IBM Security Identity Manager
Version 7.0.0.2

Installation Topics

IBM Security Identity Manager
Version 7.0.0.2

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 1, “Installation of prerequisite components,” on page 3
- 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. 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 1. 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 1. 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 2. 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 7.

Table 3. 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 3. 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 9.

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 6.3, 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`

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 `init`*db_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 `init`*db_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 16.
     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 26.

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 27.

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 3 and "Installation and configuration of a directory server" on page 21.

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.

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 4. 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.

For more information about IBM Security Directory Integrator, see Directory Integrator support. .

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 36.

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 40.

About this task

See Table 5 that lists the external user registry options that you can configure or reconfigure.

Table 5. 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 5. 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 5 on page 37.
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 5 on page 37.
   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 71.
2. Collect the information that is required to configure the Application Server security domain.

   For example, for an LDAP user registry:

Table 6. 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 6. 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 7. 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 8. 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 9. 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 10. 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 10. 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 2. 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.

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.
   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. Change the virtual appliance password. After you change the virtual appliance password, continue to the next screen.

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

5. 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.

6. 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
```

7. 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
```

8. Configure the time settings for the virtual appliance.

   Note: If you want 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
```

9. Review the summary of configuration details.
10. 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.

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."

   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 51.

   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 53.

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 45.
- 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

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.
   - **Configured login**: `admin`
   - **Password**: `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.
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 1 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 working. 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 1 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 3. Upgrading the IBM Security Identity Manager virtual appliance

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.

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 partition 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_*.pkg` build.
2. Access the command-line interface (CLI) of the virtual appliance by using either an `ssh` session or the console.
3. Copy the `isim_*.pkg` to a USB device.
4. Attach the USB device to your virtual system.
5. In the virtual appliance CLI, run the **`isim`** command to display the `isim` prompt.
6. At the `isim` prompt, run the **`firmware_update`** command.
   a. Run the **`list_firmware`** command to list the firmware updates from a USB device.
   b. Run the **`transfer_firmware`** command to transfer the firmware updates from a USB device to the virtual system.

      Note: To install a firmware upgrade, you must first transfer it to the virtual system.
   c. Run the **`install_firmware`** command.
   d. Select the index of the firmware update that you want to install to the virtual system and press **Enter**.

      The results are as follows:

1) The upgrade process formats Partition 2 and installs the new firmware update on it.
2) When you apply the firmware update, your policies and settings are copied from Partition 1 to Partition 2.
3) On completion, the process indicates you to restart the virtual system.

e. Type the **reboot** command and press **Enter** to restart the virtual system by using Partition 2. Partition 2 is now the active partition.

   The results are as follows:

   1) After the virtual appliance restarts from the Partition 2, all the configuration that were part of Partition 1, is applied to the Partition 2.
   2) After the configuration is applied to the virtual appliance, the process indicates you to restart the virtual appliance.

f. Restart the virtual appliance to complete the upgrade process.

g. For the Identity data store, clear the **Service Integration Bus**. See Reconfiguring the data store connection.

h. Restart the Identity service.

i. 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.

j. 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:

   1) Check and fix any errors if the upgrade process failed.
   2) Use Partition 1 to set it as the active partition and restart it.

      Partition 1 now becomes the active partition.

Chapter 4. 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 5. 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 6. 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 7. 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 11. 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.

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

P

R

S

T

U

V

W

X

Printed in USA