IBM Security Identity Manager
Version 7.0.2

Installation Guide

IBM

Contents

Tables

Part 1. Installation

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

© Copyright IBM Corp. 2019, 2020

Chapter 1. Software firewall configuration in the virtual appliance

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

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

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

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

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

Table 1 on page 3 describes a list of available ports that you can use to work with IBM Security Identity Manager virtual appliance:

Table 1. Port numbers

Port numbers	Used by
22	Secure Shell (SSH)
161	SNMP server, if configured
443	Secure appliance management interface
1098	Security Directory Integrator web server port
1099	RMI Dispatcher service
9056	Cluster Manager secure administrator host
9057	Cluster Manager bootstrap address
9058	Cluster Manager soap port
9061	Cluster Manager CSIV2 SSL server authentication listener address
9062	Cluster Manager CSIV2 SSL mutual authentication listener address
9063	Cluster Manager ORB Listener
9064	Cluster Manager cell discovery address
9065	Cluster Manager DCS Unicast address
2809	Nodeagent bootstrap address
5001	Nodeagent IPv6 multicast discovery address
7272	Nodeagent node discovery address
8878	Nodeagent soap port
9201	Nodeagent CSIV2 SSL server authentication listener address

© Copyright IBM Corp. 2019, 2020

Table 1. Port numbers (continued)

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

Chapter 2. Installation of prerequisite components

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

Database installation and configuration

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

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

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

- IBM DB2® database
- Oracle database

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

Worksheet

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

Table 2. Typical database worksheet

Field name	Description	Default or example value	Your value
Host name	Name of the computer that hosts the database.		
Port number	Database service listening port.	Examples: 50000, 50002, or 60000	
Database name	Name of the IBM Security Identity Manager database.	Example: **`itimdb`**	
Admin ID	Database administrator user ID.	Example: **`db2admin`** **Note:** 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`**	
Database password	The password for the **`itimuser`** user ID.		

Before you install the database product

Before you install the database product, you must:

© Copyright IBM Corp. 2019, 2020

- 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)

    https://www.ibm.com/support/knowledgecenter/SSEPGG_11.1.0/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

Important: IBM Security Identity Manager might require Db2 to run with a required level of the Db2 fix pack. Always check the IBM Security Identity Manager software product compatibility report for the latest updates to prerequisites and minimum supported level of fix packs for your Db2 version.

If you do not have a Db2 database server, you can install Db2® Enterprise Server Edition Version 11.1.4.4. The IBM Security Identity Manager product package, that you can download from Passport Advantage® Online, includes an activation key to download Db2 Enterprise Server Edition Version 11.1.4.4 from Fix Central. After you download Db2 Enterprise Server Edition Version 11.1.4.4, see the Db2 product documentation for installation instructions.

For more information about installing Db2 and any fix packs, see the 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.

Table 3. Db2 database typical configuration parameters on UNIX and Linux systems

UNIX and Linux systems	Description	Value
Db2 administrator user ID and instance name	The user ID that is used to connect to DB2 as the Db2 administrator and instance owner.	`db2admin` **Note:** If you do not use the middleware configuration utility, this value is `db2inst1` by default.
Db2 instance password	The password for the administrator user ID.	A user-defined value.
Db2 instance home directory	The home directory of the Db2 administrator and instance owner.	• AIX: `/home/db2admin` • Linux: `/home/db2admin` • Linux for System z®: `/home/db2admin`

User names and passwords on Windows systems

The following table shows the default values that are created on Windows systems.

Table 4. Db2 database typical configuration parameters on Windows systems

Windows systems	Description	Value
Db2 instance name	The name of the Db2 instance.	db2admin **Note:** Db2 defaults to an instance value of Db2.
Administrative user ID	The user ID that is used to connect to Db2 as the Db2 administrator and instance owner.	db2admin
Password	The password for the administrator user ID.	A user-defined value.
Db2 instance home directory	The home directory of the Db2 administrator and instance owner.	*drive* For example, `C:`

Related concepts

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.

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

You can configure parameters for DB2 and IBM Security Directory Server.

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.

Related tasks

Determining the correct service listening port and service name
You must verify that the correct service name and listening port are specified.

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

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.

Related tasks

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.

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

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.

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:

  a. 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.

  b. Click **Add User**.

  c. 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.

  d. 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.

Related tasks

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.

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

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.

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.
Related tasks
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.

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.

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.

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.

Related tasks

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.

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.

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

Determining the correct service listening port and service name

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. If you migrated DB2 8.2 to DB2 9.5, DB2 9.7, DB2 10.1, or DB2 11, 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`

Related concepts

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.

Related tasks

Ensuring that CUR_COMMIT is ON on DB2 version 9.7 and later versions
Databases that are updated from versions earlier than DB2 version 9.7 have this parameter set to **DISABLED**. It must be set to ON.

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

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

About this task

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

Procedure

1. Determine whether the **cur_commit** is set to ON.

   Enter the commands

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

2. Look for the Currently Committed parameter **CUR_COMMIT**.

   It must be set to ON.

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

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

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

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

   Issue the commands

   ```
   db2stop
   db2start
   ```

   Note:

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

What to do next

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

Related concepts

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.

Related tasks

Determining the correct service listening port and service name
You must verify that the correct service name and listening port are specified.

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.

Related concepts

Change of the DB2 application heap size
Loading many users can encounter performance issues.

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.

Related tasks

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.

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.

Related concepts

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.

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, Oracle 18c or Oracle 19c Database, you must create a 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.

Related concepts

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

Related tasks

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.

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.

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, Oracle 18c, or Oracle 19c Database, you must create a 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.

Related concepts

Tasks for creating the database

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

Oracle database performance tuning

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

Related tasks

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.

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

Related concepts

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

Related tasks

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.

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.

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.

Related tasks

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.

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.

Related tasks

Enabling XA recovery operations

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

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.

Related concepts

Tasks for creating the database

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

Oracle database performance tuning

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

Related tasks

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.

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.

Related concepts

Preinstall configuration for authentication with an external user registry
IBM Security Identity Manager supports use of an external user registry for authentication. You must configure the registry before installing the product.

Related tasks

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.

Installing IBM Security Directory Server

These steps provide information about installing IBM Security Directory Server with the IBM Passport Advantage packages that are provided with the IBM Security Identity Manager product. These packages do not contain embedded middleware for DB2 and Application Server. For installation packages 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 packages provided with the IBM Security Identity Manager product, if DB2 is not already installed.
2. Install IBM Security Directory Server from the package 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.

Configuring IBM Security Directory Server manually

You can configure the directory server manually.

Before you begin

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

Related concepts

Successful suffix object configuration verification
You must verify that the LDAP suffix was added successfully.

Related tasks

Updating the IBM Security Directory Server configuration for IBMLDAP_ATTR_INCLUDE_BINARY to FALSE
After installing specific fixes for IBM Security Directory Server, the default IBM Security Directory Server configuration parameter **IBMLDAP_ATTR_INCLUDE_BINARY** might change to TRUE. This parameter change results in problems with LDAP adapter reconciliation or a lack of data for the *Individual Accounts by Role associated with a provisioning policy* report.

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

Updating the IBM Security Directory Server configuration for IBMLDAP_ATTR_INCLUDE_BINARY to FALSE

After installing specific fixes for IBM Security Directory Server, the default IBM Security Directory Server configuration parameter **IBMLDAP_ATTR_INCLUDE_BINARY** might change to TRUE. This parameter change results in problems with LDAP adapter reconciliation or a lack of data for the *Individual Accounts by Role associated with a provisioning policy* report.

About this task

By installing certain fixes that address APARS on certain versions of Directory Server, these fixes change the default value for the **IBMLDAP_ATTR_INCLUDE_BINARY** configuration parameter from FALSE to TRUE:

```
IBMLDAP_ATTR_INCLUDE_BINARY=TRUE
```

This issue occurs with the following APARs and Directory Server versions:

- IO20253 in Version 6.1.0.59
- IO20254 in Version 6.2.0.34
- IO19599 in Version 6.3.0.26
- IO21537 in Version 6.3.1.5

For more information, see https://www.ibm.com/support/pages/node/544007.

Procedure

- Change the IBM Security Identity Manager Directory Server or target Directory Server configuration, by editing the directory server ibmslapd.conf file.

Under the `cn=Front End, cn=Configuration` entry:

Specify the following configuration:

```
ibm-slapdSetenv: IBMLDAP_ATTR_INCLUDE_BINARY=FALSE
```

Restart the IBM Security Directory Server for changes to take effect.

- Upgrade IBM Security Directory Server to the following version, where the behavior is no longer the default setting.
  - `IO23920` in Version 6.4.0.5

What to do next

If there were issues before, you can attempt to reconcile or synchronize data between IBM Security Identity Manager with IBM Security Directory Server again.

Related concepts

Successful suffix object configuration verification
You must verify that the LDAP suffix was added successfully.

Related tasks

Configuring IBM Security Directory Server manually
You can configure the directory server manually.

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

Successful suffix object configuration verification

You must 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
```

Related tasks

Configuring IBM Security Directory Server manually
You can configure the directory server manually.

Updating the IBM Security Directory Server configuration for IBMLDAP_ATTR_INCLUDE_BINARY to FALSE
After installing specific fixes for IBM Security Directory Server, the default IBM Security Directory Server configuration parameter **`IBMLDAP_ATTR_INCLUDE_BINARY`** might change to TRUE. This parameter change results in problems with LDAP adapter reconciliation or a lack of data for the *Individual Accounts by Role associated with a provisioning policy* report.

Manually tuning the IBM Security Directory Server database

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

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.

Related concepts

Successful suffix object configuration verification
You must verify that the LDAP suffix was added successfully.

Related tasks

Configuring IBM Security Directory Server manually
You can configure the directory server manually.

Updating the IBM Security Directory Server configuration for IBMLDAP_ATTR_INCLUDE_BINARY to FALSE
After installing specific fixes for IBM Security Directory Server, the default IBM Security Directory Server configuration parameter **`IBMLDAP_ATTR_INCLUDE_BINARY`** might change to TRUE. This parameter change results in problems with LDAP adapter reconciliation or a lack of data for the *Individual Accounts by Role associated with a provisioning policy* report.

Security configuration of the directory server

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

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

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

Configuration of SSL for IBM Security Directory Server

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

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

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

Related concepts

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

Configuration of SSL for Oracle Directory Server Enterprise Edition

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

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

Related concepts

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

Preinstall configuration for authentication with an external user registry

IBM Security Identity Manager supports use of an external user registry for authentication. You must configure the registry before installing the product.

Any user registry that can be configured as Application Server user realm can be used as an authentication user registry for IBM Security Identity Manager. Application Server supports four types of user realms: federated repositories, local operating system, Stand-alone LDAP registry, and custom LDAP registry. The example configuration described in this documentation uses a stand-alone LDAP user registry.

Note: For more information about Application Server user realms, see the Application Server section in the IBM Knowledge Center.

To use an external user registry as an authentication registry for IBM Security Identity Manager, complete the following tasks:

1. Collect information from the external user registry.
2. Add required users to the external user registry.
3. Configure a Application Server security domain.

Related concepts

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.

Related tasks

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.

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 Appendix A, "User registry configuration for external user registry," on page 87.
2. Collect the information that is required to configure the Application Server security domain.

   For example, for an LDAP user registry:

Table 5. 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
The attribute names for group membership	member and uniqueMember

Related tasks

Adding required users to the external user registry
You must add required users to the external user registry.

Configuring a Application Server security domain
Application Server supports Security Domains that have the flexibility to use different security configurations.

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 6. 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 7. 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 8. 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**.

Related tasks

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.

Configuring a Application Server security domain
Application Server supports Security Domains that have the flexibility to use different security configurations.

Configuring a Application Server security domain

Application Server supports Security Domains that have the flexibility to use different security configurations.

About this task

You can configure Application Server to use different security attributes, such as the `UserRegistry`, for different applications. This example configuration creates a security domain for IBM Security Identity Manager with a stand-alone LDAP user registry.

You can skip the next procedure if either of the following conditions apply:

- You already configured Application Server global security with the user registry that you want to use for IBM Security Identity Manager authentication.
- You already configured a security domain for Application Server with the user registry that you want to use for IBM Security Identity Manager authentication.

Note: During IBM Security Identity Manager installation, you can choose to use the existing realm for the application server.

Procedure

1. Log on to the administrative console as an administrator.
2. Go to **Security > Security** domains. Click **New** to create a security domain for IBM Security Identity Manager.
3. Enter a name you want in the **Name** field. Click **OK** and save the changes.
4. After the new security domain is created, click the security domain name to configure the security attributes for the domain.
5. When you click the security domain name, the Security Domain page is shown. You must configure a number of settings. In the Assigned Scopes section, select the Application Server where IBM Security Identity Manager is to be installed.
6. In the Security Attributes section:
   a) Under Application Security, click **Enable application security**.
   b) For Java 2 Security, accept the default of **Disabled**, to optimize performance.
   c) Under User Realm, select **Standalone LDAP registry** and click **Configure...**
7. On the Stand-alone LDAP registry page, provide the values specified in the table:

Table 9. Security domain configuration for stand-alone LDAP registry

Field	**Description**
Realm name	Provide the realm name as whatever you want.
Type of LDAP server:	For this example, IBM Tivoli® Directory Server
Host	The IBM Security Directory Server host name or IP address
Port	The LDAP server port for IBM Security Directory Server
Base DN	The base DN of the LDAP registry

Table 9. Security domain configuration for stand-alone LDAP registry (continued)

Field	Description
Bind DN	The user DN that is bound to the LDAP registry.
Bind password	The password of the bind user.

8. Click **Test Connection** to ensure that Application Server can communicate with the LDAP registry.
9. After the connection test is successful, click **OK** and save the changes.
10. After the user realm basic security attributes are configured, set the advanced LDAP settings for this user realm.
    a) Click the security domain name.
    b) Click **Configure** (next to the realm name).
    c) Select **Set Advanced Lightweight Directory Access Protocal (LDAP) user registry setting** link on the Stand-alone LDAP registry attribute setting page.
11. Click **OK** and save the changes. From the Stand-alone LDAP registry page, click **OK** and save the changes.
12. When you save the changes, you are redirected to the domain list page. Select the domain name to continue configuring the remaining security attributes for this domain.

    Review the default settings and change any that apply to your deployment.
13. Click **OK** and save the changes.
14. Restart Application Server.

Results

You completed the Application Server security domain configuration. You can now install IBM Security Identity Manager.

Related tasks

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.

Adding required users to the external user registry
You must add required users to the external user registry.

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 10. 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
   ```

Related concepts

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.

Preinstall configuration for authentication with an external user registry
IBM Security Identity Manager supports use of an external user registry for authentication. You must configure the registry before installing the product.

Optionally installing IBM Security Directory Integrator

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

Before you begin

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

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

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

About this task

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

Procedure

1. Install the required fix packs.

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

   - Support

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

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

2. Install agentless adapters

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

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

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

What to do next

Manually install agentless adapters and adapter profiles on remote systems. See "Installing agentless adapters" on page 36 and "Installing agentless adapter profiles" on page 38.

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 7.2. 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 7.2
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\V7.2"
   -DUSER_SELECTED_SOLDIR="C:\Program Files\IBM\TDI\V7.2\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/V7.2"
   -DUSER_SELECTED_SOLDIR="/opt/IBM/TDI/V7.2/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\V7.2"
```

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/V7.2"
```

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 29.

About this task

See Table 11 on page 40 that lists the external user registry options that you can configure or reconfigure.

Table 11. 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 11. 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 11 on page 40.
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 11 on page 40.
   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 Appendix A, "User registry configuration for external user registry," on page 87.
2. Collect the information that is required to configure the Application Server security domain.

   For example, for an LDAP user registry:

Table 12. 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
The attribute names for group membership	member and uniqueMember

Related tasks

Adding required users to the external user registry
You must add required users to the external user registry.

Configuring a Application Server security domain
Application Server supports Security Domains that have the flexibility to use different security configurations.

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 13. 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 14. 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`

Table 14. Example entries for required naming attributes for the default administrative user and the default system user accounts (continued)

Attribute	Example value for the default administrative user	Example value for the default system user
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 15. 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**.

Related tasks

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.

Configuring a Application Server security domain
Application Server supports Security Domains that have the flexibility to use different security configurations.

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 16. Installation and data synchronization process

Task	For more information
Install Cognos Business Intelligence.	1. Access http://www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0/com.ibm.swg.ba.cognos.cbi.doc/welcome.html. 2. Search for **Install and configure server components**.

Table 16. Installation and data synchronization process (continued)

Task	For more information
Install Framework Manager.	1. Access http://www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0/com.ibm.swg.ba.cognos.cbi.doc/welcome.html. 2. Search for **Installing IBM Cognos Framework Manager**.
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

Optionally, you can install IBM Framework Manager if you want to customize the reports or models.

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

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

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

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

Amazon EC2 support

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

Amazon EC2 is a web service that provides:

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

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

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

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

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

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

About this task

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

Procedure

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

Sequence	Command	Description
1	ec2-import-volume	Imports the appliance VHD into Amazon EC2.
2	ec2-describe-conversion-tasks	Monitors the **ec2-import-volume** task to show when the task is complete.
3	ec2-create-snapshot	Creates a snapshot of the imported disk image. This snapshot is required during the AMI registration process.
4	ec2-describe-snapshots	Monitors the status of the snapshot creation to show when the snapshot task is complete.

© Copyright IBM Corp. 2019, 2020

Sequence	Command	Description
5	ec2-register	Registers a snapshot as a new AMI. You must use the following parameter values when you register the AMI: **architecture:** x86_64 **kernel:** Use the appropriate parameter value for the kernel ID. **root device name:** /dev/xvda **virtualization type:** paravirtual
6	ec2-delete-disk-image	Removes the uploaded disk image from the storage bucket. The image is no longer required after you finish registering an AMI from the image.

Launching the appliance AMI

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

About this task

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

Procedure

1. Log in to the Amazon EC2 console.
2. Go to **INSTANCES** > **Instances** > **Launch Instance**.
3. Select the IBM Security Identity Manager AMI that you want to launch.
4. Click **Launch**.
5. In the **Choose an Instance Type** window, select an instance type and click **Next: Configure Instance Details**.
6. In the **Configure Instance Details** window, select the options that best fit your environment and click **Next: Add Storage**.
7. In the **Add Storage** window, validate the storage and click **Next: Tag Instance**.
8. In the **Tag Instance** window, add any desired tags and then click **Click Next: Configure Security Group**.
9. In the **Configure Security Group** window, ensure that the selected security group allows inbound SSH and HTTPS access to the appliance. Restrict the access to only those IP addresses from which the appliance is administered. Click **Review and Launch**.
10. Review the details in the **Review Instance** window and click **Launch**.
11. In the **Select an existing key pair or Create a new key pair** window, you can opt to **Proceed without a key pair**. Check the acknowledgment check box. Click **Launch Instances** to proceed.

    Note: You do not need to associate a key pair with the instance. If you want to log on to the console of the launched instance, log on as the **admin** user.

12. Click **NETWORK & SECURITY** > **Network Interfaces**.
    a) Click **Create Network Interface**.
    b) On the **Create Network Interface** window, select a subnet and an appropriate security group.

       Since IBM Security Identity Manager requires 3 network interface cards, you must create another network interface.

       Note: By default, only one network interface is created with every instance. This interface is the primary interface, which cannot be removed from the instance.
    c) Select a network interface. Right-click the interface and click **Change** > **Source/Dest.Check** > **Disable**.

       Repeat this step for all the interfaces.
13. Select the appliance instance and complete these steps.
    a) Right-click the appliance instance.
    b) Select **Instance State** > **Stop**.
    c) Right-click the appliance instance.
    d) Select **Networking** > **Attach Network Interface**.

       Similarly, attach another network interface and start the instance.
14. Go to **INSTANCES** > **Instances** to check the status of the appliance instance.

Microsoft Azure support

The IBM Security Identity Manager virtual appliance can be installed on Microsoft Azure.

The Security Identity Manager virtual appliance for Microsoft Azure is distributed as a preinstalled disk image of the virtual appliance in the VHD format.

Deploying Security Identity Manager on Microsoft Azure involves the following processes:

1. Creating an Azure-ready VHD or obtaining the Azure-ready VHD.
2. Uploading the Azure-ready VHD to Microsoft Azure.
3. Creating an image from the uploaded VHD.
4. Deploying the image as a new virtual machine using Azure Portal or the command line.
5. Setting up the ports for the Security Identity Manager management and application interfaces in the Azure dashboard.

Creating a custom size Azure compliant Virtual Hard Disk (VHD) file

IBM provides an Azure-compliant VHD file that can be used to deploy Security Identity Manager to Azure.

About this task

The size of the VHD file is 100 GB. If you want to use a size other than 100 GB, you can create a custom pre-installed Security Identity Manager image for Azure manually. After the Security Identity Manager installation finishes, it is not possible to resize the hard disk. This process requires a Microsoft Hyper-V environment and the Security Identity Manager firmware installation ISO.

These steps apply to Hyper-V Manager version 10 and similar.

Procedure

1. In the Hyper-V Manager, create a new virtual machine using the wizard. n the wizard, follow these steps:
    a) When prompted to Specify Generation, select the **Generation 1** option.
    b) When prompted to Assign Memory, enter 16384MB or more. This amount can be changed later after installation.

c) When prompted to Configure Networking, no network connection is required.

d) When prompted to Connect Virtual Hard Disk, create a new virtual hard disk. Set the size of the virtual disk to the desired custom size. This size can not be changed after installation finishes.

e) When prompted for Installation Options, attach the Security Identity Manager installation ISO.

2. Start the newly created virtual machine.

   a) When you start the virtual machine for the first time, press Enter to begin with the virtual appliance installation process.

   b) Select the language that you want to use during the installation.

   c) Type `yes` to continue.

3. When the installation process is complete, unmount the installation media, and reboot the VM. After it reboots, the login prompt is displayed. Do not do any configuration and shutdown the VM.

4. In the **Actions** tab, click **Edit Disk**. The Edit Virtual Hard Disk Wizard is started. In the wizard, follow these steps:

   a) When prompted to Locate Disk, select the VHD file associated with the virtual machine created earlier.

   b) When prompted to Choose Action, select the **Convert** option.

   c) When prompted to Choose Disk Format, select **VHD**. Azure does not support the VHDX format.

   d) When prompted to Choose Disk Type, select **Fixed** size. Azure does not support dynamically expanding or thin-provisioned disks.

   e) When prompted to Configure Disk, choose a new location to save the converted disk to.

5. After the Edit Virtual Hard Disk Wizard is complete, the newly converted VHD is ready to be uploaded to Microsoft Azure.

   Note:

   - The Security Identity Manager firmware must not be configured before preparing it to upload to Azure. If the machine is not in the unconfigured state when first started on Azure, it will not correctly detect the Azure environment.
   - It is possible to convert the VHD using other methods, such as the Powershell extensions for Hyper-V and qemu-img.
   - The firmware installation must take place in a Microsoft Hyper-V environment. For example, you can not install Security Identity Manager in VMware and convert it to an Azure-appropriate VHD. The hypervisor that the Security Identity Manager firmware is installed in must be the same as its intended execution environment. Microsoft Hyper-V Generation 1 is considered to be the same hardware as Microsoft Azure by the Security Identity Manager firmware.
   - For details about the VHD requirements, see the General Linux Installation Notes topic on the Microsoft Azure documentation website.

Uploading the Azure-ready VHD to Azure and creating an Azure Image

To deploy a virtual machine in Microsoft Azure, an Azure-compliant VHD file that contains the Security Identity Manager firmware must be uploaded to a storage account and then used to create an image. The created image artifact acts as a template and can be deployed multiple times.

About this task

These instructions demonstrate how to perform the steps using the Azure Portal (portal.azure.com). But you can also use the Azure CLI tools or any other Azure capable API to complete these steps.

Procedure

1. Upload the VHD file using the Azure Portal.

   a) In the Azure Portal, select Storage Accounts.

   b) Select the storage account where the Security Identity Manager VHD file will be uploaded to.

    - If you do not have a storage account, click **Add** to create one.
    - Note that the selected location will dictate where the image can be created and subsequently deployed to.

    c) Under **BLOB SERVICE**, select **Containers**.

    d) Select a container to upload the Security Identity Manager VHD file to.

    - If you do not have a storage container, click Add Container to create one.

    e) Click Upload and select the Azure-compliant Security Identity Manager VHD file to upload.

    - Ensure that the Blob type is set to Page Blob.

    This process might take a long time depending on your network connection and the location of your Azure storage account.

2. Create an image using the Azure Portal.

    a) In the Azure Portal, select **Images**.

    b) Click Add to create a new image.

        1) Give the image a name. Remember that this image is a template that will later be deployed to a virtual machine with a different name.

        2) Ensure that the location is the same as the location of your storage account.

        3) In the OS disk section:

            a) Select Linux and the OS type.

            b) Click **Browse** on the **Storage Blob** field. A new panel will list your storage accounts. Using this panel, navigate through the storage account and container to locate the Security Identity Manager VHD that was uploaded.

        4) Click **Create** to begin the image creation process. This process typically takes minutes to complete.

    c) When the process has completed, return to the Images pane and verify that the new image was created.

    This image can now be used to deploy new Security Identity Manager virtual machines in Azure.

Creating a Security Identity Manager virtual machine from an image in Azure

An image artifact in Azure can be used to create a new virtual machine in Azure. The same image can be deployed multiple times to create multiple Security Identity Manager virtual machines.

About this task

These instructions demonstrate how to perform the steps using the Azure Portal (portal.azure.com). But you can also use the Azure CLI tools or any other Azure capable API to complete these steps.

Procedure

1. In the Azure Portal, select **Images**.
2. Select the previously created Security Identity Manager image.
3. In the **Overview** pane, click **Create VM**.

    a) In the **Basics** page:

        1) Enter a name for the new virtual machine.

        2) Enter a user name, and select the **Password Authentication** type. If you provide a user name and password, or provide an SSH public key, Security Identity Manager will take no action. To login, use the default admin user.

        3) Complete the form and click **OK**.

    b) In the **Choose a size** page:

        1) Select an appropriate size for the new virtual machine, keeping in mind the recommended hardware configuration.
        2) Click **Select** to continue.
    c) In the **Disk settings** page, select **Standard HDD**.
    d) In the **Settings** page:
        1) Configure the network settings.
        2) Click **OK** to continue.
    e) In the **Summary** page, revise the configuration and click **OK** to create the Security Identity Manager virtual appliance.
4. After deployment is complete, shutdown the virtual machine and add two additional network interfaces. Boot up the virtual machine again.

What to do next
Set up the virtual appliance. See Chapter 4, “Set up the virtual appliance,” on page 65.

Setting up the Security Identity Manager ports in Microsoft Azure

When an Security Identity Manager virtual machine is deployed in Microsoft Azure, by default interface M.1 will be configured with a single DHCP IP address of the management type. The address can be used to access the LMI and SSH. The Azure fabric will assign the networks private IP address specified during deployment to this adapter using DHCP.

By default, no ports are forwarded from the public IP address to the private IP address.

You must add ports under inbound port rules for the Security Identity Manager interfaces in the Azure dashboard.

- Add the following ports to access the local management interface:
  - 22
  - 9443
  - 10443
- Add the following ports to access the application interface:
  - 9343
  - 10443
  - 11443

Additional interfaces can be configured using the Azure command line tools. The Azure Portal does not provide the capability of creating a virtual machine with more than one interface or for adding additional interfaces to an existing virtual machine.

Addresses other than the first private IP address on M.1 must be manually configured within Security Identity Manager. Configure the network settings of Security Identity Manager to match the private IP addresses configured on each adapter in Azure.

The Security Identity Manager virtual machine runs the Windows Azure Agent daemon to communicate with the Azure fabric.

- The log file can be viewed on the application log files page under `azure/waagent.log` or by viewing the **Boot Diagnostics** panel in the Azure Portal.
- The Windows Azure Agent will periodically make requests to an internal Azure endpoint (typically within 168.0.0.0/8 169.0.0.0/8) to report deployment and heartbeat status.

Unsupported functionality for Security Identity Manager in Microsoft Azure

Security Identity Manager virtual machines that are running in Microsoft Azure do not support certain features.

Security Identity Manager does not support the following deployment features:

- User creation
- SSH public key authentication
- Data disks
- Local storage SSD
- Extensions
- Guest OS Diagnostics

Security Identity Manager does not support the following runtime features:

- Disk management
- Extensions (including the Basic Metrics extension)
- Resource health reporting
- User Account Management
- Reset password

Microsoft Hyper-V support

The IBM Security Identity Manager virtual appliance can be installed on a Microsoft Hyper-V Server 2016.

The IBM Security Identity Manager virtual appliance for Microsoft Hyper-V is distributed as a pre-installed disk image of the virtual appliance in the Hyper-V VHD or VHDX formats.

Installing the virtual appliance on Microsoft Hyper-V using VHD

Use the provided image to install the virtual appliance. Follow this procedure to create a virtual machine and to start the virtual appliance setup wizard. The virtual hard disk is created in VHD format.

Procedure

1. Create a virtual machine with Microsoft Hyper-V.

   Follow these guidelines to create the virtual machine.

   - The instructions for creating a virtual machine might differ depending on your Windows version. See the Hyper-V documentation that suits your version for specific instructions.
   - Ensure that the virtual machine has enough allocated disk space to store the configuration and log file data for the appliance. Allocate at least 100 GB of disk space for the appliance.
   - Specify `Generation 1` as the virtual machine generation. The virtual appliance must be run as a `Generation 1` virtual machine. `Generation 2` virtual machines are not supported.
   - Enter the memory size. The minimum memory size is 16 GB.
   - Set the number of network connections, depending on your requirements.

     You must provision at least three network interfaces to set up the virtual machine. Only two interfaces are needed for normal operations: M.1 and P.1. The M.2 interface is used for high availability.

     First interface (eth0)
     M.1 is the first management interface (LMI).

     Second interface (eth1) - optional
     M.2 is the second management interface (LMI). It is used for high availability.

     Third interface (eth2)
     P.1 is the first application interface for the Security Identity Manager application.

- Each network adapter must be of the type `Network Adapter`. The `Legacy Network Adapter` type is not supported.
- The Hard Drive and DVD Drive must be attached to IDE Controller 0 and IDE Controller 1, respectively.

2. Start the virtual machine.

   ⚠ **Attention:** If the hard disk that is attached to the virtual machine already contains a Linux partition, the installer always runs in interactive mode.

3. Enter YES to proceed with the installation. Alternatively, if you do not want to proceed with the installation, enter NO to move to the reboot prompt.
4. Examine the installation messages to ensure that the installation was successful. After the installation process is complete, unmount the installation media and select **Enter** to reboot the appliance.

What to do next

Set up the virtual appliance. See Chapter 4, “Set up the virtual appliance,” on page 65.

Installing the virtual appliance on Microsoft Hyper-V using ISO

Use the provided image to install the virtual appliance. Follow this procedure to create a virtual machine and to start the virtual appliance setup wizard. The virtual hard disk is created in VHDX format.

Procedure

1. In the Hyper-V Manager, create a new virtual machine using the wizard. In the wizard, follow these steps:
   a) When prompted to Specify Generation, select the **Generation 1** option.
   b) When prompted to Assign Memory, enter 16384MB or more. This amount can be changed later after installation.
   c) When prompted to Configure Networking, no network connection is required.
   d) When prompted to Connect Virtual Hard Disk, create a new virtual hard disk. Set the size of the virtual disk to the desired custom size. This size can not be changed after installation finishes.
   e) When prompted for Installation Options, attach the Security Identity Manager installation ISO.
   f) Attach 2 more network adapters to the virtual machine, so that there is a total of 3 network adapters.

   You must provision at least three network interfaces to set up the virtual machine. Only two interfaces are needed for normal operations: M.1 and P.1. The M.2 interface is used for high availability.

   First interface (eth0)
   M.1 is the first management interface (LMI).

   Second interface (eth1) - optional
   M.2 is the second management interface (LMI). It is used for high availability.

   Third interface (eth2)
   P.1 is the first application interface for the Security Identity Manager application.
2. Start the newly created virtual machine.
   a) When you start the virtual machine for the first time, press `Enter` to begin with the virtual appliance installation process.
   b) Select the language that you want to use during the installation.
   c) Type `yes` to continue.
3. When the installation process is complete, unmount the installation media, and reboot the virtual machine. After it reboots, the login prompt is displayed.

   The installation is completed.

What to do next

Set up the virtual appliance. See Chapter 4, “Set up the virtual appliance,” on page 65.

KVM support

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

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

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

Hardware requirements

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

Software requirements

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

Installing the virtual appliance with KVM

Install the virtual appliance with KVM.

Procedure

1. Run the **`virt-manager`** command to open the **Virtual Machine Manager**.
2. Click **Create a New Virtual Machine**.
3. On the wizard, enter a name for the virtual machine.
4. Select **Local install media (ISO image or CDROM)**.
5. Click **Forward**.
6. Select **Use ISO image** and click **Browse** to select the product ISO file.
7. Select the operating system as Linux with Version Generic 3.x kernel.
8. Click **Forward**.
9. Enter the memory size.
   For example, 16 GB.
10. Set the number of CPUs.
    For example, 8.
11. Click **Forward**.
12. Enter the disk size of the virtual machine.
    For example, 100 GB.

    Note: Only half of the allocated disk space is available to the virtual appliance. The virtual appliance has two partitions; Partition 1 and Partition 2. Either partition can be active and the disk space is divided equally among the two partitions. For example, if the allocated disk space is 100 GB then Partition 1 has 50 GB and Partition 2 has 50 GB disk space. Since only one partition can be active at a time, only 50 GB disk space is available to the virtual appliance.
13. Click **Forward**.
14. Select the network bridge.
15. Select **Customize configuration before install**.
16. Click **Finish**.

17. Click **Add Hardware**.
18. Select **Network**.
19. Select the network bridge and click **Finish**.
20. Click **Add Hardware** again.
21. Select **Network**.
22. Select the network bridge and click **Finish**.
23. On the KVM console, follow the steps to complete the installation.
24. Press Enter key after the disk partitioning and installation is complete.

    Wait for the appliance login prompt to be displayed.
25. Provide the following user credentials when the system restarts after the virtual appliance installation.
    - **Unconfigured login**: `admin`
    - **Password**: `admin`

Results

Proceed with setting up the initial virtual appliance. See "Setting up the initial IBM Security Identity Manager virtual appliance" on page 58.

VMware support

The IBM Security Identity Manager virtual appliance can be installed on a VMware ESXi hypervisor.

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

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

Setting up the virtual machine

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

Procedure

1. Download the `isim_*.iso` build.
2. Create a virtual machine on ESXi 5.x with the following configuration.

   a) Select **Custom**.

   b) Provide a name for the virtual machine.

   c) Choose the destination storage for this virtual machine.

   d) Set virtual machine version to 8 or later.

   e) For the IBM Security Identity Manager virtual appliance, set the guest operating system to Linux. Under **Version**, select **Other 3.x Linux (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.

   Note: Only half of the allocated disk space is available to the virtual appliance. The virtual appliance has two partitions; Partition 1 and Partition 2. Either partition can be active and the disk space is divided equally among the two partitions. For example, if the allocated disk space is 100 GB then Partition 1 has 50 GB and Partition 2 has 50 GB disk space. Since only one partition can be active at a time, only 50 GB disk space is available to the virtual appliance.

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" on page 58.

Setting up the initial IBM Security Identity Manager virtual appliance

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

Procedure

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

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

Select option: 4


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

Select option: 1
```

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

```
FIPS 140-2 Mode Configuration

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

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

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

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

Select option: 1


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

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

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

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

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

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

   Set a strong password. It must be at least 8 characters and contain one uppercase and one lowercase character, one numerical character, and one special character. You can try special characters such as !, @, #, or %. The special character cannot be any of the following symbols : <, >, `, &, $, \, ", :, and |.

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

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


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


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

Select option: n
```

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

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


Select option: 1

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


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

Select option: n
```

7. Change the host name.

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

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

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

Select option: n
```

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

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

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

Select option: 3

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

9. Configure the DNS for the virtual appliance.

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

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

Select option: 1

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


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

Select option: n
```

10. Configure the time settings for the virtual appliance.

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

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

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

Select option: n
```

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

Results

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

What to do next

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

XenServer support

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

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

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

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

Installing the virtual appliance by using XenCenter

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

Before you begin

Make sure that you have the following prerequisites:

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

Procedure

1. In the XenCenter console, expand the XenCenter icon on the left.
2. Right-click the attached hypervisor and select **Import**.
3. In the **Import Source** window:
   a) Click **Browse**.
   b) Select the VHD image to be imported and click **Open**.

    c) Click **Next**.

4. In the **VM Definition** window:

    a) Specify the name, number of CPUs, and memory of the virtual machine.

    Note: In most scenarios, assign the virtual machine at least one processor and 2 GB of memory. These settings can be adjusted after the virtual machine starts running.

    b) Click **Next**.

5. In the **Location** window:

    a) Select the destination hypervisor from the drop-down list on the right.

    b) Click **Next**.

6. In the **Storage** window:

    Note: Only half of the allocated disk space is available to the virtual appliance. The virtual appliance has two partitions; Partition 1 and Partition 2. Either partition can be active and the disk space is divided equally among the two partitions. For example, if the allocated disk space is 100 GB then Partition 1 has 50 GB and Partition 2 has 50 GB disk space. Since only one partition can be active at a time, only 50 GB disk space is available to the virtual appliance.

    a) Select **Place imported virtual disks onto specified target SRs**.

    b) Click **Next**.

7. In the **Networking** window:

    a) Select the network to be used for the first management interface.

    b) Click **Next**.

8. In the **OS Fixup Settings** window:

    a) Select **Don't use Operating System Fixup**.

    b) Click **Next**.

9. In the **Transfer VM Settings** window:

    a) Specify the settings to suit your network environment.

    Note: A valid IP address, subnet, and gateway is required.

    b) Click **Next**.

10. In the **Finish** window, click **Finish** to start the import.

    Note: The import operation might take a considerable amount of time to complete. You can click the **Logs** tab to check the progress of the import.

11. Start the imported virtual machine.

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

Chapter 4. Set up the virtual appliance

Use the following tasks to set up the virtual appliance.

Managing the index page

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

Before you begin

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

Procedure

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

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

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

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

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

   For more information, see "Configuring the IBM Security Identity Manager by using the initial configuration wizard" on page 66.

   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 67.

   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 69.

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 58.
- Collect the following information that is associated with the tasks you are about to do:
  1. Setup mode selection

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

  You can download a sample configuration file from the page.

About this task

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

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

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

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

Procedure

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

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

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

Option	Description
Guided Configuration	Define the configuration details a step at a time with the wizard. To continue, go to step "4" on page 66.
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" on page 67.

4. From the **Application Interfaces Configuration** page, configure the application interfaces and click **Next page**.

For more information about application interfaces, see Managing the application interfaces.

Note:

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

5. Configure the mail server and click **Next page**.

   For more information about application interfaces, see Managing the mail server configuration.
6. Configure the database settings for the `Identity data store` and click **Next page**.

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

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

   Guided Configuration

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

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

   Advanced Configuration

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

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

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

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

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

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

Before you begin

Configure the initial virtual appliance settings.

About this task

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

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

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

Procedure

1. In the **Connect to Primary** tab of the **Setup Progress** page, provide the details of the primary node.

a) Type the host name in the **Primary node host name** field.
This host name must be the fully qualified domain name. For example, `isimva1.jk.example.com`.

The primary node host name must be same that was used to create the primary virtual appliance host name.

b) Type the user ID in the **Primary node administrator** field.
The user ID must be the same ID that you used to log on to the IBM Security Identity Manager virtual appliance For example, `admin`.

c) Type the password in the **Primary node administrator password** field.
For example, `admin`.

2. Click **Test Connection** to validate the details and to verify this connection of the member node with the primary node.

   The system notifies you that the connection to the primary node was successful.

   Note: If you modified any of the parameters in the Advanced Tuning Parameters panel for the Primary node, ensure that the same modifications are also applied to the member node before you complete any other steps. For more information, see Advanced tuning parameters.
3. 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.
4. From the **Application Interfaces Configuration** page, configure the application interfaces.

   For more information about application interfaces, see Managing the application interfaces.

   Note:

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

   The **Completion** tab is displayed.
6. 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.
7. Optional: To review or edit the data in the **Connect to Primary** tab, click **Previous page**.
8. 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. The backup node helps the administrator to recover from any primary node failures or disasters. Recover to a new primary node with the same configurations and customizations as the earlier primary node by using the following steps:

1. Apply a snapshot of the primary node on the backup node.
2. Download the primary node snapshot from the backup node.
   - Create a IBM Security Identity Manager virtual appliance system with the same details as the earlier primary node.
   - During the IBM Security Identity Manager virtual appliance installation, select the option to set the system as the primary node. Do not configure any mode selections or appliance interface configurations.
   - Apply the snapshot by using the snapshot option that is available on the left pane of the configuration page.

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 is 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 virtual appliance console.
2. In the **Quick Links** widget of the **Appliance Dashboard**, click a console link to open the application. The administrative console links that you can view are as follows:

   - Identity Administration Console
   - Identity Service Center

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

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

Chapter 5. Upgrade the virtual appliance

Use the following tasks to upgrade the virtual appliance.

Before you begin

Start the **Appliance Dashboard**, and verify the status of the following entries:

- Cluster Manager Server and Security Identity Manager Server must be started.
- Identity data store and Directory Server status must be started.
- IBM Security Identity Manager application must be up and running.
- With the **Notifications** widget, ensure that there are no pending notifications. For clustered environments, all member nodes must be available and in a synchronized state.
- If Identity External User Registry, Single Sign-On and other features are configured, then ensure that it is in a working configuration.

Note: Direct upgrades from IBM Security Identity Manager, Version 7.0.0 to the latest version of IBM Security Identity Manager is not supported. You must first upgrade from IBM Security Identity Manager, Version 7.0.0 to IBM Security Identity Manager, Version 7.0.1. Then, upgrade from IBM Security Identity Manager, Version 7.0.1 to the latest version of IBM Security Identity Manager.

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

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

Before you begin

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

About this task

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

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

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

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

Procedure

1. Download the `isim_*.zip` package from the IBM Fix Central.
2. Extract the `isim_*.pkg` build to a location of your choice.
3. Access the command-line interface (CLI) of the virtual appliance with either an `ssh` session or the console.
4. Copy the `isim_*.pkg` to a USB device.
5. Attach the USB device to your virtual system.

© Copyright IBM Corp. 2019, 2020

6. In the virtual appliance CLI, run the **isim** command to display the `isim` prompt.
7. Choose from either of the following steps depending upon the version.
   - For upgrade from IBM® Security Identity Manager virtual appliance 7.0.1 or later, complete these steps.
     a. At the `isim` prompt, run the **upgrade** command.
     b. Run the **list** command to list the firmware updates.
     c. Run the **transfer** command to transfer the firmware updates to the virtual system.

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

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

   The results are as follows:

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

   The results are as follows:

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

    Do the following actions:

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

    Partition 1 now becomes the active partition.

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

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

Before you begin

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

About this task

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

Procedure

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

   Usage:

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

   Example:

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

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

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

   Note: Run this command after you transfer the `.pkg` file.

   - For upgrade from IBM® Security Identity Manager virtual appliance 7.0.1 or later, run this command:

     ```
     isim > upgrade > install
     ```

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

     ```
      isim > firware_update > install_firmware
     ```

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

   The results are as follows:

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

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

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

9. Type the **`reboot`** command and press Enter to restart the virtual system.

   Partition 2 is now the active partition.

   The results are as follows:

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

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

10. For the Identity data store, clear the **Service Integration Bus** before you restart the IBM Security Identity Manager. See Clear the service integration bus.
11. Restart the IBM Security Identity Manager.
12. Configure the application interface only after you upgrade the primary node and all member nodes.

    You must configure application interface on the primary node first and then on the member nodes. For more information, see Managing the application interfaces.

13. Optional: Back up Partition 2 in to Partition 1 after the successful completion of the firmware upgrade.

    The backup process overwrites the information that is in Partition 1.

    Do the following actions:

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

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

    Partition 1 now becomes the active partition.

Chapter 6. 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.

Related concepts

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.

Group settings
You can select to modify the group properties automatically.

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.

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.

© Copyright IBM Corp. 2019, 2020

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.

Related concepts

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

Group settings
You can select to modify the group properties automatically.

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.

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.

Related concepts

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

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.

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.

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**.

Related concepts

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

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.

Group settings
You can select to modify the group properties automatically.

Chapter 7. 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.

Related concepts

Login behavior
Click **Set Systems Security** > **Configure Forgotten Password Settings**, to modify the login properties.

Challenge behavior
Click **Set Systems Security** > **Configure Forgotten Password Settings** to modify the challenge properties.

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.

Related concepts

Forgotten password authentication
Click **Set Systems Security** > **Configure Forgotten Password Settings** to modify forgotten password authentication.

Challenge behavior

© Copyright IBM Corp. 2019, 2020

Click **Set Systems Security** > **Configure Forgotten Password Settings** to modify the challenge properties.

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.

Related concepts

Forgotten password authentication
Click **Set Systems Security** > **Configure Forgotten Password Settings** to modify forgotten password authentication.

Login behavior
Click **Set Systems Security** > **Configure Forgotten Password Settings**, to modify the login properties.

Chapter 8. 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 1.8.x version over 1.8.0 to work. Alternatively, Security Identity Manager can use static versioning of the Java plug-in.

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:
  a) 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.

  b) Register the Java plug-in with the browser.

© Copyright IBM Corp. 2019, 2020

Chapter 9. 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 17. 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\V6.4\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.

© Copyright IBM Corp. 2019, 2020

What to do next

Continue with "Verifying access for the administrator account" on page 86.

Verifying access for the administrator account

Verify that the administrator account is configured correctly.

About this task

Ensure that IBM Security Identity Manager administrator can successfully log in by authenticating with the external user registry

Procedure

1. Log on to the IBM Security Identity Manager administration console

   Access the default URL, where `hostIP` is the IP address or fully qualified domain name of the server that runs IBM Security Identity Manager:

   ```
   http://hostIP:9080/itim/console
   ```

2. Use the administrator name that you specified during the IBM Security Identity Manager installation.

   The default administrator account is `ITIM Manager`, but you had the option of specifying a different name.

3. Enter the password you specified for your administrator account.

   The default password is `secret`.

Results

If you can log in successfully by supplying the password you used for the default administrator user, then you successfully configured the LDAP user registry as an external authentication user registry for IBM Security Identity Manager.

Appendix A. 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" on page 28 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" on page 87.

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.*

© Copyright IBM Corp. 2019, 2020

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

IBM®