IBM Security Identity Manager
Version 6.0.0.4

Installation Topics

IBM Security Identity Manager
Version 6.0.0.4

Installation Topics

Table of contents

Table list

Part 1. Installation

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

Chapter 1. IBM Security Identity Manager components

You must install and configure components for IBM® Security Identity Manager.

To determine the supported release levels and fix pack specifications, see *Software prerequisites* on the IBM Security Identity Manager product documentation site. Specifications are provided for operating systems and components.

IBM Security Identity Manager provides lifecycle management of user accounts on remote resources with adapters to provide communication.

The IBM Security Identity Manager product:

- Provides user accounts to authorized users on one or more resources to which IBM Security Identity Manager adapters are connected
- Runs in a WebSphere® Application Server environment, either in a single-server or a cluster configuration
- Stores historical and pending data in a database server
- Stores user account and organizational data in an LDAP directory server
- Stores IBM Security Identity Manager information for auditing and reporting in the database
- Provides administration from a client interface in a web browser. The interface communicates through an HTTP server and WebSphere Web Server plug-in or a WebSphere Application Server embedded HTTP transport

IBM Security Identity Manager requires the installation and configuration of the components described in the following sections.

Database server products

IBM Security Identity Manager stores transactional and historical data in a database server. For example, the IBM Security Identity Manager provisioning processes use a relational database to maintain their current state and their history.

Computers that communicate with the database require a Java™ Database Connectivity driver (JDBC driver). For example, a JDBC driver enables an IBM Security Identity Manager server to communicate with the data source. IBM Security Identity Manager supports a JDBC type 4 driver to connect a Java-based application to a database.

The supported database products are IBM DB2® database, Oracle database and MS SQL Server database.

.

For more information about supported database server products, see Database server support.

Directory server products

IBM Security Identity Manager stores the current state of managed identities in an LDAP directory, including user account and organizational data.

IBM Security Identity Manager supports the following products:

- IBM Security Directory Server.
- Oracle Directory Server Enterprise Edition

For more information about supported directory server products, see Directory server support.

IBM Security Directory Integrator

IBM Tivoli® Directory Integrator is an optional installation component that synchronizes identity data in different directories, databases, and applications.

IBM Tivoli Directory Integrator synchronizes and manages information exchanges between applications or directory sources.

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

WebSphere Application Server

The WebSphere Application Server is the primary component of the IBM Security Identity Manager environment. The WebSphere Application Server runs a Java virtual machine, providing the runtime environment for the enterprise application code.

The application server provides containers that specialize in running specific Java application components.

An HTTP server and WebSphere Web Server plug-in

An HTTP server is an optional component that provides administration of Security Identity Manager through a client interface in a web browser.

Security Identity Manager requires the installation of a WebSphere Web Server plug-in with the HTTP server. WebSphere Application Server provides separate installers to install the IBM HTTP Server and WebSphere Web Server plug-in. You can install these components either with the WebSphere Application Server or on a separate computer.

Note: If an HTTP server is used, you must map the Security Identity Manager applications to the HTTP web server name. Use the WebSphere Application Server administrative console to map. For more information about mapping the applications, see "Mapping the IBM Security Identity Manager application" on page 122.

IBM Security Identity Manager Server

The Security Identity Manager Server and its adapters provision identities to a set of heterogeneous resources.

These resources might be operating systems, data stores, or other applications.

Security Identity Manager Adapters

Security Identity Manager adapters enable the Security Identity Manager Server to connect to a set of heterogeneous resources. These resources can be operating systems, data stores, or other applications, to provision identities.

Chapter 2. Installation planning for deployments

To prevent initial deployment problems, consider providing a variation of the following planning activities that are appropriate for your site. Plan before installing IBM Security Identity Manager and subsequent fix packs.

- Establish a working practice that provides comprehensive and relevant IBM Security Identity Manager information to all the specialists who install middleware. For example, have the team meet regularly to enumerate their problems and share their solutions.
- To ensure coordination, designate one person as a focal point for concerns that flow between your site and IBM customer support specialists.
- If possible, reduce the number of specialists who install and configure the applications. Encourage communication flow between specialists in the following ways.
  - Provide a comprehensive library or list of FTP servers and websites for prerequisite installation and configuration information.
  - Ensure that the specialists who install IBM Security Identity Manager have root or Administrator authority for the prerequisite middleware on the middleware servers.
  - Ensure that all elements of the system or solution have sufficient privileges to provide accounts.
  - Support a centralized problem and solution database that identifies troubleshooting actions and assigns action owners.
  - Maintain a common library of scripts that automate the start processes.
  - Create a change control database that coordinates all customization activities.
  - Determine a working practice in which specialists provide a record of critical values of configuration parameters like the ones that this publication provides. Ensure that all specialists have access and use a common worksheet that centralizes the information.

    For example, each installation chapter in this manual provides a checklist of prerequisites that must be installed, configured, and running before you begin installation. Additionally, “Security configuration of the directory server” on page 143 provides a centralized collection point for critical values such as user IDs, passwords, and security settings. For more information about prerequisite levels and fix packs or patches, see *Software prerequisites* on the IBM Security Identity Manager product documentation site.

WebSphere security configuration

IBM Security Identity Manager requires that WebSphere Application Server administrative security and application security are enabled.

Administrative security

The default installation for WebSphere Application Server configures administrative security as part of global security. If you are installing a new WebSphere server, accept the default setting to enable administrative security. If you plan to use an existing WebSphere Application Server for which administrative security is turned off, you must enable it before installing IBM Security Identity

Manager. The IBM Security Identity Manager installation program verifies that administrative security is on.

Application security

Application security must be turned on for the application server in which IBM Security Identity Manager is deployed. There are different ways to enable application security for the application server that hosts IBM Security Identity Manager, based on whether you configure a security domain.

If a security domain *is not* configured for IBM Security Identity Manager, you must turn on application security for global security.

If a security domain *is* configured for IBM Security Identity Manager:

- If the application security setting for global security is turned *off*, you must turn on application security for the security domain.
- If the application security setting for global security is turned *on*, you can use the application security setting from global security. Optionally, you can also turn on application security for the security domain.

Java 2 Security

IBM Security Identity Manager provides an installer that configures the IBM Security Identity Manager security domain. This installer requires that Java 2 Security is disabled in the WebSphere Global Security settings. If Java 2 Security must be enabled to meet other requirements, you can modify the `server.policy` file to grant IBM Security Identity Manager JAR files permission to be in `WAS_PROFILE_HOME/classes`.

To grant the permission, open the `WAS_PROFILE_HOME/properties/server.policy`, on either a single server or on a cluster setup node, and add this statement:

```
grant codeBase "file:${user.install.root}/classes/-" {
      permission java.security.AllPermission;
    };
```

Note: After the IBM Security Identity Manager installation is complete, you must remove the changes you made to the `server.policy` file.

Custom registry

IBM Security Identity Manager provides a default *custom registry*. You do not have to use this registry for authentication. You can choose to use an *external registry*. An external user registry is any other registry that can be configured with WebSphere Application Server. You can use an existing registry or configure a new one.

The IBM Security Identity Manager installation program prompts you whether you want to use the custom registry.

- If you use the custom registry, the IBM Security Identity Manager installation program programmatically creates a security domain, enables application security, and configures it to the IBM Security Identity Manager custom registry.
- If you use an external registry, you must manually configure application security. This installation guide provides instructions for how to complete the configuration. If you want to use an external registry:

1. Before installing IBM Security Identity Manager, complete the instructions in "Preinstall configuration for authentication with an external user registry" on page 69.
2. During the IBM Security Identity Manager installation, choose *not* to use the custom registry.
3. After installing IBM Security Identity Manager, complete the instructions in "Postinstall configuration of an external user registry for authentication" on page 156.

Configuration options

Security Identity Manager can be configured in either a single-server or a clustered environment.

Before you install Security Identity Manager, you must determine how to configure WebSphere Application Server either in a single-server or a clustered configuration.

Single-server configuration

A single-server configuration contains the WebSphere Application Server base server and Security Identity Manager on one computer. Other required applications can run on the same computer or a different computer. You must ensure that the computer has the required memory, speed, and available disk space to meet the workload.

A single-server configuration requires the following components and products:

- A database server
- A directory server
- IBM Tivoli Directory Integrator (optional)
- WebSphere Application Server base server
- Security Identity Manager Server
- Security Identity Manager Adapters

Clustered configuration

A cluster configuration contains WebSphere Application Server profiles, which are logical groups of one or more application servers on computers. Profiles within an administrative domain called a cell, which the deployment manager manages. A profile agent manages all managed processes on the profile by communicating with the deployment manager to coordinate and synchronize the configuration. The deployment manager is the administrative process that provides a centralized management view and control for all elements in the cell, including the management of clusters.

Security Identity Manager assumes that the operating system is the same for each cluster member.

For example, all Security Identity Manager cluster members run on the IBM AIX® operating system. To avoid problems with identity feeds, do not use more than one operating system type within an Security Identity Manager cluster.

Security Identity Manager supports both horizontal and vertical cluster configurations, where each clustered node hosts one or more application servers.

Each node consists of one computer, controlled by a deployment manager on a separate server. The remaining applications are configured on additional computers.

Ensure that the system clocks of all the servers in your WebSphere Application Server clustered environment are synchronized to within 5 minutes of the deployment manager server. The servers must also be set to the same time zone. For information about synchronizing the servers, see the WebSphere product information at http://pic.dhe.ibm.com/infocenter/wasinfo/v8r5/index.jsp and search on `system clocks`.

Example

This task is an example cluster configuration:

- On the computer where you want to have the deployment manager, install the following components and products:
  - The WebSphere Application Server deployment manager
  - A JDBC driver, if required
  - The Security Identity Manager Server
- A cluster member is an instance of aWebSphere Application Server cluster. On *each* cluster member, install the following components and products:
  - WebSphere Application Server base server
  - Security Identity Manager Server
  - A JDBC driver, if required
- On one or more additional computers that can be in or out of the cluster, install the following components and products:
  - A database server
  - A directory server
  - IBM Tivoli Directory Integrator (optional)
  - An IBM HTTP Server and WebSphere Application Server plug-in (optional)

    For WebSphere Application Server 8.5, if you optionally use the HTTP server and plug-in, you also need to install the WebSphere Customization Toolbox. It is required for configuration of the plug-in that the HTTP Server uses. For information about how to install WebSphere Customization Toolbox, see Installing and using the WebSphere Customization Toolbox.

This task is an example configuration only. A topology might configure these components on computers that are all inside the cluster. The deployment manager might be installed on the same computer as the WebSphere Application Server base server. You must ensure that the computer has the required memory, speed, and available space to meet the additional load.

Chapter 3. Installation preparation

The installation process includes a sequence of installing and configuring the Security Identity Manager components. Before you install the Security Identity Manager Server, the prerequisite components must already be installed and configured.

The Security Identity Manager Server requires the following components:

- A database
- A directory server
- Tivoli Directory Integrator (optional)
- WebSphere Application Server

Follow the instruction in the next sections to ensure that you meet all the installation requirements.

Preinstallation roadmap

The preinstallation consists of a collection of activities that install and configure the components necessary for the installation of Security Identity Manager.

The major tasks to preinstall and test IBM Security Identity Manager are:

1. Determine the IBM Security Identity Manager Server topology. The information in this chapter describes the major configuration choices.
2. Ensure that the operating system of each physical server is at the level that IBM Security Identity Manager requires. For more information about software and hardware requirements, see *Hardware and software requirements* on the IBM Security Identity Manager product documentation site.
3. Ensure that the database server is installed and preconfigured. See "Database installation and configuration" on page 15 for steps to prepare the database.
4. Ensure that the directory server is installed and preconfigured. See "Installation and configuration of a directory server" on page 36 for steps to prepare the directory server.
5. Ensure that IBM Security Directory Integrator is installed and preconfigured if you decide to use it. See "Optionally installing IBM Security Directory Integrator" on page 47 for steps to prepare IBM Tivoli Directory Integrator.
6. Determine that the WebSphere Application Server is ready. See "Installation and configuration of WebSphere Application Server" on page 51 for steps to prepare the WebSphere Application Server in a single-cluster or cluster configuration.

Downloading Security Identity Manager

Security Identity Manager can be downloaded from IBM Passport Advantage®.

Before you begin

Ensure that you have a customer account number and password for IBM Passport Advantage.

About this task

Go to the Security Identity Manager download page:

Downloads

Procedure

1. Click the tab for your operating system.
2. After reviewing the packages, scroll down to the "Download package" table.
3. Click the download option. You are taken to the IBM Passport Advantage page.
4. Log in and follow the instructions.

What to do next

Install and configure the prerequisite components.

Fix pack downloads

You can download fix packs from the IBM Security Identity Manager Support website.

IBM Security Identity Manager fixes and information about fix pack installation are available at this website: Downloads.

Setting the SOAP timeout interval before fix pack installation

Installing fix packs requires a sufficient time interval to avoid timeout exceptions.

Before you begin

To avoid timeout exception errors during fix pack installation, before every fix pack installation, set the SOAP timeout interval to at least 15 minutes (900 seconds).

Note: If the interval is not sufficient, you can use an interval of 0 (zero), which specifies that the timeout interval is unlimited.

Procedure

1. Edit the `soap.client.props` file. This file is in the *`WAS_HOME`*`\profiles\`*`profile_name`*`\properties` directory.
2. Set the `com.ibm.SOAP.requestTimeout` property to 0. For example,
   `com.ibm.SOAP.requestTimeout=0`
3. Save the changes to the file.

What to do next

Install the fix pack if applicable.

Chapter 4. Installation of prerequisite components

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

Configuring a Red Hat Linux server

If you are installing on Red Hat Linux Enterprise 6.0 or 5.0, you must complete configuration tasks before you install IBM Security Identity Manager.

About this task

Before you install IBM Security Identity Manager, ensure that you disable Security Enhanced Linux (SEL). The installer might fail because of SEL default policy restrictions. Also, verify that you have the correct Linux packages installed.

For more recent information about installing Red Hat Linux Enterprise version 5.0 or 6.0, go to the WebSphere Application Server section of the IBM Knowledge Center. Search on *Preparing Linux systems for installation*.

Procedure

1. To determine whether Security Enhanced Linux is installed and running in an enforcement mode, run the **sestatus** command or check the `/etc/sysconfig/selinux` file. To disable SEL, choose one of the following actions:
   - Set SEL in permissive mode and run the **setenforce 0** command as a superuser.
   - Modify the `/etc/sysconfig/selinux` file, and restart the computer.
2. Run the **rpm -qa | grep** *package_name* command for each of the following packages to ensure that they are installed.

   Note: These packages must be present on the system for IBM Security Identity Manager and its prerequisite middleware to install correctly.

Table 1. Packages that are required for installation on Red Hat 6.0

Minimal required package level	WebSphere Application Server 7.0	WebSphere Application Server 8.5
compat-libstdc++-33-3.2.3-69	✓	✓
compat-db-4.6.21-15	✓	✓
gtk2-2.18.9-4	✓	✓
gtk2-engines-2.18.4-5	✓	✓
libXp-1.0.0-15.1	✓	✓
libXmu-1.0.5-1	✓	✓
libXtst-1.0.99.2-3	✓	✓
pam-1.1.1-4	✓	✓
rpm-build-4.8.0-12	✓	✓
elfutils-0.148-1	✓	✓

Table 1. Packages that are required for installation on Red Hat 6.0 (continued)

Minimal required package level	WebSphere Application Server 7.0	WebSphere Application Server 8.5
elfutils-libs-0.148-1	✓	✓
libXft-2.1.13-4.1	✓	✓
ksh-20100621-2	✓	✓
libstdc++-4.4.4-13		✓

Platforms that support both 32-bit and 64-bit applications require both the 32-bit and 64-bit versions of these packages:

Table 2. Packages that are required to support 32 and 64-bit applications

Minimal required package level	WebSphere Application Server 7.0	WebSphere Application Server 8.5
compat-libstdc++-33-3.2.3-69	✓	✓
compat-db-4.6.21-15	✓	✓
gtk2-2.18.9-4	✓	✓
gtk2-engines-2.18.4-5	✓	✓
libXp-1.0.0-15.1	✓	✓
libXmu-1.0.5-1	✓	✓
libXtst-1.0.99.2-3	✓	✓
pam-1.1.1-4	✓	✓
libXft-2.1.13-4.1	✓	✓
libstdc++-4.4.4-13		✓
libgcc_s.so.1		✓
libgtk-x11-2.0.so.0		✓
libpk-gtk-module.so		✓
libcanberra-gtk-module.so		✓

If you are installing on Red Hat Linux Enterprise 5.0, run the **rpm -qa | grep** *package_name* command for each of the following packages to ensure that they are installed.

Table 3. Packages that are required for installation on Red Hat 5.0

Minimal required package level	WebSphere Application Server 7.0	WebSphere Application Server 8.5
compat-libstdc++-33-3.2.3-61	✓	✓
compat-db-4.2.52-5.1	✓	✓
gtk2-2.18.9-4	✓	✓
gtk2-engines-2.18.4-5	✓	✓
libXp-1.0.0-8	✓	✓
libXmu-1.0.2-5	✓	✓
libXtst-1.0.1-3.1	✓	✓
pam-0.99.6.2-3.26.e15	✓	✓

Table 3. Packages that are required for installation on Red Hat 5.0 (continued)

Minimal required package level	WebSphere Application Server 7.0	WebSphere Application Server 8.5
rpm-build-4.4.2.37.*architecture*.e15 or later	✓	✓
libXft-2.1.10-1.1	✓	✓
libstdc++-4.1.2-48		✓
ksh-20080202-14		✓

Platforms that support both 32-bit and 64-bit applications require both the 32-bit and 64-bit versions of these packages:

Table 4. Packages that are required to support 32 and 64-bit applications

Minimal required package level	WebSphere Application Server 7.0	WebSphere Application Server 8.5
compat-libstdc++-33-3.2.3-61	✓	✓
compat-db-4.2.52-5.1	✓	✓
gtk2-2.18.9-4	✓	✓
gtk2-engines-2.18.4-5	✓	✓
libXp-1.0.0-8	✓	✓
libXmu-1.0.2-5	✓	✓
libXtst-1.0.1-3.1	✓	✓
pam-0.99.6.2-3.26.e15	✓	✓
libXft-2.1.10-1.1	✓	✓
libstdc++-4.1.2-48		✓

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
- Micorsoft SQL Server 2008

For more information about supported database releases and required fix packs, see Database server support.

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 5. Typical database worksheet

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

Before you install the database product

Before you install the database product, you must:

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

    Not required.
  - Solaris
  - Linux (Red Hat and SUSE)

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

    Not required.

Installation and configuration of the IBM DB2 database

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

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

DB2 installation

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

User data

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

User names and passwords on UNIX and Linux systems

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

Table 6. DB2 database typical configuration parameters on UNIX and Linux systems

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

User names and passwords on Windows systems

The following table shows the default values that are created on Windows systems. If you choose not to use the middleware configuration utility to create a DB2 instance, installing DB2 can also create the default DB2 instance. For more information about using the middleware configuration utility, see "Running the middleware configuration utility" on page 19.

Table 7. 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:`

Installation of the required fix packs

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

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

Did you create a DB2 instance during installation	Windows operating system	UNIX and Linux operating systems

Yes	Enter the **db2level** command from the DB2 command window:
	`db2level`
		Log on with the DB2 instance user ID and enter the **db2level** command:
		`su - DB2_instance_ID`
		`db2level`

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

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

Verify the DB2 installation.

Verifying the installation

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

Before you begin

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

Procedure

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

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

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

IBM DB2 database configuration

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

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

The middleware configuration utility:

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

The middleware configuration utility can be run manually or silently. For more information about silent configuration, see “Configuring DB2 silently” on page 22.

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

Running the middleware configuration utility:

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

Before you begin

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

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

```
umask 022
```

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

Procedure

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

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

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

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

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

6. From the IBM DB2 Database Configuration Options page, provide the following information, and then click **Next**
   - DB2 administrator ID or instance name

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

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

     Type the password again.
   - DB2 server database home

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

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

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

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

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

     Type the password again.
   - Group for the DB2 administrator

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

   Note: The dollar sign ($) has special meaning in the installer frameworks that are used by the middleware configuration utility. Avoid $ in any field values. The installer framework or operating system platform might do variable substitution for the value.
7. If you changed the default DB2 instance name, or if a DB2 instance exists with that name, you are prompted with a warning message. If you are using the DB2 instance only for IBM Security Identity Manager, click **Yes**. Do not share the instance with another program.
8. Review your configuration options before you click **Next** to begin the configuration process.
9. The configuration can take up to several minutes to complete. After the configuration completes successfully, click **Finish** to exit the deployment wizard. This step concludes the middleware configuration process for DB2 Database.

What to do next

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

Configuring DB2 silently:

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

Before you begin

Verify that the DB2 database is installed correctly.

Procedure

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

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

   Where `cfg_itim_mw` is:

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

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

What to do next

Verify the service listening port and service name.

Manual configuration of the DB2 server:

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

Configuring the DB2 server requires the following steps:

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

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

Creating a user on Windows and UNIX systems:

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

Before you begin

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

About this task

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

To create a user, follow these steps:

Procedure

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

What to do next

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

Create the Security Identity Manager database.

Creating a user on a Linux system:

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

Before you begin

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

About this task

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

Procedure

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

- Use the console command interface to enter the command:

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

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

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

The Add User window opens.

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

What to do next

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

Create the IBM Security Identity Manager database.

Creating the Security Identity Manager database:

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

Before you begin

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

Procedure

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

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

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

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

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

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

What to do next

Confirm that TCP/IP communication is specified.

Ensuring that TCP/IP communication is specified:

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

Before you begin

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

Procedure

Enter the command:

```
db2set -all DB2COMM
```

A list of values is returned.

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

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

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

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

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

What to do next

Install and configure another component.

Determining the correct service listening port and service name:

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

Before you begin

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

About this task

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

The DB2 default instance differs depending on your operating system.

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

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

Procedure

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

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

Look for the SVCENAME attribute to locate the service name.

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

   The services file has the following path:

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

DB2 database performance tuning tasks

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

Configuring TCP KeepAlive settings:

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

Before you begin

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

Procedure

1. Log in as a system administrator.
2. Run these commands on the computer where your DB2 Server is.
   - On the Linux operating system, enter these commands:

     ```
     echo 30 >  /proc/sys/net/ipv4/tcp_keepalive_intvl
     echo 30 > /proc/sys/net/ipv4/tcp_keepalive_time
     ```

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

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

   ```
   # /etc/init.d/network restart
   ```

What to do next

Restart the computer for the changes to take effect.

Change of the DB2 application heap size:

Loading many users can encounter performance issues.

You might see this message:

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

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

Installation and configuration of the Oracle database

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

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

Tasks for creating the database

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

Note: To use multiple instances of Security Identity Manager with the same Oracle database server, there is an additional task. See "Multiple instances of IBM Security Identity Manager with an Oracle database server" before creating the database.

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

1. Back up an existing database.
2. Install the Oracle database server.

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

Multiple instances of IBM Security Identity Manager with an Oracle database server:

If you want to point several instances of IBM Security Identity Manager to multiple databases on the same Oracle server, copy and modify the `$ISIM_home/config/rdbms/oracle/enrole_admin.sql` file.

You need to copy and modify this code example in the `$ISIM_home/config/rdbms/oracle/enrole_admin.sql` file.

The value `enrole1_data_001.dbf` is changed to `enrole1_data_002.dbf` in this example. Modify this value incrementally in each copy of the code. Do this task for each additional IBM Security Identity Manager instance used on the same Oracle server.

Note: The two lines where the code needs to be modified are highlighted in **bold**.

Example

```
# pwd
/u02/enrole/config/rdbms/oracle
# more enrole_admin.sql
CREATE TABLESPACE enrole_data
DATAFILE 'enrole1_data_002.dbf'
```

```
SIZE 160M
AUTOEXTEND ON
NEXT 20M
MAXSIZE 1024M
DEFAULT STORAGE (INITIAL 10M
NEXT 1M
PCTINCREASE 10)
PERMANENT
ONLINE
LOGGING;

CREATE TABLESPACE enrole_indexes
DATAFILE 'enrole1_idx_002.dbf'
SIZE 160M
AUTOEXTEND ON
NEXT 20M
MAXSIZE 1024M
DEFAULT STORAGE (INITIAL 10M
NEXT 1M
PCTINCREASE 10)
PERMANENT
ONLINE
LOGGING;

CREATE USER enrole IDENTIFIED BY enrole
DEFAULT TABLESPACE enrole_data
QUOTA UNLIMITED ON enrole_data
QUOTA UNLIMITED ON enrole_indexes;
GRANT CREATE SESSION TO enrole;
GRANT CREATE TABLE to enrole;
#
```

Backup of an existing database:

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

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

Installation of the Oracle database server:

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

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

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

Configuring the init.ora file:

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

Before you begin

You need to have the Oracle database server installed.

Procedure

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

     Copy the *ORACLE_HOME*/product/<*version number*>/dbhome_1/dbs/init.ora file to a new *ORACLE_HOME*/dbs/init*db_name*.ora file.
2. Based on your environment requirements, tune the value of the following parameters in the `init`*db_name*`.ora` file:

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

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

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

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

What to do next

Set the environment variables.

Environment variable settings for the Oracle database:

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

Required environment variables include:

- ORACLE_SID=itimdb
- ORACLE_BASE=/home/oracle/app/oracle
- ORACLE_HOME=$ORACLE_BASE/product/11.2.0/dbhome_1
- PATH=$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.

Oracle JDBC driver installation:

IBM Security Identity Manager Version 6.0 requires the Oracle 11g Release 1 (11.1.0.7.0) JDBC driver whether you are using an Oracle 10g or 11g database. For Oracle 12 c Release 1 (12.1.0.2) you must download the `ojdbc6.jar` file.

Copy the Oracle JDBC driver from the Oracle server directory into a directory on the computer where IBM Security Identity Manager is to be installed. For example, for the Windows operating system, create a directory: `C:\isim_jdbcdriver`. For the UNIX or Linux operating system, create a directory: `/isim_jdbcdriver`. Copy the JDBC driver file to this directory and then point to this directory during installation.

You can also download the driver from the Oracle website. The installation program prompts for the directory that contains the JDBC driver and the driver name. In a cluster configuration, the JDBC driver is required on the computer that has the deployment manager and on each cluster member computer.

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 28.
     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:

```
# sqlplus "/ as sysdba"

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

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

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

What to do next

Tune the database performance.

Oracle database performance tuning

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

Enabling XA recovery operations:

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

Before you begin

Ensure that you have database administrator authority.

About this task

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

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

Procedure

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

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

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

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

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

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

What to do next

Tune additional settings.

Configuring TCP KeepAlive settings:

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

Before you begin

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

Procedure

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

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

What to do next

Restart the computer for the changes to take effect.

Starting the Oracle product and the listener service

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

Before you begin

You must have an Oracle database installed.

Procedure

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

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

     Enter these commands:

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

     Use the Services menu to start the Oracle TNS listener named `OracleOraDb10_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 additional components.

Installation and configuration of SQL Server 2008 on the Windows operating system

IBM Security Identity Manager supports the use of the SQL Server 2008 database. You must install and configure the database before you install IBM Security Identity Manager.

Note: The Identity Service Center does not support Microsoft SQL Server database. Use DB2 database or Oracle database instead.

SQL Server 2008 installation

You must prepare and install the SQL Server 2008 before it can be used with the IBM Security Identity Manager.

Complete the following procedures before installing SQL Server 2008 on a Windows system:

1. Obtain the latest SQL Server 2008 service pack.
2. Log on to the Windows system with an Administrator account before starting the SQL Server 2008 installation.

Installing the server

You might install SQL Server 2008 on the same computer or on a computer that is separate from IBM Security Identity Manager. After installing SQL Server 2008, install the latest SQL Server 2008 service pack. For more information about installing SQL Server 2008, see the documentation available at the SQL Server official website.

Note: When you install SQL Server 2008, you must set the code page for the database to be not case-sensitive (CI).

Configuration of SQL Server 2008

You must complete several post-installation tasks to configure SQL Server 2008 for IBM Security Identity Manager.

The post-installation tasks include:

- Installing the SQL Server JDBC driver
- Configuring SQL Server 2008 for XA transactions
- Verify the security configuration for SQL Server 2008

SQL Server JDBC driver installation:

Security Identity Manager version 6.0 requires SQL Server 2008 JDBC Driver 3.0.

Copy the SQL Server JDBC driver from the SQL Server 2008 into a directory on the computer where Security Identity Manager is to be installed. You can also download the driver from the Microsoft website. The Security Identity Manager installation program prompts for the directory that contains the JDBC driver and

the driver name. In a cluster configuration, the JDBC driver is required on the computer that has the deployment manager and on each cluster member computer.

For example, on the computer on which Security Identity Manager is to be installed, you must:

1. Create a directory `C:\itim_jdbcdriver\`.
2. Copy the JDBC driver file to that directory.
3. Point to this directory during installation.

Configuring SQL Server 2008 for XA transactions:

You need to run MS DTC service and configure the JDBC distributed transaction components for the SQL server.

Before you begin

The JDBC driver was downloaded and extracted from this website: http://msdn.microsoft.com/en-us/data/aa937724.aspx.

Procedure

Assuming that you installed the MS SQL Server 2008 JDBC driver 3.0 at *JDBC_DRIVER_INSTALL_DIR*, open the JDBC_DRIVER_INSTALL_DIR\help\html\574e326f-0520-4003-bdf1-62d92c3db457.htm file. Follow the instructions in *Understanding XA Transactions* for these sections.

1. Running the MS DTC Service
2. Configuring the JDBC Distributed Transaction Components

Note: You do not have to complete the section titled *Configuring the User-Defined Roles*. Security Identity Manager creates the necessary ID and associate with the SqlJDBCXAUser role for you.

Verifying the security configuration for SQL Server 2008:

Use the SQL Server Management Studio to verify the security configurations for the SQL Server 2008.

Before you begin

You must finish downloading and installing SQL Server 2008.

Procedure

1. Start the Microsoft SQL Server Management Studio.
2. Right click the SQL server root node, and click **Properties**.
3. Select **Security** from the Select a page panel.
4. Ensure that **SQL Server and Windows Authentication Mode** is selected.
5. Click **OK**.

What to do next

Create the Security Identity Manager database.

Creating the Security Identity Manager database

You must complete several post-installation tasks to create the Security Identity Manager database.

Before you begin

Ensure that SQL Server 2008 is installed and configured.

Procedure

1. Start the Microsoft SQL Server Management Studio.
2. Select the tree, right-click on the **Databases** node, and select **New Database**.
3. Under Database name, type in a database name such as `itimdb`, and click **OK**.
4. For data files and transaction logs, enter the following values:
   - Initial file size: 20 MB
   - Automatically grow files
   - Allow unrestricted file growth

   Note: Ensure that the SQL server is in mixed authentication mode.

What to do next

Install and configure additional components.

Installation and configuration of a directory server

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

The supported combinations of directory servers and required fix packs are described in Directory server support.

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 fixes and 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. For more information, see Operating system support .

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

Installing IBM Security Directory Server

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

To install IBM Tivoli Directory Server, follow these steps.

Procedure

1. Install DB2 from the DVD provided with the IBM Security Identity Manager product, if DB2 is not already installed.
2. Optional. You need this step only when you use the WebSphere Application Server application client for IBM Security Directory Server. Install WebSphere Application Server from the DVD provided with the IBM Security Identity Manager product. If you are installing IBM Security Identity Manager on the same computer as IBM Security Directory Server, you must complete the WebSphere Application Server installation first. For more information, see "Installing WebSphere Application Server 7.0 in a single-server environment" on page 59.
3. Install IBM Security Directory Server from the DVD provided with the IBM Security Identity Manager product.
4. During the IBM Security Directory Server installation, you must select **Custom** as the installation type. Click **Next**.
5. In the next panel, do *not* select DB2 Database, or embedded WebSphere Application Server. You *must* select the supported IBM Security Directory Server. Other features are optional. Click **Next**.
6. In the next panel, the installer detects your WebSphere Application Server. You might be prompted to select a custom location of the WebSphere Application Server installation path. You can also choose to skip the deployment of Web Administration Tools. Click **Next**.
7. Review the summary and click **Install** to install IBM Security Directory Server.

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

What to do next

Install any required fix packs.

Required fix pack installation

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

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

Verifying that the correct fix pack is installed

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

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

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

IBM Security Directory Server configuration

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

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

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

Running the middleware configuration utility:

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

Before you begin

Note: The middleware configurtion utility does not support IBM Security Directory Server 6.3.1. You must configure version 6.3.1 manually. See "Configuring IBM Security Directory Server manually" on page 41.

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

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

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

```
umask 022
```

About this task

The middleware configuration utility:

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

The middleware configuration utility can be run manually or silently. For more information about silent configuration, see "Configuring IBM Security Directory Server silently" on page 43.

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

Procedure

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

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

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

   This command configures the graphical user interface for the middleware configuration utility to correctly display configuration panels during the middleware configuration. If you do not run this command before starting the middleware configuration utility, you encounter display problems in the language selection panel.
3. Start the middleware configuration utility in the base directory of the DVD or a download directory:
   - AIX operating systems: Start the middleware configuration utility by running the `cfg_itim_mw_aix` program.
   - Linux for xSeries operating systems: Start the middleware configuration utility by `running the cfg_itim_mw_xLinux` program.

- Linux for pSeries operating systems: Start the middleware configuration utility by running the `cfg_itim_mw_pLinux` program.
- Linux for zSeries operating systems: Start the middleware configuration utility by running the `cfg_itim_mw_zLinux` program.
- Windows operating systems: Start the middleware configuration utility by using the `cfg_itim_mw.exe` program if the Windows autorun feature is disabled.

Each platform requires a file called `cfg_itim_mw.jar` to go along with the native program. The JAR file and the native program must be in the same directory location.

4. Select your language, and click **OK**.
5. From the Product Configuration panel, check only **Configure IBM Tivoli Directory Server**, and click **Next**.
6. You can receive a warning if IBM Tivoli Directory Server is not at the correct level or not installed. Action might be required to make sure that IBM Tivoli Directory Server is at the correct level. To bypass this warning, click **Next**.
7. From the IBM Tivoli Directory Server configuration options panel, provide the following information, and then click **Next**.
   - Directory server administrator ID and instance name

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

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

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

     Type the password again.
   - Group for the DB2 administrator

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

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

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

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

   Note: The dollar sign ($) has special meaning in the installer frameworks used by the middleware configuration utility. Avoid $ in any field values. The installer framework or operating system platform might do variable substitution for the value.
8. Provide the following LDAP information, and then click **Next**.
   - Administrator DN

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

- Administrator DN password

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

- Password confirmation

  Type the password again.

- User-defined suffix

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

- Non-SSL port

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

  Note: This default port might conflict with other services. For example, a Windows server can run Windows Active Directory services, which use a default port of 389.

9. Review your configuration options before clicking **Next** to begin the configuration process.
10. The configuration can take up to several minutes to complete. When the configuration completes successfully, click **Finish** to exit the deployment wizard.

What to do next

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

Configuring IBM Security Directory Server manually:

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

Before you begin

You must have the directory server and a database installed. See "Database installation and configuration" on page 15 and "Installation and configuration of a directory server" on page 36.

About this task

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

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

Procedure

1. Create a user. Issue one of these commands.
   - On Windows operating systems

     `LDAP_Install_Location\sbin\idsadduser -u` *`ldapinst`* `-w` *`ldapinstpwd`*

Where

ldapinst is the user name.

ldapinstpwd is the password.

- On UNIX or Linux operating systems

  `LDAP_Install_Location/sbin/idsadduser -u ldapinst -w ldapinstpwd -g idsldap –l /home/ldapinst`

  Where

  ldapinst is the user name.

  ldapinstpwd is the password.

  idsldap is the default LDAP group.

  /home/ldapinst is the instance home directory.

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

   Where

   ldapinst is the LDAP instance name.

   encryptionseed is the encryption seed.

   /home/ldapinst is the instance home directory.

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

   Where

   ldapinst is the LDAP instance name.

   dbadmin is the database administrator name.

   dbadminpwd is the database administrator password.

   dbname is the database name.

   /home/ldapinst is the instance home directory.

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

   Where

   ldapinst is the LDAP instance name.

   `cn=root` is the Principal DN.

   `root` is the Principal DN password.

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

   Where

   ldapinst is the LDAP instance name.

   `dc=com` is the suffix.

6. Start the directory server instance.

   - On Windows operating systems

     Use the Windows Services application to start the LDAP instance.

   - On UNIX or Linux operating systems issue the command.*LDAP_Install_Location*`/sbin/ibmslapd -I ldapinst -n -t`

7. Create an ldif file such as `dccom.ldif` with the following content.

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

8. Run the following command. *LDAP_Install_Location*/bin/idsldapadd -p *ldap_server_port* -D *bind_dn* -w *bind_dn_password* -f dccom.ldif

   Where

   ldap_server_port is the port on which the LDAP server listens.

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

   bind_dn_password is the password for authentication

   dccom.ldif is the name of the ldif file.

   For example,

   On Windows operating systems

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

   On UNIX or Linux operating systems

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

Configuring IBM Security Directory Server silently:

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

Before you begin

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

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

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

```
umask 022
```

About this task

The middleware configuration utility:

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

To start the middleware configuration utility silently:

Procedure

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

3. From a command window, run this command:
   cfg_itim_mw –W ITIM.responseFile=cfg_itim_mw.rsp –silent

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

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

What to do next

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

Successful suffix object configuration verification:

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

To verify the suffix object configuration, enter this command:

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

The options are:

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

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

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

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

Manually tuning the IBM Security Directory Server database:

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

Before you begin

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

Procedure

1. Open a DB2 command window.

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

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

   The value of *itim_dbname* is a name such as `itimdb`. The value of *itim_dbmemory* is `40000` for a single-server installation, `COMPUTED` for all platforms except AIX and Windows. For AIX and Windows, the value is `AUTOMATIC`. For more information about performance parameter tuning for DB2, see *Security Identity Manager Performance Tuning Guide*.

3. Stop and start the DB2 server to reset the configuration. After you have reset the configuration, stop and start the DB2 server to allow the changes to take effect. Enter the following commands:

   ```
   db2stop
   db2start
   ```

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

What to do next

Install and configure another component.

Installation and configuration of Oracle Directory Server Enterprise Edition

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

Oracle Directory Server Enterprise Edition installation

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

Configuring Oracle Directory Server Enterprise Edition

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

Before you begin

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

Procedure

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

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

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

   - For UNIX or Linux operating systems:

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

   - For Windows operating systems:

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

2. Start the IBM Security Identity Manager LDAP server. Type this command:
   ```
   ./dsadm start instance-path
   ```

   For example:
   - For UNIX or Linux operating systems:
     ```
     ./dsadm start /local/itimldap
     ```
   - For Windows operating systems:
     ```
     dsadm.exe start \local\itimldap
     ```
3. Create a root suffix. Type this command:
   ```
   ./dsconf create-suffix –h host –p portnumber rootsuffix
   ```

   For example:
   - For UNIX or Linux operating systems:
     ```
     ./dsconf create-suffix –h localhost –p 1389 dc=com
     ```
   - For Windows operating systems:
     ```
     dsconf.exe create-suffix –h localhost –p 1389 dc=com
     ```

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

   If you receive the following message, use the **--unsecured** parameter:
   ```
   Unable to bind securely on host:portNumber
   ```

   For example:
   - For UNIX or Linux operating systems:
     ```
     ./dsconf create-suffix -–unsecured –h localhost –p 1389 dc=com
     ```
   - For Windows operating systems:
     ```
     dsconf.exe create-suffix -–unsecured –h localhost –p 1389 dc=com
     ```
4. Create and save a file named `dcequalscom.ldif` with the following content:
   ```
   dn:dc=com
   dc:com
   objectclass:top
   objectclass:domain
   ```
5. Import the `dcequalscom.ldif` file to the `dc=com` root suffix. Type this command:
   ```
   ./dsconf import -p portnumber -e path/dcequalscom.ldif rootsuffix
   ```

   For example:
   - For UNIX or Linux operating systems:
     ```
     ./dsconf import -p 1389 -e /temp/dcequalscom.ldif dc=com
     ```
   - For Windows operating systems:
     ```
     dsconf.exe import -p 1389 -e \temp\dcequalscom.ldif dc=com
     ```

   If you receive the following message, use the **--unsecured** parameter:
   ```
   Unable to bind securely on host:portNumber
   ```
   - For UNIX or Linux operating systems:
     ```
     ./dsconf import --unsecured -p 1389 -e /temp/dcequalscom.ldif dc=com
     ```
   - For Windows operating systems:
     ```
     dsconf.exe import --unsecured -p 1389 -e \temp\dcequalscom.ldif dc=com
     ```
6. Restart the directory server.

What to do next

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

Install and configure another component.

Optionally installing IBM Security Directory Integrator

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

Before you begin

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

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

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

About this task

The information in this chapter is not a substitute for the more extensive, prerequisite documentation that is provided by the directory integrator product itself.

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

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

Procedure

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

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

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

   Adapters works with IBM Security Identity Manager to manage resources. Agent-based adapters require the installation of the adapter on the managed resource and the installation of an adapter profile on the IBM Security Identity

Manager Server. Agentless adapters require adapter installation on the computer that hosts IBM Security Directory Integrator. They also require the installation of an adapter profile on the IBM Security Identity Manager Server.

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

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

What to do next

Manually install agentless adapters and adapter profiles on remote systems. See "Installing agentless adapters" and "Installing agentless adapter profiles" on page 51.

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 6.0. The adapters must be installed on the IBM Security Directory Integrator. IBM Security Identity Manager version 6.0 supports IBM Security Directory Integrator versions 7.1 and 7.1.1. You can install the adapters interactively or silently.

Before you begin

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

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

Note: The LDAP adapter requires the Dispatcher only.

About this task

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

Procedure

1. To install the Dispatcher interactively, run these commands:
   a. For Windows operating systems, type:
      ```
      cd \download\adapters
      ```
      Then type the following text as a single command:
      ```
      ITDI_HOME\jvm\jre\bin\java.exe -jar DispatcherInstall_70.jar
      ```
   b. For UNIX and Linux operating systems, type:

```
cd /download/adapters
```

Then type the following text as a single command:

```
ITDI_HOME/jvm/jre/bin/java -jar DispatcherInstall_70.jar
```

2. To install the Dispatcher silently, run these commands:
   a. For Windows operating systems, type:

      ```
      cd \download\adapters
      ```

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

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

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

      ```
      ITDI_HOME\jvm\jre\bin\java.exe -jar DispatcherInstall.jar -i silent
      -DUSER_INSTALL_DIR="C:\Program Files\IBM\TDI\V7.1"
      -DUSER_SELECTED_SOLDIR="C:\Program Files\IBM\TDI\V7.1\timsol"
      -DUSER_INPUT_PORTNUMBER=1099
      -DUSER_DISPATCHER_SERVICE_NAME="ISIM Adapters"
      ```

      Where:

      -DUSER_INSTALL_DIR
      Overrides the default Security Directory Integrator installation path.

      -DUSER_SELECTED_SOLDIR
      Overrides the default adapters solutions directory.

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

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

   b. For UNIX and Linux operating systems, type:

      ```
      cd /download/adapters
      ```

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

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

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

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

      Where:

      -DUSER_INSTALL_DIR
      Overrides the default Security Directory Integrator installation path.

      -DUSER_SELECTED_SOLDIR
      Overrides the default adapters solutions directory.

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

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

3. To install the UNIX and Linux adapter interactively, run these commands:
   a. For Windows operating systems, type:
   ```
   cd \download\adapters
   ```
   Then type the following text as a single command:
   ```
   ITDI_HOME\jvm\jre\bin\java.exe -jar PosixAdapterInstall_70.jar
   ```
   b. For UNIX and Linux operating systems, type:
   ```
   cd /download/adapters
   ```
   Then type the following text as a single command:
   ```
   ITDI_HOME\jvm\jre\bin\java.exe -jar PosixAdapterInstall_70.jar
   ```
4. To install the UNIX and Linux adapter, or the LDAP adapter, in silent mode, run these commands:
   a. For Windows operating systems, type:
   ```
   cd \download\adapters
   ```
   To install the adapter in silent mode with the default settings, issue the command:
   ```
   ITDI_HOME\jvm\jre\bin\java.exe -jar PosixAdapterInstall_70.jar -i silent
   ```
   To install the adapter in silent mode and changing default settings, use the **-D** parameter. For example:
   ```
   ITDI_HOME\jvm\jre\bin\java.exe -jar PosixAdapterInstall_70.jar -i silent
    -DUSER_INSTALL_DIR="C:\Program Files\IBM\TDI\V7.1"
   ```
   Where

   -DUSER_INSTALL_DIR
   Overrides the default Security Directory Integrator installation path.
   b. For UNIX and Linux operating systems, type:
   ```
   cd /download/adapters
   ```
   To install the adapter in silent mode with the default settings, issue the command:
   ```
   ITDI_HOME/jvm/jre/bin/java -jar PosixAdapterInstall_70.jar -i silent
   ```
   To install the adapter in silent mode and changing default settings, use the **-D** parameter. For example:
   ```
   ITDI_HOME/jvm/jre/bin/java -jar PosixAdapterInstall_70.jar -i silent
    -DUSER_INSTALL_DIR="/opt/IBM/TDI/V7.1"
   ```
   Where

   -DUSER_INSTALL_DIR
   Overrides the default Security Directory Integrator installation path.

Installing agentless adapter profiles

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

About this task

To install agentless adapter profiles, you can run command lines on both Windows and UNIX or Linux operating systems. You can also install them by selecting **Configure System** > **Manage Service Types** > **Import** from the IBM Security Identity Manager user interface.

Procedure

1. For Windows operating system, run these commands.

```
cd ISIM_HOME\config\adapters "ISIM_HOME/bin/win/config_remote_services.cmd"
 -profile LdapProfile -jar LdapProfile.jar

"ISIM_HOME/bin/win/config_remote_services.cmd" -profile PosixSolarisProfile -jar
PosixSolarisProfile.jar

"ISIM_HOME/bin/win/config_remote_services.cmd" -profile PosixLinuxProfile -jar
PosixLinuxProfile.jar

"ISIM_HOME/bin/win/config_remote_services.cmd" -profile PosixHpuxProfile -jar
PosixHpuxProfile.jar

"ISIM_HOME/bin/win/config_remote_services.cmd" -profile PosixAixProfile -jar
PosixAixProfile.jar
```

2. For UNIX or Linux operating systems, run these commands.

```
-bash-3.00# cd ISIM_HOME/bin/unix
-bash-3.00# ./config_remote_services.sh -profile LdapProfile -jar /opt/IBM/isim
/config/adapters/LdapProfile.jar

-bash-3.00# ./config_remote_services.sh -profile PosixSolarisProfile -jar /opt
/IBM/isim/config/adapters/PosixSolarisProfile.jar

-bash-3.00# ./config_remote_services.sh -profile PosixLinuxProfile -jar /opt
/IBM/isim/config/adapters/PosixLinuxProfile.jar

-bash-3.00# ./config_remote_services.sh -profile PosixHpuxProfile -jar /opt
/IBM/isim/config/adapters/PosixHpuxProfile.jar

-bash-3.00# ./config_remote_services.sh -profile PosixAixProfile -jar /opt
/IBM/isim/config/adapters/PosixAixProfile.jar
```

Installation and configuration of WebSphere Application Server

WebSphere Application Server delivers a secure, scalable application infrastructure for Security Identity Manager Server. WebSphere Application Server can run in a single-server or a cluster server environment.

This section describes generic steps to create a WebSphere Application Server environment before you install the Security Identity Manager Server. These steps apply for either single-server or cluster configurations. The supported releases and required fix packs for WebSphere Application Server are described in WebSphere Application Server requirements on the IBM Knowledge Center.

Note:

SSLv3 contains a vulnerability that has been referred to as the Padding Oracle On Downgraded Legacy Encryption (POODLE) attack. SSLv3 is enabled by default in IBM WebSphere Application Server. This vulnerability affects all versions and releases of IBM WebSphere Application Server, IBM WebSphere Application Server Full Profile, IBM WebSphere Application Server Liberty Profile and IBM WebSphere Application Server Hypervisor Edition.

See the following documentation before you configure the WebSphere Application server environment.

WebSphere Application server
Security Bulletin: Vulnerability in SSLv3 affects IBM WebSphere Application Server (CVE-2014-3566) at http://www.ibm.com/support/docview.wss?uid=swg21687173

HTTP server front ends for cluster environments
Security Bulletin: Vulnerability in SSLv3 affects IBM HTTP Server (CVE-2014-3566) at http://www.ibm.com/support/docview.wss?uid=swg21687172

Installing WebSphere Application Server 8.5

If you want to use the Identity Service Center, you must install WebSphere Application Server 8.5. The installation of WebSphere Application Server 8.5 uses the IBM Installation Manager. The previous version, WebSphere Application Server 7.0, used the InstallAnywhere for installation.

Before you begin

The Identity Service Center requires WebSphere Application Server 8.5 with fix pack 2.

You must have the IBM Installation Manager installed. For instructions about how to install the Installation Manager, go to the WebSphere Application Server section of the IBM Knowledge Center. Search on *Installing Installation Manager and preparing to install the product*.

About this task

For more information about installing WebSphere Application Server 8.5, go to the WebSphere Application Server section of the IBM Knowledge Center. Search on *Installing the product on distributed operating systems using the GUI*.

Procedure

1. Start the Installation Manager.

   Tip: You can start the Installation Manager in group mode with the **./IBMIM** command.
   - Group mode allows multiple users to use a single instance of IBM Installation Manager to manage software packages.
   - For more information about using group mode, read the Group mode roadmaps in the IBM Installation Manager Version 1.6 product documentation or the IBM Installation Manager Version 1.5 product documentation.
2. Click **Install**.

Note: If you are prompted to authenticate, use the IBM ID and password that you used for registration to the program website.
The Installation Manager searches its defined repositories for available packages.

3. Perform the following actions.
   a. Select **IBM WebSphere Application Server** and the appropriate version. If the product is previously installed on a WebSphere Application Server installation on your system, a message displays indicating that the product is already installed. To create another installation of the product in another location, click **Continue**.

      Tip:

      If the **Search service repositories during installation and updates** option is selected on the Installation Manager Repository preference page and you are connected to the Internet, you can click **Check for Other Versions and Extensions** to search for updates in the default update repositories for the selected packages. In this case, you do not need to add the specific service-repository URL to the Installation Manager Repository preference page.

      If you have downloaded and extracted both the WebSphere Application Server 8.5 GA Version repository and the WebSphere Fix Pack 2 repository, you can add them to the Installation Manager's repository before your installation. In this way, the Installation Manager can automatically recognize them and then offer the one option to install both WebSphere Application Server 8.5 and the fix pack at the same time.
   b. Select the fixes to install. Any recommended fixes are selected by default.

      If there are recommended fixes, you can select the option to show only recommended fixes and hide non-recommended fixes.
   c. Click **Next**.

   Note: The Installation Manager might prompt you to update to the latest level of the Installation Manager when it connects to the repository. If you are prompted to do so, update to the newer version before you continue. Read the IBM Installation Manager Version 1.6 product documentation or the IBM Installation Manager Version 1.5 product documentation for information about automatic updates.
4. Accept the terms in the license agreements and click **Next**.
5. Specify the installation root directory for the product binary files, which are also referred to as the core product files or system files. The panel also displays the shared resources directory and disk-space information.

   Note: The first time that you install a package by using the Installation Manager, specify the shared resources directory. The shared resources directory is where the installation artifacts are located and can be used by one or more package groups. Use your largest drive for this installation. You cannot change the directory location until after you uninstall all packages.

   Restriction:

   - Deleting the default target location and leaving an installation-directory field empty prevents you from continuing the installation process.
   - Do not use symbolic links as the destination directory.

Symbolic links are not supported.

- Do not use a semicolon in the directory name.

  A semicolon is the character that is used to construct the class path on Windows systems. If the target directory includes a semicolon, WebSphere Application Server cannot be installed properly.
- The maximum path length on the Windows Server 2008, Windows Vista, and Windows 7 operating systems is 60 characters.

6. Click **Next**.
7. Select the languages for which translated content is installed. English is always selected.
8. Click **Next**.
9. Select the check boxes for the following features.
   - **WebSphere Application Server Full Profile**.

     Selecting this application-server feature gives you the traditional standards-based Java Platform, Enterprise Edition (Java EE) compliant application foundation. It offers a broad programming model choice and low total cost of ownership through high performance and high manageability.

     – **EJBDeploy tool for pre-EJB 3.0 modules**.

       This option installs the **EJBDeploy** tool for pre-EJB 3.0 modules.

       Before you deploy applications on the server, you must run the **EJBDeploy** tool on applications that contain EJB modules, which are based on specifications before EJB 3.0. Running the **EJBDeploy** tool generates deployment code for enterprise beans in the application. Beginning with the EJB 3.0 specification, the EJBDeploy tool is no longer required because WebSphere Application Server uses a new feature that is called **JITDeploy**. It automatically generates code when the application starts.

       Tip: Unexpected errors might occur if applications that are provided with IBM WebSphere Application Server require the optional **EJBDeploy** tool for pre-EJB 3.0 modules but the feature is not installed. If you deploy and use applications that might require pre-EJB 3.0 modules, include the optional **EJBDeploy** feature in all WebSphere Application Server installations by servers that run the pre-EJB 3.0 applications.

       Tip: You can run the Installation Manager later to modify this installation, and then add or remove this feature.

     – **Standalone thin clients, resource adapters, and embeddable containers**

       IBM thin clients and resource adapters provide a set of clients and resource adapters for various technologies, such as JAX-WS, JAX-RPC, JAX-RS, XML, EJB, JPA, JMS, and more. An embeddable container runs in a stand-alone Java Platform, Standard Edition environment. For example, you can use the embeddable EJB container to run enterprise beans outside the application server.

       - **Standalone thin clients and resource adapters**

         This option installs the IBM stand-alone thin clients and resource adapters.

         IBM thin clients provide a set of clients for various technologies, such as JAX-WS, JAX-RPC, JAX-RS, XML, EJB, JPA, JMS, and more. IBM resource adapters provide the resource adapters for JMS.

- **Embeddable EJB container**

  This option installs the embeddable EJB container.

  The embeddable EJB container is a Java Archive (JAR) file that you can use to run enterprise beans in a stand-alone Java Platform, Standard Edition environment. You can run enterprise beans by using this embeddable container outside the application server. The embeddable EJB container is a part of the EJB 3.1 specification and is primarily used for unit testing enterprise beans business logic.

Tip: You can run the Installation Manager later to modify this installation and add or remove these features.

- **IBM WebSphere SDK for Java Technology Edition 6.0**
  - **IBM 64-bitWebSphere SDK for Java**

10. Click **Next**.
11. Review the summary information and click **Install**.
    - If the installation is successful, the program displays a message of successful installation.

      Note: The program might also display important post-installation instructions as well.
    - If the installation is not successful, click **View Log File** to troubleshoot the problem.
12. Select one of the following options to create the necessary profile when this installation is finished.
    - **Select Profile Management Tool**: to create a profile if you want to open the full **Profile Management Tool** and create a profile when this installation is finished.
    - **Select Profile Management Tool to create an application server profile for a development environment**: if you want to create an application server profile with settings appropriate for a development environment when this installation is finished.

      Note: The development settings are appropriate for a development environment where frequent application updates are performed and system resources are at a minimum. Do not use the development settings for production servers.
    - Select **None** if you do not want to create a profile when this installation is finished.

    Restriction: The option to start the **Profile Management Tool** is only available when a version of WebSphere Application Server containing the **Profile Management Tool** is installed.
13. Click **Finish**.
14. Click **File** > **Exit** to close the Installation Manager.
15. Verify that the correct version of WebSphere Application Server is installed. Run either **versionInfo.sh** or the **versioninfo.bat** command. The example shows typical system output.

```
--------------------------------------------------------------------------------
IBM WebSphere Product Installation Status Report
--------------------------------------------------------------------------------

Report at date and time July 22, 2013 1:41:44 PM EDT
```

```
Installation
-------------------------------------------------------------------------------
Product Directory    /products/IBM/WebSphere/AppServer
Version Directory    /products/IBM/WebSphere/AppServer/properties/version
DTD Directory        /products/IBM/WebSphere/AppServer/properties/version/dtd
Log Directory        /var/ibm/InstallationManager/logs

Product List
-------------------------------------------------------------------------------
ND                       installed

Installed Product
-------------------------------------------------------------------------------
Name                 IBM WebSphere Application Server Network Deployment
Version              8.5.0.2
ID                   ND
Build Level          cf011242.02
Build Date           10/17/12
Package              com.ibm.websphere.ND.v85_8.5.1.20121017_1724
Architecture         System z (64 bit)
Installed Features   IBM 64-bit WebSphere SDK for Java
                     WebSphere Application Server Full Profile
                     EJBDeploy tool for pre-EJB 3.0 modules
                     Embeddable EJB container
                     Stand-alone thin clients and resource adapters

-------------------------------------------------------------------------------
End Installation Status Report
-------------------------------------------------------------------------------
```

Note: If the fix pack is installed, the version is 8.5.0.2.

What to do next

You can create a stand-alone application server profile or a management profile with an administrative agent server by using the **Profile Management Tool** or the **manageprofiles** command. For information about setting up profiles and creating clusters, see the WebSphere Application Server of the IBM Knowledge Center.

Creating clusters with WebSphere Application Server 8.5

A cluster is a set of application servers that you manage together as a way to balance workload. You must create two server clusters in your WebSphere Application Server environment. One cluster hosts the IBM Security Identity Manager application. The other cluster is used as a messaging service.

Before you begin

For more recent information about installing WebSphere Application Server 8.5, go to the WebSphere Application Server section of the IBM Knowledge Center.

Before you create a cluster:

- Ensure that all node agents are running.
- Review the content of the topic "Clusters and workload management", in the WebSphere documentation, especially the information about setting cluster weights.
- Decide whether you want enterprise bean requests routed to the node on which the client resides.

- Determine the appropriate configuration settings for the first cluster member. A copy of the first cluster member that you create is stored as part of the cluster data. It becomes the template for all additional cluster members that you create.
- Decide on which node you want the first cluster member to reside.

Ensure that the system clocks of all the servers in your WebSphere Application Server clustered environment are synchronized to within 5 minutes of the deployment manager server. The servers must also be set to the same time zone. For information about synchronizing the servers, see the WebSphere product information at the WebSphere Application Server section of the IBM Knowledge Center. Search on `system clocks`.

About this task

You might want to create a cluster if you must:

- Balance your client requests across multiple application servers.
- Provide a highly available environment for your applications.

By using a cluster, you can manage a group of application servers as a single unit. You can distribute client requests among the application servers that are members of the cluster.

Procedure

1. Use the following web address to access the administrative console:

   `http://`*`hostname`*`:`*`port`*`/ibm/console`

   The value of *hostname* is either the fully qualified host name or the IP address of the WebSphere Application Server deployment manager. The value of *port* is the port number for the WebSphere administrative HTTP transport.
2. In the administrative console, click **Servers** > **Clusters** > **WebSphere application server clusters** > **New**. The Create a new cluster wizard starts.
3. Specify a name for the cluster.
4. Select **Prefer local** if you want to enable host-scoped routing optimization. This option is enabled by default. When this option is enabled, if possible, EJB requests are routed to the client host. This option improves performance because client requests are sent to local enterprise beans.

   Note: If you enable the **`preferLocal`** optimization, the deployment manager must be running to affect the configuration. If the deployment manager is shut down, preferLocal optimization is not performed and requests might be dispersed across all the members of the cluster.
5. Click **Next**.
6. Choose whether to create an empty cluster or to create the first member of the cluster. If you decide to create an empty cluster, to add members to this cluster, in the administrative console, click **Servers** > **Clusters** > **WebSphere application server clusters** > *cluster_name* > **Clusters members** > **New**.

   To create an empty cluster:

   a. Select **None. Create an empty cluster**.
   b. Click **Next** to display a summary of the defined cluster.
   c. Click **Finish** to create the cluster, or click **Cancel** if you decide not to create this cluster.

When you create the first cluster member, a copy of the first cluster member that you create is stored as part of the cluster data. It becomes the template for all additional cluster members that you create.

a. Specify the name of the first cluster member.

b. Select the node on which you want this cluster member to reside.

c. Specify the weight value for the cluster member. The weight value controls the amount of work that is directed to the application server. The weight value represents a relative proportion of the workload that is assigned to a particular application server. The larger the weight value is, the larger the workload that is assigned. The value can range from 0 - 20.

d. Select **Generate unique HTTP ports** if you want to generate unique port numbers for every HTTP transport that is defined in the source server. Cluster members do not have HTTP transports or HTTP transport channels that conflict with any of the other servers that are defined on the same node. This option is selected by default. If you clear this option, all of the cluster members use the same HTTP ports.

e. Select the core group to which you want this cluster member to belong. You are prompted for the core group only if you have more than one core group that is defined for this cluster.

f. Select one of the following options to determine how the server resources are promoted in the cluster.

- **Cluster** to move the resources of the first cluster member to the cluster level. The resources of the first cluster member replace the resources of the cluster.
- **Server** to maintain the server resources at the new cluster member level. The cluster resources remain unchanged.
- **Both** to copy the resources of the cluster member (server) to the cluster level. The resources of the first cluster member replace the resources of the cluster. The same resources exist at both the cluster and cluster member scopes.

g. Select one of the following options as the basis for the first cluster member.

- Create the member by using an application server template.
- Create the member by using an existing application server as a template.
- Create the member by converting an existing application server.

Note: You can add an existing application server to the cluster only if you select that server as the first cluster member. You cannot add other existing application servers to that cluster after you create the first cluster member. If you add an existing server to a cluster, the only way to remove that server from the cluster is to delete the server. Therefore, you might want to use the existing server as a template for the first cluster member instead of as the cluster member. If you keep the original application server out of the cluster, you can reuse that server as the template if you must rebuild the configuration.

7. Click **Next**.

8. Create more cluster members. Before you create more cluster members, check the configuration settings of the first cluster member. These settings are displayed at the bottom of the Create more cluster members panel of the Create a new cluster wizard. For each additional member that you want to create:

a. Specify a unique name for the member. The name must be unique within the node.

b. Select the node to which you want to assign the cluster member.
c. Specify the weight that you want given to this member. The weight value controls the amount of work that is directed to the application server. The weight value represents a relative proportion of the workload that is assigned to a particular application server. The larger the weight value is, the larger the workload that is assigned. The value can range from 0 - 20.
d. Select **Generate unique HTTP** ports if you want to generate unique port numbers for every HTTP transport that is defined in the source server.
e. Click **Add member**. You can edit the configuration settings of any of the newly created cluster members other than the first cluster member. You can also create more cluster members. Click **Previous** to edit the properties of the first cluster member. The settings for the first cluster member become the settings for the cluster member template that is automatically created when you create the first cluster member.

9. When you finish creating cluster members, click **Next**.
10. View the summary of the cluster and then click **Finish** to create the cluster. Click **Previous** to return to the previous wizard panel and change the cluster, or click **Cancel** to exit the wizard without creating the cluster.
11. To further configure a cluster, click **Servers** > **Clusters** > **WebSphere application server clusters** > ***name of the cluster***. Only the **Configuration** and **Local Topology** tabs are displayed until you save your changes.
12. Click **Review** to review your cluster configuration settings. Repeat the previous step if you must make more configuration changes.
13. If you do not want to make any additional configuration changes, select **Synchronize changes with Nodes** and then click **Save**. Your changes are saved and synchronized across all of your nodes.

    Note: If you click **Save**, but do not select Synchronize changes with Nodes, when you restart the cluster, the product does not start the cluster servers. It cannot find them on the node. If you want to always synchronize your configuration changes across your nodes, you can select **Synchronize changes with Nodes** as one of your console preferences
14. Restart the cluster.

Results

You created a cluster to which you can assign work requests. The **Runtime** and **Local Topology** tabs are displayed the next time that you access the page.

What to do next

Install Security Identity Manager.

Installing WebSphere Application Server 7.0 in a single-server environment

Installing WebSphere Application Server Version 7 is a two-step process.

Before you begin

Before you install WebSphere Application Server:

- Read the WebSphere Application Server installation guide.

- Determine whether you are installing WebSphere Application Server in a single-server or cluster environment.
- Ensure that your system meets the product hardware and software requirements.
- Ensure that all required operating system fix packs are in place. For more information about tuning operating systems for the WebSphere Application Server, see this website: Tuning operating systems.

For more information about installing the WebSphere Application Server, see the following websites:

- Hardware and software requirements:

  Hardware and software requirements
- Support:

  Product Support
- IBM Knowledge Center:

  WebSphere Application Server

About this task

The two steps for the installation process are:

1. Installing a shared set of core product files by using the WebSphere Application Server installation product.
2. Using profiles to define multiple application server runtime environments. Each of these profiles has its own administrative interfaces that share the core files. Profiles are necessary for the environment to function. There are three types of profiles that you can create:

   Application server profile
   This profile can run as a stand-alone node or run as part of a deployment manager cell.

   Deployment manager profile
   This profile provides centralized management of application servers.

   Custom profile
   This profile must be federated and then customized through the deployment manager. A custom profile does not have its own administrative console. It is managed under the deployment manager node.

   For example, after the core files are installed, create one or more deployment manager profiles, application server profiles, or custom profiles. You can create a profile at any time after installation by using the Profile Creation wizard GUI or the **manageprofiles** command.

Additional configuration steps are required if you want to install the IBM HTTP Server and WebSphere Web Server plug-in. See "Installation and configuration of IBM HTTP Server and WebSphere Web Server plug-in (optional)" on page 67.

Procedure

1. Install the WebSphere Application Server product from the root user on the UNIX systems, or from a user with administrator authority on the Windows operating system.
2. Start the WebSphere Application Server installation program.

3. Select the **Application Server** profile. By default, administrative security is activated. Administrative security protects your server from unauthorized users.
4. Enter any additional values that the WebSphere installation program requires.
5. When installation is complete, download and install the Update Installer for WebSphere Application Server from the product support website: Product Support.
6. Use the Update Installer to install a service pack that contains a supported version of WebSphere Application Server. See *WebSphere Application Server requirements* on the IBM Security Identity Manager product documentation site. Make sure that you use the same operating system administrator account that you used for the installation.
7. Ensure that you use the Java Runtime Environment (JRE) version 1.6 SR10 Fix Pack 1. You can download the service release and follow the instructions to apply the fix at this WebSphere Application Server fix pack website: Downloads.
8. After you apply the WebSphere Application Server fix pack, start WebSphere Application Server. Use one of the following commands:
   - Windows operating systems:

     WAS_PROFILE_HOME\bin\startServer.bat *server_name*
   - UNIX or Linux operating systems:

     WAS_PROFILE_HOME/bin/startServer.sh *server_name*

   where *server_name* is the name of WebSphere Application Server. For example, server1.
9. Open the First Steps panel for WebSphere Application Server and click **Installation Verification** to verify that there are no installation problems. To run the first steps, use one of the following commands:
   - Windows operating systems:

     WAS_PROFILE_HOME\firststeps\firststeps.bat
   - UNIX or Linux operating systems:

     WAS_PROFILE_HOME/firststeps/firststeps.sh
10. Verify that the WebSphere Application Server fix pack is at the correct level. Use one of the following commands:
    - Windows operating systems:

      WAS_PROFILE_HOME\bin\versionInfo.bat
    - UNIX or Linux operating systems:

      WAS_PROFILE_HOME/bin/versionInfo.sh

    For example, the version output for the WebSphere Application Server base might be:

    ```
    Installed Product
    ------------------------------------------------
    Name     IBM WebSphere Application Server
    Version  7.0.0.23
    ID       BASE
    ```
11. Use the following web address to access the administrative console:

    http://*hostname*:*port*/ibm/console

    The value of *hostname* is either the fully qualified host name or the IP address of the computer on which you installed the WebSphere Application Server base product. The value of *port* is the port number for the WebSphere

administrative HTTP transport. The default value is 9060. If there is another instance of the WebSphere Application Server on the computer, the port number might not be 9060.

12. Examine the `SystemOut.log` and `SystemErr.log` files in *WAS_PROFILE_HOME*`\logs\`*server_name* to ensure that there are no other problems. For more information, see "Log files" on page 180.

What to do next

Install IBM Security Identity Manager Server.

Installing WebSphere Application Server 7.0 in a cluster environment

You must install WebSphere Application Server 7.0 on each computer in the cluster. You also need to create a deployment manager.

Before you begin

Ensure that the system clocks of all the servers in your WebSphere Application Server clustered environment are synchronized to within 5 minutes of the deployment manager server. The servers must also be set to the same time zone. For information about synchronizing the servers, see the WebSphere product information at WebSphere Application Server Version 7.0 section of the IBM Knowledge Center and search on `system clocks`.

Procedure

1. Install the WebSphere Application Server package.
2. Create a deployment manager profile.
3. On each computer in the cluster:
   a. Install the WebSphere Application Server package.
   b. Create a custom profile.
   c. Federate the node to the cell managed by the deployment manager.

   More configuration steps are required if you want to install the IBM HTTP Server and WebSphere Web Server plug-in. See "Installation and configuration of IBM HTTP Server and WebSphere Web Server plug-in (optional)" on page 67.

Installing the WebSphere Application Server deployment manager

The deployment manager provides centralized management of application servers.

Procedure

1. Install the WebSphere Application Server product from the root user on UNIX systems, or from a user with administrator authority on the Windows operating system.
2. Start the WebSphere Application Server installation program.
3. Select the **Deployment Manager** profile. By default, administrative security is activated. Administrative security protects your server from unauthorized users.
4. Enter any additional values that the WebSphere installation program requires.
5. When installation is complete, the First Steps panel is opened. Click **Installation Verification** to verify whether there are any installation problems.

- Windows operating systems:

  ```
  WAS_NDM_PROFILE_HOME\firststeps\firststeps.bat
  ```

- UNIX or Linux operating systems:

  ```
  WAS_NDM_PROFILE_HOME/firststeps/firststeps.sh
  ```

6. Download and install the Update Installer for WebSphere Application Server from the product support website.
7. Use the Update Installer to install a service pack that contains a supported version of WebSphere Application Server. See WebSphere Application Server requirements on the IBM Security Identity Manager product documentation site. Ensure that you use the same operating system administrator account that you used for the installation.
8. Ensure that you are using the IBM Java 2 Platform Standard Edition Development Kit 1.5 Service Release 6 or later. To verify the service release level of IBM Java, run the following command:

   - Windows operating systems:

     ```
     <WAS_NDM_PROFILE_HOME>\java\bin\java.exe -version
     ```

   - UNIX or Linux operating systems:

     ```
     <WAS_NDM_PROFILE_HOME>/java/bin/java -version
     ```

   If you intend to activate Java 2 security, Service Release 6 is needed. You can download the service release and follow the instructions to apply the fix at this WebSphere Application Server fix pack website: Downloads.
9. After you apply the WebSphere Application Server fix pack, start the deployment manager. Use one of the following commands:

   - Windows operating systems

     WAS_NDM_PROFILE_HOME\bin\startManager.bat

   - UNIX or Linux operating systems

     WAS_NDM_PROFILE_HOME/bin/startManager.sh

10. Verify that the WebSphere Application Server fix pack is at the correct level. Use one of the following commands:

    - Windows operating systems
      - Cluster member

        WAS_PROFILE_HOME\bin\versionInfo.bat

      - Deployment manager

        WAS_NDM_PROFILE_HOME\bin\versionInfo.bat
    - UNIX or Linux operating systems
      - Cluster member

        WAS_PROFILE_HOME/bin/versionInfo.sh

      - Deployment manager

        WAS_NDM_PROFILE_HOME/bin/versionInfo.sh

    The version output for WebSphere Application Server base, for example, might be:

    - WebSphere Application Server base

      ```
      Installed Product
      ------------------------------------------------
      Name     IBM WebSphere Application Server
      Version  7.0.0.23
      ID       BASE
      ```

    - Deployment manager

```
Installed Product
------------------------------------------------
Name     IBM WebSphere Application Server Deployment Manager
Version  7.0.0.23
ID       ND
```

11. Use the following web address to access the administrative console:

    `http://hostname:port/ibm/console`

    The value of *hostname* is either the fully qualified host name or the IP address of the computer on which you installed the WebSphere Application Server base product. The value of *port* is the port number for the WebSphere administrative HTTP transport. The default value is 9060. If there is another instance of the WebSphere Application Server on the computer, the port number might not be 9060.

12. Examine the `SystemOut.log` and `SystemErr.log` files in the *WAS_NDM_PROFILE_HOME*`\logs\`*dm_server_name* directory to ensure that there are no other problems.

What to do next

Install WebSphere Application Server on each node member.

Installing the WebSphere Application Server product on each node member

Install WebSphere Application Server on each cluster member host and federate each node member to the cell.

Procedure

1. Install the WebSphere Application Server product from the root user on UNIX systems, or from a user with administrator authority on the Windows operating system.
2. Start the WebSphere Application Server installation program.
3. Select the **Custom** profile.
4. In the **Federation** panel, complete these fields:
   a. Type the host name or IP address of the deployment manager.
   b. Type the SOAP port of the deployment manager or accept the default port.
   c. If administrative security is enabled, type the deployment manager administrative user name and password.
5. When installation is complete, download and install the Update Installer for WebSphere Application Server from the product support website.
6. Use the Update Installer to install a service pack that contains a supported version of WebSphere Application Server. See *Software prerequisites* on the IBM Security Identity Manager product documentation site. Make sure that you use the same operating system administrator account that you used for the installation.
7. Ensure that you are using the IBM Java 2 Platform Standard Edition Development Kit 1.5 Service Release 6 or later. To verify the service release level of IBM Java, run the following command:
   - Windows operating systems:

     `<WAS_NDM_PROFILE_HOME>\java\bin\java.exe -version`
   - UNIX or Linux operating systems:

     `<WAS_NDM_PROFILE_HOME>/java/bin/java -version`

If you intend to enable Java 2 security, Service Release 6 is required. You can download the service release and follow the instructions to apply the fix at this WebSphere Application Server fix pack website: Downloads.

8. After you apply the WebSphere Application Server fix pack, start the WebSphere Application Server. Use one of the following commands:
   - Windows operating systems:
     WAS_PROFILE_HOME\bin\startServer.bat
   - UNIX or Linux operating systems:
     WAS_PROFILE_HOME/bin/startServer.sh
9. Open the First Steps panel for WebSphere Application Server and click **Installation Verification** to verify that there are no installation problems. To run the first steps, use one of the following commands:
   - Windows operating systems:
     WAS_PROFILE_HOME\firststeps\firststeps.bat
   - UNIX or Linux operating systems:
     WAS_PROFILE_HOME/firststeps/firststeps.sh

What to do next

Verify the federation of nodes within the cell.

Manually federating a WebSphere Application Server node member

This step is optional if during the installation you either used a custom profile but did not federate the node to the cell or created a base WebSphere Application Server profile, which does not federate the node member.

Before you begin

Ensure that you created a deployment manager and installed WebSphere Application Server on each computer in the cluster.

Procedure

In the **addnode** command, add these parameters: **username dmgr_admin_user_id** and **password dmgr_admin_user_id**. Run one of these commands:

- Windows operating systems:
  WAS_HOME\bin\addNode.bat *dmgr_host portnumber* -profileName *profile_name* -username *dmgr_admin_user_id* -password *dmgr_admin_user_id*
- UNIX or Linux operating systems:
  WAS_HOME/bin/addNode.sh *dmgr_host portnumber* -profileName *profile_name* -username *dmgr_admin_user_id* -password *dmgr_admin_user_id*

The value of *WAS_HOME* is the location of the WebSphere Application Server home directory where the WebSphere Application Server core files are installed. The *dmgr_host* parameter is the host name of the computer on which the deployment manager is installed. The *portnumber* parameter specifies the SOAP port number that is assigned to the deployment manager. The default port number is 8887.
A node agent is created and started after a node is successfully added to a cell.

What to do next

Verify the federation of nodes within the cell.

Verifying the federation of nodes within the cell

After federating the node members in the cell, you must verify that the nodes are running correctly.

Before you begin

Ensure that you completed the necessary steps to federate node members.

Procedure

1. Use the following web address to access the administrative console.

   `http://hostname:port/ibm/console`

   The value of *hostname* is either the fully qualified host name or the IP address of the WebSphere Application Server deployment manager. The value of *port* is the port number for the WebSphere administrative HTTP transport. The default value is 9060. If there is another instance of the WebSphere Application Server on the computer, the port number might not be 9060.
2. Click **System administration** from the Integrated Solutions Console root structure.
3. Click Nodes. Verify that the manager node and federated nodes are listed and are available. You can also click **Nodeagent** to see the status of all node agents.

What to do next

Create WebSphere clusters for IBM Security Identity Manager.

Creating the WebSphere clusters for the Security Identity Manager application

You must create two server clusters in your WebSphere Application Server environment. One cluster hosts the Security Identity Manager application. The other cluster is used as a messaging service.

Before you begin

Before you create the cluster, make sure that all node agents are running.

Procedure

1. Use the following web address to access the administrative console:

   `http://hostname:port/ibm/console`

   The value of *hostname* is either the fully qualified host name or the IP address of the WebSphere Application Server deployment manager. The value of *port* is the port number for the WebSphere administrative HTTP transport. The default value is 9060. If there is another instance of the WebSphere Application Server on the computer, the port number might not be 9060.
2. Click **Servers** from the Integrated Solutions Console root structure.
3. Click **Clusters** > **WebSphere Application Server clusters**.
4. Specify the name of the host application cluster. For example, `ITIM_Application_Cluster`. The cluster name must be unique within the cell.
5. Use the default check box settings, and click **Next**.
6. Specify a member name for the first cluster member.
7. Specify the node you want to use to host the first cluster member.
8. Click **Create the member using an application server template** and select **default**.

9. Keep all other default settings and click **Next**.
10. Create a cluster member for each server in the topology. For `ITIM_Application_Cluster`, you must create at least one server on every node. If resources are available and you want to use a vertical cluster topology, you can define more than one server per node.
    a. Specify a member name and select a node.
    b. Click **Add Member**.
    c. Click **Next** when you finish adding cluster members.
11. Verify the summary of information and click **Finish**.
12. Repeat this process for the messaging cluster, specifying unique names for the messaging cluster and cluster members, such as `ITIM_Messaging_Cluster`. Define at least two application servers on separate nodes.
13. When you finish creating the second cluster, click **Servers** from the Integrated Solutions Console root structure.
14. Click **Clusters** to verify that your clusters are displayed.
15. Click the name of each cluster and click **Cluster members** to view detailed information about each cluster member.

What to do next

Install the Security Identity Manager Server.

Installation and configuration of IBM HTTP Server and WebSphere Web Server plug-in (optional)

You can install the IBM HTTP Server and the WebSphere Web Server plug-in on the same computer that has the deployment manager. However, you might want to install the IBM HTTP Server and the WebSphere Web Server plug-in on a separate computer for additional security and load balancing.

IBM HTTP Server

For information about installing IBM HTTP Server, see the product documentation for IBM HTTP Server for WebSphere Application Server in the IBM WebSphere Application Server section of the IBM Knowledge Center.

WebSphere Web Server plug-in

For information about installing the WebSphere Web Server plug-in, see *Installing Web server plug-ins* in the WebSphere Application Server, Network Deployment Version 7.0 section of the IBM Knowledge Center.

If an HTTP server is used, you must use the administrative console to map the IBM Security Identity Manager applications to the HTTP web server name. See "Mapping the IBM Security Identity Manager application" on page 122 for the mapping procedure.

WebSphere Application Server performance tuning tasks

Performance issues can occur after you initially configure WebSphere Application Server These tasks describe actions you can take to ensure that WebSphere Application Server runs correctly.

Disabling Performance Monitoring Infrastructure (PMI) tracking

By default, WebSphere Application Server has the Performance Monitoring Infrastructure (PMI) enabled and set at the Basic level. At this level, URIRequestCount and URIServiceTime monitoring is enabled. These enablements cause performance problems when using the Console GUI because of the unique URLs that are generated for that interface.

Before you begin

Ensure that WebSphere Application Server is correctly installed on your system.

About this task

To prevent performance degradation, either disable PMI entirely or disable these specific PMI flags:

Procedure

1. Log on to the administrative console.
2. From the left navigation pane, click **Monitoring and Tuning** > **Performance Monitoring Infrastructure (PMI)**.
3. Click the name of the server you want to manage.
4. Select **Custom** and click the **Custom** link.
5. Select **Web Applications** from the tree listing.
6. Select **URIConcurrentRequests**.
7. Select **URIRequestCount**.
8. Select **URIServiceTime**.
9. Click **Disable** at the top of the pane.
10. Click **Save** to save the configuration.
11. Repeat this procedure for each application server that runs Security Identity Manager.
12. Restart all application servers for the changes to take effect.

What to do next

Do additional tuning.

Changing TCP KeepAlive settings on WebSphere Application Server

The failover design of the messaging engine relies upon the database connections to be 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 install WebSphere Application Server correctly on your system.

Procedure

1. Log in as a system administrator.
2. Run the following command:

```
echo 30 >  /proc/sys/net/ipv4/tcp_keepalive_intvl
```

Note: These settings are also used by IPv6 implementations.

3. Verify the update by checking the file `tcp_keepalive_intvl` to see that the value now is 30.

What to do next

Do additional tuning.

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 WebSphere Application Server user realm can be used as an authentication user registry for IBM Security Identity Manager. WebSphere 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 WebSphere Application Server user realms, see the WebSphere 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 WebSphere security domain.

Collecting information from the external user registry

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

Procedure

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

   The exact steps for installing and configuring are specific to the user registry product. For example, for an LDAP registry, you must create a suffix, a domain, a user template, and a user realm. For an example of an IBM Security Directory Server user registry, see "User registry configuration for external user registry," on page 293.
2. Collect the information that is required to configure the WebSphere security domain.

   For example, for an LDAP user registry:

Table 8. User registry configuration settings needed for WebSphere 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

Table 8. User registry configuration settings needed for WebSphere security domain configuration (continued)

Setting	Example
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

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 9. 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 10. 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 11. 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**.

Configuring a WebSphere security domain

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

About this task

You can configure WebSphere 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 WebSphere 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 WebSphere 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 WebSphere 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 12. 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 Tivoli Directory Server host name or IP address
Port	The LDAP server port for IBM Tivoli Directory Server
Base DN	The base DN of the LDAP registry
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 WebSphere 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 WebSphere Application Server.

Results

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

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 13. Installation and data synchronization process

Task	For more information
Install Cognos Business Intelligence.	1. Access http://www.ibm.com/support/knowledgecenter/SSEP7J_10.2.1/com.ibm.swg.ba.cognos.cbi.doc/welcome.html. 2. Search for **Install Cognos BI on one computer**. 3. Additionally, install IBM Cognos fix pack 1.
Install Framework Manager.	1. Access http://www.ibm.com/support/knowledgecenter/SSEP7J_10.2.1/com.ibm.swg.ba.cognos.cbi.doc/welcome.html. 2. Search for **Installing Framework Manager**.
Complete the data synchronization.	Go to Data synchronization **Note:** Run the data synchronization before you generate the reports to obtain the latest report data.

Cognos reporting

Security Identity Manager Version 6.0 fix pack 2Version 7.0 installs Cognos reports and models. To use these new reports and models, see the Cognos reporting documentation at IBM Cognos Business Intelligence documentation.

You can find the Cognos reports and models that are specific to Security Identity Manager at:

- *ISIM_HOME*/extensions/6.0/Cognos/Model/ISIMReportingModel_6.0 – ISIM model files
- *ISIM_HOME*/extensions/6.0/Cognos/Reports/ISIMReportingPackage_6.0.zip – ISIM report files

If Shared Enablement (SA) is enabled for IBM Security Privileged Identity Manager, you can find the models and reports specific to it at:

- *ISIM_HOME*/extensions/6.0/Cognos/Model/SAReportingModel_6.0 – ISPIM model files
- *ISIM_HOME*/extensions/6.0/Cognos/Reports/SAReportingPackage_6.0.zip – ISPIM report files

Chapter 5. Installation of Security Identity Manager Server

You can install and configure the IBM Security Identity Manager Server in either a single-server or a clustered environment.

You can also install and configure it silently. For more information, see Chapter 6, "Silent installation and configuration," on page 105.

If you plan to use Security Identity Manager Identity Service Center, you must install Security Identity Manager v 6.0 Fix Pack 2. For information about the installation of Security Identity Manager v 6.0 Fix Pack 2, see the Readme document *ISIM6.0.0FP2_InstallAndConfig_README.pdf*.

Preinstallation worksheet

The following table provides the typical preinstallation configuration parameters.

Table 14. Preinstallation worksheet

Field name	Description	Default or example value	Your value
ISIM_HOME	The installation directory for the IBM Security Identity Manager Server.	**Windows operating systems:** *path*\IBM\isim **UNIX or Linux operating systems:** *path*/IBM/isim	
WAS_HOME	The installation directory for WebSphere Application Server.	**Windows operating systems:** *path*\IBM\WebSphere\AppServer **UNIX or Linux operating systems:** *path*/IBM/WebSphere/AppServer	
WebSphere Application Server profile name	The name of the WebSphere Application Server profile.	**Single-server:** AppSrv01 **Deployment manager:** Dmgr01 **Cluster member:** Custom01	
WebSphere Application Server server name	The name of the WebSphere Application Server.	**Example:** server1	
Computer host name	The host name of the computer.		

Table 14. Preinstallation worksheet (continued)

Field name	Description	Default or example value	Your value
WebSphere Application Server administrator user ID	User name that is used to administer WebSphere Application Server. Used to restart WebSphere Application Server. This field is optional.	**Example:** `wsadmin`	
WebSphere Application Server administrator password	Password that is used with the WebSphere user name. This field is optional.		
Keystore password	Used to unlock the IBM Security Identity Manager keystore file that stores the encryption key to encrypt IBM Security Identity Manager sensitive data.		
ITDI_HOME	The directory that contains the IBM Tivoli Directory Integrator Server code and where adapters are installed. This field is optional depending on whether you are using IBM Tivoli Directory Integrator.	**Windows operating systems:** *path*`\IBM\TDI\V7.1` **UNIX or Linux operating systems:** *path*`/IBM/TDI/V7.1`	
TIVOLI_COMMON_DIRECTORY	The central location for all serviceability-related files, such as logs and first-failure capture data.	**Windows operating systems:** *path*`\IBM\tivoli\common` **UNIX or Linux operating systems:** *path*`/IBM/tivoli/common`	
Application cluster name	Application cluster name that is defined in the target WebSphere Application Server cell.	*isim_application_cluster*	

Table 14. Preinstallation worksheet (continued)

Field name	Description	Default or example value	Your value
Messaging cluster name	Messaging cluster name that is defined in the target WebSphere Application Server cell.	*isim_messaging_cluster*	

Note: If you are installing IBM Security Identity Manager on a Red Hat Linux server, complete these steps:

1. Ensure that you disable Security Enhanced Linux (SEL) before the installation. The installer might fail because of SEL default policy restrictions.
   - To determine whether Security Enhanced Linux is installed and running in an enforcement mode, run the **sestatus** command or check the `/etc/sysconfig/selinux` file.
   - To disable SEL, set SEL in permissive mode and run the **setenforce 0** command as a superuser, or modify the `/etc/sysconfig/selinux` file and reboot the system.
2. Ensure that you installed the necessary packages on the system before the installation. Run the `rpm -qa | grep` *package_name* command for each of the packages to ensure that they are properly installed. These packages must be present on the system for IBM Security Identity Manager and the prerequisite middleware to be installed correctly. For more information about Red Hat Enterprise Linux and WebSphere Application Server support, see "Hardware and software requirements" in *Product Overview Guide*.

   For the Red Hat Enterprise Linux 6 information, see "Configuring a Red Hat Linux server" on page 13.

Installation roadmap

The installation process consists of activities of installing, configuring, and verifying the Security Identity Manager Server.

The tasks to install and test the Security Identity Manager Server include:

1. Installing the Security Identity Manager Server on one of these configurations:
   - Single-server installation. Security Identity Manager supports both regular and silent installation. For more information about single-server installation, see "Installing IBM Security Identity Manager Server in a single-server environment" on page 80.
   - Cluster installation. Security Identity Manager supports both regular and silent installation. For more information about cluster installation, see "Installing IBM Security Identity Manager in a clustered environment" on page 91

   Note: For steps to upgrade from an existing installation of Security Identity Manager, see Chapter 15, "IBM Security Identity Manager upgrade," on page 229.

   For steps for a silent installation of Security Identity Manager, see Chapter 6, "Silent installation and configuration," on page 105.

2. Verifying that the Security Identity Manager Server and its components are correctly installed. See Chapter 7, "Verification of the installation," on page 113.
3. Configuring Security Identity Manager. See Chapter 8, "Configuration of the Security Identity Manager Server," on page 119.
4. Troubleshooting any problems that happened during the installation and startup. For more information, see Chapter 10, "Troubleshooting," on page 167.

Worksheet

The following table provides the typical system configuration parameters:

Installation worksheet

Field name	Description	Default or example value	Your value
Heart beat (seconds)	Defines how frequently a scheduling thread queries the scheduled message stores for events to process.	30	
Recycle bin age limit (days)	Specifies the number of days that an object remains in the recycle bin of the system before it becomes available for deletion by cleanup scripts.	62	
Maximum pool size	Specifies the maximum number of connections that the LDAP Connection Pool can have at any time.	100	
Initial pool size	Specifies the initial number of connections to be created for the LDAP Connection Pool.	50	
Increment count	Specifies the number of connections to be added to the LDAP Connection Pool when a connection is requested after all connections are in use.	3	
Database pool initial capacity	Specifies the initial number of JDBC connections.	5	
Database pool maximum capacity	Specifies the maximum number of JDBC connections that the Security Identity Manager Server can open to the database at any time.	50	
Logging trace level	Specifies the amount of information written to the log file.	MIN	

Installation worksheet

Field name	Description	Default or example value	Your value
Security Identity Manager Base Server URL	Specifies the published login Universal Resource Locator (URL) for the Security Identity Manager Server. It is the first part of a URL that is sent to the recipient of mail messages at run time.	Examples: `http://hostname:9080/itim/console`	
Mail from	Specifies the Security Identity Manager system administrator email address for your site.	Example: `admin@mysite.com`	
Mail server name	Specifies the SMTP mail host that sends mail notification and functions as the mail gateway.	Example: `smtp.mysite.com`	
Customer logo	Specifies the path and file name of the logo graphic.	`ibm_banner.gif`	
Customer logo link	Specifies an optional URL link activated by clicking the logo image.	`www.ibm.com`	
List page size	Specifies how many items that require a search in the directory show on lists throughout the user interface.	50	
Encryption	Option to encrypt the passwords used for database and directory server connections and the password of Security Identity Manager System User used for System authentication.	True (On)	
WebSphere Administrator	Specifies the WebSphere administrator and the WebSphere administrator password.		
WebSphere Administrator Password	Specifies the WebSphere administrator password.		
Security Identity Manager System User	Specifies the Security Identity Manager System user ID.		
Security Identity Manager System User Password	Specifies the Security Identity Manager System User password **Note:** The Security Identity Manager System User password is restricted to 12 characters.		

Installing IBM Security Identity Manager Server in a single-server environment

You must perform multiple tasks to install and configure the IBM Security Identity Manager Server in a single-server environment.

Before you begin

Before you begin to install Security Identity Manager Server in a single-server environment, complete these tasks:

- Ensure that the system on which you install IBM Security Identity Manager must be secured during the installation process.
- Determine which product DVDs that you need to install IBM Security Identity Manager. For itemized DVD contents, see the text file `itim-6.0-dvd-images-operatingsystem.txt` that is provided with the DVD image. For a complete list of these image files, see "Downloading Security Identity Manager" on page 11.
- Ensure that free disk space and memory requirements are met. Additionally, ensure that there is adequate free disk space in the system temp directory and in the *WAS_PROFILE_HOME* directory. The target computer must meet the computer requirements described in *Hardware and software requirements* on the IBM Security Identity Manager product documentation site.
- Ensure that you have the needed administrative authority. On Windows systems, the logon user ID must be in the Administrators Group. On UNIX systems, the logon user ID must be root.
- Installing the Security Identity Manager Server writes data to the Security Identity Manager database.
- Ensure that the prerequisite applications are installed and running:

Prerequisite	For more information, see
Database	"Database installation and configuration" on page 15
Directory server	"Installation and configuration of a directory server" on page 36
Directory integrator (optional)	"Optionally installing IBM Security Directory Integrator" on page 47
WebSphere Application Server	"Installation and configuration of WebSphere Application Server" on page 51

  Only IBM Security Identity Manager and WebSphere Application Server require installation on the same computer. All other applications can be run locally or remotely to the computer on which Tivoli Identity Manager is installed. IBM Tivoli Directory Integrator is an optional component.
- Ensure that IBM Security Identity Manager Java 2 Security is disabled when the IBM Security Identity Manager installer is run. See "WebSphere security configuration" on page 7.
- If you want IBM Security Identity Manager to use an external user registry for authentication, complete the steps in "Preinstall configuration for authentication with an external user registry" on page 69.
- Ensure that the WebSphere Application Server can be stopped and started before you install the Security Identity Manager server. To be sure, stop and start the WebSphere Application Server. For more information about these steps, see "Installation and configuration of WebSphere Application Server" on page 51.

- Capture the details of your configuration. For a detailed list of configuration parameters, see *Preinstallation worksheet* in Chapter 4, "Installation of prerequisite components," on page 13.
- If you are upgrading a version of Security Identity Manager that is already on the computer, see Chapter 15, "IBM Security Identity Manager upgrade," on page 229. That topic provides more information about protecting Security Identity Manager customization and data.

Procedure

1. Start the installation wizard
2. Complete the installation wizard pages
3. Respond to major installation actions.

Starting the installation wizard

Use the installation wizard to install the IBM Security Identity Manager Server in a single-server environment. All other components must be already installed.

Before you begin

Ensure that you completed all the prerequisite tasks that are specified in "Installing IBM Security Identity Manager Server in a single-server environment" on page 80.

Note: If you are installing IBM Security Identity Manager on a computer that runs Windows Server 2012, you must set the compatibility mode before you start the installation wizard. Copy the `instwin.exe` file to your file system.

1. Navigate to the IBM Security Identity Manager installation directory.
2. Right click `instwin.exe`.
3. Click **Properties** > **Compatibility**.
4. Select the **Run this program in compatibility mode for:** check box.
5. From the list select **Windows 7**.
6. Click **OK**.

Procedure

1. Log on to an account with system administration privileges on the computer where the IBM Security Identity Manager Server is to be installed.
2. Start the installation program, or insert the product DVD into the DVD drive. To locate the correct DVD for your environment, see "Downloading Security Identity Manager" on page 11.
3. Run the installation program.
   - On the Windows operating systems:
     a. Click **Start** > **Run**.
     b. Enter the drive and path where the installation program is located and then enter the following command:

        ```
        instwin.exe
        ```

        The Welcome window opens.
   - On the UNIX or Linux operating systems:

     Note: The installation program on a UNIX or Linux system needs at least 150 MB of free space in the `/tmp` directory. If your system does not have enough space, set the *IATEMPDIR* environment variable to a directory on a disk partition that has enough free disk space.

To set the variable, enter one of the following commands at the command-line prompt before you run the installation program again:

– Bourne shell (sh), ksh, bash, and zsh:

```
$ IATEMPDIR=temp_dir
$ export IATEMPDIR
```

– C shell (csh) and tcsh:

```
$ setenv IATEMPDIR temp_dir
```

where *temp_dir* is the path to the directory, for example, `/your/free/directory`, where free disk space is available.

a. Open a command shell prompt window and select the directory where the installation program is located.

b. Enter one of the following commands for the Security Identity Manager installation program:

– AIX operating systems:

```
instaix.bin
```

– Linux operating systems:

```
instlinux.bin
```

– Linux for pSeries operating systems:

```
instzlinup.bin
```

– Linux for zSeries operating systems:

```
instzlinux.bin
```

The installation program starts and opens the Welcome window.

What to do next

Complete the installation wizard pages.

Completing the installation wizard pages

Use the first set of installation wizard pages to set up the installation.

Before you begin

Ensure that the installation wizard is started.

About this task

The dollar sign ($) has special meaning in the installer frameworks used by Install Anywhere. Do not use $ in any field values. The installation program framework or operating system platform might do variable substitution for the value.

Follow the procedure to complete the installation wizard pages.

Procedure

1. To change the language that is used for the installation wizard pages, select another language from the list and click **OK**. This choice affects only the installation wizard but not the language version of IBM Security Identity Manager to be installed.

   Note: The license is always shown in the system locale but not the installation language selected.

2. Click **Next** to advance past the copyright and legal text.

Note: If you are installing IBM Security Identity Manager on the AIX system and unable to see the copyright text, you must adjust the contrast color setting of the system. Change the contrast color setting from High to Low.

3. In the License Agreement window, read the license agreement and decide whether to accept its terms. To accept the terms and continue with the installation, select **Accept** and then click **Next**. Optionally click **Print** to print out the license agreement.
4. Specify the installation directory and click **Next**.
   - Accept the default *ISIM_HOME* installation directory. Or,
   - Click **Choose** to select another directory.
5. In the Installation Type window, select **Single WebSphere Application Server**. Then click **Next**. The WebSphere Application Server Installation Directory window opens with a value for the WebSphere Application Server installation directory or *WAS_HOME* directory.

   Note:
   - If you have WebSphere Application Server version 8.5 installed, the field is blank. You must click **Choose** to browse to and select the installation directory.
   - There can be multiple installations of the WebSphere Application Server on a computer. If the directory is not the directory in which you intend to install the IBM Security Identity Manager Server, click **Choose**. Enter the correct directory value and click **Next**.
6. From the WebSphere profile selection panel, select the WebSphere Application Server profile name in which IBM Security Identity Manager is to be installed from the list. Click **Next**.
7. Verify the following WebSphere Application Server data and click **Next**.
   - The WebSphere Application Server name, *server1* by default, where you intend to deploy the IBM Security Identity Manager Server.
   - The host name of the computer. Accept the shown value unless the computer has multiple host names and the WebSphere Application Server is installed under a host name other than the shown value.
8. If WebSphere Application Server administrative security is on, you must specify the administrator user ID and password, then click **Next**.
9. Select the type of security domain window for WebSphere Application configuration and click **Next**.
   - Select **Yes** to use the IBM Security Identity Manager custom registry.
   - Select **No** to use the existing security domain and registry.

   Note: If you select **Yes**, the new security domain is created and configured with the custom registry provided by IBM Security Identity Manager. IBM Security Identity Manager uses this custom registry for authentication decisions. If you select **No**:
   - IBM Security Identity Manager uses the current security domain configured for the application server. To review the preinstall instructions for how to configure the external user registry, see "Preinstall configuration for authentication with an external user registry" on page 69.
   - You must complete post-installation configuration steps after the installation wizard completes. See "Postinstall configuration of an external user registry for authentication" on page 156.

10. Enter the System user name and password and click **Next**. If you selected to create a security domain in the previous step, `isimsystem` is entered as the default System user.
11. In the Database Type window, select one of the following database types and then click **Next**.
    - IBM DB2 Universal Database
    - Oracle Database
    - Microsoft SQL (only listed for Windows operating systems)

    Caution windows open to confirm that these conditions are true:
    - If DB2 is selected, click **Continue**.
    - If the Oracle database or the Microsoft SQL database is selected, a window prompts you for the location and name of the JDBC driver. Provide the location and name, and click **Next**. For more information, see "Oracle JDBC driver installation" on page 30 or "SQL Server JDBC driver installation" on page 34.
    - The directory server version must be at the correct level. Confirm that the version is correct and click **Continue**.
12. In the Keystore Password window, specify the keystore password. The keystore password entered here is used to unlock the IBM Security Identity Manager keystore file. This file stores the encryption key used to encrypt the IBM Security Identity Manager sensitive data. Click **Next**.
13. Select whether to install Agentless adapters on IBM Tivoli Directory Integrator and click **Next**.

    The installation program installs these POSIX adapters for the following managed resources:
    - AIX
    - HP-UX
    - LDAP
    - Linux
    - Solaris

    Installation programs for the agentless adapters are in the *ISIM_HOME*`\config\adapters` directory. If needed, you can reinstall adapters later. The IBM Security Identity Manager installation program installs POSIX adapters. However, it is a good practice that you install the latest adapter profiles. For more information about manual adapter installation, see "Installing agentless adapters" on page 48 and "Installing agentless adapter profiles" on page 51.
14. In the Location of IBM Tivoli Directory Integrator window, in the Directory Integrator Home Directory field, enter or confirm the correct directory value and click **Next**. Optionally click **Choose** to select another location.
15. In the Do you want to install Shared Access Module window, decide whether you want to install Shared Access Module:
    - Select **Yes** if you purchased Shared Access Module. The installation program installs IBM Security Identity Manager with the Shared Access Module component.
    - Select **No** if you did not purchase Shared Access Module. The installation program installs only IBM Security Identity Manager Server. You can always install Shared Access Module separately later when you need it.

    Click **Next**.

16. In the Tivoli Common Directory window, accept the default directory that the installation program defines, or choose a new one. Click **Next**. Ensure that the directory has at least 25 MB of free space. The Tivoli Common Directory is the central location for all serviceability-related files, such as logs and first-failure capture data.
17. In the Single Server Pre-Installation Summary window, review the following information. If everything is acceptable, click **Install**.
    - The product name.
    - The IBM Security Identity Manager installation directory.
    - Your choice to install agentless adapters.
    - The WebSphere Application Server installation directory.
    - The required and available free disk space.

    Note: After you click **Install**, if you click **Cancel** to cancel the installation, you get a message that IBM Security Identity Manager is not installed. However, files are not automatically cleaned up through this action and this condition might result in a partial installation. Clean up any partial installation manually before running **Install** again.
18. When installation is complete, click **Done**. The installation program copies IBM Security Identity Manager files to the *ISIM_HOME* directory.

What to do next

Resolve any installation errors.

If you are using Microsoft SQL server 2008, you must change the lockTimeout value. This change must happen after the installation of IBM Security Identity Manager is complete when the data sources are already set up in WebSphere Application Server. To change the **lockTimeout** value:

1. Log on to the WebSphere Application Server administrative console.
2. Select **Resources**, then click **lockTimeout** > **JDBC** > **Data sources** > **ITIM Data Source** > **Custom properties**.
3. Set the **locktimeout** value to -1.
4. Click **OK**.
5. Save the change.

Response to major installation errors

The installation program copies Security Identity Manager files to the *ISIM_HOME* directory. It opens a series of progress windows for additional, major installation setup and configuration. This section addresses the errors that occur during this setup.

For more information, see “Verifying that the IBM Security Identity Manager Server is operational in a single-server environment” on page 116.

Correcting the WebSphere Application Server start error

The WebSphere Application Server must be running to allow IBM Security Identity Manager deployment and configuration to occur. The IBM Security Identity Manager installation program verifies the status of the WebSphere Application Server. If the WebSphere Application Server is not running, the installation program attempts to start the WebSphere Application Server.

Before you begin

Ensure that the WebSphere Application Server is installed correctly.

About this task

If the IBM Security Identity Manager installation program fails to start the WebSphere Application Server, an error message is shown.

If an error occurs:

Procedure

Do either of these steps:

- Quit the installation program and complete these steps:
  1. Resolve the problem that prevents starting the WebSphere Application Server.
  2. Manually delete all files in the *ISIM_HOME* directory.
  3. Run the installation program again.
- Continue the installation program after you ensure that you can manually start and stop the WebSphere Application Server without error. Complete these steps:
  1. Stop the WebSphere Application Server:
     - Windows operating systems

       WAS_PROFILE_HOME\bin\stopServer.bat *servername*
     - UNIX or Linux operating systems

       WAS_PROFILE_HOME/bin/stopServer.sh *servername*
  2. Start the WebSphere Application Server:
     - Windows operating systems

       WAS_PROFILE_HOME\bin\startServer.bat *servername*
     - UNIX or Linux operating systems

       WAS_PROFILE_HOME/bin/startServer.sh *servername*

Gathering database data and configuring the database

In this step, the IBM Security Identity Manager installation program sets up the Security Identity Manager database.

Before you begin

Ensure that the database is installed correctly.

About this task

If an error occurs, examine the error and provide a corrective action. There is more information in the *ISIM_HOME*\install_logs\dbConfig.stdout log file. See the documentation that the database product provides.

Continue the installation program. When the installation is completed, follow these steps:

Procedure

1. Save the current log data by renaming the *ISIM_HOME*\install_logs\dbConfig.stdout log file.

2. Make sure that the IBM Security Identity Manager messaging engine is not running. Log in to the WebSphere administrative console, and complete these steps:
   a. Click **Service Integration** > **Buses**.
   b. Click **itim_bus** if it exists.
   c. In the Topology section, click **Messaging engines**.

      For a single-server installation, you see an engine named *nodename.servername*-itim_bus.

      For a cluster installation, you see *n*+1 messaging engines, where *n* is the number of cluster members. An additional messaging engine is used for the messaging cluster.
   d. Select one or more messaging engines and click **Stop**.
3. When the correction is complete, use this command to configure the IBM Security Identity Manager database:
   - Windows operating systems:

     ISIM_HOME\bin\DBConfig.exe
   - UNIX or Linux operating systems:

     ISIM_HOME/bin/DBConfig

   New log data is recorded in the *ISIM_HOME*\install_logs\dbConfig.stdout log file.

What to do next

The **DBConfig** command creates the database table definitions that IBM Security Identity Manager requires. Run this command only if the command failed to configure the database during installation. If the database tables were previously set, running the **DBConfig** command first drops all the existing database tables. For more information, see "Manually starting the **DBConfig** database configuration tool" on page 119.

Proceed to the next step in the installation program.

Gathering directory server data and configuring the directory server

In this step, the IBM Security Identity Manager installation program sets up the LDAP schema and the default data entries for IBM Security Identity Manager.

Before you begin

Ensure that the directory server is installed correctly.

About this task

If an error occurs, record the error message. The message might describe a problem in setting up the LDAP schema or creating a configuration of data on the directory server.

Continue the installation program. When the installation is completed, complete these steps:

Procedure

1. Examine the errors and provide a corrective action. There is more information in the *ISIM_HOME*\install_logs\ldapConfig.stdout log file. See the documentation that the directory server product provides.
2. Save the current log data by renaming the *ISIM_HOME*\install_logs\ldapConfig.stdout log file.
3. When the correction is complete, use this command to configure the directory server:
   - Windows operating systems:
     ISIM_HOME\bin\ldapConfig.exe
   - UNIX or Linux operating systems:
     ISIM_HOME/bin/ldapConfig

   New log data is recorded in the *ISIM_HOME*\install_logs\ldapConfig.stdout log file.

What to do next

Running the **ldapConfig** command restores default values that Security Identity Manager uses. If you changed the value of any of these attributes, such as the password of the itim manager user ID, the value is overwritten. Do not run the **ldapConfig** command a second time, unless the LDAP configuration failed during the IBM Security Identity Manager Server installation process. For more information, see "Configuration of the directory server" on page 121.

Proceed to the next step in the installation program.

Gathering IBM Security Identity Manager data and configuring the IBM Security Identity Manager Server

The IBM Security Identity Manager installation program copies a set of property files to the *ISIM_HOME*\data directory. During this step, you can use the GUI to change some of the properties.

Before you begin

The installation program also configures the WebSphere environment settings that the IBM Security Identity Manager Server requires. This step takes several minutes to complete.

About this task

If an error occurs, record the error message. The message might describe a problem in configuring the WebSphere environment settings that the IBM Security Identity Manager Server requires.

Continue the installation program. When the installation is completed, complete these steps:

Procedure

1. Examine the errors and provide a corrective action. There is more information in the *ISIM_HOME*\install_logs\runConfigFirstTime.stdout log file. See the documentation that the WebSphere product provides.
2. When the correction is complete, use this command to update commonly used properties:

- Windows operating systems:
  ISIM_HOME\bin\runConfig.exe
- UNIX or Linux operating systems:
  ISIM_HOME/bin/runConfig

The **runConfig** utility also accepts an **install** parameter. Use **runConfig** with the **install** parameter when there is a problem reported for **runConfig** during the installation. If the **install** option is used, the system configuration requires several minutes to complete.

- Windows operating systems:
  ISIM_HOME\bin\runConfig.exe install
- UNIX or Linux operating systems:
  ISIM_HOME/bin/runConfig install

New log data is recorded in the *ISIM_HOME*\install_logs\runConfig.stdout log file.

What to do next

For more information, see "Configuration of commonly used system properties" on page 123.

Proceed to the next step in the installation program.

Correcting the deployment error

The IBM Security Identity Manager application runs within the WebSphere Application Server as an enterprise application. The IBM Security Identity Manager installation program uses the WebSphere command-line interface (wsadmin) to deploy the IBM Security Identity Manager application onto the WebSphere Application Server.

Before you begin

Ensure that WebSphere Application Server is installed correctly.

About this task

Deploying the IBM Security Identity Manager application also completes certain configuration steps on the WebSphere Application Server. These steps require several minutes to complete.

When the deployment is completed, the IBM Security Identity Manager files are in these directories:

- *WAS_PROFILE_HOME*\installedApps*cellname*\ITIM.ear
- *WAS_PROFILE_HOME*\config\cells*cellname*applications\ITIM.ear

Note: For the deployment manager node, these files are only in the *WAS_NDM_PROFILE_HOME*\config\cells*cellname*\applications\ITIM.ear directory.

Complete these steps, if you received an error message during the deployment.

Procedure

1. Correct the error.
   - If the log data indicates:

- A failure to establish a SOAP connection to the WebSphere Application Server configuration manager.
- Some type of WebSphere Application Server scripting error.

a. Exit the installation program.
b. Resolve the problem that prevents connection to the WebSphere Application Server or a problem described as a scripting error. For more information, see the WebSphere documentation.
c. Manually delete all files in the *ISIM_HOME* directory.
d. Run the installation program again.

- If the log data indicates that failure is caused by a timeout:
  - Continue the installation program.
  - When or if the installation program completes, delete the following directories if they exist.
    - *WAS_PROFILE_HOME*\installedApps*cellname*\ITIM.ear
    - *WAS_PROFILE_HOME*\config\cells*cellname*applications\ITIM.ear

2. Run one of these commands to deploy the IBM Security Identity Manager Server onto the WebSphere Application Server.
   - If WebSphere administrative security and application security is on, enter one of these commands:
     - Windows operating systems

       ```
       ISIM_HOME\bin\setupEnrole.exe install server:server_name user:user_id
       password:pwd ejbuser:ejb_user_id ejbpassword:ejbpassword
       ```

     - UNIX or Linux operating systems

       ```
       ISIM_HOME\bin\setupEnrole.sh install server:server_name user:user_id
       password:pwd ejbuser:ejb_user_id ejbpassword:ejbpassword
       ```

     The value of *server_name* is the name of the WebSphere Application Server on which the IBM Security Identity Manager application is deployed. The value of *user_id* is the WebSphere administrator user ID, such as *wsadmin*. The value of *pwd* is the password for the WebSphere administrator user ID, such as *secret*. The value of *ejb_user_id* is the IBM Security Identity Manager System user ID, which uses the WebSphere Application Server administrator user ID by default.

     Note: If the EJBUser ID contains a value with a space in between, such as *Bob Smith*, you must add a quotation mark to this value. The command, for example, must be entered as:

     ```
     SetupEnrole.exe install server:server1 user:wsadmin password:secret
     ejbuser:"Bob Smith" ejbpassword:secret
     ```

   - If WebSphere administrative security and application security is off, enter one of these commands:
     - Windows operating systems

       ```
       ISIM_HOME\bin\setupEnrole.exe install server:server_name
       ```

     - UNIX or Linux operating systems

       ```
       ISIM_HOME\bin\setupEnrole.exe install server:server_name
       ```

     The default of *server_name* is server1.

Restarting the WebSphere Application Server

If an error message indicates failure to restart the WebSphere Application Server, complete the installation and then attempt to restart the WebSphere Application Server.

Before you begin

Ensure that the WebSphere Application Server is installed correctly.

Procedure

1. Stop the WebSphere Application Server.
   - Windows operating systems

     WAS_PROFILE_HOME\bin\stopServer.bat *servername -user userid -password userpassword*
   - UNIX or Linux operating systems

     WAS_PROFILE_HOME/bin/stopServer.sh *servername -user userid -password userpassword*
2. Start the WebSphere Application Server.
   - Windows operating systems

     WAS_PROFILE_HOME\bin\startServer.bat *servername*
   - UNIX or Linux operating systems

     WAS_PROFILE_HOME/bin/startServer.sh *servername*

What to do next

Verify the installation. See Chapter 7, "Verification of the installation," on page 113.

Installing IBM Security Identity Manager in a clustered environment

You must perform multiple tasks to install and configure the IBM Security Identity Manager Server in a clustered environment. The installation program installs only the Security Identity Manager Server.

Before you begin

Read "Configuration options" on page 9.

Complete these tasks:

- Ensure that the system on which you install IBM Security Identity Manager must be secured during the installation process.
- Determine which product DVDs that you must install Security Identity Manager. For itemized DVD contents, see a text file such as `itim-6.0-dvd-images-operatingsystem.txt` that is provided with the DVD image. For a complete list of these image files, see "Downloading Security Identity Manager" on page 11.
- Meet free disk space and memory requirements on every computer in the cluster. Ensure that there is adequate free disk space in the system temp directory and in the *WAS_PROFILE_HOME* and *WAS_NDM_PROFILE_HOME* directories. The target computers must meet the computer requirements that are described in *Hardware and software requirements* in *Product overview* of the Security Identity Manager product documentation site.
- Ensure that you have the needed administrative authority. On the Windows systems, the logon user ID must be in the Administrators Group. On the UNIX systems, the logon user ID must be root.
- Installing the Security Identity Manager Server writes data to the Security Identity Manager database. Ensure that you have installed this database. If you use DB2, ensure that you have the required fix packs installed too and you run the middleware configuration utility. For more information, see "Database installation and configuration" on page 15.

- In a cluster, the name of the Security Identity Manager installation directory must be the same for all cluster members. Specify an identical directory to avoid later runtime difficulties in identity feed activities on different cluster member computers.
- Ensure that the prerequisite applications are installed and running:

Prerequisite	For more information, see
Database	"Database installation and configuration" on page 15
Directory server	"Installation and configuration of a directory server" on page 36
Directory integrator (optional)	"Optionally installing IBM Security Directory Integrator" on page 47
WebSphere Application Server	"Installation and configuration of WebSphere Application Server" on page 51

  Only IBM Security Identity Manager and WebSphere Application Server require installation on the same computer. All other applications can be run locally or remotely to the computer on which IBM Security Identity Manager is installed. IBM Tivoli Directory Integrator is an optional component.
- Ensure that IBM Security Identity Manager Java 2 Security is disabled when the IBM Security Identity Manager installer is run. See "WebSphere security configuration" on page 7.
- If you want IBM Security Identity Manager to use an external user registry for authentication, complete the steps in "Preinstall configuration for authentication with an external user registry" on page 69.
- Determine that the WebSphere Application Server cell and cluster are ready for IBM Security Identity Manager installation. Complete the steps to construct a WebSphere Application Server cell and a cluster, described in "Installation and configuration of WebSphere Application Server" on page 51.

  These processes must be running before and after you install the IBM Security Identity Manager Server:
  - Deployment manager
  - WebSphere Application Server node agents
- Capture the details of your configuration. For a detailed list of configuration parameters, see *Preinstallation worksheet* in Chapter 5, "Installation of Security Identity Manager Server," on page 75.
- If you are upgrading a version of IBM Security Identity Manager that is already on the computer, see Chapter 15, "IBM Security Identity Manager upgrade," on page 229. That topic provides more information about protecting IBM Security Identity Manager customizations and data.

About this task

Installation in a cluster configuration requires that you install the IBM Security Identity Manager Server on the following computers:

- The deployment manager

  Install the IBM Security Identity Manager Server on the computer that has the deployment manager *before* you install the IBM Security Identity Manager Server on cluster nodes. The deployment of the IBM Security Identity Manager application and the configuration of the database and the directory server for IBM Security Identity Manager occur during this installation. The deployment manager distributes and expands the IBM Security Identity Manager application to all cluster member computers.

- Cluster members

  Repeat the steps to install the IBM Security Identity Manager Server on each computer that is a cluster member. The installation program does these tasks:

  – Copies IBM Security Identity Manager files to the target computer.

  – Configures the WebSphere Application Server that hosts the cluster member.

  Installing the IBM Security Identity Manager Server on clusters must be done sequentially, one computer at a time. Running the IBM Security Identity Manager installation program simultaneously on more than one computer might result in synchronization problems with the WebSphere master configuration file.

Note: If the same computer has both the deployment manager and an IBM Security Identity Manager cluster member, you *must* select both node types when you run the installation program.

To install the IBM Security Identity Manager Server in a clustered environment:

Procedure

1. Start the installation wizard.
2. Complete the installation wizard pages.
3. Respond to major installation actions.

Starting the installation wizard

Use the installation wizard to install the IBM Security Identity Manager Server in a clustered environment. All other components must be already installed.

Before you begin

Ensure that you completed all the prerequisite tasks that are specified in "Installing IBM Security Identity Manager in a clustered environment" on page 91.

Note: If you are installing IBM Security Identity Manager on a computer that runs Windows Server 2012, you must set the compatibility mode before you start the installation wizard. Copy the `instwin.exe` file to your file system.

1. Navigate to the IBM Security Identity Manager installation directory.
2. Right click `instwin.exe`.
3. Click **Properties** > **Compatibility**.
4. Select the **Run this program in compatibility mode for:** check box.
5. From the list select **Windows 7**.
6. Click **OK**.

Procedure

1. Log on to an account with system administration privileges on the computer where the IBM Security Identity Manager Server is to be installed.
2. Install the installation program, or insert the IBM Security Identity Manager product DVD into the DVD drive. To locate the correct DVD for your environment, see "Downloading Security Identity Manager" on page 11.
3. Run the installation program.
   - Windows operating systems:
     a. Click **Start** > **Run**.
     b. Enter the drive and path where the installation program is and then enter the following command:

```
instwin.exe
```

The Welcome window opens.

- UNIX or Linux operating systems:

  The installation program on a UNIX or Linux system needs at least 150 MB of free space in the `/tmp` directory. If your system does not have enough space, set the *IATEMPDIR* environment variable to a directory on a disk partition that has enough free disk space.

  To set the variable, enter one of the following commands before you run the installation program again:

  – Bourne shell (sh), ksh, bash, and zsh:

    ```
    $ IATEMPDIR=temp_dir
    $ export IATEMPDIR
    ```

  – C shell (csh) and tcsh:

    ```
    $ setenv IATEMPDIR temp_dir
    ```

  where *temp_dir* is the path to the directory, for example, `/your/free/directory`, where free disk space is available.

  a. Open a command shell prompt window and select the directory where the installation program is.
  b. Enter one of the following commands for the installation program:
     – AIX operating systems:

       ```
       instaix.bin
       ```

     – Linux operating systems:

       ```
       instlinux.bin
       ```

     – Linux for pSeries operating systems:

       ```
       instplinux.bin
       ```

     – Linux for zSeries operating systems:

       ```
       instzlinux.bin
       ```

The installation program starts and opens the Welcome window.

What to do next

Complete the installation wizard pages.

Completing the installation wizard pages

Use the first set of installation wizard pages to set up the installation.

Before you begin

Ensure that the installation wizard is started.

About this task

The dollar sign ($) has special meaning in the installation program frameworks used by Install Anywhere. Do not use $ in any field values. The installation program framework or operating system platform might do variable substitution for the value.

Follow this procedure to complete the installation wizard pages.

Procedure

1. To change the language for the installation wizard pages, select another language from the list and click **OK**. This choice affects only the installation wizard and not the language version of the IBM Security Identity Manager Server to be installed.

   Note: The license is always shown in the system locale and not the installation language selected.
2. Click **Next** to advance past the copyright and legal text.

   Note: If you are installing IBM Security Identity Manager on the AIX system and unable to see the copyright text, you must adjust the contrast color setting of the system. Change the contrast color setting from High to Low.
3. In the License Agreement window, read the license agreement and decide whether to accept its terms. To accept the terms and continue with the installation, select **Accept**, and then click **Next**. Optionally click **Print** to print out the license agreement.
4. In the Installation Directory window, specify the installation directory and click **Next**.
   - Accept the default *ISIM_HOME* installation directory.
   - Select **Choose** to select another directory.
5. In the Installation Type window, select **WebSphere cluster**. Then, click **Next**.
6. In the Installing IBM Security Identity Manager on a Cluster Environment window, read the conditions that apply to a cluster environment. Click **Next**. Before continuing, apply any other changes that are necessary to configure the environment for these conditions. For example, verify that the deployment manager and all WebSphere node agents are running. For more information, see "Verifying the federation of nodes within the cell" on page 66.
7. In the Choose Cluster Node Type window, select one or both of these node types.
   - Deployment manager

     You must install IBM Security Identity Manager first on the computer that has the deployment manager.
   - Cluster member

     Install IBM Security Identity Manager on every cluster member that does not have the deployment manager on the same computer. If you have the deployment manager and an IBM Security Identity Manager cluster member on the same computer, you must select both node types.

   The WebSphere Application Server Installation Directory window opens with a value for the WebSphere Application Server installation directory or *WAS_HOME* directory.
   - If you have WebSphere Application Server version 8.5 installed, the field is blank. You must click **Choose** to browse to and select the installation directory.
   - There can be multiple installations of the WebSphere Application Server on a computer. If the directory is not the directory in which you intend to install the IBM Security Identity Manager Server, click **Choose**. Enter the correct directory value and click **Next**.
8. Specify a WebSphere profile name and click **Next**.

- If you selected a cluster member for the IBM Security Identity Manager installation, select the WebSphere Application Server profile that hosts the cluster member.
- If you selected the deployment manager for the IBM Security Identity Manager installation, select the WebSphere Application Server profile name from the list. This profile name is the network deployment manager in which IBM Security Identity Manager is to be installed.

If you selected the deployment manager for the IBM Security Identity Manager installation, caution windows open. These windows confirm that the directory server version is at the correct level. Confirm that the version is correct and click **Continue**.

9. In the data window that requests the cluster name, enter the names of both the IBM Security Identity Manager application cluster and the messaging cluster you created. Then click **Next**.
10. Verify the host name of the computer and click **Next**. Accept the value unless the computer has multiple host names and either the deployment manager or WebSphere Application Server is installed under other host name.
11. If WebSphere Application Server administrative security is on, specify the administrator user ID and password, then click **Next**.
12. This step is only for installation on the system with deployment manager. Select the type of security domain window for WebSphere Application Server configuration and click **Next**.
    - Select **Yes** to use the IBM Security Identity Manager custom registry.
    - Select **No** to use the existing security domain and registry.

    Note: If you select **Yes**, the new security domain is created and configured with the custom registry provided by IBM Security Identity Manager. IBM Security Identity Manager uses this custom registry for authentication decisions. If you select **No**:
    - IBM Security Identity Manager uses the current security domain configured for the application server. To review the preinstall instructions for how to configure the external user registry, see "Preinstall configuration for authentication with an external user registry" on page 69.
    - You must complete post-installation configuration steps after the installation wizard completes. See "Postinstall configuration of an external user registry for authentication" on page 156.
13. This step is only for installation on the system with deployment manager. Enter the IBM Security Identity Manager System user name and password and click **Next**. If you selected to create a security domain in the previous step, `isimsystem` is entered as the default IBM Security Identity Manager System user.
14. In the Database Type window, select one of the following database types, and then click **Next**.
    - DB2 Database
    - Oracle Database

    Caution windows open to prompt you to confirm that these conditions are true:
    - If DB2 is selected, click **Continue**.
    - If the Oracle database is selected, a window prompts you for the location and name of the JDBC driver. Provide the location and name, and click **Next**. For more information, see Installing the Oracle JDBC driver.

15. In the Keystore Password window, specify the keystore password. The keystore password entered here is used to unlock the IBM Security Identity Manager keystore file. This file stores the encryption key used to encrypt IBM Security Identity Manager sensitive data. Then, click **Next**.

    IBM Security Identity Manager creates the keystore file itim_keystore.jceks at the deployment manager node under the *WAS_NDM_PROFILE*\config\cells*cell_name*\isim directory. This file then propagates to all cluster member nodes in the *WAS_PROFILE_HOME*\config\cells*cell_name*\isim directory. The installer verifies the keystore password by attempting to open the keystore on installing IBM Security Identity Manager at the cluster member node. It does not happen when the deployment manager node and cluster member node are on the same computer. If the password is not correct, or the keystore file is not present, an error message occurs. If the keystore file is not present, copy the file from the deployment manager node to the cluster member node, and click **Next** again.

16. Select whether to install Agentless Adapters on IBM Tivoli Directory Integrator and click **Next**.

    The IBM Security Identity Manager installation program installs these POSIX adapters for the following managed resources:

    - AIX
    - HP-UX
    - LDAP
    - Linux
    - Solaris

    Installation programs for the agentless adapters that are installed by the IBM Security Identity Manager installation program are in the *ISIM_HOME*\config\adapters directory. If needed, you can reinstall adapters later. The Security Identity Manager installation program installs POSIX adapters. However, it is a good practice that you install the latest adapter profiles. For more information about manual adapter installation, see "Installing agentless adapters" on page 48 and "Installing agentless adapter profiles" on page 51.

    Note: If IBM Tivoli Directory Integrator is installed remotely, select **Do Not Install Agentless Adapters**.

17. In the Location of IBM Tivoli Directory Integrator window, enter or confirm the correct directory value and click **Next**. Optionally click **Choose** to enter another location.

18. In the Do you want to install Shared Access Module window, decide whether you want to install Shared Access Module:

    - Select **Yes** if you need and purchased Shared Access Module. The installer installs IBM Security Identity Manager with the Shared Access Module component.
    - Select **No** if you do not want to install Shared Access Module. The installer installs only IBM Security Identity Manager. You can always install Shared Access Module separately later when you need it.

19. In the Tivoli Common Directory window, accept the default directory that the IBM Security Identity Manager installation program defines, or choose a new one. Then, click **Next**. Ensure that the directory has at least 25 MB of free space. The Tivoli Common Directory is the central location for all serviceability-related files, such as logs and first-failure capture data.

20. In the Pre-Installation Summary window, review the following information. If everything is acceptable, click **Install**.
    - The product name.
    - The IBM Security Identity Manager installation directory.
    - Your choice to install agentless adapters.
    - The WebSphere Application Server installation directory.
    - The required and available free disk space.
    - Your choice to install Shared Access Module.

    Note: After you click **Install**, if you click **Cancel** to cancel the installation, you get a message that IBM Security Identity Manager is not installed. However, files are not automatically cleaned up through this action, and this condition might result in a partial installation. Clean up any partial installation manually before running **Install** again.
21. While installation is in progress, the Database Configuration window opens. Complete these fields: Host Name, Port Number, Database Name, Admin ID, and Admin Password. Click **Test** to test the database connection. If the database is connected, click **OK**.
22. The Database Configuration window opens for you to enter IBM Security Identity Manager User ID and User Password. Then click **Continue**.
23. The Directory Configuration window opens. Enter the information in these fields: Principal DN, Password, Host Name, and Port. Click Test to test the directory connection. If the directory is connected, click **OK**.

    Note: Testing connection is mandatory. You cannot continue configuring directory unless the directory is connected.
24. The Directory Configuration window opens for you to enter more information.

    Note: You must remember the information that you enter in these fields. Later when you install the product on each cluster member, you must enter the same information.
    Click **Continue**.
25. The System Configuration window opens. On the Mail tab, enter the information in the fields and click **OK**.
26. When installation is complete, click **Done**. The installation program copies Security Identity Manager files to the *ISIM_HOME* directory.
27. For each cluster member installation, repeat Step 1 to Step 20. When the installation is in progress, the System Configuration window opens for you to verify the information and test the connection:
    a. On the Mail tab, verify the information to ensure that it matches the first installation.
    b. On the General tab, verify the information to ensure that it matches the first installation.
    c. On the Directory tab, enter the password and host name and verify other information on this tab. Click **Test** to test the connection.
    d. On the Database tab, enter the password and check other information on this tab. Click **Test** to test the database connection.
    e. Verify the information on the Logging tab to ensure that it matches the first installation.

f. Verify and update the information on the UI tab. Ensure that it matches the first installation.
g. Enter the IBM Security Identity Manager user ID and password that you use for the first installation on the Security tab.
h. After verifying all information on the tabs, click **OK**.

28. When installation is complete, click **Done**.

What to do next

If the installation is completed successfully, go to the next step: "Starting clusters" on page 103. If errors occur during the installation, see "Response to major installation errors" to correct errors.

Response to major installation errors

The IBM Security Identity Manager installation program opens a series of progress windows for additional, major installation setup and configuration. This section addresses the errors that occur during this setup.

IBM Security Identity Manager files copied to the target computer

The installation program copies Security Identity Manager files to the *ISIM_HOME* directory.

If installation is on the deployment manager, the next step is gathering database data and configuring the database.

Correcting the database setup error

When setting up the database, if an error occurs, check the information in the *ISIM_HOME*\install_logs\dbConfig.stdout log file. Also see the documentation that the database product provides.

Before you begin

Ensure that the database is installed correctly.

Procedure

1. Save the current log data by renaming the *ISIM_HOME*\install_logs\dbConfig.stdout log file.
2. Make sure that the IBM Security Identity Manager messaging engine is not running. Log on to the WebSphere administrative console, and complete these steps:
   a. Click **Service Integration** > **Buses**.
   b. Click **itim_bus**, if it exists.
   c. In the Topology section, click **Messaging engines**.

      For a single-server installation, you see an engine named *nodename.servername*-itim_bus.

      For a cluster installation, you see *n*+1 messaging engines, where *n* is the number of IBM Security Identity Manager cluster members. An additional messaging engine is used for the IBM Security Identity Manager messaging cluster.
   d. Select one or more messaging engines and click **Stop**.
3. Use this command to configure the IBM Security Identity Manager database:
   - Windows operating systems

ISIM_HOME\bin\DBConfig.exe

- UNIX or Linux operating systems

  ISIM_HOME/bin/DBConfig

New log data is recorded in the *ISIM_HOME*\install_logs\dbConfig.stdout log file.

Note: The **DBConfig** command creates the database table definitions that IBM Security Identity Manager requires. Run this command only if the command failed to configure the database during installation. If the IBM Security Identity Manager database tables were previously set, running the **DBConfig** command first can drop all the existing IBM Security Identity Manager tables. For more information, see "Manually starting the **DBConfig** database configuration tool" on page 119.

Correcting the directory server setup error

When setting up the LDAP schema and configuring data on the directory server, if an error occurs, record the error message.

Before you begin

Ensure that the directory server is installed correctly.

Procedure

1. When the installation is completed, examine the errors and provide a corrective action. There is more information in the *ISIM_HOME*\install_logs\ldapConfig.stdout log file. You might also need to see documentation that the directory server product provides.
2. Save the current log data by renaming the *ISIM_HOME*\install_logs\ldapConfig.stdout log file.
3. When the correction is complete, use this command to configure the directory server:
   - Windows operating systems

     ISIM_HOME\bin\ldapConfig.exe
   - UNIX or Linux operating systems

     ISIM_HOME/bin/ldapConfig

   New log data is recorded in the *ISIM_HOME*\install_logs\ldapConfig.stdout log file.

   Note: Running the **ldapConfig** command restores default values that IBM Security Identity Manager uses. If you changed the value of any of these IBM Security Identity Manager attributes, such as the password of the itim manager user ID, the value is overwritten. Do not run the **ldapConfig** command a second time, unless the LDAP configuration fails during the IBM Security Identity Manager Server installation process.

What to do next

For more information, see "Configuration of the directory server" on page 121.

Correcting the IBM Security Identity Manager Server setup error

The IBM Security Identity Manager installation program also configures the WebSphere environment settings that the IBM Security Identity Manager Server requires. This step takes several minutes to complete. If an error occurs, record the

error message. The message might describe a problem in configuring the WebSphere environment settings that the IBM Security Identity Manager Server requires.

Before you begin

The IBM Security Identity Manager installation program copies a set of property files to the *ISIM_HOME*\data directory. During this step, you can use the GUI to change some of the IBM Security Identity Manager properties.

If the installation is on a cluster member, ensure that the directory and database connection information that you enter on the Directory and Database tabs match the information when you configure the deployment manager. The default database user ID is isimuser. The user password is the password that is used for the user ID isimuser during the deployment manager setup. The user ID and password used for the cluster member must be the same as the user ID and password used on the deployment manager. If any user information is incorrect, IBM Security Identity Manager does not function properly.

Procedure

1. Examine the errors and check the *ISIM_HOME*\install_logs\runConfigFirstTime.stdout log file. There is more information in the log file that can help solve the problems. You might also need to see documentation that the WebSphere product provides.
2. When the correction is complete, use this command to update commonly used IBM Security Identity Manager properties:
   - Windows operating systems

     ISIM_HOME\bin\runConfig.exe
   - UNIX or Linux operating systems

     ISIM_HOME/bin/runConfig

   The runConfig utility also accepts an **install** parameter. Use runConfig with the **install** parameter when there is a problem reported for runConfig during the IBM Security Identity Manager installation. If the **install** option is used, the system configuration requires several minutes to complete.
   - Windows operating systems

     ISIM_HOME\bin\runConfig.exe install
   - UNIX or Linux operating systems

     ISIM_HOME/bin/runConfig install

   New log data is recorded in the *ISIM_HOME*\install_logs\runConfig.stdout log file.

   For more information, see "Configuration of commonly used system properties" on page 123.

Correcting the deployment error

The IBM Security Identity Manager application runs within the WebSphere Application Server as an enterprise application. The IBM Security Identity Manager installation program uses the WebSphere command-line interface (wsadmin) to deploy the IBM Security Identity Manager application onto the WebSphere Application Server. If the deployment fails, an error message provides the location of the setupEnrole.stdout log file.

Before you begin

Ensure that WebSphere Application Server is installed correctly.

About this task

When the deployment is completed, the IBM Security Identity Manager files are in *WAS_NDM_PROFILE_HOME*\config\cells*cellname*applications\ITIM.ear directory.

Examine the errors in the setupEnrole.stdout log file. Then, complete these tasks:

Procedure

1. If the log data indicates following errors, complete these steps:
   - A failure to establish a SOAP connection to the WebSphere Application Server configuration manager.
   - Some type of WebSphere Application Server scripting error.

   a. Exit the IBM Security Identity Manager installation program.
   b. Resolve the problem that prevents connection to the WebSphere Application Server or a problem described as a scripting error. For more information, see the WebSphere documentation.
   c. Manually delete all files in the *ISIM_HOME* directory.
   d. Run the IBM Security Identity Manager installation program again.
2. If the log data indicates that failure is caused by a timeout, complete these steps:
   a. Continue the IBM Security Identity Manager installation program.
   b. When or if the IBM Security Identity Manager installation program completes, delete the following directory if it exists. *WAS_NDM_PROFILE_HOME*\config\cells*cellname*\applications\ITIM.ear.
   c. Run one of these commands to deploy the IBM Security Identity Manager Server onto the WebSphere Application Server.
      - If WebSphere administrative security and application security is on, enter one of these commands:
        – Windows operating systems

          ```
          ISIM_HOME\bin\setupEnrole.exe install server:server_name user:user_id
          password:pwd ejbuser:ejb_user_id ejbpassword:ejbpassword
          ```

        – UNIX or Linux operating systems

          ```
          ISIM_HOME\bin\setupEnrole.sh install server:server_name user:user_id
          password:pwd ejbuser:ejb_user_id ejbpassword:ejbpassword
          ```

          The value of *user_id* is the WebSphere administrator user ID, such as *wsadmin*. The value of *pwd* is the password for the WebSphere administrator user ID, such as *secret*. The value of *ejb_user_id* is the IBM Security Identity Manager EJB user ID, which uses the WebSphere Application Server administrator user ID by default.

          Note: If the EJBUser ID contains a value with a space in between, such as *Bob Smith*, you must add a quotation mark to this value. The command, for example, must be entered as:

          ```
          SetupEnrole.exe install server:server1 user:wsadmin password:secret
          ejbuser:"Bob Smith" ejbpassword:secret
          ```

      - If WebSphere administrative security and application security is off, enter one of these commands:
        – Windows operating systems

ISIM_HOME\bin\setupEnrole.exe install server:*server_name*

– UNIX or Linux operating systems

ISIM_HOME\bin\setupEnrole.exe install server:*server_name*

The default of *server_name* is server1.

Starting clusters

You must restart all node agents where cluster members are running before starting your clusters.

Before you begin

Ensure that the Security Identity Manager installation finished. Ensure that all configuration and security modifications are completed.

Procedure

1. Start both the Security Identity Manager application and the Security Identity Manager messaging cluster.
   a. Click **Servers** > **Clusters**.
   b. Select the Security Identity Manager clusters.
   c. Click **Start**. The Security Identity Manager application starts when the clusters start.
2. Verify that all required cluster members are started.
   a. Click **Applications** > **Enterprise Applications**. Examine the status of the Security Identity Manager application.
   b. Click **Servers** > **Application Servers**. Examine the status of the cluster members.
   c. Examine the log files for other problems. For more information, see "Log files" on page 180.
3. If the status of the Security Identity Manager application indicates a partial start, complete these steps:
   a. Locate the computer that has the cluster member that fails to start.
   b. Examine the following log files of the computer where the cluster member is to determine whether the Security Identity Manager Server started successfully:
      - WAS_PROFILE_HOME\logs\server_name\SystemOut.log
      - TIVOLI_COMMON_DIRECTORY\CTGIM\logs\trace.log
   c. Correct the problem. Then, use the WebSphere administrative console to start the cluster member.

What to do next

Verify the installation. See Chapter 7, "Verification of the installation," on page 113.

Chapter 6. Silent installation and configuration

You can install IBM Security Identity Manager in a silent mode. Silent mode reads response files that contain values to configure the directory server, database server, WebSphere Application Server, and IBM Security Identity Manager. Silent installation is supported in both single-server and cluster environments and for clean installation and upgrade.

The installation program receives data from the two response files: `installvariables.properties` and `configResponse.properties`. The `installvariables.properties` file has the installer-related values such as the installation directory, database type, or directory server type. The `configResponse.properties` file has the properties required for database configuration, LDAP configuration, and system configuration programs with different prefixes for each configuration program:

Database configuration
`dbConfigResponse.`*propertyName=value*

LDAP configuration
`ldapConfigResponse.`*propertyName=value*

System configuration
`sysConfigResponse.`*propertyFileName.propertyName=value*

There are different file names for an upgrade scenario. You need the following set of response files for clean installation and upgrade depending on the application server type.

Clean installation

- For single-server or deployment manager:
  `installvariables.properties, configResponse.properties`
- For cluster members:
  `installvariables.properties, configResponseCM.properties`

Upgrade

- For single-server or deployment manager:
  `installvariablesUpgrade.properties, configResponseUpgrade.properties`
- For cluster members:
  `installvariablesUpgrade.properties, configResponseCMUpgrade.properties`

You can use a different file name for the installation response file, for example, `installvariablesUpgrade.properties`. It can be passed to the installer with the **-f** flag, but the name of the configuration response file must always be `configResponse.properties`.

For the system configuration program, the `configResponse.properties` or `configResponseUpgrade.properties` template contains only the minimum set of required system properties with a prefix `sysConfigResponse`. You can add additional system properties to the file if necessary. Use this convention:
`sysConfigResponse.`*propertyFileName.propertyName=value*

For example, an IBM Tivoli Directory Server configuration has an authorization ID as *cn=root*:

```
sysConfigResponse.enRoleLDAPConnection.java.naming.provider.url=ldap:
//hostname:389
sysConfigResponse.enRoleLDAPConnection.java.naming.security.principal=cn=root
sysConfigResponse.enRoleLDAPConnection.java.naming.security.credentials=xxxxxx
```

The system configuration program that runs in silent mode sets the values of the listed properties in the `enRoleLDAPConnection.properties` file.

The silent installer reads the values from the `configResponse.properties` file and configures the IBM Security Identity Manager components. If a specific component configuration fails, then the utilities and the associated `.lax` file can be found in *ISIM_HOME*`\bin`. Each component of the installation can run silently by modifying the `IS_SILENT=<true/false>` property in the `.lax` file of the component.

Example response files

Example response files are in the base DVD in the `response_files` directory.

Completing a silent installation in a single-server environment

Use these steps to complete either a clean or an upgrade silent installation in a single-server environment.

Before you begin

Before you run the silent installation, you must install and configure any necessary middleware, such as a directory server, database server, directory integrator, and application server. Ensure that all these components are working correctly and that you entered the correct data. Any errors in setting up the system can result in the failure of silent installation.

Procedure

1. For a clean installation:
   a. Copy the response files `installvariables.properties` and `configResponse.properties` to a directory on the target computer.
   b. Update the response files with the correct values.
   c. Run `inst`*`platform`* `-i silent -f installvariables.properties` if you have the installer and the response files in the same directory. The names for the system platform installer programs are:
      - Windows operating systems: instwin.exe
      - AIX operating systems: instaix.bin
      - Linux operating systems: instlinux.bin
      - Linux for System p Operating Systems: instplinux.bin
      - Linux for System z Operating Systems: instzlinux.bin

      Note: If you have the installer and response files in the different directory or different drive, use the relative or absolute path for the `installvariables.properties` file. You must also use the absolute path for the `configResponse.properties` file. For example, if the response files are in the `C:\temp` directory on a Windows system, use this command:

      ```
      instwin.exe -i silent -f C:\temp\installvariables.properties
      -DITIM_CFG_RESP_FILE_DIR=C:/temp
      ```

UNIX systems use a different installer command, such as **instaix.bin** for AIX and a different path.

2. For an upgrade installation:
   a. Copy the response files `installvariablesUpgrade.properties` and `configResponseUpgrade.properties` to a directory on the target computer.
   b. Rename the `configResponseUpgrade.properties` file as `configResponse.properties`
   c. Update the response files with the correct values.
   d. Run `inst`*`platform`* `-i silent -f installvariablesUpgrade.properties` if you have the installer and response files in the same directory. The names for the system platform installer programs are:
      - Windows operating systems: instwin.exe
      - AIX operating systems: instaix.bin
      - Linux operating systems: instlinux.bin
      - Linux for System p Operating Systems: instplinux.bin
      - Linux for System z Operating Systems: instzlinux.bin

      Note: If you have the installer and response files in the different directory or different drive, use the relative or absolute path for the `installvariablesUpgrade.properties` file. You also must use the absolute path for the `configResponse.properties` file. For example, if the response files are in the `C:\temp` directory on a Windows system, use this command:

      ```
      instwin.exe -i silent -f C:\temp\installvariables.properties
      -DITIM_CFG_RESP_FILE_DIR=C:/temp
      ```

      UNIX systems use a different installer command, such as **instaix.bin** for AIX, and a different path.

What to do next

Silent installation might take some time to complete. To check on the installation progress, check the `itim_install_activity.log` file. This file is in the *`ISIM_HOME`*`\install_logs` directory.

Verify the installation and resolve any problems that happened during installation and startup. For more information, see *Verifying the installation*.

Completing a silent installation in a clustered environment

Use these steps to complete either a clean or an upgrade silent installation in a clustered environment.

Before you begin

Before you run the silent installation, you must install and configure any necessary middleware, such as a directory server, database server, directory integrator, and application server. Ensure that all these components are working correctly and that you entered the correct data. Any errors in setting up the system can result in the failure of silent installation.

Procedure

1. For a clean installation:

a. On the deployment manager, copy the response files `installvariables.properties` and `configResponse.properties` to a directory on the target computer.
b. Update the response files with the correct values.
c. Run `inst`*`platform`* `-i silent -f installvariables.properties` if you have the installer and response files in the same directory. The names for the system platform installer programs are:
   - Windows operating systems: instwin.exe
   - AIX operating systems: instaix.bin
   - Linux operating systems: instlinux.bin
   - Linux for System p Operating Systems: instplinux.bin
   - Linux for System z Operating Systems: instzlinux.bin

   Note: If you have the installer and response files in the different directory or different drive, use the relative or absolute path for the `installvariables.properties` file. You must also use the absolute path for the `configResponse.properties` file. For example, if the response files are in the `C:\temp` directory on a Windows system, use this command:

   ```
   instwin.exe -i silent -f C:\temp\installvariables.properties
   -DITIM_CFG_RESP_FILE_DIR=C:/temp
   ```

   UNIX systems use a different installer command, such as **`instaix.bin`** for AIX, and a different path.
d. On the cluster members, copy the response files `installvariables.properties` and `configResponseCM.properties` to a directory on the target computer.
e. Rename the `configResponseCM.properties` file as `configResponse.properties`.
f. Update the response files with the correct values.
g. Run `inst`*`platform`* `-i silent -f installvariables.properties` if you have the installer and response files in the same directory. The names for the system platform installer programs are:
   - Windows operating systems: instwin.exe
   - AIX operating systems: instaix.bin
   - Linux operating systems: instlinux.bin
   - Linux for System p Operating Systems: instplinux.bin
   - Linux for System z Operating Systems: instzlinux.bin

   Note: If you have the installer and response files in the different directory or different drive, use the relative or absolute path for the `installvariables.properties` file. You must also use the absolute path for the `configResponse.properties` file. For example, if the response files are in the `C:\temp` directory on a Windows system, use this command:

   ```
   instwin.exe -i silent -f C:\temp\installvariables.properties
   -DITIM_CFG_RESP_FILE_DIR=C:/temp
   ```

   UNIX systems use a different installer command, such as **`instaix.bin`** for AIX, and a different path.

2. For an upgrade installation:

a. On the deployment manager, copy the response files `installvariablesUpgrade.properties` and `configResponseUpgrade.properties` to a directory on the target computer.
b. Rename the `configResponseUpgrade.properties` file as `configResponse.properties`.
c. Update the response files with the correct values.
d. Run `inst`*`platform`* `-i silent -f installvariablesUpgrade.properties` if you have the installer and response files in the same directory. The names for the system platform installer programs are:
   - Windows operating systems: instwin.exe
   - AIX operating systems: instaix.bin
   - Linux operating systems: instlinux.bin
   - Linux for System p Operating Systems: instplinux.bin
   - Linux for System z Operating Systems: instzlinux.bin

   Note: If you have the installer and the response files in the different directory or different drive, use the relative or absolute path for the `installvariablesUpgrade.properties` file. You must also use the absolute path for the `configResponse.properties` file. For example, if the response files are in the `C:\temp` directory on a Windows system, use this command:

   ```
   instwin.exe -i silent -f C:\temp\installvariables.properties
   -DITIM_CFG_RESP_FILE_DIR=C:/temp
   ```

   UNIX systems use a different installer command, such as **`instaix.bin`** for AIX, and a different path.
e. On the cluster members, copy the response files `installvariablesUpgrade.properties` and `configResponseCMUpgrade.properties` to a directory on the target computer.
f. Rename the `configResponseCMUpgrade.properties` file as `configResponse.properties`.
g. Update the response files with the correct values.
h. Run `inst`*`platform`* `-i silent -f installvariablesUpgrade.properties` if you have the installer and response files in the same directory. The names for the system platform installer programs are:
   - Windows operating systems: instwin.exe
   - AIX operating systems: instaix.bin
   - Linux operating systems: instlinux.bin
   - Linux for System p Operating Systems: instplinux.bin
   - Linux for System z Operating Systems: instzlinux.bin

   Note: If you have the installer and the response files in the different directory or different drive, use the relative or absolute path for the `installvariablesUpgrade.properties` file. You must also use the absolute path for the `configResponse.properties` file. For example, if the response files are in the `C:\temp` directory on a Windows system, use this command:

   ```
   instwin.exe -i silent -f C:\temp\installvariables.properties
   -DITIM_CFG_RESP_FILE_DIR=C:/temp
   ```

   UNIX systems use a different installer command, such as `instaix.bin` for AIX, and a different path.

What to do next

Silent installation might take some time to complete. To check on the installation progress, check the `itim_install_activity.log` file. This file is in the *ISIM_HOME*`\install_logs` directory.

Verify the installation and resolve any problems that happened during installation and startup. For more information, see *Verifying the installation*.

Silent installation response files

Example response files are provided in the base DVD in the `response_files` directory.

Configuring the database silently

If the database configuration failed during the silent installation, you can correct the information in the `configResponse.properties` file and then start a silent database configuration.

Before you begin

Obtain the correct database information for the response file.

Procedure

1. Copy the `configResponse.properties` file to a directory on the target computer.
2. Update the `configResponse.properties` file with correct database information.
3. Edit the *ISIM_HOME*`/bin/DBConfig.lax` file to set the value for the following properties:

   ```
   IS_SILENT=true
   RESPONSE_FILE=full path to the configResponse.properties file
   ```

4. Start the database configuration program:

   ISIM_HOME`/bin/DBConfig`

Example

Example response files are in the base DVD in the `response_files` directory.

What to do next

The database configuration might take a few minute to complete. To monitor on the configuration progress, see the `dbConfig.stdout` file in the *ISIM_HOME*`/install_logs` directory.

Configuring the directory server silently

If the directory server configuration failed during the silent installation, follow these steps to configure the directory server silently.

Before you begin

Obtain the correct directory server information for the response file.

Procedure

1. Copy the configResponse.properties file to a directory on the target computer.
2. Update configResponse.properties file with correct database information.
3. Edit the *ISIM_HOME*/bin/ldapConfig.lax file to set the value for the following properties:

   ```
   IS_SILENT=true
   RESPONSE_FILE=full path to the configResponse.properties file
   ```

4. Start the LDAP configuration program:

   ```
   ISIM_HOME/bin/ldapConfig
   ```

Example

Example response files are provided in the base DVD in the response_files directory.

What to do next

The directory server configuration might take a few minute to complete. To monitor on the configuration progress, view the ldapConfig.stdout file in the *ISIM_HOME*/install_logs directory.

Configuring the system silently in a single-server environment

If the system configuration failed during the silent installation, follow these steps to configure the system silently.

Before you begin

Obtain the correct system information for the response file.

Procedure

1. Copy the configResponse.properties file to a directory on the target computer.
2. Update the configResponse.properties file with correct system information.
3. Edit the *IISIM_HOME*/bin/DBConfig.lax file to set the value for the following properties:

   ```
   IS_SILENT=true
   RESPONSE_FILE=full path to the configResponse.properties file
   ```

4. Start the WebSphere Application Server.
5. Start the server configuration program:

   ```
   ISIM_HOME/bin/runConfig -install
   ```

Example

Example response files are provided in the base DVD in the response_files directory.

What to do next

The system configuration might take a few minute to complete. To monitor the configuration progress, see the runConfig.stdout file in the *ISIM_HOME*/install_logs directory.

Configuring the system silently in a clustered environment

If the system configuration failed during the silent installation, follow these steps to configure the system again silently.

Before you begin

Obtain the correct system information for the response file.

Procedure

1. On the deployment manager, copy the `configResponse.properties` file to a directory on the target computer.
2. On the cluster member system, copy the `configResponseCM.properties` file and rename it to `configResponse.properties` in a directory on the target computer.
3. Update the `configResponse.properties` file with correct system information.
4. Edit the *ISIM_HOME*`/bin/DBConfig.lax` file to set the value for the following properties:

   ```
   IS_SILENT=true
   RESPONSE_FILE=full path to the configResponse.properties file
   ```
5. Start the WebSphere deployment manager and all the node agents.
6. Start the server configuration program:

   ISIM_HOME`/bin/runConfig -install`

Example

Example response files are provided in the base DVD in the `response_files` directory.

What to do next

The system configuration might take a few minute to complete. To monitor the configuration progress, see the `runConfig.stdout` file in the *ISIM_HOME*`/install_logs` directory.

Chapter 7. Verification of the installation

You must verify that the database, the directory server, and other programs that the Security Identity Manager Server uses are correctly configured. They must also be in full communication with the Security Identity Manager Server.

Verifying that the WebSphere Application Server is running

The WebSphere Application Server on which the Security Identity Manager application is deployed must be running.

Before you begin

Ensure that you completed all the installation and configuration tasks for Security Identity Manager and its components.

Procedure

Enter one of these commands:

- Windows operating systems

  WAS_PROFILE_HOME\bin\serverStatus.bat -all
- UNIX or Linux operating systems

  WAS_PROFILE_HOME/bin/serverStatus.sh -all

Note: If you do not find the process running, run one of these commands to start the server:

- Windows operating systems
  - *WAS_PROFILE_HOME*\bin\startServer.bat *server_name*
- UNIX or Linux operating systems -
  - *WAS_PROFILE_HOME*/bin/startServer.sh *server_name*

  The value of *server_name* is the name of the WebSphere Application Server. For example, server1.

What to do next

Additionally, examine the log files in the logs directory for entries that indicate the status of server1. For example, examine the log files in the *WAS_PROFILE_HOME*\logs\server1 directory.

If you cannot start the server, see Chapter 10, “Troubleshooting,” on page 167.

Start the WebSphere administrative console and complete additional verification tasks.

Starting the WebSphere Application Server administrative console

You must have the WebSphere Application Server administrative console running so that you can verify that the Security Identity Manager components are running correctly.

Before you begin

You must have a WebSphere Application Server user ID. If security is enabled, you also need a password.

Procedure

1. On a web browser, enter this address:
   `http://hostname:port/ibm/console`

   The value of *hostname* is the fully qualified host name or the IP address of the computer on which the WebSphere Application Server is running. The value of *port* is the port number for the WebSphere administrative HTTP transport. The default value is 9060.
2. Enter your user ID and, if required, password.
3. Click **OK**.

What to do next

You can continue with various administrative tasks to verify the Security Identity Manager installation.

Verifying the database connections

Before starting the Security Identity Manager Server, use the WebSphere administrative console to test the database connection.

Before you begin

Ensure that the database is installed and running.

Ensure that the WebSphere Application Server is running and that the WebSphere administrative console is started.

Procedure

1. Log on to the WebSphere administrative console.
2. **Resources** > **JDBC** > **Data Sources**.
3. Select **ITIM Data Source**.
4. Click **Test Connection**. A message opens that indicates the test result.
5. Repeat these steps for:
   - **ITIM Bus DataSource**
   - Additionally for clusters only, **ITIM Bus Shared DataSource**

What to do next

If any connections do not work, see Chapter 10, “Troubleshooting,” on page 167.

Perform other verification tasks.

Verifying that the directory server is running correctly

This information describes the steps to ensure that the installed directory server for Security Identity Manager is running.

Before you begin

Ensure that the directory server is installed.

Procedure

1. Determine whether the IBM Tivoli Directory Server is running
   - Windows operating systems:
     a. Click **Start** > **Programs** > **Administrative Tools** > **Services**.
     b. Locate the directory server entry, such as the supported IBM Tivoli Directory Server Instance - ldapdb2.
     c. Ensure that the directory server service is started.

        If the service was not started, select it, and then select **Action** > **Start** from the main menu of the Services window.
   - UNIX or Linux operating systems:

     Ensure that the ibmslapd process is running. Enter this command:

     ```
     ps -ef | grep ibmslapd
     ```

     If the IBM Tivoli Directory Server is running, a process ID (PID) number is returned. If a PID number is not returned, the server must be restarted.

     a. Stop the server:

        ```
        ibmslapd -I instancename -k
        ```

     b. Start the server:

        ```
        ibmslapd -I instancename
        ```
2. If the IBM Tivoli Directory Server is running, you must ensure that the IBM Tivoli Directory Server is not in configuration mode only. Enter this command:

   ```
   ldapsearch -s base -b " " objectclass=* ibm-slapdisconfigurationmode
   ```

   If the IBM Tivoli Directory Server is not in configuration mode, the value of the ibm-slapdisconfigurationmode parameter is `FALSE`. The **`ldapsearch`** command opens a connection to an LDAP server, binds, and starts a search. The -s parameter specifies the scope of the search to be base, one, or sub, which searches the base object, one level, or subtree. The -b parameter uses *searchbase* as the starting point for the search, instead of the default.

What to do next

Perform additional verification tasks.

Checking the Security Identity Manager bus and messaging engine

Before starting the Security Identity Manager Server, use the WebSphere administrative console to check the status of the bus and messaging engine.

Before you begin

Ensure that the WebSphere Application Server is running and that the WebSphere administrative console is started.

Procedure

1. Log on to the WebSphere administrative console.
2. **Service Integration** > **Buses**.
3. Click **itim_bus**, if it exists.

4. In the Topology section, click **Messaging engines**.
5. Check the engine name and its status.
   - For a single-server installation, you see an engine named *nodename.servername*-itim_bus.
   - For a cluster installation, you see *n*+1 messaging engines, where *n* is the number of Security Identity Manager cluster members. An additional messaging engine is used for the Security Identity Manager messaging cluster. Start all of these messaging engines.

   If a message engine is not started, click the messaging engine name and click **Start**.

What to do next

If you cannot start the messaging engine, see Chapter 10, "Troubleshooting," on page 167.

Perform other verification tasks.

Verification of the IBM Security Identity Manager Server

After verifying that all installed components are running, verify that the Security Identity Manager Server is running correctly.

You install Security Identity Manager in either of these environments:

- Single-server
- Clustered

Select the appropriate method to verify that the Security Identity Manager Server is running correctly.

Verifying that the IBM Security Identity Manager Server is operational in a single-server environment

Before continuing with any post-installation or configuration tasks, you must verify that you can log on to IBM Security Identity Manager through the WebSphere administrative console.

Before you begin

Ensure that you completed all the installation tasks for IBM Security Identity Manager and that all the required components are running.

Ensure that the WebSphere Application Server is running and that the administrative console is started.

Procedure

1. Log on to WebSphere administrative console.
2. On the administrative console, click **Applications** > **Enterprise Application** and verify that the IBM Security Identity Manager Server is running. For additional steps to verify that the IBM Security Identity Manager Server and other processes are running, see Chapter 7, "Verification of the installation," on page 113.
3. Log on to the IBM Security Identity Manager Server through the WebSphere embedded HTTP transport. On a browser, enter this web address:

`http://hostname:port/itim/console`

The value of *hostname* is the host name of the WebSphere Application Server. The value of *port* is the default port number of the WebSphere virtual host. The default port number is 9080. If you have multiple installations of the WebSphere Application Server on the same system, this port number might have a different value, such as 9081. If an HTTP server is used as the front-end proxy, the port number can be removed. The browser displays the IBM Security Identity Manager logon window.

4. Enter the administrator user ID (`itim manager`) and password (`secret`).

   Note: It is a good practice to create a backup administrator user ID. This ID must have the same access rights as the `itim manager` user ID.

5. Change your password. After the first successful logon, the logon window immediately prompts you to change the administrator password. Ensure that your password change is successful. After you change the password, you are ready to create your organization object and a user that is termed an ITIM User.
6. After a successful logon through the embedded HTTP transport, log on to the IBM Security Identity Manager Server through the IBM HTTP Server. Do this logon only if the IBM HTTP Server and the WebSphere Web Server plug-in are installed and configured. On a browser, enter this web address:

   `http://hostname:port/itim/console`

   The value of *hostname* is the host name of the IBM HTTP Server. The value of *port* is the port number of the WebSphere virtual host. The default port number is 9080. If an HTTP server is used as the front-end proxy, the port number can be removed.

What to do next

If you cannot start and log on to IBM Security Identity Manager, see Chapter 10, "Troubleshooting," on page 167.

Perform optional post-installation or configuration tasks. See Chapter 8, "Configuration of the Security Identity Manager Server," on page 119.

Verifying that the Security Identity Manager Server is operational in a clustered environment

Before continuing with any post-installation or configuration tasks, you must verify that you can log on to Security Identity Manager through the WebSphere administrative console.

Before you begin

Ensure that you completed all the installation tasks for Security Identity Manager. Ensure that all the required components are running.

Ensure that the WebSphere Application Server is running and that the WebSphere administrative console is started.

Procedure

1. Log on to the WebSphere administrative console.
2. Start both the Security Identity Manager application and the Security Identity Manager messaging cluster.
   a. Click **Servers** > **Clusters**.

b. Select the Security Identity Manager clusters.
c. Click **Start**. The Security Identity Manager application starts when the clusters start.

3. Log on to Security Identity Manager Server by using the WebSphere embedded HTTP transport. At a browser window, enter this command:

   `http://hostname:port/itim/console/`

   The value of *hostname* is the fully qualified name or IP address of the computer that hosts the WebSphere Application Server cluster member and the Security Identity Manager Server application. The value of port is the port number of the WebSphere virtual host. The default port number is 9080. If you have multiple instances of the WebSphere Application Server on the same computer, the port number might be a different value, such as 9081. If an HTTP server is used as the front-end proxy, the port number can be removed. For more information, see "Determining the port number of the default host" on page 178. The browser displays the Security Identity Manager logon window.

4. Enter the Security Identity Manager Server administrator user ID (`itim manager`) and password. Immediately after installation, the value of the password is `secret`.

   Note: It is advisable to create a backup administrator user ID. This ID must have the same access rights as the `itim manager` user ID.

5. Change your password. After a first, successful logon, the logon window immediately prompts you to change the administrator password. Ensure that your password change is successful. After you change the password, you are ready to create your organization object and a user that is termed an ITIM User.

What to do next

If you cannot start and log on to Security Identity Manager, see Chapter 10, "Troubleshooting," on page 167.

Perform optional post-installation or configuration tasks. See Chapter 8, "Configuration of the Security Identity Manager Server," on page 119.

Chapter 8. Configuration of the Security Identity Manager Server

After verifying the installation, you can complete various optional post-installation tasks, correct configuration errors, or change configuration settings.

During the Security Identity Manager installation process, various configuration tools such as `DBConfig` and `ldapConfig` run automatically. If a problem occurred during the installation, or if you chose not to run the configuration tools during the installation, you can run the processes manually. You can also use these manual processes to modify the configuration.

Configuration of the Security Identity Manager database

The Security Identity Manager installation program automatically uses the `DBConfig` database configuration tool to set up the database to work with Security Identity Manager. This configuration occurs either during a single-server installation or during a cluster installation on the deployment manager.

For more information about initial installation and configuration for a database, see "Database installation and configuration" on page 15.

Manually starting the `DBConfig` database configuration tool

The **`DBConfig`** command creates the database table definitions that IBM Security Identity Manager requires. Run this command only if the command failed to configure the database during installation. If the database tables were previously set, running the **`DBConfig`** command first drops all the existing database tables. If database table drop is canceled, the database configuration can fail and you must manually run the **`DBConfig`** command.

Before you begin

If you run this command after installation, ensure that the messaging engines under the service integration bus (`itim_bus`) are stopped from the WebSphere Application Server administrative console before running **`DBConfig`**. To stop the service integration bus, log on to the WebSphere administrative console, and complete these steps:

1. Click **Service Integration** > **Buses**.
2. Click **itim_bus**, if it exists.
3. In the Topology section, click **Messaging engines**.

   For a single-server installation, you see an engine named *nodename.servername*-itim_bus.

   For a cluster installation, you see *n*+1 messaging engines, where *n* is the number of IBM Security Identity Manager cluster members. An additional messaging engine is used for the IBM Security Identity Manager messaging cluster.
4. Select all messaging engines and click **Stop**.

About this task

Running the database configuration tool writes data to the *ISIM_HOME*\install_logs\dbConfig.stdout log file. If you want to save the original file, back up the file before running the command. The database configuration requires several minutes to complete.

Note: You must run the **runConfig** command after running **DBConfig** to ensure that database changes are updated.

To manually start the database configuration tool **DBConfig**:

Procedure

1. Back up the *ISIM_HOME*\install_logs\dbConfig.stdout.
2. Stop the WebShpere Application Server. See "Stop of WebSphere Application Server on the new production environment" on page 279.
3. Run one of these commands:
   - Windows operating systems:
     ISIM_HOME\bin\DBConfig.exe
   - UNIX or Linux operating systems:
     ISIM_HOME/bin/DBConfig

   A database configuration window opens to configure the database property file and to set up tables in the IBM Security Identity Manager database. The fields in the window might vary, depending on which database you use.
4. Complete the Database Information fields. The data is required to configure and connect to the database.
   - Host Name

     Specify the name of the database host.
   - Port Number

     Specify the port number of the database instance.
   - Database Name

     For DB2or Microsoft SQL databases:
     Specify the database name.

     For Oracle database:
     a. Click **SID** or **Service Name**.
     b. Specify the Oracle system identifier (SID) or service name, depending on your selection.
   - Admin ID

     Specify the administrator ID for the database host. Ensure that the administrator ID has the rights to create table space and stop and start the database.
   - Admin Password

     Specify the password for the administrator ID.
5. Click **Test** to ensure that the connection to the database is active. When the database connection test is successful, the User Password field becomes active and the **Test** button changes to **Continue**. The user ID field shows the default value itimuser, although you can change this user ID. For DB2 database, ensure that the user ID itimuser exists before you proceed to the next step.

6. Enter the correct password for the existing database user ID that is named `itimuser`, and then click **Continue**. The database configuration requires several minutes to complete.
7. If the initial DBConfig was canceled or failed with errors during the installation, you must run one of these commands to update changes:

   Note: If IBM Security Identity Manager was originally installed with Privileged Identity Manager enabled, rerunning the **DBConfig** tool wipes out Privileged Identity Manager-specific data from database. You must rerun **SAConfig** tool to add back the Privileged Identity Manager-specific data.

   - Windows operating systems:

     ISIM_HOME\bin\runConfig.exe install
   - UNIX or Linux operating systems:

     ISIM_HOME/bin/runConfig install
8. If your deployment includes the shared access module, you must reconfigure the shared access module now.

   See the IBM Security Privileged Identity Manager product documentation at http://www.ibm.com/support/knowledgecenter/SSRQBP/welcome.
9. Start the WebSphere Application Server See "Starting WebSphere Application Server" on page 286.

What to do next

Perform additional manual configuration tasks.

Configuration of the directory server

The Security Identity Manager installation program automatically uses the `ldapConfig` database configuration tool to set up the directory server to work with Security Identity Manager. This configuration occurs during a single-server installation, or during a cluster installation on the deployment manager.

For more information about initial installation and configuration for a directory server, see "Installation and configuration of a directory server" on page 36.

Manually running the `ldapConfig` configuration tool

To avoid the loss of existing directory server data, you must *not* manually run this tool unless a directory server configuration problem occurs during installation.

Before you begin

Running the directory server configuration tool writes data to the *ISIM_HOME*\install_logs\ldapConfig.stdout log file. If you want to save the original file, back up the file before running the command.

About this task

Running the **ldapConfig** command restores the default values that Security Identity Manager uses. If you changed the value of any of these Security Identity Manager attributes, such as the password of the `itim manager` user ID, the value is overwritten. Do not run the **ldapConfig** command a second time, unless the LDAP configuration fails during the Security Identity Manager Server installation process.

The directory server configuration requires several minutes to complete.

Procedure

1. Back up the *ISIM_HOME*\install_logs\ldapConfig.stdout.
2. Run one of these commands:
   - Windows operating systems -
     ISIM_HOME\bin\ldapConfig.exe
   - UNIX or Linux operating systems -
     ISIM_HOME/bin/ldapConfig
3. Enter the values for the LDAP Server Information fields (Principal DN, Password, Host Name, Port) to set up the connection to the directory server. For example, the value of the **Host Name** field is the fully qualified host name of the computer on which the directory server is running.
4. Click **Test** to ensure that the connection to the directory server can be established. When the test for a connection to the directory server is successful, the fields in the Security Identity Manager Directory Information section become active.
5. Enter the values for the Security Identity Manager Directory Information fields. You can configure these fields:

   Number of hash buckets
   Specify the number of hash buckets.

   Specify the name of your organization
   Specify the name of your organization. For example, My Organization.

   Default Org Short Name
   Specify the short name of your organization. For example, myorg.

   Identity Manager DN Location
   Specify the Security Identity Manager suffix. For example, dc=com.
6. When you are finished, click **Continue**.
7. If your deployment includes the shared access module, you must reconfigure the shared access module now.

   See the IBM Security Privileged Identity Manager product documentation.

What to do next

Perform additional manual configuration tasks.

Mapping the IBM Security Identity Manager application

If an HTTP server is used, use the administrative console to map the IBM Security Identity Manager application to the IBM HTTP web server.

Before you begin

Ensure that WebSphere Application Server is installed and that the administrative console is running. You must have administrative privileges.

Procedure

1. Log on to the administrative console on the WebSphere Application Server Network Deployment Manager for the IBM Security Identity Manager cluster. Use WebSphere Application Server administrator credentials to log in.
2. Click **Applications** > **Application Types** > **WebSphere enterprise applications** in the task menu.

3. Click **ITIM** in the Enterprise Applications list.
4. Click **Manage Modules**.
5. Select the ITIM Application Cluster name (not the JMS cluster name) and select the check boxes for these modules:
   - PasswordSynch
   - ITIM_Console
   - EnRole
   - ITIM_Self_Service
   - ITIM_Self_Service_Help
   - ITIM_Console_Help
   - ITIM_Message_Help
   - EHS3.01
   - PasswordReset
   - ITIM Web Services
   - Credential Vault
   - isim_isc_subforms
6. Click **Apply** (next to the Clusters and servers field).
7. Click **OK**.
8. Click **Save configuration** in the message box.

Configuration of commonly used system properties

You configure the Security Identity Manager Server by managing system properties. For example, a system property determines how the server responds to the correct completion of a challenge question. System properties can be modified at any time.

You might need to restart the Security Identity Manager Server when changes are made to certain system properties such as the server startup modules. These properties are not recognized unless you restart the server. Restart the Security Identity Manager Server after modifying any property with the system configuration tool. Changes to other system properties can be recognized within 30 seconds. Logging properties can be changed without restarting the server and changes take effect within 5 minutes.

You use the following methods to modify the system properties.

Manually running the `runConfig` system configuration tool

The Security Identity Manager installation program automatically runs the `runConfig` system configuration tool. However, you can also use the `runConfig` utility to modify the properties that you set during the installation. You can also correct system configuration errors that occurred during installation.

Before you begin

Running the system configuration tool writes log data to the *ISIM_HOME*\`install_logs\runConfig.stdout` log file. If you want to save the original file, back up the file before running the command.

About this task

In addition to editing commonly used system properties for the IBM Security Identity Manager Server, you can also configure WebSphere Application Server settings for the IBM Security Identity Manager application.

You can use the system configuration tool for both a single-server and cluster configuration, which includes the deployment manager and the cluster members.

To update commonly used IBM Security Identity Manager properties:

Procedure

1. Run one of the following commands
   - Windows operating systems:
     ISIM_HOME\bin\runConfig.exe
   - UNIX or Linux operating systems:
     ISIM_HOME/bin/runConfig

   Note: The `runConfig` utility only updates the properties you entered in the runConfig window. It can be used with an **`install`** parameter when there is a problem reported for `runConfig` during the IBM Security Identity Manager installation. `runConfig` **`install`** starts a full system reconfiguration.
   - Windows operating systems:
     ISIM_HOME\bin\runConfig.exe install
   - UNIX or Linux operating systems:
     ISIM_HOME/bin/runConfig install

   If the **`install`** option is used, the system configuration requires several minutes to complete.
2. Click the **Mail** tab.

   The **Mail** tab of the system configuration tool displays mail notification and gateway parameters:
   - In the **IBM Security Identity Manager Base URL** field, specify the login Universal Resource Locator (URL) for the IBM Security Identity Manager Server. This address is the first part of a URL that is sent to the recipient of mail messages at run time. The URL also points to the login page of the IBM Security Identity Manager administrative console.

     The value is the URL of the proxy server (for example, the IBM HTTP Server). Specify the host name (or IP address) and port in the base URL. Ensure that the value matches the published login URL to your IBM Security Identity Manager system.
     – Single-server configuration

       Base URL is the address of the web server (for example, the IBM HTTP Server) which by default uses port `80`.
     – Cluster configuration

       Base URL is the address of the web server that load-balances to all application server instances in the cluster, instead of a specific application server instance.

     For IPv6, literal addresses must be enclosed in brackets. For example,
     `jdbc:db2://[abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd]:50002/itimdb`

     where abcd is a hexadecimal number from 0000-FFFF.

- In the **Mail From** field, specify the address to the IBM Security Identity Manager system administrator email address for your site. All email is delivered from the `Mail From` parameter. You must change this address, otherwise you send spam to the email address listed.
- In the **Mail Server Name** field, specify the SMTP mail host that sends mail notification. SMTP mail servers are supported. The SMTP host is the mail gateway. For example, enter a host name such as `swiftcreek.mycity.ibm.com`.

3. Click the **General** tab. The **General** tab of the system configuration tool configures the general information about the IBM Security Identity Manager Server.

   The following field values on the **General** tab are pre-filled by the installation program:

   - **Heart Beat** (seconds)

     The **Scheduling Information** field displays information about how frequently a scheduling thread queries the scheduled message stores for events to process (Heart Beat). You might want to consider performance issues before you enable a more frequent beat. Only system administrators can modify the Heart Beat, which is measured in seconds.

   - **Recycle Bin Age Limit** (days)

     When you delete IBM Security Identity Manager objects (such as organization units, persons, or accounts), the objects are not immediately removed from the system. Instead, they are moved to a recycle bin container. Emptying the recycle bin is a separate deletion process that involves running cleanup scripts.

     The recycle bin is disabled by default but can be enabled by editing the `enRole.properties` file in the *ISIM_HOME*`\data` directory.

     For example, to avoid assigning an old user ID to a new user, the assignment process might check the recycle bin to determine whether an old user ID exists. You might set the value of the recycle bin interval to an interval that determines the length of time to retain old user IDs.

     The Recycle Bin Age Limit field specifies the number of days that an object remains in the recycle bin before it becomes available for deletion. The cleanup scripts can remove only those objects that are older than the age limit setting. For example, if the age limit setting is 62 days (the default value), only objects of more than 62 days can be deleted.

     You can use the following scripts to either manually remove or to schedule the periodic cleanup of recycle bin entries with expired age limits:

     – Windows operating systems:

       ISIM_HOME`\bin\win\ldapClean.cmd`

     – UNIX or Linux operating systems:

       ISIM_HOME`/bin/unix/ldapClean.sh`

       To schedule periodic cleanup, create a UNIX cron job such as the following example:

       ISIM_HOME`/bin/unix/schedule_garbage.cron`

4. Click the **Database** tab. The **Database** tab displays general database information and database pool information. The tab also has a **Test** button to test the connection to the database. If you update any field on this tab, click **Test** to ensure that the connection works. Changing the configuration after the system is set up can have detrimental effects.

Depending on the type of connection that is used, one of several windows is displayed when configuring database properties. The window in this example displays the **Database** tab when IBM Security Identity Manager does not use an Oracle client to connect to the Oracle database.

If this installation is on a cluster member, the information must match the database specification previously made for the deployment manager.

- In the **JDBC URL** field, specify the URL value with type 4 JDBC Driver URL format.

  For IPv6, literal addresses must be enclosed in brackets. For example,

  `jdbc:db2://[abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd]:50002/itimdb`

  where *abcd* is a hexadecimal number from `0000-FFFF`.
- In the **Database User** and the **User Password** fields, specify the database account and password that IBM Security Identity Manager uses to log on to the database. The default user ID is `itimuser`, which is created by the IBM Security Identity Manager database configuration program (DBConfig). The account must have a valid user password.
- The database pool information determines the number of JDBC connections. For more information about supported JDBC drivers, see "Database server products" on page 3.
  - In the **Initial Capacity** field, specify the initial number of JDBC connections.
  - In the **Maximum Capacity** field, specify the maximum number of JDBC connections that the IBM Security Identity Manager Server can open to the database at any one time.

5. Click the **Directory** tab. The **Directory** tab of the system configuration tool displays directory connection information and LDAP connection pool information. The tab also has a **Test** button to test the connection to the directory server. If you update any field on this tab, click **Test** to ensure that the connection works.

   The information is pre-filled for the deployment manager, but not for a WebSphere Application Server. If necessary, modify the following information for the directory server:

   - Principal DN and password that the IBM Security Identity Manager Server uses to log on to the directory server.
   - Host name or IP address for the directory server.

     For IPv6, literal addresses must be enclosed in brackets. For example,

     [*abcd*:*abcd*:*abcd*:*abcd*:*abcd*:*abcd*:*abcd*:*abcd*]

     where *abcd* is a hexadecimal number from 0000-FFFF.
   - Port number for the directory server.
   - The LDAP connection pool information defines a pool of LDAP connections accessible by the IBM Security Identity Manager Server. After a connection is established and data is stored in the LDAP directory server, changing the host name or the port number might have detrimental effects.
     - In the **Maximum Pool Size** field, specify the maximum number of connections that the LDAP Connection Pool can have at any time.
     - In the **Initial Pool Size** field, specify the initial number of connections to be created for the LDAP Connection Pool.

- In the **Increment Count** field, specify the number of connections to be added to the LDAP Connection Pool. This increment occurs every time a connection is requested after all connections are in use.

6. Click the **Logging** tab. You can use the **Logging** tab of the system configuration tool to set the level of tracing. Choose one of these values:

   MIN Writes less information to the log file. Use this setting for best performance.

   MID Writes an increased amount of information to the log file.

   MAX Writes the maximum amount of information to the log file. The increased amount of logging activity might affect performance. This setting is approximately the equivalent of VERBOSE.

7. Click the **UI** tab.

   The **UI** tab of the system configuration tool displays information to customize the IBM Security Identity Manager Server GUI.

   - In the **Customer Logo** field:
     - Specify the file name of the logo graphic. The file must be in the default directory, and you must copy the file to that location.
     - Specify an optional URL link activated by clicking the logo image. The link can be any URL. System administrators can specify these two variables to replace the IBM logo with their company logo throughout the IBM Security Identity Manager system. The default IBM logo file is the `ibm_banner.gif` file, which is in the *`WAS_PROFILE_HOME`*`\installedApps\`*`cellname`*`\ITIM.ear\itim_console.war\html\images` directory. In a cluster configuration, this default logo can be found in the node member workstation and not on the Deployment Manager workstation.
   - In the **List Page Size** field, specify how many items that require a search in the directory are displayed on lists throughout the user interface. If the total number of items exceeds the set List Page Size, the list is spread over multiple pages. For example, the value controls the size of the name list that opens when you browse the **My Organization** > **Manage People** tab in the IBM Security Identity Manager GUI.

8. Click the **Security** tab. The **Security** tab displays information to manage database, LDAP, and application server user IDs and passwords that are stored in the properties files. The tab displays the encryption settings and application server user management preferences in IBM Security Identity Manager.

   By default, passwords in the IBM Security Identity Manager property files are encrypted.

   - In the **Encryption** box, check the box to encrypt the passwords for database and directory server connections and password of system user for system authentication. The encryption flags are set to true. Clear the box to decrypt the passwords and set the flags to false. The flags are represented by the following properties in the `enRole.properties` file:

     ```
     enrole.password.database.encrypted
     enrole.password.ldap.encrypted
     enrole.password.appServer.encrypted
     ```

   - In the **WebSphere Administrator** and **WebSphere Administrator Password** fields, specify the WebSphere administrator and the WebSphere administrator password. The fields are pre-filled if WebSphere administrative security and application security is on, and an administrator user ID and password are entered. The fields are blank if WebSphere administrative security and application security is not on.

- In the **Identity Manager System User** and **Identity Manager System User Password** fields, specify the system user and user password. The fields initially take the values of the WebSphere Administrator and Password fields.

  If you define your own system user during installation to be different from the WebSphere Administrator, you might need to modify the **Identity Manager System User** and **Identity Manager System User Password** fields. If you change the value of the system user ID or user password on this system configuration Security window and run `runConfig` as a stand-alone command, additional manual steps are required. These steps are necessary after IBM Security Identity Manager installation to map the security role to the IBM Security Identity Manager user to start IBM Security Identity Manager. For more information, see "Mapping an administrative user to a role" on page 149.

What to do next

Perform additional manual configuration tasks.

Manual modification of system properties

Alternatively, you can manually modify system properties by editing the appropriate property file.

System and supplemental property files are on the IBM Security Identity Manager Server in the *ISIM_HOME*\data directory. These files contain all the system and supplemental properties used by the server. For more information about system properties in the `enRole.properties` file, see *System property configuration in enRole.properties* on the Security Identity Manager product documentation site.

Modification of system properties with the IBM Security Identity Manager graphical user interface

You can also modify certain system properties from within the Configuration section of the main menu navigation bar in the IBM Security Identity Manager Server graphical user interface (GUI).

From **Set Systems Security** > **Set Security Properties**, you can modify the following security properties:

- Password settings
- Security Identity Manager login account settings
- Group settings
- Default settings for provisioning policy when a new service is created

From **Set Systems Security** > **Configure Forgotten Password Settings**, you can modify the following properties:

- Enable forgotten password authentication
- Login behavior
- Challenge behavior settings

Security properties

From **Set Systems Security** > **Set Security Properties**, you can modify these security properties.

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

Password settings:

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

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

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

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

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

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

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

IBM Security Identity Manager login account settings:

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

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

Identity account password expiration period in days
This property is only for the Security Identity Manager Server account. Type an interval, in days, after which the password expires for an Security Identity Manager account. The user must change the password before this period is reached. Whenever a new password is set for the Security Identity Manager Server account, the password expiration period is affected from that time. You can disable password expiration by setting this value to zero. The default value of 0 indicates that the account password never expires.

Maximum number of incorrect login attempts
Type the number of incorrect login attempts that can occur before an Security Identity Manager account is suspended. The default value of 0 indicates that there is no limit.

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

Group settings:

You can select to modify the group properties automatically.

Click **Set Systems Security** > **Set Security Properties**, to modify the group properties.

Automatically populate IBM Security Identity Manager groups

Select this check box to automatically put the IBM Security Identity Manager accounts of newly named service owners in the default Service Owner group. The automatic action is enabled or disabled immediately. You do not need to restart Security Identity Manager. For example, membership in a group can take place when you create or modify a service, specifying a service owner.

Additionally, the Security Identity Manager accounts of newly named managers are automatically put in the default Manager group. For example, this action can occur when you create or modify a user who is a subordinate, specifying the manager of the user.

Automatic group membership is not supported when the service owner is a role.

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

Default settings for provisioning policy when a new service is created:

Select the default setting for provisioning policies when new services are created. You might not want to create a default policy when a new service is created if the amount of time to evaluate the default policy for all users is significant.

Click **Set Systems Security** > **Set Security Properties** to modify the default settings for provisioning policies when new services are created. If you do not want to create a default policy, select **No, I will manually configure a policy later** and then click **OK**.

Then, when you create a service, the default setting for provisioning policies is set to **No, I will manually configure a policy later**.

Forgotten password settings

From **Set Systems Security** > **Configure Forgotten Password Settings**, you can modify the properties for forgotten password.

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

Forgotten password authentication:

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

Select this check box to activate the forgotten password authentication. If the authentication is activated, the login page opens a **Forgot your password?** prompt for users who forget their passwords. A user who provides the correct responses to the questions receives a new, automatically generated password. If the check box is cleared, no prompt occurs on the login page. Users must contact the help desk assistants or system administrators for help in resetting their passwords.

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

Login behavior:

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

When the user successfully answers the questions
Select the login behavior:

Change password and log in to system
Logs the user in to the system and requires a password change.

Reset and email password
Resets the password, and sends the new password to the email address of the user.

Message suspending account for failed answers
Type the message the user receives after failing to enter the correct answers.

Send message to email address
Type the email address to receive messages.

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

Challenge behavior:

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

Select whether the user or the administrator defines challenge questions.

Users define their own questions

Select for users to provide their questions.

Number of questions user sets up
Type the number of questions that the user must provide.

Number of correct answers user must enter
Type the number of correct answers that the user must provide to gain access to the system.

Administrator provides predefined questions

Select the option to define the set of questions that the users must answer and the language in which the question is used. When the option is selected, the Specify Forgotten Password Question section opens.

Specify Forgotten Password Question
Click to expand this section to specify the question that you want users to answer.

New challenge question
Type the question that you want users to answer and click **Add**.

Locale Select the language in which the question is used and click **Add**.

Challenge questions table
The **Challenge questions** table contains the list of questions that you added and that you can choose to have users answer. To sort

the table by a specific column, click the arrow in the column heading. The table contains these columns:

Select Select this check box to choose an existing question.

Locale Displays the language used in the question.

Question
Displays the text of a question.

Click **Remove** to remove a selected question.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

User has a choice of predefined questions?

No, answer all questions
Displays all predefined questions, which the user must answer correctly.

Yes, user selects which questions to answer
Displays the number of questions that the user selects and must answer correctly after forgetting a password. Type the number of questions that the user selects.

No, answer a subset of questions that the system provides
Displays a random subset of predefined questions, which the user must answer correctly after forgetting a password.

Number of questions user sets up
Type the number of questions that the user configures.

Number of correct answers user must enter
Type the number of questions that the user must correctly answer. This field is available, if the user must answer a subset of questions that the system provides.

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

Security configuration

You must configure security for Security Identity Manager and the middleware components.

For more information about security, see *Security* on the IBM Security Identity Manager product documentation site.

Security configuration of the database server

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

Configuration of SSL for the IBM DB2 database server

The SSL communication can be used between the IBM DB2 database server and Security Identity Manager server to secure the database communication. This task can be done only after Security Identity Manager is installed. You cannot configure the database through the SSL connection while you are installing Security Identity Manager.

You must configure the IBM DB2 database server and certificates to use SSL. The following sections provide the procedures to configure the SSL communication between Security Identity Manager and IBM DB2 database server.

Enabling of SSL on the IBM DB2 database server:

The IBM DB2 database server is configured to listen on a secure port with a defined certificate. The certificate authority must be in the signer certificate database on the SSL client.

You can use GSKit to create the certificates and key database file or extract the server certificate. You must copy the certificate on the system where the IBM Security Identity Manager server runs. You must also know the location of the server certificate to set up a trusted certificate for IBM Security Identity Manager in a later task.

For more information about activating SSL on database for IBM DB2 database server, see the documentation available in the IBM DB2 Knowledge Center.

Configuration of the SSL client to trust the database server certificate:

The IBM Security Identity Manager Server does not operate as an embedded part of WebSphere Application Server. It operates as a Java application and uses Java Secure Socket Extension (JSSE) to implement SSL support.

SSL certificates and CA certificates are retrieved in a standard Java truststore or keystore format. The truststore and keystore use the same file formats that the Java virtual machine and WebSphere Application Server use for other certificate configuration. You can use standard Java tools to maintain the truststore and keystore, for example, the IBM Key Management utility tool or the Java keytool command-line utility.

The self-signed certificate or CA certificate for the database server needs to be imported into the truststore to configure the SSL connection to the database server. This truststore is used by the IBM JSSE, which is part of WebSphere Application Server. Additionally, you must configure IBM Security Identity Manager to use SSL to communicate with the database Server.

The following sections describe the various tasks to import a signer certificate into truststore and configure IBM Security Identity Manager to establish the SSL connection with the DB2 database.

Importing the signer certificate to the WebSphere Application Server certificate store:

The DB2 signer certificate must be available in the application server so that the IBM Security Identity Manager Server can establish and validate the SSL connection.

Before you begin

Ensure that WebSphere Application Server is running and that you start the administrative console. You also need WebSphere Application Server administrative user ID and password.

About this task

Import the signer certificate for the DB2 database into the WebSphere Application Server certificate store file.

The following procedure is one of many alternative ways to make the signer certificate available to the application server.

Procedure

1. Log on to the WebSphere Application Server administrative console
2. Select **Security** > **SSL certificate and key management**.
3. Click **Key stores and certificates** under **Related items**.
4. For a single server environment, select **NodeDefaultTrustStore**. Otherwise, select **CellDefaultTrustStore** for a clustered environment.
5. Select **Signer certificates** under **Additional Properties**.
6. Select **Retrieve from port** to contact the port and request the signer.
7. Enter the host name of the DB2 server, the SSL port number, and an alias for the certificate to be imported.
8. Select **Retrieve signer information**. The signer information is displayed.
9. Click **OK** to import the certificate.
10. Click **Save**.

What to do next

Restart WebSphere Application Server to use this certificate

Installing the signer certificate in the JSSE truststore:

Use this procedure to install the signer certificate and add it to the certificate store. The certificate store is used to run the configuration and stand-alone utilities in IBM Security Identity Manager.

Before you begin

For this task, the default truststore that is present in the JRE of WebSphere Application Server is used. The iKeyman utility is used to configure the certificates. Alternately, you can create your own certificate store location and use it to specify the JSSE System Properties in the configuration files.

About this task

Install the signer certificate in the JSSE truststore. For a clustered environment, the certificate store is required for the IBM Security Identity Manager instance that is deployed on the deployment manager and each member of the cluster.

Procedure

1. Start the iKeyman utility. The utility (`ikeyman.bat` or `ikeyman.sh`) is in the *`WAS_HOME`*`/bin` directory.
2. From the **Key Database File** menu, select **Open**.
3. For the key database type, select **JKS**.
4. In the **File Name** field, type `cacerts`.
5. In the **Location** field, type `WAS_HOME/java/jre/lib/security/`.

6. In the password prompt window, enter the password and then confirm it. The default password is `changeit`.
7. Click **OK**.
8. Add the certificate that you created for the database server into this certificate store by following these steps.
   a. In the main window, in the Key database content area, select **Signer Certificates** from the list.
   b. Click **Add**.
   c. In the **Certificate file name** field, browse and locate the server certificate file that was created for the database server, which is in Base64 encoded ASCII data.

      Verify that the appropriate directory is displayed in the **Location** field.
   d. Click **OK**.
   e. In the prompt, type a label for this certificate. Type `DATABASECA`.
   f. Click **OK**.

   Note: If you are not able to locate the server certificate file, extract it from the server certificate store. For the IBM DB2 database server, use the iKeyman utility to extract the certificate.

   The certificate is added in the certificate store. You can now close the iKeyman utility.

What to do next

Use the certificate store to specify the JSSE system properties in the configuration files.

Configuring the IBM Security Identity Manager property file:

You must configure IBM Security Identity Manager to use an SSL connection.

Before you begin

Ensure that the IBM Security Identity Manager installation process is completed.

About this task

The `ISIM_HOME/data/enRoleDatabase.properties` file is updated. For the clustered environment, the configuration steps must be done on the IBM Security Identity Manager instances on the deployment manager and each member of the cluster.

Procedure

1. Back up the `ISIM_HOME/data/enRoleDatabase.properties` file.
2. Use any text editor to edit the `ISIM_HOME/data/enRoleDatabase.properties` file and make the following changes:
   a. Change the port number in the database url for the `database.jdbc.driverUrl` property file to the SSL port number configured on the database server. Set `sslConnection=true` property in the database url as shown in the following example. Ensure that the `ssl` property is the first property that is set to the database url.

      ```
      database.jdbc.driverUrl=jdbc:db2://localhost:50000/
      ISIMDB:sslConnection=true;
      ```

Note: The property and its value are one line.

b. Set the value of the `database.db.security.protocol` property file to `ssl`. This value is used to connect to the database securely while the DBConfig utility is running.

```
database.db.security.protocol=ssl
```

3. Save the updates.

What to do next

Configure the `ISIM_HOME/bin/DBUpgrade.lax` file with the steps that are given in "Running DBUpgrade with SSL" on page 140. This configuration is required to run the DBUpgrade utility during the IBM Security Identity Manager fix pack installation.

Configuring the IBM Security Identity Manager data source:

After you configure WebSphere Application Server and IBM Security Identity Manager to use SSL connection, you must configure the IBM Security Identity Manager data source.

Before you begin

You must make the signer certificate for the database server available to WebSphere Application Server. You must also finish configuring IBM Security Identity Manager to use SSL communication with database server.

Ensure that WebSphere Application Server is running and that you start the WebSphere Application Server administrative console. You also need the WebSphere Application Server administrative user ID and password.

About this task

Configure the IBM Security Identity Manager data source in WebSphere Application Server.

Procedure

1. Log on to the WebSphere Application Server administrative console.
2. Select **Resources** > **JDBC** > **Data sources** in the WebSphere Application Server administrative console.
3. Follow these steps for all the IBM Security Identity Manager application-related data source such as **ITIM Data Source**, **ITIM Bus DataSource**, and **ITIM Bus Shared DataSource** in a clustered environment.
   a. Click the data source to be configured.
   b. Click **Custom properties** under the **Additional Properties** heading.
   c. Click **New** to create the `sslConnection` property with the following values:
      - **Scope**: Use default
      - **Name**: sslConnection
      - **Value**: true
      - **Type**: java.lang.Boolean
   d. Click **Apply** to save the changes.
   e. Change the port number in the **Port number** field to the SSL port number that is configured on the database server.

f. Click **Apply** to save the changes.
g. Verify that other properties, database server, database name, database user name, and password are properly set.
h. Verify whether the connection to the database is working by clicking **Test connection**.

What to do next

Restart WebSphere Application Server.

The IBM Security Identity Manager configuration tools and stand-alone utilities with SSL:

IBM Security Identity Manager provides utilities to configure database schema, LDAP, and commonly used system properties. The following sections describe how to run the IBM Security Identity Manager configuration tools and utilities with SSL connection to the database server

Running DBConfig with SSL:

Follow these steps to manually run the DBConfig utility.

Before you begin

Ensure that the IBM Security Identity Manager installation process is completed. You must also ensure that all the steps that are required to configure IBM Security Identity Manager for SSL to communicate with the IBM DB2 database server are done.

About this task

You must edit the `ISIM_HOME/bin/DBConfig.lax` file to specify the JSSE system properties. For a clustered environment, configure it on an IBM Security Identity Manager instance that is deployed on the deployment manager only.

Procedure

1. Verify that `enRoleDatabase.properties` has `database.db.security.protocol` set to **ssl**.
2. Back up the `ISIM_HOME/bin/DBConfig.lax` file.
3. Use any text editor to edit the `ISIM_HOME/bin/DBConfig.lax` file.

   Add this property, which is one line:

   ```
   lax.nl.java.option.additional=-Djavax.net.ssl.trustStoreType=jks
   -Djavax.net.ssl.trustStore=/opt/IBM/WebSphere/AppServer/java/jre/lib/security/
   cacerts
   -Djavax.net.ssl.trustStorePassword=changeit
   -Djava.ext.dirs=/opt/IBM/WebSphere/AppServer/java/jre/lib/ext:/opt/IBM/
   WebSphere/AppServer/plugins:/
   opt/IBM/WebSphere/AppServer/lib:/opt/IBM/WebSphere/AppServer/lib/ext
   ```

   On the Microsoft Windows operating system:

   ```
   lax.nl.java.option.additional=-Djavax.net.ssl.trustStoreType=jks
   -Djavax.net.ssl.trustStore=C:\Progra~1\IBM\WebSphere\AppServer\java\jre\lib\
   security\cacerts
   -Djavax.net.ssl.trustStorePassword=changeit
   ```

```
-Djava.ext.dirs=C:\Progra~1\IBM\WebSphere\AppServer\java\jre\lib\ext;C:\
Progra~1\IBM\WebSphere\AppServer\plugins;C:\Progra~1\IBM\WebSphere\AppServer\
lib;C:\Progra~1\IBM\WebSphere\AppServer\lib\ext
```

4. Save the updates.

   Note:
   - On the UNIX operating systems, the delimiter for the list of directories in `java.ext.dirs` must be a colon.
   - On the Microsoft Windows operating systems:
     - The delimiter for these directories must be a semi-colon.
     - Use 8.3 notation for the directory names as there can be no spaces in the list.

   Depending on the version of WebSphere Application Server and the JSSE configuration, you might have to specify more JAR files in the class path.

What to do next

Run the DBConfig utility.

Running SAConfig with SSL:

Follow these steps to run the SAConfig utility.

Before you begin

Ensure that the IBM Security Identity Manager installation process is completed. Follow all the steps to configure IBM Security Identity Manager to use SSL to communicate with the IBM DB2 database server.

Note: You must perform the SSL configuration before you install Fix Pack 2 for IBM Security Identity Manager version 6.0. It ensures that the SSL configuration you performed to the SAConfig.lax is copied to the new SAUpgrade utility lax file in the fix pack and also reapplied during the fix pack installation.

About this task

You must edit the `ISIM_HOME/bin/SAConfig.lax` file to specify the JSSE system properties. For a clustered environment, this configuration must be done on an IBM Security Identity Manager instance that is deployed on the deployment manager and each member of the cluster.

Procedure

1. Before you run the **SAConfig** utility, verify that the properties `database.jdbc.driverUrl` and `database.db.security.protocol` in `ISIM_HOME/data/enRoleDatabase.properties` file are set to use SSL communication with database server.
2. Back up the `ISIM_HOME/bin/SAConfig.lax` file.
3. Edit the `ISIM_HOME/bin/SAConfig.lax` file in any text editor.

   Add this property, which is one line:

```
lax.nl.java.option.additional=-Djavax.net.ssl.trustStoreType=jks
-Djavax.net.ssl.trustStore=/opt/IBM/WebSphere/AppServer/java/jre/lib/security/
cacerts
-Djavax.net.ssl.trustStorePassword=changeit
```

```
-Djava.ext.dirs=/opt/IBM/WebSphere/AppServer/java/jre/lib/ext:/opt/IBM/
WebSphere/AppServer/plugins:/
opt/IBM/WebSphere/AppServer/lib:/opt/IBM/WebSphere/AppServer/lib/ext
```

On the Microsoft Windows operating system:

```
lax.nl.java.option.additional=-Djavax.net.ssl.trustStoreType=jks
-Djavax.net.ssl.trustStore=C:\Progra~1\IBM\WebSphere\AppServer\java\jre\lib\
security\cacerts
-Djavax.net.ssl.trustStorePassword=changeit
-Djava.ext.dirs=C:\Progra~1\IBM\WebSphere\AppServer\java\jre\lib\ext;C:\
Progra~1\IBM\WebSphere\Ap
pServer\plugins;C:\Progra~1\IBM\WebSphere\AppServer\lib;C:\Progra~1\IBM\
WebSphere\AppServer\lib\ext
```

4. Save the updates.

   Note:

   - On the UNIX operating systems, the delimiter for the list of directories must be a colon.
   - On the Microsoft Windows operating systems:
     - The delimiter for these directories must be a semi-colon.
     - Use 8.3 notation for the directory names as there can be no spaces in the list.

   Depending on the version of WebSphere Application Server and the JSSE configuration, you might have to specify more JAR files in the class path.

What to do next

Run the **SAConfig** utility.

Running runConfig with SSL:

Follow these steps to manually run the **runConfig** utility.

Before you begin

Ensure that all the steps required to configure IBM Security Identity Manager to use SSL to communicate with the IBM DB2 database server are done.

About this task

You must edit the `ISIM_HOME/bin/runConfig.lax` file to specify the JSSE system properties. For a clustered environment, this configuration must be done on an IBM Security Identity Manager instance that is deployed on the deployment manager and each member of the cluster.

Procedure

1. Before you run the **runConfig** utility, verify that `database.jdbc.driverUrl` and `database.db.security.protocol` in the `ISIM_HOME/data/enRoleDatabase.properties` file are set to use SSL communication with the database server.
2. Back up the `ISIM_HOME/bin/runConfig.lax` file.
3. Edit the `ISIM_HOME/bin/runConfig.lax` file in any text editor.

   Add this property, which is one line:

```
-Djavax.net.ssl.trustStore=/opt/IBM/WebSphere/AppServer/java/jre/lib/security/
cacerts
-Djavax.net.ssl.trustStorePassword=changeit
-Djava.ext.dirs=/opt/IBM/WebSphere/AppServer/java/jre/lib/ext:/opt/IBM/
WebSphere/AppServer/plugins:/opt/IBM/WebSphere/AppServer/lib:/opt/IBM/
WebSphere/AppServer/lib/ext
```

On the Microsoft Windows operating system:

```
lax.nl.java.option.additional=-Djavax.net.ssl.trustStoreType=jks
-Djavax.net.ssl.trustStore=C:\Progra~1\IBM\WebSphere\AppServer\java\jre\lib\
security\cacerts
-Djavax.net.ssl.trustStorePassword=changeit
-Djava.ext.dirs=C:\Progra~1\IBM\WebSphere\AppServer\java\jre\lib\ext;C:\
Progra~1\IBM\WebSphere\AppServer\plugins;C:\Progra~1\IBM\WebSphere\
AppServer\lib;C:\Progra~1\IBM\WebSphere\AppServer\lib
\ext
```

4. Save the updates.

   Note:

   - On the UNIX operating systems, the delimiter for the list of directories in `java.ext.dirs` must be a colon.
   - On the Microsoft Windows operating systems:
     - The delimiter for these directories must be a semi-colon.
     - Use 8.3 notation for the directory names as there can be no spaces in the list.

   Depending on the version of WebSphere Application Server and the JSSE configuration, you might have to specify more JAR files in the class path.

What to do next

Run the **runConfig** utility.

Running DBUpgrade with SSL:

Follow these steps to run the **DBUpgrade** utility manually, or during a fix pack installation.

Before you begin

Ensure that all the steps that are required to configure IBM Security Identity Manager to use SSL to communicate with the IBM DB2 database server are done.

About this task

You must edit the `ISIM_HOME/bin/DBUpgrade.lax` file to specify the JSSE system properties. For a clustered environment, the configuration must be done on an IBM Security Identity Manager instance that is deployed on the deployment manager only.

Procedure

1. Before you run the **DBUpgrade** utility, verify that `database.jdbc.driverUrl` and `database.db.security.protocol` in the `ISIM_HOME/data/enRoleDatabase.properties` file are set to use SSL communication with the database server.
2. Back up the `ISIM_HOME/bin/DBUpgrade.lax` file.

3. Edit the ISIM_HOME/bin/DBUpgrade.lax file in any text editor.

   Add this property, which is one line:

   ```
   lax.nl.java.option.additional=-Djavax.net.ssl.trustStoreType=jks
   -Djavax.net.ssl.trustStore=/opt/IBM/WebSphere/AppServer/java/jre/lib/
   security/cacerts
   -Djavax.net.ssl.trustStorePassword=changeit
   -Djava.ext.dirs=/opt/IBM/WebSphere/AppServer/java/jre/lib/ext:/opt/IBM/
   WebSphere/AppServer/plugins:/opt/IBM/WebSphere/AppServer/lib:/opt/IBM/
   WebSphere/AppServer/lib/ext
   ```

   On the Microsoft Windows operating system:

   ```
   lax.nl.java.option.additional=-Djavax.net.ssl.trustStoreType=jks
   -Djavax.net.ssl.trustStore=C:\Progra~1\IBM\WebSphere\AppServer\java\jre\lib\
   security\cacerts
   -Djavax.net.ssl.trustStorePassword=changeit
   -Djava.ext.dirs=C:\Progra~1\IBM\WebSphere\AppServer\java\jre\lib\ext;C:\
   Progra~1\IBM\WebSphere\AppServer\plugins;C:\Progra~1\IBM\WebSphere\
   AppServer\lib;C:\Progra~1\IBM\WebSphere\AppServer\lib\ext
   ```

   Note:

   - On the UNIX operating systems, the delimiter for the list of directories in java.ext.dirs must be a colon.
   - On the Microsoft Windows operating systems:
     - The delimiter for these directories must be a semi-colon.
     - Use 8.3 notation for the directory names as there can be no spaces in the list.

   Depending on the version of WebSphere Application Server and the JSSE configuration, you might have to specify more JAR files in the class path.
4. Save the updates.
5. Test if the property is set correctly.
   a. Make the same updates from the previous steps to the ISIM_HOME/bin/runConfig.lax file.
   b. Click **Test** on the database screen. If the test returns a success message, the property is set correctly.
   c. Click **Cancel** and quit **runConfig**. Do not click **Ok** or **Apply**.

What to do next

Run the **DBUpgrade** utility.

Running the Security Identity Manager stand-alone utilities:

You must add a Java runtime property to utilities that access the database server with SSL.

Before you begin

Ensure that the IBM Security Identity Manager installation is completed and it is configured with the database server to use SSL.

About this task

The following utilities present in the ISIM_HOME/bin/<platform> directory can directly access the database:

- config_remote_services
- CrystalConfigWAS
- CrystalUpgradeWAS
- DBPurge
- remove_service_profiles
- startIncrementalSynchronizerCMD_WAS
- startIncrementalSynchronizerUI_WAS
- itim_report_data_sync_utility

To successfully run the utilities when SSL is configured, you must complete the following steps.

Procedure

1. Verify that the properties database.jdbc.driverUrl and database.db.security.protocol in the ISIM_HOME/data/enRoleDatabase.properties file are set to use SSL to communicate with the database server.
2. Back up the utility file before you edit it.
3. Open the utility file in a text editor. For example, DBPurge.sh or DBPurge.cmd

   Add this property as a Java runtime property. The property is one line.

   ```
   -Djavax.net.ssl.trustStoreType=type_of_truststore -Djavax.net.ssl.
   trustStore=truststore_location
   -Djavax.net.ssl.trustStorePassword=truststore_password
   -Djava.ext.dirs=WAS_HOME/java/jre/lib/ext:WAS_HOME/plugins:
   WAS_HOME/lib:WAS_HOME/lib/ext
   ```

   When DBPurge.sh is modified for SSL, it looks like this example:

   ```
   $JAVA -Djavax.net.ssl.trustStoreType=jks -Djavax.net.ssl.trustStore=/opt/
   ibm/cacerts
   -Djavax.net.ssl.trustStorePassword=changeit
   -Djava.ext.dirs=/opt/IBM/WebSphere/AppServer/java/jre/lib/ext:/opt/IBM/
   WebSphere/AppServer/plugins:/opt/IBM/WebSphere/AppServer/lib/
   ext -Xms64m -Xmx256m -classpath $CLASSPATHcom.ibm.itim.systemConfig.cleanup.
   DBPurgeMain $*
   ```
4. Save the changes to the utility file.

   Note:

   - On the UNIX operating systems, the delimiter for the list of directories in java.ext.dirs must be a colon.
   - On the Microsoft Windows operating systems:
     - The delimiter for these directories must be a semi-colon.
     - Use 8.3 notation for the directory names because there can be no spaces in the list.

   Depending on the version of WebSphere Application Server and the JSSE configuration, you might have to specify more JAR files in the class path.

What to do next

Use the utilities.

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 or Oracle Directory Server Enterprise Edition to store Security Identity Manager information, you must set the server to use SSL. Then you must configure the SSL certificates that you want to use.

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

Configuration of SSL for IBM Security Directory Server

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

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

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

Configuration of SSL for Oracle Directory Server Enterprise Edition

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

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

Configuration of the SSL client to trust the LDAP server certificate

The Security Identity Manager Server does not operate as an embedded part of WebSphere Application Server. It operates as a Java application and uses Java secure socket extension (JSSE) to implement SSL support.

SSL certificates and CA certificates are retrieved from a standard format Java truststore or keystore. The truststore and keystore use the same file formats that the Java virtual machine and WebSphere Application Server use for other certificate configuration. You can use standard Java tools to maintain the trust and keystores, including the IBM Key Management tool and the Java Keytool command-line utility.

To configure the SSL connection between the Security Identity Manager Server and LDAP Server, you must import the self-signed certificate or CA certificate created for the LDAP Server into the truststore. This truststore is used by the IBM JSSE, which is part of WebSphere Application Server. Additionally, you must first

configure Security Identity Manager to use SSL when communicating with the LDAP Server. Configure Security Identity Manager to use the `ldaps` protocol instead of the `ldap` protocol.

Installing the self-signed certificate in the JSSE truststore:

Use this procedure to install the self-signed certificate and to add it to the certificate store.

Before you begin

For this task, the default truststore that is present in the JRE of the WebSphere Application Server is used. Also, the *ikeyman* utility is used to configure the certificates

Procedure

1. Start the *ikeyman* utility. The utility (`ikeyman.bat` or `ikeyman.sh`) is in the *WAS_HOME*`\bin`.
2. From the Key Database File menu, select **Open**.
3. In the key database type, select **JKS**.
4. In the File Name field, type `cacerts`.
5. In the Location field, type `WAS_HOME\java\jre\lib\security\`.
6. In the Password Prompt window, type the password for the keystore in the Password and Confirm Password window. The default password is `changeit`.
7. Click **OK**.
8. Add the certificate you created for the LDAP server into this certificate store.
   a. In the main window, in the Key database content area, select **Signer Certificates** from the list.
   b. Click **Add**.
   c. In the Certificate file name field, browse and locate the server certificate file that was created for the LDAP server, which is in **Binary Der data**. Verify that the appropriate directory is displayed in the Location field.
   d. Click **OK**.
   e. In the prompt, type a label for this certificate. For example, type `LDAPCA`.
   f. Click **OK**.

   Note: If you are not able to locate the server certificate file as previously described, follow these steps to extract it from the server certificate store:
   - For IBM Tivoli Directory Server, use the *ikeyman* utility to extract the certificate.
   - For Oracle Directory Server, follow these steps to extract the server certificate:
     a. Find the alias of the certificate. From `ODSEE-install/bin` directory, run:
        ```
        ./dsadm list-certs <instance-home-dir-path>
        ```
     b. Show the certificate and redirect the output to a `Binary Der` file, assuming the alias of the certificate is *defaultCert*:
        ```
        ./dsadm show-cert -F der -o cert.der <instance-home-dir-path> defaultCert
        ```

   `cert.der` is the requisite server certificate file.
   The certificate is added for the LDAP Server. You can now close the *ikeyman* utility.

What to do next

Configure Security Identity Manager to use SSL when communicating with the LDAP server.

Configuring Security Identity Manager to use SSL when communicating with the LDAP server:

After importing the LDAP self-signed certificate, you must configure Security Identity Manager Server to complete the SSL connection.

Before you begin

You must finish installing the self-signed certificate for the LDAP server in the JSSE truststore.

Procedure

1. Edit the `enRoleLDAPConnection.properties` file. This file is in the *ISIM_HOME*`\data` directory.
   a. Set the port value on the `java.naming.provider.url` property to the SSL port number configured on directory server [LDAP]. For example,
      ```
      java.naming.provider.url=ldaps://localhost:636
      ```
   b. Set the value of the `java.naming.security.protocol` property to `ssl`. This setting directs the Security Identity Manager Server to use SSL to communicate to LDAP. Alternately you can change the protocol in `java.naming.provider.url` from ldap to ldaps. For example,
      ```
      java.naming.security.protocol=ssl
      ```
2. Save the changes.

What to do next

Perform other security-related tasks.

Defining the truststore and password as a custom property on the JVM:

Security Identity Manager Server does not use the WebSphere Application Server SSL Configuration Repositories settings in the WebSphere administrative console **Security | SSL** tab. Instead, you must configure the SSL settings to specify the javax properties.

Before you begin

Ensure that the WebSphere Application Server is running and that you start the WebSphere administrative console. You also need WebSphere Application Server administrative user ID and password.

Procedure

1. Select **Servers** > **Application Servers** > *server_name* > **Process Definition** > **Java Virtual Machine** > **Custom Properties** > **New**.
2. Define the name of the javax properties that you changed by using the **ikeyman** key management tool. In "Installing the self-signed certificate in the JSSE truststore" on page 144, you installed certificates into the truststore of the JVM used by WebSphere Application Server. Alternately you can create your own certificate store location, for which you must define some additional properties.

This table provides information about the javax properties you must define.

Table 15. Truststore javax properties

Property name	Description	Default value
javax.net.ssl.trustStore	File path of the truststore file. If you do not use javax.net.ssl.keyStore to specify a client certificate, you can use the truststore to install CA certificates and client certificates.	*jre_install_dir*\lib\security\cacerts Example: C:\Program Files\WebSphere\AppServer\java\jre\lib\security\cacerts
javax.net.ssl.trustStorePassword	Password that protects the truststore.	changeit
javax.net.ssl.trustStoreType	Key database type. This property is required for truststore. The value is specified when creating a self-signed certificate.	jks

What to do next

Perform additional security-related tasks.

Running ldapConfig with SSL:

If LDAP is configured to use SSL only, the **ldapConfig** utility does not work during a new Security Identity Manager installation. Skip the **ldapConfig** during the installation process

Before you begin

Ensure that the Security Identity Manager installation process is completed.

About this task

Run **ldapConfig** after accomplishing this procedure:

Procedure

1. Verify that enRoleLDAPConnections.properties has java.naming.security.protocol set to **ssl**.
2. Edit *ISIM_HOME*\bin\ldapConfig.lax file.

   Note: The CA certificate is required to verify the authenticity of the authority that issued an LDAP server certificate. Skip this step if the CA certificate is installed in the truststore of the JVM that is used by **ldapConfig**.

   Add this property, which is one line:

   ```
   lax.nl.java.option.additional=-Djavax.net.ssl.
   trustStoreType=jks
   -Djavax.net.ssl.trustStore=/opt/IBM/WebSphere/AppServer/java/
   jre/lib/security/cacerts -Djavax.net.ssl.trustStorePassword
   =changeit -Djava.ext.dirs=/opt/IBM/WebSphere/AppServer/java/
   jre/lib/ext:/opt/IBM/WebSphere/AppServer/plugins:/opt/IBM/
   WebSphere/AppServer/lib:/opt/IBM/WebSphere/AppServer/lib/ext
   ```

What to do next

Run the **ldapConfig** utility.

Perform additional security-related tasks.

Running ldapUpgrade:

If LDAP is configured to use SSL only with Security Identity Manager, follow these steps to run the ldapUpgrade utility during a fix pack installation.

Before you begin

Security Identity Manager must be installed and the fix pack downloaded.

Procedure

1. Before running the ldapUpgrade utility, verify that enRoleLDAPConnections.properties, has java.naming.security.protocol set to **ssl**.
2. Edit *ISIM_HOME*\bin\ldapUpgrade.lax file.

   Add this property, which is one line:

   ```
   lax.nl.java.option.additional=-Djavax.net.ssl.
   trustStoreType=jks
   -Djavax.net.ssl.trustStore=/opt/IBM/WebSphere/AppServer/java/
   jre/lib/security/cacerts -Djavax.net.ssl.trustStorePassword
   =changeit -Djava.ext.dirs=/opt/IBM/WebSphere/AppServer/java/
   jre/lib/ext:/opt/IBM/WebSphere/AppServer/plugins:/opt/IBM/
   WebSphere/AppServer/lib:/opt/IBM/WebSphere/AppServer/lib/ext
   ```

   For example, on the Windows operating system:

   ```
   lax.nl.java.option.additional=-Djavax.net.ssl.trustStoreType=jks
   -Djavax.net.ssl.trustStore=
   C:\Progra~1\IBM\WebSphere\AppServer\java\jre\lib\security\cacerts
   -Djavax.net.ssl.trustStorePassword=changeit
   -Djava.ext.dirs= C:\Progra~1\IBM\WebSphere\AppServer\java\jre\lib\ext;
   C:\Progra~1\IBM\WebSphere\AppServer\plugins;
   C:\Progra~1\IBM\WebSphere\AppServer\lib;
   C:\Progra~1\IBM\WebSphere\AppServer\lib\ext
   ```

   Note: On the UNIX systems, the delimiter for the list of directories in java.ext.dirs must be a colon. On the Windows systems, the delimiter for these directories must be a semi-colon. Also, on Windows systems, use 8.3 notation for the directory names as there can be no spaces in the list.
3. Test if this property is set correctly.
   a. Copy the property into the *ISIM_HOME*\bin\ldapConfig.lax file.
   b. Click **Test** on the ldapConfig screen. If the test returns a success message, the property is set correctly.

      Note: Do not click **Continue** on the ldapConfig screen. Click **Cancel** to exit.

What to do next

Run the ldapUpgrade utility.

Perform additional security-related tasks.

Running the utilities that access the LDAP server with SSL:

You must add a Java runtime property to utilities to that access the LDAP server with SSL.

Before you begin

Ensure that the Security Identity Manager installation is completed.

About this task

To successfully run the following utilities present in the *ISIM_HOME*\bin\platform directory:

- addindex
- addintegrity
- config_remote_services
- createLinks
- ldapClean
- remove_service_profiles
- loadDSMLSchema
- serviceability
- syncISIMData

you must complete these steps when SSL is configured:

Procedure

1. Verify that enRoleLDAPConnections.properties, has java.naming.security.protocol set to **ssl**.
2. Open the utility file (for example, addindex.sh or addindex.cmd) with a text editor.
3. Add this property as a Java runtime property. The property is one line.

   ```
   -Djavax.net.ssl.trustStoreType=type_of_truststore
   -Djavax.net.ssl.trustStore=truststore_location -Djavax.net.ssl.
   trustStorePassword=truststore_password -Djava.ext.dirs=WAS_HOME
   \java\jre\lib\ext:WAS_HOME\plugins:WAS_HOME\lib:WAS_HOME\lib\ext
   ```

   For example, ldapClean.sh modified for SSL looks like this example:

   ```
   $JAVA -Djavax.net.ssl.trustStoreType=jks -Djavax.net.ssl.trustStore=
   /opt/ibm/cacerts -Djavax.net.ssl.trustStorePassword=changeit -Djava.ext.
   dirs=/opt/IBM/WebSphere70/AppServer/java/jre/lib/ext:
   /opt/IBM/WebSphere70/AppServer/plugins:/opt/IBM/WebSphere61/
   AppServer/lib:/opt/IBM/WebSphere70/AppServer/lib/ext -cp $CLASSPATH
   com.ibm.itim.systemConfig.LdapSweeper
   ```

4. Save the changes to the utility file.

What to do next

Use the utilities.

Perform additional security-related tasks.

Security configuration for WebSphere Application Server

If you chose to activate administrative security and application security on the WebSphere Application Server, additional security configuration might be required.

Each of these security tasks applies to both single and multi-node deployments. You can complete these additional security tasks:

- Map the `itimadmin` administrative user to the ITIM_SYSTEM role to further limit access.
- If the WebSphere administrators or Security Identity Manager system users are modified outside of Security Identity Manager, run the **runConfig** command to update the Security Identity Manager configuration.
- If you also activated Java 2 security, modify the `library.policy` file and verify that the `was.policy` file exists.
- Modify the token expiration to prevent accidental timeouts in a cluster configuration.
- Activate FIPS compliance for WebSphere Application Server.

Mapping an administrative user to a role

You can map an administrative user to an Security Identity Manager role. The installer typically map during the installation process. However, this task is required if you change the Security Identity Manager System user ID after you install Security Identity Manager.

Before you begin

Ensure that the WebSphere Application Server is running and that the WebSphere administrative console is started.

Procedure

1. On the WebSphere administrative console, click **Applications** > **Enterprise Applications**.
2. Click **ITIM**.
3. In Detail Properties, scroll down and click **Security role to user/group mapping**.
4. Select the check box for **ITIM_SYSTEM**.
5. Click **Map users**.
6. Click **Search**.
7. Select the Security Identity Manager System User (For example, `wasadmin`) from the list.
8. Click **OK**.
9. To prevent unauthorized access, clear the **Everyone?** or **All Authenticated?** check boxes.
10. Save the configuration changes.

What to do next

Continue with other security-related tasks.

Updating the WebSphere administrator and the Security Identity Manager system user

If you changed the **WebSphere Administrator** or **Security Identity Manager System User** fields, you must update the Security Identity Manager configurations with new values.

Before you begin

Ensure that the Security Identity Manager installation process is completed.

Procedure

1. Start the system configuration tool. Issue one of these commands:
   - For Windows operating systems -
     ISIM_HOME\bin\runConfig
   - For UNIX or Linux operating systems -
     ISIM_HOME/bin/runConfig.sh
2. Select the **Security** tab.
   a. Update the **WebSphere Administrator** field and its password with the `wasadmin` user ID that you created in the local OS registry.
   b. Update the **Identity Manager System User** field and its password with the `itimadmin` user ID that you created in the local operating system registry.
3. Click **OK**.

What to do next

Perform additional security-related tasks.

Activating Java 2 security by creating and modifying policy files

If you want to turn on Java 2 security, you must create the `library.policy` file. You must also modify the `was.policy` file to add permissions to access any necessary resources.

Before you begin

If you intend to activate Java 2 security, use the IBM Java 2 Platform Standard Edition Development Kit 1.5 Service Release 6 or later version. You can download the service release. Follow the instructions to apply the fix at the WebSphere Application Server fix pack website.

About this task

Activating Java 2 security for the Security Identity Manager application enforces Java 2 security on all applications that run on the WebSphere Application Server. If you activate Java 2 security for the Security Identity Manager application, configure all other applications that run on the WebSphere Application Server.

Procedure

1. Create the `library.policy` file to add permissions to access any necessary resources.
   a. Create the `library.policy` file in the following directory location: *WAS_PROFILE_HOME*/config/cells/*cellname*/nodes/*nodename*.
   b. Edit the `library.policy` file. Add this statement:

```
grant {
permission java.security.AllPermission;
}
```

Note: This sample policy file provides blanket access to the Security Identity Manager shared library. It does not provide any extra security. Set the policy file according to your security requirements by configuring this file correctly.

2. Ensure that the `was.policy` file exists. The Security Identity Manager installation program automatically creates a sample `was.policy` file. This file has all the permissions that the Security Identity Manager application runs with Java 2 security. If the file does not exist, you must:
   a. Create the file in the following directory on the node: *WAS_PROFILE_HOME*/config/cells/*cellname*/applications/ITIM.ear/deployments/*application_name*/META-INF
   b. Edit the `was.policy` file. Add this statement:

```
grant codeBase "file::${application}" {
permission java.security.AllPermission;
};
```

Note: This sample policy file provides blanket access to Security Identity Manager. It does not provide any extra security. Set the policy file according to your security requirements by configuring this file correctly.

What to do next

Run Java 2 security.

Running Java 2 security on single-node deployments:

You must restart Security Identity Manager to run Java 2 security.

Before you begin

Ensure that Java 2 security is enabled and that Security Identity Manager is installed in a single-node deployment.

Ensure that the WebSphere Application Server is running and that the WebSphere administrative console is started.

Procedure

1. Log on to the WebSphere administrative console.
2. Click **Applications** > **Enterprise Applications**.
3. Select the check box for **ITIM** and click **Stop**. Wait for the Security Identity Manager application to stop.
4. Click **Start.**

What to do next

Perform additional security-related tasks.

Running Java 2 security on multi-node deployments:

To run the Java 2 security component you must synchronize the nodes in the cell.

Before you begin

Ensure that Java 2 security is enabled and that Security Identity Manager is installed in a multi-node (clustered) deployment.

Ensure that the WebSphere Application Server is running and that the WebSphere administrative console is started.

Procedure

1. Log on to the WebSphere administrative console.
2. Click **Server** > **Clusters**.
3. Select the check box next to the cluster name and click **Stop**. Wait for the cluster to stop.
4. Click **Start.**

What to do next

Perform additional security-related tasks.

Increasing the timeout interval

Security uses a Lightweight Third Party Authentication (LTPA) token that expires after an interval of system inactivity. You must ensure that the token expiration value is large enough to prevent accidental timeouts in a cluster configuration.

Before you begin

Ensure that the WebSphere Application Server is running and that the WebSphere administrative console is started.

About this task

The default token expiration value is 120 minutes, which might not be large enough to use with Security Identity Manager. On some systems, the actual timeout interval might be shorter than the value that is specified. A timeout might prevent you from logging on. When a timeout occurs, you must recycle the deployment manager, the cluster, and all node agents.

Procedure

1. Log on to the WebSphere administrative console.
2. Click **Security** > **Global security** > **LTPA**.
3. Set the LTPA timeout interval to a value that exceeds the longest anticipated interval of system inactivity at your site.

What to do next

Perform more security-related tasks.

FIPS compliance for WebSphere Application Server

Federal Information Processing Standards (FIPS) are guidelines that set for software and hardware computer security products. Products that support FIPS standards can be set into a mode where the product uses only FIPS approved algorithms and methods.

Security toolkits typically support both FIPS approved and non-FIPS approved functions. In FIPS mode, the product is incapable of using any non-FIPS approved methods.

You need to ensure that Java uses these IBM cryptographic providers for all cryptographic functions. Check the `java.security` file in the *WAS_HOME*`\java\jre\lib\security` directory for the following entries in the cryptographic provider list. Add these entries to the list if they do not exist.

```
security.provider.1=com.ibm.crypto.fips.provider.IBMJSSE2
security.provider.2=com.ibm.crypto.fips.provider.IBMJCEFIPS
```

Note: The order in which you specify the security providers is important. The security providers are processed in numeric order. The first security provider that supports the encryption method requested is used. On Solaris systems, the first provider must always be `sun.security.provider.Sun`.

Activating FIPS compliance for WebSphere Application Server:

After you set the cryptographic provider list, you must start the WebSphere Application Server to use FIPs. You must also set the environment variable to restrict the IBMJSSE2 provider to FIPS-compliant algorithms.

Before you begin

The IBM cryptographic providers must exist in the `java.security` file.

Ensure that the WebSphere Application Server is running and that the administrative console is started.

For more information about activating FIPS in WebSphere Application Server, see the documentation available in the WebSphere Application Server section of the IBM Knowledge Center.

Procedure

1. Log on to the administrative console.
2. Activate FIPS for WebSphere Application Server.
   a. Click **Security** > **SSL certificate and key management** > **Manage FIPS**.
   b. Select the **Enable FIPS 140-2** option.
   c. Click **Apply**.
   d. Save the configuration changes.
3. Set the environment variable to restrict the IBMJSSE2 provider to FIPS-compliant algorithms.
   a. Click **Server** > **Application Server** > **Server types** > **WebSphere Application Server**.
   b. Click a server, such as `server1`.
   c. In the **Server Infrastructure** field, click the link **Java and Process Management** > **Process Definition**.
   d. In the A**dditional Properties** field, click the link for **Java Virtual Machine**.
   e. In the **Generic JVM Arguments** field, set the environment variable by adding the following statement:
      ```
      -Dcom.ibm.jsse2.JSSEFIPS=true
      ```
4. Save the changes.

What to do next

Run the cipher migration tool.

The cipher migration tool:

A cipher migration utility, changeCipher, is provided to change cipher keys and transition from non-compliant FIPS algorithms to FIPS-compliant algorithms and keys. Using the new cipher key, the migration utility re-encrypts all data in the property files and in LDAP.

The utility is found in the following location:

- On Windows operating systems:
  ISIM_HOME\bin\win\changeCipher.cmd
- On UNIX or Linux operating systems:
  ISIM_HOME/bin/unix/changeCipher.sh

Run the utility on a single server or at the deployment manager to migrate the data in the LDAP repository and in the property files. Also run the utility on each managed node (in a clustered environment) to migrate the property files on that node.

The following example shows the supported usage and command-line parameters for the changeCipher command:

```
changekey     {keystore_name} {keystore_password}
                    [-algorithm AES] [-keysize 128 | 192 | 256]
                    [-skiperrors]
resume        [-skiperrors]
```

For example, to migrate cipher settings from PBEWithMD5AndDES to AES, run the following command:

```
changeCipher changekey itimKeystore2.jceks sunshine
```

This command completes the following tasks:

- Generates a 128-bit AES key and writes it to the specified keystore
- Migrates encrypted data in the LDAP repository to the new cipher.

  Note: The new encrypted data is longer. If the attribute length in LDAP is too small you get an Object Class violation and the script ends.
- Migrates the encrypted data in the property files to the new cipher
- Sets the new cipher settings to `enrole.properties`

While running, the tool creates and maintains a file which contains its current state information. This file is written to *ISIM_HOME*\temp\CipherMigrator.properties. If an error occurs during migration (for instance, if the LDAP server shuts down), correct the problem and start the tool with the **resume** parameter. This parameter tells the utility to pick up from where it left off before the error occurred.

The optional **–skiperrors** parameter tells the tool to continue running even if it encounters data that cannot be decrypted with the old cipher. If specified, undecipherable LDAP data does not cause the tool to fail.

Back up all LDAP data before running the tool. There are a number of things that can go wrong when migrating LDAP data. For example, if the keystore file is

accidentally deleted before the LDAP migration is completed, some of the encrypted LDAP data becomes inaccessible. Backing up LDAP data along with the current keystore ensures you can return to a safe state.

Before running the tool, stop the Tivoli Identity Manager Server. Ensure that there are no pending transactions in the database because encrypted data in the database is not migrated.

For each LDAP object, the cipher migration utility decrypts the attribute with the old cipher and re-encrypts the attribute with the new cipher. No changes are made to attributes that are hashed.

By default, the Java Cryptography Extension (JCE) is shipped with restricted or limited strength ciphers. To use 192-bit and 256-bit Advanced Encryption Standard (AES) encryption algorithms, you must apply unlimited jurisdiction policy files. For more information, see the following website:http://www.ibm.com/developerworks/java/jdk/security/index.html

IBM Security Identity Manager configuration to run as a non-root process

For system security, you can assign the ownership of the profile directory and log directory to a non-root user.

1. Create a WebSphere profile and assign the ownership to a non-root user. See *Creating a profile as an installer and assigning ownership to a non-user* in the WebSphere Application Server Information Center.
2. Ensure that the non-root user has:
   - Read access to the files in *ISIM_HOME*/dirs directory.
   - Read and write accesses to the Security Identity Manager log files. For example, /opt/IBM/tivo../../common/CTGIM/logs/.

     Note: Ensure that the non-root user has permissions for the WebSphere and Security Identity Manager log files. If logs exist that are owned by root, either remove them or change the permissions on them.
     See *Granting write permissions of files and directories to a non-root user for profile creation* for instructions in the WebSphere Application Server Information Center.

Installing the Java plug-in

If the Java plug-in is not installed on your system, or is not at a supported level, the browser prompts you to install the plug-in.

Before you begin

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

About this task

The Java plug-in provides a connection between browsers and the Java platform, and enables IBM Security Identity Manager applets to run within a browser.

Security Identity Manager allows administrators to choose between static or dynamic versioning of the Java plug-in. By default, Security Identity Manager uses dynamic versioning that allows any 1.5.x version over 1.5.0 to work. Alternatively, Security Identity Manager can use static versioning of the Java plug-in, such as version 1.5.0_02.

External websites that provide plug-ins can change. Administrators might also create an internal website to download the Java plug-in. For more information about selecting static and dynamic versioning, or defining download locations, see the *ISIM_HOME*\data\ui.properties file.

Complete these steps to install the plug-in:

Procedure

- On Windows systems, the Internet Explorer or Mozilla Firefox browser prompts you to install the Java plug-in and automatically register it with the browser.

  If your browser does not prompt for the Java plug-in, you can obtain the Java plug-in from the Java SE page of the Oracle website.
- On UNIX and Linux systems, you must complete these manual steps to install and register the Java plug-in:
  1. Obtain the Java plug-in from one of these websites:
     - Linux systems: the *Java SE* page of the Oracle website.
     - AIX systems: *AIX Download and service information* of the IBM developerWorks® website.
  2. Register the Java plug-in with the browser.

Postinstall configuration of an external user registry for authentication

If you installed IBM Security Identity Manager to use an external user registry for authentication, you must complete postinstall configuration steps.

The postinstall configuration steps are:

1. Removing the requirement for password change.
2. Configuring an administrator account in an external user registry.
3. Verifying access for the administrator account.
4. Configuring the WebSphere account repository setting.

Continue with "Removal of the requirement for password change."

Removal of the requirement for password change

Modify the configuration so that you are not required to change the password when you log on to the administrative console.

Modify the configuration so that the **Change password at next logon** attribute is disabled for the default administration account. Set the `erChangePswdRequired` attribute of **ITIM Manager** to `false`.

Use the configuration utilities for your user registry. The following topics describe how to modify the configuration for IBM Security Directory Server. One topic describes how to use a graphical administration utility. The other topic describes how to use command-line utilities.

Continue with one of the following topics:

- "Disabling the password change attribute by using command-line utilities"
- "Disabling the password change attribute with the web administration utility" on page 158

Disabling the password change attribute by using command-line utilities

Modify the configuration so that you are not required to change the password when you log on to the administrative console.

About this task

Use command-line utilities to configure the attribute. If you prefer to use a graphical administration utility, do not complete these steps. Instead, see "Disabling the password change attribute with the web administration utility" on page 158.

Procedure

1. Display the attributes for the default administration account.

   For example, when the default administration account is `ITIM Manager`:

   ```
   ldapsearch -D "cn=root" -w mypassword -L -b "dc=com" "eruid=ITIM Manager"
   ```

   Example results of the search:

   ```
   eruid=ITIM Manager,uo=systemUser,ou=itim,ou=org,dc=com
   eruid=ITIM Manager
   erpswdlastchanged=201204221506Z
   erchangepwrequired=true
   ```

2. Save the attributes to a file.

   For example:

   ```
   ldapsearch -D "cn=root" -w mypassword -L -b "dc=com"
       "eruid=ITIM Manager"
   > myfile
   ```

3. Use an editor to set `erchangepwrequired=false`.
4. Run an LDAP command to load the file with the attribute `erchangepwrequired=false`.

   For example:

   ```
   ./ldapmodify -D "cn=root" -w mypassword -f myfile
   ```

   Example output:

   ```
   Operation 0 modifying entry eruid=ITIM Manager,ou=systemUser,
      ou=tim,ou=org,
   dc=com
   ```

5. Verify that the configuration succeeded.

   For example:

   ```
   ldapsearch -D "cn=root" -w mypassword -L -b "dc=com" "eruid=ITIM Manager"
   ```

   Example results of the search:

   ```
   eruid=ITIM Manager,uo=systemUser,ou=itim,ou=org,dc=com
   eruid=ITIM Manager
   erpswdlastchanged=201204221506Z
   erchangepwrequired=false
   ```

What to do next

Continue with "Configuring an administrator account in an external user registry" on page 158.

Disabling the password change attribute with the web administration utility

Modify the configuration so that you are not required to change the password when you log on to the administrative console.

About this task

You can use the administration utility for your directory server. The following procedure describes how to use the IBM Security Directory Server web administration tool.

If you prefer to use command-line utilities, do not use this procedure. Instead, see "Disabling the password change attribute by using command-line utilities" on page 157.

Procedure

1. Log on to the IBM Security Directory Server web administration tool as the administrator.
2. Go to **Directory management > Manage entries**. Find the `ITIM Manager` entry. `ITIM Manager` is the default administrator account.
3. Click `eruid=ITIM Manager` and click **Next**.

   Note: If you specified a different account for the default administrator, modify that account instead of `ITIM Manager`. For example, on UNIX operating systems you cannot create account names with spaces. In this case, some administrators create a different account name, such as `itimManager`.
4. On the Edit an entry page, select **Optional attributes**.
5. Scroll down to the `erChangePswdRequired` attribute and change the value to **False**.
6. Click **Finish** to save the changes.

What to do next

Continue with "Configuring an administrator account in an external user registry."

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 16. Sample **ldapmodify** command to change administrator account*

Entry	Description
ldapmodify	This command is in *TDS_HOME*/bin directory. For example: **Windows** C:\Program Files\LDAP\V6.3\bin **UNIX or Linux** *TDS_HOME*/bin
hostIP	The IP address of the IBM Security Directory Server, where the IBM Security Identity Manager LDAP data is stored.
adminDN	The administrator DN. For example, cn=root
adminPassword	The administrator password
filePath	The path to the file that you created in the previous step.

3. Update the IBM Security Identity Manager properties file ISIM_HOME/data/enRole.properties with the new default administrator ID.

   Example entry:

   `enrole.defaultadmin.id=itimManager`

4. Restart the WebSphere application server, to load the updated values from the property file.

What to do next

Continue with "Verifying access for the administrator account."

Verifying access for the administrator account

Verify that the administrator account is configured correctly.

About this task

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

Procedure

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

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

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

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

   The default administrator account is `ITIM Manager`, but you had the option of specifying a different name.
3. Enter the password you specified for your administrator account.

   The default password is `secret`.

Results

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

What to do next

Continue with "Configuring the WebSphere account repository setting."

Configuring the WebSphere account repository setting

Use the administration console to remove the default value for the WebSphere account repository attribute.

About this task

You can use the administration console to manage services. When you select **Manage Services** on the console, you can select a service, and then access a Service Information page. You can use this page to update the attribute values for the service.

To complete the configuration for external user registry, you must modify the value for the **WebSphere account repository** attribute on the Service Information page for the ITIM Service. The value in the field specifies the account repository service that is used by IBM Security Identity Manager for authentication. By default, this field is set to `ITIM Service` to support the IBM Security Identity Manager *custom registry*.

You chose to use an *external registry* instead of the custom registry. To complete configuration for the external registry, you must remove the default value from the field.

Procedure

1. If you are not currently logged on to the IBM Security Identity Manager administration console, log in now as the administrator.

   For login instructions, see "Verifying access for the administrator account" on page 159.
2. Click **Manage Services**.
3. On the Select a Service page, click **Search**.

   The search results display a table with an entry for each configured service.
4. In the table, select the check box for **ITIM Service**.
5. Click **Change**.
6. On the Service Information page, locate the **WebSphere account repository** field. This field has the value `ITIM Service`. Click **Clear**.

The **WebSphere account repository** field is now empty.

For more information, see the online help. To view the online help, click the **?** icon. The browser displays the Change a Service help file in a new browser window. Click **Service Information**. On the Service Information help page, click **ITIM Service**. Review the contents of this page.

7. Click **OK**.

Results

Configuration of the external user registry for authentication is now complete.

For information about how to use the external registry, see the example tutorial *Configuring and using IBM Security Identity Manager with an external user registry*. This document is on the file system where your code was installed. See *ISIM_HOME*/extensions/6.0/doc/authentication/Using_an_External_User_Registry.odt.

Chapter 9. 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 or Oracle Directory Server Enterprise Edition to store Security Identity Manager information, you must set the server to use SSL. Then you must configure the SSL certificates that you want to use.

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

Configuration of SSL for IBM Security Directory Server

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

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

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

Configuration of SSL for Oracle Directory Server Enterprise Edition

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

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

Configuration of the SSL client to trust the LDAP server certificate

The Security Identity Manager Server does not operate as an embedded part of WebSphere Application Server. It operates as a Java application and uses Java secure socket extension (JSSE) to implement SSL support.

SSL certificates and CA certificates are retrieved from a standard format Java truststore or keystore. The truststore and keystore use the same file formats that the Java virtual machine and WebSphere Application Server use for other certificate configuration. You can use standard Java tools to maintain the trust and keystores, including the IBM Key Management tool and the Java Keytool command-line utility.

To configure the SSL connection between the Security Identity Manager Server and LDAP Server, you must import the self-signed certificate or CA certificate created for the LDAP Server into the truststore. This truststore is used by the IBM JSSE, which is part of WebSphere Application Server. Additionally, you must first configure Security Identity Manager to use SSL when communicating with the LDAP Server. Configure Security Identity Manager to use the `ldaps` protocol instead of the `ldap` protocol.

Installing the self-signed certificate in the JSSE truststore

Use this procedure to install the self-signed certificate and to add it to the certificate store.

Before you begin

For this task, the default truststore that is present in the JRE of the WebSphere Application Server is used. Also, the *ikeyman* utility is used to configure the certificates

Procedure

1. Start the *ikeyman* utility. The utility (`ikeyman.bat` or `ikeyman.sh`) is in the *WAS_HOME*`\bin`.
2. From the Key Database File menu, select **Open**.
3. In the key database type, select **JKS**.
4. In the File Name field, type `cacerts`.
5. In the Location field, type `WAS_HOME\java\jre\lib\security\`.
6. In the Password Prompt window, type the password for the keystore in the Password and Confirm Password window. The default password is `changeit`.
7. Click **OK**.
8. Add the certificate you created for the LDAP server into this certificate store.
   a. In the main window, in the Key database content area, select **Signer Certificates** from the list.
   b. Click **Add**.
   c. In the Certificate file name field, browse and locate the server certificate file that was created for the LDAP server, which is in **Binary Der data**. Verify that the appropriate directory is displayed in the Location field.
   d. Click **OK**.
   e. In the prompt, type a label for this certificate. For example, type `LDAPCA`.
   f. Click **OK**.

   Note: If you are not able to locate the server certificate file as previously described, follow these steps to extract it from the server certificate store:
   - For IBM Tivoli Directory Server, use the *ikeyman* utility to extract the certificate.
   - For Oracle Directory Server, follow these steps to extract the server certificate:
     a. Find the alias of the certificate. From `ODSEE-install/bin` directory, run:
        ```
        ./dsadm list-certs <instance-home-dir-path>
        ```
     b. Show the certificate and redirect the output to a `Binary Der` file, assuming the alias of the certificate is *defaultCert*:
        ```
        ./dsadm show-cert -F der -o cert.der <instance-home-dir-path> defaultCert
        ```

`cert.der` is the requisite server certificate file.
The certificate is added for the LDAP Server. You can now close the *ikeyman* utility.

What to do next

Configure Security Identity Manager to use SSL when communicating with the LDAP server.

Configuring Security Identity Manager to use SSL when communicating with the LDAP server

After importing the LDAP self-signed certificate, you must configure Security Identity Manager Server to complete the SSL connection.

Before you begin

You must finish installing the self-signed certificate for the LDAP server in the JSSE truststore.

Procedure

1. Edit the `enRoleLDAPConnection.properties` file. This file is in the *ISIM_HOME*`\data` directory.
   a. Set the port value on the `java.naming.provider.url` property to the SSL port number configured on directory server [LDAP]. For example,
      `java.naming.provider.url=ldaps://localhost:636`
   b. Set the value of the `java.naming.security.protocol` property to `ssl`. This setting directs the Security Identity Manager Server to use SSL to communicate to LDAP. Alternately you can change the protocol in `java.naming.provider.url` from ldap to ldaps. For example,
      `java.naming.security.protocol=ssl`
2. Save the changes.

What to do next

Perform other security-related tasks.

Chapter 10. Troubleshooting

Troubleshooting information helps you to resolve problems with the Security Identity Manager installation.

IBM Security Identity Manager Server issues

You can resolve some of the common issues that you might encounter when you install IBM Security Identity Manager Server.

Problems when starting the installation program

If you cannot start the Security Identity Manager installation program, check the system requirements.

- Is there enough real memory available to run the installation program? For more information, see *Hardware and Software requirements* on the IBM Security Identity Manager product documentation site.
- Are the correct operating system levels, patches, and space requirements provided for the hardware and software prerequisites? For more information, see *Hardware and Software requirements* on the IBM Security Identity Manager product documentation site.
- Does the installation program have the correct file permissions to run? Administrative privileges are required.
- Is your firewall preventing processes that are active during installation from accessing external resources? For example, if you have a firewall that prevents **ldapsearch** from connecting to the directory server, the IBM Security Identity Manager installation fails.
- If the installation is on a UNIX or Linux system, do you have the correct permissions and display variables set?

  A common mistake is to log on to the desktop and omit disabling access control. Then use Telnet or SSH to connect to a remote host on which you intend to install the IBM Security Identity Manager Server. To correct this problem:

  1. Run this command at the command shell of your desktop to disable access control for the X Server:

     ```
     xhost +
     ```

  2. Use Telnet or SSH to connect to the remote host. Run this command to set the DISPLAY environment variable:

     ```
     export DISPLAY=hostname:0.0
     ```

     The value of *hostname* is the host name or IP address of your local desktop computer.

IBM Security Identity Manager configuration errors

Check the IBM Security Identity Manager activity summary log file (`itim_install_activity.log`). For the Linux and UNIX systems, this file is in the `/opt/IBM/isim/install_logs` directory. If a non-fatal error is reported and it involves **DBConfig**, **ldapConfig**, or system configuration, you can use stand-alone IBM Security Identity Manager configuration utilities to recover.

IBM Security Identity Manager Server does not start

If the IBM Security Identity Manager Server does not start, examine the following log files. Correct the errors that are recorded.

- *WAS_PROFILE_HOME*\logs*server_name*\SystemOut.log

  The value of *PROFILE* is the name of the WebSphere Application Server profile that runs IBM Security Identity Manager.

  The value of *server_name* is typically server1 for single-server environments.
- *TIVOLI_COMMON_DIRECTORY*\CTGIM\logs\trace.log

  In this directory, also examine the msg.log file. Installing IBM Security Identity Manager Server defines the value of *TIVOLI_COMMON_DIRECTORY*.

Unable to log on to Security Identity Manager

If continued attempts fail to log on to Security Identity Manager, determine whether the SystemOut.log file contains errors about referencing the Security Identity Manager properties files.

Before you begin

Ensure that the WebSphere Application Server is running and that the WebSphere administrative console is started.

Ensure that the *ISIM_HOME*\data directory contains the properties files.

Procedure

1. To verify that the WebSphere Application Server references the *ISIM_HOME*\data directory, log on to the WebSphere administrative console.
2. Click **Servers** > **Application Server** > **Server types** > **WebSphere Application Server**.
3. Select a server such as server1 and under **Server Infrastructure** > **Java and Process Management**, click **Process Definition**.
4. In the Process Definition, click **Java Virtual Machine**.
5. Ensure that the **Classpath** field specifies the *ISIM_HOME*\data directory.

What to do next

If continued attempts fail, examine the status of the Security Identity Manager middleware. See

- "Verifying the database connections" on page 114
- "Verifying that the directory server is running correctly" on page 114

The messaging engine does not start

If the messaging engine does not start, you need to check the data source connection.

Before you begin

Ensure that the WebSphere Application Server is running and that the WebSphere administrative console is started.

Procedure

1. Log in to the WebSphere administrative console.
2. **Service Integration** > **Buses**.
3. Click **itim_bus**, if it exists.
4. In the Topology section, click **Messaging engines**.
5. Click the message engine name.
6. Under the Additional Properties section, click **Message store** to see the data source JNDI name.
7. From this JNDI name, link to the Security Identity Manager data source defined under the Resources section.
8. Test the data source connection. See "Verifying the database connections" on page 114.
   - If the data source connection test fails, see "Database connections fail."
   - If the connection test succeeds, examine the *WAS_PROFILE_HOME*\logs\server_name\SystemOut.log file to determine the reason that the messaging engine cannot be started.

What to do next

Perform additional troubleshooting or return to verification tasks.

Database issues

You can resolve some of the common database issues that you might encounter when you install IBM Security Identity Manager Server.

Database connections fail

You can correct any connections that did not work when you verified the database connections.

Before you begin

Ensure that the WebSphere Application Server is running and that the WebSphere administrative console is started.

About this task

This task uses IBM DB2 values. If you are using a Microsoft SQL server or an Oracle database, complete similar steps with the appropriate values. For more information, see your database product documentation.

Procedure

1. Verify that the CLASSPATH value is correct. The CLASSPATH definition of the JDBC provider is set up during the Security Identity Manager installation.
   a. Log on to the WebSphere administrative console.
   b. Click **Resources** > **JDBC** > **JDBC Providers** > **ITIM XA DB2 JDBC Provider**.
   c. Examine the properties to verify that the CLASSPATH value is correct. For example, its value is like these values for DB2:

```
$ITIM_DB_JDBC_DRIVER_PATH\db2jcc.jar
$ITIM_DB_JDBC_DRIVER_PATH\db2jcc_license_cisuz.jar
$ITIM_DB_JDBC_DRIVER_PATH\db2jcc_license_cu.jar
```

d. To determine the value of $ITIM_DB_JDBC_DRIVER_PATH, click **Environment** > **WebSphere Variables**. Scroll through the list to locate the variable and confirm it is correct.

2. Verify that the DB2 user ID and password are correct.
   a. Log on to the WebSphere administrative console.
   b. Click **Resources** > **JDBC** > **Data Sources** > **ITIM ITIM Data Source**.
   c. Examine these fields to verify the correct values:
      - Component-managed Authentication Alias

        The value is `itim-init`.
      - Container-managed Authentication Alias

        The value is `itim-init`.
3. Under the Related Items category, click **JAAS - J2C authentication data** Examine the Alias list to ensure that an itim-init entry exists.
   a. Click **itim-init**.
   b. Verify that the value of the user ID field is identical to the Tivoli Identity Manager Database User specified in *ISIM_HOME*`\data\enRole.properties` file, for example, `itimuser`. Do not change this value.
   c. Note the password field. If you use this field to reset the password, ensure that the password value that you enter is identical to the value defined in the *ISIM_HOME*`\data\enRoleDatabase.properties` file.
4. Ensure that other database settings are correct. Check the status of the DB2 service listening port (typically 50000, 50002, or 60000) by using a utility such as netstat. The system `etc` directory contains a file called `services` that contains the actual port number that is being used. For more information, see "Determining the correct service listening port and service name" on page 25.
5. If DB2 is not listening on the port and you are using IPv6 and UNIX/Linux to connect to DB2, modify your /etc/hosts file.
   a. On the workstation that runs IPv6, append these two lines to your `/etc/hosts` file:

      ```
      IPv4_address hostname
      IPv6_address hostname
      ```

      For example, if the host name is `myhost`, the IPv6_address is 0000:ffff:ffff:0000:20e:cff:fe50:39c8 and the IPv4_address is 192.168.4.4, then you must append these two lines in the `/etc/hosts` file.

      ```
      192.168.4.4 myhost
      0000:ffff:ffff:0000:20e:cff:fe50:39c8 myhost
      ```
   b. Log in as the DB2 instance owner and restart the DB2 server by issuing the following commands:

      ```
      db2stop
      db2start
      ```
   c. Ensure that DB2 is running on the IPv6 address by issuing the following command:

      ```
      netstat -an | grep db2port
      ```

      For example, if the db2 is running on the port 50000, then you see the following line as the output:

      ```
      tcp        0      0 :::50000                :::*                    LISTEN
      ```

What to do next

Perform additional troubleshooting or return to verification tasks.

SQL server does not prompt for password change

When the itim manager account logs in for the first time, the user is typically prompted to change the password. This prompt might not occur if you are using SQL Server 2008.

Before you begin

Security Identity Manager and Microsoft SQL Server must be installed.

Procedure

1. To resolve the password prompt issue, log on to the SQL Server 2008 host computer.
2. Start the Microsoft SQL Server Management Studio.
3. Expand the SQL server in the object explorer.
4. Expand **Databases** and move to the master database.
5. Expand **Security** > **Schemas**.
6. Right click **DBO** and click **Properties**.
7. Click **Permissions**, click **Add**, and browse to add the required users.
8. Grant all permissions to these required users and click **OK**.
9. Restart the server, disconnect, and reconnect with user `sa` in mixed authentication mode.

What to do next

Perform additional troubleshooting or return to verification tasks.

Database configuration is too restrictive for SQL Server

Security Identity Manager is configured with Microsoft SQL Server 2008 as the Security Identity Manager database. You might receive a permission denied message in `trace.log` file.

Before you begin

Security Identity Manager and Microsoft SQL Server must be installed.

About this task

This error message might occur the first time that you access the Security Identity Manager Server after you run the DBConfig.

```
javax.transaction.xa.XAException: java.sql.SQLException:
Failed to create the XA control connection.
Error: EXECUTE permission denied on object 'xp_sqljdbc_xa_init',
database 'master', schema 'dbo'.
```

To resolve this issue, complete following steps:

Note: In this task, *itimuser* is the database user configured for Security Identity Manager database, and *itimdb* is the name of the database configured for Security Identity Manager.

Procedure

1. Stop the application server.
2. Start the Microsoft SQL Server Management Studio.
3. Expand the SQL server in the object explorer.
4. Expand **Databases** and delete *itimdb*.
5. Delete the *itimuser* schema from master database.
   a. Expand **DatabasesSystem DatabasesmasterSecuritySchemas**.
   b. Delete itimuser.
6. Delete itimuser, ITIML000, ITIML001, and so on, and log in from **SecurityLogins**.
7. Create a database.
8. Perform the dbConfig operation.
9. Start the application server.

   Note: If name of the database or database user is changed, run the runConfig utility and restart the application server.

What to do next

Perform additional troubleshooting or return to verification tasks.

Fixing data replication errors for invalid object names

Data replication errors can occur in a cluster environment if the shared access configuration utility was not run.

About this task

When IBM Security Identity Manager is deployed in a cluster environment, and shared access is configured, data replication can report errors. The errors indicate that an invalid object name was found. The pattern of the error is:

```
Invalid object name itimuser.isim_object_name
```

For example:

```
Invalid object name 'itimuser.erAccountItem'
Invalid object name 'itimuser.erServiceItem'
Invalid object name 'itimuser.erSystemUser'
```

In this case, data replication fails if you run **DBConfig** to drop all database tables but do not run **SAConfig** to repopulate the tables that are specific to the shared access module.

The file *ISIM_HOME*/data/dataSynchronization.properties contains entries that are configured to replicate, such as erAccountItem or erServiceItem. However, the replication component cannot find the target replication table that is specified in DB_REPLICATION_CONFIG. In this case, the component defaults to the class name.

To fix this problem, complete the steps in the following procedure.

Procedure

1. On the deployment manager, change directory to the bin directory in IBM Security Identity Manager installation location and run the **SAConfig** utility.

   For example:

Table 17. Running SAConfig

Operating system	Command
Windows	In `C:\Program Files\IBM\isim\bin`, either click `SAConfig` or open a command window and enter **`SAConfig`**.
UNIX or Linux	In `/opt/IBM/isim/bin`, enter **`./SAConfig`**.

2. Update the `clipassword` property in the `ISIM_HOME/data/KMIPServer.properties` file.

   You can specify any string value. For example:

   ```
   clipassword=test
   ```

   Note: Edit this file only on the deployment manager.

3. Configure the keystore files for the credential vault server.

   Note: Complete this step only on the deployment manager. You do not need to complete it on the cluster members.

   In the following command, ensure that the value of the -p parameter matches the value you specified for clipassword in the `ISIM_HOME/data/KMIPServer.properties` file.

   Use the command for your operating system:

   - On the Windows operating systems, enter:

     ```
     cd /d "ISIM_HOME\lib"
     ```

     From the *ISIM_HOME*`\lib` directory, run the following command:

     ```
     "ISIM_HOME\jre\jre\bin\java" -cp
     com.ibm.sec.authz.jaccplus_7.3.1.jar;
     com.ibm.sec.authz.xacml4j_7.3.1.jar;
     j2ee.jar;
     ojdbc.jar;
     db2jcc.jar;
     db2jcc_license_cu.jar;
     sqljdbc.jar;
     com.ibm.tklm.kmip.jar;
     CVCommon.jar;
     CVCore.jar;
     CVCli.jar;
     com.ibm.tklm.credvault.common.jar;
     commons-cli.jar;
     com.ibm.cv.kmip.ext.jar
     -DKMIPConfigProperties="$USER_INSTALL_DIR$$\$data$\$KMIPServer.properties"
     -Djava.security.auth.login.config==login.config
     -Djava.security.auth.policy==jaas.policy
     com.ibm.cv.cli.CVShell -u test -p test
     ```

   - On the UNIX or Linux operating systems, enter:

     ```
     cd "ISIM_HOME/lib"
     ```

     From the *ISIM_HOME*`\lib` directory, run the following command:

     ```
     "ISIM_HOME/jre/jre/bin/java" -cp
     com.ibm.sec.authz.jaccplus_7.3.1.jar:
     com.ibm.sec.authz.xacml4j_7.3.1.jar:
     j2ee.jar:
     ojdbc.jar:
     db2jcc.jar:
     db2jcc_license_cu.jar:
     sqljdbc.jar:
     com.ibm.tklm.kmip.jar:
     CVCommon.jar:
     CVCore.jar:
     CVCli.jar:
     ```

```
com.ibm.tklm.credvault.common.jar:
commons-cli.jar:
com.ibm.cv.kmip.ext.jar:
-DKMIPConfigProperties="$USER_INSTALL_DIR$$/$data$/$KMIPServer.properties"
-Djava.security.auth.login.config==login.config
-Djava.security.auth.policy==jaas.policy
com.ibm.cv.cli.CVShell -u test -p test
```

The command generates two credential vault keystore files, `cvKeystore.jceks` and `pwdEncKeystore.jceks`, under the *ISIM_HOME*`/data/keystore` directory. It updates the credential vault database data entry and the encryption key in *ISIM_HOME*`/data/KMIPServer.properties`.

4. Copy the generated keystore files and `KMIPServer.properties` to the `WAS_DM_profile_path/config/cells/`*cellName*`/itim` directory.

   Note: Complete this step only on the deployment manager. You do not need to complete it on the cluster members.
5. Manually synchronize the nodes from the WebSphere Application Server Deployment Manager console.
6. On each cluster member, copy the following credential vault files from the WebSphere profile directory hierarchy to the IBM Security Identity Manager data directory hierarchy:

Table 18. Credential vault server files to copy

Copy this file:	To this location:
WAS_PROFILE_PATH`/config/cells/`*cellName*`/itim/cvKeystore.jceks`	*ISIM_HOME*`/data/keystore/cvKeystore.jceks`
WAS_PROFILE_PATH`/config/cells/`*cellName*`/itim/pwdEncKeystore.jceks`	*ISIM_HOME*`/data/keystore/pwdEncKeystore.jceks`
WAS_PROFILE_PATH`/config/cells/`*cellName*`/itim/KMIPServer.properties`	*ISIM_HOME*`/data/KMIPServer.properties`

7. Restart the WebSphere Application Server cluster.

Directory server issues

You can resolve some of the common directory server issues that you might encounter when you install IBM Security Identity Manager Server.

The directory server does not start

If the directory server fails to start after a restart attempt, examine the ibmslapd.log file.

Check the ibmslapd.log file for messages that indicate whether the directory server is completely or partially started. Perform the corrective actions.

The location of the log file depends on the IBM Tivoli Directory Server version:

- Windows operating systems:

  ITDS_INSTANCE_HOME`\logs\ibmslapd.log`. For example, the file is in the `C:\idsslapd-ldapdb2\logs` directory.
- UNIX or Linux operating systems:

  ITDS_INSTANCE_HOME`/ibmslapd.log`. On Linux, for example, the file is in the `/home/ldapdb2/idsslapd-ldapdb2/logs` directory.

IBM Security Directory Server LDAP configuration or upgrade might hang on AIX systems

LDAP configuration might hang during IBM Security Identity Manager installation on AIX systems if you use IBM Security Directory Server Version 6.3 with fix pack 21 or lower. An LDAP upgrade might also hang when you apply a fix pack to an existing IBM Security Identity Manager installation.

The problem affects IBM AIX version 6.1 and higher systems. To avoid the problem, install IBM Security Directory Server version 6.3 interim fix 6.3.0.26 on the IBM Security Directory Server. The interim fix installation requires that you also update any prerequisite IBM Global Security ToolKit (GSKit) packages.

Version of IBM Security Directory Server is not recognized

On the Red Hat Linux Enterprise 6.0 operating system, the middleware configuration utility might not recognize a supported version of the IBM Security Directory Server and generate error messages.

If you are installing IBM Security Identity Manager version 6.0 on Red Hat Linux Enterprise 6.0, these messages might be displayed:

- `CTGIMP557I You can override the installation directory for product IBM Tivoli Directory Server by cancelling this configuration program and then running this configuration program again followed by the option: "-W ITIMRSP.idsInstalledDir=directory".`
- `CTGIMP556W If you continue configuring with missing or unsupported products with this configuration program, you are proceeding at your own risk. This configuration program does not support using IBM Security Identity Manager with missing or incorrect versions of this product.`

If you installed a supported version of IBM Security Directory Server such as 6.2.0.3, you can ignore these messages and continue with the installation.

Tivoli Directory Integrator issue

You might encounter a problem, when you install IBM Security Directory Integrator version 7.1 on Red Hat Linux Enterprise 6.0.

launchpad.sh fails to start the installation of IBM Tivoli Directory Integrator

When the installation launchpad for IBM Security Directory Integrator version 7.1 fails to start on Red Hat Linux Enterprise 6.0 using `launchpad.sh`, use `install_tdi71_linux_x86.bin` instead.

Web browser issues

You can resolve some of the common web browser issues that you might encounter, when you install Security Identity Manager Server.

IBM Security Identity Manager Logon failures

You might not be able to log on to Security Identity Manager for various reasons. For example, you might be using an unsupported web browser.

For a list of supported browsers, see *Browser requirements for client connections* on the Security Identity Manager product documentation site.

Ensuring that the browser registers the Java plug-in

Security Identity Manager uses applets that require the Java plug-in, which is provided by the Java 2 Runtime Environment, Standard Edition (JRE). The Java plug-in provides a connection between browsers and the Java platform, and enables applets to run within a browser. For more information about the version of the Java plug-in that Security Identity Manager supports, see *Software prerequisites* on the Security Identity Manager product documentation site.

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. For more information about these steps, see *Installing the Java plug-in* on the Security Identity Manager product documentation site.

Avoiding two web browser sessions on the same computer

Do not start two separate browser sessions from the same client computer. The two sessions are regarded as one session ID, which causes problems with data.

Enabling active scripting on Microsoft Internet Explorer

For Microsoft Internet Explorer, ensure that the Active Scripting item is enabled in the Scripting section of the Internet Options.

Before you begin

You must have a supported version of Internet Explorer installed.

Procedure

1. Start Internet Explorer.
2. Click **Tools** > **Internet Options** on the main menu.
3. On the Security tab, click the **Internet** icon, and then click **Custom Level**.
4. In the Scripting, Active Scripting area, select **Enable**.
5. Click **OK**.
6. In the Internet Options window, click **OK**.

What to do next

Perform additional troubleshooting or return to verification tasks.

WebSphere Application Server issues

You can resolve some of the common WebSphere Application Server issues that you might encounter when you install Security Identity Manager Server.

The Security Identity Manager application runs within the WebSphere Application Server as an enterprise application. The Security Identity Manager installation program uses the WebSphere command-line interface (`wsadmin`) to deploy the Security Identity Manager application onto the WebSphere Application Server. Deploying the Security Identity Manager application also completes certain configuration steps on the WebSphere Application Server.

When the deployment completes, the Security Identity Manager files are in these directories:

- *WAS_PROFILE_HOME*\installedApps*cellname*\ITIM.ear

- *WAS_PROFILE_HOME*\config\cells*cellname*\applications\ITIM.ear

If the deployment fails, check the installation log files under the *ISIM_HOME*\install_logs\ directory. Start with the itim_install_activity.logfile. Also examine the setupEnrole.stdout log file.

Correcting connection scripting errors

Use this task if the log data indicates a failure to establish a SOAP connection to the WebSphere Application Server configuration manager. You can also use this task for WebSphere Application Server scripting errors.

Before you begin

Ensure that the WebSphere Application Server and Security Identity Manager are installed.

Procedure

1. Resolve the problem that prevents the connection to the WebSphere Application Server or the problem described as a scripting error. For more information, see the WebSphere documentation.
2. Run one of the following commands to deploy the Security Identity Manager Server onto the WebSphere Application Server.
   - If WebSphere administrative security and application security is on, enter one of these commands:
     - Windows operating systems:

       ```
       ISIM_HOME\bin\setupEnrole.exe install server:server_name user:user_id
       password:pwd ejbuser:ejb_user_id ejbpassword:ejbpassword
       ```

     - UNIX or Linux operating systems:

       ```
       ISIM_HOME\bin\setupEnrole.sh install server:server_name user:user_id
       password:pwd ejbuser:ejb_user_id ejbpassword:ejbpassword
       ```

     The value of *server_name* is the name of the WebSphere Application Server on which the Security Identity Manager application is deployed. The value of *user_id* is the WebSphere administrator user ID, such as *wsadmin*. The value of *pwd* is the password for the WebSphere administrator user ID, such as *secret*. The value of *ejb_user_id* is the Identity Manager System user ID, which uses the WebSphere Application Server administrator user ID by default.

     Note: If the Identity Manager System user ID contains a value with a space in between, such as *Bob Smith*, you must add a quotation mark to this value. The command, for example, must be entered as:

     ```
     SetupEnrole.exe install server:server1 user:wsadmin password:secret
     ejbuser:"Bob Smith" ejbpassword:secret
     ```

   - If WebSphere administrative security and application security is off, enter one of these commands:
     - Windows operating systems:

       ```
       ISIM_HOME\bin\setupEnrole.exe install server:server_name
       ```

     - UNIX or Linux operating systems:

       ```
       ISIM_HOME\bin\setupEnrole.exe install server:server_name
       ```

     The default of *server_name* is server1.

What to do next

Perform additional troubleshooting or return to verification tasks.

Correcting timeout errors

If the log data indicates that the failure is caused by a timeout error, continue the Security Identity Manager installation process.

Before you begin

Ensure that the Security Identity Manager installation process is complete.

Procedure

1. Delete these directories if they exist.
   - *WAS_PROFILE_HOME*\installedApps*cellname*\ITIM.ear
   - *WAS_PROFILE_HOME*\config\cells*cellname*\applications\ITIM.ear
2. Run one of the following commands to deploy the Security Identity Manager Server onto the WebSphere Application Server.
   - If WebSphere administrative security and application security is on, enter one of these commands:
     - Windows operating systems:

       ```
       ISIM_HOME\bin\setupEnrole.exe install server:server_name user:user_id
       password:pwd ejbuser:ejb_user_id ejbpassword:ejbpassword
       ```

     - UNIX or Linux operating systems:

       ```
       ISIM_HOME\bin\setupEnrole.sh install server:server_name user:user_id
       password:pwd ejbuser:ejb_user_id ejbpassword:ejbpassword
       ```

     The value of *server_name* is the name of the WebSphere Application Server on which the Security Identity Manager application is deployed. The value of *user_id* is the WebSphere administrator user ID, such as *wsadmin*. The value of *pwd* is the password for the WebSphere administrator user ID, such as *secret*. The value of *ejb_user_id* is the system user ID, which uses the WebSphere Application Server administrator user ID by default.

     Note: If the system user ID contains a value with a space in between, such as *Bob Smith*, you must add a quotation mark to this value. The command, for example, must be entered as:

     ```
     SetupEnrole.exe install server:server1 user:wsadmin password:secret
     ejbuser:"Bob Smith" ejbpassword:secret
     ```

   - If WebSphere administrative security and application security is off, enter one of these commands:
     - Windows operating systems:

       ```
       ISIM_HOME\bin\setupEnrole.exe install server:server_name
       ```

     - UNIX or Linux operating systems:

       ```
       ISIM_HOME\bin\setupEnrole.exe install server:server_name
       ```

     The default of *server_name* is server1.

What to do next

Perform additional troubleshooting or return to verification tasks.

Determining the port number of the default host

If you have multiple instances of WebSphere Application Server running on the same computer, the port number might be a different value.

Before you begin

Ensure that the WebSphere Application Server is running and that the WebSphere administrative console is started.

Procedure

1. Log on to the WebSphere administrative console.
2. **Server** > **Application servers**.
3. Click the server that hosts the Security Identity Manager application cluster member.
4. Under the Communications section, click the **Ports** link.
5. Find the port number listed next to the WC_defaulthost port name. This port number is the one used to connect to Security Identity Manager.

What to do next

Perform additional troubleshooting or return to verification tasks.

Changing the WSSession cache size

The cache limit of the WSSession cache can be changed manually in the WebSphere Application Server administrative console.

Procedure

1. From the administrative console, go to **Resources** > **Object cache instances** tab.
2. Change the cache size of WSSession_cache.

IIA:Runconfig updateRealmName.py fails

IIA:Runconfig updateRealmName.py fails when the customer Security Domain User Realm is set to use Global Security.

Before you begin

Ensure that the WebSphere Application Server is running and that the WebSphere administrative console is started.

About this task

This error occurs because the user registry specified does not exist in the configuration. The realm was not correctly configured for the security domain. To prevent this error when configuring Global Security to use federated repositories:

Procedure

1. On the Security Domains page, expand **User Realm:**
2. Click **Customize for this domain**.
3. In the **Realm type** field, select the setting that matches the realm settings on the Global Security page.
4. Continue the configuration process.

Installing IBM Security Identity Manager version 6.0 Fix Pack 2 on Windows Server 2012

IBM Security Identity Manager supports Windows Server 2012. However, the **Updater installer** utility (Updi) that is used to install the fix pack does not recognize Windows Server 2012 as a supported operating system.

Before you begin

WebSphere Application Server version 8.5 recognizes Windows Server 2012 as a supported operating system. If you want to install IBM Security Identity Manager version 6.0 on Windows Server 2012, you must install WebSphere Application Server version 8.5 first.

About this task

To install IBM Security Identity Manager version 6.0 and Fix Pack 2 on Windows Server 2012:

Procedure

1. Download IBM WebSphere Updater installer version 7.0.0.27.
2. Use the Updi installer to install IBM Security Identity Manager version 6.0 and Fix Pack 2 on Windows Server 2012.
3. When the message is displayed that Windows Server 2012 is not a supported operating system, click **Continue**.
4. Complete the installation wizard tasks.

Log files

After the system configuration is completed, you can find the log files in these locations.

File names	Description and location
• WebSphere Application Server logs	Installation log files for WebSphere Application Server. The <WAS_HOME>/AppServer/profiles/<APP_SERVER>/logs/directory contains the logs for WebSphere Application Server.
• isim_install.stdout • isim_install.stderr	Standard out and error log files for Security Identity Manager. In the system root directory.
• dbConfig.stdout • ldapConfig.stdout • dbUpgrade.stdout • ldapUpgrade.stdout • itim_installer_debug.txt • runConfigFirstTime.stdout • runConfig.stdout • setupEnrole.stdout • StartStopWas.stdout • itim_install_activity.log	In the ISIM_HOME\install_logs directory.

File names	Description and location
• trace.log • msg.log	In the `TIVOLI_COMMON_DIRECTORY\CTGIM\logs\` directory. The Tivoli Common Directory is the central location for all serviceability-related files, such as log files and first-failure capture data.
cfg_itim_mw.log	The middleware configuration utility log file. In the System %TEMP% directory.

Chapter 11. Uninstallation of Security Identity Manager

Use the uninstallation program to remove Security Identity Manager.

The Security Identity Manager uninstallation program complete the following tasks:

- Removes all files in the *ISIM_HOME* directory that the Security Identity Manager installation program created. It removes the certificates in the *ISIM_HOME*\cert directory and the itimKeystore.jceks keystore file in the *ISIM_HOME*\config\keystore directory.
- Clears all configuration settings that were created for the Security Identity Manager Server on the WebSphere Application Server.
- Removes the Security Identity Manager Server from these computers:

  Single-server configuration:
  The computer that has the WebSphere Application Server.

  Cluster configuration:

  The computer that has the deployment manager.

  Uninstalling from the deployment manager removes the availability of the Security Identity Manager Server to the cluster. The deployed Security Identity Manager application files are automatically removed from Security Identity Manager cluster members.

Reboot the Windows operating system after uninstallation to clean up any residual Security Identity Manager files that were not removed during the uninstallation process.

What is not removed

Uninstalling the Security Identity Manager Server does not modify existing database tables or the directory server schema and data. The Security Identity Manager log files are not removed.

For more information about manually removing the database tables, directory server schema, and log files, see "Manually removing components".

Uninstalling the server

You can uninstall Security Identity Manager from UNIX, Linux, or Windows operating systems by using the Security Identity Manager uninstallation program. On Windows operating systems you, can also use the Add/Remove Programs from the Windows Control Panel.

Before you begin

Before you uninstall the Security Identity Manager Server, complete these tasks:

- Single-server configuration:
  - Back up any certificates in the *ISIM_HOME*\cert directory and the itimKeystore.jceks keystore file in the *ISIM_HOME*\config\keystore directory.
  - Ensure that the WebSphere Application Server is running.

- Cluster configuration:
  - Back up any certificates in the *ISIM_HOME*\cert directory and the itimKeystore.jceks keystore file in the *ISIM_HOME*\config\keystore directory.
  - Ensure that the node agents are running and that the deployment manager is also running.

About this task

If you are planning to reinstall Security Identity Manager, use the Security Identity Manager uninstallation program.

- Single-server configuration:

  Run the command on computer on which the Security Identity Manager Server is installed.
- Cluster configuration:

  Run the command on each cluster member first, and then run the command on the computer on which the deployment manager is installed.

Procedure

1. Uninstall the Security Identity Manager by entering this command: *ISIM_HOME*\itimUninstallerData\Uninstall_ITIM
2. Complete the uninstallation wizard panels and confirm that you want to uninstall the Security Identity Manager Server
3. Reboot the Windows system after uninstallation to clean up any residual Security Identity Manager files that were not able to be removed during uninstallation.

What to do next

- Verify that the Security Identity Manager Server is removed.
- Manually remove other components.

Uninstalling the server from Windows Server 2012

You can uninstall Security Identity Manager from the Windows 2012 operating systems by using the Security Identity Manager uninstallation program. On Windows operating systems, you can also use the Add/Remove Programs from the Windows Control Panel.

Before you begin

Before you uninstall the Security Identity Manager Server, complete these tasks:

- Single-server configuration:
  - Back up any certificates in the *ISIM_HOME*\cert directory and the itimKeystore.jceks keystore file in the *ISIM_HOME*\config\keystore directory.
  - Ensure that the WebSphere Application Server is running.
- Cluster configuration:
  - Back up any certificates in the *ISIM_HOME*\cert directory and the itimKeystore.jceks keystore file in the *ISIM_HOME*\config\keystore directory.
  - Ensure that the node agents are running and that the deployment manager is also running.

About this task

If you are planning to reinstall Security Identity Manager, use the Security Identity Manager uninstallation program.

- Single-server configuration:

  Run the command on computer on which the Security Identity Manager Server is installed.
- Cluster configuration:

  Run the command on each cluster member first, and then run the command on the computer on which the deployment manager is installed.

Procedure

1. Navigate to *ISIM_HOME*\itimUninstallerData\Uninstall_ITIM.
2. Right click **Uninstall_ITIM** and select **Properties**.
3. Click **Advanced**.
4. Click **Compatibility**.
5. Select the check box for **Run this program in compatibility mode for:** Select **Windows 7** as the operating system.
6. Under **Privilege level**, select the check box for **Run this program as an administrator**.
7. Click **OK**.
8. Complete the uninstallation wizard panels and confirm that you want to uninstall the Security Identity Manager Server.
9. Restart the Windows system after uninstallation to clean up any residual Security Identity Manager files that were not able to be removed during uninstallation.

Verifying that the Security Identity Manager Server is uninstalled

Before removing components, you need to verify that the Security Identity Manager was removed.

Before you begin

Ensure that you finish running the uninstallation utility.

Procedure

1. Examine the *ISIM_HOME* directory and remove any residual Security Identity Manager directories, configuration files, and log files.
2. Start the WebSphere administrative console and log in.
3. From the navigation tree, find the target node, and click the **Applications > Enterprise Applications** link.

   A list is displayed of the enterprise applications that are installed on the application server.

   If you see an application named ITIM listed, the uninstallation process was unable to automatically remove the Security Identity Manager Server from the WebSphere Application Server. You can remove the application manually. For more information, see "Manually removing the Security Identity Manager Server from WebSphere Application Server".

What to do next

Manually remove other components.

Manual removal of components

After running the uninstall utility, you need to manually stop or remove additional components.

Manually removing the Security Identity Manager Server from the WebSphere Application Server

If the uninstall utility did not remove the Security Identity Manager Server, you must remove it manually.

Before you begin

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

Procedure

1. To uninstall the Security Identity Manager Server in a single-server or a cluster configuration, select **Applications > Enterprise Applications**.
2. Select the **ITIM** application.
3. Click **Stop**.
4. When the Tivoli Identity Manager application stops, select the **ITIM** application again.
5. Click **Uninstall**.
6. Manually ensure that the ITIM.ear directory is removed.
   a. Open the applications directory:
      - Single-server and each cluster member
        WAS_PROFILE_HOME\config\cells*cellname*\applications

        Note:
        1) If the `.ear` file is already removed, cluster members do not have the application directory.
        2) The `.ear` file also must be removed from the *WAS_PROFILE_HOME*\config\cells*cellname*\installedApps\ITIM.ear directory.
      - Deployment manager
        WAS_NDM_PROFILE_HOME\config\cells*cellname*\applications
   b. If the ITIM.ear directory exists, remove the directory.

What to do next

Remove other components.

Stopping and removing the Security Identity Manager messaging engine

To completely uninstall Security Identity Manager, you must uninstall the messaging engine as well.

Before you begin

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

Procedure

1. To stop and remove the Security Identity Manager Server messaging engine in a single-server or a cluster configuration, select **Service Integration > Buses**.
2. Click **itim_bus**.
3. In the Topology section, click **Messaging engines**.

   For a single-server installation, you see an engine named *nodename.servername*-itim_bus.

   For a cluster installation, you see n+1 messaging engines, where n is the number of Security Identity Manager cluster members. An additional messaging engine is used for the Security Identity Manager messaging cluster.
4. Select one or more messaging engines and click **Stop**.
5. Remove the itim_bus configuration from the WebSphere administrative console.
6. In the Security Identity Manager database, drop the tables and schema used by the messaging engines. See the documentation for your database system for the appropriate commands.

Example

The file *ISIM_HOME*/config/rdbms/dbtype/drop_itim_sib.ddl provides an example.

What to do next

Remove additional components.

Removal of other Security Identity Manager configuration settings from the WebSphere Application Server

You must manually remove other Security Identity Manager configuration settings from the WebSphere Application Server to complete the uninstallation.

Complete the following tasks on the WebSphere administrative console.

Removal of the components of the Identity Service Center

If you installed the Identity Service Center in your system, you must manually remove some optional components that were installed with the fix pack installer.

These components are:

- WebSphere Composite Unit
- WebSphere Enterprise Business Asset
- WebSphere Business Level Application

You must perform the removal procedures in the following order:

1. Uninstall IBM Security Identity Manager.
2. Remove all additional components that are described in "Manual removal of components" on page 186.
3. Manually remove these components of the Identity Service Center:
   a. WebSphere Composite Unit
   b. WebSphere Enterprise Business Asset

c. WebSphere Business Level Application

When you remove the components of the Identity Service Center, you must also follow the sequence of this component list to prevent errors.

Manually removing the WebSphere Composite Unit (CU):

If you installed the Identity Service Center in your system, you must first manually remove the WebSphere Composite Unit after you uninstall IBM Security Identity Manager.

Before you begin

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

Procedure

1. From the WebSphere Application Server administrative console, select **Applications** > **Application Types** > **Business-level Applications**.
2. Select the **IdentityServiceCenterApplication** application.
3. Click **Stop**.
4. When the Identity Service Center stops, click the application name. A window opens to display the information about the asset. It includes details about the Composite Unit, **com.ibm.isim_CU.eba**.
5. Select **com.ibm.isim_CU.eba**.
6. Click **Delete**. A window opens to confirm the deletion of the Composite Unit from the Business-level application: **WebSphere:cuname=com.ibm.isim_CU.eba**.
7. Click **OK**.
8. Click **Save**.

Manually removing the WebSphere Enterprise Business Asset:

After uninstalling IBM Security Identity Manager, you must also manually remove the WebSphere Enterprise Business Asset if you installed the Identity Service Center in your system.

Before you begin

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

Procedure

1. From the WebSphere Application Server administrative console, select **Applications** > **Application Types** > **Assets**.
2. Select the **com.ibm.isim_6.0.0.v<version>.eba** asset.
3. Click **Delete**. A window opens to confirm the deletion of the asset.
4. Confirm the name **WebSphere:assetname=com.ibm.isim_6.0.0.v<version>.eba**.
5. Click **OK**.
6. Click **Save**.

Manually removing the WebSphere Business Level Application:

After uninstalling IBM Security Identity Manager, you must manually remove the WebSphere Business Level Application if you installed the Identity Service Center in your system.

Before you begin

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

Procedure

1. From the WebSphere Application Server administrative console, select **Applications** > **Application Types** > **Business-level Applications**.
2. Select the **IdentityServiceCenterApplication** application.
3. Click **Delete**. A window opens to confirm the deletion of the Business Level Asset: **WebSphere:blaname=IdentityServiceCenterApplication**.
4. Click **OK**.
5. Click **Save**.

Removing the JDBC providers and data sources

You must manually remove JDBC provider configuration settings from the WebSphere Application Server to complete the uninstallation.

Before you begin

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

Procedure

1. From the WebSphere administrative console, click **Resources** > **JDBC** > **JDBC Providers**.
2. Choose **All scopes** as the scope level.
3. Select the JDBC provider names that start with "ITIM XA" or "ITIM non-XA".
4. Click **Delete**. The JDBC providers and the associated data sources are both removed.
5. Click **Save** to save the configuration.

What to do next

Remove additional Security Identity Manager configuration settings from the WebSphere Application Server.

Removal of the JMS queue connection factories, queues, and activation specifications

You must manually remove the JMS configuration settings from the WebSphere Application Server to complete the uninstallation.

Use the WebSphere administrative console to complete the removal tasks.

Removing the JMS queue connection factories:

You must manually remove the JMS queue connection factory configuration settings from the WebSphere Application Server to complete the uninstallation.

Before you begin

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

Procedure

1. Click **Resources** > **JMS** > **Queue connection factories**.
2. Choose **All scopes** as the scope level.
3. Select **ITIM Queue Connection Factory** and **ITIM Shared Queue Connection Factory**.
4. Click **Delete**.
5. Click **Save** to save the configuration.

What to do next

Remove the JMS configuration settings for

- Queues
- Activation specification

Removing the JMS queue:

You must manually remove the JMS queue configuration settings from the WebSphere Application Server to complete the uninstallation.

Before you begin

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

Procedure

1. Click **Resources** > **JMS** > **Queues** .
2. Choose **All scopes** as the scope level.
3. Select all the queue names that start with "itim".
4. Click **Delete**.
5. Click **Save** to save the configuration.

What to do next

Remove the JMS configuration settings for:

- Queue connection factory
- Activation specification

Removing the JMS activation specifications:

You must manually remove the JMS activation specification configuration settings from the WebSphere Application Server to complete the uninstallation.

Before you begin

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

Procedure

1. Click **Resources** > **JMS** > **Activation specifications**.
2. Choose **All scopes** as the scope level.

3. Select all the specification names that start with "itim".
4. Click **Delete**.
5. Click **Save** to save the configuration.

What to do next

Remove the JMS configuration settings for:

- Queue connection factory
- Queues

Removing object cache instances

You must manually remove the object cache instances from WebSphere Application Server to complete the uninstallation.

Before you begin

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

Procedure

1. Click **Resources** > **Cache instances** > **Object cache instance**.
2. Choose **All scopes** as the scope level.
3. Select **LdapCache** and **SecondaryLdapCache**.
4. Click **Delete**.
5. Click **Save** to save the configuration.

What to do next

Remove additional Security Identity Manager configuration settings from WebSphere Application Server.

Removing security settings

You must manually remove the security settings from the WebSphere Application Server to complete the uninstallation.

Before you begin

Log on to the WebSphere administrative console.

Procedure

1. Click **Global Security** > **Java Authentication and Authorizations** > **J2C authentication data**.
2. Select **itim_init** and **itim_jms**.
3. Click **Delete**.
4. Click **Save** to save the configuration.
5. Click **Global Security** > **Java Authentication and Authorizations** > **Application logins**.
6. Select **ITIM** and **serviceLoginContext**.
7. Click **Delete**.
8. Click **Save** to save the configuration.

What to do next

Remove additional IBM Security Identity Manager configuration settings from the WebSphere Application Server.

Removing core group policies (cluster environments only)

This task applies to a cluster environment only. You must manually remove the core group policies from the WebSphere Application Server to complete the uninstallation.

Before you begin

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

Procedure

1. Click **Servers** > **Core group settings**.
2. Click **DefaultCoreGroup**.
3. Click **Policies**.
4. Select all the policy names that start with "itim_bus".
5. Click **Delete**.
6. Click **Save** to save the configuration.

What to do next

Remove additional Security Identity Manager configuration settings from the WebSphere Application Server.

Removing shared libraries

You must manually remove the shared libraries from WebSphere Application Server to complete the uninstallation.

Before you begin

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

Procedure

1. Click **Environment** > **Shared Libraries**.
2. Choose **All scopes** as the scope level.
3. Select **ITIM_LIB**.
4. Click **Delete**.
5. Click **Save** to save the configuration.

What to do next

Remove additional Security Identity Manager configuration settings from WebSphere Application Server.

Removing the JVM class path

You must manually remove the JVM class path from WebSphere Application Server to complete the uninstallation.

Before you begin

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

Procedure

1. Click **Servers** > **WebSphere Application Server** > *servername* > **Java and Process Management** > **Process definition** > **Java Virtual Machine**.
2. Remove {*ISIM_HOME*}**/data** from the class path field.
3. Click **Save** to save the configuration.

What to do next

Remove additional IBM Security Identity Manager configuration settings from WebSphere Application Server.

Removing WebSphere variables

You must manually remove the WebSphere variables from WebSphere Application Server to complete the uninstallation.

Before you begin

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

Procedure

1. Click **Environment** > **Shared Libraries**.
2. Choose **All scopes** as the scope level.
3. Select all variables with the name of "*ISIM_HOME*" and "ITIM_DB_JDBC_DRIVER_PATH".
4. Click **Delete**.
5. Click **Save** to save the configuration.

What to do next

Remove additional Security Identity Manager configuration settings from WebSphere Application Server.

Manually removing other files or directories

You must manually remove any residual Security Identity Manager files to complete the uninstallation.

Before you begin

Ensure that you ran the uninstallation utility and removed all components.

Procedure

1. Restart the operating system after uninstallation.
2. Examine the *ISIM_HOME* directory.
3. Remove any residual files:
   - Security Identity Manager directories
   - Configuration files
   - Log files
   - .dll files

- .so files
- .a files
- .jar files

4. Restart the operating system.

What to do next

Reinstall Security Identity Manager.

Chapter 12. Security Identity Manager reinstallation

You might want to clean up the database and the LDAP server before running the Security Identity Manager installation program again, for a cleaner installation. Ensure that the Security Identity Manager messaging engine is not running. Restart the Windows system after uninstallation and before attempting to reinstall.

Ensuring that IBM Security Identity Manager objects are removed from the Oracle Directory Server Enterprise Edition

Before you reinstall IBM Security Identity Manager, ensure that any previous IBM Security Identity Manager schema objects, object classes, and other attributes are removed from the Oracle Directory Server Enterprise Edition.

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.

Procedure

1. Start the Oracle Directory Server Enterprise Edition administrative console.
2. On the Configuration tab, remove the IBM Security Identity Manager suffix.
3. On the Directory tab, complete these steps:
   a. Remove the IBM Security Identity Manager domain.
   b. Click **Config** > **Plugins**. Then, open the properties for the referential integrity postoperation entry and delete all attributes that begin with the characters `er`.
4. Stop the directory server.
5. Open the *ldapServerInstance*`\config\schema\99user.ldif` file. Then, remove all IBM Security Identity Manager object classes and attribute types that begin with the characters `er`.
6. Start the directory server.

What to do next

Next you can install IBM Security Identity Manager.

Part 2. Optional configuration

You can complete optional configuration tasks as needed for your deployment.

- Language pack installation
- "Change of the language display of the browser" on page 200
- "Adapter and profile installation" on page 201
- "Change of cluster configurations after IBM Security Identity Manager is installed" on page 204
- "Downloading and installing the product documentation site files" on page 206
- "Installing the Incremental Data Synchronizer" on page 207
- Chapter 14, "Reconfiguration for authentication with an external user registry," on page 217

Chapter 13. Optional post-installation tasks

After installing Security Identity Manager, you can optionally install language packs, adapter profiles, or change cluster configurations.

Installing a language pack

After installing Security Identity Manager, you can install a language pack that provides support for languages other than English.

Before you begin

Ensure that you verified that Security Identity Manager Server and related processes are running.

Before you run the Security Identity Manager language pack setup program, ensure that the version of the Java Runtime Environment that Security Identity Manager requires is accessible from the command line.

For example, you can use the version of Java that comes with WebSphere Application Server. Enter this command:

```
WAS_HOME\java\bin\java -fullversion
```

You receive a response like the following example:

```
java full version "1.5.0 IBM Windows 32 build pwi32devifx-20061107
(iFix 111765 SR3 + 111700)"
```

Procedure

1. Download the language pack installer JAR file.
2. Use command-line mode to install the language pack by using the itimlp_setup.jar file. For example, enter this language pack command at a command prompt:

   ```
   WAS_HOME\java\bin\java –jar itimlp_setup.jar
   ```

   Note: For Linux, ensure that you use the version of Java installed with WebSphere Application Server, in *WAS_HOME*/java/bin, to install the language pack.
   The Security Identity Manager language pack setup program starts.
3. To complete the language pack installation, follow the instructions that are displayed in the setup program windows.
4. Restart the WebSphere Application Server to activate these changes.
   a. Stop the WebSphere Application Server:
      - On the Windows operating systems, run the following command:
        – *WAS_HOME*\bin\stopServer.bat *server_name*
      - On the UNIX or Linux operating systems, run the following command:
        – *WAS_HOME*E/bin/stopServer.sh *server_name*

        The value of *server_name* is the name of the WebSphere Application Server. For example, server1.

   b. Start the WebSphere Application Server:
      - On the Windows operating systems, run the following command:

– *WAS_HOME*\bin\startServer.bat *server_name*

- On the UNIX or Linux operating systems, run the following command:
  – *WAS_HOME*/bin/startServer.sh *server_name*

  The value of *server_name* is the name of the WebSphere Application Server. For example, server1.

What to do next

Change the language of the browser.

Note: To uninstall the language pack from the system, change to the *ISIM_HOME*\timlp directory, and then enter this language pack command at a command prompt:

```
java –jar timlp_uninstall.jar
```

Change of the language display of the browser

After the language pack is successfully installed, you can change the language displayed in the Security Identity Manager interface. You change the interface language by changing the language preference for your browser.

Changing the language display of Internet Explorer

You can change the language displayed in the Security Identity Manager interface by changing the language preference for Internet Explorer version 7.0.

Before you begin

Ensure that the correct language pack is installed. Make language preference changes before logging in to Security Identity Manager.

Procedure

1. Select **Tools** > **Internet Options**.
2. On the General tab, click **Languages**.
3. Click **Add**.
   a. Select the languages to add.
   b. Click **OK**.
4. Select a language and set the language priority. Use the buttons to move the priority up or down.
5. Click **OK**.
6. Click **OK** again to save your changes.

What to do next

Perform other post-installation tasks.

Configure Security Identity Manager.

Changing the language display of Mozilla Firefox

You can change the language displayed in the Security Identity Manager interface by changing the language preference for Mozilla Firefox.

Before you begin

Ensure that the correct language pack is installed. Make language preference changes before logging in to Security Identity Manager.

Procedure

1. Select **Tools** > **Options**.
2. On the Content tab, under the Languages section click **Choose**.
3. From the Select a language to add menu, select a language. Click **Add**.
4. Set the language preference. Use the buttons to move the preference up or down.
5. Click **OK**.

What to do next

Perform other post-installation tasks.

Adapter and profile installation

Installing an adapter involves two steps: importing the adapter profile (or service type) and running the adapter installer.

You can use IBM Security Identity Manager adapters to connect IBM Security Identity Manager to a set of heterogeneous resources. These resources can be operating systems, data stores, or other applications for provisioning identities.

An adapter is a program that provides an interface between a managed resource and the Security Identity Manager Server. Adapters function as trusted virtual administrators on the target platform for account management. For example, adapters create accounts, suspend accounts, and modify account attributes.

An Security Identity Manager adapter can be either agent-based or agentless:

Agent-based adapters
: Consists of the agent adapter code installed on the managed resource and the profile installed on the Security Identity Manager Server side.

Agentless adapters
: Consists of the agentless adapter code installed on the system that hosts the IBM Tivoli Directory Integrator and the profile that is installed on Security Identity Manager. The adapter code is separate from the managed resource with which it is designed to communicate.

  Note: For agentless adapters, the SSH process or daemon must be active on the managed resource.

The IBM Security Identity ManagerSecurity Identity Manager installation program always installs the following agentless adapter service types:

- AIX profile (UNIX adapter)
- Solaris profile (UNIX adapter)
- HP-UX profile (UNIX adapter)
- Linux profile (Linux adapter)
- LDAP profiles (LDAP adapter)

The IBM Security Identity Manager installation program optionally installs the adapters for the listed service types. You must take additional steps to install the adapter if you chose not to install the adapters during the Security Identity Manager installation or if the adapter is not installed as a service type with Security Identity Manager.

Note: Download and install the latest adapter and its profile even if it is installed by the Security Identity Manager installation program.

Adapters are available at this location:

- On the IBM Passport Advantage website:
  http://www.ibm.com/software/sw-lotus/services/cwepassport.nsf/wdocs/passporthome

An adapter is packaged as a compressed file that contains these common elements:

- Service definition file, or adapter profile, which is an archiveJava (JAR) file that contains the profile, such as `WinLocalProfile.jar`.
- An executable installation program to install the adapter.
- Documentation in Portable Document Format (PDF) that includes release notes and an installation and configuration guide.

Installing an adapter

You must start the adapter installer.

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.

Procedure

1. Open the compressed adapter file.
2. Open the pdf file that contains the installation and configuration guide.
3. Install and configure the adapter, following the steps that the installation and configuration guide provides.

Installing adapter profiles

You can install and import any adapter profiles that you did not install during the Security Identity Manager installation process.

Before you begin

Ensure that you verified that Security Identity Manager Server and related processes are running.

About this task

Note: If you upgraded from Tivoli Identity Manager version 5.0 and are using a service instance that was created with a Tivoli Identity Manager 5.0 profile, you must upgrade to the 6.0 adapter before you create groups on the service. The adapters for Tivoli Identity Manager 5.0 do not support group management.

For more information about the role of adapters, see *Security Identity Manager adapters*.

To install and import adapter profiles:

Procedure

1. Open and extract the compressed adapter file.
2. Place the JAR file that contains the adapter profile in a temporary directory on the computer that is running Security Identity Manager.
3. As administrator, open the Tivoli Identity Manager user interface.
4. Click **Configure System** > **Manage Service Types**.
5. On the Manage Service Types window, click **Import**.
6. On the **Service Definition File** field, click **Browse**.
7. Locate and select the JAR file that contains the adapter profile. Then click **Open**.
8. Click **OK**.
9. On the Success page, click **Close**.

What to do next

Perform other post-installation tasks.

Installing the adapter language pack

With the adapters language pack, all languages are automatically made available to the adapters. You do not need to install a separate language pack to get the specific language.

Before you begin

Download the Security Identity Manager Language Pack v6.*x* for Adapters from IBM Passport Advantage® at `http://www.ibm.com/software/howtobuy/passportadvantage/pao_customers.htm`

Verify that the Security Identity Manager server and related processes are running.

About this task

This task is for Administrators only.

When you import the adapters language pack, any previously installed language pack is overlaid.

Procedure

1. Log in to the IBM Security Identity Manager console.
2. Click **Configure System** > **Manage Service Types**.
3. On the Manage Service Types window, click **Import**.
4. On the **Service Definition File** field, click **Browse**.
5. Search for the `timx_agents.jar` file and click **Open**. This file contains the translated labels for all adapters in all the supported languages.
6. Click **OK**.
7. On the Success page, click **Close**.

Change of cluster configurations after IBM Security Identity Manager is installed

This information describes how to expand or reduce the members in a cluster for performance reasons after IBM Security Identity Manager is installed.

Expanding a cluster horizontally

You can add a member to an existing cluster.

Before you begin

Ensure that Security Identity Manager was installed in a clustered configuration.

See also *Setting up the full profile* from the WebSphere Application Server section of the IBM Knowledge Center: **Network Deployment (Distributed operating systems), Version 8.5** > **Setting up the application serving environment**.

Procedure

1. Create a profile on a new computer and federate the new node into the cell.
   - Create a custom profile on the new computer and federate the profile into the deployment manager cell.
   - Create a base profile on the new computer and then run the **addNode** command to federate the new node into the cell. For more information, see "Manually federating a WebSphere Application Server node member" on page 65.
2. Create an Security Identity Manager cluster member on the new node. Repeat this procedure to create cluster members on both the application cluster and the messaging engine cluster. On the WebSphere administrative console, complete these steps:
   a. Click **Servers** > **Cluster**.
   b. On the next window, click the Security Identity Manager cluster name.
   c. Click **Cluster Members**, then click **New**.
   d. Select the node name that is the node that you added to the cell. Enter the node name. Then, click **Next**.
   e. Verify the summary window, then click **Finish**.
   f. Save the changes.
3. Run the Security Identity Manager installation program on the new computer, choosing cluster member installation.
4. Set the policy for the association of the messaging engine and the cluster member. Run the following command on the deployment manager node:
   - On the Windows operating systems, type:
     ```
     ISIM_HOME\bin\runConfig.exe install
     ```
   - On the UNIX or Linux operating systems, type:
     ```
     ISIM_HOME/bin/runConfig install
     ```
5. Start the new cluster member.
   a. Click **Servers** > **Cluster**.
   b. Select the cluster.
   c. Click **Cluster Members**.
   d. Select the new member and click **Start**.

What to do next

Perform other post-installation tasks.

Expanding a cluster vertically

You can add a server to an existing node anywhere in an existing cluster.

Before you begin

Ensure that Security Identity Manager is installed in a clustered configuration.

About this task

You might want to expand an existing cluster vertically if the physical computer that runs WebSphere Application Server has processor or memory capacity that is not fully used.

Procedure

1. Ensure that the cluster is running.
2. Use the WebSphere console to add a server to the cluster that is defined for the existing Security Identity Manager application. On the WebSphere Administration Console, complete these steps:
   a. Click **Servers > Clusters > WebSphere application server clusters**.
   b. Click the name of the cluster to which you want to add more servers. The cluster can be an application cluster or a messaging cluster.

      For example, `ITIM Application Cluster` or `ITIM Messaging Cluster`.
   c. On the Configuration tab, in the Additional Properties section, click **Cluster members**.
   d. On the Cluster Members page, click **New**.
   e. Define a new server by providing the necessary information:
      1) Enter a name in the **Member name** field.
      2) Select the node on which the server runs.
      3) Provide a value for the **Weight** field.
      4) Ensure the **Generate unique HTTP ports** check box is selected.
      5) Click **Add Member**.

      You can define more servers by repeating these steps with different names and nodes as needed.
   f. Verify that the new member is listed in the table at the bottom of the page. Click **Next**.
   g. Verify the summary information and click **Finish**. Verify that the new member is listed in the table of cluster members.
   h. Save the WebSphere configuration.

   After all WebSphere changes are made, continue with the next step.
3. Run the following command on the deployment manager node:

   Note: You do not have to restart Security Identity Manager.
   - On the Windows operating systems, type:

     `ISIM_HOME\bin\runConfig.exe install`
   - On the UNIX or Linux operating systems, type:

     `ISIM_HOME/bin/runConfig install`

4. From the WebSphere console, you can now start the servers in the cluster. The servers can be used immediately.

Reducing a cluster

You can remove a cluster member from an existing cluster.

Before you begin

Ensure that Security Identity Manager was installed in a clustered configuration.

Procedure

1. Run the Security Identity Manager uninstallation program on the computer that has the cluster member that you intend to remove. For more information, see Chapter 11, "Uninstallation of Security Identity Manager," on page 183.
2. On the WebSphere administrative console, delete the cluster members from both Security Identity Manager clusters.

What to do next

Perform other post-installation tasks.

Configure Security Identity Manager.

Downloading and installing the product documentation site files

You can download the IBM Security Identity Manager product documentation site files and also install them locally to the IBM Security Identity Manager server.

Before you begin

To view the IBM Security Identity Manager on the web, access this site:

http://www.ibm.com/support/knowledgecenter/SSRMWJ_6.0.0.4/com.ibm.isim.doc_6.0.0.4/kc-homepage.htm

Procedure

1. Print these instructions.
2. Close this instance of the product documentation site.
3. Access the following website:

   http://www.ibm.com/support/knowledgecenter/SSRMWJ_6.0.0.4/com.ibm.isim.doc_6.0.0.4/kc-homepage.htm
4. Download the `com.ibm.isim.doc_6.0.zip` file, which contains the IBM Security Identity Manager product documentation site.
5. Extract the `com.ibm.isim.doc_6.0.zip` file into this directory:

   `WAS_HOME\profiles\`*`profilename`*`\installedApps\`*`cellname`*`\ITIM.ear\itim_iehs_help.war\WEB-INF\lib\eclipse\plugins`
6. Ensure that the `plugins` directory now contains this additional directory:

   `com.ibm.isim.doc_6.0`
7. Restart the WebSphere Application Server.
8. To open the product documentation site, complete these steps:
   a. Restart the IBM Security Identity Manager server.
   b. Log in as the system administrator: *isim manager*.

c. In the browser **Address** field, type the following address on one line:

   `http://hostname:9080/itim/concepthelp/topic/com.ibm.itim.doc_6.0/ic-homepage.htm`

   The value of *hostname* is the host name of the computer on which theIBM Security Identity Manager server runs.

9. After the IBM Security Identity Manager product documentation site opens, use the browser **Tools** menu to bookmark the address for future use.

What to do next

To restart only the product documentation site, complete these steps:

1. On the WebSphere Application Server, click **Applications** > **Enterprise Applications**.
2. Stop and start the product documentation site application.
3. Refresh the browser session for the IBM Security Identity Manager product documentation site.

Installing the Incremental Data Synchronizer

The Incremental Data Synchronizer is a separately installed utility that provides fast synchronization of data and access control item between the directory server that IBM Security Identity Manager uses and the IBM Security Identity Manager database.

The Incremental Data Synchronizer can be installed on the same computer that has the IBM Security Identity Manager Server, or on a separate computer. For performance reasons, it is a good practice that you install the Incremental Data Synchronizer on a separate computer.

Installing the Incremental Data Synchronizer on a separate system

You can install and configure the Incremental Data Synchronizer on a separate computer other than the computer on which the IBM Security Identity Manager Server is installed.

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.

If you install a new version of IBM Security Identity Manager, you must complete the procedures in this section to ensure that the files on both systems are compatible. In this case, edit the properties files after they are copied and ensure that the correct values are set.

If you upgrade WebSphere Application Server on the system where IBM Security Identity Manager is installed, you must copy the new `JAR` files to the system on which the Incremental Data Synchronizer is installed. Or, you must install the new WebSphere Application Server thin client files on the system on which the Incremental Data Synchronizer is installed.

If you upgrade DB2 on the system where the IBM Security Identity Manager is installed, install the new DB2 client on the system on which the Incremental Data Synchronizer is installed.

About this task

The value *synchronizer_computer* is the computer on which the Incremental Data Synchronizer is installed.

itim_computer is the computer on which IBM Security Identity Manager is installed. This value is provided during the Security Identity Manager installation. This name can be found in the directory path in the WebSphere Application Server installation directory where the `itim.ear` file exists.

Procedure

1. Copy the *ISIM_HOME* directory from the *itim_computer* to the *synchronizer_computer*.
2. Install Application Client for WebSphere Application Server on the *synchronizer_computer* in the *WAS_CLIENT_HOME* directory.
3. Use the appropriate client installer for the operating system of *synchronizer_computer*. Application Client provides a client runtime that enables the Incremental Data Synchronizer to communicate with WebSphere Application Server. The Incremental Data Synchronizer needs only Java EE and thin clients, so select only that option during installation of the Application Client.
4. Copy the `app_ejb.jar`, `api_ejb.jar`, and `wf_ejb.jar` files from the *WAS_HOME*`/profiles/`*profile_name*`/installedApps/`*cell_name*`/itim.ear` directory on the *itim_computer* to the *ISIM_HOME*`/lib` directory on the *synchronizer_computer*.
5. Copy the `jaas_login_was.conf` file from the *ISIM_HOME*`/extensions/examples/apps/bin` directory on the *itim_computer* to the *ISIM_HOME*`/data` directory on the *synchronizer_computer*.
6. Create a directory named `logs` in the *ISIM_HOME* directory on the *synchronizer_computer*. Trace log files, such as `trace.log` and `trace1.log`, are generated in this directory.
7. Modify the *ISIM_HOME*`/data/enroleLogging.properties` file on *synchronizer_computer*:
   a. Set the `handler.file.fileDir` property to point to the *ISIM_HOME*`/logs` directory.
   b. Set the `handler.file.security.fileDir` property to point to the *ISIM_HOME*`/logs` directory.
8. Ensure that the *changelog* feature is enabled in the directory server instance. For example:
   - For IBM Security Directory Server, use the instance configuration tool (`LDAP/sbin/idsxcfg`) to configure *changelog* for a directory instance.
   - For the directory administration console in Sun Directory Server Enterprise Edition, open a directory server instance and enable **retro changelog plug-in** under the **plug-ins** section. It enables the *changelog* feature for a Sun Directory Server Enterprise Edition directory server.

     To enable the *changelog* feature with a command, enter:

     ```
     dsconf set-server-prop -h host -p port retro-cl-enabled:on
     ```
9. Enable the *changelog* processing on the *itim_computer*.

a. Open the adhocreporting.properties file in the *ISIM_HOME*/data directory.
b. Set the following options:
   - changelogEnabled=true
   - changelogBaseDN=*changelog_base_dn*

   The *changelog_base_dn* is the base DN that holds the *changelog* entries in the directory server. For example:

   changelogBaseDN=cn=changelog

10. Optional: To enable schema enforcement in the *ISIM_HOME*/data/adhocreporting.properties file on the *itim_computer*, enter:

    enableDeltaSchemaEnforcer=true

11. Optional: Modify the *ISIM_HOME*/data/adhocreporting.properties file to enable *changelog* pruning. Set the following property if you want to prune already processed *changelog* entries. This property is specific to the Sun Directory Server Enterprise Edition directory server. For example:

    enableChangelogPruning=true

12. Modify the *ISIM_HOME*/data/enrole.properties file on *synchronizer_computer* to point to the WebSphere Application Server bootstrap port on the *itim_computer*.

    Set enrole.appServer.url=iiop://*itim_computer*:2809

13. Optional: Tune the Incremental Data Synchronizer by modifying the *ISIM_HOME*/data/enRole.properties file on the *synchronizer_computer*. You might also consider altering the same values for the *itim_computer*. For more information about these properties, see *IBM Security Identity Manager Performance and Tuning Guide*:
    - enroleconnectionpool.initialpoolsize
    - enroleconnectionpool.maxpoolsize
    - enroleconnectionpool.prefsize
    - enroleconnectionpool.incrementcount

14. If the database is DB2 and it is on the *itim_computer*, copy the db2jcc.jar and db2jcc_license_cu.zip files from the *itim_computer* to the *ISIM_HOME*/lib directory on *synchronizer_computer*.

    Note: By default, these two files might already be present in the *ISIM_HOME*/lib directory on the *synchronizer_computer*. These files can be copied from the *itim_computer*.

15. Optional: If the database used is Oracle and it is not on *synchronizer_computer*, install an Oracle client on *synchronizer_computer* to connect to the Oracle database used by *itim_computer*.
16. Ensure that the ojdbc14.jar file is in the *ISIM_HOME*/lib directory of the *synchronizer_computer*.
17. Modify the enRoleDatabase.properties file and the enRoleLDAPConnection.properties file in the *ISIM_HOME*/data directory on the *synchronizer_computer* to include the Security Identity Manager database and directory server details. These files can be copied from the *itim_computer*.
18. Copy the sas.client.props file from the *WAS_CLIENT_HOME*/properties directory on the *synchronizer_computer* to the *ISIM_HOME*/data directory on the *synchronizer_computer*. The sas.client.props file is the CSIv2 properties file and is required by the Incremental Data Synchronizer to securely authenticate against Security Identity Manager.

19. If SSL is not supported or not used in Security Identity Manager, ensure that the com.ibm.CSI.performTransportAssocSSLTLSSupported property in the *ISIM_HOME*/data/sas.client.props file on the *synchronizer_computer* is set to false.
20. Set *ISIM_HOME* and *WAS_HOME* script variables to point to *ISIM_HOME* and *WAS_CLIENT_HOME* directories, as follows:
    a. Edit the following two script files in the *ISIM_HOME*/bin/[*win*|*unix*] directory on *synchronizer_computer*. The location of these files depends on your operating system.

       Microsoft Windows operating systems
       - startIncrementalSynchronizerCMD_WAS.bat
       - startIncrementalSynchronizerUI_WAS.bat

       UNIX operating systems
       - startIncrementalSynchronizerCMD_WAS.sh
       - startIncrementalSynchronizerUI_WAS.sh

    b. Use the user interface script to run incremental synchronization through a simple Java Swing user interface.
    c. If administrative security is disabled in WebSphere Application Server, uncomment and use the appropriate Java command that is described in the script.

Installing the Incremental Data Synchronizer on the same system

You can install and configure the Incremental Data Synchronizer on the same computer on which the IBM Security Identity Manager Server is installed.

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.

Procedure

1. Copy the app_ejb.jar, api_ejb.jar, and wf_ejb.jar files from *WAS_HOME*/*profile_name*/installedApps/*cell_name*/ITIM.ear to the *ISIM_HOME*/lib directory.
2. Copy the jaas_login_was.conf file from the *ISIM_HOME*/extensions/*version number*/examples/apps/bin directory to the *ISIM_HOME*/data directory.
3. Ensure that the *changelog* feature is enabled in the directory server instance. For example:
   - For IBM Security Directory Server, use the instance configuration tool (LDAP/sbin/idsxcfg) to configure *changelog* for a directory instance.
   - From the directory administration console in Sun Directory Server Enterprise Edition, open a directory server instance and enable **retro changelog plugin** under the **plug-ins** section. This action enables the *changelog* feature for a Sun One Directory server.

     To use the command to enable the *changelog* feature, enter:

     ```
     dsconf set-server-prop -h host -p port retro-cl-enabled:on
     ```

4. Enable *changelog* processing on the *itim_computer*. Edit the `adhocreporting.properties` file in the *ISIM_HOME*`/data` directory and set the following options:
   - `changelogEnabled=true`
   - `changelogBaseDN=`*changelog_base_dn*

   The *changelog_base_dn* is the base DN that holds the *changelog* entries in the directory server. For example:

   ```
   changelogBaseDN=cn=changelog
   ```
5. Optional: Enable schema enforcement in the *ISIM_HOME*`/data/adhocreporting.properties` file on the *itim_computer* as follows:

   ```
   enableDeltaSchemaEnforcer=true
   ```
6. Optional: Modify the *ISIM_HOME*`/data/adhocreporting.properties` file to enable *changelog* pruning. Set the following property if you want to prune already processed *changelog* entries. This property is specific to the Sun Directory Server Enterprise Edition directory server. For example:

   ```
   enableChangelogPruning=true
   ```
7. Take one of the following actions, depending on which database is used by IBM Security Identity Manager:
   - DB2

     If DB2 is on the `itim_computer`, copy the `db2jcc.jar` and `db2jcc_license_cu.zip` files from the `SQLLIB/java` directory to the `ISIM_HOME/lib` directory. By default, these two files might already be in the `ISIM_HOME/lib` directory.
   - Oracle

     Ensure that the `ojdbc14.jar` file is present in the *ISIM_HOME*`/lib` directory.
   - Microsoft SQL Server

     Ensure that the `sqljdbc.jar` file is present in the *ISIM_HOME*`/lib` directory.
8. Copy the `sas.client.props` file from the *WAS_HOME* `/profiles/`*profile_name*`/properties` directory to the *ISIM_HOME*`/data` directory. *WAS_HOME* is the directory where WebSphere Application Server is installed. The `sas.client.props` file is the CSIv2 properties file and is required by the Incremental Data Synchronizer to securely authenticate against Security Identity Manager.
9. If SSL is not supported in Security Identity Manager, ensure that `com.ibm.CSI.performTransportAssocSSLTLSSupported` property is set to `false` in the *ISIM_HOME*`/data/sas.client.props` file.
10. Update the host name and bootstrap port details in the `ISIM_HOME/data/sas.client.props` file of the node where you want to run the Incremental Data Synchronizer. For example:

    ```
    com.ibm.CORBA.securityServerHost=localhost
    com.ibm.CORBA.securityServerPort=2809
    ```

    Note: Update the `sas.client.props` file only if you configured the cluster setup.
11. Set *ISIM_HOME* and *WAS_HOME* script variables to point to Security Identity Manager Server and WebSphere Application Server installation.
    a. Edit the following two script files in the *ISIM_HOME*`/bin/[`*win*`|`*unix*`]` directory. The location of these files depends on your operating system.

       Microsoft Windows operating systems

       - `startIncrementalSynchronizerCMD_WAS.bat`

- `startIncrementalSynchronizerUI_WAS.bat`

UNIX operating systems

- `startIncrementalSynchronizerCMD_WAS.sh`
- `startIncrementalSynchronizerUI_WAS.sh`

b. Use the user interface script to run incremental synchronization through a simple Java Swing user interface.

c. If administrative security is disabled in WebSphere Application Server, uncomment it and use the appropriate Java command that is described in the script.

Utility for external report data synchronization

The report data synchronization utility is a separately installed utility that synchronizes data and access control items between the directory server and the IBM Security Identity Manager database. The synchronized data is used for running the reports.

You can install, configure, and run the utility either on the same computer as IBM Security Identity Manager or on a different computer. If you install the utility on a different computer, that computer does not require the installation of the WebSphere Application Server, a directory server, or a database.

System requirements

The report data synchronization utility has these system requirements.

Table 19. System requirements for report data synchronization utility

Operating system requirements	Platform	Patch, or maintenance requirements
Microsoft Windows Server 2008 Enterprise Edition	x86-64	Service Pack 1
Microsoft Windows Server 2008 Enterprise Edition	x86-32	Service Pack 1
Microsoft Windows Server 2008 Release 2 Enterprise Edition	x86-64	None
Microsoft Windows Server 2003 Enterprise Edition	x86-32	Service Pack 2
Microsoft Windows Server 2003 Release 2 Enterprise Edition	x86-32	Service Pack 2
SUSE Linux Enterprise Server 11.0	x86-64	Service Pack 1
SUSE Linux Enterprise Server 11.0	x86-32	None
Red Hat Enterprise Linux AS Version 4	x86-32	Update 6
Oracle Solaris 10	SPARC 64-bit	None
AIX Version 6.1	System P 64-bit	Technology level 7, Service Pack 1

Java Runtime Environment (JRE) requirements

The report data synchronization utility requires either the IBM JRE or the WebSphere JRE. The following table describes the relation between JRE requirements and the supported operating systems.

Table 20. JRE requirements for the report data synchronization utility

Operating system	32-bit IBM JRE 1.6.0	JRE of the 32-bit WebSphere 7.0	JRE of the 64-bit WebSphere 7.0
Microsoft Windows Server 2008 Enterprise Edition Service Pack 1 x86-64			✓
Microsoft Windows 2008 Enterprise Edition Service Pack 1 x86-32		✓	
Microsoft Windows Server 2008 Release 2 Enterprise Edition x86-64			✓
Microsoft Windows Server 2003 Service Pack 2 Enterprise Edition x86-32		✓	
Microsoft Windows Server 2003 Release 2 Service Pack 2 Enterprise Edition x86-32		✓	
SUSE Linux Enterprise Server 11.0 Service Pack 1 x86-64	✓		✓
SUSE Linux Enterprise Server 11.0 x86-32	✓	✓	
Red Hat Enterprise Linux AS Version 4 with Update 6, 32-bit		✓	
Oracle Solaris 10 64-bit			✓
AIX Version 6.1 Technology level 7, Service Pack 1, 64-bit	✓		✓

Hardware requirements

The report data synchronization utility has these hardware requirements.

Table 21. Hardware requirements for report data synchronization utility

System components	Minimum values*	Suggested values**
System memory (RAM)	2 gigabytes	4 gigabytes
Processor speed	Single 2.0-gigahertz Intel or pSeries processor	Dual 3.2-gigahertz Intel or pSeries processors
Disk space for utility and log files	50 megabytes	250 megabytes
* Minimum values: These values enable a basic use of IBM Security Identity Manager. ** Suggested values: You might need to use larger values that are appropriate for your production environment.		

Installing the report data synchronization utility

This section describes how to install the utility.

Before you begin

Make sure that your environment meets the system requirements.

About this task

To install the report data synchronization utility, complete these steps:

Procedure

1. Locate the `isim_report_data_sync_utility.zip` file in the *ISIM_HOME*`/bin` directory. *ISIM_HOME* is the directory where IBM Security Identity Manager is installed.
2. If you use the *Advanced Encryption Standard* or the `AES` encryption algorithm, then locate the keystore file in the *ISIM_HOME*`/data/keystore` directory.
3. If you use `AES`, copy the compressed file and the keystore file to the computer on which you plan to install, configure, and run the utility.
4. Extract the `isim_report_data_sync_utility.zip` file.
5. If you use the `AES` encryption algorithm, access the directory where you extracted the utility, and copy the keystore file into the extracted `data/keystore` directory.
6. Required: If you install the utility on UNIX or Linux platforms, then ensure that the **`SyncData.sh`** file has execute permission. Run this command:

   ```
   chmod +x SyncData.sh
   ```

What to do next

See "Configuring the report data synchronization utility."

Configuring the report data synchronization utility

After you install the data synchronization utility, you must configure it.

Before you begin

- Verify that the `data` directory exists under the directory in which you extracted the utility. All the property files are in the `data` directory.
- Know the database and directory server credentials information that you created during IBM Security Identity Manager installation.

Procedure

1. Access the directory in which you extracted the utility in "Installing the report data synchronization utility" on page 213.
2. Go to the `data` directory.
3. Modify the property files. See Table 22.

Table 22. Property files to modify

Property file name	Actions
`encryptionKey.properties`	Provide the appropriate value for the `encryption.password` property.

Table 22. Property files to modify (continued)

Property file name	Actions
enRole.properties	• Provide the appropriate values for these properties: – enrole.password.database.encrypted – enrole.password.ldap.encrypted – enrole.encryption.password.encoded • Provide the *Lightweight Directory Access Protocol* or the LDAP default tenant ID: enrole.defaulttenant.id • Provide the LDAP server information: – enrole.ldapserver.root – enrole.ldapserver.home • Provide the appropriate values for the following encryption properties: – enrole.encryption.algorithm – enrole.encryption.passwordDigest • If you use the *Advanced Encryption Standard* or the AES encryption algorithm, then set the value of the enrole.encryption.keystore property. Set it to the name of the file that you copied into the data/keystore directory during the installation steps.
enRoleDatabase.properties	Provide the appropriate values for these properties: • database.db.type • database.db.owner • database.db.user • database.db.password • database.jdbc.driverUrl • database.jdbc.driver
enRoleLDAPConnection.properties	Provide the appropriate values for these properties: • java.naming.provider.url • java.naming.security.principal • java.naming.security.credentials
enRoleLogging.properties	• Specify the directory where you want the trace and log files to be generated: – handler.file.fileDir – handler.file.security.fileDir – handler.ffdc.baseDir – handler.ffdc.fileCopy.filesToCopy
ReportDataSynchronization.properties	Provide the appropriate values for these properties: • report.data.synchronization.utility.server.name **Note:** If you do not specify a value for this property, the host name is used as the server name. • report.data.synchronization.utility.user.name

4. Optional: Consider changing additional properties related to data synchronization, specifying values similar to those values that would be specified in the deployed IBM Security Identity Manager environment.
5. Optional: Set the -JAVA_HOME operating system environment variable to the location of the Java runtime environment.

What to do next

Run the report data synchronization utility. See “Administering > Report administration > Data synchronization > Utility for external report data

synchronization > Running the report data synchronization utility" on the IBM Security Identity Manager product documentation site.

Utility for access catalog data synchronization

The access catalog data synchronization utility is a separately installed utility that synchronizes data and access control items between the LDAP server and the IBM Security Identity Manager database. The synchronized data is used to search an existing access catalog and to resynchronize data between LDAP and the database.

Note:

- The fix pack installer installs the utility only if you select to enable the Identity Service Center during fix pack installation.
- You must run the utility on the same computer as IBM Security Identity Manager. For steps to run the utility, see the readme file that is provided in the fix pack.

Regular expressions for access requests

If a regular expression is used for group access authorization for access requests in the Identity Service Center provisioning policy, you must copy and extract the `isim_regexp.jar` file from the IBM Security Identity Manager Server to the directory where DB2 or Oracle is installed. (The IBM Security Identity Manager Server is the server where IBM Security Identity Manager is installed.)

Note: If a regular expression is not used to authorize group entitlement in the provisioning policy, then these manual steps are *not* required.

IBM DB2 database

If IBM Security Identity Manager and IBM DB2 are installed on the same computer, you can use the following commands to extract the `isim_regexp.jar` file:

```
#cd $DB2_HOME$/function/
#cp -p $ISIM_HOME$/lib/isim_regexp.jar
#jar -xvf isim_regexp.jar
```

`$ISIM_HOME$` is the installation home directory for IBM Security Identity Manager, and `$DB2_HOME$` is the installation home directory for DB2.

Oracle database

If you use an Oracle database, use the following steps:

1. Copy the `isim_regexp_for_oracle.jar` file to your Oracle database system. The file is in the `ISIM_HOME/lib` directory, where `ISIM_HOME` is the installation home directory for IBM Security Identity Manager.
2. Load the JAR file into the database. You can use the following command:

   ```
   loadjava -user itimuser/password isim_regexp_for_oracle.jar
   ```

   In this command, *itimuser* and *password* are the DB2 credentials for the user. By default, the user name is `itimuser`. The password is the password that the user provides during the installation.

Chapter 14. Reconfiguration for authentication with an external user registry

You can reconfigure middleware to support authentication with an external user registry.

IBM Security Identity Manager supports authentication through two different deployment configurations. The default configuration is to use a custom user registry provided by IBM Security Identity Manager. Alternatively, you can configure the deployment to use a user registry that is not provided by IBM Security Identity Manager. The user registry that is not provided by IBM Security Identity Manager is called an *external user registry*.

This section describes how to reconfigure the middleware used by IBM Security Identity Manager to support an external user registry.

Note: Use this section only if you installed IBM Security Identity Manager to use the default custom registry and now want to switch to an external user registry. If you installed IBM Security Identity Manager to use an external user registry but did not complete the postinstall configuration, do not use this section. Instead, complete the postinstall tasks in "Postinstall configuration of an external user registry for authentication" on page 156.

To review how IBM Security Identity Manager uses WebSphere Application Server security, see "WebSphere security configuration" on page 7.

The reconfiguration tasks are:

1. Addition of required users to the user registry
2. Reconfiguration of the WebSphere security domain
3. Verifying access for the administrator account

To complete the reconfiguration tasks, continue with "Adding required users to the external user registry."

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 23. 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 creating a user depend on the type of user registry. You can use the **ldapadd** command to add a required user for the IBM Security Directory Server registry.

Using the command line, issue the following command:

```
ldapadd -D Bind DN -w Bind PW -p Port -f filename
```

For example:

```
ldapadd -D cn=root -w root -p 389 -f filename
```

where *filename* contains the following details:

```
dn:cn=ITIM Manager,dc=com
objectclass:person
objectclass:inetOrgPerson
cn:System Administrator
sn:Administrator
uid:ITIM Manager
userpassword:secret

dn:cn=isimsystem,dc=com
objectclass:person
objectclass:inetOrgPerson
cn:isimsystem
sn:isimsystem
uid:isimsystem
userpassword:isimsystem
```

Alternatively, the following procedure describes how to use the IBM Security Directory Server web administration tool to add the required users.

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 24. 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 25. 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**.

Results

The entries are added to the LDAP server.

What to do next

Continue with "Reconfiguration of a WebSphere security domain."

Reconfiguration of a WebSphere security domain

You must reconfigure the WebSphere security domain for IBM Security Identity Manager.

Complete the following configuration tasks:

1. "Reconfiguring the WebSphere user realm type" on page 220
2. "Updating properties files" on page 221
3. "Unmapping roles for the system user" on page 222
4. "Remapping roles for the system user" on page 223
5. "Remapping the service bus user role for the system user" on page 223
6. "Verifying access for the administrator account" on page 224

Continue with "Reconfiguring the WebSphere user realm type" on page 220.

Reconfiguring the WebSphere user realm type

You must reconfigure the user realm type for the WebSphere security domain.

Before you begin

When IBM Security Identity Manager was installed, the installation wizard created a default WebSphere security domain called `ISIMSecurityDomain`. You must modify configuration settings for this domain to switch from a custom registry to a stand-alone LDAP registry.

Procedure

1. To modify `ISIMSecurityDomain` to use a stand-alone LDAP registry, log on to the WebSphere Application Server Administrative Console.
2. Stop the ISIM enterprise application.
3. Click **Security** > **Security domains**.
4. Click the **ISIMSecurityDomain** link.
5. On the ISIMSecurityDomain page, in the **Security Attributes** section, expand **User Realm**.
6. Ensure that **Customize for this domain** is selected.
7. From the **Realm type** list, select **Standalone LDAP registry**.
8. Click **Configure** to open the Stand-alone LDAP registry page.
9. Select **Provide a realm name** and type a realm name. For example, `newRealm`.
10. From the **Type of LDAP server** list, select your LDAP server. For example, **IBM Tivoli Directory Server**.
11. Provide the LDAP configuration property values in the following fields:
    - **Host**
    - **Port**
    - **Base distinguished name (DN)**
    - **Bind distinguished name (DN)**
    - **Bind password**

    For example, provide the property values for the IBM Security Directory Server from the following table:

Table 26. LDAP configuration for the IBM Security Directory Server

Configuration property	Example values
Host	*your_host_name*
Port	389 (or the port your directory server is listening on)
Base distinguished name (DN)	*c=us*
Bind distinguished name (DN)	*cn=root*
Bind password	*your_current_password*

12. Click **Test Connection** to verify the connection information.
13. Click **OK** and then click **Save** to save the changes.
14. On the Stand-alone LDAP registry page, in the **Additional Properties** section, click the **Advanced Lightweight Directory Protocol (LDAP) user registry settings** link.

15. On the Advanced Lightweight Directory Access Protocol (LDAP) user registry settings page, in the **General Properties** section, replace the existing value with `(&(uid=%v)(objectclass=inetOrgPerson))` in the **User filter** field.
16. Click **OK** and then click **Save** to save the changes.
17. If necessary (in case there is change in login or password), update the Java 2 Connector (J2C) global alias definition from **Resources > Resource Adapters** for the **isimsystem** user.
18. Stop WebSphere Application Server. Stop each node in a cluster environment.

What to do next

Continue with "Updating properties files."

Updating properties files

Update IBM Security Identity Manager properties files to reflect the new realm type and any changes to the system user configuration.

About this task

When you reconfigured the WebSphere security domain, you specified a new realm name. You must update an IBM Security Identity Manager property file with the new realm name.

When you added required users to the external user registry, you specified an account name or password for the IBM Security Identity Manager system user. Optionally, you might specify different values that were used previously in the custom registry. In this case, you must run the IBM Security Identity Manager configuration utility.

Procedure

1. If you changed the account name or password for the system user when adding user, update the configuration.

   Note: If you did *not* change the account name or password, skip this step.

   a. Use the command for your operating system:
      - Windows operating systems:
        ISIM_HOME`\bin\runConfig.exe`
      - UNIX or Linux operating systems:
        `ISIM_HOME/bin/runConfig`
   b. Click the Security tab.
   c. In the Identity Manager System User and Identity Manager System User Password fields, specify your new values for the IBM Security Identity Manager system user and the system user password.

   Note: Ignore the **runConfig** warning that WebSphere cannot be contacted. The warning is expected because WebSphere is stopped.
2. Open for editing the `enRole.properties` file in your Security Identity Manager environment.

   For example, on UNIX or Linux systems, the file path is `/opt/IBM/isim/data/enRole.properties`.
3. Reset the default realm name to match the realm name you provided for the standalone LDAP registry.

Example settings:

Table 27. Example setting for realm name in enRole.properties

Old setting	`enrole.appServer.realm=itimCustomRealm`
New setting	`enrole.appServer.realm=`*`your_realm_name`* For example:`enrole.appServer.realm=newRealm`

4. Save the file.
5. Start WebSphere Application Server.

What to do next

Continue with "Unmapping roles for the system user."

Unmapping roles for the system user

Remove the WebSphere mappings of roles for the system user.

About this task

IBM Security Identity Manager runs as an enterprise application called `ITIM` in WebSphere. The configuration for the ITIM application includes mappings for roles used by the IBM Security Identity Manager system user. As part of reconfiguring the middleware to support an external user registry, you must remap the roles. In this task, you must unmap the existing roles.

The default IBM Security Identity Manager system user is `isimsystem`. Your deployment might use a different name, depending on the name specified during initial installation.

Procedure

1. Log on to the WebSphere administrative console.
2. Select **Application** > **Application Types** > **WebSphere Enterprise Application** > **ITIM**.
3. Go to the Configuration tab and the Detail Properties section, and click **User RunAs roles**.
4. On the User RunAs roles panel, select the **ITIM_SYSTEM** check box and click **Remove**.

   This action removes the system user name from the ITIM_SYSTEM role
5. Click **OK** and then click **Save**.
6. Return to the page: **Application** > **Application Types** > **WebSphere Enterprise Applications** > **ITIM**.
7. Go to the Configuration tab and the Detail Properties section, and click **Security role to user/group mapping**.
8. Select the **ITIM_SYSTEM** check box and click **Map Users**.
9. In the Map users/groups window, select the system user name from the **Selected** list. Click **Remove** to move the system user name to the **Available** list.

   The default system user name is `isimsystem`.
10. Click **OK** twice to first close the Map users/groups window and then the Security role to user/group mapping window. Save the changes to the master configuration.

What to do next

Continue to "Remapping roles for the system user."

Remapping roles for the system user

Remove the WebSphere mappings of roles for the system user.

Procedure

1. Log in to the WebSphere administrative console.
2. Select **Application** > **Application Types** > **WebSphere Enterprise Application** > **ITIM**.
3. Go to the Configuration tab, and go to the Detail Properties section, and click **Security role to user/group mapping**.
4. Select the **ITIM_SYSTEM** check box and click **Map Users**.
5. On the Map users/groups window, go to the **Search string** field, and enter a string that finds the registry entry for your system user. **isimsystem** and click **Search**.

   For example, if your system user is the default `isimsystem`, enter the string `*isimsystem*`.

   The result of the search must reflect the syntax of *isimsystem* user entry or DN on your stand-alone LDAP registry. For example, the result might be *cn=isimsystem, c=us*.
6. The results of your search display in the **Available** list. Select the entry (in this example, *cn=isimsystem, c=us*). Click the **Add** arrow button to move the user into the **Selected** list.
7. Click **OK** twice to first close the Map users/groups window and then the Security role to user/group mapping window. Save the changes to the master configuration.
8. Return to **Application** > **Application Types** > **WebSphere Enterprise Applications** > **ITIM**.
9. Go to the Configuration tab and the Detail Properties section, and click **User RunAs Roles**.
10. In the User RunAs Roles window, enter the system user name in the **username** field, and the system user password in the **password** field.

    The user ID must be the short name of what was previously used, for example, *cn=isimsystem, c=us*. In this case, the username is `isimsystem`..
11. Select the **ITIM_SYSTEM** check box and click **Apply**.
12. Verify that the user name *isimsystem* is now listed as in the **User name** column of the Role entry for **ITIM_SYSTEM.**
13. Click **OK** and click **Save**.

What to do next

Continue with "Remapping the service bus user role for the system user"

Remapping the service bus user role for the system user

Remap the WebSphere role configuration for the service bus user role.

Procedure

1. Under **Service Integration > Buses**, click the **Enabled** link in the **Security** column for the `itim_bus` resource.

2. On the **Security for bus itim_bus** page, under **Authorization Policy** click **Users and groups in the bus connector role**.
3. On the **Users and groups in the bus connector role page**, remove the system user. For example, `isimsystem`.
4. On the same page, click **New** and add the system user (for example, `isimsystem`) from your external user registry repository.
5. In the SIB Security Resource wizard:
   a. On the Search for Users or Groups page, in the **Search pattern** field, enter an asterisk '*', and click **Next**.
   b. On the Select Users and Groups page, select your system user. For example, `isimsystem`. Click **Next**.
   c. On the Summary page, review the configuration and click **Finish**.
6. Return to **Security for bus itim_bus**, and under **Authorization Policy** click **Manage default access roles**.
7. On the **Default access roles** page, expand **Default access**, select the system user (`isimsystem`), and click **Remove**.
8. On the **Security for bus itim_bus** page, click **Add**.
9. Add the system user from the external user registry repository. In the SIB Security Resource wizard:
   a. On the Search for Users or Groups page, in the **Search pattern** field, enter an asterisk "*", and click **Next**.
   b. On the Select Users and Groups page, select your system user. For example, `isimsystem`. Click **Next**.
   c. On the Select Role Types page, select **Sender**, **Browser**, **Receiver**, and **Creator**.
   d. On the Summary page, review the configuration and click **Finish**.
10. Set the IBM Security Identity Manager application target deployment status back to **start**.
11. Save the changes.
12. Start the IBM Security Identity Manager application.

Results

Continue with "Verifying access for the administrator account."

Verifying access for the administrator account

Verify that the administrator account is configured correctly.

About this task

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

Procedure

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

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

   `http://hostIP:9080/itim/console`
2. Use the administrator name that you specified when you added the required users to the external user registry.

The default administrator account is `ITIM Manager`.

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 administrator user, then you successfully configured the LDAP user registry as an external authentication user registry for IBM Security Identity Manager.

Part 3. Upgrade

IBM Security Identity Manager supports in-place upgrade and separate system upgrade with data migration.

Chapter 15. IBM Security Identity Manager upgrade

The Security Identity Manager installation program upgrades a computer that has the previous versions of Tivoli Identity Manager. Some manual steps are required to preserve or recustomize settings. This section describes upgrading both single-server and cluster configurations.

Security Identity Manager installation program supports upgrades from:

- Tivoli Identity Manager Version 5.0
- Tivoli Identity Manager Version 5.1

Pre-upgrade requirements for modifying your Java applications to use new authentication methods

Authentication for Java applications is now performed through WebSphere Application Server. All programs, new or old, must use the new authentication.

Important: Your custom applications *must* be updated to use the new authentication APIs before you upgrade to IBM Security Identity Manager version 6.0. Applications written with version 5.1 authentication APIs do not work in version 6.0. Attempting to upgrade without modifying them will cause the upgrade to fail.

See Authentication API.

Description of the upgrade process

The upgrade process has the following major tasks.

1. Migrate your operating system to a level that this release of IBM Security Identity Manager supports. Ensure that the system has the required fix pack or patches. For more information about operating system requirements, see *Hardware and software requirements* on the IBM Security Identity Manager product documentation site.

   Note: If you are upgrading from Linux SUSE 9 to SUSE 10.0 and 11.0, make sure to back up your existing `/etc/services` file before the upgrade. Copy the file back to the `/etc` directory after upgrade.
2. Migrate your database to the supported version and ensure that you run database commands.
3. Migrate your directory server to the supported version and ensure that you run directory server commands.
4. If you are using IBM Tivoli Directory Integrator, migrate it to the supported version.
5. Upgrade the Tivoli Identity Manager Server and use the IBM Security Identity Manager Version 6.0 installation program.

   The installation program upgrades:

   - The database schema and data
   - The directory server schema and data
   - The WebSphere Application Server configuration for IBM Security Identity Manager

- The IBM Security Identity Manager property files
- Other IBM Security Identity Manager files.

During the upgrade process, the *ITIM_HOME*\data directory is backed up to the *ITIM_HOME*\data\backup directory for later recovery if necessary.

The upgrade is for upgrading IBM Tivoli Identity Manager server only. The upgrade of the adapters does not happen until this server upgrade is complete and stable. For detailed information about the upgrade of the adapters, see the adapter documentation on the IBM Security Identity Manager product documentation site.

Note: To upgrade, you must select the current *ITIM_HOME* directory as the IBM Security Identity Manager version 6.0 installation location. After an upgrade, you can validate the current version by examining the copyright notice in the header of the Messages.properties file in the *ITIM_HOME*\data directory.

6. If WebSphere Application Server Version 7.0 is already installed, ensure that you have the required fix packs installed. If you are currently running WebSphere Application Server Version 6.1, you must upgrade IBM Security Identity Manager with a separate installation of WebSphere Application Server Version 7.0 and install all required fix packs.
7. If you are currently running WebSphere Application Server Version 6.1 or Version 7.0, you cannot migrate it to WebSphere Application Server Version 8.5. You must upgrade IBM Security Identity Manager with a separate installation of WebSphere Application Server Version 8.5 and install all required fix packs.
8. After the upgrade of IBM Tivoli Identity Manager server is complete, upgrade their adapters to adapters of IBM Security Identity Manager Version 6.0. For more information, see "Upgrade of adapters" on page 248.

Processes and settings that the upgrade process preserves

The upgrade process preserves running workflow processes that pend for approval or other related actions such as password changes.

The upgrade process preserves the following settings:

- Certificate authority (CA) certificates. Security Identity Manager demonstration certificates are updated.
- Security Identity Manager properties defined in the following files:
  - adhocreporting.properties
  - cvserver.properties
  - CustomLabels.properties
  - CustomLabels_en.properties
  - dataSynchronization.properties
  - encryptionKey.properties
  - enrolepolicies.properties
  - enroleworkflow.properties
  - enroleAuditing.properties
  - enroleExtensionAttributes.properties
  - enRole.properties
  - enRoleAuthentication.properties
  - enRoleDatabase.properties
  - enRoleEntityHiddenAttributes.properties

  - enRoleHiddenAttributes.properties
  - enRoleHiddenOperations.properties
  - enRoleHiddenSearchAttributes.properties
  - enRoleLDAPConnection.properties
  - enRoleLogging.properties
  - enRoleMail.properties
  - entitlementHiddenAttributes.properties
  - KMIPServer.properties
  - passwordrules.properties
  - pim.properties
  - reporttabledeny.properties
  - rest.properties
  - ReportDataSynchronization.properties
  - scriptframework.properties
  - SelfServiceHelp.properties
  - SelfServiceHomePage.properties
  - SelfServiceScreenText.properties
  - SelfServiceScreenText_en.properties
  - SelfServiceUI.properties
  - ui.properties
  - wsExtensions.properties
- The following workflow system files in the data\workflow_systemprocess directory:
  - notifytemplate.html

    Note: The notification template was modified after Tivoli Identity Manager Version 5.0. To use the new template, rename notifytemplate.html.5.0 back to notifytemplate.html. For more information about migration of notification templates, see "Migration of notification templates" on page 244.
  - multiaccountdelete.xml
  - multiaccountrestore.xml
  - multiaccountsuspend.xml
- Any default notification templates stored in LDAP.

Processes and settings that are not preserved, or require manual upgrade

The upgrade process does *not* preserve the following workflow processes, which you must stop or allow to complete before you upgrade IBM Security Identity Manager.

- Provisioning Policy Add/Modify/Remove
- Dynamic Role Add/Modify/Remove
- Reconciliations
- Identity feeds

All other customized data and settings are lost after the upgrade process. For more information, see "Manual preservation of the customized data" on page 243

These user customizations are not preserved:

- Custom logos used in a Welcome page and XLS style sheets. If you modified the welcome page, you must reimplement the `Styles.css` file.
- Any customized WebSphere Application Server configurations. Examples include:
  - ITIM_CLIENT role mapping, which must be remapped.
  - Shared library used by Tivoli Identity Manager through a WebSphere Application Server shared library definition.

Additionally, manually upgrade the following components:

- IBM Security Identity Manager JAR files that the IBM Security Identity Manager client applications use.

  IBM Security Identity Manager client applications must replace their current `itim_api.jar`, `api_ejb.jar`, `itim_server_api.jar`, and `jlog.jar` files with those files from IBM Security Identity Manager Version 6.0.

  For any Security Identity Manager client application that has a duplicate copy of properties files on the client side, take these steps:

  1. Rename the duplicate property files on the client application to preserve any manual changes that you made.
  2. Copy the property files from the IBM Security Identity Manager Server to the duplicate copy on the client application.
  3. If you manually changed the duplicate property files earlier, manually apply the changes again.
- The HR Feed services forms in Tivoli Identity Manager 5.1 add a check box for evaluating Separation Of Duty policies. To enable this feature, use **Configure System** -> **Design Form** to include the new attribute **erevaluatesod** in the HR feed service definition form. The **erevaluatesod** attribute is of the type Boolean and needs to be included as a check box on the form.
- IBM Security Identity Manager Version 6.0 has a new attribute `errepositoryservice` added to the ITIM Service form. The attribute is labeled as **WebSphere account repository** on the Service Information page. After upgrading from Tivoli Identity Manager 5.0 or 5.1, the default ITIM Service DN value is set to the ITIM Service instance. However, the ITIM Service form is not automatically upgraded with this attribute as some users might have the customized ITIM Service form. To view or update this attribute value, you must manually add this attribute to the ITIM Service form through the form designer applet. If you use the external user registry as an authentication user registry after the upgrade, this step is required. To use the form designer applet to add the attribute, complete these steps:

  1. From the IBM Security Identity Manager administration console, select **Configure System** > **Design Forms**.
  2. In the Design Form panel, double-click **Service** > **ITIM**.
  3. Under Attribute List in the right panel, double-click **errepositoryservice**. The `errepositoryservice` attribute is added to ITIM Service.
  4. Right click **[TextField]** next to **$errepositoryservice** and select **Change To** > **Search Control**. The Search Control Editor window opens.
  5. Select **Service** from the Category list.
  6. Select **Single Value** from the Type list.
  7. Select the **Search entire organization (current container only if not checked)** box.
  8. Click **OK** to close the window.

9. Save the form.

- Manually upgrade the access control items. For more details, see "Manual upgrade of the access control items" on page 248.

Preparing to upgrade IBM Security Identity Manager

Before you can upgrade IBM Security Identity Manager, you must complete some system tasks.

Procedure

1. Reduce system activity before you start the upgrade process. Avoid starting policy enforcements or reconciliation requests before you upgrade IBM Security Identity Manager. Do not delete entries directly from the SCHEDULED_MESSAGES table in the IBM Security Identity Manager database.
2. Complete or stop the following workflow processes, which are not preserved during upgrade:
   - Provisioning Policy Add/Modify/Remove
   - Dynamic Role Add/Modify/Remove
   - Reconciliations
   - Identity feeds
3. Shut down API clients and turn off web access to the IBM Security Identity Manager application. These actions ensure that no new workflow requests are submitted before the upgrade process.
4. Back up the IBM Security Identity Manager database and ensure that the database server is running. Then, migrate the database server to the supported version.
   - DB2 database

     For information about upgrading DB2 database, see this website: http://pic.dhe.ibm.com/infocenter/db2luw/v9r7/topic/com.ibm.db2.luw.doc/welcome.html

     Note: Upon upgrade of DB2 database, the port number might change. Verify that the port number you are using. For more information, see "Determining the correct service listening port and service name" on page 25.
   - Oracle

     For information about upgrading Oracle, see documentation on the Oracle website.
   - SQL Server 2008

     For information about upgrading SQL Server 2008, see documentation on the Microsoft SQL Server website.

     For information about configuring SQL Server 2008, see "Configuration of SQL Server 2008" on page 34.
5. Migrate the directory server to the supported version. Then, back up the IBM Security Identity Manager schema and data, and ensure that the directory server is running. For Tivoli Identity Manager Version 5.0 or 5.1 recovery purposes, export the Tivoli Identity Manager LDAP directory to an LDIF file.

   Note: Migration is not necessary if you are using the currently supported IBM Security Directory Server or Sun Directory Server Enterprise Edition 6.3.1 and 7.0. They are supported directory servers.

If you migrate IBM Security Directory Server to the new LDAP instance, run the system configuration tool `runConfig` to update the associated property files with the new LDAP instance data.

For the Windows operating system, run:

```
runConfig.exe
```

For the UNIX or Linux operating system, run:

```
./runConfig
```

6. If you are currently running WebSphere Application Server Version 6.1, you cannot migrate it to WebSphere Application Server Version 7.0. In addition, you cannot migrate from WebSphere Application Server Version 7.0 to Version 8.5. You must upgrade IBM Security Identity Manager with a separate installation of either WebSphere Application Server Version 7.0 or Version 8.5. You must also complete these steps:
   - Single-server: Install any necessary fix packs.
   - Cluster: Install any necessary fix packs.
7. On a single-server configuration, and on each cluster member in a cluster configuration, complete these steps:
   a. Back up the *itim* directory.
   b. If you are upgrading from Tivoli Identity Manager 5.0 or 5.1, access the *WAS_HOME*\installedApps*cellname*\ITIM.ear directory and store any customized files in a temporary holding area.
8. Ensure that the appropriate servers are running in the WebSphere environment. Complete this step:
   - Single-server configuration:

     Start WebSphere Application Server with the latest fix packs that you installed. For the most current fix pack and possible APARs, see the IBM Security Identity Manager product documentation site.
   - Cluster configuration:

     Use the administrative console to ensure that the deployment manager and all the nodes are federated. Ensure that the node agents are running and that the latest fix packs are installed. For the most current fix pack and possible APARs, see the IBM Security Identity Manager product documentation site.
9. Stop the IBM Tivoli Identity Manager application and WebSphere server.
   - Single-server configuration:

     Stop the IBM Tivoli Identity Manager application and WebSphere server on which IBM Tivoli Identity Manager is running.
   - Cluster configuration:

     Stop the IBM Tivoli Identity Manager application and WebSphere cluster on which IBM Tivoli Identity Manager application is running.

Clearing the service integration bus

Before you upgrade from Tivoli Identity Manager 5.0 or 5.1 to Security Identity Manager Version 6.0, you must clear out the Service Integration Bus (SIB) data from the restored database.

Before you begin

Ensure that the free disk space and virtual memory requirements are met. Additionally, ensure that there is adequate free disk space in the system temp

directory. The target system must meet the hardware and software requirements described in *Hardware and software requirements* on the Security Identity Manager product documentation site.

Ensure that you have the needed administrative authority. On Windows systems, the login user ID must be in the Administrators Group. For DB2 or Oracle, on Linux systems, the login user ID must be root.

Ensure that the Security Identity Manager database is running.

Procedure

1. On the target Security Identity Manager Version 6.0 server, start the database. Use the instructions for your type of database:
   - DB2
     a. Open a DB2 command window.
     b. UNIX or Linux: Log on as the DB2 instance owner and enter `db2` to open a DB2 command window.

        Windows: Click **Start** > **Run**, and enter `db2cmd`. When the DB2 command window opens, enter `db2`.
     c. Connect to the database as the DB2 instance owner by using the command:

        `connect to itimdb user instance_owner using instance_owner_password`

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

     Start the Oracle database.
   - Microsoft SQL
     a. Start the Microsoft SQL Server Management Studio.
     b. Go to the database used for Security Identity Manager Version 6.0.
     c. Right click the database and click **New Query**.
2. Enter the DELETE SQL statements required to delete all data from the tables in the SIB schemas.

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

   The SIB schema, *schema_name* is:

Table 28. Service integration bus schema names

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

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

Upgrading a single-server from Tivoli Identity Manager Version 5.0 or 5.1 to IBM Security Identity Manager Version 6.0

Use this procedure to migrate your single-server configuration from a previous version of Tivoli Identity Manager to the current version of IBM Security Identity Manager.

Before you begin

Ensure that you completed the steps in "Preparing to upgrade IBM Security Identity Manager" on page 233. You also need:

- Database administrative user ID and password
- WebSphere Application Server administrative user ID and password
- At least 150 MB of free space in the `/tmp` directory

About this task

The upgrade process completes these tasks in a single-server configuration:

1. Backs up files in the *ITIM_HOME*`\data` directory.
2. Replaces the files in the *ITIM_HOME* directory.
3. Checks the WebSphere Application Server Version status and tries to start WebSphere Application Server if it is not running. See Step 8 in "Preparing to upgrade IBM Security Identity Manager" on page 233.
4. Starts the system configuration tool (**runConfig**) to prompt the user to examine current system configuration values.
5. Updates several properties files. For more information, see "Processes and settings that the upgrade process preserves" on page 230.
6. Configures WebSphere Application Server for IBM Security Identity Manager Version 6.0.
7. Upgrades the IBM Security Identity Manager database schema and data.
8. Upgrades the IBM Security Identity Manager directory server schema and data.
9. Deploys the IBM Security Identity Manager application (ITIM.ear) to WebSphere Application Server.
10. Stops and starts WebSphere Application Server and the Security Identity Manager application.

Procedure

1. Run the installation program.
   - For Windows operating systems:
     a. Click **Start** > **Run**.
     b. Enter the drive and path where the installation program is located and then enter this command:`instwin.exe`

     The Welcome window opens.
   - For UNIX or Linux operating systems:

a. Open a command shell prompt window and find the directory where the installation program is located.
b. Enter the following command for the IBM Security Identity Manager installation program:
   - AIX operating systems: `instaix.bin`
   - Linux operating systems: `instlinux.bin`
   - Linux for System p® operating systems: `instplinux.bin`
   - Linux for System z Operating Systems: `instzlinux.bin`
   - Solaris operating systems: `instsol.bin`

   The installation program starts and opens the Welcome window.

   The installation program on a UNIX or Linux system requires at least 150 MB of free space in the `/tmp` directory. If you do not have enough space, set the *IATEMPDIR* environment variable to a directory on a disk partition with enough free disk space. To set the variable, enter one of the following commands at the command-line prompt before running the installation program again:
   - Bourne shell (sh), ksh, bash, and zsh:

     ```
     $ IATEMPDIR=temp_dir
     $ export IATEMPDIR
     ```
   - C shell (csh) and tcsh:

     ```
     $ setenv IATEMPDIR temp_dir
     ```

   where *temp_dir* is the path to the directory, for example, `/your/free/directory`, where free disk space is available.

2. Select the appropriate language and click **OK**.
3. Click **Next** to advance past the copyright and legal text.

   Note: If you are installing IBM Security Identity Manager on the AIX system and unable to see the copyright text, you must adjust the contrast color setting of the system. Change the contrast color setting from High to Low.
4. In the License Agreement window, read the license agreement and decide whether to accept its terms. If you do:
   a. Select **Accept**.
   b. Click **Next**.
5. In the Choose Install Directory window, you *must* select the existing Tivoli Identity Manager home directory that you want to upgrade.
   - Accept the existing directory. Or,
   - Click **Choose** and select the correct directory.

   a. Click **Next**.
6. In the Upgrade IBM Security Identity Manager window, click **Continue to Next** to start the upgrade.
7. Read the caution windows to ensure that the prerequisite applications meet the requirements that IBM Security Identity Manager supports. Then, click **Next**.
8. In the WebSphere Application Server installation directory window, specify the location of WebSphere Application Server. Click **Next**. There can be multiple instances of WebSphere Application Server on the computer.
9. Choose the WebSphere Application Server base profile where the IBM Security Identity Manager application is to be deployed. Click **Next**.

10. If WebSphere Application Server administrative security is on, a WebSphere Application Server user ID and password window opens. Enter the user ID and password and click **Next**.
11. Select the type of security domain window for WebSphere Application configuration and click **Next**.
    - Select **Yes** to use the IBM Security Identity Manager custom registry.
    - Select **No** to use the existing security domain and registry.

    Note: If you select **Yes**, the custom registry provided by IBM Security Identity Manager is used for authentication decisions. If you select **No**, the existing user registry for the WebSphere security domain is used for authentication decisions. If you select **No**, you must complete post-installation configuration steps after the installation wizard completes. See "Postinstall configuration of an external user registry for authentication" on page 156.
12. Enter the IBM Security Identity Manager System user name and password and click **Next**. If you selected to create a security domain in the previous step, `isimsystem` is entered as the default IBM Security Identity Manager System user.
13. In the Java home window, note the directory to which IBM Security Identity Manager Version 6.0 now points. You might need to manually migrate any files that reference the previous directory to reference the current directory. Click **OK**.
14. If you use Oracle database or Microsoft SQL Server, a Where is the JDBC Driver? Window is presented. Specify the JDBC driver location and name. Click **Next**. For more information, see "Oracle JDBC driver installation" on page 30 and "SQL Server JDBC driver installation" on page 34.

    Note: If you are upgrading from Tivoli Identity Manager 5.1 on WebSphere Application Server 6.1.1 to Security Identity Manager 6.0 on WebSphere Application Server 7.0, the JDBC driver setup panel does not open. Additional manual steps are needed for the Oracle database.
    a. After deploying IBM Security Identity Manager 6.0 on WebSphere Application Server 7.0 Fix Pack 5, remove the `ojdbc.jar` file from `ISIM_HOME/lib` and replace it with `ojdbc6.jar`. Then, rename `ojdbc6.jar` to `ojdbc.jar`. This action is necessary because WebSphere Application Server 7.0 uses JDK1.6.
    b. Clear the service integration bus. See "Clearing the service integration bus" on page 264 in this chapter.
15. In the Tivoli Common Directory window, accept the default directory for the Tivoli Common Directory or specify a different directory. Click **Next**. The IBM Security Identity Manager installation program creates the CTGIM subdirectory to store serviceability-related files for IBM Security Identity Manager. Ensure that the directory has at least 25 MB of free space.
16. In the Pre-install Summary window, click **Install**. The installation program starts the system configuration tool `runConfig` for you to change configuration settings, if necessary. For more information about **runConfig**, see "Configuration of commonly used system properties" on page 123.
    a. In the System Configuration Tool window, examine the values of all parameters, which are preserved from the previous version of Tivoli Identity Manager.
    b. On the Database tab, verify that the JDBC URL has the correct format of type 4 JDBC driver URL, and click **Test** to test the database connection.

c. Change the IBM Security Identity Manager System user ID and password on the **Security** tab, if they are different from the WebSphere Application Server administrative user ID and password.

d. Verify the values and click **OK**. The system configuration requires several minutes to complete.

The installer starts the database upgrade program to upgrade the database schema and data.

17. Provide the database administrative user ID and password to create or upgrade the database schema required for the messaging engine. If the administrative user ID does not have the privileges to create the database schema, an error message is generated during the upgrade. Run the *ISIM_HOME*\bin\DBUpgrade program after the upgrade completes and enter the correct database administrative ID. This program ensures that the database schema and tables for the messaging engine are created. The installer starts the LDAP upgrade program to upgrade the LDAP schema and data silently.

    Note: For Oracle Directory Server Enterprise Edition, if the upgrade adds new indexes, you must index your data again after the upgrade is complete.

What to do next

After the installation is complete, you must manually update any customizations which were not preserved during the upgrade process. For more information, see "Manual preservation of the customized data" on page 243.

Upgrading from Tivoli Identity Manager Version 5.0 or 5.1 cluster configuration to IBM Security Identity Manager Version 6.0

Use this procedure to migrate your cluster configuration from a previous version of IBM Tivoli Identity Manager to the current version.

Before you begin

Ensure that you completed the steps in "Preparing to upgrade IBM Security Identity Manager" on page 233. You also need:

- Database administrative user ID and password
- WebSphere Application Server administrative user ID and password
- At least 150 MB of free space in the /tmp directory for the UNIX or Linux operating system.

About this task

The upgrade process has these tasks in a cluster configuration:

1. Backs up files in the *ITIM_HOME*\data directory.
2. Replaces the files in the *ITIM_HOME* directory.
3. On the computer that has the deployment manager installed, complete these tasks:
    a. Start the system configuration tool (**runConfig**) for the user to examine current system configuration values.
    b. Updates several properties files. For more information, see "Processes and settings that the upgrade process preserves" on page 230.

c. Configures WebSphere Application Server for IBM Security Identity Manager Version 6.0.
d. Upgrades the IBM Security Identity Manager database schema and data.
e. Upgrades the IBM Security Identity Manager directory server schema and data.

4. On each computer that has a cluster member, starts the system configuration tool **runConfig**. This tool:
   - Asks the user to examine current system configuration values.
   - Updates several properties files.
   - Configures WebSphere Application Server for IBM Security Identity Manager.

   For more information, see "Processes and settings that the upgrade process preserves" on page 230.

Procedure

1. Run the installation program on the deployment manager and on each cluster member computer.
   - For Windows operating systems:
     a. Click **Start** > **Run**.
     b. Enter the drive and path where the installation program is and then enter the following command:`instwin.exe`

     The Welcome window opens.
   - For UNIX of Linux operating systems:
     a. Open a command shell prompt window and find the directory where the installation program is located.
     b. Enter the following command for the Security Identity Manager installation program:
        - AIX operating systems: `instaix.bin`
        - Linux operating systems: `instlinux.bin`
        - Linux for System p operating systems: `instplinux.bin`
        - Linux for System z operating systems: `instzlinux.bin`
        - Solaris operating systems: `instsol.bin`

     The installation program starts and opens the Welcome window.

     The installation program on a UNIX or Linux system requires at least 150 MB of free space in the `/tmp` directory. If you do not have enough space, set the *IATEMPDIR* environment variable to a directory on a disk partition with enough free disk space. To set the variable, enter one of the following commands at the command-line prompt before running the installation program again:
     - Bourne shell (sh), ksh, bash, and zsh:

       ```
       $ IATEMPDIR=temp_dir
       $ export IATEMPDIR
       ```

     - C shell (csh) and tcsh:

       ```
       $ setenv IATEMPDIR temp_dir
       ```

     where *temp_dir* is the path to the directory, for example `/your/free/directory`, where free disk space is available.
2. Select the appropriate language and click **OK**.
3. Click **Next** to advance past the copyright and legal text.

Note: If you are installing IBM Security Identity Manager on the AIX system and unable to see the copyright text, you must adjust the contrast color setting of the system. Change the contrast color setting from High to Low.

4. In the License Agreement window, read the license agreement and decide whether to accept its terms. If you do:
   a. Select **Accept**.
   b. Click **Next**.
5. In the IBM Security Identity Manager Installation Directory window, you *must* select the existing Tivoli Identity Manager home directory that you want to upgrade.
   - Accept the existing directory. Or,
   - Click **Choose** and select the correct directory.
6. Click **Next** to proceed to the next step.
7. In the Upgrade IBM Security Identity Manager window, click **Continue to Next** to start the upgrade.
8. A warning window opens to confirm whether you want to upgrade to IBM Security Identity Manager 6.0. Click **Continue to Next** to proceed to the upgrade.
9. A warning window opens to remind you that Security Identity Manager must not co-exist in two versions of WebSphere Application Server. Click **OK**.
10. Read the caution windows to ensure that the prerequisite applications meet the requirements that IBM Security Identity Manager supports. Then, click **OK**.
11. If the IBM Security Identity Manager cluster member is installed on the computer, specify the WebSphere Application Server installation directory, click **Next**. Then select the WebSphere Application Server profile name and click **Next**.
12. If the deployment manager is installed on the computer, specify the deployment manager installation directory, click **Next**. Then select the WebSphere Deployment Manager profile name and click **Next**.
13. If WebSphere Application Server administrative security is on, a WebSphere Application Server Administrator Credentials window is presented. Enter the administrator user ID and password and then click **Next**.
14. Enter the IBM Security Identity Manager System user name and password and click **Next**. If you selected to create a security domain in the previous step, `isimsystem` is entered as the default System user.
15. If you use Oracle database or Microsoft SQL Server, a Where is the Microsoft SQL Server JDBC Driver? Window opens. Specify the JDBC driver location and name. Click **Next**. For more information, see “Oracle JDBC driver installation” on page 30 and “SQL Server JDBC driver installation” on page 34.
16. The Supported version of Directory Server is Required window opens to remind you of installing a directory server. Click **Continue**.
17. In the New Java Home window, note the directory to which IBM Security Identity Manager Version 6.0 now points. You might need to manually migrate any files that reference the previous directory to the current directory. Click **OK**.
18. Click **Next** to advance past the Upgrade Agentless Adapters separately window.
19. In the Do you want to install Shared Access Module window, decide whether you want to install Shared Access Module:

- Select **Yes** if you need and purchased Shared Access Module. The installer installs IBM Security Identity Manager with the Shared Access Module component.
- Select **No** if you did not purchase Shared Access Module. You can always install Shared Access Module separately later when you need it.

20. In the Tivoli Common Directory window, accept the default directory for the Tivoli Common Directory or specify a different directory. Click **Next**. The installation program creates the CTGIM subdirectory to store serviceability-related files for IBM Security Identity Manager. Ensure that the directory has at least 25 MB of free space.
21. In the Pre-install Summary window, click **Install**. The installation program starts the system configuration tool `runConfig` for you to change configuration settings, if necessary. For more information about this tool, see "Configuration of commonly used system properties" on page 123.
    a. In the System Configuration Tool window, examine the values of all parameters, which are preserved from the previous version of Tivoli Identity Manager.
    b. On the Directory tab, verify the values and click **Test** to test the directory server connection.
    c. On the Database tab, verify that the JDBC URL has the correct format of type 4 JDBC driver URL. Click **Test** to test the database connection.
    d. If the user ID and password are different from the WebSphere Application Server administrative user ID and password, change the EJB user ID and password on the **Security** tab . The EJB user ID and password are the IBM Security Identity Manager System user name and password that you specified in step 14.
    e. Verify the values and click **OK**. The system configuration requires several minutes to complete.

    After the first installation, for the cluster member installation only, the System Configuration panel is shown for you to verify the information and test the connection:
    a. On the Mail tab, verify the information to ensure that it matches the first installation.
    b. On the General tab, verify the information to ensure that it matches the first installation.
    c. On the Directory tab, enter the password and host name and verify other information on this tab. Click **Test** to test the connection.
    d. On the Database tab, enter the password and check other information on this tab. Click **Test** to test the database connection.
    e. Verify the information on the Logging tab to ensure that it matches the first installation.
    f. Verify and update the information on the UI tab. Ensure that it matches the first installation.
    g. Enter the IBM Security Identity Manager user ID and password that you use for the first installation on the **Security** tab. The default user ID is `isimsystem`.
    h. After verifying all information on the tabs, click **OK**.

    Note: This system configuration panel is available on systems with the deployment manager and cluster member. It is not shown on systems with the cluster member upgrade only.

On the deployment manager, the installer starts the database upgrade program to upgrade the database schema and data.

22. Provide the database administrative user ID and password to create or upgrade the database schema required for the messaging engine.

    If the administrative user ID does not have the privileges to create the database schema, an error message is generated during the upgrade. Run the *ISIM_HOME*\bin\DBUpgrade program after the upgrade completes and enter the correct database administrative ID. This program ensures that the database schema and tables for the messaging engine are created.

    After running DBUpgrade, the installation program starts the LDAP upgrade program to upgrade the LDAP schema and data silently.

    Note: For Sun Enterprise Directory Server 6.3, if the upgrade adds new indexes, you must index your data again after upgrading to IBM Security Identity Manager Version 6.0 is completed.

23. Click **Done** to exit the installation.

What to do next

After the installation is complete, you must manually update any customizations which were not preserved during the upgrade process. For more information, see "Manual preservation of the customized data." You must also run this upgrade procedure for each cluster member.

Manual preservation of the customized data

To preserve customized data that is not preserved by the upgrade process, complete these manual tasks if applicable.

For more information about processes that are not preserved, see "Processes and settings that are not preserved, or require manual upgrade" on page 231.

Manual application of Java security

Manually apply the changes that you made for the previous IBM Development Kit for Java to the new IBM Development Kit for Java.

Customization of logos and style sheets

If you need to insert customized logos and style sheets in the *WAS_HOME**cellname*\ITIM.ear directory, restore these files from a backup location.

Preserving WebSphere Application Server customization

You can preserve WebSphere customization, such as specific JAR files by using the settings for a WebSphere Application Server shared library.

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

For a shared library, you must define the name of the shared library to the newly deployed Security Identity Manager Version 6.0. For example, Tivoli Identity Manager Version 5.0 or 5.1 might load a shared library with a name such as user_shared_library.

Complete these tasks on the WebSphere Application Server administrative console to associate the previously defined shared library with Security Identity Manager Version 6.0:

Procedure

1. Click **Applications** > **Enterprise Applications** > **ITIM**.
2. Click **Shared library references**.
   a. Select the shared library.
   b. Click **OK**.
3. Click **Apply** to apply the changes.
4. Save the configuration.
5. Restart the WebSphere Application Server to enable the changes.

What to do next

You can preserve other customizations.

Updating the report tables

After upgrading to IBM Security Identity Manager Version 6.0, the tables that contain the report data lose all data. You must run data synchronization to get back data.

Procedure

1. Log on to the IBM Security Identity Manager administrative console.
2. Go to **Reports** > **Data Synchronization**.
3. Click **Run Synchronization Now**. The table is updated with valid report data.

Migration of notification templates

Updating the default templates in the Tivoli Identity Manager 5.0 or 5.1 environment, does not upgrade notification templates. The Security Identity Manager upgrade program does not overwrite (upgrade) any notification templates.

To migrate old notification templates to match them in Security Identity Manager, you must manually update both the XML Text Template Language (XTTL) content and style.

The following table lists templates and their locations in the Security Identity Manager configuration file `tenant.tmpl`. Use this list as a reference for the updated default notification template content.

Table 29. Templates contained in tenant.tmpl

Template name	Template DN
Todo Item Reminder Notification	cn=Reminder,erglobalid=<%config.workflow %>,ou=config,ou=itim, <%tenant.dn%>

Table 29. Templates contained in tenant.tmpl (continued)

Template name	Template DN
Default Compliance Alert Notification	cn=Compliance,erglobalid=<%config.workflow%>,ou=config,ou=itim,<%tenant.dn%>
Default New Account Notification	cn=NewAccount,erglobalid=<%config.workflow%>,ou=config,ou=itim,<%tenant.dn%>
Default New Password Account Notification	cn=NewPassword,erglobalid=<%config.workflow%>,ou=config,ou=itim,<%tenant.dn%>
Default Change Account Notification	cn=ChangeAccount,erglobalid=<%config.workflow%>,ou=config,ou=itim,<%tenant.dn%>
Default Restore Account Notification	cn=RestoreAccount,erglobalid=<%config.workflow%>,ou=config,ou=itim,<%tenant.dn%>
Default Suspended Account Notification	cn=SuspendedAccount,erglobalid=<%config.workflow%>, ou=config,ou=itim,<%tenant.dn%>
Default Deprovision Account Notification	cn=Deprovision,erglobalid=<%config.workflow%>,ou=config,ou=itim,<%tenant.dn%>
Default Activity Timeout Notification	cn=ActivityTimeout,erglobalid=<%config.workflow%>,ou=config,ou=itim,<%tenant.dn%>
Default Process Timeout Notification	cn=ProcessTimeout,erglobalid=<%config.workflow%>,ou=config,ou=itim,<%tenant.dn%>
Default Process Completion Notification	cn=ProcessCompletion,erglobalid=<%config.workflow%>, ou=config,ou=itim,<%tenant.dn%>
Default ManualActivity Notification	cn=ManualActivityApproval,erglobalid=<%config.workflow%>,ou=config,ou=itim,<%tenant.dn%>
Default ManualActivityRFI Notification	cn=ManualActivityRFI,erglobalid=<%config.workflow%>, ou=config,ou=itim,<%tenant.dn%>
Default ManualActivityWorkOrder Notification	cn=ManualActivityWorkOrder,erglobalid=<%config.workflow%>, ou=config,ou=itim,<%tenant.dn%>

XML Text Template Language (XTTL) contents

To upgrade to Security Identity Manager version 6.0 from Tivoli Identity Manager 5.0, new XTTL contents are needed for the default workflow notification templates.

The following XTTL contents are needed for the default workflow notification templates if upgrading from Tivoli Identity Manager version 5.0:

Todo Item Reminder Notification

Remove:

```
<RE key="escalation_note"/> <escalationTime/>
```

Add:

```
<RE><KEY><JS>  var currentDate = new Date();
var currentTime = currentDate.getTime();
if (currentTime < reminderCtx.getEscalationDate().getTime())
{
   return "workitem_due_note";
}
else
{
  return "workitem_overdue_note";
}
</JS></KEY>
<PARM><escalationTime/></PARM>
</RE>
```

Updating XML Text Template Language (XTTL) contents

Use this procedure to add or modify the XTTL contents of the default workflow notification templates.

Before you begin

To modify the contents of default workflow notification templates, log on to the Security Identity Manager Version 6.0 GUI administrative console with administrative permission.

About this task

Use this procedure to change the default workflow notification templates that are necessary to upgrade to the current level of Security Identity Manager. You can add, delete, or modify the XTTL contents.

Procedure

1. Go to **Configure System** > **Workflow Notification Properties**
2. Select the template you want to modify and click **Change**.
3. On the Notification Template page, modify the appropriate section of the notification template.
4. Click **OK**.

What to do next

Modify additional workflow templates XXTL content.

Update notification template style.

Notification template style

Use the following template to design email notifications (XHTML templates).

To design an XHTML template, use the following cascading style sheet (CSS) file and images:

- Imperative style sheet

  BASE_URL/console/css/imperative.css
- Images
  - Tivoli logo

    BASE_URL/console/html/images/left-tiv-1.gif
  - IBM banner

    BASE_URL/console/html/images/ibm_banner.gif

– Background image
  BASE_URL/console/html/images/mid-part-1.gif
– Template body
  BASE_URL/console/html/images/portfolio_background.gif

Note: The value of *BASE_URL* is http://*servername*:*port*/itim

Background colors

The following colors are used to format the background:

- Title bar: `#a8a8a8`
- Tables containing values: `gray` and `EBEDF3`
- Copy Right Table: `#a8a8a8`

Style sheets

To apply a style sheet, link the style sheet in the following way:

```
<link type="text/css" title="Styles" rel="stylesheet"
href="BASE_URL/console/css/imperative.css" />
```

Note: The value of *BASE_URL* is http://*servername*:*port*/itim

The text-description class of the preceding CSS is used to format the text in the email notification. For example, to format the title, use the following code:

```
<!-- Title Bar -->
<table width="100%" border="0" cellpadding="0" cellspacing="0">
 <tbody>
 <tr bgcolor="#a8a8a8">
  <td height="20" width="8"></td>
  <!-- ITIM Notification Label -->
      <td height="20" class="text-description" width="979"
      valign="middle">$TITLE</td>
      <td height="20" width="5"></td>

 </tr>
 </tbody>
</table>
```

Updating notification template style

Use this procedure to add or modify the style of the default workflow notification templates.

Before you begin

To modify the style of default workflow notification templates, log on to the Security Identity Manager Version 6.0 GUI administrative console with administrative permission.

Procedure

1. Go to **Configure System** > **Workflow Notification Properties**
2. Select the template you want to modify and click **Change**.
3. On the Notification Template page, modify the appropriate section of the notification template.
4. Click **OK**.

What to do next

Modify workflow templates XXTL content.

Manual upgrade of the access control items

The upgrade process does not change the access control items for the existing organizations. IBM Security Identity Manager provides default access control items to define permissions to the user and members in other group. However, to specify certain operations and permissions for the targeted persona, you must manually create the access control items.

For upgrading from IBM Tivoli Identity Manager 5.0 and 5.1 to IBM Security Identity Manager 6.0, the following new operations are available for you to manually create customized access control items.

- New operations for Service:
  - Customize Account Form
  - Enforce Policy
  - Retry Blocked Requests
- New operation for ITIM Service:
  - Enforce Policy

For upgrade from version 5.0 to version 6.0, three new default access control items are introduced:

- Default access control item for Separation of Duty Policy: Grant All to Owner
- Default ACI for Separation of Duty Policy: Grant Search to Auditor Group
- Default ACI for Service Group: Grant All (except for Add operation) to Access Owner

For the shared access module, the shared access enablement tool, SAConfig, creates new access control items.

To view the default access control items, including items for the shared access module, see the topic "Default access control items" in the *IBM Security Identity Manager Administration Guide*. For information about how to create an access control item, see "Creating an access control item" in the *IBM Security Identity Manager Administration Guide*.

Upgrade of adapters

The adapters and profiles of IBM Security Identity Manager Version 5.0 and 5.1 are supported on IBM Security Identity Manager Version 6.0 during the IBM Security Identity Manager upgrade. When the upgrade is complete, you must upgrade your adapters to IBM Security Identity Manager Version 6.0.

Each adapter can have specific instructions to upgrade to IBM Security Identity Manager Version 6.0. See the specific adapter documentation and package for more details.

The following requirements apply to all adapter upgrades:

- The adapters of IBM Security Identity Manager Version 6.0 must be used with the profile version 6.0 of the adapters.
- For all version 6.0 adapters that run on Security Directory Integrator, Dispatcher Version 6.0 is required.

- Dispatcher Version 6.0 can be used only with the version 6.0 adapters and profiles.
- For all adapters that do not require Security Directory Integrator (ADK-based adapters), they must not be installed on Windows servers where adapters before the 6.0 version are installed. All adapters must be upgraded simultaneously on the same server because of the sharing of DLLs.

Chapter 16. Separate system upgrade and data migration

Use these tasks to migrate database and directory data from an existing Tivoli Identity Manager to a separate environment that runs Security Identity Manager Version 6.0.

These tasks require the installation of middleware and the upgrade and installation of Security Identity Manager Version 6.0. The topics include best practices for the upgrade and migration from production environments.

Supported upgrade paths

Table 30. Upgrade paths to Security Identity Manager Version 6.0

From	To
Tivoli Identity Manager Version 5.0 that is deployed on WebSphere Application Server 6.1	Security Identity Manager Version 6.0 that is deployed on WebSphere Application Server 7.0
Tivoli Identity Manager Version 5.1 that is deployed on WebSphere Application Server 6.1 or WebSphere Application Server 7.0	Security Identity Manager Version 6.0 that is deployed on WebSphere Application Server 7.0
Security Identity Manager Version 6.0 that is deployed on WebSphere Application Server 7.0	Security Identity Manager Version 6.0 that is deployed on WebSphere Application Server 8.5

Security Identity Manager Version 6.0 supports data migration among supported UNIX based operating systems. Data that resides in HP_UX environments can be migrated to any of the supported UNIX environments. Data can also be migrated between Windows operating systems. Data, however, cannot be migrated from UNIX environments to Windows environments or from Windows environments to UNIX environments.

To migrate data, previous versions of Tivoli Identity Manager must have the minimum fix packs and interim fixes installed. See Recommended fixes for IBM Security Identity Manager.

See the Security Identity Manager product documentation to review:

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

For known issues about migrating data, see "Post migration troubleshooting and known issues" on page 288.

Migration process overview

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

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

- In the Tivoli Identity Manager Version 5.0 or 5.1 server environment:
  1. Stop WebSphere Application Server and any connections to the Tivoli Identity Manager database if necessary.
  2. Back up and export the following data from middleware servers to a temporary file directory:
     - Database server components
     - Directory server components

  Note: After the backup and export are completed, you can bring the Tivoli Identity Manager Version 5.0 or 5.1 server environment back into production. You can load production data into the new Security Identity Manager Version 6.0 system at a later date. You can migrate data to a test environment before a production cutover to the new system. Any changes you make to Security Identity Manager data on the new system are overwritten when you reimport the Tivoli Identity Manager Version 5.0 or 5.1 production data during the final cutover.
- In the Security Identity Manager Version 6.0 server environment:
  1. Install the required middleware (at the required release and fix pack level).
  2. Optionally run the middleware configuration utility for DB2 Universal Database and IBM Tivoli Directory Server.

Database migration

Security Identity Manager Version 6.0 supports data migration from most databases supported on Tivoli Identity Manager Version 5.0 or 5.1.

To determine release levels for the supported databases, see *Database server requirements* on the Security Identity Manager product documentation site.

DB2 Universal Database migration

Use these scenarios to migrate DB2 Universal Database data to a version that Security Identity Manager Version 6.0 supports.

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

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

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

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

These procedures document the steps to migrate a DB2 database from a Linux for System z to an X86Linux system. To migrate other combinations of systems that use big endian and small endian, the procedures are similar, however, changes to

the commands might be required. For the exact syntax and details of the DB2 commands, see the IBM Knowledge Center http://www.ibm.com/support/knowledgecenter/SSEPGG/welcome.

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

Exporting DB2 Universal Database data:

DB2 Universal Database provides a **DB2MOVE** utility. Use the export options provided with this utility to move data from a 5.0 or 5.1 system. to a 6.0 system before the upgrade.

About this task

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

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

These variables are required for the commands:

Table 31. Export command values

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

Each command creates these files:

Table 32. Export command output files

File name	Description
`EXPORT.out`	The summarized result of the EXPORT action.
`db2move.lst`	The list of original table names, their corresponding PC/IXF file names (`tab`*`nnn`*`.ixf`), and message file names `tab`*`nnn`*`.ixf`). This list, the exported PC/IXF files, and LOB files (`tab`*`nnn`*`c.`*`yyy`*) are used as input to the **db2move IMPORT** or **LOAD** action.
`tab`*`nnn`*`.ixf`	The exported PC/IXF file of a specific table. "*nnn*" is the table number.
`tab`*`nnn`*`.msg`	The export messages file of the corresponding table. "*nnn*" is the table number.

Table 32. Export command output files (continued)

File name	Description
tab*nnnc*.*yyy*.lob	The exported LOB files of a specific table. "*nnn*" is the table number. "*c*" is a letter of the alphabet. "*yyy*" is a number that ranges 001 - 999. These files are created only if the table that is being exported contains LOB data.

Procedure

1. Log in as the root user to the system on which the DB2 database is installed.
2. Go to *DB2 installation directory*/bin directory. Ensure that the /bin directory does not contain tabnn.msg, tabnn.ixf, db2move.lst, IMPORT/EXPORT.out, or tab*.lob files that are generated as part of any previous import or export activity. If such files are present, you can move them to different directory.
3. Type and run the command on one line.

   ```
   ./db2move source database name export –u database user name -p database user password
   -tn RESOURCE_PROVIDERS,LCR_INPROGRESS_TABLE,PO_TOPIC_TABLE,SCHEDULED_MESSAGE,NEXTVALUE,
   PROCESS,SYNCH_POINT,PASSWORD_TRANSACTION,LISTDATA,REPORT,ENTITY_COLUMN,COLUMN_REPORT,
   AUTHORIZATION_OWNERS,ACI,ACI_ROLEDNS,ACI_PRINCIPALS,ACI_PERMISSION_ATTRIBUTERIGHT,
   ACI_PERMISSION_CLASSRIGHT,ENTITLEMENT,ENTITLEMENT_PROVISIONINGPARAMS,
   SYNCHRONIZATION_HISTORY,SYNCHRONIZATION_LOCK,RESOURCES_SYNCHRONIZATIONS,CHANGELOG,
   SERVICE_ACCOUNT_MAPPING,RECONCILIATION,AUTH_KEY,POLICY_ANALYSIS,COMPLIANCE_ALERT,
   AUDIT_EVENT,I18NMESSAGES,BULK_DATA_SERVICE,MIGRATION_STATUS,
   RECERTIFICATIONLOG,SCRIPT,MANUAL_SERVICE_RECON_ACCOUNTS,VIEW_DEFINITION,COMMON_TASKS,
   SUMMARY_ORDER,PASSWORD_SYNCH,ROLE_INHERITANCE,SOD_POLICY,SOD_VIOLATION_HISTORY,
   SOD_VIOLATION_STATUS,RECERTIFIER_DETAILS_INFO
   ```

   The output files are created in the *DB2 installation directory*/bin directory.
4. Move these files into a separate folder, such as /parent_export.
5. Type and run the command on one line.

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

   The output files are created in the *DB2 installation directory*/bin directory.
6. Move these files into a separate folder, such as /child1_export.
7. Type and run the command on one line.

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

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

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

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

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

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

10. Move these files into a separate folder, such as /child3_export.
11. Go to ITIM_HOME/config/rdbms/db2 directory and copy enrole_admin.sql, enrole.ddl, and itim_sib.ddl to a directory, such as /DDL_Files.

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

What to do next

Create the database and copy the exported data to it.

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

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

Before you begin

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

About this task

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

Table 33. Command values

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

Procedure

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

   See "Database installation and configuration" on page 15. Because this operation is a migration, ensure that you create the same 5.0 or 5.1 database system user, for example, `itimuser`. The user must have the same rights and privileges it had on the old system.
2. Run the middleware configuration tool to create the DB2 instance.

   See "Running the middleware configuration utility" on page 19. When you run the middleware configuration tool to configure DB2 Universal Database, the database user field is set to `itimuser` as a default value. Modify the database user field to the same database user that is used in your previous Tivoli Identity Manager database. Use the same database user name and the password that is used in Tivoli Identity Manager Version 5.0 or 5.1. This name is the schema name and the password is already saved in properties files in the *OLD_ITIM_HOME*`\data` directory. These values cannot be changed during the upgrade.
3. Copy the DDL and SQL files from the `/DDL_Files` directory that you created in the "Exporting DB2 Universal Database data" on page 253 procedure. Put them in any directory on the target computer. In this case, the X86Linux system, which uses the little endian format.
4. Go to the DB2 installation directory/bin directory and connect to the database that you created. Run the command

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

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

   ```
   db2 disconnect all
   ```
7. Go to the DB2 installation directory/bin directory and connect to the database that you created. Run the command

   `db2 connect to` *database name* `user` *database user name* `using` *database user password*
8. Run the `enrole.dll` file that you copied in step 3. Run the command:

   `db2 -tf` *directory path*`/enrole.dll`
9. Disconnect from the database. Run the command:

   ```
   db2 disconnect all
   ```

What to do next

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

Importing the data to the X86Linux DB2 setup from the Linux on z System platform:

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

Before you begin

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

About this task

Use the procedure to import the data from the directories that you created on your Linux for System z operating system for "Exporting DB2 Universal Database data" on page 253. The commands correspond to the export commands that you ran in that procedure. Run the commands in sequence. Perform these steps on the X86Linux system DB2 setup.

These variables are required for the commands:

Table 34. Import command values

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

Each command creates these files:

Table 35. Import command output files

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

Procedure

1. Log in as the root user to the X86Linux system on which the new DB2 database is installed.
2. Go to the *DB2 installation directory*`/bin` directory. All the actions must be done in this directory.
3. Copy the data from the `/parent_export` directory that you created into the *DB2 installation directory*`/bin` directory.
   a. Type and run the command on one line.
      ```
      ./db2move <target database name> import –u <database user name> –p <database user password>
      ```
      The output files are created in the *DB2 installation directory*`/bin` directory.
   b. Move these files into a separate folder, such as `/parent_import`.
   c. Remove `tabnn.ixf` and `db2move.lst` files from the *DB2 installation directory*`/bin` directory.
4. Copy the data from the `/child1_export` directory that you created into the *DB2 installation directory*`/bin` directory.
   a. Type and run the command on one line.
      ```
      ./db2move <target database name> import –u <database user name> –p <database user password>
      ```
      The output files are created in the *DB2 installation directory*`/bin` directory.

b. Move these files into a separate folder, such as /child1_import.
c. Remove tabnn.ixf and db2move.lst files from the *DB2 installation directory*/bin directory.

5. Copy the data from the /child2_export directory that you created into the *DB2 installation directory*/bin directory. Type and run the command on one line.

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

a. Type and run the command on one line.

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

The output files are created in the *DB2 installation directory*/bin directory.
b. Move these files into a separate folder, such as /child2_import.
c. Remove tabnn.ixf and db2move.lst files from the *DB2 installation directory*/bin directory.

6. Copy the data from the /child3_export directory that you created into the *DB2 installation directory*/bin directory. Type and run the command on one line.

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

a. Type and run the command on one line.

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

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

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

What to do next

You can now use this database for Security Identity Manager migration. See "Upgrade to IBM Security Identity Manager 6.0" on page 271

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

Use these tasks to migrate DB2 Universal Database data to a version that Security Identity Manager Version 6.0 supports.

Backing up DB2 Universal Database data:

DB2 Universal Database provides backup and restore commands. Use these commands to move data from the 5.0 or 5.1 system to the 6.0 system before the upgrade.

Before you begin

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

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

Procedure

1. Open a DB2 command window.
   - UNIX and Linux: Log on as the DB2 instance owner and enter `db2` to open a DB2 command window.
   - Windows: Click **Start** > **Run**, and enter `db2cmd`. When the DB2 command window opens, enter `db2`.
2. Close all connections to the Tivoli Identity Manager database (stop WebSphere and any other tools).
   - When upgrading on a WebSphere single server, stop the Tivoli Identity Manager application and the WebSphere server on which the Tivoli Identity Manager application is running.
   - When upgrading on a WebSphere cluster, stop the Tivoli Identity Manager application and the WebSphere cluster on which the Tivoli Identity Manager application is running.
   - If necessary, run this command to force all connections to close:

     ```
     force application all
     ```
3. Back up the Tivoli Identity Manager database.

   Issue the command:

   ```
   backup database ITIM_DB to OLD_DB2_BACKUP_DIR
   ```

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

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

What to do next

Install the new version of DB2 Universal Database.

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

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

Before you begin

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

Procedure

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

   See *Installing and configuring the IBM(r) DB2(r) database* in the *IBM Security Identity Manager Installation Guide* on the Security Identity Manager product documentation site. Because this operation is a migration, ensure that you create the same 5.0 or 5.1 database system user, for example, `enrole`. The user must have the same rights and privileges it had on the old system.
2. Run the middleware configuration tool to create the DB2 instance.

   See "Running the middleware configuration utility" on page 19. When you run the middleware configuration tool to configure DB2 Universal Database, the database user field is set to `itimuser` as a default value. Modify the database user field to the same database user that is used in your previous Tivoli Identity Manager database. Use the same database user name and the password that is used in Tivoli Identity Manager Version 5.0 or 5.1. This name is the schema name and the password is already saved in properties files in the *OLD_ITIM_HOME*`\data` directory. These values cannot be changed during the upgrade.
3. Copy the contents of the Tivoli Identity Manager database backup directory to the target server, for example `/60data/db2`. Ensure that the database instance owner you create has permission to read the target directory and subfiles.

What to do next

Restore data to the new version of DB2 Universal Database.

Restoring the DB2 Universal Database data:

DB2 Universal Database provides restore commands. Use these commands to restore saved data from the 5.0 or 5.1 system to the 6.0 system after the upgrade.

Before you begin

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

About this task

DB2 Universal Database provides backup and restore commands. Use these commands to move data from the 5.0 or 5.1 system to the 6.0 system before the upgrade.

Procedure

1. Open a DB2 command window.
   - UNIX and Linux: Log on as the DB2 instance owner and enter `db2` to open a DB2 command window.

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

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

   ```
   restore db itimdb from OLD_DB2_TEMP_DATA
   ```

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

3. Stop and start the DB2 server to reset the configuration. Enter the following commands:

   ```
   db2stop
   db2start
   ```

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

   a. `force application all`

      This command deactivates the database.

   b. `db2start`.

What to do next

Tune the database for optimal performance by applying the latest tuning settings. See the Tuning IBM DB2 section of the Security Identity Manager Performance Tuning Guide for details.

For information about backup and restore of DB2 Universal Database, see the DB2 section of the IBM Knowledge Center.

Clearing the service integration bus:

When you upgrade from Tivoli Identity Manager 5.0 or 5.1 running on WebSphere Application Server 6.1 to Security Identity Manager Version 6.0 on WebSphere Application Server 7, you must clear the Service Integration Bus (SIB) data from the restored database.

Before you begin

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

Ensure that the Security Identity Manager database is running.

Procedure

1. Open a DB2 command window.
   - UNIX or Linux: Log on as the DB2 instance owner and enter `db2` to open a DB2 command window.
   - Windows: Click **Start** > **Run**, and enter `db2cmd`. When the DB2 command window opens, enter `db2`.
2. Connect to the database as the DB2 instance owner by using the command:

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

   where:

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

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

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

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

   The SIB schema, *schema_name* is:

   Table 36. Service integration bus schema names

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

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

Oracle database migration

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

Exporting Oracle data

The Oracle database export (EXP) and import (IMP) utilities are used to back up the logical database and recovery. They are also used to migrate Oracle data from one server, database, or schema to another.

Before you begin

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

Procedure

1. On the server that runs Oracle database for Tivoli Identity Manager Version 5.0 or 5.1, log in as the Oracle database instance owner.
2. Ensure that the *ORACLE_HOME* and *ORACLE_SID* environment variables are set correctly. *ORACLE_HOME* is the Oracle default installation directory. *ORACLE_SID* is the Tivoli Identity Manager database instance.
   a. Check your environmental variables for the following entries This example is for a Windows home directory.

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

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

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

   The *system_pwd* is the password for the system user. The *path* is the path of the file, such as `C:\51data\oracle` or `/opt/51data/oracle`. The *itim_username* is the Tivoli Identity Manager Version 5.0 or 5.1 database user, such as `enrole` or `itimuser`.
4. Copy the contents of the directory you exported over to the target server, for example `/61data/oracle`. Ensure that the database instance owner `enrole` that you created has permission to read the target directory and subfiles.

What to do next

Install the new version of Oracle database.

Installing Oracle database and importing data

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

Before you begin

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

Procedure

1. On the target Security Identity Manager Version 6.0 server, install the supported version of Oracle database. See “Installation and configuration of the Oracle database” on page 27 in the *IBM Security Identity Manager Installation Guide* on the Security Identity Manager product documentation site.
2. Configure the Oracle database instance. The following `enrole_admin.sql` file helps to configure the new Oracle database instance for the migration. Replace *itimuserTag* with your Tivoli Identity Manager Version 5.0 or 5.1 database user, such as `enrole`. Replace *itimuserPwdtag* with the Tivoli Identity Manager Version 5.0 or 5.1 database user password. If the database user ID and password are not the same as the previous version, the Security Identity Manager upgrade fails.

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

   CREATE TABLESPACE enrole_indexes
   DATAFILE 'enrole1_idx_001.dbf'
   SIZE 32M
   AUTOEXTEND ON
   NEXT 32M
   MAXSIZE unlimited
   ```

```
DEFAULT STORAGE (INITIAL 10M
                                 NEXT 1M
                                 PCTINCREASE 10)
PERMANENT
ONLINE
LOGGING;
CREATE USER itimuserTag IDENTIFIED BY itimuserPwdtag
  DEFAULT TABLESPACE enrole_data
  QUOTA UNLIMITED ON enrole_data
  QUOTA UNLIMITED ON enrole_indexes;
GRANT CREATE SESSION TO itimuserTag;
GRANT CREATE TABLE to itimuserTag;
GRANT CREATE ANY PROCEDURE to itimuserTag;
GRANT CREATE VIEW to itimuserTag;
```

3. Ensure that the *ORACLE_HOME* and *ORACLE_SID* environment variables are set correctly. *ORACLE_HOME* is the Oracle default installation directory. *ORACLE_SID* is the Tivoli Identity Manager database instance.
4. Run the preceding `enrole_admin.sql` file with the **sqlplus** utility.

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

   The *system_pwd* is the password for the system user. The *path* is the path of the file. Running this script file creates the required Security Identity Manager table spaces and creates the database user (specified by itimuserTag) with required permissions.
5. After creating the table spaces, enter the following command on one line to import the Tivoli Identity Manager Version 5.0 or 5.1 exported data:

   ```
   imp system/system_pwd file=path\itim51.dmp log=path\itim516exp.log
    fromuser=itim_username
   ```

   The *system_pwd* is the password for the system user. The *path* is the path of the file, such as `C:\51data\oracle` or `/opt/51data/oracle`. The *itim_username* is the Tivoli Identity Manager Version 5.0 or 5.1 database user, such as `enrole` or `itimuser`.

What to do next

After you complete the upgrade and installation, you must tune the database for optimal performance by applying the latest tuning settings. See the Tuning Oracle section of the Security Identity Manager Performance Tuning Guide for details.

Clearing the service integration bus

For Separate Systems Upgrades from Tivoli Identity Manager 5.0 or 5.1 to Security Identity Manager Version 6.0, you must clear out the Service Integration Bus (SIB) data from the restored database.

Before you begin

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

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

Ensure that the Security Identity Manager database is running.

Procedure

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

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

   The SIB schema, *schema_name* is:

Table 37. Service integration bus schema names

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

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

What to do next

Migrate the directory server.

SQL Server migration

Use these tasks to import Microsoft SQL Server data to a system and version of SQL Server that Security Identity Manager Version 6.0 supports.

Backing up SQL Server data

Use the Microsoft SQL Server backup and restoration utilities to move SQL Server data from one server, database, or schema to another. Move the data from the 5.0 or 5.1 system to the 6.0 system before the upgrade.

Before you begin

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

Procedure

1. On the server that runs SQL Server for Tivoli Identity Manager Version 5.0 or 5.1, start Microsoft SQL Server Management Studio and go to the Tivoli Identity Manager database.
2. Right click the Tivoli Identity Manager database (`itimdb`) and select **Tasks** > **Backup**.
3. Click **Add** to provide a file name such as `itimdb.bak`.

4. Accept the defaults for the other options, and click **OK**.

What to do next

Continue with "Installing SQL Server and importing data."

Installing SQL Server and importing data

Install the required level of Microsoft SQL Server.

Before you begin

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

Procedure

1. On the server that runs SQL server for Security Identity Manager, install SQL Server 2008.

   Use the same Tivoli Identity Manager Version 5.0 or 5.1 database system user on the new system.
2. After creating the Security Identity Manager Version 6.0 database, right click the database and click **Tasks** > **Restore** > **Database**
3. In the Restore Database window under the General page:
   a. Select the **From device** source for restore option.
   b. Click the ellipsis (**...**).
   c. Click **Add**.
   d. Select the **Restore** check box for the Tivoli Identity Manager Version 5.0 or 5.1 database backup file name (`itimdb.bak`).
4. On the Options page:
   a. Select **Overwrite the existing database option**.
   b. Click **OK**.
5. Configure SQL Server database for IBM Security Identity Manager Version 6.0.
   a. Start the SQL Server Enterprise Manager.
   b. Go to the database used for IBM Security Identity Manager Version 6.0
   c. Right click the database and click **New Query**.
   d. Enter the following user scripts to configure SQL:

      ```
      sp_addlogin itimuserTag, itimuserPwdTag;
      sp_adduser itimuserTag, itimuserTag, db_owner;
      use master;
      sp_grantdbaccess itimuserTag, itimuserTag;
      sp_addrolemember [SqlJDBCXAUser], itimuserTag;
      use itimdbTag;
      sp_change_users_login  'Update_One', 'itimuserTag', 'itimuserTag'
      ```

      - Replace *itimuserTag* with your Tivoli Identity Manager Version 5.0 or 5.1 database user. For example `enrole`.
      - Replace *itimuserPwdTag* with the Tivoli Identity Manager Version 5.0 or 5.1 database user password.
      - Replace *itimdbTag* with the database instance name.

      Note: The *itimuserTag* database might already be restored with database *itimdbTag*. If it is restored and the user script fails, you can ignore the failure.
6. Restart SQL Server 2008.

What to do next

Continue with "Clearing the service integration bus."

Clearing the service integration bus

Clear the Service Integration Bus (SIB) data from the restored database.

Before you begin

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

Verify that the Security Identity Manager database is running.

Procedure

1. On the server that runs SQL Server for Security Identity Manager Version 6.0, start the Microsoft SQL Server Management Studio.
2. Go to the database used for Security Identity Manager Version 6.0.
3. Right click the database and click **New Query**.
4. Enter the DELETE SQL statements required to delete all data from the tables in the SIB schemas.

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

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

   The SIB schema, *schema_name* is:

Table 38. Service integration bus schema names

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

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

What to do next

Upgrade the directory server.

Directory server migration

Security Identity Manager Version 6.0 supports data migration from most directory servers supported on Tivoli Identity Manager Version 5.0 or 5.1.

See *Directory server requirements* in the *IBM Security Identity Manager Product Overview Guide* on the Security Identity Manager product documentation site.

Tivoli Directory Server migration

Use these tasks to migrate Tivoli Directory Server data to a version that Security Identity Manager Version 6.0 supports.

Tivoli Identity Manager Version 5.0 supports IBM Tivoli Directory Server Version 6.0, 6.1, and 6.2. Tivoli Identity Manager Version 5.1 supports IBM Tivoli Directory Server Version 6.1, 6.2, and 6.3. You must migrate your directory server data to a version that Security Identity Manager Version 6.0 supports.

See *Directory server requirements* in the *IBM Security Identity Manager Product Overview Guide* on the Security Identity Manager product documentation site.

Backing up directory server data

Export the directory server data to a file before moving to a directory server version that Security Identity Manager Version 6.0 supports.

Procedure

1. Log in as an administrator with root privileges.

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

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

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

What to do next

Continue with "Installing Tivoli Directory Server on the target server."

Installing Tivoli Directory Server on the target server

Install a version of IBM Security Directory Server that Security Identity Manager Version 6.0 supports.

Before you begin

Verify that your directory server data is backed up.

Procedure

1. Log on as an administrator with root privileges, on the target Security Identity Manager Version 6.0 server.
2. Install the supported version of IBM Security Directory Server.

   See Installation and configuration of IBM Tivoli Directory Server.

3. Run the middleware configuration tool to create the IBM Security Directory Server instance.

   See "Running the middleware configuration utility" on page 19.

   - Ensure that the same Tivoli Identity Manager Version 5.0 or 5.1 root suffix is created and used.
   - Use the same encryption seed value as the old Security Directory Server instance. Otherwise the data from the old Security Directory Server instance must be exported to use the seed and salt keys from the new instance.
4. Copy the schema file `V3.modifiedschema` from the *OLD_ITDS_INSTANCE_HOME*`\etc` directory of the Security Directory Server instance home directory used by Tivoli Identity Manager Version 5.*x* server. Paste the file to the *NEW_ITDS_INSTANCE_HOME*`\etc` directory of the Security Directory Server instance that the Security Identity Manager Version 6.0 server uses.

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

What to do next

Continue with "Importing directory server data."

Importing directory server data

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

Procedure

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

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

   Where:

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

Results

When running the bulkload command, the following errors might occur.

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

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

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

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

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

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

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

   Where:

   – *bind DN* is the distinguished name (DN) of the directory server
   – *password* is the DN password
   – *hostname* is the name of the computer where Security Directory Server is installed
   – *port* is the port number on which Security Directory Server is listening
2. Replace the value of *ibm-slapdCryptoSync*, *ibm-slapdCryptoSalt* with the values returned by the **ldapsearch** command in the *ldap_output_file* file. This file is generated as output of the **db2ldif** command, for example *old_ldif_data.ldif*.
3. Run the **bulkload** command again.

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

What to do next

Tune LDAP for optimal performance by applying the latest tuning settings. See *Tuning Tivoli Directory Server* in *Security Identity Manager Performance Tuning Guide*..

Oracle directory server data migration

Use these tasks to migrate Oracle (formerly Sun) directory server data to a version that IBM Security Identity Manager Version 6.0 supports.

See *Directory server support* in the *IBM Security Identity Manager Product Overview Guide* on the IBM Security Identity Manager product documentation site.

For complete information about migrating Oracle directory servers to Oracle Directory Server Enterprise Edition 6.3.1, 7.0, or 11.1.1, see to the Oracle website at http://www.oracle.com.

Installing Sun Directory Server Enterprise Edition and importing data on the same system

After backing up your directory server data, install a version of Sun Directory Server Enterprise Edition that IBM Security Identity Manager Version 6.0 supports.

Before you begin

View *Directory server support* in the *IBM Security Identity Manager Product Overview Guide* on the Security Identity Manager product documentation site.

Ensure that you back up your directory server data.

You must be logged in as an administrator with root privileges.

Procedure

1. Install the supported version of Sun Directory Server Enterprise Edition (on the same system) and create an LDAP instance. For example:

   ```
   DSEE7.0_HOME/bin/dsadm create -p 389 -P 636 /export/home/itimldap
   ```

2. Create a root suffix that is the same as the root suffix of the previous version of Sun ONE Directory Server. For example:

   ```
   DSEE7.0_HOME/bin/dsconf create-suffix -h localhost -p 389 -e dc=com
   ```

3. Use the **dsmig** command to migrate the schema, configuration, and data on the same system. For example:

   ```
   DSEE7.0_HOME/bin/dsmig migrate-schema old-instance-path new-instance-path
   DSEE7.0_HOME/bin/dsmig migrate-config old-instance-path new-instance-path
   DSEE7.0_HOME/bin/dsmig migrate-data old-instance-path new-instance-path
   ```

   You can also use a single command to migrate the schema, configuration, and data on the same system. For example:

   ```
   DSEE7.0_HOME/bin/dsmig migrate-all old-instance-path new-instance-path
   ```

What to do next

After you complete the upgrade and installation of Security Identity Manager, tune LDAP for optimal performance by applying the latest tuning settings. See *Tuning Sun Enterprise Directory Server* in the *Performance* topic on the Security Identity Manager product documentation site.

Upgrade to IBM Security Identity Manager 6.0

The following sections provide information about how to upgrade to Security Identity Manager Version 6.0, both for single-server and cluster environments.

The supported upgrade paths are:

Table 39. Upgrade paths to Security Identity Manager Version 6.0

From	To
Tivoli Identity Manager Version 5.0 that is deployed on WebSphere Application Server 6.1	Security Identity Manager Version 6.0 that is deployed on WebSphere Application Server 7.0
Tivoli Identity Manager Version 5.1 that is deployed on WebSphere Application Server 6.1 or WebSphere Application Server 7.0	Security Identity Manager Version 6.0 that is deployed on WebSphere Application Server 7.0
Security Identity Manager Version 6.0 that is deployed on WebSphere Application Server 7.0	Security Identity Manager Version 6.0 that is deployed on WebSphere Application Server 8.5

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

To run the installation program to upgrade to Security Identity Manager Version 6.0, copy the existing Tivoli Identity Manager home directory to the target environment.

Before you begin

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

About this task

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

Procedure

1. Copy the directory.
   - For UNIX or Linux systems
     a. Go to the UNIX or Linux root directory.
     b. Create a .tar file by entering the full path of *OLD_ITIM_HOME*. For example,

        ```
        tar –cvf itim.tar OLD_ITIM_HOME
        ```

        If you are running Security Identity Manager in a cluster environment, create separate .tar files for the deployment manager and cluster members.
     c. Copy the itim.tar file to the target server root directory. For a cluster environment, copy the .tar file from the old deployment manager to the new deployment manager and old cluster members to new cluster members.
     d. Extract the *OLD_ITIM_HOME* directory on one or more servers with the following command:

        ```
        tar –xvf itim.tar
        ```
   - For Windows systems
     a. Create a compressed file of the *OLD_ITIM_HOME* directory. For a cluster environment, create separate compressed files for the deployment manager and cluster members.
     b. Copy the compressed file to the target server. For a cluster environment, copy the compressed file from the old deployment manager to the new deployment manager and old cluster members to new cluster members.
     c. Extract the *OLD_ITIM_HOME* directory on one or more servers to the same drive location where Security Identity Manager is installed.
2. If you plan to upgrade an existing Security Identity Manager 6.0 from a WebSphere Application Server 7.0 environment to a new Security Identity Manager 6.0 in a WebSphere Application Server 8.5 environment, perform the following steps. The upgrade uses the InstallAnywhere Graphic User Interface that is provided with the GA version of the Security Identity Manager Version 6.0 product.

a. Prepare your new Security Identity Manager 6.0 in a WebSphere Application Server 8.5 environment. The best practice is to use the same directory that was previously used on the system. For example, if you used `C:\Program Files (x86)\IBM\isim` as the installation directory, you must use that same path on the target system. It minimizes the number of changes in your upgrade process.

b. Update `ITIM.product` file in your `<itim_home>/properties/version` directory:
   1) Locate `<version>6.0.0.0</version>`.
   2) Change only the version information from <version>6.0.0.0</version> to <version>5.2.0.0</version>.
   3) Save and exit the file.

c. Change the directory to the `<itim_home>/data` directory and back up any files that must be merged during the installation.

d. Create a backup copy of the existing files with only the .bak extension for:
   1) `copy encryptionKey.properties encryptionKey.bak`.
   2) `copy enRole.properties enRole.bak`
   3) `copy KMIPServer.properties KMIPServer.bak`

e. Ensure that you have read and followed the instructions from the Chapter 16, "Separate system upgrade and data migration," on page 251 sections before you start the InstallAnywhere installer for Security Identity Manager.

What to do next

Run the Security Identity Manager installation program.

Running the Security Identity Manager installation program

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

Before you begin

Before you run the Security Identity Manager Version 6.0, installation program. Ensure that you imported or restored the directory and database data you copied onto the respective directory and database servers. Additionally, ensure that the following middleware is running at the supported release level and fix pack:

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

See *Hardware and software requirements* in the *IBM Security Identity Manager Product Overview Guide* on the Security Identity Manager product documentation site. For instructions about installing and configuring these middleware products, see Chapter 4, "Installation of prerequisite components," on page 13 on the Security Identity Manager product documentation site.

About this task

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

To upgrade to Security Identity Manager Version 6.0:

Procedure

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

        AIX systems
        ```
        instaix.bin
        ```

        Linux systems
        ```
        instlinux.bin
        ```

        zLinux systems
        ```
        instzlinux.bin
        ```

        Note: To run the installation program on a UNIX or Linux system, you need at least 150 MB of free space in the `/tmp` directory. If you do not have sufficient space, set the IATEMPDIR environment variable to a directory on a disk partition with enough free disk space. To set the variable, enter one of the following commands at the command-line prompt before running the installation program again.

        Bourne shell (sh), ksh, bash, and zsh
        ```
        $ IATEMPDIR=temp_dir
        $ export IATEMPDIR
        ```

        C shell (csh) and tcsh
        ```
        $ setenv IATEMPDIR temp_dir
        ```

        temp_dir is the path to the directory, for example `/your/free/directory`, where free disk space is available.

     The Welcome window opens.
4. Select the language and click **OK**.
5. If you agree with the terms, accept the license agreement and click **Next**.

6. In the Choose Install Directory window, you must select the existing Tivoli Identity Manager home directory that you want to upgrade. Accept the default directory, or click **Choose** and select the correct directory. Then, click **Next**.
7. In the Upgrade Security Identity Manager window, click **Continue to Next** to start the upgrade.
8. Read the caution windows to ensure that the prerequisite applications meet the requirements that Security Identity Manager supports. Then, click **Next**.
9. In the Installation Directory of WebSphere Application Server window, confirm the WebSphere Application Server directory and click `Next`.
10. In the WebSphere Profile Selection window, select the WebSphere Application Server profile name, and click **Next**.
11. If you are running Security Identity Manager in a cluster environment, enter the application and messaging cluster names, and click **Next**.

    Note: The cluster names you enter do not have to match the previous version of Tivoli Identity Manager, but they must exist from the configuration of WebSphere Application Server. For more information about configuring WebSphere Application Server for Security Identity Manager, see "Installation and configuration of WebSphere Application Server" on page 51 on the Security Identity Manager product documentation site.
12. In the WebSphere Application Server Data window, enter or accept the application server name. Ensure that the correct host name for the new computer is shown, and click **Next**.
13. If you are running Security Identity Manager in a cluster environment, verify the host name of the system on which WebSphere Application Server and Security Identity Manager are to be installed. Click **Next**.
14. If WebSphere administrative security and application security is turned on, in the WebSphere Application Server Administrator Credentials window, enter the WebSphere Application Server administrator user ID and password, and click **Next**.
15. If you are prompted for the Java Database Connectivity (JDBC) driver, enter the directory location for the JDBC driver and the driver name, and click **Next**.

    Note: If you are upgrading from Tivoli Identity Manager 5.1 to Security Identity Manager 6.0 on WebSphere Application Server 7.0, the JDBC driver setup panel is not displayed. Additional manual steps are needed for the Oracle database.

    a. After deploying Tivoli Identity Manager 5.1 on WebSphere Application Server 7.0 Fix Pack 5, remove the ojdbc.jar file from *ISIM_HOME*`/lib` and replace it with ojdbc6.jar. Then, rename ojdbc6.jar to ojdbc.jar. This renaming is necessary because WebSphere Application Server 7.0 uses JDK1.6.
16. In the Tivoli Common Directory window, select the location of the Tivoli Common Directory or another directory, and click **Next**. The directory you select is the central location for all serviceability-related files, such as logs and first-failure capture data.
17. In the Pre-Installation Summary window, verify that the information is correct and click **Install**.
18. When the System Configuration tool window is shown on the screen, enter the correct values for Security Identity Manager Version 6.0. Confirm or update the correct values for the following directory, database, and mail

server fields on each tab. These values must be changed from the old information used in the previous version of Tivoli Identity Manager.

- Database
  - JDBC URL

    Enter the JDBC URL with the correct database host name, port number, and database name for Security Identity Manager Version 6.0. For example, if you are using the DB2 database “itimdb” running at the host 10.1.1.1 on port 50000, then you enter:jdbc:db2://10.1.1.1:50000/itimdb

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

  After you enter the information, click **Test** to test the connection.

  Note: The Database User and User Password fields are disabled. When you create the database user for Security Identity Manager Version 6.0, make sure that you use the same database user ID and password that you used for the previous Tivoli Identity Manager server.
- Directory
  - Principal DN
  - Password
  - Host Name
  - Port

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

19. Click **OK** after you change or verify all the fields on all the tabs. The database upgrade program is started to upgrade the database schema and data. The database upgrade can take some time to complete, and progress is not displayed. After it is complete, the LDAP upgrade program is started to upgrade the LDAP schema and data. This upgrade can also take some time. You can look at the log files in the *ISIM_HOME*\install_logs directory to see the upgrade progress, specifically the following log files:
    - itim_install_activity.log
    - dbUpgrade.stdout
    - ldapUpgrade.stdout
    - runConfigFirstTime.stdout
20. When the installation program is finished, click **Done**.

What to do next

Confirm you can log on to the Security Identity Manager Version 6.0 system. Use the user ID and the password that was used in the previous version of Tivoli Identity Manager to log on.

Post-installation tasks

Perform these tasks after you migrated to Security Identity Manager Version 6.0.

Reinitialization of the configuration for authentication with an external user registry

If you migrated your existing Version 6.0 installation from WebSphere Application Server Version 7 to Version 8.5, the following information applies.

If you used the procedures in "Upgrade to IBM Security Identity Manager 6.0" on page 271 to migrate, you must reconfigure the security domain.

The migration of Version 6.0 from WebSphere Version 7 to a WebSphere Version 8.5 environment, resets the external user registry to ISIM security. To configure your system to use the external user registry again, you must reconfigure the security domain on WebSphere. See "Reconfiguration of a WebSphere security domain" on page 219.

Restarting and reindexing Sun Enterprise Directory Server Version 6.3.1 and 7.0

Use this task to enable Security Identity Manager Version 6.0 to connect to your Sun Enterprise Directory Server.

Before you begin

The Security Identity Manager Version 6.0 must be installed.

About this task

If you migrated data from Sun ONE Directory Server, after the Security Identity Manager Version 6.0 installation is completed, you must stop Security Identity Manager. Start your directory server and then reindex the directory server. Otherwise Security Identity Manager cannot connect to the directory server.

To reindex Sun Enterprise Directory Server:

Procedure

1. From the Sun Enterprise Directory Server console, click the **Configuration** tab.
2. Reindex the directory server.
   a. Select the directory server.
   b. Open the **Data** tree.
   c. Click the exported root suffix.
   d. Select **Reindex**.
3. Select **Check All**.
4. Click **OK**.

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

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

About this task

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

Procedure

1. From the administrative console, click **Environment** > **Virtual Hosts** > **default_host** > **Host Aliases**.
2. In Host Aliases, click **New** to create an alias.

3. In the **Host Name** field, enter *, and in the **Port** field, enter the port number and click **OK**.

   Note: To find the default host port, click **Servers** > **Applications Servers** > **ServerName** > **ports**. Look for the values of WC_defaulthost and WC_defaulthost_secure, where serverName is the server name of the application cluster member where Security Identity Manager is deployed.
4. Save the configuration changes.
5. Complete a Full Synchronization of the WebSphere Application Server nodes.

Preserving custom logos

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

The `ui.properties` file property named `enrole.ui.customerLogo.image` still points to the location specified in 5.0 or 5.1. However, this pointer defaults to a path inside the `enrole.ear` or `ITIM.ear` directory. You must copy the image file from the old location to the new location.

For information about customizing logos and style sheets, see "Manual preservation of the customized data" on page 243 on the Security Identity Manager product documentation site.

Verification of the installation

After you complete the installation, confirm that you can log on to the Security Identity Manager Version 6.0 system.

Log on to Security Identity Manager Version 6.0. Use the administrator user ID and password that was used in the previous version of Tivoli Identity Manager.

For more information about verifying the Security Identity Manager Version 6.0 installation, see "Verifying the installation" on page 19.

Performance tuning

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

For instance, on systems that run DB2 Universal Database, you might benefit from enabling autoresize on your table spaces. Although enabled is the default setting, verify that you have autoresize enabled. Issue the command:

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

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

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

Post-upgrade production cutover

This section provides information about how to conduct a post-upgrade production cutover.

While you are conducting the upgrade process and testing the new production system, the old production system continues to capture changes made in production. The Security Identity Manager upgrade does not provide a mechanism

to capture these changes and import them to the upgraded system that runs Version 6.0. Security Identity Manager does provide the capability to capture current data from the old production system and import it to the new environment without installing an entirely new Security Identity Manager 6.0 environment.

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

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

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

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

Production cutover roadmap

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

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

1. Shut down WebSphere Application Server on the new production environment.
2. Prepare the following new production servers for data import:
   - Directory server
   - Database server (preparing data is not necessary for DB2 Universal Database or SQL Server)
3. Shut down WebSphere Application Server on the old production environment.
4. Capture the data from the following old production servers:
   - Directory server
   - Database server
5. Import the Tivoli Identity Manager directory data from the old production environment to the new environment.
6. Import the Tivoli Identity Manager database data from the old production environment to the new environment.
7. Run the LDAP upgrade tool to migrate directory server data to Security Identity Manager Version 6.0.
8. Run the database upgrade tool to migrate database server data to Security Identity Manager Version 6.0.
9. Start WebSphere Application Server on the new production environment.
10. Apply performance tuning setting to directory and database servers.

Stop of WebSphere Application Server on the new production environment

Stop WebSphere Application Server on the new production environment.

Stop both the application server and the message server. If you are deploying into a WebSphere cluster environment, you must stop the application servers and message servers on all cluster members.

You can stop servers either by using the WebSphere console or by using commands from a command line. When working in a WebSphere cluster, it is easier to use the WebSphere console to stop the application and message servers.

Note: Optional: If your deployment includes an HTTP Server, stop the server.

WebSphere command-line commands:

- Windows

  WAS_PROFILE_HOME\bin\stopServer.bat *servername*
- UNIX or Linux

  WAS_PROFILE_HOME/bin/stopServer.sh *servername*

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

-user *WAS_username* - password *WAS_user_password*

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

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

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

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

Reconfiguring the IBM Tivoli Directory Server instance

You must configure your directory server instance to run in the Security Identity Manager Version 6 environment.

Before you begin

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

Procedure

1. Stop IBM Tivoli Directory Server.

   Issue this command.

   ibmslapd -I *ldap_instance_name* -k
2. Start the IBM Tivoli Directory Server Instance Administration tool.

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

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

   Additionally, choose to delete the database.
4. Run the Security Identity Manager middleware configuration utility to create an Security Identity Manager LDAP instance.

   Make the instance name and passwords the same as the previously created instance. For more information about creating the LDAP instance, see "Installing Tivoli Directory Server on the target server" on page 268.

Note: If you do not want to destroy the LDAP instance and run the middleware configuration utility again, you can reconfigure the database. Use the **idsxcfg** or **idsucfgdb** and **idscfgdb** commands. When you reconfigure the database, the tuning settings that were applied to the LDAP instance by the middleware configuration utility are not saved. You must update the database with the tuning settings. See the Database servers used with IBM Security Identity Manager section of the Security Identity Manager Performance Tuning Guide.

What to do next

Reconfigure the database instance.

Reconfiguring the Sun Enterprise Directory Server instance

You must configure your directory server instance to run in the Security Identity Manager Version 6 environment.

Before you begin

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

Procedure

1. Load the Sun Enterprise Directory Server console and log in as an administrator.
2. Select the migrated LDAP server and click **Open** to open the management console for the server.
3. Click the **Configuration** tab and expand the **Data** subtree.
4. Find the suffix that houses the current Security Identity Manager data, right click the suffix, and select **Delete**.
5. After the suffix is deleted, right click the **Data** subtree and click **New Suffix**. Then re-create the same suffix as before.
6. Stop the LDAP server.

What to do next

Reconfigure the database instance.

Reconfiguring the Oracle database instance

You must configure your database instance to run in the Security Identity Manager Version 6 environment.

Before you begin

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

Procedure

1. Use the **dbca** command or other tools to remove the Security Identity Manager database and instance that was created for the test environment.
2. After the database is removed, create a database with the same name by using the migration commands previously provided. For more information, see "Oracle database migration" on page 262.
3. Configure the Oracle database instance.

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

a. Edit the file.

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

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

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

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

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

4. Run the enrole_admin.sql file that you edited in the previous step with the **sqlplus** utility: sqlplus system/*system_pwd* @*path*\enrole_admin.sql . The system_pwd is the password for the system user. The *path* is the path of the file. Running this script file creates the required Security Identity Manager table spaces and creates the database user (enrole) with required permissions.

What to do next

Capture and import the old production server data.

Capturing and importing of the production server data

Use these tasks to transfer Tivoli Identity Manager 5.0 or 5.1 production server data to the new production environment.

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

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

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

Procedure

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

   For more information, see "Backing up directory server data" on page 268.
2. Copy the schema file `V3.modifiedschema` from the *OLD_ITDS_HOME*`\etc` directory of the IBM Tivoli Directory Server used by Tivoli Identity Manager version 5.0 or 5.1 server.
3. Paste the schema file `V3.modifiedschema` to the *NEW_ITDS_HOME*`\etc` directory of the IBM Tivoli Directory Server used by the Security Identity Manager version 6.0 server.
4. Import the directory server data.

   For more information, see "Importing directory server data" on page 269.

What to do next

Capture and import database information.

Capturing and importing the contents of the Sun Enterprise Directory Server production server data

Use this task to transfer Sun Enterprise Directory Server production server data to the new production environment.

Procedure

1. On the old production server, export the directory server data.
2. Copy the `99user.ldif` schema file from the *path*`/slapd-serverID/config/schema` directory to the Security Identity Manager version 6.0 server directory server schema directory.
3. Stop the LDAP server.
4. Run this command to import the data.

   ```
   ldif2db -n instance_name -i ldif_output_file
   ```

   The *instance_name* is the name of the old instance. The *instance_name* is the name of the file you exported from the previous version of Sun Enterprise Directory Server.

What to do next

Capture and import database information.

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

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

Procedure

1. Back up the DB2 Universal Database data.

   For more information, see "Backing up DB2 Universal Database data" on page 258.

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

   Ensure that the database instance owner `enrole` that you created previously has permission to read the target directory and files within.
3. Restore the database data. For more information.

   For more information, see "Restoring the DB2 Universal Database data" on page 260

What to do next

Clear the service integration bus.

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

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

Procedure

1. Export the Oracle database data. For more information. For more information, see "Exporting Oracle data" on page 262.
2. Enter this command on one line, to import the Tivoli Identity Manager Version 5.0 or 5.1 exported data.

   ```
   imp system/system_pwd file=path\itimxx.dmp log=path\itimxxexp.log
   fromuser=itim_username
   ```

   The *system_pwd* is the password for the system user. The *path* is the path of the file you copied. (For example C:*xx*data\oracle or /opt/*xx*data/oracle. *xx* is the version number of you previous version of Tivoli Identity Manager (5.0 or 5.1). The *itim_username* is the name of the Tivoli Identity Manager (5.0 or 5.1) database user, such as `enrole`.

What to do next

Run the upgrade commands.

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

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

Procedure

1. Export the SQL Server database.

   For more information, see "Backing up SQL Server data" on page 265.
2. On the new production server database, right-click the database and select **Tasks** > **Restore** > **Database**.
3. In the Restore Database, select the General page. Provide the Tivoli Identity Manager Version 4.6 database backup file name (`itimdb.bak`).
   a. Select the **From device** source for restore option.
   b. Click **ellipsis (...)**.
   c. Provide the Tivoli Identity Manager Version 5.*X* database backup file name (itimdb.bak).
4. After adding the backup file to the list, select the check box to select the file and click **Options** in the left pane.

5. On the Options page, select **Overwrite the existing database option** and click **OK**.
6. Configure SQL with the following user script:

   ```
   sp_addlogin itimuserTag, itimuserPwdTag;
   sp_adduser itimuserTag, itimuserTag, db_owner;
   use master;
   sp_grantdbaccess itimuserTag, itimuserTag;
   sp_addrolemember [SqlJDBCXAUser], itimuserTag;
   use itimdbTag;
   ```

   Replace *itimuserTag* with your Tivoli Identity Manager Version 5.*X* database user, for example `enrole`. Replace *itimuserPwdTag* with your Tivoli Identity Manager Version 5.*X* database user password. Replace *itimdbTag*with the database instance name.
7. Use this script to configure SQL.

   ```
   sp_change_users_login  'Update_One', 'itimuserTag', 'itimuserTag'
   ```

   Replace *itimuserTag* with your Tivoli Identity Manager Version 5.*X* database user, for example `enrole`.
8. Restart SQL Server 2008.

What to do next

Clear the service integration bus.

Clearing of the service integration bus

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

For Separate Systems Upgrades from Tivoli Identity Manager 5.*X* to Security Identity Manager 6.0 server, the Service Integration Bus (SIB) data from the restored database must be cleared out.

- For DB2 servers, see "Clearing the service integration bus" on page 261.
- For Microsoft SQL servers, see "Clearing the service integration bus" on page 267.

Commands to migrate directory and database data

Use these commands to upgrade imported data to the Security Identity Manager version 6.0 level.

After importing the directory and database data on the new production environment, run the **ldapUpgrade** and **DBUpgrade** utilities. Running these utilities upgrades imported data to the Security Identity Manager version 6.0 level. Depending on the size of the data pool, this process can take some time. To confirm that the upgrade is completed, you can check the `DBUpgrade.stdout` and `ldapUpgrade.stdout` log files in the *NEW_ISIM_HOME*`\install_logs` directory.

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

Continue with "Running ldapUpgrade and DBUpgrade."

Running ldapUpgrade and DBUpgrade

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

About this task

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

Procedure

1. Run the **ldapUpgrade** command.

   Windows operating systems
   NEW_ITIM_HOME\bin\ldapUpgrade

   UNIX or Linux operating systems
   NEW_ITIM_HOME/bin/ldapUpgrade

   Note: If Oracle Enterprise Directory Server is used, you must reindex the directory server. For more information, see "Restarting and reindexing Sun Enterprise Directory Server Version 6.3.1 and 7.0" on page 277.
2. Run the **DBUpgrade** command to upgrade the IBM Security Identity Manager database.

   Windows
   NEW_ITIM_HOME\bin\DBUpgrade

   UNIX or Linux
   NEW_ITIM_HOME/bin/DBUpgrade
3. Select one of the following options:
   - If you did not select to install Shared Access during the upgrade installation, the task is complete.
   - If you selected to install Shared Access during the upgrade installation, you must manually reconfigure it after the **ldapUpgrade** and **DBUpgrade** commands complete. Continue with Configuring shared access during upgrade on a WebSphere cluster.

Starting WebSphere Application Server

Start WebSphere Application Server to complete the production cutover.

About this task

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

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

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

Procedure

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

- Windows
  WAS_PROFILE_HOME\bin\startServer.bat *servername*
- UNIX or Linux

WAS_PROFILE_HOME/bin/startServer.sh *servername*

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

-user *WAS_username* - password *WAS_user_password*

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

What to do next

Perform new production environment post-cutover tasks.

New production environment post-cutover tasks

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

Restarting and reindexing Sun Enterprise Directory Server Version 6.3.1 and 7.0

Use this task to enable Security Identity Manager Version 6.0 to connect to your Sun Enterprise Directory Server.

Before you begin

The Security Identity Manager Version 6.0 must be installed.

About this task

If you migrated data from Sun ONE Directory Server, after the Security Identity Manager Version 6.0 installation is completed, you must stop Security Identity Manager. Start your directory server and then reindex the directory server. Otherwise Security Identity Manager cannot connect to the directory server.

To reindex Sun Enterprise Directory Server:

Procedure

1. From the Sun Enterprise Directory Server console, click the **Configuration** tab.
2. Reindex the directory server.
   a. Select the directory server.
   b. Open the **Data** tree.
   c. Click the exported root suffix.
   d. Select **Reindex**.
3. Select **Check All**.
4. Click **OK**.

LDAP recycle bin cleanup

If the `enrole.recyclebin.enable` property from `enRole.properties` is set to `false`, ensure that the recycle bin in LDAP is empty. Otherwise, previously deleted entities might be returned by searches.

If `enrole.recyclebin.enable` is set to `false`, the LDAP recycle bin might contain deleted entries after the upgrade. These entries were deleted from a previous version of Tivoli Identity Manager. They might be returned by Security Identity

Manager user interface when searching for entries. If this problem exists then you must delete all the entries from the recycle bin in LDAP server or set this property to `true`.

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

Verification of the installation

After you complete the installation, confirm that you can log on to the Security Identity Manager Version 6.0 system.

Log on to Security Identity Manager Version 6.0. Use the administrator user ID and password that was used in the previous version of Tivoli Identity Manager.

For more information about verifying the Security Identity Manager Version 6.0 installation, see "Verifying the installation" on page 19.

Performance tuning

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

For instance, on systems that run DB2 Universal Database, you might benefit from enabling autoresize on your table spaces. Although enabled is the default setting, verify that you have autoresize enabled. Issue the command:

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

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

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

Post migration troubleshooting and known issues

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

The following issues are known to occur after an upgrade to IBM Security Identity Manager version 6.0.

Default data does not get loaded

Some default data specific to IBM Security Identity Manager are not loaded at upgrade time.

For example, default access control items (ACIs) are not loaded. These items are not copied to prevent interference with ACIs from previous versions.

Additional files copied for services

If services point to a file on the file system such as an identity feed, copy the given file to the new IBM Security Identity Manager version 6.0 server. You must also update the service to point to the new file location on the IBM Security Identity Manager version 6.0 server. This document only instructs you to copy over the contents of the *OLD_ITIM_HOME* directory.

GetDN supported only on erPolicyMembership or erPolicyTarget

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

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

DB2 restoration error

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

Use the following commands, if you receive this error.

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

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

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

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

JavaScript from previous version returns empty

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

An explicit return statement is needed with the IBM JavaScript Engine. For more information, see *Migrating custom FESI extensions to the IBM(r) JSEngine* in the Reference section of the Security Identity Manager product documentation site.

Compilation failures

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

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

Cluster installation error

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

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

```
WASX7017E: Exception received while running file
   "C:\Program Files\IBM\itim\config\was\setEVCluster.jacl";
    exception information:
```

```
com.ibm.websphere.management.exception.ConfigServiceException
java.lang.reflect.UndeclaredThrowableException:
java.lang.reflect.UndeclaredThrowableException
```

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

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

Part 4. Appendixes

Appendix. User registry configuration for external user registry

If you want to use an external user registry for authentication, and do not already have a registry, you must create registry entries.

The topic "Preinstall configuration for authentication with an external user registry" on page 69 describes how to prepare an existing user registry for use as an external user registry for authentication. However, if you do not have an existing user registry, you must create one first. The instructions describe how to configure a new user registry so that it can be prepared for use as an external user registry for authentication.

These instructions present one example of how to configure a user registry by using the graphical administration tool for IBM Security Directory Server. Alternatively, you can use a command-line utility such as **ldapadd**. If you are using a different user registry product, your configuration steps can differ.

The task sequence is:

1. Create a suffix.

   The example uses a suffix `dc=mycorp`
2. Create a domain.

   The example uses a domain `dc=mycorp`.
3. Create a user template.
4. Create a user realm.

   The example uses a realm `dc=mycorp`. IBM Security Identity Manager requires two user accounts in the realm. The user accounts are an administrator user and a system user. For the administrative user, we use `ITIM Manager`. For the system user, we use `isimsystem`.

This example creates a suffix `dc=mycorp`.

To begin configuration, see "Creating a suffix."

Creating a suffix

You can use the IBM Security Directory Server Instance Administration utility to create a suffix.

Procedure

1. Start the IBM Security Directory Server Instance Administration tool.
2. In the Instance Administration tool, select the instance and click **Start/Stop...** to stop the server. The server must be stopped to create a suffix.
3. Click **Stop server** to stop the server. Click **Close** to close the Manage server state window.
4. In the Instance Administration tool, click **Manage....**
5. In the IBM Security Directory Server Configuration tool, go to **Manage suffixes**. In the Suffix DN field, enter the suffix name `dc=mycorp`. Click **Add** and click **OK**.

6. When the `dc=mycorp` suffix is added, start the IBM Security Directory Server server.

What to do next

Continue with the instructions in *Creating a domain, user template, and user realm*.

Creating a domain, user template, and user realm

You can use the IBM Security Directory Server web administration tool to create a domain, user template, and user realm.

About this task

This task shows how to use the graphical user interface.

If the web administration tool is not installed, see the IBM Security Directory Server documentation for installation instructions: http://www.ibm.com/support/knowledgecenter/SSVJJU/welcome?

Note: Alternatively, you can use an **`ldapadd`** command.

Procedure

1. Start the IBM Security Directory Server web administration tool and log on to your LDAP server as an administrator.
2. Go to **Directory management** > **Manage entries** and click **Add...** to create a domain.
3. In the Structural Object Class field, select **domain** and click **Next**.
4. On the Select auxiliary object classes panel, you do not need to specify any settings. Click **Next**.
5. On the Required Attributes panel, enter `dc=mycorp` in the **Relative DN** field. In the Required attribute section, in the **dc** field, enter `mycorp`. Click **Next**.
6. You do not need to set any values on the Optional attributes page. Scroll to the bottom of the panel and click **Finish**.
7. A confirmation page displays, and asks if you want to add a similar entry. Click **No** to go back to the Manage entries page.
8. On the Manage entries page, ensure that the `dc=mycorp` domain is created and listed in the RDN column.
9. Optionally, you can create a user template. If you do not want a user template, continue to the next step to create the user domain. To create a user template:
   a. Go to the **Realms and templates --> Manage user templates** page and click **Add...**.
   b. On the Add user template page, enter a name in the **User template name** filed and enter a value in the **Parent DN** filed. Click **Next**.

      For this example, **User template name** can be `mycorpUserTempl` and **Parent DN** is `dc=mycorp`.
   c. Select a value for the **Structural object class** for this user template. For this example, select menu item **inetOrgPerson**. Click **Next**.
   d. Enter a value in the **Naming attribute** field. For this example, enter `uid`. Click **Edit...** to add the password field to the required attributes tab.
   e. On the Edit tab page, select the **userPassword** attribute and click **Add**.

f. When **userPassword** is added, go to the **Selected attributes** field and move **userPassword** to the bottom. Click **OK**.

g. Click **Finish** to create the user template.

h. Verify that the user template `mycorpUserTempl` is created.

   On the Manage user templates page, verify the existence of the entry `cn=mycorpusertempl,dc=mycorp`.

10. On the **Realms and templates --> Manage realms** page, click **Add...** to create a user realm for the user template that you created.
11. On the Add realm page, enter values in the **Realm name** field and the **Parent DN** field, and click **Next**.

    For example, **Realm name** can be `mycorpUserRealm` and **Parent DN** is `dc=mycorp`.
12. On the Add realm page, go to the **User template** menu and select the user template that you created. Click **Edit...**.

    In this example, the value in the User template field is `cn=mycorpusertempl,dc=mycorp`.
13. On the Search filter page, accept the default settings and click **OK**.
14. Click **Finish** to complete the creation of a user realm.
15. Select **Realms and templates > Manage realms**. Ensure that the new realm is listed.

    For this example, ensure that there is an entry `cn=mycorpuserrealm,dc=mycorp`.

Results

The user registry is now configured.

Index

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Printed in USA