IBM Security Identity Manager
Version 7.0.1.10

Installation Topics

IBM Security Identity Manager
Version 7.0.1.10

Installation Topics

Table of contents

Table list

Part 1. Installation

Use the instructions in this part to install IBM Security Identity Manager.

- IBM® Security Identity Manager components
- Installation planning for deployments
- Installation preparation
- Chapter 2, "Installation of prerequisite components," on page 5
- Installation of Security Identity Manager Server
- Silent installation and configuration
- Verification of the installation
- Configuration of the Security Identity Manager Server
- Troubleshooting
- Uninstallation of Security Identity Manager
- Security Identity Manager reinstallation

Chapter 1. Software firewall configuration in the virtual appliance

Before you start the installation of IBM Security Identity Manager virtual appliance, check the considerations for the port numbers, apart from host names, user accounts, and fix packs.

Having a software firewall on the virtual appliance helps to control only the necessary ports for IBM Security Identity Manager to work.

IBM Security Identity Manager hides all the unwanted ports and provides only those ports that are required by the virtual appliance.

Use the default ports for a standard installation on a clean computer. For advanced or custom deployments, you might have to use different port numbers. If you intend to use the default ports, ensure that the port is not yet assigned and are available before you use the product installation program.

- Check the availability of the ports that are required by the IBM Security Identity Manager virtual appliance.
- Open a port checking utility on the computer. Alternatively, check the firewall rules for the system.
- If the port is already assigned, choose another value when prompted by the installation program.

Table 1 describes a list of available ports that you can use to work with IBM Security Identity Manager virtual appliance:

Table 1. Port numbers

Port numbers	**Used by**
22	Secure Shell (SSH)
161	SNMP server, if configured
443	Secure appliance management interface
1098	Security Directory Integrator web server port
1099	RMI Dispatcher service
9056	Cluster Manager secure administrator host
9057	Cluster Manager bootstrap address
9058	Cluster Manager soap port
9061	Cluster Manager CSIV2 SSL server authentication listener address
9062	Cluster Manager CSIV2 SSL mutual authentication listener address
9063	Cluster Manager ORB Listener
9064	Cluster Manager cell discovery address
9065	Cluster Manager DCS Unicast address
2809	Nodeagent bootstrap address
5001	Nodeagent IPv6 multicast discovery address
7272	Nodeagent node discovery address
8878	Nodeagent soap port

Table 1. Port numbers (continued)

Port numbers	Used by
9201	Nodeagent CSIV2 SSL server authentication listener address
9202	Nodeagent CSIV2 SSL mutual authentication listener address
9353	Nodeagent DCS Unicast address
9900	Nodeagent ORB Listener
9067	Application server bootstrap port
9068	Application server SOAP port
9069	Application server ORB Listener
9071	Application server CSIV2 SSL mutual authentication listener address
9072	Application server CSIV2 SSL server authentication listener address
9073	Application server DCS Unicast address
9082	Application port
9089	Application server SIB secure address
9092	Message Server bootstrap port
9093	Message Server soap port
9094	Message Server ORB listener
9096	Message Server CSIV2 SSL mutual authentication listener address
9097	Message Server CSIV2 SSL server authentication listener address
9112	Message Server DCS Unicast address
9102	Message Server secure default host
9109	Message Server SIB endpoint secure address

Chapter 2. Installation of prerequisite components

You must install and configure the prerequisite components before you install the Security Identity Manager Server.

Database installation and configuration

IBM Security Identity Manager stores transactional and historical data that includes schedules and audit data in a database. Before you install the IBM Security Identity Manager Server, you must install and configure a database.

Note: This information is not a substitute for the more extensive, prerequisite documentation that is provided by the database products. For more information about databases, see the product-related websites.

You can choose to install and configure one of these databases:

- IBM DB2® database
- Oracle database

For more information about supported database releases and required fix packs, see Hardware and software requirements.

Worksheet

This worksheet lists the typical information that you need to install and configure a database. Depending on the database that you install, you might need more information.

Table 2. Typical database worksheet

Field name	**Description**	**Default or example value**	**Your value**
Host name	Name of the computer that hosts the database.		
Port number	Database service listening port.	Examples: 50000, 50002, or 60000	
Database name	Name of the IBM Security Identity Manager database.	Example: `itimdb`	
Admin ID	Database administrator user ID.	Example: `db2admin` **Note:** If you do not use the middleware configuration utility, this value is *db2inst1* by default on UNIX systems.	
Admin password	Password for the database administrator user ID.		
Database user ID	The account that IBM Security Identity Manager uses to log on to the database.	Example: `itimuser`	

Table 2. Typical database worksheet (continued)

Field name	Description	Default or example value	Your value
Database password	The password for the **itimuser** user ID.		

Before you install the database product

Before you install the database product, you must:

- Read the installation information that the database product provides.
- Ensure that your environment meets the product hardware and software requirements.
- Verify that all required operating system patches are in place.
- Ensure that kernel settings are correct for some operating systems, such as the Solaris and Linux operating systems. Each database application specifies its own requirements, such as more operating system values. Before you install the application, read its documentation for these additional settings. For example, see the IBM websites for kernel settings that DB2 requires:
  - AIX®

    Not required.
  - Linux (Red Hat and SUSE)

    http://www.ibm.com/support/knowledgecenter/SSEPGG_10.1.0/com.ibm.db2.luw.qb.server.doc/doc/t0008238.html
  - Windows

    Not required.

Installation and configuration of the IBM DB2 database

Before you can use IBM Security Identity Manager, you must install and configure the IBM DB2 Universal Database™ (DB2). The configuration steps create a database for later use by the IBM Security Identity Manager Server installation program. The installation program populates the database with data objects.

You can install DB2 on the same computer with IBM Security Identity Manager or on a separate computer. Installing DB2 on the same computer requires the installation of a Java™ Database Connectivity driver (JDBC driver, type 4). A JDBC driver makes IBM Security Identity Manager communicate with the data source. Installing DB2 automatically installs the type 4 JDBC driver.

For more information, see Hardware and software requirements.

DB2 installation

IBM Security Identity Manager requires DB2 to run with a required level of the DB2 fix pack. For more information about installing DB2 and any fix packs, see the IBM Security Identity Manager product documentation site for documentation that the database product provides.

User data

The DB2 installation requires that you specify some system data, such as the DB2 administrator user ID and password. The installation wizard provides both status reports and an initial verification activity.

User names and passwords on UNIX and Linux systems

The following table shows the default values that are created on UNIX and Linux systems. Record this information, which is required to configure the DB2 database that IBM Security Identity Manager uses. If you choose not to use the middleware configuration utility to create a DB2 instance, installing DB2 can create a default DB2 instance.

Table 3. DB2 database typical configuration parameters on UNIX and Linux systems

UNIX and Linux systems	Description	Value
DB2 administrator user ID and instance name	The user ID that is used to connect to DB2 as the DB2 administrator and instance owner.	`db2admin` **Note:** If you do not use the middleware configuration utility, this value is `db2inst1` by default.
DB2 instance password	The password for the administrator user ID.	A user-defined value.
DB2 instance home directory	The home directory of the DB2 administrator and instance owner.	• AIX: `/home/db2admin` • Linux: `/home/db2admin` • Linux for System z®: `/home/db2admin` • Linux for System z: `/home/db2admin` • Solaris: `/export/home/db2admin`

User names and passwords on Windows systems

The following table shows the default values that are created on Windows systems. If you choose not to use the middleware configuration utility to create a DB2 instance, installing DB2 can also create the default DB2 instance. For more information about using the middleware configuration utility, see "Running the middleware configuration utility" on page 9.

Table 4. DB2 database typical configuration parameters on Windows systems

Windows systems	Description	Value
DB2 instance name	The name of the DB2 instance.	db2admin **Note:** DB2 defaults to an instance value of DB2.
Administrative user ID	The user ID that is used to connect to DB2 as the DB2 administrator and instance owner.	db2admin
Password	The password for the administrator user ID.	A user-defined value.

Table 4. DB2 database typical configuration parameters on Windows systems (continued)

Windows systems	Description	Value
DB2 instance home directory	The home directory of the DB2 administrator and instance owner.	*drive* For example, `C:`

Installation of the required fix packs

Some versions of DB2 require a fix pack. You can check whether one is required and obtain it from the DB2 support website.

The command for installing a fix pack for DB2 depends on your operating system and whether you created an instance during installation.

Did you create a DB2 instance during installation	Windows operating system	UNIX and Linux operating systems
Yes	Enter the **db2level** command from the DB2 command window: `db2level`	Log on with the DB2 instance user ID and enter the **db2level** command: `su - DB2_instance_ID db2level`

No	Run the regedit command and look for the information in the following location: `HKEY_LOCAL_MACHINE\SOFTWARE\IBM\DB2\InstalledCopies\db2_name\CurrentVersion`	Enter the db2ls command:
		`DB_HOME/install/db2ls`
		or
		`/usr/local/bin/db2ls`

For more information, see *Database server requirements* on the IBM Security Identity Manager product documentation site and the documentation that the DB2 fix pack provides.

Verify the DB2 installation.

Verifying the installation

The installation wizard provides a status report when the installation is complete. Additionally, run the DB2 First Steps operation to verify that the installation is successful.

Before you begin

For more information about verifying the DB2 installation, visit this website: Verifying the installation using the command line processor.

Procedure

1. To run the DB2 First Steps operation, choose your operating system first:
   - UNIX or Linux operating systems
   - Windows operating systems
2. Complete the following step according to your operation system:
   - On the UNIX or Linux operating systems:

     Enter this command:`DB_INSTANCE_HOME/sqllib/bin/db2fs`
   - On the Windows operating systems:

Click **Start** > **Programs** > **IBM DB2** > *DB2 Copy Name* > **Set-up Tools** > **First Steps**

IBM DB2 database configuration

The IBM Security Identity Manager installation product includes a middleware configuration utility that creates database instances and user IDs. It also configures parameters for DB2 and IBM Security Directory Server.

Default values are supplied for many of the typical parameters and all the advanced parameters. If an entered parameter, such as the DB2 instance ID, exists, the middleware configuration utility skips the task of creation. You can choose to keep those values, or provide values of your own. Required fields are marked by an asterisk (*). You can revisit any panel in the deployment wizard by clicking **Back** until you reach the panel.

The middleware configuration utility:

- Creates user IDs if needed
- Creates DB2 instances if needed
- Creates databases if needed
- Tunes DB2 (buffer pool, log tuning)
- Configures some DB2 settings (DB2ENVLIST=EXTSHM, DB2COMM=tcpip)

The middleware configuration utility can be run manually or silently. For more information about silent configuration, see "Configuring DB2 silently" on page 11.

Note: The middleware configuration utility stores by default any input you provide in a response file called `db2ldap.rsp` in the system temp directory; for example, the `/tmp` directory. This file is normally cleaned up after the utility completes. If you cancel the utility before it completes, this file might not be erased.

Running the middleware configuration utility:

You can run the middleware configuration utility to set DB2 parameters for later IBM Security Identity Manager deployment.

Before you begin

On Windows operating systems, you must be an administrator or have administrative authority.

On UNIX and Linux operating systems, you must be a root user. Additionally, the umask setting must be 022. To verify the umask setting, run the command **`umask`** and set the umask value to 022:

```
umask 022
```

Note: Record the values that you provide for the middleware configuration utility for later use with the **`DBConfig`** and **`ldapConfig`** utilities that are used during IBM Security Identity Manager Server installation.

You must run the middleware configuration utility from the computer where IBM DB2 and IBM Security Directory Server are installed. Before you run the utility on RHEL, install the following 32-bit and 64-bit required libraries:

- `compat-libstdc++-33-3.2.3-69`

- `compat-db-4.6.21-15`
- `libXp-1.0.0-15.1`
- `libXmu-1.0.5-1`
- `libXtst-1.0.99.2-3`
- `pam-1.1.1-10`
- `libXft-2.1.13-4.1`
- `gtk2-2.18.9-10`
- `gtk2-engines-2.18.4-5`

Procedure

1. Log on to an account with system administration privileges on the computer where DB2 is installed.
2. If you are installing on AIX in Japanese, Korean, Simplified Chinese, or Traditional Chinese, complete the following steps:

   Note: If you are not installing on AIX in one of these languages, skip this task and continue to the next step.

   a. Locate the `cfg_itim_mw.jar` file from the middleware configuration utility compressed file. The middleware configuration utility compressed file can be found from the product DVD or a download directory.

   b. Run this command: `java -jar cfg_itim_mw.jar`

   This command configures the graphical user interface for the middleware configuration utility to correctly display configuration pages during the middleware configuration. If you do not run this command before you start the middleware configuration utility, you encounter display problems in the language selection page.
3. Start the middleware configuration utility in the base directory of the DVD or a download directory:
   - **AIX operating systems**: Start the middleware configuration utility by running the `cfg_itim_mw_aix` program.
   - **Linux for xSeries operating systems**: Start the middleware configuration utility by running the `cfg_itim_mw_xLinux` program.
   - **Linux for pSeries operating systems**: Start the middleware configuration utility by running the `cfg_itim_mw_pLinux` program.
   - **Linux for zSeries operating systems**: Start the middleware configuration utility by running the `cfg_itim_mw_zLinux` program.
   - **Windows operating systems:** Start the middleware configuration utility by using the `cfg_itim_mw.exe` program if the Windows autorun feature is disabled.

   Each platform requires a file that is named `cfg_itim_mw.jar` to go along with the native program. The JAR file and the native program must be in the same directory location.
4. Select your language, and click **OK**.
5. From the Product Configuration page, check only **Configure IBM DB2 Universal Database**, and click **Next**. If DB2 is not at the correct level or not installed, you can receive a warning. You must ensure that DB2 is at the correct level. To bypass this warning, click **Next**.
6. From the IBM DB2 Database Configuration Options page, provide the following information, and then click **Next**
   - DB2 administrator ID or instance name

Provide the user ID that is used to connect to DB2 Database as the DB2 administrator. For example, `db2admin`. If this value is new, the utility creates a user ID and instance name. If you provide an existing user ID and instance name, no new user ID or instance is created.

- DB2 administrator password

  Enter the password that you set for the DB2 Database administrator account.
- Password confirmation

  Type the password again.
- DB2 server database home

  Provide the directory where the DB2 instance is located. For example, C: or `/home/`*`dbinstancename`*.
- DB2 database name

  Provide the name of the database you are creating. For example, `itimdb`.
- IBM Security Identity Manager database user ID

  Provide the user ID for the database you are creating. For example, `itimuser`.

  Note: On Windows systems, disable password expiration for this user account after you run the utility.
- Password for IBM Security Identity Manager database user ID:

  Provide the password for the database user ID.
- Password confirmation

  Type the password again.
- Group for the DB2 administrator

  Select a valid group, of which root is a member, to associate the DB2 administrator ID instance name. For example, `bin`. This value is available only for UNIX or Linux operating systems.

Note: The dollar sign ($) has special meaning in the installer frameworks that are used by the middleware configuration utility. Avoid $ in any field values. The installer framework or operating system platform might do variable substitution for the value.

7. If you changed the default DB2 instance name, or if a DB2 instance exists with that name, you are prompted with a warning message. If you are using the DB2 instance only for IBM Security Identity Manager, click **Yes**. Do not share the instance with another program.
8. Review your configuration options before you click **Next** to begin the configuration process.
9. The configuration can take up to several minutes to complete. After the configuration completes successfully, click **Finish** to exit the deployment wizard. This step concludes the middleware configuration process for DB2 Database.

What to do next

Verify that the middleware configuration utility completed for DB2 without error, check the `cfg_itim_mw.log` in the system temp directory.

Configuring DB2 silently:

You can use the command line and the `-silent` option to start the middleware configuration utility silently.

Before you begin

Verify that the DB2 database is installed correctly.

Procedure

1. Copy the sample `cfg_itim_mw.rsp` response file (or `cfg_itim_mw_windows.rsp` for Windows systems) to a directory on the target computer.
2. Update the response file with the correct values. Make sure that the configureDB2 value is set to `yes`. If you are not configuring the directory server at the same time, make sure that the configureLDAP value is set to `no`.
3. From a command window, run this command:

   ```
   cfg_itim_mw –W ITIM.responseFile=cfg_itim_mw.rsp –silent
   ```

   Where `cfg_itim_mw` is:
   - **AIX operating systems**: `cfg_itim_mw_aix`
   - **Linux for xSeries operating systems**: `cfg_itim_mw_xLinux`
   - **Linux for pSeries operating systems**: `cfg_itim_mw_pLinux`
   - **Linux for zSeries operating systems**: `cfg_itim_mw_zLinux`
   - **Windows operating systems**: `cfg_itim_mw_windows`

   Note: If you run the middleware configuration utility silently, the response file is updated during the configuration process.

What to do next

Verify the service listening port and service name.

Manual configuration of the DB2 server:

You can manually configure the DB2 server. The DB2 settings described in this information are initial settings that might require runtime adjustment.

Configuring the DB2 server requires the following steps:

1. Creating a user on the operating system.
2. Creating the IBM Security Identity Manager database.
3. Ensuring that TCP/IP communication is specified.

For more information, see the *IBM Security Identity Manager Performance Tuning Guide* technical supplement.

Creating a user on Windows and UNIX systems:

Use this procedure to create an operating system user named `itimuser` on the computer on which the DB2 server is installed.

Before you begin

No special privileges are required for this user. Ensure that a password change is not required at the next logon and that the password never expires.

About this task

The Security Identity Manager Server uses the default user ID `itimuser` to access the database. You can create a user ID other than the default user ID or use an existing user ID.

To create a user, follow these steps:

Procedure

1. As root or as Administrator, start the system management tool for your operating system.
   - AIX operating systems: SMIT or SMITTY
   - Solaris: System Management Console (SMC)
   - Windows: Click **Start** > **Administrative Tools** > **Computer Management** > **Local Users and Groups** > **Users**.
2. Add a user `itimuser` and set the user password.
3. Exit the system management tool.

What to do next

Test the user access. Ensure that you can log on with the user ID `itimuser` without encountering a password reset.

Create the Security Identity Manager database.

Creating a user on a Linux system:

You can use the console command interface or the GUI utility to create a user named `itimuser` on the computer on which the DB2 server is installed.

Before you begin

No special privileges are required for this user. Ensure that a password change is not required at the next logon and that the password never expires.

About this task

The IBM Security Identity Manager Server uses the default user ID `itimuser` to access the database. You can also create your own user ID.

Procedure

There are two methods to create a user on a Linux system:

- Use the console command interface to enter the command:

  ```
  useradd -d /home/itimuser -p password itimuser
  ```

  The -d switch specifies the home directory. The entry `itimuser` specifies the user ID that is created.
- Use the graphical User Manager application to create a user on the Red Hat Enterprise Linux system:
  1. Use one of these methods to create a user:
     - From the graphical User Manager application, select **Applications** > **System Settings** > **Users and Groups**. Or,

- Start the graphical User Manager by typing `redhat-config-users` at a shell prompt.

The Add User window opens.

2. Click **Add User**.
3. In the Create New User dialog box, enter a `username`, the full name of the user for whom this account is being created, and a password.
4. Click **OK**.

What to do next

Test the user access. Ensure that you can log on with the user ID `itimuser` without encountering a password reset.

Create the IBM Security Identity Manager database.

Creating the Security Identity Manager database:

You can specify any name for the IBM Security Identity Manager database, such as `itimdb`.

Before you begin

You must have IBM DB2 database installed and configured on your system.

Procedure

1. In the DB2 command window, enter these commands to create the database:

```
db2 create database itim_dbname using codeset UTF-8 territory us
db2 connect to itim_dbname user itim_dbadmin_name using itim_dbadmin_password
db2 create bufferpool ENROLEBP size automatic pagesize 32k
db2 update db cfg for itim_dbname using logsecond 12
db2 update db cfg for itim_dbname using logfilsiz 10000
db2 update db cfg for itim_dbname using auto_runstats off
db2 disconnect current
```

The value of *itim_dbname* is a name such as `itimdb`. For more information about performance parameter tuning for DB2, see the *IBM Security Identity Manager Performance Tuning Guide*.

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

After you created and configured the IBM Security Identity Manager database, stop and start the DB2 server to allow the changes to take effect. Enter the following commands:

a. db2stop If entering db2stop fails and the database remains active, enter `db2 force application all` to deactivate the database. Enter `db2stop` again.
b. db2start

What to do next

Confirm that TCP/IP communication is specified.

Ensuring that TCP/IP communication is specified:

Installing DB2 specifies TCP/IP communication by default. However, you need to confirm that TCP/IP communication is specified on the DB2 server and on the DB2 client.

Before you begin

You must have IBM DB2 database installed and configured on your system.

Procedure

Enter the command:

```
db2set -all DB2COMM
```

A list of values is returned.

- If a `tcpip` entry is not in the list that was returned, enter this command. Include `tcpip` *and* any other values that were returned in the list that the command provided.

  ```
  db2set DB2COMM=tcpip,values_from_db2set_command
  ```

  For example, if the `db2set -all DB2COMM` command returned values such as `npipe` and `ipxspx` in the list, specify these values again when you enter the `db2set` command the second time:

  ```
  db2set DB2COMM=tcpip,npipe,ipxspx
  ```

A list of values that include `tcpip` is returned.

What to do next

Install and configure another component.

Determining the correct service listening port and service name:

Running the middleware configuration utility configures the service listening port number and the database service name. However, you must verify that the correct service name and listening port are specified.

Before you begin

You must have IBM DB2 database installed and configured on your system.

About this task

A service listening port is associated with each DB2 instance. The port is used for establishing a DB2 connection from a DB2 application to the database owned by the instance.

The DB2 default instance differs depending on your operating system.

- On Windows operating systems: DB2
- On UNIX and Linux operating systems: db2inst1

The default service port number for the DB2 default instance that is created during the DB2 server installation is 50000. Running the middleware configuration utility to create a DB2 instance, the default service port number of the instance is 50002. If you migrated DB2 8.2 to DB2 9.5, DB2 9.7, or DB2 10.1, the DB2 migration utility resets the DB2 instance. The DB2 migration utility might also reset the service port of the instance to 60000.

Procedure

1. To determine whether the correct service name or service listening port is defined. Enter the command

```
db2 connect to itim_dbname user itim_dbadmin_id using itim_dbadmin_password
db2 get dbm cfg
```

Look for the SVCENAME attribute to locate the service name.

2. Locate the statement that specifies the current port number in the services file on the computer where the DB2 server is.

   The services file has the following path:

   - Windows operating systems: `%SYSTEMROOT%\system32\drivers\etc\services`
   - UNIX or Linux operating systems: `/etc/services`

Ensuring that `CUR_COMMIT` is `ON` on DB2 version 9.7 and later versions:

Databases that are updated from versions earlier than DB2 version 9.7 have this parameter set to **`DISABLED`**. It must be set to `ON`.

About this task

Installing DB2 9.7 or later versions sets the **`cur_commit`** parameter to `ON` by default. Databases that are upgraded from a previous release have this parameter set to `DISABLED`. For the proper functioning of IBM Security Identity Manager and to prevent deadlocks during peak load, this parameter must be set to `ON`.

Procedure

1. Determine whether the **`cur_commit`** is set to `ON`. Enter the commands

   ```
   db2 connect to itim_dbname user itim_dbadmin_id using itim_dbadmin_password
   db2 get database configuration
   ```

2. Look for the Currently Committed parameter **`CUR_COMMIT`**. It must be set to ON.

   ```
   Currently Committed (CUR_COMMIT) = ON
   ```

3. If it is not set to `ON`, issue the following commands to enable it.

   ```
   db2 update db cfg  for itim_dbname using cur_commit on
   db2 disconnect current
   ```

4. Stop and start the DB2 server to set the configuration. Issue the commands

   ```
   db2stop
   db2start
   ```

   Note:

   If **`db2stop`** fails and the database remains active, enter **`db2 force application all`** to deactivate the database. Then, enter **`db2stop`**.

What to do next

After you create and configure the IBM Security Identity Manager database, stop and start the DB2 server for the changes to take effect.

DB2 database performance tuning tasks

Performance issues can occur after you initially configure DB2. Performance tuning tasks can ensure that DB2 runs correctly.

Configuring TCP KeepAlive settings:

The failover design of the messaging engine relies upon the database connections that are broken when a messaging engine instance fails. In order for failover to occur in high availability environments, ensure that the system notices the broken connection in a timely manner and releases database locks. This task is done by configuring the TCP KeepAlive settings.

Before you begin

You must have DB2 database installed and configured on your system.

Procedure

1. Log in as a system administrator.
2. Run these commands on the computer where your DB2 Server is.
   - On the Linux operating system, enter these commands:
     ```
     echo 30 >  /proc/sys/net/ipv4/tcp_keepalive_intvl
     echo 30 > /proc/sys/net/ipv4/tcp_keepalive_time
     ```

     Note: These settings are also used by IPv6 implementations.
   - On the Windows operating system, follow this step:

     Run `regedit` to edit the Windows Registry key in the `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters` directory.
3. Restart your computer for changes to take effect. For the Linux operating system, run this command:
   ```
   # /etc/init.d/network restart
   ```

What to do next

Restart the computer for the changes to take effect.

Change of the DB2 application heap size:

Loading many users can encounter performance issues.

You might see this message:

```
Not enough storage available for processing the sql statements.
```

To provide additional storage space, change the DB2 application heap size to a larger value. Use the *IBM Security Identity Manager Performance Tuning Guide* to tune DB2 for all systems for both production and test environments.

Installation and configuration of the Oracle database

IBM Security Identity Manager supports the use of the Oracle database. You must install and configure the database before you install IBM Security Identity Manager.

In all cases, see the installation and migration guides that the Oracle Corporation provides for complete information.

Tasks for creating the database

You must perform a sequence of tasks to create an Oracle database for use with Security Identity Manager.

To create an Oracle database for IBM Security Identity Manager, complete these steps:

1. Back up an existing database.

2. Install the Oracle database server.

   Note: If you are using the Oracle 12c Database, you must create an non-container database. When you create the database, ensure that the **Create as a Container database** check box is clear.
3. Configure the init.ora file.
4. Set the environment variables
5. Install the Oracle JDBC driver.

Backup of an existing database:

Before you begin to install the Oracle product or upgrade an existing database, make a full backup of any existing database.

Review the preliminary steps that the documentation from the Oracle Corporation provides for upgrading an Oracle database.

Installation of the Oracle database server:

You might install the Oracle database server on the same computer or on a computer that is separate from IBM Security Identity Manager.

For information about installing the Oracle database server, see documentation available at Oracle official website. If you are using the Oracle 12c Database, you must create an non-container database. When you create the database, ensure that the **Create as a Container database** check box is clear.

Note: If you manually create the Oracle database for Security Identity Manager, you must manually install the JVM feature. Otherwise any transactions from Security Identity Manager can fail later. You are not required to manually create the database and install the JVM feature. You can use the Oracle Database Configuration Assistant wizard to create the database and install the JVM feature.

Configuring the init.ora file:

After installing an Oracle database server, you must configure the `init.ora` file for the IBM Security Identity Manager database.

Before you begin

You need to have the Oracle database server installed.

Procedure

1. Copy the `init.ora` file.
   - Windows operating systems:
     a. Under the `*ORACLE_HOME*\admin\` directory, create a directory named `*db_name*\pfile`. The value of *db_name* might be *itimdb*.
     b. Copy the sample `initsmpl.ora` file from the `*ORACLE_HOME*\db_1\admin\sample\pfile\` directory to the `*ORACLE_HOME*\admin\db_name\pfile` directory.
     c. Rename the new `init.ora` file to a value of `init*db_name*.ora`.
   - UNIX or Linux operating systems:

     Copy the `*ORACLE_HOME*/product/<*version number*>/dbhome_1/dbs/init.ora` file to a new `*ORACLE_HOME*/dbs/init*db_name*.ora` file.

2. Based on your environment requirements, tune the value of the following parameters in the `initdb_name.ora` file:

   ```
   db_name=itimdb
   compatible=<version number>
   processes=150
   shared_pool_size=50000000
   ```

   Additionally, define three control files for the IBM Security Identity Manager database. This example statement defines the control files for the UNIX operating system:

   ```
   control_files=(ORACLE_HOME/oradata/db_name/control01.ctl,
   ORACLE_HOME/oradata/db_name/control02.ctl,
   ORACLE_HOME/oradata/db_name/control03.ctl)
   ```

   Use the *IBM Security Identity Manager Performance Tuning Guide* to tune Oracle database for all systems for both production and test environments.
3. Manually create all the directories defined in the `initdb_name.ora` file.

What to do next

Set the environment variables.

Environment variable settings for the Oracle database:

Set the environment variables for Oracle by editing the `.profile` file.

Required environment variables include:

- ORACLE_SID=itimdb
- ORACLE_BASE=/home/oracle/app/oracle
- ORACLE_HOME=$ORACLE_BASE/product/12.1.0/dbhome_1
- PATH=$ORACLE_HOME/bin;$PATH

Source the profile on UNIX operating systems that update the environment variables in the current session. This task ensures that Security Identity Manager can communicate with the database. To source the profile, enter the following command:

```
# . /.profile
```

For more information, see the Oracle official website.

Creating the Security Identity Manager database

This step is required only if you do not use the Oracle Database Configuration Assistant wizard, which creates the Security Identity Manager database. To use the Oracle Database Configuration Assistant wizard to create database, see "Creating Database with the Oracle Database Configuration Assistant" from the Oracle Official website.

Before you begin

You must finish installing the Oracle database.

Procedure

1. Manually create an Security Identity Manager database.
   - Windows operating systems:
     a. Create the instance with this command on one line:

```
# oradim -new -sid db_name -pfile ORACLE_HOME\admin\db_name\pfile\
initdb_name.ora
```

The value of the **-sid** parameter specifies the database instance name. For example, the value of *db_name* might be `itimdb`. The value of the **-pfile** parameter specifies the file that you previously configured in "Configuring the init.ora file" on page 18.

b. Start the database instance with these commands:

```
# sqlplus "/ as sysdba"
SQL> startup nomount pfile=ORACLE_HOME\admin\db_name\pfile\initdb_name.ora
```

c. Verify that the Windows service OracleService *db_name* is started.

- UNIX or Linux operating systems:

  Start the database instance with these commands:

```
# ./sqlplus "/ as sysdba"
SQL> startup nomount pfile= ORACLE_HOME/dbs/initdb_name.ora
```

2. Use an SQL script like the following example to create your database. Change the values in the script to match any requirements at your site. In this example, the value of the *db_name* is an instance name such as `itimdb`.

```
--  Create database
CREATE DATABASE db_name
    CONTROLFILE REUSE
    LOGFILE '/u01/oracle/db_name/redo01.log' SIZE 1M REUSE,
            '/u01/oracle/db_name/redo02.log' SIZE 1M REUSE,
            '/u01/oracle/db_name/redo03.log' SIZE 1M REUSE,
            '/u01/oracle/db_name/redo04.log' SIZE 1M REUSE
    DATAFILE '/u01/oracle/db_name/system01.dbf' SIZE 10M REUSE
      AUTOEXTEND ON
      NEXT 10M MAXSIZE 200M
    CHARACTER SET UTF8;

-- Create another (temporary) system tablespace
CREATE ROLLBACK SEGMENT rb_temp STORAGE (INITIAL 100 k NEXT 250 k);

-- Alter temporary system tablespace online before proceeding
ALTER ROLLBACK SEGMENT rb_temp ONLINE;

-- Create additional tablespaces ...
-- RBS: For rollback segments
-- USERs: Create user sets this as the default tablespace
-- TEMP: Create user sets this as the temporary tablespace
CREATE TABLESPACE rbs
    DATAFILE '/u01/oracle/db_name/db_name.dbf' SIZE 5M REUSE AUTOEXTEND ON
      NEXT 5M MAXSIZE 150M;
CREATE TABLESPACE users
    DATAFILE '/u01/oracle/db_name/users01.dbf' SIZE 3M REUSE AUTOEXTEND ON
      NEXT 5M MAXSIZE 150M;
CREATE TABLESPACE temp
    DATAFILE '/u01/oracle/db_name/temp01.dbf' SIZE 2M REUSE AUTOEXTEND ON
      NEXT 5M MAXSIZE 150M;

-- Create rollback segments.
CREATE ROLLBACK SEGMENT rb1 STORAGE(INITIAL 50K NEXT 250K)
  tablespace rbs;
CREATE ROLLBACK SEGMENT rb2 STORAGE(INITIAL 50K NEXT 250K)
  tablespace rbs;
CREATE ROLLBACK SEGMENT rb3 STORAGE(INITIAL 50K NEXT 250K)
  tablespace rbs;
CREATE ROLLBACK SEGMENT rb4 STORAGE(INITIAL 50K NEXT 250K)
  tablespace rbs;

-- Bring new rollback segments online and drop the temporary system one
ALTER ROLLBACK SEGMENT rb1 ONLINE;
ALTER ROLLBACK SEGMENT rb2 ONLINE;
ALTER ROLLBACK SEGMENT rb3 ONLINE;
ALTER ROLLBACK SEGMENT rb4 ONLINE;

ALTER ROLLBACK SEGMENT rb_temp OFFLINE;
DROP ROLLBACK SEGMENT rb_temp ;
```

Note: Use *Security Identity Manager Performance Tuning Guide* to tune the Oracle database for all systems, both for production and test environments.

3. Install the JVM for the database. Use these commands:

```
For UNIX:
# sqlplus "/ as sysdba"

SQL> @$ORACLE_HOME/rdbms/admin/catalog.sql
SQL> @$ORACLE_HOME/rdbms/admin/catproc.sql
SQL> @$ORACLE_HOME/javavm/install/initjvm.sql
SQL> @$ORACLE_HOME/xdk/admin/initxml.sql
SQL> @$ORACLE_HOME/xdk/admin/xmlja.sql
SQL> @$ORACLE_HOME/rdbms/admin/catjava.sql

SQL> connect system/manager
SQL> @$ORACLE_HOME/sqlplus/admin/pupbld.sql

For Windows:
# sqlplus "/ as sysdba"
SQL> @%ORACLE_HOME%/rdbms/admin/catalog.sql
SQL> @%%$ORACLE_HOME%/rdbms/admin/catproc.sql
SQL> @%%$ORACLE_HOME%/javavm/install/initjvm.sql
SQL> @%%$ORACLE_HOME%/xdk/admin/initxml.sql
SQL> @%%$ORACLE_HOME%/xdk/admin/xmlja.sql
SQL> @%%$ORACLE_HOME%/rdbms/admin/catjava.sql

SQL> connect system/manager
SQL> @%ORACLE_HOME/sqlplus/admin/pupbld.sql
```

The value of the *manager* parameter is the password for the system user account.

What to do next

Tune the database performance.

Oracle database performance tuning

To ensure that the Oracle database functions correctly, you can enable XA recovery or configure TCP setting.

Enabling XA recovery operations:

Oracle requires the granting of special permissions to enable XA recovery operations.

Before you begin

Ensure that you have database administrator authority.

About this task

Failure to enable XA recovery can result in the following error:

```
WTRN0037: The transaction service encountered an error on an xa_recover operation.
```

Procedure

1. As the database administrator, connect to the database by issuing this command: **sqlplus /AS SYSDBA**.
2. Run these commands:

   ```
   grant select on pending_trans$ to public;
   grant select on dba_2pc_pending to public;
   grant select on dba_pending_transactions to public;
   grant execute on dbms_system to itim_db_user;
   ```

   where *itim_db_user* is the user that owns the IBM Security Identity Manager database, such as itimuser.
3. Stop and restart the database instance for these changes to take effect.
   - Start the database instance with the following commands:

     ```
     # ./sqlplus "/ as sysdba"
     SQL> startup nomount pfile= ORACLE_HOME/dbs/initdb_name.ora
     ```
   - Stop the database instance with this command:

     ```
     SQL> SHUTDOWN [mode]
     ```

     where *mode* is *normal*, *immediate*, or *abort*.

What to do next

Tune additional settings.

Configuring TCP KeepAlive settings:

The failover design of the messaging engine relies upon the database connections that are broken when a messaging engine incarnation fails. In order for failover to occur in high availability environments, ensure that the RDBMS detects the broken connection in a timely manner and releases database locks. This task is done by configuring the TCP KeepAlive settings.

Before you begin

You need to have an Oracle database installed and configured on your system.

Procedure

1. Log in as a system administrator.
2. Select the following path in the left pane:

   ```
   My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\
   Parameters
   ```
3. Right click in the right pane and select **New** > **DWORD Value**
4. Enter the name as KeepAliveInterval for the new parameter.
5. Right click this new parameter and select **Modify**.
6. Select **Base as Decimal** and enter the value as 30000 (30000 milliseconds = 30 seconds).
7. Similarly, add another DWORD value with name KeepAliveTime and set the value equal to 30000.

What to do next

Restart the computer for the changes to take effect.

Starting the Oracle product and the listener service

To use the Oracle database with IBM Security Identity Manager, you must start both the product and listener service.

Before you begin

You must have an Oracle database installed.

Procedure

1. Start the Oracle database.
   - Windows operating systems:

     Use the **Services** menu to start the Oracle database service called `OracleService`*`db_name`*.
   - UNIX and Linux operating systems:

     Enter these commands:

     ```
     # su - oracle
     # ./sqlplus "/ as sysdba"
     # SQL> startup
     ```
2. Start the Oracle listener service.
   - Windows operating systems:

     Use the **Services** menu to start the Oracle TNS listener named `OracleOraDb12_home1TNSListener`. If the Oracle listener service is idle, start the listener.
   - UNIX and Linux operating systems:

     Enter these commands:

     ```
     # su - oracle
     # ./lsnrctl start
     ```

     To ensure that Oracle processes are started, enter this command:

     ```
     ps -ef | grep ora
     ```

     To ensure that the listener is running, enter this command:

     ```
     # ./lsnrctl status
     ```

What to do next

Install and configure more components.

Installation and configuration of a directory server

Security Identity Manager stores user account and organizational data, but not scheduling and audit data, in a directory server. The information describes configuring the directory server for use by Security Identity Manager.

The supported combinations of directory servers and required fix packs are specified in Hardware and software requirements.

This information is not a substitute for the more extensive, prerequisite documentation that is provided by the directory server product itself. For more information, see Hardware and software requirements. For downloads, see IBM software product support website.

Before you install the directory server product

Before you install the directory server product, you must consider these points:

- Read the installation guide that the directory server product provides.
- Ensure that your installation meets the directory server hardware and software requirements.

Installation and configuration of IBM Security Directory Server

You can install the IBM Security Directory Server on the same computer with IBM Security Identity Manager or on a separate computer.

The supported versions of IBM Security Directory Server support the operating system releases that IBM Security Identity Manager supports.

The IBM Security Directory Server uses DB2 database as a data store and WebSphere® Application Server for the web administration tool.

Installing IBM Security Directory Server

These steps provide information about installing IBM Security Directory Server with the DVDs that are provided with the IBM Security Identity Manager product. These DVDs do not contain embedded middleware for DB2 and Application Server. For installation DVDs that contain the embedded middleware, you can optionally install embedded DB2 and Application Server for IBM Security Directory Server. Your installation process might vary.

Before you begin

For information about installing the directory server, see documentation that the directory server product provides. For example, access this website: http://www.ibm.com/software/sysmgmt/products/support/IBMDirectoryServer.html.

About this task

You cannot use embedded DB2 for the IBM Security Identity Manager database or embedded Application Server.

To install IBM Security Directory Server, follow these steps.

Procedure

1. Install DB2 from the DVD provided with the IBM Security Identity Manager product, if DB2 is not already installed.
2. Install IBM Security Directory Server from the DVD provided with the IBM Security Identity Manager product.
3. During the IBM Security Directory Server installation, you must select **Custom** as the installation type. Click **Next**.
4. In the next panel, do *not* select DB2 Database, or embedded Application Server. You *must* select the supported IBM Security Directory Server. Other features are optional. Click **Next**.
5. In the next panel, the installer detects your Application Server. You might be prompted to select a custom location of the Application Server installation path. You can also choose to skip the deployment of Web Administration Tools. Click **Next**.
6. Review the summary and click **Install** to install IBM Security Directory Server.

For information about installing the directory server, see the IBM Knowledge Center.

What to do next

Install any required fix packs.

Required fix pack installation

If your version of IBM Security Directory Server requires a fix pack, obtain and install the fix pack.

For information about fix packs, see the IBM support website http://www.ibm.com/support/entry/portal/support.

Verifying that the correct fix pack is installed

To verify that the correct fix pack is installed on IBM Security Directory Server, issue the following command:

- AIX: `lslpp -l 'idsldap*'`
- Linux: `rpm -qa | grep idsldap`
- Windows:
  1. From the command prompt, go to `<IDS_HOME>\bin`.
  2. Run this command:
     ```
     idsversion.cmd
     ```

For more information, see Hardware and software requirements and the documentation that the IBM Security Directory Server fix pack provides.

IBM Security Directory Server configuration

Setting up IBM Security Directory Server requires creating the LDAP suffix for your organization before you install the IBM Security Identity Manager Server. Setting up the IBM Security Directory Server also requires configuring the IBM Security Identity Manager referential integrity file. An LDAP suffix, also known as a naming context, is a distinguished name (DN) that identifies the top entry in a locally held directory hierarchy.

The IBM Security Identity Manager installation product includes a middleware configuration utility. This utility creates database instances and user IDs. It configures referential integrity and parameters for DB2 and IBM Security Directory Server. Default values are supplied for many of the typical parameters and all the advanced parameters. If an entered parameter, such as the directory server administrator ID, exists, the middleware configuration utility skips the task of creation. You can choose to keep those values, or provide values of your own. Required fields are marked by an asterisk (*). You can revisit any panel in the deployment wizard by clicking **Back** until you reach the panel.

Note: The middleware configuration utility stores by default any input you provide in a response file called `db2ldap.rsp` in the system temp directory, for example the `/tmp` directory. This file is normally cleaned up after the utility completes. If you cancel the utility before it completes, this file might not be erased.

Running the middleware configuration utility:

You can run the middleware configuration utility to set IBM Security Directory Server parameters for later IBM Security Identity Manager deployment.

Before you begin

Note: The middleware configurtion utility does not support IBM Security Directory Server 6.3.1. You must configure version 6.3.1 manually. See "Configuring IBM Security Directory Server manually" on page 28.

On Windows operating systems, you must be an administrator or have administrative authority.

On UNIX and Linux operating systems, you must be a root user. Additionally, the umask setting must be 022. To verify the umask setting, issue the command: **umask**.

To set the **umask** value to 022, issue this command:

```
umask 022
```

About this task

The middleware configuration utility:

- Creates user IDs if needed
- Creates IBM Security Directory Server instances if needed
- Creates directory server databases if needed
- Tunes LDAP (buffer pool, log tuning)
- Adds the LDAP suffix
- Configures the non-SSL port
- The IBM Security Directory Server supported versions configure the referential integrity plug-in for IBM Security Identity Manager.

The middleware configuration utility can be run manually or silently. For more information about silent configuration, see "Configuring IBM Security Directory Server silently" on page 30.

To start the middleware configuration utility for IBM Security Directory Server manually:

Procedure

1. Log on to an account with system administration privileges on the computer where IBM Security Directory Server is installed.
2. If you are installing on AIX in Japanese, Korean, Simplified Chinese, or Traditional Chinese, complete the following steps:

   Note: If you are not installing on AIX in one of these languages, skip this task and continue to the next step.

   a. Locate the `cfg_itim_mw.jar` file from the middleware configuration utility compressed file. The middleware configuration utility compressed file can be found in the base directory of the product DVD or a download directory.
   b. Run this command: `java -jar cfg_itim_mw.jar`

This command configures the graphical user interface for the middleware configuration utility to correctly display configuration panels during the middleware configuration. If you do not run this command before starting the middleware configuration utility, you encounter display problems in the language selection panel.

3. Start the middleware configuration utility in the base directory of the DVD or a download directory:
   - AIX operating systems: Start the middleware configuration utility by running the `cfg_itim_mw_aix` program.
   - Linux for xSeries operating systems: Start the middleware configuration utility by `running the cfg_itim_mw_xLinux` program.
   - Linux for pSeries operating systems: Start the middleware configuration utility by running the `cfg_itim_mw_pLinux` program.
   - Linux for zSeries operating systems: Start the middleware configuration utility by running the `cfg_itim_mw_zLinux` program.
   - Windows operating systems: Start the middleware configuration utility by using the `cfg_itim_mw.exe` program if the Windows autorun feature is disabled.

   Each platform requires a file called `cfg_itim_mw.jar` to go along with the native program. The JAR file and the native program must be in the same directory location.
4. Select your language, and click **OK**.
5. From the Product Configuration panel, check only **Configure IBM Tivoli Directory Server**, and click **Next**.
6. You can receive a warning if IBM Security Directory Server is not at the correct level or not installed. Action might be required to make sure that IBM Security Directory Server is at the correct level. To bypass this warning, click **Next**.
7. From the IBM Security Directory Server configuration options panel, provide the following information, and then click **Next**.
   - Directory server administrator ID and instance name

     Provide the user ID that is used to connect to IBM Security Directory Server as the directory server administrator. For example, `itimldap`.

     Note: On Windows systems, disable password expiration for this user account after running the utility.
   - Directory server administrator password

     Enter the password that you set for the IBM Security Directory Server administrator account.
   - Password confirmation

     Type the password again.
   - Group for the DB2 administrator

     Select from the list a valid group, of which root is a member, to associate the DB2 administrator ID. For example, `bin`. This value is available only for UNIX or Linux operating systems.
   - Directory server database home

     Provide the directory where the DB2 instance of directory server is. For example, C: or `/home/`*`directory_server_instancename`*.
   - Directory server database name

     Provide the name of the database you are creating. For example, `ldapdb2`.

- Encryption seed

  Provide an encryption key, which can be any word or phrase. The key is used to encrypt IBM Security Identity Manager passwords and other sensitive text. The encryption seed must be at least 12 characters in length.

  Note: The dollar sign ($) has special meaning in the installer frameworks used by the middleware configuration utility. Avoid $ in any field values. The installer framework or operating system platform might do variable substitution for the value.

8. Provide the following LDAP information, and then click **Next**.
   - Administrator DN

     The user ID that represents the principal distinguished name. This DN is the root suffix for IBM Security Identity Manager. For example, `cn=root`.
   - Administrator DN password

     The password of the user ID that represents the principal distinguished name. For example, `secret`.
   - Password confirmation

     Type the password again.
   - User-defined suffix

     Provide the LDAP suffix. This suffix can be any valid suffix and is used as the context root under which IBM Security Identity Manager information is located. For example, choose `dc=com`.
   - Non-SSL port

     The port on which the directory server is listening. The default port is 389.

     Note: This default port might conflict with other services. For example, a Windows server can run Windows Active Directory services, which use a default port of 389.
9. Review your configuration options before clicking **Next** to begin the configuration process.
10. The configuration can take up to several minutes to complete. When the configuration completes successfully, click **Finish** to exit the deployment wizard.

What to do next

This task concludes the middleware configuration process for IBM Security Directory Server. To verify the middleware configuration utility completed for IBM Security Directory Server without error, check the `cfg_itim_mw.log` in the system temp directory.

Configuring IBM Security Directory Server manually:

If the middleware configuration utility does not support your version of the directory server, you must configure the directory server manually.

Before you begin

You must have the directory server and a database installed. See "Database installation and configuration" on page 5 and "Installation and configuration of a directory server" on page 23.

About this task

To configure the directory server, you must create and configure a directory server instance.

Enter all commands on a single line. The command might be split in the document for formatting purposes.

Procedure

1. Create a user. Issue one of these commands.
   - On Windows operating systems
     ```
     LDAP_Install_Location\sbin\idsadduser -u ldapinst -w ldapinstpwd
     ```
     Where

     ldapinst is the user name.

     ldapinstpwd is the password.
   - On UNIX or Linux operating systems
     ```
     LDAP_Install_Location/sbin/idsadduser -u ldapinst -w ldapinstpwd -g
     idsldap –l /home/ldapinst
     ```
     Where

     ldapinst is the user name.

     ldapinstpwd is the password.

     idsldap is the default LDAP group.

     /home/ldapinst is the instance home directory.
2. Create a directory server instance. Issue the command.
   ```
   IBM Security Identity Manager LDAP_Install_Location/sbin/idsicrt -I ldapinst -e encryptionseed
   –l /home/ldapinst
   ```
   Where

   ldapinst is the LDAP instance name.

   encryptionseed is the encryption seed.

   /home/ldapinst is the instance home directory.
3. Create a database for the LDAP instance. Issue the command.
   ```
   LDAP_Install_Location/sbin/idscfgdb -I ldapinst -a dbadmin -w dbadminpwd
   -t dbname -l /home/ldapinst
   ```
   Where

   ldapinst is the LDAP instance name.

   dbadmin is the database administrator name.

   dbadminpwd is the database administrator password.

   dbname is the database name.

   /home/ldapinst is the instance home directory.
4. Set the password for directory server instance Principal DN. Issue the command.
   ```
   LDAP_Install_Location/sbin/idsdnpw -I ldapinst -u cn=root -p
   root
   ```
   Where

   ldapinst is the LDAP instance name.

   `cn=root` is the Principal DN.

   `root` is the Principal DN password.
5. Add the suffix `dc=com` in the directory server instance. Issue the command on a single line.
   ```
   LDAP_Install_Location/sbin/idscfgsuf -I ldapinst -s dc=com
   ```

Where

ldapinst is the LDAP instance name.

dc=com is the suffix.

6. Start the directory server instance.
   - On Windows operating systems

     Use the Windows Services application to start the LDAP instance.
   - On UNIX or Linux operating systems issue the command.*LDAP_Install_Location*/sbin/ibmslapd -I *ldapinst* -n -t
7. Create an ldif file such as dccom.ldif with the following content.

   ```
   dn:dc=com
   objectclass:domain
   ```
8. Run the following command. *LDAP_Install_Location*/bin/idsldapadd -p *ldap_server_port* -D *bind_dn* -w *bind_dn_password* -f dccom.ldif

   Where

   ldap_server_port is the port on which the LDAP server listens.

   bind_dn is the distinguished name that binds to the LDAP directory.

   bind_dn_password is the password for authentication

   dccom.ldif is the name of the ldif file.

   For example,

   On Windows operating systems

   ```
   Program Files\IBM\ldap\V6.3.1\bin\idsldapadd -D cn=root -w secret -p 389
   -f dccom.ldif
   ```

   On UNIX or Linux operating systems

   ```
   /opt/IBM/ldap/V6.3.1/bin/idsldapadd -D cn=root -w secret -p 389 -f
   dccom.ldif
   ```

Configuring IBM Security Directory Server silently:

You can run the middleware configuration utility to set IBM Security Directory Server parameters for later Security Identity Manager deployment.

Before you begin

On Windows operating systems, you must be an administrator or have administrative authority.

On UNIX and Linux operating systems, you must be a root user. Additionally, the umask setting must be 022. To verify the umask setting, issue the command: **umask**.

To set the **umask** value to 022, issue the command:

```
umask 022
```

About this task

The middleware configuration utility:
- Creates user IDs if needed
- Creates IBM Security Directory Server instances if needed
- Creates directory server databases if needed
- Tunes LDAP (buffer pool, log tuning)
- Adds the LDAP suffix

- Configures the non-SSL port
- The IBM Security Directory Server supported versions configure the referential integrity plug-in for Security Identity Manager.

To start the middleware configuration utility silently:

Procedure

1. Copy the sample response file `cfg_itim_mw.rsp` (or `cfg_itim_mw_windows.rsp` for Windows systems) to a directory on the target computer.
2. Update the response file with the correct values. Make sure that the `configureLDAP` value is set to `yes`. If you are not configuring the database server at the same time, make sure the `configureDB2` value is set to `no`.
3. From a command window, run this command:

   ```
   cfg_itim_mw –W ITIM.responseFile=cfg_itim_mw.rsp –silent
   ```

   where *cfg_itim_mw* is:
   - AIX operating systems: **`cfg_itim_mw_aix`**
   - Linux for xSeries operating systems: **`cfg_itim_mw_xLinux`** program
   - Linux for pSeries operating systems: **`cfg_itim_mw_pLinux`** program
   - Linux for zSeries operating systems: **`cfg_itim_mw_zLinux`** program
   - Windows operating systems: **`cfg_itim_mw_windows`**

   Note: If you run the middleware configuration utility silently, the response file is updated during the configuration process.

What to do next

This task concludes the middleware configuration process for IBM Security Directory Server. To verify the middleware configuration utility completed for IBM Security Directory Server without error, check the `cfg_itim_mw.log` in the system temp directory.

Successful suffix object configuration verification:

After running the middleware configuration utility, you need to verify that the LDAP suffix was added successfully.

To verify the suffix object configuration, enter this command:

- Windows operating systems: `ITDS_HOME\bin\ldapsearch.cmd -h localhost -b dc=com "(objectclass=domain)"`
- UNIX or Linux operating systems: `ITDS_HOME/bin/ldapsearch.sh -h localhost -b dc=com "(objectclass=domain)"`

The options are:

-h Specifies a host on which the LDAP server is running.

-b Specifies the search base of the initial search instead of the default.

The output confirms that you configured permissions for `dc=com` and initialized the suffix with data.

```
dc=com
objectclass=domain
objectclass=top
dc=com
```

Manually tuning the IBM Security Directory Server database:

You can manually tune the performance of the DB2 instance that IBM Security Directory Server uses.

Before you begin

Ensure that a DB2 database is installed and configured on your system

Procedure

1. Open a DB2 command window.
2. In the DB2 command window, enter these commands to tune the IBM Security Directory Server database instance:

   ```
   db2 connect to itds_dbname user itds_dbadmin_name using itds_dbadmin_password
   db2 alter bufferpool IBMDEFAULTBP size automatic
   db2 alter bufferpool ldapbp size automatic
   db2 update db cfg for itds_dbname using logsecond 12
   db2 update db cfg for itds_dbname using logfilsiz 10000
   db2 update db cfg for itds_dbname using database_memory itds_dbmemory
   db2 disconnect current
   ```

   The value of *itim_dbname* is a name such as `itimdb`. The value of *itim_dbmemory* is `40000` for a single-server installation, `COMPUTED` for all platforms except AIX and Windows. For AIX and Windows, the value is `AUTOMATIC`. For more information about performance parameter tuning for DB2, see *Security Identity Manager Performance Tuning Guide*.
3. Stop and start the DB2 server to reset the configuration. After you have reset the configuration, stop and start the DB2 server to allow the changes to take effect. Enter the following commands:

   ```
   db2stop
   db2start
   ```

   If entering `db2stop` fails and the database remains active, enter `db2 force application all` to deactivate the database. Enter `db2stop` again.

What to do next

Install and configure another component.

Security configuration of the directory server

Secure socket layer (SSL) communication is used between an LDAP server and Security Identity Manager to secure communications. You must configure the LDAP server to use SSL for secure communications.

If you are using IBM Security Directory Server to store Security Identity Manager information, you must set the server to use SSL. Then you must configure the SSL certificates that you want to use.

This task can be done only after installing Security Identity Manager. If you want to configure LDAP only through an SSL connection, skip the LDAP configuration during the installation and run **`ldapConfig`** after the installation completes.

Configuration of SSL for IBM Security Directory Server:

To have secure socket layer (SSL) communication between IBM Security Directory Server and Security Identity Manager, you must configure IBM Security Directory Server to listen on a port with a defined certificate. The certificate authority must be in the signer certificate database on the SSL client.

Use GSKit to create the key database file and certificates. Make sure to extract the server certificate (the one created for the LDAP server) for client use. The certificate must be copied to the system where Security Identity Manager is running. The location of the server certificate is required to set up a trusted certificate for Security Identity Manager in a later task.

For more information about activating SSL on LDAP for IBM Security Directory Server, see the documentation available in the IBM Security Directory Server section of the IBM Knowledge Center.

Configuration of SSL for Oracle Directory Server Enterprise Edition:

Security Identity Manager supports SSL communication with Oracle Directory Server Enterprise Edition. Oracle Directory Server comes pre-configured with SSL.

For more information about configuring the clients to communicate with Oracle Directory Server, see the documentation available at the official Oracle website.

Installation and configuration of Oracle Directory Server Enterprise Edition

Security Identity Manager requires a directory server. You can install and configure Oracle Directory Server Enterprise Edition.

Oracle Directory Server Enterprise Edition installation

For the instructions and more information about installing the Oracle Directory Server Enterprise Edition, see the official Oracle website.

Configuring Oracle Directory Server Enterprise Edition

After you install Oracle Directory Server Enterprise Edition, configure it for use with IBM Security Identity Manager.

Before you begin

Ensure that you downloaded and installed Oracle Directory Server Enterprise Edition.

Procedure

1. Create an IBM Security Identity Manager LDAP server instance. Type this command:

   ```
   ./dsadm create -p portnumber -P SSL-port instance-path
   ```

   Where *portnumber* is the port number for the Oracle Directory Server Enterprise Edition, and *SSL-port* is the SSL port number for the Oracle Directory Server Enterprise Edition. For example:

   - For UNIX or Linux operating systems:

     ```
     ./dsadm create –p 1389 –P 1363 /local/itimldap
     ```

   - For Windows operating systems:

     ```
     dsadm.exe create –p 1389 –P 1363 C:\itimldap
     ```

2. Start the IBM Security Identity Manager LDAP server. Type this command:

   ```
   ./dsadm start instance-path
   ```

   For example:

   - For UNIX or Linux operating systems:

     ```
     ./dsadm start /local/itimldap
     ```

   - For Windows operating systems:

     ```
     dsadm.exe start \local\itimldap
     ```

3. Create a root suffix. Type this command:

   ```
   ./dsconf create-suffix –h host –p portnumber rootsuffix
   ```

   For example:

   - For UNIX or Linux operating systems:

     ```
     ./dsconf create-suffix –h localhost –p 1389 dc=com
     ```

   - For Windows operating systems:

     ```
     dsconf.exe create-suffix –h localhost –p 1389 dc=com
     ```

   This command creates the root suffix dc=com on the LDAP server.

   If you receive the following message, use the **--unsecured** parameter:

   ```
   Unable to bind securely on host:portNumber
   ```

   For example:

   - For UNIX or Linux operating systems:

     ```
     ./dsconf create-suffix -–unsecured –h localhost –p 1389 dc=com
     ```

   - For Windows operating systems:

     ```
     dsconf.exe create-suffix -–unsecured –h localhost –p 1389 dc=com
     ```

4. Create and save a file named dcequalscom.ldif with the following content:

   ```
   dn:dc=com
   dc:com
   objectclass:top
   objectclass:domain
   ```

5. Import the dcequalscom.ldif file to the dc=com root suffix. Type this command:

   ```
   ./dsconf import -p portnumber -e path/dcequalscom.ldif rootsuffix
   ```

   For example:

   - For UNIX or Linux operating systems:

     ```
     ./dsconf import -p 1389 -e /temp/dcequalscom.ldif dc=com
     ```

   - For Windows operating systems:

     ```
     dsconf.exe import -p 1389 -e \temp\dcequalscom.ldif dc=com
     ```

   If you receive the following message, use the **--unsecured** parameter:

   ```
   Unable to bind securely on host:portNumber
   ```

   - For UNIX or Linux operating systems:

     ```
     ./dsconf import --unsecured -p 1389 -e /temp/dcequalscom.ldif dc=com
     ```

   - For Windows operating systems:

     ```
     dsconf.exe import --unsecured -p 1389 -e \temp\dcequalscom.ldif dc=com
     ```

6. Restart the directory server.

What to do next

Oracle Directory Server Enterprise Edition access control instructions might activate anonymous read access. To provide more secure data, modify the default access control instructions to disable anonymous read access. For more information, see the Oracle Directory Server Enterprise Edition documentation.

Install and configure another component.

Setting up the directory server for SSL connection

To set up an IBM Security Identity Manager virtual appliance, you can set up the directory server for an SSL connection.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

The `iKeyman` utility is in the IBM Security Directory Server.

Procedure

1. Create a certificate. Use the `iKeyman` utility to create a self-signed certificate and extract the certificate to make it available for secure communication.
   a. Start the `iKeyman` utility. For example, type the `gsk7ikm` command in the `/usr/local/ibm/gsk7/bin` directory.
   b. If the `iKeyman` utility cannot locate Java, run this command: **`export JAVA_HOME=opt/IBM/ldapv6.3/java/jre`**
   c. On the IBM Key Management page, select **Key Database File** > **Open** > **New**.
   d. Select a default database type of CMS.
   e. In the **File Name** field, type a name for the CMS key database file. For example, type: `LDAPSERVER_TEST1234.kdb`.

      For example, the value specifies *application_serverhostname*.

      application is the directory server, and *serverhostname* is the server that has the directory server.
   f. In the **Location** field, specify a location to store the key database file. For example, type `/certs`.
   g. Click **OK**.
   h. On the **Password** menu:
      1) Type and then confirm a password, such as `Pa$$word1`.
      2) Specify the highest password strength possible.
      3) Specify **Stash the password to a file?**.
      4) Click **OK**.
   i. Select **Create** > **New Self Signed Certificate** and specify a label that matches the CMS key database file name, such as `LDAPSERVER_TEST1234.`

      This example uses the same name (`LDAPSERVER_TEST1234`) for both the certificate name and the key database file that contains the certificate.
   j. Type `IBM` in the **Organization** field, accept the remaining field default values, and click **OK**. A self-signed certificate, including public and private keys, now exists.
   k. For subsequent use with clients, extract the contents of the certificate into an ASCII Base-64 Encoded file. Complete these steps:

1) Select **Extract Certificate**.

2) Specify a data type of DER Data.

A file with an extension of `.der` contains binary data. This format can be used only for a single certificate. Specify this format to extract a self-signed certificate.

3) Specify the name of the certificate file name you created, such as `LDAPSERVER_TEST1234.der`.

4) Specify a location, such as `/certs`, in which you previously stored the key database file.

5) Click **OK**.

l. Verify that the `/certs` directory contains the following files:

Table 5. Files in the `/certs` *directory*

File	Description
LDAPSERVER_TEST1234.crl	Not used in this example.
LDAPSERVER_TEST1234.der	The certificate.
LDAPSERVER_TEST1234.kdb	Key database file that has the certificate.
LDAPSERVER_TEST1234.rdb	Not used in this example.
LDAPSERVER_TEST1234.sth	Stash file that has the password

Note: If you use an existing or newly acquired certificate from a CA, copy it to the `/certs` directory on root file system of the directory server.

For more information, see:

- IBM Security Directory Server administration topics on securing directory communications at:

  http://www.ibm.com/support/knowledgecenter/SSVJJU_6.3.1/com.ibm.IBMDS.doc_6.3.1/welcome.htm

- *IBM Global Security Kit Secure Sockets Layer Introduction and iKeyman User's Guide* at:

  http://www.ibm.com/support/docview.wss?uid=pub1sc23651000

2. Enable the directory server for an SSL connection. Use an LDIF file to configure SSL on the directory server and to specify a secure port.

   a. If the directory server is not running, start the server. For example, on UNIX, type the command as `/opt/IBM/ldap/V6.3/sbin/ibmslapd -I itimldap`, where **-I** specifies the instance.

   b. Create an LDIF file, such as `ssl.ldif`, with the following data:

```
dn: cn=SSL,cn=Configuration
changetype: modify
replace: ibm-slapdSecurity
ibm-slapdSecurity: sslonly
-
replace: ibm-slapdSslKeyDatabase
ibm-slapdSslKeyDatabase: /certs/LDAPSERVER_TEST1234.kdb
-
add:ibm-slapdSslKeyDatabasePW
ibm-slapdSslKeyDatabasePW: server
```

Note: The empty lines that contain only the - (hyphen) character are expected for LDIF file formatting.

To change the secured port from the default port number 636, add these additional lines:

```
replace: ibm-slapdSecurePort
ibm-slapdSecurePort: 637
```

If you have more than one certificate, specify the certificate name as follows to manage the SSL connection for the directory server:

```
add: ibm-slapdSslCertificate
ibm-slapdSslCertificate: certificatename
```

c. Place the LDIF file in the following directory:

```
/opt/IBM/ldap/V6.3/bin
```

d. Run the **idsldapmodify** command, which modifies the password policy by adding the LDIF file to the process.

```
idsldapmodify -D cn=root -w passwd -i ssl.ldif
```

-D Binds to the LDAP directory, which is `cn=root` in this example.

-w Uses the *passwd* value, which is the directory server administrator password, as the password for authentication.

-i Reads the entry modification information from an LDIF file instead of from standard input. In this example, the file is named `ssl.ldif`.

A successful result produces a message similar to the following one:

```
Operation 0 modifying entry cn=SSL,cn=Configuration
```

e. Test the directory server to confirm that it is listening on the default secure port 636. Follow these steps:

1) Stop the directory server. Type the command as `/opt/IBM/ldap/V6.3/sbin/ibmslapd -k -I itimldap`.

2) Start the directory server. Type the command as `/opt/IBM/ldap/V6.3/sbin/ibmslapd -I itimldap`, where **-I** specifies the instance.

3) Determine whether the directory server is listening on port 636.

For example, display statistics for the network interface with the directory server by typing the command as `netstat -an |grep 636`.

A return message that indicates the port is listening might be this example:

```
tcp    0   0 9.42.62.72:636  0.0.0.0:*   LISTEN
```

Optionally installing IBM Security Directory Integrator

IBM Security Directory Integrator synchronizes and manages information exchanges between applications or directory sources. This section focuses on installing the IBM Security Directory Integrator for use by IBM Security Identity Manager.

Before you begin

Before you install IBM Security Directory Integrator, complete these steps:

- Read the installation guide that the directory integrator product provides.
- Ensure that your installation meets the directory integrator hardware and software requirements.
  - Hardware and software requirements, and documentation
  - Fixes

  See the IBM Support Portal at `http://www.ibm.com/support/entry/portal/support?brandind=Tivoli`

About this task

The information in this chapter is not a substitute for the more extensive, prerequisite documentation that is provided by the directory integrator product itself. You can install theIBM Security Directory Integrator on the same computer with IBM Security Identity Manager or on a separate computer.

Procedure

1. Install the required fix packs. If your version of the IBM Security Directory Integrator requires a fix pack, obtain and install the fixes. For more information, see the support website:
   - Support

     IBM Support Portal at `http://www.ibm.com/support/entry/portal/support?brandind=Tivoli`
   - Product documentation site

     IBM Knowledge Center at `http://www.ibm.com/support/knowledgecenter/SSCQGF/welcome`
2. Install agentless adapters

   Adapters works with IBM Security Identity Manager to manage resources. Agent-based adapters require the installation of the adapter on the managed resource and the installation of an adapter profile on the IBM Security Identity Manager Server. Agentless adapters require adapter installation on the computer that hosts IBM Security Directory Integrator. They also require the installation of an adapter profile on the IBM Security Identity Manager Server.

   You can install IBM Security Directory Integrator on the same computer as IBM Security Identity Manager or remotely. If you install IBM Security Identity Manager locally, the installation program automatically installs agentless adapters. You can also choose to automatically install agentless adapter profiles. If you install IBM Security Identity Manager remotely, you must manually install the agentless adapters on the computer that hosts IBM Security Directory Integrator. You must manually install agentless adapter profiles on the computer that hosts IBM Security Identity Manager.

   Note: You must wait until you finish installing IBM Security Identity Manager before you can *manually* install the agentless adapters and adapter profiles.

What to do next

Manually install agentless adapters and adapter profiles on remote systems. See "Installing agentless adapters" and "Installing agentless adapter profiles" on page 41.

Install and configure other components.

Installing agentless adapters

The UNIX and Linux adapter and the LDAP adapter are the two agentless adapters that are bundled with the IBM Security Identity Manager version 7.0. The adapters must be installed on the IBM Security Directory Integrator. IBM Security Identity Manager version 7.0 supports IBM Security Directory Integrator versions 7.1 and 7.1.1. You can install the adapters interactively or silently.

Before you begin

You must install the following components for the adapter to function correctly:

1. IBM Security Directory Integrator version 7.1.1
2. The Dispatcher
3. The UNIX and Linux adapter

Note: The LDAP adapter requires the Dispatcher only.

About this task

You can install the Dispatcher and the UNIX and Linux adapter, or the LDAP adapter interactively or silently. The Dispatcher must be installed on Security Directory Integrator before you install the UNIX and Linux adapter.

Procedure

1. To install the Dispatcher interactively, run these commands:
   a. For Windows operating systems, type:
      ```
      cd \download\adapters
      ```
      Then type the following text as a single command:
      ```
      ITDI_HOME\jvm\jre\bin\java.exe -jar DispatcherInstall_70.jar
      ```
   b. For UNIX and Linux operating systems, type:
      ```
      cd /download/adapters
      ```
      Then type the following text as a single command:
      ```
      ITDI_HOME/jvm/jre/bin/java -jar DispatcherInstall_70.jar
      ```
2. To install the Dispatcher silently, run these commands:
   a. For Windows operating systems, type:
      ```
      cd \download\adapters
      ```
      To install the Dispatcher in silent mode with the default settings, run the command:
      ```
      ITDI_HOME\jvm\jre\bin\java.exe -jar DispatcherInstall.jar -i silent
      ```
      To install the Dispatcher in silent mode and with one or more custom settings, use the **-D** parameter. For example:
      ```
      ITDI_HOME\jvm\jre\bin\java.exe -jar DispatcherInstall.jar -i silent
      -DUSER_INSTALL_DIR="C:\Program Files\IBM\TDI\V7.1"
      -DUSER_SELECTED_SOLDIR="C:\Program Files\IBM\TDI\V7.1\timsol"
      -DUSER_INPUT_PORTNUMBER=1099
      -DUSER_DISPATCHER_SERVICE_NAME="ISIM Adapters"
      ```
      Where:

      -DUSER_INSTALL_DIR
      Overrides the default Security Directory Integrator installation path.

      -DUSER_SELECTED_SOLDIR
      Overrides the default adapters solutions directory.

      -DUSER_INPUT_RMI_PORTNUMBER
      Overrides the default RMI port number on which the dispatcher listens.

-DUSER_DISPATCHER_SERVICE_NAME
Specifies the name of the Dispatcher service on the Windows operating system.

b. For UNIX and Linux operating systems, type:

```
cd /download/adapters
```

To install the Dispatcher in silent mode with the default settings, run the command:

```
ITDI_HOME\jvm\jre\bin\java -jar DispatcherInstall.jar -i silent
```

To install the Dispatcher in silent mode and with one or more custom settings, use the **-D** parameter. For example:

```
ITDI_HOME/jvm/jre/bin/java -jar DispatcherInstall.jar -i silent
-DUSER_INSTALL_DIR="/opt/IBM/TDI/V7.1"
-DUSER_SELECTED_SOLDIR="/opt/IBM/TDI/V7.1/timsol"
-DUSER_INPUT_PORTNUMBER=1099
-DUSER_DISPATCHER_SERVICE_NAME="ISIM Adapters"
```

Where:

-DUSER_INSTALL_DIR
Overrides the default Security Directory Integrator installation path.

-DUSER_SELECTED_SOLDIR
Overrides the default adapters solutions directory.

-DUSER_INPUT_RMI_PORTNUMBER
Overrides the default RMI port number on which the dispatcher listens.

-DUSER_DISPATCHER_SERVICE_NAME
Specifies the name of the Dispatcher service on the Windows operating system.

3. To install the UNIX and Linux adapter interactively, run these commands:

a. For Windows operating systems, type:

```
cd \download\adapters
```

Then type the following text as a single command:

```
ITDI_HOME\jvm\jre\bin\java.exe -jar PosixAdapterInstall_70.jar
```

b. For UNIX and Linux operating systems, type:

```
cd /download/adapters
```

Then type the following text as a single command:

```
ITDI_HOME\jvm\jre\bin\java.exe -jar PosixAdapterInstall_70.jar
```

4. To install the UNIX and Linux adapter, or the LDAP adapter, in silent mode, run these commands:

a. For Windows operating systems, type:

```
cd \download\adapters
```

To install the adapter in silent mode with the default settings, issue the command:

```
ITDI_HOME\jvm\jre\bin\java.exe -jar PosixAdapterInstall_70.jar -i silent
```

To install the adapter in silent mode and changing default settings, use the **-D** parameter. For example:

```
ITDI_HOME\jvm\jre\bin\java.exe -jar PosixAdapterInstall_70.jar -i silent
 -DUSER_INSTALL_DIR="C:\Program Files\IBM\TDI\V7.1"
```

Where

-DUSER_INSTALL_DIR
Overrides the default Security Directory Integrator installation path.

b. For UNIX and Linux operating systems, type:

```
cd /download/adapters
```

To install the adapter in silent mode with the default settings, issue the command:

```
ITDI_HOME/jvm/jre/bin/java -jar PosixAdapterInstall_70.jar -i silent
```

To install the adapter in silent mode and changing default settings, use the **-D** parameter. For example:

```
ITDI_HOME/jvm/jre/bin/java -jar PosixAdapterInstall_70.jar -i silent
 -DUSER_INSTALL_DIR="/opt/IBM/TDI/V7.1"
```

Where

-DUSER_INSTALL_DIR
Overrides the default Security Directory Integrator installation path.

Installing agentless adapter profiles

Use the following procedure to install the agentless adapter profiles. It is a good practice to always download the latest POSIX adapters from the adapter download site.

About this task

You can install agentless adapter profiles from the IBM Security Identity Manager user interface.

Procedure

1. From the **Appliance Dashboard**, go to the Quick Links widget.
2. Click the **Identity Administration Console** link.
3. Log in to the IBM Security Identity Manager console.
4. From the IBM Security Identity Manager console, select **Configure System** > **Manage Service Types** > **Import**.

Configuring the Identity external user registry

Use the Identity External User Registry Configuration page to configure or reconfigure the external user registry for the IBM Security Identity Manager virtual appliance.

Before you begin

Make sure to add the required users to the Identity external user registry before you work from the Identity External User Registry Configuration page.

For more information, see “Adding required users to the external user registry” on page 45.

About this task

See Table 6 that lists the external user registry options that you can configure or reconfigure.

Table 6. Identity external user registry configuration details.

Button	Identity external user registry options
Configure	**External registry type** Select an external registry type from the list: • IBM Security Directory Server • Sun Java System Directory Server • Microsoft Active Directory **Host name** Specify the name of the server that hosts the directory server. The acceptable formats for the host name are FQDN, IPv4, and IPv6. For example, `isimldap.example.com`. **Port** Specify the directory service port. For example, `389`. You can select or clear the **SSL** check box to manage the secure connection. **Principal DN** Specify the principal distinguished name. For example, `cn=root`. **Password** Specify the password for the principal distinguished name. **External registry DN location** Specify the location of the external registry DN. For example, `dc=com`. **Identity Manager system user** Specify the name for the IBM Security Identity Manager system user. For example, `isimsystem`. **Identity Manager system user password** Specify the password for the IBM Security Identity Manager system user. **User Filter** Filters the registry for the IBM Security Identity Manager user. Specify the LDAP filter that is based on the directory server attributes.

Table 6. Identity external user registry configuration details (continued).

Button	Identity external user registry options
Reconfigure	**External registry type** Select an external registry type from the list: • IBM Security Directory Server • Microsoft Active Directory • Sun Java System Directory Server **Host name** Specify the name of the server that hosts the directory server. The acceptable formats for the host name are FQDN, IPv4, and IPv6. For example, `isimldap.example.com`. **Port** Specify the directory service port. For example, `389`. You can select or clear the **SSL** check box to manage the secure connection. **Principal DN** Specify the principal distinguished name. For example, `cn=root`. **Password** Specify the password for the principal distinguished name. **External registry DN location** Specify the location of the external registry DN. For example, `dc=com`. **Identity Manager system user** Specify the name for the IBM Security Identity Manager system user. For example, `isimsystem`. **Identity Manager system user password** Specify the password for the IBM Security Identity Manager system user. **User Filter** Filters the registry for the IBM Security Identity Manager system user. Specify the LDAP filter that is based on the directory server attributes.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Configure** > **Manage Server Setting** > **Identity External User Registry Configuration**. The Identity External User Registry Configuration page displays the Identity External User Registry Configuration table.
2. Click **Configure**.
3. In the Identity External User Registry Configuration Details window, specify the expected variable values. For more information, see Table 6 on page 42.
4. Click **Save Configuration** to complete this task.

Note: The directory server configuration takes some time. Do not refresh or close the page. Wait for the configuration process to complete.
A message in the **Notifications** widget indicates you to restart the IBM Security Identity Manager Server.

5. From the **Server Control** widget, do these steps.
   a. Select **Security Identity Manager server**.
   b. Click **Restart**.

   See Viewing the Server Control widget.
6. Synchronize the member nodes of the cluster with the primary node. See Synchronizing a member node with a primary node.
7. From the **Server Control** widget, restart the IBM Security Identity Manager Server again on the primary node.
8. Log on to the IBM Security Identity Manager Console from the primary node by using the Identity external user registry user credentials.
9. Optional: To reconfigure an existing external user registry, do these steps:
   a. From the Identity External User Registry Configuration table, select a record. For example, `IBM Security Identity Manager User Registry`.
   b. Click **Reconfigure**.
   c. In the Edit Identity External User Registry Configuration Details window, edit the configuration variables. For more information, see Table 6 on page 42.
   d. Click **Save Configuration** to complete this task.

Collecting information from the external user registry

You must collect configuration settings from the external user registry for use when adding required users and configuring the security domain.

Procedure

1. If you do not already have the user registry installed, complete the installation and configuration.

   The exact steps for installing and configuring are specific to the user registry product. For example, for an LDAP registry, you must create a suffix, a domain, a user template, and a user realm. For an example of an IBM Security Directory Server user registry, see “User registry configuration for external user registry,” on page 123.
2. Collect the information that is required to configure the Application Server security domain.

   For example, for an LDAP user registry:

Table 7. User registry configuration settings needed for Application Server security domain configuration

Setting	Example
LDAP server host IP address	your host IP address
LDAP server port address	your LDAP server port
The bind user name and the password.	cn=root / secret
The base DN of user repository	dc=mycorp
The object class name for the user	InetOrgPerson
The relative naming attribute for the user	uid
The object class names for groups.	groupOfNames and groupOfUniqueNames

Table 7. User registry configuration settings needed for Application Server security domain configuration (continued)

Setting	Example
The attribute names for group membership	member and uniqueMember

Adding required users to the external user registry

You must add required users to the external user registry.

About this task

IBM Security Identity Manager requires the existence of two accounts:

Table 8. Default account names for required users

Account usage	Default account name
Default administrative user	`ITIM Manager`
Default system user	`isimsystem`

You can choose to use a different account name for each of the accounts. You might want to use a different account name if you already have administrative or system user account names in an existing external user registry. You might want to use a different account name for the administrative user if your operating system does not support spaces in account names. For example, if the user registry is on a Linux system, you might want to specify an account name of `itimManager` instead of `ITIM Manager`.

The exact steps for creation of a user depend on the type of user registry. The following steps describe how to use the IBM Security Directory Server administration tool to add the required users. Alternatively, you can create an **`ldapadd`** command, or use LDIF files.

Procedure

1. Log on to the IBM Security Directory Server web administration tool.
2. From the navigation tree, click **Directory Management** > **Add an entry** to open the Select object class tab of the Add an entry page.
3. Select **inetOrgPerson** from the **Structural Object classes** list.
4. Click **Next** to open the Select auxiliary object classes tab.
5. Click **Next** in the Select auxiliary object classes tab to open the Required attributes tab.
6. Provide the values for the following attributes in the Required attributes tab:
   - **Relative DN**
   - **Parent DN**
   - **cn**
   - **sn**

   You can use the default administrative user ID (uid) `ITIM Manager`, the default system user ID (uid) `isimsystem`, or specify a different uid. The following table shows example entries for the required attributes, when you use the default administrative user ID or the default system user ID:

Table 9. Example entries for required naming attributes for the default administrative user and the default system user accounts

Attribute	Example value for the default administrative user	Example value for the default system user
Relative DN	`cn=ITIM Manager`	`cn=isimsystem`
Parent DN	`dc=com`	`dc=com`
cn	`System Administrator`	`isimsystem`
sn	`Administrator`	`isimsystem`

7. Click **Next** to open the Optional attributes tab.
8. Provide the values for the following attributes in the Optional attributes tab:
   - **uid**
   - **userPassword**

   For example, provide the optional attribute values from the following table:

Table 10. Optional attribute values for the default administrative user and the default system user accounts

Attribute	Example value for the default administrative user	Example value for the default system user
uid	`ITIM Manager`	`isimsystem`
userPassword	The default password for the `ITIM Manager` account is `secret`. You can specify your own password.	The default password for the `isimsystem` account is `secret`. You can specify your own password.

9. Click **Finish**.

Installation of IBM Cognos reporting components

Installation of IBM Cognos® reporting components is optional. You need these components only if you use the Cognos based reports. You must complete the installation and data synchronization process before you can access and work with Security Identity Manager Cognos reports.

Note: IBM Cognos reporting does not support Microsoft SQL Server database. Use DB2 database or Oracle database instead.

The following table describes the installation and synchronization process.

Table 11. Installation and data synchronization process

Task	For more information
Install Cognos Business Intelligence.	1. Access http://www.ibm.com/support/knowledgecenter/SSEP7J_10.2.1/com.ibm.swg.ba.cognos.cbi.doc/welcome.html. 2. Search for **Install Cognos BI on one computer**. 3. Additionally, install IBM Cognos fix pack 1.
Install Framework Manager.	1. Access http://www.ibm.com/support/knowledgecenter/SSEP7J_10.2.1/com.ibm.swg.ba.cognos.cbi.doc/welcome.html. 2. Search for **Installing Framework Manager**.

Table 11. Installation and data synchronization process (continued)

Task	For more information
Complete the data synchronization.	Go to Data synchronization **Note:** Run the data synchronization before you generate the reports to obtain the latest report data.

Cognos reporting

Security Identity Manager installs Cognos reports and models. To use these new reports and models, see the Cognos reporting documentation at IBM Cognos Business Intelligence documentation.

You can find the Cognos reports and models that are specific to Security Identity Manager from the **Appliance Dashboard** of the IBM Security Identity Manager virtual appliance console. Do these steps:

1. Log on to the IBM Security Identity Manager virtual appliance console to open the **Appliance Dashboard**.
2. From the top-level menu of the **Appliance Dashboard**, select **Configure** > **Advanced Configuration** > **Custom File Management** to display the Custom File Management page.
3. Click the **All Files** tab.
4. Go to `directories/utilities`.
5. Select `extensions.zip` and click **Download**.
6. Extract the `extensions.zip` file.
7. Go to `/extensions/`*`version_number`*`/Cognos`. For example, *version_number* is `7.0`.

Chapter 3. Installation of the IBM Security Identity Manager virtual appliance

Use the following tasks to install and set up the IBM Security Identity Manager virtual appliance.

VMware support

The IBM Security Identity Manager virtual appliance can be installed on a VMware, Versions ESXi 5.0, 5.1, 5.5, and 6.0.

The IBM Security Identity Manager virtual appliance for VMware is distributed as a pre-installed disk image of the virtual appliance in `.iso` format.

To deploy the `.iso` virtual appliance image to VMware, use the VMWare vSphere console.

Setting up the virtual machine

Set up the virtual machine that you must use to host the IBM Security Identity Manager.

Procedure

1. Download the `isim_*.iso` build.
2. Create a virtual machine on ESXi 5.x with the following configuration.
   a. Select **Custom**.
   b. Provide a name for the virtual machine.
   c. Choose the destination storage for this virtual machine.
   d. Set virtual machine version to 8 or later.
   e. For the IBM Security Identity Manager virtual appliance, the expected guest operating system is Linux with version 2.6.x 64 bit.
   f. Enter the number of virtual sockets and cores per virtual sockets for the virtual machine. For example, enter the value as `2` for the following options to sum up the total number of cores to `4`.
      - **Number of virtual sockets**
      - **Number of cores per virtual socket**
   g. Enter the memory size. See Hardware and software requirements.
   h. Set the number of network connections.

      Important: You must create at least three network interfaces to set up the virtual machine.
   i. Set **VMXNET 3** as the network adapter for better results. You can also use the **E1000** adapter to set up the virtual machine.
   j. Set the SCSI controller type to **LSI Logic Parallel**.
   k. Select the **Create a new virtual disk** option as the type of disk to use.
   l. Enter the disk size for the virtual machine. See Hardware and software requirements.
   m. Accept the default settings in the Advanced Options page.
3. Check summary for the configuration accuracy.

4. Select the **Edit the virtual machine settings before completion** check box to proceed.
5. Click **Add** in the **Hardware** tab of the Virtual Machine Properties window.
6. Choose **CD/DVD drive**.
7. Select the type of media that you want the virtual drive to access. For example, select **Use ISO image**.
8. Browse to the location of the `.iso` file that is uploaded in the data store.
9. Click **Finish** on the Add Hardware window.
10. Select the **Connect at power on** check box on the Virtual Machine Properties window.
11. Click **Finish** on the Virtual Machine Properties window.
12. Click **Power on the virtual machine** to proceed with the IBM Security Identity Manager virtual appliance installation.
13. Optional: To mount or change the IBM Security Identity Manager media for an existing virtual machine, do these steps.
    a. List the options. Right-click on virtual machine that you created, and then select **Edit Settings**.
    b. Click **Add** in the **Hardware** tab of the Virtual Machine Properties window.
    c. Choose **CD/DVD drive 1**.
    d. Browse to the location of the `.iso` file that is uploaded in the data store.
    e. Select the type of media that you want the virtual drive to access. For example, select **Use ISO image**.
    f. Select the **Connect at power on** check box on the Virtual Machine Properties window.
    g. Click **Power on the virtual machine** to proceed with the IBM Security Identity Manager virtual appliance installation.

What to do next

Proceed with the IBM Security Identity Manager virtual appliance installation.

Installing the IBM Security Identity Manager virtual appliance

Install the IBM Security Identity Manager virtual appliance after you set up the virtual machine.

Procedure

1. When you start the virtual machine for the first time, press enter to continue with the IBM Security Identity Manager virtual appliance installation.
2. Select the language that you want to use during the installation. For example, specify 1 for **English**.
3. Enter as `yes` to proceed with the firmware image installation process.
4. When the installation process is complete, do these steps to unmount the installation media.
    a. Right-click on the virtual machine, and then select **Edit Settings**.
    b. On the **Hardware** tab of the Virtual Machine Properties window, select **CD/DVD drive 1**.
    c. Clear these device status option check boxes.
       - **Connected**
       - **Connect at power on**

5. Click **OK** to close the Virtual Machine Properties window.
6. Select **Yes** and click **OK** to confirm the installation media disconnection.
7. Press the Enter key and then press any key to continue with the installation process.

Results

Proceed with setting up the initial virtual appliance. See "Setting up the initial IBM Security Identity Manager virtual appliance."

Setting up the initial IBM Security Identity Manager virtual appliance

For the virtual appliance, the appliance setup wizard runs the first time when you connect to the virtual console of an unconfigured virtual appliance.

Procedure

1. Provide the following user credentials when the system restarts after the IBM Security Identity Manager virtual appliance installation:
   - **Unconfigured login** - `admin`
   - **Password** - `admin`
2. On the IBM Security Identity Manager virtual appliance setup wizard screen, press Enter to continue.
3. Choose one of these options to proceed.
   - Press 1 to choose the language.
   - Press 2 to read the IBM terms.
   - Press 3 to read the non-IBM terms.
   - Press 4 to accept the license terms.

```
Software License Agreement
Currently selected language: English
1: Select language for license display
2: Read IBM terms
3: Read non-IBM terms
4: Proceeed to acceptance

Select option: 4


By choosing 'I agree,' you agree that (1) you have had the opportunity to
review the terms of both the IBM and non-IBM licenses presented above and (2)
such terms govern this transaction. If you do not agree, choose 'I do not
agree'.
1: I agree
2: I do not agree

Select option: 1
```

4. Select whether or not to enable FIPS 140-2 mode.

```
FIPS 140-2 Mode Configuration

You must enable FIPS mode in order to comply with FIPS 140-2 and NIST 800131a.

If you select to enable FIPS mode, appliance will be rebooted immediately to
perform FIPS power-up integrity checks.
Do not choose to enable FIPS mode without reading the FIPS section in the user
guide.

If you choose to enable FIPS mode now, you cannot disable it later without
reinstalling the appliance.

FIPS 140-2 Mode is not enabled.
1: Enable FIPS 140-2 Mode
x: Exit
p: Previous screen
n: Next screen

Select option: 1


FIPS 140-2 Configuration
Enable FIPS 140-2 mode?
1: yes
2: no
Enter index:
```

If you enter 2, the wizard proceeds to step 5. If you enter 1, the wizard asks for your confirmation.

```
You have selected to enable FIPS mode. The appliance will now reboot to perform
the FIPS integrity checks.
When appliance comes back up, you will need to login as admin user to complete
the setup.
Enter 'YES' to confirm:
```

After you enter YES to confirm, FIPS is enabled in the background and the system reboots.

After you log in, you are again prompted to accept the Software License Agreement (step 3). The wizard then proceeds to step 5.

5. Change the virtual appliance password. After you change the virtual appliance password, continue to the next screen. Set a strong password. It must be at least 8 characters and contain one upper and one lowercase character, one numerical character, and one special character. The special character cannot be < (less than), > (greater than), ` (back tick), & (ampersand), ; (semi-colon), $(dollar), or | (bar).

   Note: If 10 consecutive unsuccessful login attempts occur in an hour, the account is locked for an hour automatically.

```
Appliance Password
Password changes are applied immediately.
Password has not been modified.
1: Change password
x: Exit
p: Previous screen


Change Password
Enter old password:
Enter new password:
Confirm new password:
Password changed successfully.


Appliance Password
Password changes are applied immediately.
Password has been modified.
1: Change password
x: Exit
p: Previous screen
n: Next screen

Select option: n
```

6. Generate the IBM Security Identity Manager keystore. After you create the IBM Security Identity Manager keystore, continue to the next screen.

```
ISIM Keystore
Keystore changes are applied immediately.
Keystore has not been modified.
1: Generate ISIM Keystore
x: Exit
p: Previous screen


Select option: 1

Generate ISIM Keystore
Enter keystore password:
Confirm keystore password:
Keystore successfully generated.


ISIM Keystore
Keystore changes are applied immediately.
Keystore has not been modified.
1: Generate ISIM Keystore
x: Exit
p: Previous screen
n: Next screen

Select option: n
```

7. Change the host name. Use a registered host name or static IP address to manage the virtual appliance for networking and recording important information for configuring the virtual appliance network.

```
Change the Host Name
Enter the new host name: isimva.us.example.com

Host Name Configuration
Host name: isimva.us.example.com
1: Change the host name
x: Exit
p: Previous screen
n: Next screen

Select option: n
```

Note: The host name is cited in the SSL certificate for the virtual appliance.

8. Configure network interface M1 with the IP address, subnet mask, and default gateway.

```
Management Interface Settings
1: Display device settings
2: Display policy
3: Configure M.1
4: Configure M.2
x: Exit
p: Previous screen
n: Next screen

Select option: 3

Configure M.1
Select an IPv4 configuration mode:
1: Automatic
2: Manual
Enter index: 2
Enter the IPv4 address: 192.0.2.21
Enter the IPv4 subnet mask: 255.255.254.0
Enter the IPv4 default gateway: 192.0.2.12
Select an IPv6 configuration mode:
1: Automatic
2: Manual
Enter index: 1
```

9. Configure the DNS for the virtual appliance. Use only a DNS registered IP address to manage the virtual appliance for configuring the virtual appliance network.

```
DNS Configuration
No DNS servers configured.
1: Set DNS server 1
2: Set DNS server 2
3: Set DNS server 3
x: Exit
p: Previous screen
n: Next screen

Select option: 1

Set DNS Server 1
Enter the DNS Server IP address: 198.51.100.0


DNS Configuration
DNS server 1: 198.51.100.0
1: Set DNS server 1
2: Set DNS server 2
3: Set DNS server 3
x: Exit
p: Previous screen
n: Next screen

Select option: n
```

10. Configure the time settings for the virtual appliance.

    Note: To use this virtual appliance as a member node in the cluster, use the same date and time settings that you used to set up the virtual appliance for the primary node.

```
Time Configuration
Time configuration changes are applied immediately.
Time: 08:28:58
Date: 09/09/2013
Time Zone: Asia/Kolkata
1: Change the time
2: Change the date
3: Change the time zone
x: Exit
p: Previous screen
n: Next screen

Select option: n
Command cancelled
1: Change the time
2: Change the date
3: Change the time zone
x: Exit
p: Previous screen
n: Next screen

Select option: n
```

11. Review the summary of configuration details.
12. Press 1 to accept the configuration.

Results

A message indicates that the policy changes are successfully applied and the local management interface is restarted.

What to do next

Log on to the IBM Security Identity Manager virtual appliance console.

XenServer support

The IBM Security Identity Manager virtual appliance can be installed on a XenServer hypervisor, Version 6.5.

When the virtual appliance is installed on XenServer, it runs in paravirtualized (PV) mode rather than hardware assisted virtualization (HVM) mode.

The IBM Security Identity Manager virtual appliance for XenServer is distributed as a pre-installed disk image of the appliance in Virtual Hard Disk (VHD) format. Standard installation ISO images cannot be used due to some restrictions with XenServer.

To deploy the VHD appliance image to XenServer, use the XenCenter console.

Installing the virtual appliance by using XenCenter

Import the VHD image to XenServer with XenCenter to install the virtual appliance.

Before you begin

Make sure that you have the following prerequisites:

- A functional XenServer environment, which is used as the hypervisor to host the VHD image.

- A configured XenCenter installation, which is used to deploy the VHD image.

Procedure

1. In the XenCenter console, expand the XenCenter icon on the left.
2. Right-click the attached hypervisor and select **Import**.
3. In the Import Source window:
   a. Click **Browse**.
   b. Select the VHD image to be imported and click **Open**.
   c. Click **Next**.
4. In the VM Definition window:
   a. Specify the name, number of CPUs, and memory of the virtual machine.

      Note: In most scenarios, assign the virtual machine at least one processor and 2 GB of memory. These settings can be adjusted after the virtual machine starts running.
   b. Click **Next**.
5. In the Location window:
   a. Select the destination hypervisor from the drop-down list on the right.
   b. Click **Next**.
6. In the Storage window:
   a. Select **Place imported virtual disks onto specified target SRs**.
   b. Click **Next**.
7. In the Networking window:
   a. Select the network to be used for the first management interface.
   b. Click **Next**.
8. In the OS Fixup Settings window:
   a. Select **Don't use Operating System Fixup**.
   b. Click **Next**.
9. In the Transfer VM Settings window:
   a. Specify the settings to suit your network environment.

      Note: A valid IP address, subnet, and gateway is required.
   b. Click **Next**.
10. In the Finish window, click **Finish** to start the import.

    Note: The import operation might take a considerable amount of time to complete. You can click the **Logs** tab to check the progress of the import.
11. When the import is complete, run the following commands on the XenServer console to set the image to paravirtualized mode.

```
xe vm-list (to get the uuid for the VM)
xe vm-param-set uuid=<vm uuid> HVM-boot-policy=""
xe vm-param-set uuid=<vm uuid> PV-bootloader=pygrub
xe vm-disk-list (to get the uuid for the disk - VBD entry)
xe vbd-param-set uuid=<disk uuid> bootable=true
```

    For example:

```
[root@xenserver ~]# xe vm-list name-label="autodeploy"
uuid ( RO)           : 6288a6a6-8577-5444-6ed5-46d2a097be54
     name-label ( RW): autodeploy
    power-state ( RO): halted
[root@xenserver ~]# xe vm-param-set uuid=6288a6a6-8577-5444-6ed5-46d2a097be54 HVM-boot-policy=""
[root@xenserver ~]# xe vm-param-set uuid=6288a6a6-8577-5444-6ed5-46d2a097be54 PV-bootloader=pygrub
[root@xenserver ~]# xe vm-disk-list vm="autodeploy"
Disk 0 VBD:
uuid ( RO)             : b0d08251-7f08-8b4e-3913-e71052dd7b13
    vm-name-label ( RO): autodeploy
       userdevice ( RW): xvda

Disk 0 VDI:
uuid ( RO)             : 8dfa6027-1ef3-408b-a9ed-efa751d41720
       name-label ( RW): amapp-template_vdi
    sr-name-label ( RO): Local storage
     virtual-size ( RO): 107376279552

[root@xenserver ~]# xe vbd-param-set uuid=b0d08251-7f08-8b4e-3913-e71052dd7b13 bootable=true
```

12. Start the imported virtual machine.

    Note: At least 3 network interfaces must be configured in order for the virtual appliance to start. Sometimes the XenCenter must be restarted before the new virtual appliance can be started correctly.

Amazon EC2 support

You can deploy IBM Security Identity Manager to the Amazon Elastic Compute Cloud (Amazon EC2) environment.

Amazon EC2 is a web service that provides:

- Scalable computing capacity in the Amazon Web Services (AWS) cloud
- Capability to deploy an Amazon Machine Image (AMI)

Deploying IBM Security Identity Manager to Amazon EC2 involves the following processes:

1. Create an Amazon Machine Image (AMI) from the appliance VHD image.
2. Launch an instance of the AMI in Amazon EC2.

For details about how to use the Amazon EC2 command line interface to launch an instance, see Launching an Instance Using the Amazon EC2 CLI.

Creating an Amazon Machine Image (AMI) from the Virtual Hard Disk (VHD) file

Upload the appliance VHD image to Amazon EC2 and create an AMI so that it can be deployed in Amazon EC2.

About this task

Follow these steps to manually upload an image and create an AMI with the Amazon EC2 console.

Procedure

1. Download and install the Amazon EC2 API Tools. You can download the tool from the Amazon EC2 API Tools page.
2. Run the following commands in the specified sequence to upload the VHD to Amazon EC2 and create an AMI.

Sequence	Command	Description
1	ec2-import-volume	Imports the appliance VHD into Amazon EC2.
2	ec2-describe-conversion-tasks	Monitors the **ec2-import-volume** task to show when the task is complete.
3	ec2-create-snapshot	Creates a snapshot of the imported disk image. This snapshot is required during the AMI registration process.
4	ec2-describe-snapshots	Monitors the status of the snapshot creation to show when the snapshot task is complete.
5	ec2-register	Registers a snapshot as a new AMI. You must use the following parameter values when you register the AMI: **architecture:** x86_64 **kernel:** Use the appropriate parameter value for the kernel ID. **root device name:** /dev/xvda **virtualization type:** paravirtual
6	ec2-delete-disk-image	Removes the uploaded disk image from the storage bucket. The image is no longer required after you finish registering an AMI from the image.

Launching the appliance AMI

Launch an instance of the appliance AMI to run the appliance in Amazon EC2.

About this task

Follow these steps to manually launch an instance of the appliance AMI with the Amazon EC2 console.

Procedure

1. Log in to the Amazon EC2 console.
2. Go to **INSTANCES** > **Instances** > **Launch Instance**.

3. Select the IBM Security Identity Manager AMI that you want to launch.
4. Click **Launch**.
5. In the Choose an Instance Type window, select an instance type and click **Next: Configure Instance Details**.
6. In the Configure Instance Details window, select the options that best fit your environment and click **Next: Add Storage**.
7. In the Add Storage window, validate the storage and click **Next: Tag Instance**.
8. In the Tag Instance window, add any desired tags and then click **Click Next: Configure Security Group**.
9. In the Configure Security Group window, ensure that the selected security group allows inbound SSH and HTTPS access to the appliance. Restrict the access to only those IP addresses from which the appliance is administered. Click **Review and Launch**.
10. Review the details in the Review Instance window and click **Launch**.
11. In the Select an existing key pair or Create a new key pair window, you can opt to **Proceed without a key pair**. Check the acknowledgment check box. Click **Launch Instances** to proceed.

    Note: You do not need to associate a key pair with the instance. If you want to log on to the console of the launched instance, log on as the **admin** user.
12. Click **NETWORK & SECURITY** > **Network Interfaces**.
    a. Click **Create Network Interface**.
    b. On the Create Network Interface window, select a subnet and an appropriate security group. Since IBM Security Identity Manager requires 3 network interface cards, you must create another network interface.

       Note: By default, only one network interface is created with every instance. This interface is the primary interface, which cannot be removed from the instance.
    c. Select a network interface. Right-click the interface and click **Change** > **Source/Dest.Check** > **Disable**. Repeat this step for all the interfaces.
13. Select the appliance instance and complete these steps.
    a. Right-click the appliance instance.
    b. Select **Instance State** > **Stop**.
    c. Right-click the appliance instance.
    d. Select **Networking** > **Attach Network Interface**. Similarly, attach another network interface and start the instance.
14. Go to **INSTANCES** > **Instances** to check the status of the appliance instance.

KVM support

The IBM Security Identity Manager virtual appliance can be installed on Kernel-based Virtual Machine (KVM).

The IBM Security Identity Manager virtual appliance for KVM is distributed as a pre-installed disk image of the virtual appliance in `.iso`.

To deploy the `.iso` virtual appliance image to KVM, use the KVM console.

Hardware requirements

- CPU speed: 3154 MHz.
- Disk space : 500 GB hard disk space.
- RAM : 64 GB system memory.

Software requirements

- RHEL 7.0 64-bit operating system with enabled support for virtualization.
- A network bridge is required to setup network interface for the KVMs.

Installing the virtual appliance with KVM

Install the virtual appliance with KVM.

Procedure

1. Run the `virt-manager` command to open the Virtual Machine Manager.
2. Click **Create a New Virtual Machine**.
3. On the wizard, enter a name for the virtual machine.
4. Select **Local install media (ISO image or CDROM)**.
5. Click **Forward**.
6. Select **Use ISO image** and click **Browse** to select the product ISO file.
7. Select the operating system as Linux with Version Generic 2.6.x kernel.
8. Click **Forward**.
9. Enter the memory size. For example, 1024 GB.
10. Set the number of CPUs. For example, 8.
11. Click **Forward**.
12. Enter the disk size of the virtual machine. For example, 50 GB.
13. Click **Forward**.
14. Select the network bridge.
15. Select **Customize configuration before install**.
16. Click **Finish**.
17. Click **Add Hardware**.
18. Select **Network**.
19. Select the network bridge and click **Finish**.
20. Click **Add Hardware** again.
21. Select **Network**.
22. Select the network bridge and click **Finish**.
23. On the KVM console, follow the steps to complete the installation.
24. Press Enter key after the disk partitioning and installation is complete. Wait for the appliance login prompt to be displayed.
25. Provide the following user credentials when the system restarts after the virtual appliance installation.
    - **Unconfigured login**: `admin`
    - **Password**: `admin`

Results

Proceed with setting up the initial virtual appliance. See "Setting up the initial IBM Security Identity Manager virtual appliance" on page 51.

Chapter 4. Set up the virtual appliance

Use the following tasks to set up the virtual appliance.

Managing the index page

From the index page, you can set up the IBM Security Identity Manager virtual appliance as a single server that contains the deployment manager and cluster member node. You can also set up the IBM Security Identity Manager virtual appliance to add another node to an existing single server. You can also create a backup node from the index page.

Before you begin

Depending on how your system was customized, you might not have authorization to complete this task. To obtain authorization to this task or to have someone complete it for you, contact your system administrator.

Procedure

1. In a web browser, type the host name of the IBM Security Identity Manager virtual appliance in the following format.

   ```
   https://host name of the IBM Security Identity Manager
   ```

   For example: `https://isim1.jk.example.com`
2. Log on to the IBM Security Identity Manager virtual appliance console with the administrator credentials.
   - **Configured login**: `admin`
   - **Password**: `admin`
3. Do one of the following actions to set up the type of node that you want to create.

   Set up a primary node for the IBM Security Identity Manager cluster

   Click **Setup** to set up a primary node for the IBM Security Identity Manager cluster. The Mode Selection page is displayed.

   For more information, see "Configuring the IBM Security Identity Manager by using the initial configuration wizard" on page 62.

   Set up a member node for the IBM Security Identity Manager cluster

   Click **Setup** to set up a member node for the IBM Security Identity Manager cluster. The Connect to Primary page is displayed.

   For more information, see "Setting up an IBM Security Identity Manager member node from the initial configuration wizard" on page 64.

   Set up a backup of the primary node for the IBM Security Identity Manager cluster

   Click **Setup** to set up a backup for the IBM Security Identity Manager cluster. The Connect to Primary page is displayed.

   For more information, see "Backing up a primary node from the initial configuration wizard" on page 65.

Configuring the IBM Security Identity Manager by using the initial configuration wizard

The initial configuration tasks for IBM Security Identity Manager are done in the initial configuration wizard by using the web user interface, and to get the virtual appliance to work.

Before you begin

- "Setting up the initial IBM Security Identity Manager virtual appliance" on page 51.
- Collect the following information that is associated with the tasks you are about to do:
  1. Setup mode selection

     Choose **Guided** or **Advanced**. If **Advanced**, then supply a file with all configuration details in the required format.
  2. Application Interfaces configuration
  3. Mail server configuration
  4. Database server configuration
  5. Directory server configuration

  You can download a sample configuration file from the page.

About this task

During the setup process for configuring the IBM Security Identity Manager, the Setup Progress pane displays these links.

Import Settings
Click this link to import the service settings. See Managing the export and import settings.

View logs
Click this link to check for any messages and errors in the log files. See Managing the log configuration.

Manage snapshots
Click the link to upload or apply a snapshot. See Managing the snapshots.

Procedure

1. In a web browser, type the host name of the configured virtual appliance in the following format.

   ```
   https://host name of the virtual appliance
   ```

   For example, `https://isimva1.jk.example.com`
2. Log on to the IBM Security Identity Manager virtual appliance with the administrator credentials.
   - The **Configured login** is `admin`.
   - The **Password** is `admin`.
3. Choose a configuration mode and then click **Next page**.

Option	Description
Guided Configuration	Define the configuration details a step at a time with the wizard. To continue, go to step 4 on page 63.

Option	Description
Advanced Configuration	Define the configuration by using a `properties` response file that contains the necessary predefined values for the configuration parameters. After you upload the response file, continue to step 8.

4. From the Application Interfaces Configuration page, configure the application interfaces and click **Next page**. For more information about application interfaces, see Managing the application interfaces.

   Note:

   - You can create only one application interface. Use a unique application interface across the cluster.
   - Make sure that you configure the management interface and the application interface in the same subnet.
5. Configure the mail server and click **Next page**. For more information about application interfaces, see Managing the mail server configuration.
6. Configure the database settings for the `Identity data store` and click **Next page**.

   For more information about the database settings, see Identity data store configuration.
7. Configure the directory server and click **Next page**.

   For more information about the directory server settings, see Directory Server configuration details.
8. On the **Completion Setup** page, complete the following tasks that depend on the configuration mode you selected.

   Guided Configuration

   Review the instructions and click **Complete Setup** to complete the configuration process.

   Important: When the configuration process begins, do not refresh the page or close the browser session.

   Advanced Configuration

   Review the instructions and click **Start Configuration** to begin the configuration process.

   Important: When the configuration process is completed successfully, restart the virtual appliance.

   After the configuration completes, a link to restart the virtual appliance is displayed. If the mail server configuration setup is correct, an email notification is sent when the virtual appliance configuration is complete.
9. Click the restart link to restart the IBM Security Identity Manager virtual appliance.

   Note: Check the restart status in the VMware client console.

Setting up an IBM Security Identity Manager member node from the initial configuration wizard

The initial configuration tasks for the IBM Security Identity Manager are done in the initial configuration wizard by using the web user interface to get the virtual appliance started. The initial configuration wizard configures the virtual appliance.

Before you begin

Configure the initial virtual appliance settings.

About this task

In a web browser, log on to the initial configuration wizard from the web user interface after you complete the virtual appliance logon configuration. Complete the virtual appliance setup tasks from either the command line or the IBM Security Identity Manager virtual appliance management user interface.

Use the **Set up a member node for the IBM Security Identity Manager cluster** option to set up a member node.

Note: You can set up only one member node at a time. Do not set up another member node when one member node setup is in progress.

Procedure

1. In the **Connect to Primary** tab of the Setup Progress page, provide the details of the primary node.
   a. Type the host name in the **Primary node host name** field. This host name must be the fully qualified domain name. For example, `isimva1.jk.example.com`.

      The primary node host name must be same that was used to create the primary virtual appliance host name.
   b. Type the user ID in the **Primary node administrator** field. The user ID must be the same ID that you used to log on to the IBM Security Identity Manager virtual appliance For example, `admin`.
   c. Type the password in the **Primary node administrator password** field. For example, `admin`.
2. Click **Test Connection** to validate the details and to verify this connection of the member node with the primary node.

   The View SSL certificate window is displayed.
3. From the View SSL certificate window, click **Yes** to confirm.

   The system notifies that the connection to the primary node was successful.
4. Click **Next page**. The **Application Interfaces Configuration** tab is displayed.

   Note: The **Next page** button is activated only when the connection to the primary node is successful.
5. From the Application Interfaces Configuration page, configure the application interfaces. For more information about application interfaces, see Managing the application interfaces.

   Note:

- You can create only one application interface. Use a unique application interface across the cluster.
- Make sure that you configure the management interface and the application interface in the same subnet.

6. Click **Next page**.

   The **Completion** tab is displayed.
7. Click **Fetch Configuration** to obtain configuration details from the primary node. A progress bar indicates about fetching the configuration details from the primary node. The **Start Configuration** button is activated only when the **Fetch Configuration** operation is completed successfully.
8. Optional: To review or edit the data in the **Connect to Primary** tab, click **Previous page**.
9. Click **Start Configuration** to start the initial configuration for the IBM Security Identity Manager virtual appliance. The Completion page displays the data synchronization process. Do one of these actions:
   - If the configuration is successful, a message indicates to restart the IBM Security Identity Manager virtual appliance. See Restarting or shutting down.
   - If the configuration is not complete or not successful, a message indicates the reason. Do one of the following actions:
     - Click **View logs** link to open the Log Retrieval and Configuration page and check for any messages and errors in the log files.
     - Click the **Click here** link to restart the configuration process in case of failures.

Configure the NTP server for the virtual appliance installation

The Network Time Protocol (NTP) is a protocol that is designed to accurately synchronize local time clocks with networked time servers. You can configure an NTP server to ensure that your virtual appliance is synchronized with the NTP server, which is required for cluster management.

You must have connectivity to at least one server that is running NTP.

See Managing the date and time settings to configure the NTP server for the virtual appliance installation.

Backing up a primary node from the initial configuration wizard

You can back up a primary node by using the web user interface to get the virtual appliance working. You can configure the virtual appliance by doing the initial configuration tasks from the initial configuration wizard.

Before you begin

A primary node must exist in the cluster before you back up a node to recover from any problems with the virtual appliance.

About this task

In a web browser, log on to the initial configuration wizard from the web user interface after you complete the virtual appliance logon configuration. Complete the virtual appliance setup tasks from either the command line or the IBM Security Identity Manager virtual appliance management user interface.

Use the **Set up a backup of the primary node for the IBM Security Identity Manager cluster** option to back up the node.

Procedure

1. In the **Connect to Primary** tab of the Setup Progress page, provide the details of the primary node.
   a. Type the host name in the **Primary node host name** field. For example, `isimva1.jk.example.com`.

      The primary node host name must be same that was used to create the Primary virtual appliance host name.
   b. Type the user ID in the **Primary node administrator** field. The user ID must be the same ID that you used to log on to the IBM Security Identity Manager virtual appliance For example, `admin`.
   c. Type the password in the **Primary node administrator password** field. For example, `admin`.
   d. Optional: Click **Change Schedule** to set the time interval for the backup.

      Note: The default schedule is for one time in a week.

      In the Set Time Interval window, do these steps.
      1) From the **Quick Schedule** list, select one of these options.

         Daily This option sets the schedule for a daily backup of the node.

         Weekly
         This option sets the schedule for a weekly backup of the node.

         Monthly
         This option sets the schedule for a monthly backup of the node.

         Custom
         By default, the **Custom** option sets the schedule daily at 0000 hours. You can also manually set up a schedule to back it up. Do these steps:
         a) From the **Hour of day** option, set the hour. For example, `8`.
         b) From the **Day interval** option, set the interval. For example, `1`.
         c) From the **Days of week** option, select one or more days in the week. For example, `Mon`. If you select one or more days in a week, an extra backup is taken on those specified days.

         Click **Save Configuration**.
2. Click **Complete**.

Results

The primary node details are verified. An initial snapshot is created and downloaded from the primary node after the verification is successful. The next set of snapshots are created automatically according to the specified time interval.

The system notifies that the backup of the primary node is complete. You are then redirected to the Snapshots page.

What to do next

Manage the snapshots. See Managing the snapshots.

Logging on to the consoles from the Appliance Dashboard

You can log on to the different IBM Security Identity Manager consoles from the **Appliance Dashboard**.

Procedure

1. Log on to the **Appliance Dashboard**. For more information, see Logging on to the IBM Security Identity Manager virtual appliance console.
2. In the **Quick Links** widget of the **Appliance Dashboard**, click a console link to open the application. The administrative console links that you can view are as follows:
   - Identity Administration Console
   - Identity Service Center

   For example, click **Identity Administration Console** to open and log on to IBM Security Identity Manager Console.

   Note: The default user ID is `itim manager` and password is `secret`. Change the password before you start any operations.

Chapter 5. Upgrade the virtual appliance

Use the following tasks to upgrade the virtual appliance.

Upgrading the IBM Security Identity Manager virtual appliance from a USB device

Install the firmware update to upgrade the IBM Security Identity Manager virtual appliance.

Before you begin

- Before you apply the firmware update to upgrade the IBM Security Identity Manager virtual appliance, back up your data tier, which is all the databases and the directory server.
- Ensure that the USB storage device is formatted in FAT32.

About this task

The IBM Security Identity Manager virtual appliance has two partitions with separate firmware on each partition. The partitions are swapped during the firmware updates to roll back the firmware updates when required. Either of the partitions can be active on the IBM Security Identity Manager virtual appliance.

In the factory-installed state, Partition 1 is active and contains the firmware version of the current released product. When you apply a firmware update, the update is installed on Partition 2 and your policies and settings are copied from Partition 1 to Partition 2.

The IBM Security Identity Manager virtual appliance restarts the system by using Partition 2, which is now the active partition.

The IBM Security Identity Manager virtual appliance version upgrade can be installed only by using the command-line interface (CLI).

Procedure

1. Download the `isim_*.zip` package from the IBM Fix Central.
2. Extract the `isim_*.pkg` build to a location of your choice.
3. Access the command-line interface (CLI) of the virtual appliance with either an `ssh` session or the console.
4. Copy the `isim_*.pkg` to a USB device.
5. Attach the USB device to your virtual system.
6. In the virtual appliance CLI, run the **`isim`** command to display the `isim` prompt.
7. Choose from either of the following steps depending upon the version.
   - For upgrade from IBM® Security Identity Manager virtual appliance 7.0.1 or later, complete these steps.
     a. At the `isim` prompt, run the **`upgrade`** command.
     b. Run the **`list`** command to list the firmware updates.

   c. Run the **`transfer`** command to transfer the firmware updates to the virtual system.

      Note: To install a firmware upgrade, you must first transfer it to the virtual system.
   d. Run the **`install`** command.
- For upgrade from earlier versions of IBM® Security Identity Manager virtual appliance 7.0.1, complete these steps.
   a. At the `isim` prompt, run the **`firmware_update`** command.
   b. Run the **`list`** command to list the firmware updates.
   c. Run the **`transfer_firmware`** command to transfer the firmware updates to the virtual system.

      Note: To install a firmware upgrade, you must first transfer it to the virtual system.
   d. Run the **`install_firmarwe`** command.

8. Select the index of the firmware update that you want to install to the virtual system and press Enter.

   The results are as follows:
   a. The upgrade process formats Partition 2 and installs the new firmware update on it.
   b. When you apply the firmware update, your policies and settings are copied from Partition 1 to Partition 2.
   c. On completion, the process indicates you to restart the virtual system.
9. Type the **`reboot`** command and press Enter to restart the virtual system. Partition 2 is now the active partition.

   The results are as follows:
   a. After the virtual appliance restarts from the Partition 2, all the configuration that were part of Partition 1, is applied to the Partition 2.
   b. After the configuration is applied to the virtual appliance, the process indicates you to restart the virtual appliance.
10. For the Identity data store, clear the **Service Integration Bus** before you restart the IBM Security Identity Manager. See Clear the service integration bus.
11. Restart the IBM Security Identity Manager.
12. Configure the application interface only after you upgrade the primary node and all member nodes. You must configure application interface on the primary node first and then on the member nodes. For more information, see Managing the application interfaces.
13. Optional: Back up Partition 2 in to Partition 1 after the successful completion of the firmware upgrade. The backup process overwrites the information that is in Partition 1.

    Do the following actions:
    a. Check and fix any errors if the upgrade process failed.
    b. Use Partition 1 to set it as the active partition and restart it.

    Partition 1 now becomes the active partition.

Upgrading the IBM Security Identity Manager virtual appliance with firmware update transfer utility

The IBM Security Identity Manager virtual appliance allows only firmware updates by USB device. Starting at firmware release 7.0.0.2 (7.0.0-ISS-SIM-FP0002), firmware (`.pkg`) files can be transferred with the attached Java utility. A USB device is no longer required to update the virtual appliance.

Before you begin

You must install the firmware release 7.0.0.2 (7.0.0-ISS-SIM-FP0002) or later before you can install the firmware release 7.0.0.3 or later with this utility.

About this task

This utility performs the same function as the command-line interface (CLI) command of the virtual appliance.

Procedure

1. Download the `isim_*.zip` package from the IBM Fix Central.
2. Extract the `isim_*.pkg` build to a location of your choice.
3. Copy the utility to a system where Java, Version 1.7 is installed.
4. Copy these files to the file system.
   - The `.pkg` firmware update file.
   - The keystore (`jks`) file.
5. Run the following Java command to upload the `.pkg` file.

   Usage:

   ```
   java -jar FileUpload.jar <Hostname> <AdminId> <AdminPassword> <Truststore_Filepath>
   <Truststore_Password> <Absolute path to pkg file> <sslProtocol>
   ```

   Example:

   ```
   java -jar FileUpload.jar isimva.us.ibm.com admin admin /work/temptrust.jks WebAS
         /Downloads/virtual_appliance.pkg TLSv1.2
   ```

6. Use the supplied `temptrust.jks` file if you did not update the default certificates.

   If you previously updated the default certificate on the virtual appliance, `temptrust.jks` does not work. Use an updated `jks` file that is based on your updated certificate.
7. Access the command-line interface (CLI) of the virtual appliance to install the firmware with the following command.

   Note: Run this command after you transfer the `.pkg` file.
   - For upgrade from IBM® Security Identity Manager virtual appliance 7.0.1 or later, run this command:

     `isim > upgrade > install`
   - For upgrade from earlier versions of IBM® Security Identity Manager virtual appliance 7.0.1, run this command:

     `isim > firware_update > install_firmware`
8. Select the index of the firmware update that you want to install to the virtual system and press Enter.

   The results are as follows:

   a. The upgrade process formats Partition 2 and installs the new firmware update on it.

   b. When you apply the firmware update, your policies and settings are copied from Partition 1 to Partition 2.

   c. On completion, the process indicates you to restart the virtual system.

9. Type the **`reboot`** command and press Enter to restart the virtual system. Partition 2 is now the active partition.

   The results are as follows:

   a. After the virtual appliance restarts from the Partition 2, all the configuration that were part of Partition 1, is applied to the Partition 2.

   b. After the configuration is applied to the virtual appliance, the process indicates you to restart the virtual appliance.

10. For the Identity data store, clear the **Service Integration Bus** before you restart the IBM Security Identity Manager. See Clear the service integration bus.

11. Restart the IBM Security Identity Manager.

12. Configure the application interface only after you upgrade the primary node and all member nodes. You must configure application interface on the primary node first and then on the member nodes. For more information, see Managing the application interfaces.

13. Optional: Back up Partition 2 in to Partition 1 after the successful completion of the firmware upgrade. The backup process overwrites the information that is in Partition 1.

    Do the following actions:

    a. Check and fix any errors if the upgrade process failed.

    b. Use Partition 1 to set it as the active partition and restart it.

    Partition 1 now becomes the active partition.

Chapter 6. Migration from IBM Tivoli Identity Manager 5.1 to IBM Security Identity Manager 7.0.1.10

Migrating from IBM Tivoli® Identity Manager Version 5.1 to IBM Security Identity Manager Version 7.0.1.10 is similar to a separate server migration.

Important: Before you begin migration, read the migration assessment survey at http://www.ibm.com/support/docview.wss?uid=swg21982329

Note: `PBEWithMD5AndDES` encryption is not a FIPS certified cipher. Starting from IBM Tivoli Identity Manager Version 5.0 and later, AES is the default encryption algorithm. The `PBEWithMD5AndDES` encryption algorithm is not supported for IBM Security Identity Manager 7. Ensure to migrate the data to use the new encryption algorithm, for example `AES`. IBM Tivoli Identity Manager provides a tool to change the cipher and migrate the data to use the new encryption algorithm. For more information, see “Running the cipher migration tool” in the *IBM Tivoli Identity Manager 5.1 Installation and Configuration Guide*.

Purpose

The purpose of this document is to help you get started with migration from a software stack installation to virtual appliance. That is, you can migrate from IBM Tivoli Identity Manager Version 5.1 to IBM Security Identity Manager Version 7.0.1.10.

Scope

The scope of this document is to provide data tier migration installation from within the virtual appliance. For data tier information, see the "Hardware and software requirements" in the IBM Knowledge Center **IBM Security Identity Manager 7.0.1.10** > **Product overview** > **Hardware and software requirements**.

Intended audience

Existing IBM Tivoli Identity Manager customers who want to migrate from Version 5.1 to IBM Security Identity Manager Version 7.0.1.10 can use this document for migration.

Separate system upgrade and data migration

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 7.0.1.10.

These tasks require the installation of middleware and the upgrade and installation of IBM Security Identity Manager Version 7.0.1.10. The topics include best practices for the upgrade and migration from production environments.

Supported upgrade paths

Note: These upgrade paths do not support the migration of Tivoli Identity Manager Version 5.1 that run with either an MS SQL database or a Sun One Oracle directory server.

Table 12. Upgrade paths to IBM Security Identity Manager Version 7.0.1.10

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 7.0.1.10

IBM Security Identity Manager supports data migration for both UNIX systems and Windows systems.IBM Security Identity Manager Version 7.0.1.3 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

Migration is the process of collecting configuration data and applications from an earlier installed version of IBM Tivoli Identity Manager Version 5.1 and merging them into IBM Security Identity Manager Version 7.0.1.10. This process is to ensure that the new environment is identical to the earlier environment.

At a high level the migration to the virtual appliance involves the following steps.

- Set up a supported version of the database and an IBM Directory server, then copy over the IBM Tivoli Identity data.
- Set up a virtual appliance primary node and begin migration with a response file.
- Copy over the 5.1 keystore and create property and workflow definitions in the appliance.

Planning for migration

Some migration scenarios might offer a higher availability percentage over another. In some situations, you might want to perform the migration in parallel while your source environment remains in production. In other situations, you might require the production system to be disconnected just before you go live with the newly migrated system. Depending on your needs on high availability systems, you might choose one approach or another.

Migration to Version 7.0.1.10

The major steps to migrate IBM Tivoli Identity Manager and related prerequisite middleware servers are as follows

- In the IBM Tivoli Identity Manager Version 5.1 server environment, perform the following steps.
  1. Stop WebSphere Application Server and any connections to the IBM 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 IBM Tivoli Identity Manager Version 5.1 server environment back into production. You can load production data into the new IBM Security Identity Manager Version 7.0.1.10 system later. You can migrate data to a test environment before a production cutover to the new system. Any changes that you make to IBM Security Identity Manager data on the new system are overwritten when you reimport the IBM Tivoli Identity Manager Version 5.1 production data during the final cutover.
- In the IBM Security Identity Manager Version 7.0.1.10 server environment, you must perform the following actions.
  1. Install the required middleware (at the required release and fix pack level).
  2. Optionally run the middleware configuration utility for DB2 Universal Database and IBM Tivoli Directory Server.

Data, databases, and directory server are migrated by using the configuration wizard for Version 7.0.1.10. The data migration can be done either for a single-server environment or a cluster environment that consists of multiple computers. You can migrate to IBM Security Identity Manager Version 7.0.1.10 from IBM Tivoli Identity Manager Version 5.1.

Database migration

IBM Security Identity Manager Version 7.0.1.10 supports data migration from most databases supported on IBM Tivoli Identity Manager Version 5.1.

For database requirements, see Hardware and software requirements.

DB2 Universal Database migration

Use these scenarios to migrate DB2 Universal Database data to a version that Security Identity Manager Version 7.0.1.3 supports.

The scenario that you choose depends on endian format that is used by your operating systems.

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 that are provided with this utility to move data from a 5.1 system to a Version 7.0.1.10 system before the upgrade.

About this task

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:

Table 13. Export command values

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.

Each command creates these files:

Table 14. Export command output files

File name	Description
`EXPORT.out`	The summarized result of the EXPORT action.

Table 14. Export command output files (continued)

File name	Description
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*nnnc*.*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.

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
     ```

   The output files are created in the *DB2 installation directory*/bin directory.
10. Move these files into a separate folder, such as /child3_export.
11. 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.

What to do next

Create the database and copy the exported data to it.

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 7.0 system it the target system.

Table 15. Command values

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.

Procedure

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

   See "Database installation and configuration" on page 5. 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. Run the middleware configuration tool to create the DB2 instance.

   See "Running the middleware configuration utility" on page 9. When you run the middleware configuration tool to configure DB2 Universal Database, the database user field is set to `itimuser` as a default value. Modify the database user field to the same database user that is used in your previous Tivoli Identity Manager database. 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.
3. Copy the DDL and SQL files from the `/DDL_Files` directory that you created in the "Exporting DB2 Universal Database data" on page 76 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.dll
   ```
9. Disconnect from the database. Run the command:

   ```
   db2 disconnect all
   ```

What to do next

Import the data to the new version of the DB2 Universal Database.

Importing the data to the 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” on page 76. 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:

Table 16. Import command values

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.

Each command creates these files:

Table 17. Import command output files

File name	Description
`IMPORT.out`	The summarized result of the IMPORT action.
`tab`*`nnn`*`.msg`	The import messages file of the corresponding table.

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
   ```
   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 /child3_import.
   c. 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.

What to do next

You can now use this database for Security Identity Manager migration. See Chapter 7, "Upgrade to IBM Security Identity Manager Version 7.0.1.10," on page 107

DB2 Universal Database migration to a system that has the same endian format as the source system:

Use these tasks to migrate DB2 Universal Database data to a version that Security Identity Manager Version 7.0.1.3 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 Version 7.0.1.10 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.

What to do next

Install the new version of DB2 Universal Database.

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 *Installing and configuring the IBM(r) DB2(r) database* in the *IBM Security Identity Manager Installation Guide* on the Security Identity Manager product documentation site. Because this operation is a migration, ensure that you create the same 5.1 database system user, for example, `enrole`. The user must have the same rights and privileges it had on the old system.
2. Run the middleware configuration tool to create the DB2 instance.

   See "Running the middleware configuration utility" on page 9. When you run the middleware configuration tool to configure DB2 Universal Database, the database user field is set to `itimuser` as a default value. Modify the database user field to the same database user that is used in your previous Tivoli Identity Manager database. 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.
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.

What to do next

Restore data to the new version of DB2 Universal Database.

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 Version 7.0.1.10 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 Version 7.0.1.10 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`.

What to do next

After you complete the upgrade and apply the Version 7.0.13 schema changes, tune the database for optimal performance by applying the latest tuning settings. See the Tuning IBM DB2 section of the Security Identity Manager Performance Tuning Guide for details.

For information about backing up and restoring the DB2 Universal Database, see the DB2 section of the IBM Knowledge Center.

Creating the ITIMSxxx schema:

You must perform this task if you are migrating from a setup where IBM Tivoli Identity Manager 5.1 was running on a WebSphere Application Server stand-alone server.

Before you begin

Download the Data Definition Language file (DDL).

```
DB2 - MDW_CONFIGTOOL_ROOT/MWC/migration/db2/isim_sib_template.ddl
```

Where

MDW_CONFIGTOOL_ROOT
Is the directory where you extracted the IBM Security Identity Manager Middleware Configuration Tool compressed file.

About this task

An IBM Tivoli Identity Manager 5.1 setup that was not a cluster environment does not have the ITIMSxxx schema. It is not copied over to the new DB2 database and the virtual appliance does not create it. You must run this script file to create the mandatory SIB schema for the message server messaging engine.

Procedure

1. Open a DB2 command window.

   Windows systems

   a. Click **Start** > **Run**
   b. Enter `db2`.

   UNIX or Linux systems

   a. Log on as the DB2 instance owner.
   b. Enter `db2`.
2. Connect to the database as the DB2 instance owner.

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

   Where

   itimdb Is the IBM Security Identity Manager name.

   instance_owner
   Is the owner of the DB2 instance.

   instance_owner_password
   Is the password of the DB2 instance owner.
3. Run the `isim_sib_template.ddl` file.

   ```
   db2 -tvf path\isim_sib_template.ddl
   ```

   Where

   path Is the path of the file.

   Update the file by replacing `ITIML000` with `ITIMS000`. You must also replace `itimuserTag` with your IBM Security Identity Manager database user name.

Clearing the service integration bus:

When you upgrade from Tivoli Identity Manager 5.1 running on WebSphere Application Server 6.1 to Security Identity Manager Version 7.0.1.10, 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 18. 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 7.0.1.3 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 full=y file=\itim51.dmp log=\itim51exp.log
       owner=('itimuser','ITIML000','ITIML001','ITIMS000')
   ```

   Note: Specify all owners for all the member nodes that are present in the cluster.
   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.

What to do next

Install the new version of Oracle database.

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 server, install the supported version of Oracle database for Security Identity Manager Version 7.0.1.10. See “Installation and configuration of the Oracle database” on page 17 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 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;

 CREATE TABLESPACE ITIML000_data
DATAFILE 'ITIML000.dbf'
SIZE 50M
AUTOEXTEND ON
NEXT 10M
MAXSIZE unlimited
DEFAULT STORAGE (INITIAL 10M
NEXT 1M
PCTINCREASE 10)
PERMANENT
ONLINE
```

```
LOGGING;
CREATE USER ITIML000 IDENTIFIED BY <userPwd>
DEFAULT TABLESPACE ITIML000_data
QUOTA UNLIMITED ON ITIML000_data;

CREATE TABLESPACE ITIMS000_data
DATAFILE 'ITIMS000.dbf'
SIZE 50M
AUTOEXTEND ON
NEXT 10M
MAXSIZE unlimited
DEFAULT STORAGE (INITIAL 10M
NEXT 1M PCTINCREASE 10)
PERMANENT
ONLINE
LOGGING;

CREATE USER ITIMS000 IDENTIFIED BY <userPwd>
DEFAULT TABLESPACE ITIMS000_data
QuOTA UNLIMITED ON ITIMS000_data;

CREATE TABLESPACE ITIML001_data
DATAFILE 'ITIML001.dbf' SIZE
50M AUTOEXTEND ON
NEXT 10M
MAXSIZE unlimited
DEFAULT STORAGE (INITIAL10M
NEXT 1M
PCTINCREASE 10)
PERMANENT
ONLINE
LOGGING;

CREATE USER ITIML001 IDENTIFIED BY <userPwd>
DEFAULT TABLESPACE ITIML001_data
QuOTA UNLIMITED ON ITIML001_data;

CREATE TABLE ITIML000.SIBOWNER (
ME_UUID VARCHAR(16),
INC_UUID VARCHAR(16),
VERSION INTEGER,
MIGRATION_VERSION INTEGER
)TABLESPACE ITIML000_data;
CREATE TABLE ITIML000.SIBOWNERO (
EMPTY_COLUMN INTEGER
)TABLESPACE ITIML000_data;
CREATE TABLE ITIML000.SIBCLASSMAP (
CLASSID INTEGER NOT NULL,
URI VARCHAR2(2048) NOT NULL,
PRIMARY KEY(CLASSID)
)TABLESPACE ITIML000_data;
CREATE TABLE ITIML000.SIBLISTING (
ID INTEGER NOT NULL,
SCHEMA_NAME VARCHAR2(10),
TABLE_NAME VARCHAR2(10) NOT NULL,
TABLE_TYPE CHAR(1) NOT NULL,
PRIMARY KEY(ID)
)TABLESPACE ITIML000_data;
CREATE TABLE ITIML000.SIB000(
ID NUMBER(19) NOT NULL,
STREAM_ID NUMBER(19) NOT NULL,
TYPE CHAR(2),
EXPIRY_TIME NUMBER(19),
STRATEGY INTEGER,
REFERENCE NUMBER(19),
CLASS_ID INTEGER NOT NULL,
PRIORITY INTEGER,
SEQUENCE NUMBER(19),
PERMANENT_ID INTEGER,
TEMPORARY_ID INTEGER,
LOCK_ID NUMBER(19),
DATA_SIZE INTEGER NOT NULL,
LONG_DATA BLOB,
XID VARCHAR(254),
DELETED SMALLINT,
PRIMARY KEY(ID)
) LOB(LONG_DATA) STORE AS (CACHE STORAGE(INITIAL 10M NEXT 10M))
TABLESPACE ITIML000_data;
CREATE INDEX ITIML000.SIB000STREAMIX ON
ITIML000.SIB000(STREAM_ID,SEQUENCE);
CREATE TABLE ITIML000.SIB001 (
ID NUMBER(19) NOT NULL,
STREAM_ID NUMBER(19) NOT NULL,
TYPE CHAR(2),
EXPIRY_TIME NUMBER(19),
STRATEGY INTEGER,
REFERENCE NUMBER(19),
CLASS_ID INTEGER NOT NULL,
PRIORITY INTEGER,
SEQUENCE NUMBER(19),
PERMANENT_ID INTEGER,
TEMPORARY_ID INTEGER,
LOCK_ID NUMBER(19),
DATA_SIZE INTEGER NOT NULL,
LONG_DATA BLOB,
XID VARCHAR(254),
DELETED SMALLINT,
PRIMARY KEY(ID)
) LOB(LONG_DATA) STORE AS (CACHE STORAGE(INITIAL 10M NEXT 10M))
TABLESPACE ITIML000_data;
CREATE INDEX ITIML000.SIB001STREAMIX ON
ITIML000.SIB001(STREAM_ID,SEQUENCE);
CREATE TABLE ITIML000.SIB002 (
ID NUMBER(19) NOT NULL,
STREAM_ID NUMBER(19) NOT NULL,
TYPE CHAR(2),
EXPIRY_TIME NUMBER(19),
STRATEGY INTEGER,
REFERENCE NUMBER(19),
CLASS_ID INTEGER NOT NULL,
PRIORITY INTEGER,
SEQUENCE NUMBER(19),
PERMANENT_ID INTEGER,
TEMPORARY_ID INTEGER,
LOCK_ID NUMBER(19),
DATA_SIZE INTEGER NOT NULL,
LONG_DATA BLOB,
XID VARCHAR(254),
DELETED SMALLINT,
PRIMARY KEY(ID)
) LOB(LONG_DATA) STORE AS (CACHE STORAGE(INITIAL 10M NEXT 10M))
TABLESPACE ITIML000_data;
CREATE INDEX ITIML000.SIB002STREAMIX ON
ITIML000.SIB002(STREAM_ID,SEQUENCE);
CREATE TABLE ITIML000.SIBXACTS (
XID VARCHAR2(254) NOT NULL,
STATE CHAR(1) NOT NULL,
PRIMARY KEY(XID)
)TABLESPACE ITIML000_data;
CREATE TABLE ITIML000.SIBKEYS (
ID VARCHAR2(50) NOT NULL,
LAST_KEY NUMBER(19) NOT NULL,
PRIMARY KEY(ID)
)TABLESPACE ITIML000_data;
```

```
CREATE TABLE ITIMS000.SIBOWNER (
ME_UUID VARCHAR(16),
INC_UUID VARCHAR(16),
VERSION INTEGER,
MIGRATION_VERSION INTEGER
)TABLESPACE ITIMS000_data;
CREATE TABLE ITIMS000.SIBOWNERO (
EMPTY_COLUMN INTEGER
)TABLESPACE ITIMS000_data;
CREATE TABLE ITIMS000.SIBCLASSMAP (
CLASSID INTEGER NOT NULL,
URI VARCHAR2(2048) NOT NULL,
PRIMARY KEY(CLASSID)
)TABLESPACE ITIMS000_data;
CREATE TABLE ITIMS000.SIBLISTING (
ID INTEGER NOT NULL,
SCHEMA_NAME VARCHAR2(10),
TABLE_NAME VARCHAR2(10) NOT NULL,
TABLE_TYPE CHAR(1) NOT NULL,
PRIMARY KEY(ID)
)TABLESPACE ITIMS000_data;
CREATE TABLE ITIMS000.SIB000 (
ID NUMBER(19) NOT NULL,
STREAM_ID NUMBER(19) NOT NULL,
TYPE CHAR(2),
EXPIRY_TIME NUMBER(19),
STRATEGY INTEGER,
REFERENCE NUMBER(19),
CLASS_ID INTEGER NOT NULL,
PRIORITY INTEGER, SEQUENCE NUMBER(19),
PERMANENT_ID INTEGER,
TEMPORARY_ID INTEGER,
LOCK_ID NUMBER(19),
DATA_SIZE INTEGER NOT NULL,
LONG_DATA BLOB,
XID VARCHAR(254),
DELETED SMALLINT,
PRIMARY KEY(ID)
) LOB(LONG_DATA) STORE AS (CACHE STORAGE(INITIAL 10M NEXT 10M))
TABLESPACE ITIMS000_data;
CREATE INDEX ITIMS000.SIB000STREAMIX ON
ITIMS000.SIB000(STREAM_ID,SEQUENCE);
CREATE TABLE ITIMS000.SIB001 (
ID NUMBER(19) NOT NULL,
STREAM_ID NUMBER(19) NOT NULL,
TYPE CHAR(2),
EXPIRY_TIME NUMBER(19),
STRATEGY INTEGER,
REFERENCE NUMBER(19),
CLASS_ID INTEGER NOT NULL,
PRIORITY INTEGER,
SEQUENCE NUMBER(19),
PERMANENT_ID INTEGER,
TEMPORARY_ID INTEGER,
LOCK_ID NUMBER(19),
DATA_SIZE INTEGER NOT NULL,
LONG_DATA BLOB,
XID VARCHAR(254),
DELETED SMALLINT,
PRIMARY KEY(ID)
) LOB(LONG_DATA) STORE AS (CACHE STORAGE(INITIAL 10M NEXT 10M))
TABLESPACE ITIMS000_data;
CREATE INDEX ITIMS000.SIB001STREAMIX ON
ITIMS000.SIB001(STREAM_ID,SEQUENCE);
CREATE TABLE ITIMS000.SIB002 (
ID NUMBER(19) NOT NULL,
STREAM_ID NUMBER(19) NOT NULL,
TYPE CHAR(2),
EXPIRY_TIME NUMBER(19),
STRATEGY INTEGER,
REFERENCE NUMBER(19),
CLASS_ID INTEGER NOT NULL,
PRIORITY INTEGER,
SEQUENCE NUMBER(19),
PERMANENT_ID INTEGER,
TEMPORARY_ID INTEGER,
LOCK_ID NUMBER(19),
DATA_SIZE INTEGER NOT NULL,
LONG_DATA BLOB,
XID VARCHAR(254),
DELETED SMALLINT,
PRIMARY KEY(ID)
) LOB(LONG_DATA) STORE AS (CACHE STORAGE(INITIAL 10M NEXT 10M))
TABLESPACE ITIMS000_data;
CREATE INDEX ITIMS000.SIB002STREAMIX ON
ITIMS000.SIB002(STREAM_ID,SEQUENCE);
CREATE TABLE ITIMS000.SIBXACTS (
XID VARCHAR2(254) NOT NULL,
STATE CHAR(1) NOT NULL,
PRIMARY KEY(XID)
)TABLESPACE ITIMS000_data;
CREATE TABLE ITIMS000.SIBKEYS (
ID VARCHAR2(50) NOT NULL,
LAST_KEY NUMBER(19) NOT NULL,
PRIMARY KEY(ID)
)TABLESPACE ITIMS000_data
```

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:

   ```
   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`.
6. Run the following **Post_Migration_Script.sql** script Replace *itimuserTag* with your Tivoli Identity Manager Version 5.1 database user.

   ```
   GRANT SELECT,INSERT,DELETE,UPDATE ON ITIML000.SIBOWNER TO itimuserTag;
   GRANT SELECT,INSERT,DELETE,UPDATE ON ITIML000.SIBOWNERO TO itimuserTag;
   GRANT SELECT,INSERT ON ITIML000.SIBCLASSMAP TO itimuserTag;
   GRANT SELECT,INSERT ON ITIML000.SIBLISTING TO itimuserTag;
   GRANT SELECT,INSERT,DELETE,UPDATE ON ITIML000.SIB000 TO itimuserTag;
   GRANT SELECT,INSERT,DELETE,UPDATE ON ITIML000.SIB001 TO itimuserTag;
   GRANT SELECT,INSERT,DELETE,UPDATE ON ITIML000.SIB002 TO itimuserTag;
   GRANT SELECT,INSERT,UPDATE,DELETE ON ITIML000.SIBXACTS TO itimuserTag;
   GRANT SELECT,INSERT,UPDATE ON ITIML000.SIBKEYS TO itimuserTag;
   GRANT DROP ANY TABLE TO itimuserTag;
   GRANT SELECT,INSERT,DELETE,UPDATE ON ITIML001.SIBOWNER TO itimuserTag;
   ```

```
GRANT SELECT,INSERT,DELETE,UPDATE ON ITIML001.SIBOWNERO TO itimuserTag;
GRANT SELECT,INSERT ON ITIML001.SIBCLASSMAP TO itimuserTag;
GRANT SELECT,INSERT ON ITIML001.SIBLISTING TO itimuserTag;
GRANT SELECT,INSERT,DELETE,UPDATE ON ITIML001.SIB000 TO itimuserTag;
GRANT SELECT,INSERT,DELETE,UPDATE ON ITIML001.SIB001 TO itimuserTag;
GRANT SELECT,INSERT,DELETE,UPDATE ON ITIML001.SIB002 TO itimuserTag;
GRANT SELECT,INSERT,UPDATE,DELETE ON ITIML001.SIBXACTS TO itimuserTag;
GRANT SELECT,INSERT,UPDATE ON ITIML001.SIBKEYS TO itimuserTag;
GRANT DROP ANY TABLE TO itimuserTag;

GRANT SELECT,INSERT,DELETE,UPDATE ON ITIMS000.SIBOWNER TO itimuserTag;
GRANT SELECT,INSERT,DELETE,UPDATE ON ITIMS000.SIBOWNERO TO itimuserTag;
GRANT SELECT,INSERT ON ITIMS000.SIBCLASSMAP TO itimuserTag;
GRANT SELECT,INSERT ON ITIMS000.SIBLISTING TO itimuserTag;
GRANT SELECT,INSERT,DELETE,UPDATE ON ITIMS000.SIB000 TO itimuserTag;
GRANT SELECT,INSERT,DELETE,UPDATE ON ITIMS000.SIB001 TO itimuserTag;
GRANT SELECT,INSERT,DELETE,UPDATE ON ITIMS000.SIB002 TO itimuserTag;
GRANT SELECT,INSERT,UPDATE,DELETE ON ITIMS000.SIBXACTS TO itimuserTag;
GRANT SELECT,INSERT,UPDATE ON ITIMS000.SIBKEYS TO itimuserTag;
GRANT DROP ANY TABLE TO itimuserTag;
```

What to do next

After you complete the upgrade, the installation, and applied the Security Identity Manager Version 7 schema changes, you must tune the database. For optimal performance, apply the latest tuning settings. See “Oracle database performance tuning” on page 21 and the Tuning Oracle section of the Security Identity Manager Performance Tuning Guide for details.

Creating the ITIMSxxx schema:

You must perform this task if you are migrating from a setup where IBM Tivoli Identity Manager 5.1 was running on a WebSphere Application Server stand-alone server.

Before you begin

Download the Data Definition Language file (DDL).

`Oracle -` *`BOM_Root`*`/migration/oracle/isim_sib_template.ddl`

Where

BOM_Root
: Is the directory where you uncompressed the IBM Security Identity Manager package file.

Ensure that these variables are set correctly.

ORACLE_HOME
: Is the Oracle default installation directory.

ORACLE_SID
: Is the IBM Security Identity Manager data base instance.

About this task

An IBM Tivoli Identity Manager 5.1 setup that was not a cluster environment does not have the ITIMSxxx schema. It is not copied over to the new DB2 database and the virtual appliance does not create it. You must run this script file to create the mandatory SIB schema for the message server messaging engine.

Procedure

Run the `isim_sib_template.ddl` with the **`sqlplus`** utility.

```
sqlplus system/system_pwd@path\isim_sib_template.ddl
```

Where

system_pwd
Is the password of the system user.

path Is the path of the file.

Replace *isimuserTag* with your IBM Security Identity Manager database user name.

Clearing the service integration bus:

For Separate Systems Upgrades from Tivoli Identity Manager 5.1 to Security Identity Manager Version 7.0.1.10, 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 7.0.1.10 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 19. Service integration bus schema names

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

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.

What to do next

Migrate the directory server.

Directory server migration

Security Identity Manager Version 7.0.1.10 supports data migration from most directory servers supported on Tivoli Identity Manager Version 5.1.

See Hardware and software requirements *Hardware and software requirements* in the *IBM Security Identity Manager Product Overview Guide* on the Security Identity Manager product documentation site.

Tivoli Directory Server migration

Use these tasks to migrate Tivoli Directory Server data to a version that Security Identity Manager Version 7.0.1.3 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 7.0.1.3 supports.

To migrate your directory server to a version that is supported by Security Identity Manager Version 7.0.1.3, go to http://www.ibm.com/support/knowledgecenter/SSVJJU_6.4.0/com.ibm.IBMDS.doc_6.4/c_ig_UpgradingInstances.html.

- To migrate on the same system, see http://www.ibm.com/support/knowledgecenter/SSVJJU_6.4.0/com.ibm.IBMDS.doc_6.4/t_ig_UpgradeInstanceWith_idsimigr.html
- To migrate on a separate system, see http://www.ibm.com/support/knowledgecenter/SSVJJU_6.4.0/com.ibm.IBMDS.doc_6.4/c_ig_UpgradeInst_Diff_Source_Target.html

Configuration and customization

After you migrate your Version 5.1 data over to Version 7.0.1.10, you must create your 5.1 configurations and customizations in the IBM Security Identity Manager virtual appliance.

You can use either of these methods.

- Modify property values and upload external files by using the virtual appliance interface. See “Customization and configuration with the virtual appliance interface.”
- Changing the property files and uploading external files by using the RESTful APIs.

Customization and configuration with the virtual appliance interface

You can use the virtual appliance interface to download files, externally modify them, and then upload them back into the virtual appliance.

For information about the customizations that are supported in the virtual appliance, go to https://www.ibm.com/developerworks/community/wikis/

home?lang=en#!/wiki/W746177d414b9_4c5f_9095_5b8657ff8e9d/page/Customizing %20Identity%20Manager%20in%20Virtual%20Appliance and download "Extending and Customizing the IBM Security Identity Manager".

Customizable files for the virtual appliance are maintained in folders under the `directories` folder **Configure** > **Advanced Configuration** > **Custom File Management** or under **Configure** > **Advanced Configuration** > **Update Property**.

If you have customized workflow extensions, you can add them manually to the virtual appliance **Configure** > **Advanced Configuration** > **Workflow Extension**.

In the IBM Knowledge Center, see also

- *"Managing custom files"* **IBM Security Identity Manager 7.0.1.3** > **Configuring** > **Virtual appliance configuration** > **Managing custom files**.
- *"User interface customization overview"* in the IBM Knowledge Center **IBM Security Identity Manager 7.0.1.3** > **Configuring** > **User interface customization overview**.
- *"Configuring the workflow extension"* in the IBM Knowledge Center **IBM Security Identity Manager 7.0.1.3** > **Configuring** > **Virtual appliance configuration**.

Customization and configuration with the RESTful APIs

You can use the REST APIs for three types of operations.

Manage system properties

All the Security Identity Manager properties that can be modified in the virtual appliance can be modified by using the appropriate RESTful APIs.

- Use the APIs to fetch a list of all the property files that can be modified.
- Use the Get property value and Update property value APIs to set property values and to automate bulk property changes.
- Use the Add new property and Delete property APIs to manage new properties in Security Identity Manager property files.

Manage custom property files

You can use APIs to upload new property files and manage the properties inside them. These custom property files can be downloaded or deleted.

Manage non-property files

You can use APIs to manage non-property files such as JAR files or XML files. The virtual appliance uses IBM Java 1.7. All JAR files must be compiled by that Java SDK version or an earlier version.

For more information about the RESTful APIs, n the IBM Knowledge Center, see **IBM Security Identity Manager 7.0.1.3** > **Reference** > **REST APIs**.

Post-upgrade production cutover

Use this information to conduct a post-upgrade 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 upgrade does not provide a mechanism to capture these changes and import them to the upgraded system that runs Version 7.0. 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 7.0 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. Run the LDAP migration tool. Use the CLI option **isim** > **migration** > **ldap_migrate** to migrate directory server data to Security Identity Manager Version 7.0.
8. Run the database migration tool. Use the CLI option **isim** > **migration** > **db_migrate** to migrate database server data to Security Identity Manager Version 7.0.
9. Start IBM Security Identity Manager on the new production environment.
10. Apply performance tuning setting to directory and database servers.

Stopping the Security Identity Manager server

Start the Security Identity Manager to complete the production cutover.

About this task

Stop the IBM Security Identity Managerserver in the new production environment.

Procedure

1. On the **Appliance Dashboard**, locate the **Server Control** widget. The **Server name** column displays a list of all the servers.
   - Cluster Manager server
   - IBM Security Identity Manager server
   - IBM Security Directory Integrator server
2. Select **IBM Security Identity Manager**server from the list.
3. Click **Stop** The **Server status** column displays the status of the server as **Stopped**.

Preparation of the new production environment directory server and database server for 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 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. Run the Security Identity Manager middleware configuration utility to create an 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 and run the middleware configuration utility again, you can reconfigure the database. Use the **idsxcfg** or **idsucfgdb** and **idscfgdb** commands. When you reconfigure the database, the tuning settings that were applied to the LDAP instance by the middleware configuration utility are not saved. 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.

What to do next

Reconfigure the database instance.

Reconfiguring the Oracle database instance

You must configure your database instance to run in the Security Identity Manager Version 6 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" on page 87.
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.

What to do next

Capture and import the old production server data.

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 7.0 server.
4. Import the directory server data.

   For more information, see Importing directory server data.

What to do next

Capture and import database information.

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" on page 82.
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" on page 84

What to do next

Clear the service integration bus.

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" on page 87.
2. Enter this command on one line to import the Tivoli Identity Manager Version 5.1 exported data.

   ```
   imp system/system_pwd file=path\itimxx.dmp log=path\itimxxexp.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:\xxdata\oracleor /opt/xxdata/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`.

What to do next

Run the upgrade commands.

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 7.0 server, the Service Integration Bus (SIB) data from the restored database must be cleared out. See "Clearing the service integration bus" on page 86.

Starting the Security Identity Manager server

Start the Security Identity Manager to complete the production cutover.

Procedure

1. On the **Appliance Dashboard**, locate the **Server Control** widget. The **Server name** column displays a list of all the servers.

- Cluster Manager server
- IBM Security Identity Manager server
- IBM Security Directory Integrator server

2. Select **IBM Security Identity Manager**server from the list.
3. Click **Start** The **Server status** column displays the status of the server as **Started**.

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`.

For more information about emptying the recycling bin, see *Emptying the recycle bin* in the Performance topic of the Security Identity Manager product documentation site.

Verification of the installation

After you complete the installation, confirm that you can log on to the Security Identity Manager version 7.0 system.

Log on to Security Identity Manager version 7.0. 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 7.0 installation, go to the IBM Knowledge Center, search for IBM Security Identity Manager Version 7.0.1.10, and click **Installing** > **Installation of prerequisite components** > **Database installation and configuration** > **Installation and configuration of the IBM DB2 database** > **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.

For more information about performance tuning settings, see the *Performance* topics on the Security Identity Manager product documentation site.

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 7.0.

Updating the SIB schema tables for the alternate client reroute (ACR) feature

If you are upgrading to the IBM Security Identity Manager 7.0.1.10 virtual appliance or migrating from IBM Tivoli Identity Manager 5.1 to the 7.0.1.10 virtual appliance, the SIB schema tables are not updated for the database high availability ACR feature. You might see this message in the `systemout` log file: `CWSIS1602W: Restrict long running locks feature is ignored because the datastore is not upgraded to use this feature.`

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.

About this task

The SIB schema, **`schema_name`**, values are `ITIML000`, `ITIML001`, `ITIML002`, `ITIML003`, and `ITIMS000`.

The number of schema names depends on the number of nodes in the cluster.

Updating the SIB table for a DB2 database

Procedure

1. Open a DB2 command window.

   For UNIX or Linux systems

   a. Log on as the DB2 instance owner.
   b. Enter `db2` to open a DB2 command window.

   For Windows systems

   a. Click **Start** > **Run**
   b. Enter `db2cmd` to open a DB2 command window.
   c. Enter `db2` on the DB2 command window.
2. Connect to the database as the DB2 instance owner. Issue the command

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

   Where

   itimdb Is the IBM Security Identity Manager name.

   instance_owner
   Is the owner of the DB2 instance.

   instance_owner_password
   Is the password of the DB2 instance owner.

3. In the DB2 command window, enter the SQL statements that are needed to update the tables in the SIB schemas. Issue the following commands for each of the SIB schemas in your environment:

   ```
   ALTER TABLE schema_name.SIBOWNER ADD ME_LUTS TIMESTAMP;
   ALTER TABLE schema_name.SIBOWNER ADD ME_INFO VARCHAR(254);
   ALTER TABLE schema_name.SIBOWNER ADD ME_STATUS VARCHAR(16);
   ALTER TABLE schema_name.SIB000 ADD REDELIVERED_COUNT  INTEGER;
   ALTER TABLE schema_name.SIB001 ADD REDELIVERED_COUNT  INTEGER;
   ALTER TABLE schema_name.SIB002 ADD REDELIVERED_COUNT  INTEGER;
   ```

Updating the SIB table for an Oracle database

Procedure

1. Start the Oracle database on the target Security Identity Manager Version 7.0.1.10 Oracle server.
2. Ensure that the ORACLE_HOME and ORACLE_SID environment variables are set correctly. Where

   ORACLE_HOME
   Is the Oracle default installation directory.

   ORACLE_SID
   Is the Tivoli Identity Manager database instance.
3. Run the following SQL commands with the **sqlplus** utility with Oracle system user for each of the SIB schemas in your environment.

   ```
   ALTER TABLE schema_name.SIBOWNER ADD (ME_LUTS TIMESTAMP, ME_INFO VARCHAR(254), ME_STATUS VARCHAR(
   ALTER TABLE schema_name.SIB000 ADD REDELIVERED_COUNT  INTEGER;
   ALTER TABLE schema_name.SIB001 ADD REDELIVERED_COUNT  INTEGER;
   ALTER TABLE schema_name.SIB002 ADD REDELIVERED_COUNT  INTEGER;
   ```

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 7.0 server. You must also update the service to point to the new file location on the IBM Security Identity Manager version 7.0 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 7.0, 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

You might encounter the following error in the DB2 Universal Database in Windows operating systems.

Use the following commands, if you receive this error.

```
SQL2519N The database was restored but the restored database was not
migrated to the current release. Error "-1704" with tokens "3" is returned.:
```

If this issue occurs, run the following commands to correct the issue.

```
update db cfg for itimdb using LOGFILSIZ 1000
update db cfg for itimdb using LOGPRIMARY 30
update db cfg for itimdb using LOGSECOND 20
migrate db itimdb
```

The *itimdb* is the database name for IBM Security Identity Manager. For more information about this error, see the DB2Knowledge Center. http://www.ibm.com/support/knowledgecenter/SSEPGG/welcome.

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 *Migrating custom FESI extensions to the IBM(r) JSEngine* in the Reference section of the Security Identity Manager product documentation site.

Compilation failures

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.

Chapter 7. Upgrade to IBM Security Identity Manager Version 7.0.1.10

Use this information to upgrade to IBM Security Identity Manager Version 7.0.1.10, both for single-server and cluster environments.

The supported upgrade path is

Table 20. Upgrade path to IBM Security Identity Manager Version 7.0.1.10

From	To
IBM Tivoli Identity Manager Version 5.1	IBM Security Identity Manager Version 7.0.1.10

Migrating to IBM Security Identity Manager Version 7.0.1.10

You can migrate an earlier version of the IBM Security Identity Manager to a newer version so that the new environment is identical to the earlier environment.

Before you begin

In IBM Tivoli Identity Manager Version 5.1, back up the `itimKeystore.jceks` file from *`ITIM_HOME`*`/data/keystore/`. For example, from `/opt/ibm/itim/data/keystore/`.

About this task

Complete the virtual appliance migration setup tasks from the command line and the IBM Security Identity Manager virtual appliance management user interface.

Procedure

1. Set up the IBM Security Identity Manager virtual appliance. For instructions, go to the IBM Knowledge Center, search for IBM Security Identity Manager **Version 7.0.1.10**, and click **Installing** > **Set up the virtual appliance** > **Configuring the IBM Security Identity Manager by using the initial configuration wizard**.
2. Locate the response file for migration. Download the response file in the advanced configuration mode. Set your configuration parameters for the IBM Security Identity Manager virtual appliance in a response file. Update the response file with the values that you want.
3. Uncomment the `isim.migration=true` property in to the response file.

   Note: Migration can be done through a response file only.
4. Upload the response file to configure the virtual appliance in the **Advanced Configuration** mode.
5. After the configuration is complete, click the link to access the appliance dashboard.
6. Log on to the IBM Security Identity Manager virtual appliance console. For instructions, go to the IBM Knowledge Center, search for IBM Security

Identity Manager **Version 7.0.1.10**, and click **Product overview** > **Getting started** > **Logging on to the IBM Security Identity Manager virtual appliance console**.

7. From the top-level menu of the **Appliance Dashboard**, select **Configure** > **Advanced Configuration** > **Custom File Management**.
8. From the Custom File Management page, upload the `itimKeystore.jceks` file under `directories\data\keystore`. For more information, go to the IBM Knowledge Center, search for IBM Security Identity Manager Version 7.0.1.10, and click **Configuring** > **Virtual appliance configuration** > **Managing custom files**.

   Note: `itimKeystore.jceks` file is the one that you backed up from the IBM Tivoli Identity Manager Version 5.1 installation directory.
9. Access the command-line interface (CLI) of the virtual appliance.
10. At the command-line prompt, run the **`isim keystore_password update KEYSTORE_PASSWORD`** command.
    a. Enter the *KEYSTORE_PASSWORD*.

       KEYSTORE_PASSWORD is the password of the `itimKeystore.jceks` file.

    b. Confirm the *KEYSTORE_PASSWORD*.
11. Stop the IBM Security Identity Manager and the Cluster Manager server.
    a. Go to the **Server Control** widget on the **Appliance Dashboard**.
    b. Select the **IBM Security Identity Manager server.**
    c. Click **Stop**.
    d. Select the **Cluster Manager server.**
    e. Click **Stop**.
12. Clear the **Service Integration Bus** (SIB) tables. See “Clearing the service integration bus” on page 86. For more information about clearing SIB tables, go to the IBM Knowledge Center, search for IBM Security Identity Manager **Version 7.0.1.10**, and click **Configuring** > **Virtual appliance configuration** > **Reconfiguring the data store connection** step 3.
13. Start the Cluster Manager server and the IBM Security Identity Manager server.
    a. Go to the **Server Control** widget on the **Appliance Dashboard**.
    b. Select the **Cluster Manager server.**
    c. Click **Start**.
    d. Select the **IBM Security Identity Manager server.**
    e. Click **Start**.

    For more information, go to the IBM Knowledge Center,search for IBM Security Identity Manager **Version 7.0.1.10**, and click **Administering** > **Virtual appliance management** > **Appliance Dashboard** > **Viewing the Server Control widget**.

Chapter 8. Security properties

Log on to the **Appliance Dashboard** of the IBM Security Identity Manager virtual appliance console to modify these security properties.

For more information, see Logging on to the IBM Security Identity Manager virtual appliance console.

1. In the **Quick Links** widget of the **Appliance Dashboard**, click **Identity Administration Console**.
2. Log on to the IBM Security Identity Manager Console.
3. Select **Set Systems Security** > **Set Security Properties** to modify these security properties.

Password settings

Click **Set Systems Security** > **Set Security Properties** to modify these password properties.

Enable password editing
Select this check box to enable users to type a value when changing their own passwords. Additionally, help desk assistants, service owners, and administrators can type a value when changing their own passwords, and also the passwords for other individuals. You can also select a check box by using the Tab key to give focus to the check box and then pressing the space bar.

Hide generated passwords for others
Select this check box to hide generated passwords for others. This check box is not available if password editing is enabled.

Enable password synchronization
Select this check box to synchronize any subsequent password changes on all the accounts for a user. If this check box is selected, one-password change is synchronized on all accounts for the user. If this check box is cleared, the user must select each account and change its password individually.

Set password on user during user creation
Select this check box to set the password for a user, at the time the user is created.

Password retrieval expiration period in hours
Type an interval, in hours, in which a user must retrieve a password, before the password expires. After the new account is created, the user receives an email with the URL link that provides the password. The user must get the password before this password retrieval period expires.

For the new values to take effect, you must log out and log in again.

IBM Security Identity Manager login account settings

You can modify security settings to limit the number of days an account is valid or to limit the number of incorrect login attempts.

Click **Set Systems Security** > **Set Security Properties**, to modify these login properties.

Identity account password expiration period in days

This property is only for the Security Identity Manager Server account. Type an interval, in days, after which the password expires for an Security Identity Manager account. The user must change the password before this period is reached. Whenever a new password is set for the Security Identity Manager Server account, the password expiration period is affected from that time. You can disable password expiration by setting this value to zero. The default value of 0 indicates that the account password never expires.

Maximum number of incorrect login attempts

Type the number of incorrect login attempts that can occur before an Security Identity Manager account is suspended. The default value of 0 indicates that there is no limit.

For the new values to take effect, you must log out and log in again.

Group settings

You can select to modify the group properties automatically.

Click **Set Systems Security** > **Set Security Properties**, to modify the group properties.

Automatically populate IBM Security Identity Manager groups

Select this check box to automatically put the IBM Security Identity Manager accounts of newly named service owners in the default Service Owner group. The automatic action is enabled or disabled immediately. You do not need to restart Security Identity Manager. For example, membership in a group can take place when you create or modify a service, specifying a service owner.

Additionally, the Security Identity Manager accounts of newly named managers are automatically put in the default Manager group. For example, this action can occur when you create or modify a user who is a subordinate, specifying the manager of the user.

Automatic group membership is not supported when the service owner is a role.

For the new values to take effect, you must log out and log in again.

Default settings for provisioning policy when a new service is created

Select the default setting for provisioning policies when new services are created. You might not want to create a default policy when a new service is created if the amount of time to evaluate the default policy for all users is significant.

Click **Set Systems Security** > **Set Security Properties** to modify the default settings for provisioning policies when new services are created. If you do not want to create a default policy, select **No, I will manually configure a policy later** and then click **OK**.

Then, when you create a service, the default setting for provisioning policies is set to **No, I will manually configure a policy later**.

Chapter 9. Forgotten password settings

Log on to the **Appliance Dashboard** of the IBM Security Identity Manager virtual appliance console to modify the properties for forgotten password.

For more information, see Logging on to the IBM Security Identity Manager virtual appliance console.

1. In the **Quick Links** widget of the **Appliance Dashboard**, click **Identity Administration Console**.
2. Log on to the IBM Security Identity Manager Console.
3. Select **Set Systems Security** > **Configure Forgotten Password Settings** to modify the properties for forgotten password.

Forgotten password authentication

Click **Set Systems Security** > **Configure Forgotten Password Settings** to modify forgotten password authentication.

Select this check box to activate the forgotten password authentication. If the authentication is activated, the login page opens a **Forgot your password?** prompt for users who forget their passwords. A user who provides the correct responses to the questions receives a new, automatically generated password. If the check box is cleared, no prompt occurs on the login page. Users must contact the help desk assistants or system administrators for help in resetting their passwords.

For the new values to take effect, you must log out and log in again.

Login behavior

Click **Set Systems Security** > **Configure Forgotten Password Settings**, to modify the login properties.

When the user successfully answers the questions

Select the login behavior:

Change password and log in to system

Logs the user in to the system and requires a password change.

Reset and email password

Resets the password, and sends the new password to the email address of the user.

Message suspending account for failed answers

Type the message the user receives after failing to enter the correct answers.

Send message to email address

Type the email address to receive messages.

For the new values to take effect, you must log out and log in again.

Challenge behavior

Click **Set Systems Security** > **Configure Forgotten Password Settings** to modify the challenge properties.

Select whether the user or the administrator defines challenge questions.

Users define their own questions

Select for users to provide their questions.

Number of questions user sets up
Type the number of questions that the user must provide.

Number of correct answers user must enter
Type the number of correct answers that the user must provide to gain access to the system.

Administrator provides predefined questions

Select the option to define the set of questions that the users must answer and the language in which the question is used. When the option is selected, the Specify Forgotten Password Question section opens.

Specify Forgotten Password Question
Click to expand this section to specify the question that you want users to answer.

New challenge question
Type the question that you want users to answer and click **Add**.

Locale Select the language in which the question is used and click **Add**.

Challenge questions table
The **Challenge questions** table contains the list of questions that you added and that you can choose to have users answer. To sort the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select Select this check box to choose an existing question.

Locale Displays the language used in the question.

Question
Displays the text of a question.

Click **Remove** to remove a selected question.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

User has a choice of predefined questions?

No, answer all questions
Displays all predefined questions, which the user must answer correctly.

Yes, user selects which questions to answer
Displays the number of questions that the user selects and must answer correctly after forgetting a password. Type the number of questions that the user selects.

No, answer a subset of questions that the system provides

Displays a random subset of predefined questions, which the user must answer correctly after forgetting a password.

Number of questions user sets up

Type the number of questions that the user configures.

Number of correct answers user must enter

Type the number of questions that the user must correctly answer. This field is available, if the user must answer a subset of questions that the system provides.

For the new values to take effect, you must log out and log in again.

Chapter 10. Installing the Java plug-in

If the Java plug-in is not installed on your system, or is not at a supported level, the browser prompts you to install the plug-in.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

The Java plug-in provides a connection between browsers and the Java platform, and enables IBM Security Identity Manager applets to run within a browser.

Security Identity Manager allows administrators to choose between static or dynamic versioning of the Java plug-in. By default, Security Identity Manager uses dynamic versioning that allows any 1.5.x version over 1.5.0 to work. Alternatively, Security Identity Manager can use static versioning of the Java plug-in, such as version 1.5.0_02.

External websites that provide plug-ins can change. Administrators might also create an internal website to download the Java plug-in. For more information about selecting static and dynamic versioning, or defining download locations, see the `ISIM_HOME\data\ui.properties` file.

Complete these steps to install the plug-in:

Procedure

- On Windows systems, the Internet Explorer or Mozilla Firefox browser prompts you to install the Java plug-in and automatically register it with the browser.

  If your browser does not prompt for the Java plug-in, you can obtain the Java plug-in from the Java SE page of the Oracle website.
- On UNIX and Linux systems, you must complete these manual steps to install and register the Java plug-in:
  1. Obtain the Java plug-in from one of these websites:
     - Linux systems: the *Java SE* page of the Oracle website.
     - AIX systems: *AIX Download and service information* of the IBM developerWorks® website.
  2. Register the Java plug-in with the browser.

Chapter 11. Configuring an administrator account in an external user registry

When you use an external user registry, and you set the default administrator ID to a value other than ITIM Manager, you must configure the default administrator account.

About this task

The default IBM Security Identity Manager installation creates an administrator account named ITIM Manager. You can optionally choose to use a different administrator account name. This option is useful when you install IBM Security Identity Manager into an environment that already has a WebSphere security domain that uses an external user registry.

The following procedure shows an example of how you can change the default administrator account from ITIM Manager to itimManager. This procedure assumes that you use an IBM Security Directory Server LDAP directory server, with the organizational units shown in the first step.

Procedure

1. Create a text file with the following contents:

```
dn: eruid=ITIM Manager,ou=systemUser,ou=itim,ou=org,dc=com
changetype: modrdn
newrdn: eruid=itimManager
deleteoldrdn: 1
```

2. Run an **ldapmodify** command that uses the text file you created.

   Command syntax:

```
ldapmodify -h hostIP -D adminDN -w adminPassword  -i filePath
```

Table 21. Sample **ldapmodify** *command to change administrator account*

Entry	Description
ldapmodify	This command is in *TDS_HOME*/bin directory. For example: **Windows** C:\Program Files\LDAP\V6.3\bin **UNIX or Linux** *TDS_HOME*/bin
hostIP	The IP address of the IBM Security Directory Server, where the IBM Security Identity Manager LDAP data is stored.
adminDN	The administrator DN. For example, cn=root
adminPassword	The administrator password
filePath	The path to the file that you created in the previous step.

3. Update the IBM Security Identity Manager properties file ISIM_HOME/data/enRole.properties with the new default administrator ID.

   Example entry:

```
enrole.defaultadmin.id=itimManager
```

4. Restart the WebSphere application server, to load the updated values from the property file.

What to do next

Continue with "Verifying access for the administrator account."

Verifying access for the administrator account

Verify that the administrator account is configured correctly.

About this task

Ensure that IBM Security Identity Manager administrator can successfully log in by authenticating with the external user registry

Procedure

1. Log on to the IBM Security Identity Manager administration console

   Access the default URL, where `hostIP` is the IP address or fully qualified domain name of the server that runs IBM Security Identity Manager:

   ```
   http://hostIP:9080/itim/console
   ```
2. Use the administrator name that you specified during the IBM Security Identity Manager installation.

   The default administrator account is `ITIM Manager`, but you had the option of specifying a different name.
3. Enter the password you specified for your administrator account.

   The default password is `secret`.

Results

If you can log in successfully by supplying the password you used for the default administrator user, then you successfully configured the LDAP user registry as an external authentication user registry for IBM Security Identity Manager.

Part 2. Optional configuration

You can complete optional configuration tasks as needed for your deployment.

- Language pack installation
- Change of the language display of the browser
- Adapter and profile installation
- Change of cluster configurations after IBM Security Identity Manager is installed
- Downloading and installing the product documentation site files
- Installing the Incremental Data Synchronizer
- Reconfiguration for authentication with an external user registry

Part 3. Appendixes

Appendix. User registry configuration for external user registry

If you want to use an external user registry for authentication, and do not already have a registry, you must create registry entries.

The topic Preinstall configuration for authentication with an external user registry describes how to prepare an existing user registry for use as an external user registry for authentication. However, if you do not have an existing user registry, you must create one first. The instructions describe how to configure a new user registry so that it can be prepared for use as an external user registry for authentication.

These instructions present one example of how to configure a user registry by using the graphical administration tool for IBM Security Directory Server. Alternatively, you can use a command-line utility such as **`ldapadd`**. If you are using a different user registry product, your configuration steps can differ.

The task sequence is:

1. Create a suffix.

   The example uses a suffix `dc=mycorp`
2. Create a domain.

   The example uses a domain `dc=mycorp`.
3. Create a user template.
4. Create a user realm.

   The example uses a realm `dc=mycorp`. IBM Security Identity Manager requires two user accounts in the realm. The user accounts are an administrator user and a system user. For the administrative user, we use `ITIM Manager`. For the system user, we use `isimsystem`.

This example creates a suffix `dc=mycorp`.

To begin configuration, see “Creating a suffix.”

Creating a suffix

You can use the IBM Security Directory Server Instance Administration utility to create a suffix.

Procedure

1. Start the IBM Security Directory Server Instance Administration tool.
2. In the Instance Administration tool, select the instance and click **Start/Stop...** to stop the server. The server must be stopped to create a suffix.
3. Click **Stop server** to stop the server. Click **Close** to close the Manage server state window.
4. In the Instance Administration tool, click **Manage....**
5. In the IBM Security Directory Server Configuration tool, go to **Manage suffixes**. In the Suffix DN field, enter the suffix name `dc=mycorp`. Click **Add** and click **OK**.

6. When the `dc=mycorp` suffix is added, start the IBM Security Directory Server server.

What to do next

Continue with the instructions in *Creating a domain, user template, and user realm.*

Creating a domain, user template, and user realm

You can use the IBM Security Directory Server web administration tool to create a domain, user template, and user realm.

About this task

This task shows how to use the graphical user interface.

If the web administration tool is not installed, see the IBM Security Directory Server documentation for installation instructions: http://www.ibm.com/support/knowledgecenter/SSVJJU/welcome?

Note: Alternatively, you can use an **`ldapadd`** command.

Procedure

1. Start the IBM Security Directory Server web administration tool and log on to your LDAP server as an administrator.
2. Go to **Directory management** > **Manage entries** and click **Add...** to create a domain.
3. In the Structural Object Class field, select **domain** and click **Next**.
4. On the Select auxiliary object classes panel, you do not need to specify any settings. Click **Next**.
5. On the Required Attributes panel, enter `dc=mycorp` in the **Relative DN** field. In the Required attribute section, in the **dc** field, enter `mycorp`. Click **Next**.
6. You do not need to set any values on the Optional attributes page. Scroll to the bottom of the panel and click **Finish**.
7. A confirmation page displays, and asks if you want to add a similar entry. Click **No** to go back to the Manage entries page.
8. On the Manage entries page, ensure that the `dc=mycorp` domain is created and listed in the RDN column.
9. Optionally, you can create a user template. If you do not want a user template, continue to the next step to create the user domain. To create a user template:
   a. Go to the **Realms and templates --> Manage user templates** page and click **Add...**.
   b. On the Add user template page, enter a name in the **User template name** filed and enter a value in the **Parent DN** filed. Click **Next**.

      For this example, **User template name** can be `mycorpUserTempl` and **Parent DN** is `dc=mycorp`.
   c. Select a value for the **Structural object class** for this user template. For this example, select menu item **inetOrgPerson**. Click **Next**.
   d. Enter a value in the **Naming attribute** field. For this example, enter `uid`. Click **Edit...** to add the password field to the required attributes tab.
   e. On the Edit tab page, select the **userPassword** attribute and click **Add**.

f. When **userPassword** is added, go to the **Selected attributes** field and move **userPassword** to the bottom. Click **OK**.

g. Click **Finish** to create the user template.

h. Verify that the user template `mycorpUserTempl` is created.

   On the Manage user templates page, verify the existence of the entry `cn=mycorpusertempl,dc=mycorp`.

10. On the **Realms and templates --> Manage realms** page, click **Add...** to create a user realm for the user template that you created.
11. On the Add realm page, enter values in the **Realm name** field and the **Parent DN** field, and click **Next**.

    For example, **Realm name** can be `mycorpUserRealm` and **Parent DN** is `dc=mycorp`.
12. On the Add realm page, go to the **User template** menu and select the user template that you created. Click **Edit...**.

    In this example, the value in the User template field is `cn=mycorpusertempl,dc=mycorp`.
13. On the Search filter page, accept the default settings and click **OK**.
14. Click **Finish** to complete the creation of a user realm.
15. Select **Realms and templates > Manage realms**. Ensure that the new realm is listed.

    For this example, ensure that there is an entry `cn=mycorpuserrealm,dc=mycorp`.

Results

The user registry is now configured.

Index

Printed in USA