   - When you upgrade on a WebSphere cluster, stop the Tivoli Identity Manager application and the WebSphere cluster on which the Tivoli Identity Manager application is running.
   - If necessary, run this command to force all connections to close:
     ```
     force application all
     ```

3. Back up the Tivoli Identity Manager database.

   Issue the command
   ```
   backup database ITIM_DB to OLD_DB2_BACKUP_DIR
   ```

   ITIM_DB is the name of the Tivoli Identity Manager database. For example, itimdb. *OLD_DB2_BACKUP_DIR* is a directory path to store the backup. For example, /51data/db2 on Linux or UNIX systems, or C:\temp\51data\db2 on Windows systems.

   Note: The db2admin account might not have access to other file system locations. For example, you might need to use /home/db2admin on UNIX or Linux systems.

Installing DB2 Universal Database and copying data to the target server environment

After you back up your data, use this task to update to the required level of DB2® database.

Before you begin

Ensure that you have the needed administrative authority. On Windows systems, the login user ID must be in the Administrators Group. On UNIX or Linux systems, the login user ID must be root.

Procedure

1. On the target database server, install the new version of DB2 Universal Database.

See Database installation and configuration. Because this operation is a migration, ensure that you create the same 5.0 or 5.1 database system user, for example, enrole. The user must have the same rights and privileges it had on the old system.

2. Create the DB2 instance.
3. Copy the contents of the Tivoli® Identity Manager database backup directory to the target server.
   For example, /60data/db2
   Ensure that the database instance owner you create has permission to read the target directory and subfiles.

Restoring the DB2 Universal Database data

DB2 Universal Database provides restore commands. Use these commands to restore saved data from the 5.1 system to the 6.0 system after the upgrade.

Before you begin

Ensure that you have the needed administrative authority. On Windows systems, the login user ID must be in the Administrators Group. On UNIX or Linux systems, the login user ID must be root.

About this task

DB2 Universal Database provides backup and restore commands. Use these commands to move data from the 5.1 system to the 6.0 system before the upgrade.

Procedure

1. Open a DB2® command window.

   UNIX and Linux systems

   Log on as the DB2 instance owner and enter db2 to open a DB2 command window.

   Windows systems

   Click **Start** > **Run**, and enter db2cmd. When the DB2 command window opens, enter db2.

2. In the DB2 command window, enter these commands to restore the database by using the saved DB2 data:

```
restore db itimdb from OLD_DB2_TEMP_DATA
```

   The value *itimdb* is the Security Identity Manager database name. *OLD_DB2_TEMP_DATA* is the location of the DB2 data you copied from the previous version, such as C:\temp\50data\db2.

3. Stop and start the DB2 server to reset the configuration.

   Enter the following commands:

```
db2stop
db2start
```

   If the db2stop command fails and the database remains active, enter the following commands:

   a. force application all

   This command deactivates the database.

   b. db2start.

Clearing the service integration bus

When you upgrade from Tivoli® Identity Manager 5.1 running on WebSphere® Application Server 7 to Security Identity Manager Version 6.0.2 on WebSphere Application Server 9.0.5, you must clear the Service Integration Bus (SIB) data from the restored database.

Before you begin

Ensure that you have the needed administrative authority. On Windows systems, the login user ID must be in the Administrators Group. On UNIX or Linux systems, the login user ID must be root.

Ensure that the Security Identity Manager database is running.

Procedure

1. Open a DB2 command window.

UNIX or Linux systems

Log on as the DB2 instance owner and enter db2 to open a DB2 command window.

Windows systems

Click **Start** > **Run**, and enter db2cmd. When the DB2 command window opens, enter db2.

2. Connect to the database as the DB2 instance owner by using the command:

```
connect to itimdb user instance_owner using instance_owner_password
```

Where

- *itimdb* is the Security Identity Manager database name
- *instance_owner* is the owner of the DB2 instance
- *instance_owner_password* is the password for the owner of the DB2 instance

3. In the DB2 command window, enter the DELETE SQL statements that are needed to delete all data from the tables in the SIB schemas.

Issue the following commands for each of the SIB schemas in your environment:

```
delete from schema_name.SIB000
delete from schema_name.SIB001
delete from schema_name.SIB002
delete from schema_name.SIBCLASSMAP
delete from schema_name.SIBKEYS
delete from schema_name.SIBLISTING
delete from schema_name.SIBXACTS
delete from schema_name.SIBOWNER
delete from schema_name.SIBOWNERO
```

The SIB schema, *schema_name* is

Table 1. Service integration bus schema names

Tivoli Identity Manager environment	**Schema name**
Single-server	ITIML000
Clustered	ITIML000, ITIML001, ITIML002, ITIML003, and ITIMS000 **Note** The number of schema names depends on the number of nodes in the cluster.

Note The SIBOWNERO might not exist in all Tivoli Identity Manager environments. If it does not exist and the delete statement fails, you can ignore the failure.

Oracle Database migration

Use these tasks to migrate and import Oracle database data to a system and version of Oracle database that Security Identity Manager Version 6.0 supports.

Exporting Oracle data

The Oracle database export (EXP) and import (IMP) utilities are used to back up the logical

database and recovery. They are also used to migrate Oracle data from one server, database, or schema to another.

Before you begin

Ensure that you have the needed administrative authority. On Windows systems, the login user ID must be in the Administrators Group. On UNIX or Linux systems, the login user ID must be root.

Procedure

1. On the server that runs Oracle database for Tivoli® Identity Manager Version 5.1, log in as the Oracle database instance owner.
2. Ensure that the *ORACLE_HOME* and *ORACLE_SID* environment variables are set correctly.

   ORACLE_HOME is the Oracle default installation directory. *ORACLE_SID* is the Tivoli Identity Manager database instance.
   a. Check your environmental variables for the following entries

      This example is for a Windows home directory.

      ```
      ORACLE_HOME=c:\oracle\ora92
      ORACLE_SID=itim
      ```

3. Export the Oracle database dump and log files. Issue the following command on one line:

   ```
   exp system/system_pwd file=path\itim51.dmp log=path\itim51exp.log
   owner=itim_username
   ```

   The *system_pwd* is the password for the system user. The *path* is the path of the file, such as C:\51data\oracle or /opt/51data/oracle. The *itim_username* is the Tivoli Identity Manager Version 5.1 database user, such as enrole or itimuser.
4. Copy the contents of the directory you exported over to the target server.

   For example, /61data/oracle.

   Ensure that the database instance owner enrole that you created has permission to read the target directory and subfiles.

Installing Oracle database and importing data

After you export your data, use this task to update to the required level of Oracle database.

Before you begin

Ensure that you have the needed administrative authority. On Windows systems, the login user ID must be in the Administrators Group. On UNIX or Linux systems, the login user ID must be root.

Procedure

1. On the target Security Identity Manager Version 6.0 server, install the supported version of Oracle database. See Installation and configuration of the Oracle database in the *IBM Security Identity Manager Installation Guide* on the Security Identity Manager product documentation site.
2. Configure the Oracle database instance.

   The following enrole_admin.sql file helps to configure the new Oracle database instance for the migration. Replace *itimuserTag* with your Tivoli® Identity Manager Version 5.1 database user, such as enrole. Replace *itimuserPwdtag* with the Tivoli Identity Manager Version or 5.1

database user password. If the database user ID and password are not the same as the previous version, the Security Identity Manager upgrade fails.

```
CREATE TABLESPACE enrole_data
DATAFILE 'enrole1_data_001.dbf'
SIZE 64M
AUTOEXTEND ON
NEXT 64M
MAXSIZE unlimited
DEFAULT STORAGE (INITIAL 10M
                 NEXT 1M
                 PCTINCREASE 10)
PERMANENT
ONLINE
LOGGING;

CREATE TABLESPACE enrole_indexes
DATAFILE 'enrole1_idx_001.dbf'
SIZE 32M
AUTOEXTEND ON
NEXT 32M
MAXSIZE unlimited
DEFAULT STORAGE (INITIAL 10M
                 NEXT 1M
                 PCTINCREASE 10)
PERMANENT
ONLINE
LOGGING;
CREATE USER itimuserTag IDENTIFIED BY itimuserPwdtag
 DEFAULT TABLESPACE enrole_data
 QUOTA UNLIMITED ON enrole_data
 QUOTA UNLIMITED ON enrole_indexes;
GRANT CREATE SESSION TO itimuserTag;
GRANT CREATE TABLE to itimuserTag;
GRANT CREATE ANY PROCEDURE to itimuserTag;
GRANT CREATE VIEW to itimuserTag;
```

3. Ensure that the *ORACLE_HOME* and *ORACLE_SID* environment variables are set correctly.

   ORACLE_HOME is the Oracle default installation directory. *ORACLE_SID* is the Tivoli Identity Manager database instance.
4. Run the preceding enrole_admin.sql file with the **sqlplus** utility.

   ```
   sqlplus system/system_pwd @path\enrole_admin.sql
   ```

   The *system_pwd* is the password for the system user. The *path* is the path of the file. Running this script file creates the mandatory Security Identity Manager table spaces and creates the database user (specified by itimuserTag) with mandatory permissions.
5. After the table spaces are created, enter the following command on one line to import the Tivoli Identity Manager Version 5.1 exported data:
6.
   ```
   imp system/system_pwd file=path\itim51.dmp log=path\itim516exp.log
    fromuser=itim_username
   ```

   The *system_pwd* is the password for the system user. The *path* is the path of the file, such as C:\51data\oracle or /opt/51data/oracle. The *itim_username* is the Tivoli Identity Manager Version 5.1 database user, such as enrole or itimuser.

What to do next

After you complete the upgrade, the installation, and applied the Security Identity Manager Version 6 schema changes, you must tune the database. For optimal performance, apply the latest tuning settings. See the Tuning Oracle section of the Security Identity Manager Performance Tuning Guide for details.

Clearing the service integration bus

For Separate Systems Upgrades from Tivoli® Identity Manager 5.1 to Security Identity Manager Version 6.0.2, you must clear out the Service Integration Bus (SIB) data from the restored database.

Before you begin

Ensure that the free disk space and virtual memory requirements are met. Additionally, ensure that adequate free disk space exists in the system temp directory. The target system must meet the hardware and software requirements described in *Hardware and software requirements* on the Security Identity Manager product documentation site.

Ensure that you have the needed administrative authority. On Windows systems, the login user ID must be in the Administrators Group. On Linux systems, the login user ID must be root.

Ensure that the Security Identity Manager database is running.

Procedure

1. On the target Security Identity Manager Version 6.0 Oracle server, start the Oracle database
2. Issue the following commands for each of the SIB schemas in your environment.

```
delete from schema_name.SIB000
delete from schema_name.SIB001
delete from schema_name.SIB002
delete from schema_name.SIBCLASSMAP
delete from schema_name.SIBKEYS
delete from schema_name.SIBLISTING
delete from schema_name.SIBXACTS
delete from schema_name.SIBOWNER
delete from schema_name.SIBOWNERO
```

The SIB schema, *schema_name* is

Table 1. Service integration bus schema names

Tivoli Identity Manager environment	**Schema name**
Single-server	ITIML000
Clustered	ITIML000, ITIML001, ITIML002, ITIML003, and ITIMS000

NoteThe SIBOWNERO might not exist in all Tivoli Identity Manager environments. If it does not exist and the delete statement fails, you can ignore the failure.

SQL Server migration

Contact the database provider for the procedure to migrate the tables and data from MSSQL.

Directory Server migration

Security Identity Manager Version 6.0.2 supports data migration from most directory servers supported on Tivoli® Identity Manager Version 5.1.

Tivoli Directory Server migration

Use these tasks to migrate Tivoli Directory Server data to a version that Security Identity Manager Version 6.0.2 supports.
Tivoli Identity Manager Version 5.1 supports IBM Tivoli Directory Server Version 6.1, 6.2, and 6.3. You must migrate your directory server data to a version that Security Identity Manager Version 6.0.2 supports.

Backing up directory server data

Export the directory server data to a file before you move to a directory server version that Security Identity Manager Version 6.0.2 supports.

Procedure

1. Log in as an administrator with root privileges.

   Note You do not have to stop the LDAP server.
2. Open a command window.
3. Go to the *TDS_HOME*/sbin directory and type this command:

   ```
   db2ldif -s ldap_suffix -o ldap_output_file -I ldap_instance_name
   ```

   Where
   - *ldap_suffix* is the name of the suffix on which Tivoli Identity Manager is configured, such as dc=com.
   - *ldap_output_file* is the name of the ldif output file, such as old_ldif_data.ldif.
   - *ldap_instance_name* is the name of the LDAP server instance, which can be obtained through the IBM® Security Directory Server Instance Administration tool.

Installing Tivoli Directory Server in the target server

Install a version of IBM® Security Directory Server that Security Identity Manager Version 6.0.2 supports.

Before you begin

Verify that your directory server data is backed up.

Procedure

1. Log on as an administrator with root privileges, on the target Security Identity Manager Version 6.0.2 server.
2. Install the supported version of IBM Security Directory Server.

   See Installation and configuration of IBM Tivoli Directory Server.
3. Create IBM directory Server Instance
   - Ensure that the same Tivoli Identity Manager Version 5.1 root suffix is created and used.

- Use the same encryption seed value as the old Security Directory Server instance. Otherwise, the data from the old Security Directory Server instance must be exported to use the seed and salt keys from the new instance.

4. Copy the schema file V3.modifiedschema from the *OLD_ITDS_INSTANCE_HOME*\etc directory of the Security Directory Server instance home directory used by Tivoli Identity Manager Version 5.*x* server. Paste the file to the *NEW_ITDS_INSTANCE_HOME*\etc directory of the Security Directory Server instance that the Security Identity Manager server uses.

   NoteIf you customized or modified the schema files, manually merge the changes into the new schema files.
5. Stop and start Security Directory Server to activate the changes.

Importing directory server data

Import the directory server data that you saved in a previous step during the upgrade process.

Procedure

1. Log in as an administrator with root privileges.
2. Stop the LDAP server.
3. From *TDS_HOME*/sbin, run the command:

```
bulkload -i OLD_ITDS_TEMP_DATA\ldif_output_file -I ldap_instance_name
```

   Where
   - *OLD_ITDS_TEMP_DATA* is the temporary directory location of the Security Directory Server data you copied over from the previous version. Such as C:\temp\51data\ids\.
   - *ldif_output_file* is the name of the file that you exported in a previous task. Such as old_ldif_data.ldif
   - *ldap_instance_name* is the name of the LDAP server instance. Such as itimldap. You can obtain use the Security Directory Server Instance Administration tool to obtain the instance name.

Results

When you run the **bulkload** command, the following errors might occur.

- If any of the entries in the input LDIF file exist in LDAP, the bulkload utility fails. This error might occur if the suffix you defined exists as an entry in the directory server. It might be necessary to delete all entries in the suffix (but leave the suffix) from LDAP before you run the command. You can use the **ldapsearch** commands to check for existence of entries and the **ldapdelete** command to remove these entries.
- Error codes

```
GLPCRY007E The directory key stash file is inconsistent with the
      associated encrypted data.

GLPBLK071E Bulkload is unable to run because of an initialization error.

GLPBLK030E Run DB2CMD.EXE first, and then run bulkload within the "DB2 CMD"
command interpreter.
```

To correct these errors, you must know encryption seed and salt values of the target instance. The target instance is the directory server instance where you are running the bulkload.

1. To determine the salt value of target instance, run this command from *TDS_HOME*/bin:

2. ldapsearch -D *bind DN* -w *password* -h *hostname* -p *port* -s base -b cn=crypto,cn=localhost cn=*

Where

- *bind DN* is the distinguished name (DN) of the directory server
- *password* is the DN password
- *hostname* is the name of the computer where Security Directory Server is installed
- *port* is the port number on which Security Directory Server is listening

3. Replace the value of *ibm-slapdCryptoSync*, *ibm-slapdCryptoSalt* with the values returned by the **ldapsearch** command in the *ldap_output_file* file. This file is generated as output of the **db2ldif** command, for example *old_ldif_data.ldif*.
4. Run the **bulkload** command again.

   TipYou can use "-W OUT_FILE_NAME" option with the **bulkload** command. This option places the output from the command into the specified file. The **bulkload** command runs several instances of a DB2 command to load data. Each one has its own success, error, or warning messages. Without the -W option to save the output, it is difficult to check the result.

What to do next

Tune LDAP for optimal performance by applying the latest tuning settings. See *Tuning Security Directory Server* in *Security Identity Manager Performance Tuning Guide*. Import the directory server data that you saved in a previous step during the upgrade process.

Oracle directory server data migration

IBM Security Identity Manager Version 6.0.2 does not support Oracle directory Server.
Use the IBM Software Product Compatibility Report tool to check for supported middleware at
https://www.ibm.com/software/reports/compatibility/clarity/softwareReqsForProduct.html .
If you are using Oracle directory server in ITIM 5.1 contact the product support team for migration details.

Upgrade to IBM Security Identity Manager Version 6.0.2

The following sections provide information about how to upgrade to IBM® Security Identity Manager Version 6.0.2, both for single-server and cluster environments.

Copying the existing Tivoli Identity Manager version home directory to the target environment

To run the installation program to upgrade to Security Identity Manager Version 6.0.2, copy the existing Tivoli Identity Manager home directory to the target environment.

Before you begin

Ensure that you have the needed administrative authority. On Windows systems, the login user ID must be in the Administrators Group.

About this task

The *OLD_ITIM_HOME* location from the previous version of Tivoli Identity Manager is preserved when you copy the home directory. For example, if the *OLD_ITIM_HOME* directory was C:\itim51 (Windows) or /opt/IBM/itim51 (UNIX or Linux), copy the directory to the same path on the new server before you run the installation program.

Procedure

1. Copy the directory.
   - For UNIX or Linux systems
     a. Go to the UNIX or Linux root directory.
     b. Create a .tar file by entering the full path of *OLD_ITIM_HOME*. For example,
     ```
     tar –cvf itim.tar OLD_ITIM_HOME
     ```
     If you are running Security Identity Manager in a cluster environment, create separate .tar files for the deployment manager and cluster members.
     c. Copy the itim.tar file to the target server root directory. For a cluster environment, copy the .tar file from the old deployment manager to the new deployment manager and old cluster members to new cluster members.
     d. Extract the *OLD_ITIM_HOME* directory on one or more servers with the following command:
     ```
     tar –xvf itim.tar
     ```
   - For Windows systems
     a. Create a compressed file of the *OLD_ITIM_HOME* directory. For a cluster environment, create separate compressed files for the deployment manager and cluster members.
     b. Copy the compressed file to the target server. For a cluster environment, copy the compressed file from the old deployment manager to the new deployment manager and old cluster members to new cluster members.
     c. Extract the *OLD_ITIM_HOME* directory on one or more servers to the same drive location where Security Identity Manager is installed.

Executing upgradeFrom5to60.ddl and upgradeDataFrom51to6.ddl

After copying and backing up your existing data , before running the IBM security Identity Manger installation program make sure to execute upgradeFrom5to60.ddl and upgradeDataFrom51to6.ddl
as DB owner depending on the database server you are using for IBM Security Identity Manager 6.0.2
This will create the new tables in the schema resulting no errors in the installation.

Executing ddl for IBM Database production server:

1. Place both the ddls in DB2_HOME/bin
2. In the DB2 command window ,run the command

```
db2 connect to database name user database user using database user password
db2 -tvf  upgradeFrom5to60.ddl
db2 -tvf  upgradeDataFrom51to60.ddl
```

Executing ddl for Oracle database production server:

1. Place both the ddls on the system where Oracle database server is installed
2. Run the *upgradeFrom5to60.ddl* and *upgradeDataFrom51to60.ddl* with sqlplus utility :

```
sqlplus system/system_pwd@path\upgradeFrom5to60.ddl
sqlplus system/system_pwd@path\upgradeDataFrom51to60.ddl
```

Where
system_pwd Is the password of the system user.
Path Is the path of the file.

Running the Security Identity Manager installation program

After copying and backing up your existing data, you must install the Security Identity Manager Server.

Before you begin

Before you run the Security Identity Manager Version 6.0.2, installation program. Ensure that you imported or restored the directory and database data you copied onto the respective directory and database servers. Additionally, ensure that the following middleware is running at the supported release level and fix pack:

- WebSphere® Application Server
- DB2 Universal Database or other supported middleware
- IBM® Security Directory Server or other supported middleware

See *Hardware and software requirements* in the *IBM Security Identity Manager Product Overview Guide* on the Security Identity Manager product documentation site. For instructions about installing and configuring these middleware products, see Installation of prerequisite components on the Security Identity Manager product documentation site.

About this task

If installing Security Identity Manager in a cluster environment, you must install Security Identity Manager on the deployment manager to upgrade the database and directory server before installing Security Identity Manager on cluster members.

To upgrade to Security Identity Manager Version 6.0.2:

Procedure

1. Log on to an account with system administration privileges on the computer where Security Identity Manager is going to be installed.

   On Windows systems, the login user ID must be in the Administrators Group. On Linux systems, the login user ID must be root.
2. Download the installation program, or insert the Security Identity Manager product DVD into the DVD drive.
3. Run the installation program.
   - For Windows systems
     a. Click **Start** > **Run**.
     b. Enter the drive and path where the installation program is located and then enter the command:
     ```
     instwin.exe
     ```
   - For UNIX or Linux systems
     a. Open a command shell prompt window, and go to the directory where the installation program is located.
     b. Enter the one of these commands for the installation program:

     AIX® systems
     ```
     instaix.bin
     ```

     Linux systems
     ```
     instlinux.bin
     ```

     zLinux systems
     ```
     instzlinux.bin
     ```
   - **Note**To run the installation program on a UNIX or Linux system, you need at least 150 MB of free space in the /tmp directory. If you do not have sufficient space, set the IATEMPDIR environment variable to a directory on a disk partition with enough free disk space. To set the variable, enter one of the following commands at the command-line prompt before running the installation program again.
   - **Bourne shell (sh), ksh, bash, and zsh**
     - $ IATEMPDIR=*temp_dir*
     - $ export IATEMPDIR
   - **C shell (csh) and tcsh**
     - $ setenv IATEMPDIR *temp_dir*
   - *temp_dir* is the path to the directory, for example /your/free/directory, where free disk space is available.
4. The Welcome window opens.
5. Select the language and click **OK**.
6. If you agree with the terms, accept the license agreement and click **Next**.
7. In the Choose Install Directory window, you must select the existing Tivoli® Identity Manager home directory that you want to upgrade. Accept the default directory, or click **Choose** and select the correct directory. Then, click **Next**.

8. In the Upgrade Security Identity Manager window, click **Continue to Next** to start the upgrade.
9. Read the caution windows to ensure that the prerequisite applications meet the requirements that Security Identity Manager supports. Then, click **Next**.
10. In the Installation Directory of WebSphere Application Server window, confirm the WebSphere Application Server directory and click Next.
11. In the WebSphere Profile Selection window, select the WebSphere Application Server profile name, and click **Next**.
12. If you are running Security Identity Manager in a cluster environment, enter the application and messaging cluster names, and click **Next**.

    Note The cluster names you enter do not have to match the previous version of Tivoli Identity Manager, but they must exist from the configuration of WebSphere Application Server. For more information about configuring WebSphere Application Server for Security Identity Manager, see Installation and configuration of WebSphere Application Server on the Security Identity Manager product documentation site.
13. In the WebSphere Application Server Data window, enter or accept the application server name. Ensure that the correct host name for the new computer is shown, and click **Next**.
14. If you are running Security Identity Manager in a cluster environment, verify the host name of the system on which WebSphere Application Server and Security Identity Manager are to be installed. Click **Next**.
15. If WebSphere administrative security and application security is turned on, in the WebSphere Application Server Administrator Credentials window, enter the WebSphere Application Server administrator user ID and password, and click **Next**.
16. If you are prompted for the Java™ Database Connectivity (JDBC) driver, enter the directory location for the JDBC driver and the driver name, and click **Next**.

    NoteIf you are upgrading from Tivoli Identity Manager 5.1 to Security Identity Manager 6.0.2 on WebSphere Application Server 9.0.5, the JDBC driver setup panel is not displayed. Additional manual steps are needed for the Oracle database.

    a. After deploying Tivoli Identity Manager 5.1 on WebSphere Application Server 7.0 Fix Pack 5, remove the ojdbc.jar file from *ISIM_HOME*/lib and replace it with ojdbc6.jar. Then, rename ojdbc6.jar to ojdbc.jar.
17. In the Tivoli Common Directory window, select the location of the Tivoli Common Directory or another directory, and click **Next**. The directory you select is the central location for all serviceability-related files, such as logs and first-failure capture data.
18. In the Pre-Installation Summary window, verify that the information is correct and click **Install**.
19. When the System Configuration tool window is shown on the screen, navigate to ITIM_HOME in the system directory structure for example opt/IBM/itim/bin for linux machine and C:\Program Files (x86)\IBM\itim\bin for windows and change OLD_VERSION=6.0 in dbupgrade and ldapupgrade lax files.
20. When the System Configuration tool window is shown on the screen, enter the correct values for Security Identity Manager Version 6.0.2. Confirm or update the correct values for the following directory, database, and mail server fields on each tab. These values must be changed from the old information used in the previous version of Tivoli Identity Manager.
    - Database
      - JDBC URL

Enter the JDBC URL with the correct database host name, port number, and database name for Security Identity Manager Version 6.0.2. For example, if you are using the DB2® database “itimdb” running at the host 10.1.1.1 on port 50000, then you enter:jdbc:db2://10.1.1.1:50000/itimdb

NoteThe host name can be a fully qualified domain name, IPv4 or [IPv6] address. The IPv6 address must be enclosed in square brackets.

- After you enter the information, click **Test** to test the connection.
- **Note**The Database User and User Password fields are disabled. When you create the database user for Security Identity Manager Version 6.0.2, make sure that you use the same database user ID and password that you used for the previous Tivoli Identity Manager server.
- Directory
  - Principal DN
  - Password
  - Host Name
  - Port

  After you enter the information, click **Test** to test the connection.
- Mail
  - Identity Manager Server Base URL

21. Click **OK** after you change or verify all the fields on all the tabs.

    The database upgrade program is started to upgrade the database schema and data. The database upgrade can take some time to complete, and progress is not displayed. After it is complete, the LDAP upgrade program is started to upgrade the LDAP schema and data. This upgrade can also take some time. You can look at the log files in the *ISIM_HOME*\install_logs directory to see the upgrade progress, specifically the following log files:
    - itim_install_activity.log
    - dbUpgrade.stdout
    - ldapUpgrade.stdout
    - runConfigFirstTime.stdout
22. When the installation program is finished, click **Done**.

Post-Installation tasks

Perform these tasks after you migrated to Security Identity Manager Version 6.0.2.

After upgrading to IBM® Security Identity Manager Version 6.0.2 perform the following tasks, if applicable:

- Service center access request: Ensure that you synchronize the access catalog date by using the following data synchronization utility if Service Center is enabled:

  Unix

  ISIM_HOME/bin/unix/syncISIMData.sh -syncOption Upgrade -dataType ALL

  Windows

  ISIM_HOME/bin/win/syncISIMData.cmd -syncOption Upgrade -dataType ALL

- Configure single sign-on. See Configuration of single sign-on.
- Configure the external user registry. To use an existing external user registry, see Postinstall configuration of an external user registry for authentication.
- Configure high availability and disaster recovery. See Configure high availability and disaster recovery.

Updating the default WebSphere Application Server listening port (cluster only)

Use this task to update WebSphere Application Server default host ports after installing in a cluster environment.

About this task

After the installation completes, check whether the default host ports of each application cluster member are included in the host aliases of default_host. If not, you might need to update the default WebSphere Application Server listening port by manually entering a new host alias for the port.

Procedure

1. From the administrative console, click Environment > Virtual Hosts > default_host > Host Aliases.
2. In Host Aliases, click New to create an alias.
3. In the Host Name field, enter *, and in the Port field, enter the port number and click OK.

   Note To find the default host port, click Servers > Applications Servers > ServerName > ports. Look for the values of WC_defaulthost and WC_defaulthost_secure, where serverName is the server name of the application cluster member where Security Identity Manager is deployed.

4. Save the configuration changes.
5. Complete a Full Synchronization of the WebSphere® Application Server nodes.

Preserving custom logos

Custom logos used in the UI are not preserved after upgrade. You must modify the ui.properties file.

The ui.properties file property named enrole.ui.customerLogo.image still points to the location specified in 5.1. However, this pointer defaults to a path inside the enrole.ear or ITIM.ear directory. You must copy the image file from the old location to the new location.

For information about customizing logos and style sheets, see Manual preservation of the customized data.

Verification of the installation

After you complete the installation, confirm that you can log on to the Security Identity Manager version 6.0.2 system.

Log on to Security Identity Manager version 6.0.2. Use the administrator user ID and password that was used in the previous version of Tivoli Identity Manager.

For more information about verifying the Security Identity Manager version 6.0.2 installation, see Verifying the installation..

Performance tuning

After you complete verifying the new system, apply performance tuning settings to confirm that the new system meets your performance requirements.
For instance, on systems that run DB2 Universal Database, you might benefit from enabling autoresize on your table spaces. Although enabled is the default setting, verify that you have autoresize enabled. Issue the command:

```
db2 get snapshot for tablespaces on itimdb
```

Look for the "Auto-resize enabled" line in the output.

Post-migration production cutover

Use this information to conduct a post-migration production cutover.

While you are conducting the upgrade process and testing the new production system, the old production system continues to capture changes made in production. The Security Identity Manager migration does not provide a mechanism to capture these changes and import them to the upgraded system that runs Version 6.0.2. Security Identity Manager does provide the capability to capture current data from the old production system and import it to the new environment. You must install an entirely new Security Identity Manager 6.0.2 environment.

The following data and settings are preserved from the new production system:

- WebSphere Application Server configuration settings, including performance tuning
- Tivoli Identity Manager configuration settings stored in property files

The following data and settings are *not* preserved from the new production system:

- All database server data
- All directory server data
- Any middleware that tunes settings (such as the settings for DB2 Universal Database and IBM® Security Directory Server).

Production cutover roadmap

Follow this roadmap to move from the current production environment to the new environment.

The cutover of the production environment consists of the following steps:

1. Shut down IBM® Security Identity Manager on the new production environment.
2. Prepare the following new production servers for data import:
    - Directory server
    - Database server (preparing data is not necessary for DB2 Universal Database or SQL Server)
3. Shut down WebSphere® Application Server on the old production environment.
4. Capture the data from the following old production servers:
    - Directory server
    - Database server
5. Import the Tivoli® Identity Manager directory data from the old production environment to the new environment.
6. Import the Tivoli Identity Manager database data from the old production environment to the new environment.
7. Start IBM Security Identity Manager on the new production environment.
8. Apply performance tuning setting to directory and database servers.

Stop Websphere Application Server on the new production environment

Stop WebSphere® Application Server on the new production environment.
Stop both the application server and the message server. If you are deploying into a WebSphere cluster environment, you must stop the application servers and message servers on all cluster members.
You can stop servers either by using the WebSphere console or by using commands from a command line. When working in a WebSphere cluster, it is easier to use the WebSphere console to stop the application and message servers.

Note Optional: If your deployment includes an HTTP Server, stop the server.
WebSphere command-line commands:

- Windows

WAS_PROFILE_HOME\bin\stopServer.bat *servername*

- UNIX or Linux

WAS_PROFILE_HOME/bin/stopServer.sh *servername*

Note If WebSphere administrative security is enabled, append the following flag to the end of the previous command.

-user *WAS_username* - password *WAS_user_password*

Where *WAS_username* is the WebSphere Application Server administrative user name and *WAS_user_password* is the password for the administrative user.

Preparation of the new production environment for database and directory server data import

You must prepare the new production environment for database and directory server data import. Ensure that you first stop WebSphere Application Server on the new production environment.

Note Do not prepare or reconfigure data for DB2 or SQL Server, because the process of restoring the database overwrites any configuration.

Reconfiguring the IBM Security Directory Server Instance

You must configure your directory server instance to run in the Security Identity Manager Version 6.0.2 environment.

Before you begin

You must stop WebSphere® Application Server in the new production environment.

Procedure

1. Stop IBM® Security Directory Server.

Issue this command.

ibmslapd -I *ldap_instance_name* -k

2. Start the IBM Security Directory Server Instance Administration tool.

Run this command that is in the *ITDS_HOME*\sbin directory.

idsxinst

3. Use the Instance Administration tool (idsxinst) to delete the current Security Identity Manager LDAP instance.

Additionally, choose to delete the database.

4. Create a Security Identity Manager LDAP instance.

Make the instance name and passwords the same as the previously created instance. For more information about creating the LDAP instance, see Installing Tivoli Directory Server on the target server.

Note If you do not want to destroy the LDAP instance ,use the **idsxcfg** or **idsucfgdb** and **idscfgdb** commands to reoconfigure the database. You must update the database with the tuning settings. See the Database servers used with IBM Security Identity Manager section of the Security Identity Manager Performance Tuning Guide.

Reconfiguring the Sun Enterprise Directory Server Instance

IBM Security Identity Manager Version 6.0.2 does not support Sun Enterprise directory Server.
Refer clarity reports for supported middlewares
https://www.ibm.com/software/reports/compatibility/clarity/softwareReqsForProduct.html
If you are using Sun Enterprise directory server in ITIM 5.1 contact the product support team for migration details.

Reconfiguring the Oracle database Instance

You must configure your database instance to run in the Security Identity Manager Version 6.0.2 environment.

Before you begin

The WebSphere® Application Server must be stopped in the new production environment.

Procedure

1. Use the **dbca** command or other tools to remove the Security Identity Manager database and instance that was created for the test environment.
2. After the database is removed, create a database with the same name by using the migration commands previously provided. For more information, see Oracle database migration.
3. Configure the Oracle database instance.

The following enrole_admin.sql file helps to configure the new Oracle 10g or 11g database instance for the migration.

a. Edit the file.

Note If the database user ID and password are not the same as the previous version, the Security Identity Manager upgrade fails.

b. Replace *itimuserTag* with your Security Identity Manager database user. For example enrole.

c. Replace *itimuserPwdtag* with the Security Identity Manager database user password.

```
CREATE TABLESPACE enrole_data
DATAFILE 'enrole1_data_001.dbf'
SIZE 64M
AUTOEXTEND ON
NEXT 64M
MAXSIZE unlimited
DEFAULT STORAGE (INITIAL 10M
                 NEXT 1M
                 PCTINCREASE 10)
PERMANENT
ONLINE
LOGGING;

CREATE TABLESPACE enrole_indexes
DATAFILE 'enrole1_idx_001.dbf'
SIZE 32M
AUTOEXTEND ON
NEXT 32M
MAXSIZE unlimited
DEFAULT STORAGE (INITIAL 10M
                 NEXT 1M
                 PCTINCREASE 10)
PERMANENT
ONLINE
LOGGING;
CREATE USER itimuserTag IDENTIFIED BY itimuserPwdtag
 DEFAULT TABLESPACE enrole_data
 QUOTA UNLIMITED ON enrole_data
 QUOTA UNLIMITED ON enrole_indexes;
GRANT CREATE SESSION TO itimuserTag;
GRANT CREATE TABLE to itimuserTag;
GRANT CREATE ANY PROCEDURE to itimuserTag;
GRANT CREATE VIEW to itimuserTag;
```

4. Run the enrole_admin.sql file that you edited in the previous step with the **sqlplus** utility:

sqlplus system/*system_pwd* @*path*\enrole_admin.sql . The system_pwd is the password for the system user. The *path* is the path of the file. Running this script file creates the required Security Identity Manager table spaces and creates the database user (enrole) with required permissions.

Capture and import the production server data

Use these tasks to transfer Tivoli Identity Manager 5.1 production server data to the new production environment.

After you prepare the new production environment, complete these tasks to import directory server and database information from the old environment.

Capturing and importing the contents of the Tivoli Directory Server production server data

After you complete preparing the new production server to import data, use this task to transfer Tivoli Directory Server production server data to the new production environment.

Procedure

1. On the old production server, export the directory server data.

For more information, see Backing up directory server data.

2. Copy the schema file V3.modifiedschema from the *OLD_ITDS_HOME*\etc directory of the IBM Tivoli Directory Server used by Tivoli Identity Manager version 5.1 server.
3. Paste the schema file V3.modifiedschema to the *NEW_ITDS_HOME*\etc directory of the IBM® Security Directory Server used by the Security Identity Manager version 6.0.2 server.
4. Import the directory server data.

For more information, see Importing directory server data.

Capturing and importing the contents of the Sun enterprise Directory Server Production server data

IBM Security Identity Manager Version 6.0.2 does not support Sun Enterprise directory Server.
Refer clarity reports for supported middlewares
https://www.ibm.com/software/reports/compatibility/clarity/softwareReqsForProduct.html
If you are using Sun Enterprise directory server in ITIM 5.1 contact the product support team for migration details.

Capturing and importing the contents of the DB2 database production server data

Use this task to transfer DB2® database production server data to the new production environment.

Procedure

1. Back up the DB2 Universal Database data.

For more information, see Backing up DB2 Universal Database data.

2. Copy the contents of the Tivoli® Identity Manager database backup directory to the target server. For example, /51data/db2.

Ensure that the database instance owner enrole that you created previously has permission to read the target directory and files within.

3. Restore the database data. For more information.

For more information, see Restoring the DB2 Universal Database data

Capturing and importing the contents of the oracle database production server data

Use this task to transfer Oracle database production server data to the new production environment.

Procedure

1. Export the Oracle database data.

For more information, see Exporting Oracle data.

2. Enter this command on one line to import the Tivoli Identity Manager Version 5.1 exported data.

3. imp system/*system_pwd* file=*path*\itim*xx*.dmp log=path\itim*xx*exp.log fromuser=*itim_username*

The *system_pwd* is the password for the system user. The *path* is the path of the file you copied. (For example C:*xx*data\oracle or /opt/*xx*data/oracle. *xx* is the version number of your previous version of Tivoli Identity Manager (5.1). The *itim_username* is the name of the Tivoli Identity Manager (5.1) database user, such as enrole.

Capturing and importing the contents of the Microsoft SQL database production server.

IBM Security Identity Manager Version 6.0.2 does not support Microsoft SQL database production Server.
Refer clarity reports for supported middlewares
https://www.ibm.com/software/reports/compatibility/clarity/softwareReqsForProduct.html
If you are using Microsoft SQL database production Server in ITIM 5.1 contact the product support team for migration details.

Clearing of the service integration bus

This task applies only if you are using DB2® or Microsoft SQL databases.

For Separate Systems Upgrades from Tivoli® Identity Manager 5.*X* to Security Identity Manager 6.0.2 server, the Service Integration Bus (SIB) data from the restored database must be cleared out.

- For DB2 servers, see Clearing the service integration bus.

Commands to migrate directory and database data

Use these commands to upgrade imported data to the Security Identity Manager version 6.0.2 level.

After you import the directory and database data on the new production environment, run the **ldapUpgrade** and **DBUpgrade** utilities. Running these utilities upgrades imported data to the Security Identity Manager version 6.0.2 level. Depending on the size of the data pool, this process can take some time. To confirm that the upgrade is completed, you can check the DBUpgrade.stdout and ldapUpgrade.stdout log files in the *NEW_ISIM_HOME*\install_logs directory.

If you installed the Shared Access module during the upgrade, you must reconfigure it after you import the data.

Executing upgradeFrom5to60.ddl and upgradeDataFrom51to6.ddl

Before running ldapUpgrade and DBUpgrade to import data into IBM® Security Identity Manager , execute upgradeFrom5to60.ddl and upgradeDataFrom51to6.ddl as DB owner. See Executing upgradeFrom5to60.ddl and upgradeDataFrom51to6.ddl

Running ldapUpgrade and DBUpgrade

Run **ldapUpgrade** and **DBUpgrade** to import data into IBM® Security Identity Manager.

About this task

If you are running Security Identity Manager in a cluster environment, run the **ldapUpgrade** and **DBUpgrade** commands on the system where the network deployment manager is located.

Procedure

1. Backup exisisting enRole.properties file
2. Edit the enRole.properties file , setting the following property:
   ```
   minUpgradeVersion=5.1
   ```
3. Run the **ldapUpgrade** command.

Windows operating systems

NEW_ISIM_HOME\bin\ldapUpgrade

UNIX or Linux operating systems

NEW_ISIM_HOME/bin/ldapUpgrade

Back up the existing *NEW_ISIM_HOME*\bin\DBUpgrade.lax file.

4. Edit the DBUpgrade.lax file, setting the following property:

```
OLD_VERSION=5.1
```

5. Run the **DBUpgrade** command to upgrade the IBM Security Identity Manager database.

Windows

NEW_ISIM_HOME\bin\DBUpgrade

UNIX or Linux

NEW_ISIM_HOME/bin/DBUpgrade

6. In the DBUpgrade.lax file, revert the changes to the OLD_VERSION property to blank value

Running data synchronization utility:

Ensure that you synchronize the access catalog date by using the following data synchronization utility:

Unix

ISIM_HOME/bin/unix/syncISIMData.sh -syncOption Upgrade -dataType ALL

Windows

ISIM_HOME/bin/win/syncISIMData.cmd -syncOption Upgrade -dataType ALL

Note : Any changes you make to Security Identity Manager data on the new system are overwritten when you reimport the Tivoli Identity Manager Version 5.1 production data during the final cutover.

Starting WebSphere Application Server

Start WebSphere® Application Server to complete the production cutover.

About this task

After you completed running **ldapUpgrade** and **DBUpgrade** with the imported data, start the WebSphere application servers and message servers in the new production environment.

You can either use the WebSphere console or use a command line. For cluster deployments, it is easier to use the WebSphere console.

If you previously stopped the HTTP Server, start it after you start the WebSphere servers.

Procedure

If you choose to use the command line, type the following command as applicable to your operating system:

- Windows

WAS_PROFILE_HOME\bin\startServer.bat *servername*

- UNIX or Linux

WAS_PROFILE_HOME/bin/startServer.sh *servername*

Note If WebSphere administrative security is enabled, append the following flag to the end of the previous command.

-user *WAS_username* - password *WAS_user_password*

Where *WAS_username* is the WebSphere Application Server administrative user name and *WAS_user_password* is the password for the administrative user.

New production environment post-cutover tasks

After you complete the production cutover, you must complete some post-cutover tasks.

LDAP recycle bin cleanup

If the enrole.recyclebin.enable property from enRole.properties is set to false, ensure that the recycle bin in LDAP is empty. Otherwise, previously deleted entities might be returned by searches.
If enrole.recyclebin.enable is set to false, the LDAP recycle bin might contain deleted entries after the upgrade. These entries were deleted from a previous version of Tivoli Identity Manager. They might be returned by Security Identity Manager user interface when searching for entries. If this problem exists then you must delete all the entries from the recycle bin in LDAP server or set this property to true.

Verification of the installation

After you complete the installation, confirm that you can log on to the Security Identity Manager version 6.0.2 system.

Log on to Security Identity Manager version 6.0.2. Use the administrator user ID and password that was used in the previous version of Tivoli Identity Manager.

Performance tuning

After you complete verifying the new system, apply performance tuning settings to confirm that the new system meets your performance requirements.

For instance, on systems that run DB2 Universal Database, you might benefit from enabling autoresize on your table spaces. Although enabled is the default setting, verify that you have autoresize enabled. Issue the command:
db2 get snapshot for tablespaces on *itimdb*
Look for the "Auto-resize enabled" line in the output.

Disabling Identity Service Center

If you installed IBM® Security Identity Manager 6.0.2.2, Identity Service Center is installed and started by default. To disable access to Identity Service Center, you must stop com.ibm.isim_BLA in Business-level applications.

Before you begin

Ensure that you are logged on to the WebSphere® Application Server administrative console.

Procedure

1. From the WebSphere Application Server administrative console, select Applications > Application Types > Business-level Applications.
2. Select the com.ibm.isim_BLA application.
3. Click Stop.

   A message displays that com.ibm.isim_BLA is stopped successfully.

Post-migration troubleshooting and known issues

Post-migration troubleshooting provides information about known issues when the migration is completed and provides tips for troubleshooting.

The following issues are known to occur after an upgrade to IBM® Security Identity Manager version 6.0.2.

Default data does not get loaded

Some default data specific to IBM® Security Identity Manager are not loaded at upgrade time.
For example, default access control items (ACIs) are not loaded. These items are not copied to prevent interference with ACIs from previous versions.

Extra files copied for services

If services point to a file on the file system such as an identity feed, copy that file to the new IBM Security Identity Manager version 6.0.2 server. You must also update the service to point to the new file location on the IBM Security Identity Manager version 6.0.2 server. This document instructs you to copy over the contents of the *OLD_ITIM_HOME* directory only.

GetDN supported only on erPolicyMembership or erPolicyTarget

Before you upgrade, ensure that no reports are using the GetDN function on any attributes other than the provisioning policy attributes erPolicyMembership or erPolicyTarget.

This database function is only intended for those two attributes. In IBM® Security Identity Manager version 6.0, the GetDN function is no longer needed. It does not work for other attributes. The report is not valid, and does not parse successfully. This issue extends to custom reports.

DB2 restoration error

Before you upgrade, ensure that no reports are using the GetDN function on any attributes other than the provisioning policy attributes erPolicyMembership or erPolicyTarget.

This database function is only intended for those two attributes. In IBM® Security Identity Manager version 6.0, the GetDN function is no longer needed. It does not work for other attributes. The report is not valid, and does not parse successfully. This issue extends to custom reports.

JavaScript from previous version returns empty

Because of differences between FESI and the IBM® JavaScript Engine, some of the migrated JavaScript might not work after the upgrade.

An explicit return statement is needed with the IBM JavaScript Engine. For more information, see Migration of custom FESI extensions to the IBM JSEngine.

Compilation failure

Some example classes from the extensions directory do not compile upon completion of the upgrade.

These failures are caused by changes in the class and package names.

Cluster installation error

When installing in a clustered environment, the installation process might return an error message.

Examine the *ISIM_HOME*\install_logs\runConfig.stdout directory. If you receive this message, verify that the WebSphere Application Server environment variables are defined correctly.

```
WASX7017E: Exception received while running file
  "C:\Program Files\IBM\itim\config\was\setEVCluster.jacl";
   exception information:
   com.ibm.websphere.management.exception.ConfigServiceException
   java.lang.reflect.UndeclaredThrowableException:
   java.lang.reflect.UndeclaredThrowableException
```

To verify that the WebSphere Application Server environment variables are defined correctly for the cluster member, follow these steps.

1. Verify that the NodeAgent and Deployment Manager are running.
2. Verify that the WebSphere Application Server nodes are synchronized.
3. Run the *ISIM_HOME*\bin\runConfig -install program for the cluster member.