IBM Security Role and Policy Modeler
Version 1 Release 1

Reference Guide

SC27-2798-02

IBM Security Role and Policy Modeler
Version 1 Release 1

Reference Guide

SC27-2798-02

October 2012

This edition applies to version 1.1.0.2 of IBM Security Role and Policy Modeler and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Tables

About this publication

IBM Security Role and Policy Modeler Reference Guide describes state management rules and the Extract and Load tools.

Access to publications and terminology

This section provides:

- "IBM Security Role and Policy Modeler library"
- "Online publications"
- "IBM terminology website"

IBM Security Role and Policy Modeler library

The following documents are available in the IBM® Security Role and Policy Modeler library:

- *IBM Security Role and Policy Modeler Quick Start Guide*, GI13-2313
- *IBM Security Role and Policy Modeler Product Overview Guide*, GC27-2795
- *IBM Security Role and Policy Modeler Planning Guide*, SC22-5407
- *IBM Security Role and Policy Modeler Installation and Configuration Guide*, SC27-2743
- *IBM Security Role and Policy Modeler Administration Guide*, SC27-2796
- *IBM Security Role and Policy Modeler Troubleshooting Guide*, GC27-2797
- *IBM Security Role and Policy Modeler Message Guide*, GC27-2744
- *IBM Security Role and Policy Modeler Reference Guide*, SC27-2798
- *IBM Security Role and Policy Modeler Glossary*, SC27-2800

Online publications

IBM posts product publications when the product is released and when the publications are updated at the following locations:

IBM Security Role and Policy Modeler Information Center
The http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.security.modeling.doc_1.1.0.2/ic-homepage.htm site displays the information center welcome page for this product.

IBM Security Information Center
The http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp site displays an alphabetical list of and general information about all IBM Security product documentation.

IBM Publications Center
The http://www.ibm.com/e-business/linkweb/publications/servlet/pbi.wss site offers customized search functions to help you find all the IBM publications you need.

IBM terminology website

The IBM Terminology website consolidates terminology from product libraries in one location. You can access the Terminology website at http://www.ibm.com/software/globalization/terminology.

Accessibility

Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully. With this product, you can use assistive technologies to hear and navigate the interface. You can also use the keyboard instead of the mouse to operate all features of the graphical user interface.

For additional information, see Appendix B, "Accessibility features for IBM Security Role and Policy Modeler," on page 53.

Technical training

For technical training information, see the following IBM Education website at http://www.ibm.com/software/tivoli/education.

Support information

IBM Support provides assistance with code-related problems and routine, short duration installation or usage questions. You can directly access the IBM Software Support site at http://www.ibm.com/software/support/probsub.html.

IBM Security Role and Policy Modeler Troubleshooting Guide provides details about:

- What information to collect before contacting IBM Support.
- The various methods for contacting IBM Support.
- Instructions and problem-determination resources to isolate and fix the problem yourself.

Note: The **Community and Support** tab on the product information center can provide additional support resources.

Chapter 1. State management

The term *state management* relates to the administration of one or more component states in a system or product. Managing any changes in states or operations can be challenging. When setting the states for multiple components and business logic is merged and distributed in the code, then a state management mechanism is required.

There are multiple components in IBM Security Role and Policy Modeler, such as projects, sessions, and files. Each component can have different states. The state of one component can depend upon the state of another component. State management maintains component information about the controls and their states. There can be user operations, such as deleting a file, or system operations, such as importing a file. These operations can trigger a transition from one state to another state for one or more components. There can be rules about which operation can cause which state transition, and which operation is allowed on the current state.

If an operation is not permissible, then an error message is displayed. If an operation is permissible, the subsequent state of the component is processed and completed.

Rules for session states

These rules are provided to help you understand the state transitions in a session for various operations.

The following list is a summary of state management rules for a session:

- You cannot commit any session when the status of a project is:
  - `Project creation queued`
  - `Evaluating project creation`
  - `Project scope change queued`
  - `Evaluating project scope change`
  - `Role generation queued`
  - `Evaluating role generation`
  - `Role copy queued`
  - `Copying role`

  This rule is not applicable for a delete project operation. In other words, a project that is in `Project deletion queued` or `Evaluating project deletion` state does not put any constraints on a session commit operation. A session commit is also not constrained if the status of the project is:
  - `Project creation failed`
  - `Project scope change failed`
  - `Project deletion failed`
  - `Role generation failed`
  - `Role copy failed`
  - `Membership qualifier evaluation failed`
- You cannot commit a session when the status of another session is:
  - `Commit Queued`

  - Committing
  - Commit Error
- You cannot validate a session when the status of another session is:
  - Commit Queued
  - Committing
  - Commit Error
- When you commit a session, then the status of all the projects in IBM Security Role and Policy Modeler is changed to Recalculation required. When you perform a recalculation operation for all projects, then the status is changed to Ready for editing.
- When you commit a session, then any sessions with Validated status are reverted to Draft status. This state change is done because any session commit operation changes the data available in the Identity and Entitlement database. Therefore, the previous Validated state of the session no longer holds true.
- You can validate a session when the status is Draft.
- You can commit a session when the status is Draft or Validated. If a session commit operation cannot start, then the status changes to Commit Needs Restart. This condition might exist due to several user requests in the queue. You can attempt to commit such a session later.
- If a session fails during a commit operation, then the status changes to Commit Error. Similarly, if a session fails during a validation operation, then the status changes to Validation Error. You can commit or validate a session after the administrator fixes the failure, such restarting a database.
- You can delete a session when the status is:
  - Draft
  - Committed
  - Validated

  or any other error status, such as Validation Error or File Import Error.
- You cannot delete a session when the status is:
  - Committing
  - Validating
  - Commit Error

Rules for project states

These rules are provided to help you understand the state transitions in a project for various operations.

The following list is a summary of state management rules for a project:

- A project can require recalculation due to data changes in the Identity and Entitlement database. When there is a data change, the project status is changed to Recalculation required. After you recalculate a project, the project status changes to Ready for editing.
- You cannot perform any operation when the status of a session is:
  - Commit Queued
  - Committing
  - Commit Error
- You cannot perform any operation when the status of a project is other than Ready for editing.

- You cannot edit a project when the status of a session is:
  - `Commit Queued`
  - `Committing`
  - `Commit Error`

  These states indicate that the data in the Identity and Entitlement database is undergoing changes.
- You can perform any operation or edit a project when the status is `Ready for editing`. The `Ready for editing` state indicates that a project is recalculated.
- You can delete a project when the status is `Ready for editing` or `Committed`. You can also delete a project when the status is:
  - `Project creation failed`
  - `Project scope change failed`
  - `Project deletion failed`
  - `Role generation failed`
  - `Role copy failed`
  - `Membership qualifier evaluation failed`
  - `Commit failed`

  The delete operation for a project is not dependent upon the commit operation of any session.
- You cannot create a project when the status of any session is:
  - `Commit Queued`
  - `Committing`
  - `Commit Error`
- You can recalculate a project when the status is:
  - `Ready for editing`
  - `Committed`

  or in any failed state other than `Commit failed`. The `Commit failed` state indicates that the data in the Identity and Entitlement Database is not consistent. Therefore, you cannot perform a project recalculation operation against the data. You can also recalculate a project when the status is:
  - `Project creation failed`
  - `Project scope change failed`
  - `Project deletion failed`
  - `Role generation failed`
  - `Role copy failed`
  - `Membership qualifier evaluation failed`
- You cannot recalculate a project when the status of the project is:
  - `Recalculation queued`
  - `Recalculation in progress`
- You can export a project when the status is `Ready for editing`.

Rules for file states

These rules are provided to help you understand the state transitions in a file for various operations.

The following list is a summary of state management rules for a file:

- You can add one or more files to a session that is in `Draft` state. When you add a file, the status of the session changes to `In Progress`. You can also add more files to a session, which is in the `In Progress` state.
- You can delete a file when it is in the `Imported` state or any error state.
- If the importing of one or more files fails during a session, then the status of the file and the session changes to `File Import Error`.
- When one or more files are in `Deleting` state during a session, then the status of the session changes to `Updating`.
- When the operation of importing all the files in a session is complete, then the status of all the files changes to `Imported`. At the same time, the status of the session changes to `Draft`.
- There can be errors when you import or delete a file in a session. If there are errors, then the statuses of the file and the session change to their corresponding error states. For example, if a file delete operation fails, then the statuses of the file and the session change to `File Deletion Error`. This rule shows the cumulative effect of the file operation failure on a session state.

Chapter 2. Extract and Load tools

To model existing IBM Security Identity Manager data, use the Extract and Load tools.

The Extract tool pulls the data from IBM Security Identity Manager in preparation for importing it into IBM Security Role and Policy Modeler. After you use the modeler, the Load tool puts the updated data back into IBM Security Identity Manager.

See "Process for using the tools" to determine when to use the tools and the general process.

Process for using the tools

Before using the Extract and Load tools, you must decide what data to use.

See "Software requirements for running the tools" on page 6 to ensure that you meet the proper requirements.

See "Scenarios for the Extract tool" on page 36 and "Scenarios for the Load tool" on page 45 for more information.

End-to-end process

Follow this process to model your IBM Security Identity Manager data:

1. Install and configure the Extract and Load tools.

   "Installing and configuring the tools" on page 7
2. Customize the Extract configuration file.

   "Updating the Extract configuration XML file" on page 17
3. Run the Extract tool to extract the IBM Security Identity Manager data you want to model with IBM Security Role and Policy Modeler. See one of the following topics:
   - "Running the Extract tool on AIX or Linux operating systems" on page 34
   - "Running the Extract tool on Windows operating systems" on page 32

   If you form the schema and data CSV files without using the Extract tool, you must ensure that you use the `Identity Manager` prefix. See "Prefix update for CSV files" on page 6.
4. Use the IBM Security Role and Policy Modeler administrative console to:
   a. Import the CSV files into a IBM Security Role and Policy Modeler session. See the "Importing CSV schema files" topic in the IBM Security Role and Policy Modeler Information Center.
   b. Create a project with the session data. See the "Creating role and policy projects" topic in the IBM Security Role and Policy Modeler Information Center.
   c. Update the roles and policies. See the "Role administration" topic in the IBM Security Role and Policy Modeler Information Center.
   d. Export the project to an XML file. See the "Exporting roles and policies" topic in the IBM Security Role and Policy Modeler Information Center.

5. Use the Load tool to load the identity data with the IBM Security Role and Policy Modeler updates into IBM Security Identity Manager. See one of the following topics:
   - “Running the Load tool on AIX or Linux operating systems” on page 43
   - “Running the Load tool on Windows operating systems” on page 42

Prefix update for CSV files

If you form the schema and data CSV files without using the Extract tool, ensure that you prefix the `Attribute Display Name` and `Attribute UID` properly.

These prefix updates ensure consistency of the data in IBM Security Role and Policy Modeler and IBM Security Identity Manager.

In the schema CSV file, prefix the `Attribute Display Name` and `Attribute UID` values with `Identity Manager`. For example:

```
#Define Attribute
Attribute Description,Attribute Display Name,Attribute UID,Type,Usage,Usage,Usage,Usage,
.....
"Static or Dynamic","Identity Manager roleType","Identity Manager attribute-roleType",
"String","RoleAnalysis",,,,
```

In the data CSV file, prefix the column header with `Identity Manager`:

```
"#Role","TIM-Production",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
"Role UID","Identity Manager roleType","DisplayNameStrCustAttr1","Parent Role",
"Identity Manager Org Unit",...
```

Software requirements for running the tools

Your environment must meet certain requirements to run the Extract and Load tools.

Extract tool

The following requirements must be met to run the Extract tool:

- The Extract tool must be run on the same computer where IBM Security Identity Manager version 5.1 or 6.0 is installed. Ensure that all required IBM Security Identity Manager fix packs are installed. The tool uses the WebSphere® Application Server JRE of IBM Security Identity Manager.

  Support for custom role attributes is available only when the Extract tool is run on IBM Security Identity Manager version 6.0.
- The Extract tool is supported on all of the platforms supported by IBM Security Identity Manager. Use the IBM Security Role and Policy Modeler installer to install the Extract tool. For the platforms not supported by IBM Security Role and Policy Modeler, copy the `utilities.zip` file from the utilities subdirectory of the IBM Security Role and Policy Modeler installation CD and unzip it.

Load tool

Follow these requirements to run the Load tool:

- The Load tool can run on IBM Security Identity Manager version 5.1 or 6.0. Ensure that all required IBM Security Identity Manager fix packs are installed.

  Support for custom role attributes is available only when the Load tool is run on IBM Security Identity Manager version 6.0.

- The Load tool is supported only on the IBM Security Role and Policy Modeler platforms. Use the IBM Security Role and Policy Modeler installer to install the Load tool on the platforms supported.
- The Load tool can be run locally or on a remote computer from the IBM Security Identity Manager computer.
- If the Load tool is installed on a different computer than the IBM Security Identity Manager installation, install the WebSphere Application Server 7.0 Application Client on the same computer as the Load utility. In this scenario, the load tool uses the WebSphere Application Server 7.0 Application Client JRE.

  If the Load tool is installed on the same computer where IBM Security Identity Manager is installed, then no other prerequisite is required. In this scenario, the load tool uses the WebSphere Application Server JRE.

Installing and configuring the tools

You must install and configure the Extract and Load tools before you can run them.

The following topics provide information about installing and configuring the Extract tool:

- "Installing and configuring the Extract tool on AIX or Linux operating systems" on page 8
- "Installing and configuring the Extract tool on Windows operating systems"

"Setting log file parameters" on page 15 provides information about log file configuration.

The following topics provide information about installing and configuring the Load tool:

- "Installing and configuring the Load tool on AIX or Linux operating systems" on page 11
- "Installing and configuring the Load tool on Windows operating systems" on page 10
- "Configuring a remote IBM Security Identity Manager server for the Load tool" on page 12

The following topics provide information about uninstalling the tools:

- "Uninstalling the Extract tool" on page 9
- "Uninstalling the Load tool" on page 15

Installing and configuring the Extract tool on Windows operating systems

Install the Extract tool on a Windows operating system with the IBM Security Role and Policy Modeler installer. The configuration requires setting up path variables.

Procedure

1. For platforms supported by IBM Security Role and Policy Modeler, start the IBM Security Role and Policy Modeler installer and select **Extract and Load Utilities for IBM Security Identity Manager**.

   For the platforms not supported by IBM Security Role and Policy Modeler, copy the utilities.zip file from the utilities subdirectory of the IBM Security Role and Policy Modeler installation CD and unzip it.

2. Determine where the Extract tool files were installed. For example, if your IBM Security Role and Policy Modeler installation path is `C:\Program Files\IBM\SecurityModeler`, the Extract tool files are located in `C:\Program Files\IBM\SecurityModeler\utilities\extract`.

   Table 1 lists the contents of the `extract` directory:

Table 1. Extract subdirectory contents on Windows operating systems

File or directory name	Description
`ExtractConfig.xml`	Extract configuration XML file containing the input parameters for the Extract tool.
`lib`	Directory containing the Java™ libraries that the Extract tool requires.
`Extract.cmd`	Script file that runs the Extract tool on Windows operating systems.
`log4j.properties`	File that configures the logging behavior of the Extract tool.

3. Open the `Extract.cmd` file in an editor and update the following path variables:
   a. Set the WebSphere path in the *WAS_HOME* variable. For example, set `WAS_HOME=D:\Program Files\IBM\WebSphere\AppServer`.
   b. Set the IBM Security Identity Manager installation directory path in the *ITIM_HOME* variable. For example, set `ITIM_HOME=D:\Program Files\IBM\itim`.
   c. Set the *HOME_DIR* path to the location where the `extract` subdirectory of the utilities archive is extracted. For example, set `HOME_DIR=C:\RaPM\utilties\extract`.
   d. If the IBM Security Identity Manager server is configured with a database other than IBM DB2®, for example Oracle or Microsoft SQL Server, replace the following script line:

      ```
      set CP=%CP%;%ITIM_HOME%\lib\db2jcc.jar
      ```

      with the appropriate JDBC driver file name. For example, if you are using Oracle, use the following line:

      ```
      set CP=%CP%;C:\itim_jdbcdriver\ojdbc6.jar
      ```

4. Save the `Extract.cmd` file and close the editor.
5. Edit the `ExtractConfig.xml` file to specify the attributes required for the Extract tool. See "Updating the Extract configuration XML file" on page 17.

Installing and configuring the Extract tool on AIX or Linux operating systems

Use the IBM Security Role and Policy Modeler installer to install the Extract tool on an AIX® or Linux. The configuration requires setting up path variables.

Procedure

1. For platforms supported by IBM Security Role and Policy Modeler, start the installer and select the feature **Extract and Load Utilities for IBM Security Identity Manager**.

   For the platforms not supported by IBM Security Role and Policy Modeler, copy the `utilities.zip` file from the utilities subdirectory of the IBM Security Role and Policy Modeler installation CD and unzip it.

2. Determine where the Extract tool files were installed. For example, if your IBM Security Role and Policy Modeler installation path is `/opt/IBM/SecurityModeler/utilities/extract`, the Extract tool files are located in `/opt/IBM/SecurityModeler/utilities/extract`.

   Table 2 lists the contents of the `Extract` directory:

Table 2. Extract subdirectory contents on AIX or Linux operating systems

File or directory name	Description
`ExtractConfig.xml`	Extract configuration XML file containing the input parameters for the Extract tool.
`lib`	Directory containing the Java libraries that the Extract tool requires.
`Extract.sh`	Script file that runs the Extract tool on AIX or Linux operating systems.
`log4j.properties`	File that configures the logging behavior of the Extract tool.

3. Open the `Extract.sh` file in an editor and update the following path variables:
   a. Set the WebSphere path in the *WAS_HOME* variable. For example, set `WAS_HOME=/opt/IBM/WebSphere/AppServer`.
   b. Set the IBM Security Identity Manager installation directory path in the *ITIM_HOME* variable. For example, set `ITIM_HOME=/opt/IBM/itim`.
   c. Set the *HOME_DIR* path to the location where the `extract` subdirectory of the utilities archive is extracted. For example, set `HOME_DIR=/opt/RaPM/utilties/extract`.
   d. If the IBM Security Identity Manager server is configured with a database other than IBM DB2, for example Oracle or Microsoft SQL Server, replace the following script line:

      ```
      CP=$CP:$ITIM_HOME/lib/db2jcc.jar
      ```

      with the appropriate JDBC driver file name. For example, if you are using Oracle, use the following line:

      ```
      CP=$CP:/opt/itim_jdbcdriver/ojdbc6.jar
      ```
4. Save the `Extract.sh` file and close the editor.
5. If you copied the `Extract.sh` file from a remote machine, use an operating system command to give the file permission to run. For example:

   ```
   # chmod -R 755 Extract.sh
   ```
6. Edit the `ExtractConfig.xml` file to specify the attributes required for the Extract tool. See "Updating the Extract configuration XML file" on page 17.

Uninstalling the Extract tool

Uninstall the Extract tool by using the installer or by removing the directory and its contents.

Procedure

If you used the IBM Security Role and Policy Modeler installer to install the Extract and Load tools, then use it to uninstall the tools. If you manually copied the `utilities` directory, then remove the directory and all of its contents.

Installing and configuring the Load tool on Windows operating systems

Use the IBM Security Role and Policy Modeler installer to install the Load tool on a Windows operating system. The configuration requires setting up path variables.

About this task

Note: If you run IBM Security Identity Manager on a remote server, perform the steps in "Configuring a remote IBM Security Identity Manager server for the Load tool" on page 12.

Procedure

1. Start the IBM Security Role and Policy Modeler installer and select the feature **Extract and Load Utilities for IBM IBM Security Identity Manager**.
2. Determine where the Load tool files were installed. For example, if your default installation path is `C:\Program Files\IBM\SecurityModeler`, the Load tool files are located in `C:\Program Files\IBM\SecurityModeler\utilities\load`.

   Table 3 lists the contents of the `load` directory:

Table 3. Load subdirectory contents on Windows operating systems

File or directory name	Description
`Config.properties`	Load configuration properties file containing the input parameters for the Load tool.
`lib`	Directory containing the Java libraries that the Load tool requires.
`Load.cmd`	Script file that runs the Load tool on Windows operating systems.
`log4j.properties`	File that configures the logging behavior of the Load tool.
`LoadConfig.xml`	Load configuration XML file containing the configuration of the custom attributes.

3. Open the `Load.cmd` file in an editor and update the following path variables:
   a. Set the home directory path in the *HOME_DIR* variable to the Load tool directory. For example, set `HOME_DIR=C:\utilities\load`.
   b. Set the WebSphere Application Server home directory path in the *WAS_HOME* variable. For example, set `WAS_HOME=D:\Program Files\IBM\WebSphere\AppServer`.
   c. Set the IBM Security Identity Manager installation directory path in the *ITIM_HOME* variable. For example, set `ITIM_HOME=D:\Program Files\IBM\itim`.
4. Save the `Load.cmd` file and close the editor.
5. Edit the `Config.properties` file to specify the input parameters required for the Load tool. See "Updating the Config.properties input file for the Load tool" on page 13.
6. Edit the `LoadConfig.xml` file to specify the custom attributes required for the Load tool. See "Updating the Load configuration XML file" on page 40.

Installing and configuring the Load tool on AIX or Linux operating systems

Use the IBM Security Role and Policy Modeler installer to install the Load tool on an AIX or Linux operating system. The configuration requires setting up path variables.

Before you begin

If you are running IBM Security Identity Manager on a remote server, perform the steps in "Configuring a remote IBM Security Identity Manager server for the Load tool" on page 12.

Procedure

1. Start the IBM Security Role and Policy Modeler installer and select the feature **Extract and Load Utilities for IBM IBM Security Identity Manager**.
2. Determine where the Load tool files were installed. For example, if your default installation path is `usr/IBM/SecurityModeler`, the Load tool files are located in `usr/IBM/SecurityModeler/utilities/load`.

   Table 4 lists the contents of the `load` directory:

Table 4. Load subdirectory contents on AIX or Linux operating systems

File or directory name	Description
`Config.properties`	Load configuration properties file containing the input parameters for the Load tool.
`lib`	Directory containing the Java libraries that the Load tool requires.
`Load.sh`	Script file that runs the Load tool on AIX or Linux operating systems.
`log4j.properties`	File that configures the logging behavior of the Load tool.
`LoadConfig.xml`	Load configuration XML file containing the configuration of the custom attributes.

3. Open the `Load.sh` file in an editor and update the following path variables:
   a. Set the home directory path in the *HOME_DIR* variable to the Load tool directory. For example, set `HOME_DIR=/opt/utilities/load`.
   b. Set the WebSphere Application Server home directory path in the *WAS_HOME* variable. For example, set `WAS_HOME=/opt/IBM/WebSphere/AppServer`.
   c. Set the IBM Security Identity Manager installation directory path in the *ITIM_HOME* variable. For example, set `ITIM_HOME=/opt/IBM/itim`.
4. Save the `Load.sh` file and close the editor.
5. If you copied the `Load.sh` file from a remote machine, use an operating system command to give the file permission to run. For example:

   ```
   # chmod -R 755 Load.sh
   ```

6. Edit the `Config.properties` file to specify the input parameters required for the Load tool. See "Updating the Config.properties input file for the Load tool" on page 13.
7. Edit the `LoadConfig.xml` file to specify the custom attributes required for the Load tool. See "Updating the Load configuration XML file" on page 40.

Configuring a remote IBM Security Identity Manager server for the Load tool

Configure a IBM Security Identity Manager server by copying JAR files to the appropriate directories.

Before you begin

Ensure that you installed WebSphere Application Server 7.0 Application Client on the computer where the Load tool is located.

About this task

In the configuration steps, the directory names show Windows examples. For AIX or Linux, use the appropriate directory locations.

Procedure

1. Create a local directory,`clientjars` on your system.
2. Copy the following files from the IBM Security Identity Manager server computer to the `clientjars` directory.
   - `<ITIM_HOME>\lib\itim_api.jar`
   - `<ITIM_HOME>\lib\api_ejb.jar`
   - `<ITIM_HOME>\lib\itim_common.jar`
   - `<ITIM_HOME>\lib\jlog.jar`
   - `<ITIM_HOME>\lib\aspectjrt.jar`
   - `<ITIM_HOME>\lib\jffdc.jar`
   - `<ITIM_HOME>\lib\itim_server_api.jar`
   - `<ITIM_HOME>\lib\com.ibm.cv.kmip.ext.jar`

   ITIM_HOME is the location of the IBM Security Identity Manager installation directory. For example: `C:\Program Files\IBM\itim`.
3. Copy the `data` directory, and all of its contents, from the IBM Security Identity Manager server computer to the Load tool working directory. For example, copy all the files from `<ITIM_HOME>\data` to `c:\clientjars\data` for the Load tool.

   Note: The *ITIM_HOME* path variable name must be exactly as shown, including all capital letters.
4. Open the `Load.cmd` file in an editor and update the following path variables:
   - Set the home directory path in the *HOME_DIR* variable to the Load tool directory. For example, set `HOME_DIR=C:\utilities\load`.
   - Set the WebSphere Application Server 7.0 Application Client home directory path in the *WAS_HOME* variable. For example, set `WAS_HOME=D:\Program Files\IBM\WebSphere\AppClient`.
   - Set the IBM Security Identity Manager libraries directory path in the *ITIM_HOME* variable. For example, set `ITIM_HOME=c:\clientjars`.
   - Correct all of the paths provided for the following IBM Security Identity Manager JAR files by referring to the `c:\clientjars` directory:
     - `set CP=%CP%;%ITIM_HOME%\data`
     - `set CP=%CP%;%ITIM_HOME%\lib\jlog.jar`
     - `set CP=%CP%;%ITIM_HOME%\lib\jffdc.jar`
     - `set CP=%CP%;%ITIM_HOME%\lib\itim_common.jar`

- set CP=%CP%;%ITIM_HOME%\lib\itim_api.jar
- set CP=%CP%;%ITIM_HOME%\lib\aspectjrt.jar
- set CP=%CP%;%ITIM_HOME%\lib\api_ejb.jar

For example, replace the following statement:

```
set CP=%CP%;%ITIM_HOME%\lib\jlog.jar
```

with this statement:

```
set CP=%CP%;%ITIM_HOME%\jlog.jar
```

where ITIM_HOME is set to c:\clientjars directory as previously mentioned in this step.

5. Save the Load.cmd file and close the editor.
6. Edit the Config.properties file to specify the input parameters required for the Load tool. See "Updating the Config.properties input file for the Load tool."

Updating the Config.properties input file for the Load tool

The Load tool uses the properties defined in the Config.properties file to run in a remote environment.

Note: If IBM Security Identity Manager is configured as a single server, do not specify any value for the Cluster_URL property from the Config.properties file. Optionally, you can also comment out or remove the Cluster_URL property from the Config.properties file if IBM Security Identity Manager is configured as a single server. This property is used only for cluster deployments.

The Config.properties file is in the load directory. This configuration file uses the following parameters:

HostName
Specifies the IP address or the system name on which the IBM Security Identity Manager server runs. The default value host name is localhost.

PortNumber
Specifies the Port number, or bootstrap port of WebSphere Application Server, on which the WebSphere Application Server of IBM Security Identity Manager listens. The default value is 2809.

WAS_GlobalSecurity_Enabled
Specifies the enablement of global security on the WebSphere Application Server server for IBM Security Identity Manager. The default value is true. If the value is true, you are prompted for your WebSphere Application Server user name and password when you run the Load tool.

Note: This parameter is effective only when the Load tool is run for IBM Security Identity Manager 5.1. This parameter does not apply to IBM Security Identity Manager 6.0.

OrgUnitName
Specifies the Organization container in which the new roles and separation of duty constraints are created for IBM Security Identity Manager. This parameter is also used by the Load tool to search for existing roles and separation of duty constraints in IBM Security Identity Manager.

If you do not specify this parameter or set its value, then the role and separation of duty constraint additions and modifications take place in the Default IBM Security Identity Manager organization container.

The value requires one of the following formats:

OrgUnitName=ou=orgUnit
Use this format when the container is an organization unit, Admin Domain, or Business Partner Organization.

OrgUnitName=o=org
Use this format when the container is an organization.

OrgUnitName=l=loc
Use this format when the container is location.

OrgUnitName=DN=erglobalid=6145930925968307773,ou=orgChart, erglobalid=0000000000000000000,ou=IBM,dc=com
Use this format when specifying Distinguished Name (DN) value of the container.

Note: Enter the format shown as one continuous line with no spaces. The example shown is split into two lines for readability in this document only.

PreviewMode
Specifies the value to determine preview mode. Specify `true` to only preview the statistics with the total number of roles and separation of duty constraints that might be added or modified. For the Load tool to make the additions and modifications, specify `false`. The default value is `true`.

InputFileName
Specifies the path and file name of the XML file exported from IBM Security Role and Policy Modeler. This file contains the list of roles and separation of duty constraints to be imported into IBM Security Identity Manager. The default value is `Export_RaPM_Project.xml`.

The value for this parameter can also be the complete path and file name where this file is located. For example:

```
InputFileName=F:/utilities/load/exportrole_SOD.xml
```

IgnoreUserToRoleMapping
Specifies whether the Load tool uses user-to-role membership assignments. Set this value to true if you want to avoid use of user-to-role membership assignments. By default, this attribute is set to `false`. If the Load tool is run with the false value, then it adds or deletes user members of a role in the XML file exported from IBM Security Role and Policy Modeler. If this parameter is set to true, then it ignores processing user members of a role.

Cluster_URL
Specifies the URL location value of the application server naming service. Use this parameter if IBM Security Identity Manager is configured in a cluster environment. This value must match the value of the property `enrole.appserver.url` from the `enRole.properties` file in the data directory of the IBM Security Identity Manager home directory.

For example:

```
Cluster_URL=iiop://nodeip:2810/cell/clusters/ITIMCluster
```

Usage notes:

- By default, no value is specified with this parameter. Therefore, by default, the Load tool uses the `HostName` and `PortNumber` parameters to communicate

with the IBM Security Identity Manager application configured as a single server. Specify a value for this parameter only when IBM Security Identity Manager is configured in a cluster environment.

- If this parameter is commented out or not present in the `Config.properties` file, then the Load tool uses the `HostName` and `PortNumber` parameters to communicate with the IBM Security Identity Manager application configured as a single server.
- For IBM Security Identity Manager 6.0 and later, if you run the Load tool in cluster mode, you are only prompted once to supply the IBM Security Identity Manager credentials. The WebSphere Application Server global security setting is ignored.

`Role classification values`

Specifies the role classification type. The default role classification types provided by IBM Security Identity Manager are already specified in the `Config.properties` as shown here:

```
role.classification.application=Application role
role.classification.business=Business role
```

If you have customized role classification types for the IBM Security Identity Manager server, copy these values, except `role.classification.none`, from the `CustomLabels.properties` file in the `data` subdirectory of the IBM Security Identity Manager installation directory. Then, specify the values in the `Config.properties` file.

Sample Config.properties file

The following example is for the `config.properties` file on Windows operating systems:

```
HostName=localhost
PortNumber=2809
WAS_GlobalSecurity_Enabled=true
OrgUnitName=
PreviewMode=true
InputFileName=Export_RaPM_Project.xml
IgnoreUserToRoleMapping=false
role.classification.application=Application role
role.classification.business=Business role
```

Uninstalling the Load tool

To uninstall the Load tool, use the installer or remove the directory and its contents.

Procedure

If you used the IBM Security Role and Policy Modeler installer to install the Extract and Load tools, then use it to uninstall the tools. If you manually copied the `utilities` directory, then remove the directory and all of its contents.

Setting log file parameters

You can configure the `log4j.properties` file to generate the necessary output log file for your environment. The file is packaged separately with the Extract and Load utilities.

Before you begin

Locate the `log4j.properties` file from the `extract` subdirectory or `load` subdirectory that you want to modify.

Procedure

1. Open the `log4j.properties` file in an editor.
2. Update the `log4j.appender.logFile.File` parameter to name the output file. For example, specify:

   ```
   log4j.appender.logFile.File=Extract.log
   ```
3. Update the `log4j.rootCategory` parameter to specify the log file logging type. For example, specify:

   ```
   log4j.rootCategory=DEBUG, Logfile
   ```

   This example sets the log file logging to DEBUG.
4. Save the file.

Overview of the Extract tool

Use the Extract tool to export IBM Security Identity Manager identity, role, permission, and policy data. The Extract tool defines the base schema for this data and allows for extending the schema.

The IBM Security Role and Policy Modeler server expects the data and schema to be defined with respect to the elements in the `ExtractConfig.xml` file. See "Updating the Extract configuration XML file" on page 17.

The following topics describe how to use the Extract tool after setting up the configuration file:

- "Running the Extract tool on Windows operating systems" on page 32
- "Running the Extract tool on AIX or Linux operating systems" on page 34

The Extract tool generates the following CSV files:

- `Import_Schema_Session.csv` - Defines the schema.
- `Import_Data_Session.csv` - Defines the data with respect to the elements.

The Extract tool also generates the `Extract.log` file each time it is run.

Type of data extracted

The Extract tool extracts the following data from IBM Security Identity Manager:

- Roles
- Separation of duty policies
- Users as identities for IBM Security Role and Policy Modeler
- Groups as permissions for IBM Security Role and Policy Modeler
- User accounts from the managed resources of IBM Security Identity Manager as identities for IBM Security Role and Policy Modeler
- Services defined for the managed resources in IBM Security Identity Manager as permissions for IBM Security Role and Policy Modeler
- Groups from the managed resources of IBM Security Identity Manager as permissions for IBM Security Role and Policy Modeler

- Roles from the managed resources of IBM Security Identity Manager as roles for IBM Security Role and Policy Modeler
- Provisioning policy names associated with specific roles
- Organizational hierarchy information
- User-to-role associations defined in IBM Security Identity Manager
- User-to-group associations defined in IBM Security Identity Manager as users to permissions assignment for IBM Security Role and Policy Modeler
- User-to-Service association in IBM Security Identity Manager as users to permissions assignment for IBM Security Role and Policy Modeler

In addition to the previous data, the `ExtractConfig.xml` file contains attributes and object class mapping information to get additional information from IBM Security Identity Manager.

Service type configuration

The default `ExtractConfig.xml` file contains groups to be extracted as permissions for the following service types:

- IBM Security Identity Manager Service
- Oracle EBS
- POSIX Linux
- LDAP
- Active Directory
- POSIX Solaris
- POSIX AIX

The default `ExtractConfig.xml` file contains roles from the resources to be extracted as roles for the following service types:

- Oracle EBS
- POSIX AIX

The Extract tool generates CSV file data for these service types if they are already configured with your IBM Security Identity Manager server. If you want to support a new service type or attribute, then you must customize the `ExtractConfig.xml` file. The changes in this file generate the required schema and data into a CSV file.

Updating the Extract configuration XML file

Update the extract configuration XML file to define the schema you want to use as input to the Extract tool.

Before you begin

Locate the `ExtractConfig.xml` file that was installed with the Extract tool. See "Installing and configuring the Extract tool on Windows operating systems" on page 7 or "Installing and configuring the Extract tool on AIX or Linux operating systems" on page 8.

About this task

The `ExtractConfig.xml` file defines schema elements, such as search scope, attribute name, object class, and service name. It uses the data that is extracted

from the IBM Security Identity Manager server. This file is customizable and helps in deciding what information needs to be extracted from your IBM Security Identity Manager server.

Procedure

1. Open the `ExtractConfig.xml` file in an editor.
2. Add or update elements for the schema by using the specifications described in "IBM Security Role and Policy Modeler schema elements."

   The schema elements topic provides details about how ExtractConfig.xml generates various elements of the schema and data CSV files. The elements are required when importing data into IBM Security Role and Policy Modeler.
3. Add or update the tagging to define the behavior of the Extract tool by using the specifications described in "Extract tool behavior definitions" on page 28.
4. Save the file.

What to do next

Use the Extract tool to export the data by using this configuration file. See:

- "Running the Extract tool on AIX or Linux operating systems" on page 34
- "Running the Extract tool on Windows operating systems" on page 32

IBM Security Role and Policy Modeler schema elements

The `ExtractConfig.xml` file specifies configurations that generate elements of the schema and data CSV files in the format required for importing by IBM Security Role and Policy Modeler.

Note: For details about elements of the schema and data CSV files, see the "Import administration" section of the *IBM Security Role and Policy Modeler Administration Guide*.

The `ExtractConfig.xml` file has configurations that generate schema and data CSV files. The generated files contain the following sections:

- Schema CSV file:
  - "#Define Source section"
  - "#Define Attribute section" on page 19
  - "#Define Role Type section" on page 23
- Data CSV file:
  - "#Identity section" on page 23
  - "#Permissions section" on page 24
  - "#Role section" on page 25
  - "#Separation of Duty Policy section" on page 26
  - "#User Permission Assignment section" on page 27
  - "#Role User Assignment section" on page 28
  - "#Define Hierarchical Attributes section" on page 28

#Define Source section

This section of the schema CSV file defines all sources for the data. Example sources include identities, permissions, and roles.

Purpose

The ExtractConfig.xml file has a section to define the source. This definition acts as the primary source. Other attributes can come from service entities such as account or group in IBM Security Identity Manager. For these attributes, the extract tool defines the source and also extends the attribute schema to add an attribute for each source.

Tags in the configuration file

The source data in the CSV file is generated by using the following tags defined in ExtractConfig.xml:

```
<Source-UID> </Source-UID>
<Source-Name> </Source-Name>
<Source-Description> </Source-Description>
```

<Source-UID>
UID of the source. The UID must be unique.

<Source-Name>
Name of the source. It can be a URL, the name of an application, or a short description of the source. For example, use "IBM Security Identity Manager".

<Source-Description>
Description of the source. For example, use "My IBM Security Identity Manager v5.1 Production Server".

Output

The tool generates the following information in the Import_Schema_Session.csv file:

#Define Source		
Source UID	Source Name	Source Description

#Define Attribute section

This section of the schema CSV file defines all custom attributes used for entities. For example, entities include identity, permission, role, and permission assignment.

Purpose

The ExtractConfig.xml file has a section to define additional custom attributes. IBM Security Role and Policy Modeler reserves some attributes as *core* attributes. These attributes do not need to be explicitly defined. If you need more attributes than the core attributes, define them in this section.

Note: Support for custom role attributes is available only when the Load tool is run on IBM Security Identity Manager version 6.0.

Tags in the configuration file

The following tags are defined in ExtractConfig.xml and generate the attribute data in the schema and data CSV file:

```
<Attribute>
   <Attribute-UID> </Attribute-UID>
   <Attribute-Display-Name> </Attribute-Display-Name>
   <Attribute-Description> </Attribute-Description>
```

```
   <Usage> </Usage>
   <Type> </Type>
   <ITIMAttributeMapping>
      <ITIMObjectClass>
         <name> </name>
         <attribute> </attribute>
      </ITIMObjectClass>
  </ITIMAttributeMapping>
</Attribute>
```

Note: If you do not prefix the <Attribute-UID> and <Attribute-Display-Name> tag values with the keyword Identity Manager, then the Extract tool prefixes the Identity Manager keyword to the Attribute UID and Attribute Display Name values in the Import_Schema_Session.csv file. The data CSV file also follows the same naming convention for the column headers. The data CSV file retrieves the attribute names from the schema CSV file.

Description

<Attribute-UID>
UID of the attribute. The UID must be unique.

<Attribute-Display-Name>
Name of the attribute as it appears on the IBM Security Role and Policy Modeler user interface. The name must be unique.

<Attribute-Description>
Description of the attribute.

<Usage>
Text indicating the use of an attribute. For example, it can represent a resource URI, an identity, or analysis data. The values for the Usage tag are predefined as:

- UserAnalysis
- PermissionAnalysis
- RoleAnalysis
- SoDAnalysis
- UserDisplay1-5
- PermissionDisplay1-5

These value types distinguish the attribute type as Identity, Permission, Role, or Separation of Duty.

You can indicate multiple usages by using multiple Usage tags. No data is fetched for an attribute unless its usage has at least one of the following types:

- UserAnalysis
- PermissionAnalysis
- RoleAnalysis
- SoDAnalysis

The attribute is visible in the schema CSV file, but that attribute is not visible in the data CSV file.

<Type>
Defines the type for the attribute. Specify one of the following types:

- String
- Integer
- Identity

- Hierarchical

<ITIMAttributeMapping>
<ITIMObjectClass>
<name>
<attribute>

The <ITIMAttributeMapping> tag defines attributes that have multiple usages. If the custom attribute name is common, while their sources are different, add this type of attribute by adding multiple <ITIMObjectClass> tags within the <ITIMAttributeMapping> tag. Specify the <name> tag and the <attribute> tag for the different uses.

Notes on attribute usage:

- Do not use the names of the core attributes in the <Attribute-Display-Name> tag in the ExtractConfig.xml file. Examples of core attributes are Person UID, Permission UID, and Role UID.
- The Extract tool generates the attribute Identity Manager roleType into the schema CSV file. This special attribute is a RoleAnalysis attribute. The value of this attribute is role type for the roles defined in IBM Security Identity Manager. The value can be either static or dynamic.
- You might define a custom attribute in the ExtractConfig.xml file that has one of the following issues:
  - The attribute is not configured in IBM Security Identity Manager
  - The attribute is configured, but it has no values defined

  If either of these issues occur, the data CSV file that the Extract tool creates will not have values extracted for the entities for the custom attributes. This is true even though the schema CSV file that is created contains these custom attribute names.
- The default ExtractConfig.xml file declares some attributes within the tag <NonLDAP-ITIMAttributeMapping> </NonLDAP-ITIMAttributeMapping>. These attributes are special attributes that do not have any direct attribute or object class mapping from IBM Security Identity Manager. The Extract tool uses additional processing, separate from the processing used for other attributes, to extract values for these attributes. You cannot manually add these special attributes to ExtractConfig.xml. You can, however, remove the existing attributes if they are not needed.

  The special attributes are:

  Identity Manager Service Name
  This attribute is used for extracting the service name associated with the services defined in IBM Security Identity Manager.

  Identity Manager Service Owner
  This attribute is used for extracting the service owner information associated with services defined in IBM Security Identity Manager.

  Identity Manager Resources
  This attribute is used for extracting service profile names that are defined in your IBM Security Identity Manager.

  Identity Manager Permission Assignment Type
  The value of this attribute is either group or system. The value group refers to the groups of managed resources that are defined in IBM Security Identity Manager. The value system is for the IBM Security Identity Manager groups.

Example Attribute sections

The following example shows attributes with multiple usages:

```
<Attribute>
   <Attribute-UID>uri:attribute-Acount-objectclass</Attribute-UID>
   <Attribute-Display-Name>Account Object Classes</Attribute-Display-Name>
   <Attribute-Description>Account and support data Object class names</Attribute-Description>
   <Usage>UserDisplay3</Usage>
   <Usage>PermissionDisplay3</Usage>
   <Usage>RoleAnalysis</Usage>
   <Usage>SoDAnalysis</Usage>
   <Type>String</Type>
   <ITIMAttributeMapping>
      <ITIMObjectClass>
         <name>erPosixSolarisGroup</name>
         <attribute>objectclass</attribute>
      </ITIMObjectClass>
      <ITIMObjectClass>
         <name>erSeparationOfDutyRule</name>
         <attribute>objectclass</attribute>
      </ITIMObjectClass>
      <ITIMObjectClass>
         <name>erPosixSolarisAccount</name>
         <attribute>objectclass</attribute>
      </ITIMObjectClass>
      <ITIMObjectClass>
         <name>erPosixAixAccount</name>
         <attribute>objectclass</attribute>
      </ITIMObjectClass>
   </ITIMAttributeMapping>
</Attribute>
```

The following example shows how to define the `Attribute` section to extract the value of both the static and dynamic `route info` custom role attributes:

```
<Attribute>
 <Attribute-UID>Identity Manager attribute-Role Route Info</Attribute-UID>
 <Attribute-Display-Name>Identity Manager Role Route Info</Attribute-Display-Name>

<Attribute-Description>Type of Custom Role Attribute -
  route info</Attribute-Description>
 <Usage>RoleAnalysis</Usage>
 <Type>String</Type>
 <ITIMAttributeMapping>
  <ITIMObjectClass>
   <name>erRole</name>
   <attribute>routeinfo</attribute>
  </ITIMObjectClass>
  <ITIMObjectClass>
   <name>erDynamicRole</name>
   <attribute>routeinfo</attribute>
  </ITIMObjectClass>
 </ITIMAttributeMapping>
</Attribute>
```

Output

The tool generates the following information in the schema CSV file:

#Define Attribute						
Attribute UID	Attribute Display Name	Attribute Description	Type	Usage	Usage	Usage

#Define Role Type section

This section of the schema CSV file represents the role classification types from IBM Security Identity Manager. These role types include the default types in addition to the custom types defined in your IBM Security Identity Manager server.

Purpose

This role type attribute is not provided with the ExtractConfig.xml file.

Output

The tool generates the following information in the schema CSV file:

#Define Role Type
Role Type

#Identity section

This section of the data CSV file consists of information about identities extracted from IBM Security Identity Manager. A source is associated with each of the #Identity sections. The identity data can originate from different sources, based on the attribute mapping specified in the `ExtractConfig.xml` file.

Purpose

The attribute mapping configured with the `ExtractConfig.xml` file defines both the sources and usage of identity information.

Tags in the configuration file

In the `ExtractConfig.xml`, file, the `<Attribute>` tags that have `<Usage>` sub tags, such as `UserDisplay` or `UserAnalysis`, define the additional attributes of identity information to be extracted.

Output

The tool generates the following information in the data CSV file:

#Identity	TIM-Production			
Person UID	Identity Manager Person Object classes	Source Record UID	Person Name	Custom Attr1

Person UID
Source Record UID
Person Name

These are IBM Security Role and Policy Modeler core attributes. `Person UID` acts as a primary key. The source-wise data tells only what additional attributes are from this source. In the ExtractConfig.xml file, the `<PersonUID>` tag indicates which attribute to use as `Person UID`.

The primary source is IBM Security Identity Manager, and therefore the attribute from `Person` and `BP Person` is used to define `Person UID`.

Custom Attr1

Custom Attr1is a custom identity attribute and it appears in the CSV file if

it is defined in the ExtractConfig.xml file by using the <Attribute> tag. You can use more than one of these custom attributes.

Note: The Extract tool extracts IBM Security Identity Manager users of type Person and BPPerson as identities of the primary source defined in the ExtractConfig.xml. The Extract tool can also extract accounts of the IBM Security Identity Manager users as identities.

#Permissions section

This section of the ExtractConfig.xml file represents the IBM Security Identity Manager groups. These groups are defined on your managed resources; for example, a Corporate Directory Server, database, or applications.

Purpose

This section of the data CSV file consists of IBM Security Identity Manager groups and the groups defined on your managed resources (services) as permissions. The definitions are based on the permission-mapping provided in the ExtractConfig.xml file. For all groups, the Permission Assignment Type is set to Group. The Extract tool also treats the services defined in IBM Security Identity Manager as a permission. For services, Permission Assignment Type is set to System.

Tags in the configuration file

The following tags are defined in ExtractConfig.xml and generate the permissions data in the data CSV file:

```
<ObjectClass type="Permission">
     <Mapping>
        <Name>erLDAPGroupAccount</Name>
        <SourceAttribute>erldapgrouprdn</SourceAttribute>
        <AccountAttribute>erldapgroupname</AccountAttribute>
     </Mapping>
     <ServiceClass>erLDAPRMIService</ServiceClass>
   <ServiceAsPermission>true</ServiceAsPermission>
</ObjectClass>
```

Output

The tool generates the following information in the data CSV file:

#Permission						
Permission UID	Permission Description	Identity Manager Resources	Identity Manager Permission Assignment	Identity Manager Permission Assignment Type	Permission Name	Custom Attr1

Permission UID
Permission Description
Permission Name

These are IBM Security Role and Policy Modeler core attributes. The Extract tool does not use any configuration input data while generating values for these columns.

Custom Attr1

The attribute Custom Attr1 is a custom permission attribute that appears in

the CSV file if it is defined in the ExtractConfig.xml file by using the <Attribute> tag. You can use more than one of these custom attributes.

Identity Manager Service Name
Identity Manager Permission Assignment Type
Identity Manager Resources
Refer to the #Define Attribute section for details about these attributes from the default ExtractConfig.xml file.

#Role section

This section of the data CSV file represents the roles information from IBM Security Identity Manager. The role section can also represent the roles or groups defined on your managed resources. For example, AIX Service.

Purpose

By default, the Extract tool extracts IBM Security Identity Manager static and dynamic roles without any specific attribute mappings provided in the ExtractConfig.xml file. The ExtractConfig.xml does not provide any configuration mappings for extracting roles. However, there are a few attributes with Usage as RoleAnalysis. For these attributes, the Extract tool extracts additional information associated with these roles. The roles defined with IBM Security Identity Manager managed resources (services) can be extracted by providing required information with the tag <ObjectClass type="Role">. The tag is contained in ExtractConfig.xml file.

Tags in the configuration file

The default ExtractConfig.xml file consists of following custom role attributes with usage as RoleAnalysis:

Rule Definition
This attribute generates the filter value of the dynamic roles. For the static roles this value is empty.

Identity Manager Provisioning Policy Name
If the role is associated with provisioning policies defined in IBM Security Identity Manager, then this attribute extracts the provisioning policy names.

Identity Manager Org Unit
This attribute extracts the IBM Security Identity Manager Business Unit associated with a role. This attribute is a generic attribute that is also associated with other usage purposes.

Note: The Extract tool generates RoleAnalysis attribute Identity Manager roleType with value of this attribute as role type (static or dynamic) for the roles defined in the IBM Security Identity Manager.

Output

The tool generates the following information in the data CSV file:

#Role	**Source**								
Role UID	Role Owner	Identity Manager roleType	Role Name	Role Type	Role Description	Identity Manager Rule Definition	Identity Manager Org Unit	Parent Role	Custom Attr1

Role UID
Role Name
Role Description
Role Type
Parent Role
Role Owner

These are IBM Security Role and Policy Modeler core attributes.

The `Role Type` attribute value is mapped to the role classification attribute value present on the IBM Security Identity Manager server for a role.

If you specify the **`enableURI`** parameter on the Extract tool, the `Role UID` and `Parent Role` columns show:

- Role distinguished name, if:
  - The URI is null
  - There is no URI
  - Multiple URI values exist for a role
- Role URI, if:
  - A single URI value configured in IBM Security Identity Manager exists for the role

See the following topics for more information about the **`enableURI`** parameter:

- "Running the Extract tool on AIX or Linux operating systems" on page 34
- "Running the Extract tool on Windows operating systems" on page 32

Identity Manager roleType

This attribute is present in the schema file but are not customizable. The Extract tool does not use any configuration input data while generating values for this attribute.

Custom Attr1

The attribute `Custom Attr1` is a custom attribute and it appears in the data CSV file if it is defined in the `ExtractConfig.xml` file by using the `<Attribute>` tag. You can use more than one of these custom attributes.

#Separation of Duty Policy section

This section of the data CSV file represents the separation of duty policy rules from IBM Security Identity Manager.

Tags in the configuration file

The Extract tool by default extracts IBM Security Identity Manager separation of duty policy rules without any specific attribute mapping provided in the `ExtractConfig.xml` file. However the following attributes with Usage as SoDAnalysis extract additional information associated with the separation of duty policy rules.

Identity Manager SoD Policy Name

This attribute value contains the separate of duty policy name.

Identity Manager Org Unit

This attribute extracts the IBM Security Identity Manager Business Unit associated with a separation of duty policy. This attribute is a generic attribute also associated with other usage purposes.

Output

The tool generates the following information in the data CSV file:

#Separation of Duty Policy						
Rule UID	Identity Manager SoD Policy Name	Cardinality	Role UID	Rule Description	Identity Manager Org Unit	Custom Attr1

Rule UID
Rule Description
Role UID
Cardinality

These are IBM Security Role and Policy Modeler core attributes.

If you specify the **enableURI** parameter on the Extract tool, the `Role UID` column shows:

- Role distinguished name, if:
  - The URI is null
  - There is no URI
  - Multiple URI values exist for a role
- Role URI, if:
  - A single URI value configured in IBM Security Identity Manager exists for the role

See the following topics for more information about the **enableURI** parameter:

- "Running the Extract tool on AIX or Linux operating systems" on page 34
- "Running the Extract tool on Windows operating systems" on page 32

Custom Attr1

This attribute is a custom Separation of Duty rule attribute. It appears in the CSV file if it is defined in the `ExtractConfig.xml` file by using the `<Attribute>` tag.

#User Permission Assignment section

This section of the data CSV file represents the user permission assignment information.

Consider a scenario of a IBM Security Identity Manager user who owns an account on a managed resource (service), and that account is a member of a group on that resource. If appropriate identity and permission mappings are provided in `ExtractConfig.xml` for this resource, then the Users to Permissions mapping for this resource has two entries in the data CSV file:

- Managed resource account to group
- IBM Security Identity Manager User to managed resource (service)

Purpose

The configuration file for the Extract tool has a section to define the user permissions.

#Role User Assignment section

This section of the data CSV file represents the role user assignment information.

See the following topics for more information about how the **-enableURI** parameter, specified on the Extract tool, can impact the role UID values appearing in this section:

- "Installing and configuring the Extract tool on Windows operating systems" on page 7
- "Installing and configuring the Extract tool on AIX or Linux operating systems" on page 8

#Define Hierarchical Attributes section

This section of the data CSV file represents the Organization Structure extracted from IBM Security Identity Manager as a hierarchical attribute.

Purpose

The `ExtractConfig.xml` file contains an attribute `Identity Manager Org Unit` that is used for extracting Organization Structure that you have defined with your IBM Security Identity Manager.

Extract tool behavior definitions

Define the behavior of the Extract tool by updating the Extract configuration XML file.

Specify the Extract tool behavior by using the following sections in the `ExtractConfig.xml` file:

- "Attribute schema" on page 29
- "Permissions and roles" on page 31
- "Search scope"

Search scope

This section of the `ExtractConfig.xml` file defines the scope for the Extract tool to fetch data from a IBM Security Identity Manager deployment.

Defining the <SearchScope> section

The `<SearchScope>` section can contain the following values in `<SearchSource>`.

Note: You must choose one of the following values. The section can have only one value at a time.

`Default`

The `Default` search scope considers all the IBM Security Identity Manager deployment data to be fetched by the Extract tool. This value is selected with the default `ExtractConfig.xml` file. The format of the `<SearchSource>` tag to be specified within the `ExtractConfig.xml` file is:

```
<SearchSource>
<Value>Default</Value>
</SearchSource>
```

OrgContainer

You can specify a specific organization name or a specific organization unit name as your search scope. For example `ou=IBM`. Use this option to specify Organization Containers such as location and admin domain. When you

set the scope to Organization container name or Organization name, the Extract tool limits its data extraction to data such as identities, permissions, and roles, from the specified container or its child containers. Child containers can include sub units.

The format of the <SearchSource> tag in the ExtractConfig.xml file is:

```
<SearchSource>
        <Value>OrgContainer</Value>
        <OrgContainer>ou=IBM</OrgContainer>
</SearchSource>
```

Replace the value for the <OrgContainer> tag with your required Organization Container value:

- For Organization Containers like Organization Unit, Admin Domain, or Business Partner Organization, use ou= and the value of your container.
- For location use l= and for organization user o= and the value of your container.

If duplicate organization containers exist with the same name, the Extract tool exits and notifies the user. In this case you can choose instead to specify the Distinguished Name (DN) of the required container.

DN You can specify the Distinguished Name (DN) of specific organization or a specific organization unit as your search scope. For example:

```
DN=erglobalid=8632142593905208516,ou=orgChart,
   erglobalid=00000000000000000000,ou=ibm,dc=com
```

Use this option to specify DN values of Organization Containers such as location and admin domain. When you specify a scope by Organization container DN, the Extract tool limits its data extraction to data from the specified container or its child containers. The child containers include sub units.

The format of the <SearchSource> tag in the ExtractConfig.xml file is:

```
<SearchSource>
<Value>DN</Value>
 <DN>erglobalid=8632142593905208516,ou=orgChart,
  erglobalid=00000000000000000000,ou=ibm,dc=com</DN>
</SearchSource>
```

Attribute schema

This section of the ExtractConfig.xml file defines source attributes for identity, permission, role, and separation of duty policy for the primary source. You also define all object classes from IBM Security Identity Manager for which this attribute is fetched. If any of the defined attributes come from accounts, on end resources, adopted by identity, the Extract tool updates the attribute schema and source information.

Defining the <AttributeSchema> section

Use the following tags within the <AttributeSchema> section to define the source attributes:

<Source-UID>
Defines the primary source UID.

<Source-Name>
Defines the primary source name.

<Source-Description>
Defines the description of the source.

<PersonUID>
Defines which attribute from Person or Person class must be used while generating `Person UID`. If the attribute name for this element is not a valid attribute name, then the distinguished name (DN) is used as a default attribute name.

If you specify a `Person UID` attribute that is not unique, the tool fetches multiple entries for the same person. In this case, the output CSV file contains a single record with multiple values for that person.

For example, consider the case where the maximum number of Identity columns expected in a CSV file is six. If the specified `PersonUID` value fetches two records, then the output CSV file contains 12 columns. That is, the number of duplicate records times the number of expected columns.

If a record with more than the expected number of columns is found in the output CSV file, then you must update the schema to provide a unique PersonUID. When you rerun the tool, you get the correct results.

<Attribute>
Define the attributes. The attributes defined in this section are put into the appropriate section in the CSV file.

<Attribute-UID>
Defines the attribute UID.

<Attribute-Display-Name>
Defines a unique display name. This value is put into the CSV file.

<Attribute-Description>
Describes the attribute.

<Usage>
Describes the use of the attribute. For example, it can represent a resource URI or an identity, or it can contain analysis data. The `ExtractConfig.xml` file has a provision to specify the Usage tag. Be sure that you understand the purpose of the data before you specify this Usage attribute.

The values for the Usage column are predefined. The values are:

- `UserAnalysis`
- `PermissionAnalysis`
- `RoleAnalysis`
- `SoDAnalysis`
- `UserDisplay1-5`
- `PermissionDisplay1-5`

These values distinguish the attribute type as Identity, Permission, Role, or Separation of Duty.

<Type> Defines the type for the attribute. Specify one of the following types:

- String
- Integer
- Identity
- Hierarchical

<ITIMAttributeMapping>
Contains the object class name and attribute name that retrieves the attribute value from IBM Security Identity Manager.

Permissions and roles

This section of the `ExtractConfig.xml` file defines the permissions and roles.

You can represent the permissions and roles in IBM Security Identity Manager as:

- IBM Security Identity Manager role
- IBM Security Identity Manager groups
- Roles and Groups data from the manage resources defined in IBM Security Identity Manager.

You can call them as groups, permissions, privileges, responsibilities, or roles on the end resource. Generally, this data is reconciled in IBM Security Identity Manager as support data to help in selecting, instead of typing, the value for an attribute on an account form. You define in the tool which object class holds this data and which account class consumes this data.

The tool generates Permission UID, Role UID, or both, and gets their assignment for an identity.

Defining the <PermissionRoleObjectClasses> section

The `<PermissionRoleObjectClasses>` section can contain the following tags and values:

<ObjectClass type="Permission">
Specifies the value `Permission` or the value `Role` to generate permission or role data. The default value is `Permission`.

<Mapping>
Generates the permission and Person-permission mapping. Define the following elements in this tag:

<Name> Specifies any support data object class name.

<SourceAttribute>
Specifies one of the attributes used in the support data object class.

<AccountAttribute>
Specifies the account attribute name used to display support data values.

<ServiceClass>
Specifies the service class name.

<ServiceAsPermission>true</ServiceAsPermission>
Specifies whether the service itself is to be represented as a permission. If you want the service itself to be represented as a permission, set the value to `true`. The extract tool generates permission for the service and also generates Person-permission mapping for this service.

<ServiceGroup>
Defines a service group. If multiple services point to the same resource and you want to generate permissions and permission mappings for a single service, add these service names in the `<ServiceGroup>` tag by using the `<ServiceName>` tag.

The tool generates permissions and permission mappings for only one service described in the list of services mentioned in this tag.

<GroupName>
Specifies the group name. This value is used while generating `permissionUID`. You can identify which `permissionUID` is duplicated in your IBM Security Identity Manager implementation. You can specify any value, or you can specify one of the service names from the list of service names.

<Format>
Defines the format. The format defines, in addition to the value from the source attribute, how many other values exist in the account attribute and how they are separated. The format must contain a value as keyword, and a delimiter can be, for example: `"|",",",","."`.

<RoleType>
Defines the type of role. The value for this attribute can be `Business role` or `Application role`, or the value can be blank. Remove this attribute from the configuration file if you do not want to specify a `roleType`.

<Role-Owner>
Specifies the string representing the role owner.

For example:

```
<Role-Owner>erglobalid=0000000000000000007,
    ou=0,ou=people,erglobalid=00000000000000000000,
    ou=IBM,dc=com</Role-Owner>
```

In this example, the value

```
erglobalid=0000000000000000007,ou=0,ou=people,
erglobalid=00000000000000000000,ou=IBM,dc=com
```

is treated as a Role Owner, where the value is actually the LDAP DN of a IBM Security Identity Manager user. Remove this attribute from the configuration file if no role owner is required for a role.

Running the Extract tool on Windows operating systems

Run **Extract.cmd** to retrieve the identity data from IBM Security Identity Manager. The tool then uses the schema information from the `ExtractConfig.xml` file to create schema and data CSV files.

Before you begin

Ensure IBM Security Identity Manager is up and running.

Complete the steps in “Installing and configuring the Extract tool on Windows operating systems” on page 7.

Update the `ExtractConfig.xml` configuration file. See “Updating the Extract configuration XML file” on page 17.

Procedure

1. From the command prompt, navigate to the folder where you extracted the Extract tool files. For example, go to `C:\Program Files\IBM\SecurityModeler\utilities\extract`.
2. Run **Extract.cmd** from the command prompt.

This command, without parameters, uses the default file `ExtractConfig.xml` located in the same folder from where you are running the Extract tool. If you want to specify a different file name or path, specify:**Extract.cmd** [**-enableURI**] [**-InputFileName=**"*filename*"] [**-OutputDir=**"*directoryPath*"]

where:

`enableURI`

Enables the Extract tool to use the URI information. If you do not specify this option, the distinguished name is used.

Note: The **`enableURI`** parameter is only available with IBM Security Identity Manager version 6.0 or later. In addition, the Extract tool only recognizes the URIs for roles.

If you specify the **`enableURI`** parameter for the Extract tool, you must also specify it for the Load tool. This ensures data consistency in IBM Security Identity Manager and IBM Security Role and Policy Modeler.

In IBM Security Identity Manager, a role can have single or multiple URIs. Also, a role URI is not a required attribute, so it can be null for some roles. Role URIs are not unique; therefore, it is possible that multiple roles might have the same URI.

Table 5 shows the value that is extracted depending on the URIs associated with a role.

Table 5. Value extracted using the enableURI parameter

URIs associated with a role	Value extracted	Data CSV file sections containing the value
No URI associated with a role	Distinguished Name	Role, Role User Assignment, and Separation of Duty Policy
Unique URI associated with a role	Role URI	Role, Role User Assignment, and Separation of Duty Policy
Same URI associated with multiple roles	Role URI **Note:** During import into IBM Security Role and Policy Modeler, only one of these roles having the same URI is imported; the others are ignored. No message is logged for this in the Extract log file. The messages from IBM Security Role and Policy Modeler during import indicate that the roles were skipped.	Role, Role User Assignment, and Separation of Duty Policy
Multiple URIs associated with role	Distinguished Name	Role, Role User Assignment, and Separation of Duty Policy

`InputFileName`

Defines the path and file name of the input configuration file. If you do not specify this parameter, the directory where you extracted the Extract tool files is used, and the default input configuration file is `ExtractConfig.xml`.

OutputDir
Defines the output directory where the CSV files are generated. If you do not specify this parameter, the directory where you extracted the Extract tool files is used.

Following are some examples of this command:

```
Extract.cmd

Extract.cmd -OutputDir="F:\MyDir"

Extract.cmd -enableURI -InputFileName="F:\Inputfile\ExtractConfig.xml"
  -OutputDir="F:\OutputDir"
```

3. Enter the user name and password of the IBM Security Identity Manager server from where data is to be extracted. This user must be a system user with administrative rights for the utility to run. If the user lacks administrative rights, the tool displays an error message and stops running.

Results

The following files are created in the directory you specified for *HOME_DIR* in "Installing and configuring the Extract tool on Windows operating systems" on page 7:

- `Extract.log` –The log file listing each transaction.
- `Import_Data_Session.csv` –The CSV file that contains the IBM Security Identity Manager data such as identities, roles, and permissions.
- `Import_Schema_Session.csv` -- The CSV file that contains the schema definition of the custom display and analysis attributes of IBM Security Identity Manager.

What to do next

Consult the `Extract.log` file for errors and other processing information.

Use the IBM Security Role and Policy Modeler administrative console to import and model the data. See step 4 on page 5.

Running the Extract tool on AIX or Linux operating systems

Run **`Extract.sh`** to retrieve the identity data from IBM Security Identity Manager. The tool then uses the schema information from the `ExtractConfig.xml` file to create schema and data CSV files.

Before you begin

Ensure IBM Security Identity Manager is up and running.

Complete the steps in "Installing and configuring the Extract tool on AIX or Linux operating systems" on page 8.

Update the `ExtractConfig.xml` configuration file. See "Updating the Extract configuration XML file" on page 17.

Procedure

1. From the command prompt, navigate to the folder where you extracted the Extract tool files. For example, go to `/opt/IBM/SecurityModeler/utilities/extract`.
2. Run **`Extract.sh`** from the command prompt.

This command, without parameters, uses the default file `ExtractConfig.xml` that is located in the same folder from where you are running the Extract tool. If you want to specify a different file name or path, specify:**Extract.sh** [**-enableURI**] [**-InputFileName=**"*filename*"] [**-OutputDir=**"*directoryPath*"]

where:

`enableURI`
Enables the Extract tool to use the URI information. If you do not specify this option, the distinguished name is used.

Note: The **`enableURI`** parameter is only available with IBM Security Identity Manager version 6.0 or later. In addition, the Extract tool only recognizes the URIs for roles.

If you specify the **`enableURI`** parameter for the Extract tool, you must also specify it for the Load tool. This ensures data consistency in IBM Security Identity Manager and IBM Security Role and Policy Modeler.

In IBM Security Identity Manager, a role can have single or multiple URIs. Also, a role URI is not a required attribute, so it can be null for some roles. Role URIs are not unique; therefore, it is possible that multiple roles might have the same URI.

Table 6 shows the value that is extracted depending on the URIs associated with a role.

Table 6. Value extracted using the enableURI parameter

URIs associated with a role	Value extracted	Data CSV file sections containing the value
No URI associated with a role	Distinguished Name	Role, Role User Assignment, and Separation of Duty Policy
Unique URI associated with a role	Role URI	Role, Role User Assignment, and Separation of Duty Policy
Same URI associated with multiple roles	Role URI **Note:** During import into IBM Security Role and Policy Modeler, only one of these roles having the same URI is imported; the others are ignored. No message is logged for this in the Extract log file. The messages from IBM Security Role and Policy Modeler during import indicate that the roles were skipped.	Role, Role User Assignment, and Separation of Duty Policy
Multiple URIs associated with role	Distinguished Name	Role, Role User Assignment, and Separation of Duty Policy

`InputFileName`
Defines the path and file name of the input configuration file. If you do not specify this parameter, the directory where you extracted the Extract tool files is used, and the default input configuration file is `ExtractConfig.xml`.

OutputDir
Defines the output directory where the CSV files are generated. If you do not specify this parameter, the directory where you extracted the Extract tool files is used.

Following are some examples of this command:

```
Extract.sh

Extract.sh -OutputDir="/MyDir"

Extract.sh -enableURI -InputFileName="/Inputfile/ExtractConfig.xml"
  -OutputDir="/OutputDir"
```

3. Enter the user name and password of the IBM Security Identity Manager server from where data is to be extracted. This user must be a system user with administrative rights for the utility to run. If the user lacks administrative rights, the tools displays an error message and stops running.

Results

The following files are created in the directory you specified for *HOME_DIR* in "Installing and configuring the Extract tool on AIX or Linux operating systems" on page 8:

- `Extract.log` -- The log file listing each transaction.
- `Import_Data_Session.csv` –The CSV file that contains the IBM Security Identity Manager data such as identities, roles, and permissions.
- `Import_Schema_Session.csv` – The CSV file that contains the IBM Security Identity Manager schema.

What to do next

Consult the `Extract.log` file for errors and other processing information.

Use the IBM Security Role and Policy Modeler administrative console to import and model the data. See step 4 on page 5.

Scenarios for the Extract tool

There are several scenarios that require extracting a particular set of data by using specific tags in the `ExtractConfig.xml` file.

The following topics describe these scenarios:

- "Extracting data from a specific organization container"
- "Extracting permissions and identities from managed resources" on page 37
- "Extracting roles and permissions for a single service" on page 37
- "Extracting the role URI data" on page 38

Extracting data from a specific organization container

You can provide the name or distinguished name (DN) of a IBM Security Identity Manager container from which you want to extract data. By specifying a set of tags in the Extract configuration XML file, you can get a subset of data.

About this task

For more information, see "Search scope" on page 28.

Extracting permissions and identities from managed resources

To extract permission data from a managed resource when the identities are from the IBM Security Identity Manager server, specify the proper tags in the Extract configuration XML file.

Procedure

Use the <PermissionRoleObjectClasses> section of the ExtractConfig.xml file to specify only the permission and role data for the managed resource.

- For example, with the default ExtractConfig.xml file there exists permission mappings provided for the LDAP groups.

```
<ObjectClass type="Permission">
 <Mapping>
  <Name>erLDAPGroupAccount</Name>
  <SourceAttribute>erldapgrouprdn</SourceAttribute>
  <AccountAttribute>erldapgroupname</AccountAttribute>
 </Mapping>
  <ServiceClass>erLDAPRMIService</ServiceClass>
  <ServiceAsPermission>true</ServiceAsPermission>
</ObjectClass>
```

  If you remove this entire <ObjectClass type="Permission"> tag then LDAP groups are not extracted as permissions.

  Similarly you can add your own attribute tag for your specific service to extract groups as permissions from it.

- Use the <AttributeSchema> section to provide the attribute mapping if you want to extract the identities data for that managed resource.

  For example, if your IBM Security Identity Manager deployment consists of an LDAP service for managing LDAP accounts, and you want to extract the LDAP accounts as identities, then you can specify the following attribute:

```
<Attribute>
    <Attribute-UID>attribute-LDAP-Account-UID</Attribute-UID>
    <Attribute-Display-Name>LDAP Account UID</Attribute-Display-Name>
    <Attribute-Description>Account UIDs of LDAP service</Attribute-Description>

    <Usage>UserAnalysis</Usage>
    <Type>String</Type>
    <ITIMAttributeMapping>
       <ITIMObjectClass>
           <name>erLDAPUserAccount</name>
           <attribute>eruid</attribute>
       </ITIMObjectClass>
    </ITIMAttributeMapping>
</Attribute>
```

- If the ExtractConfig.xml file does not contain a mapping for a managed resource, then no identity data is extracted for that particular resource.

Extracting roles and permissions for a single service

If multiple services point to the same resource and you want to generate permission and role mappings for a single service, add service names into a service group by specifying the proper tags in the Extract configuration XML file.

About this task

The Extract tool generates permission and role mapping for any single service from a list of services mentioned in the service groups.

Procedure

Use the <ServiceGroup> section of the ExtractConfig.xml file to generate permissions and roles for a single service.
In the following example, the services in the <ServiceName> tags point to the same managed resource and contain the same data after support data reconciliation:

```
<ServiceGroup>
    <ServiceName>Posix Solaris Service</ServiceName>
    <ServiceName>PosixSolaris Duplicate service 1</ServiceName>
    <ServiceName>PosixSolaris Duplicate service 2</ServiceName>
    <GroupName>Posix-Solaris</GroupName>
</ServiceGroup>
```

Extracting the role URI data

The role URI attribute is available with IBM Security Identity Manager 6.0. Therefore, you can extract the URI data from IBM Security Identity Manager and map it to the URI in IBM Security Role and Policy Modeler.

In IBM Security Identity Manager 5.1, the role DN is mapped to the role URI in IBM Security Role and Policy Modeler.

Run the Extract tool and specify the **-enableURI** option with your IBM Security Identity Manager 6.0 data to use this mapping. See the details about using the **-enableURI** options and its results in the following topics:

- "Running the Extract tool on Windows operating systems" on page 32
- "Running the Extract tool on AIX or Linux operating systems" on page 34

Overview of the Load tool

Use the Load tool to load the data that was modeled by using IBM Security Role and Policy Modeler back into IBM Security Identity Manager.

The Config.properties file contains the required input parameters to run the load tool with remote or local IBM Security Identity Manager environment. See "Updating the Config.properties input file for the Load tool" on page 13.

When you use the Load tool, you specify parameters as described in the following topics:

- "Running the Load tool on Windows operating systems" on page 42
- "Running the Load tool on AIX or Linux operating systems" on page 43

Note: The Load tool acts as WebSphere Application Server thin client application that connects to IBM Security Identity Manager application running inside WebSphere Application Server. If WebSphere Application Server has additional security configurations defined, refer to the WebSphere Application Server documentation for its connectivity with the thin client applications.

Supported operations and attributes

The Load tool supports the following operations on IBM Security Identity Manager:

- Static role create
- Static role update
- Dynamic role update
- Separation Of duty policy create

The Load tool supports the addition of separation of duty policy in IBM Security Identity Manager for the separation of duty constraints that were created and exported in an XML file from IBM Security Role and Policy Modeler.

- Separation of duty policy update

  The Load tool supports updating a policy rule from an existing separation of duty policy in IBM Security Identity Manager.

Note: The IBM Security Identity Manager server does not allow the association of a dynamic role with a separation of duty policy. If the exported separation of duty constraint from IBM Security Role and Policy Modeler contains one or more dynamic roles, the following actions occur:

- In preview mode, an error message is displayed.
- In normal mode, the load fails to perform an add or modify operation on the specified separation of duty constraint.

When creating or updating static roles in IBM Security Identity Manager, the Load tool supports the following list of role attributes:

- Role name
- Role description
- Role classification
- Role members, or user members, assignment, or removal
- Parent roles assignment or removal
- Role custom attribute
- Role Universal resource identifier, erURI, attribute

  The erURI attribute is supported if you run the Load tool with the **-enableURI** option on a version 6.0 IBM Security Identity Manager server.

When updating dynamic roles in IBM Security Identity Manager, the Load tool supports the following list of role attributes:

- Role name
- Role description
- Role classification
- Role custom attribute
- Role Universal resource identifier, erURI, attribute

  The erURI attribute is supported if you run the Load tool with the **-enableURI** option on a version 6.0 IBM Security Identity Manager server.

Note: The load utility has limited support for updating dynamic roles. For dynamic roles, IBM Security Identity Manager does not support updating role membership settings and role hierarchy settings. If the exported role from IBM Security Role and Policy Modeler contains either of these settings, a warning message is displayed in both preview mode and normal mode.

When creating or updating separation of duty policies, the Load tool supports the following list of attributes:

- Rule description
- Roles associated in the rule
- Count representing allowed number of roles

Updating the Load configuration XML file

Update the load configuration XML file to define the custom attributes you want to use as input into the Load tool. The Load tool only recognizes custom role attributes that you define in this configuration file.

Before you begin

Locate the `LoadConfig.xml` file that is installed with the Load tool. See one of the following topics for more information:

- "Installing and configuring the Load tool on Windows operating systems" on page 10
- "Installing and configuring the Load tool on AIX or Linux operating systems" on page 11

About this task

The `LoadConfig.xml` file defines custom attribute schema elements. The file uses the data that is extracted from the IBM Security Identity Manager server. You can customize this file and it helps determine what custom attributes to load to your IBM Security Identity Manager server.

Support for custom role attributes is available only when the Load tool is run on IBM Security Identity Manager version 6.0.

There are two methods you can use to update the configuration file. Use the first option below if the custom attributes to define are the same as those defined for the Extract configuration tool.

Procedure

Use one of the following procedures to update the Load configuration file:

- Use the Extract configuration file:
  1. Copy the `ExtractConfig.xml` file to the folder where the `LoadConfig.xml` file resides. See "Updating the Extract configuration XML file" on page 17.
  2. Back up the `LoadConfig.xml` file.
  3. Rename the copied `ExtractConfig.xml` file to `LoadConfig.xml`.
- Manually update the `LoadConfig.xml` file:
  1. Open the `LoadConfig.xml` file in an editor.
  2. Add or update the tagging to define the behavior of the Load tool using the specifications described in "Load tool behavior definitions."
  3. Save the file.

What to do next

Use the Load tool to load the data using this configuration file. See one of the following topics for more information:

- "Running the Load tool on Windows operating systems" on page 42
- "Running the Load tool on AIX or Linux operating systems" on page 43

Load tool behavior definitions

Define the behavior of the Load tool by updating the Load configuration XML file.

Specify the Load tool behavior by using the following section in the LoadConfig.xml file:

- "Attribute schema"

Attribute schema

This section of the LoadConfig.xml file defines custom source attributes for identity, permission, role, and separation of duty policy for the primary source. You also define all object classes from IBM Security Identity Manager for which this custom attribute is fetched.

Defining the <AttributeSchema> section

Note: The Load tool only recognizes custom role attributes in the <AttributeSchema> section. Therefore, only those custom role attributes that have RoleAnalysis usage defined, are recognized.

Use the following tag within the <AttributeSchema> section to define the custom source attributes:

<Attribute>
Define the custom attributes. You can define zero or more custom attributes.

<Attribute-UID>
Defines the attribute UID. This tag is optional. You can define zero or more attribute UIDs.

<Attribute-Display-Name>
Defines a unique display name. This tag is required. Define this tag one time.

<Attribute-Description>
Defines the attribute. This tag is optional. You can define zero or more attributes.

<Usage>
Describes the use of the attribute. For example, the usage can represent a resource URI or an identity, or it can contain analysis data. The LoadConfig.xml file has a provision to specify the Usage tag. Ensure that you understand the purpose of the data before you specify this Usage attribute. The values for the Usage column are predefined. The values are:

- UserAnalysis
- PermissionAnalysis
- RoleAnalysis
- SoDAnalysis
- UserDisplay1-5
- PermissionDisplay1-5

These values distinguish the attribute type as Identity, Permission, Role, or Separation of Duty. This tag is required. You can define once or more Usage tags.

<Type>
Defines the type for the attribute. Specify one of the following types:

- String
- Integer
- Identity
- Hierarchical

This tag is optional. You can define zero or more `Type` tags. If the `Type` tag is not present, then `String` type is used by default.

<ITIMAttributeMapping>
Contains the object class name and attribute name that retrieves the attribute value from IBM Security Identity Manager.

Running the Load tool on Windows operating systems

Run **Load.cmd** to load the IBM Security Role and Policy Modeler role and the separation of duty constraint data into IBM Security Identity Manager.

Before you begin

Ensure IBM Security Identity Manager is up and running.

Complete the steps in "Installing and configuring the Load tool on Windows operating systems" on page 10.

Update the `Config.properties` file that defines the parameters of the Load tool. See "Updating the Config.properties input file for the Load tool" on page 13 for more information.

Know the file and path information of the XML file for the project you exported from IBM Security Role and Policy Modeler, or copy it to the Load tool folder.

About this task

When you run **Load.cmd**, the input for the tool comes from the XML file containing roles and separation of duty constraint data exported from IBM Security Role and Policy Modeler.

The Load utility then connects with IBM Security Identity Manager and loads the role and separation of duty constraint data into IBM Security Identity Manager.

Procedure

1. From the command prompt, navigate to the folder where you extracted the Load tool files. For example, go to `C:\Program Files\IBM\SecurityModeler\utilities\load`.
2. Run **Load.cmd** from the command prompt. Use the following optional parameters for the command:

   Load.cmd [**-enableURI**] [**-PreviewMode=***value*] [**-InputFileName=**"*filename*"] [**-ConfigFileName=**"*filename*"]

   where:

   enableURI
   Enables the Load tool to use the URI information. If you do not specify this option, the distinguished name is used.

   If you specify the **enableURI** parameter for the Extract tool, you must also specify it for the Load tool. This ensures data consistency in IBM Security Identity Manager and IBM Security Role and Policy Modeler.

   Note: The **enableURI** parameter is only available with IBM Security Identity Manager version 6.0 or later. In addition, the Load tool only recognizes the URIs for roles.

PreviewMode
Specify `true` to preview only the statistics with the total number of roles and separation of duty constraints that are potentially to be added or modified. To perform the load action of the additions and modifications, specify `false`. The default value is `true`.

The preview mode statistics display the number of changes that are to be performed in the IBM Security Identity Manager server without actually performing the changes. In addition, the preview displays any errors that occurred due to these operations.

InputFileName
Specify the path and file name of the XML file exported from IBM Security Role and Policy Modeler. This file contains role and separation of duty constraint data to be imported into IBM Security Identity Manager.

ConfigFileName
Specify the path and file name of the load configuration XML file.

If you do not specify this parameter, the tool uses the directory where you extracted the Load tool files from. The default input configuration file is `LoadConfig.xml`.

The values you specify on the command line override the values you specify in the `Config.properties` file. To use the parameters specified in the `Config.properties` file, run the command without any parameters.

The following examples show how to run this command:

```
Load.cmd

Load.cmd -enableURI -PreviewMode=true
  -InputFileName="E:\Adapter Installers\RaPM\Identity-Manager-Load\Project1.xml"


Load.cmd -PreviewMode=true
  -InputFileName="E:\Adapter Installers\RaPM\Identity-Manager-Load\Project1.xml"
  -ConfigFileName="E:\Adapter Installers\RaPM\Identity-Manager-Load\LoadConfig.xml"
```

3. If you have set `WAS_GlobalSecurity_Enabled = true` in your `Config.properties` file, then the Load tool prompts for the WebSphere Application Server user name and password. Enter the user name and password of the IBM Security Identity Manager server from where data is to be loaded. This user must be a system user with administrative rights. If the user does not have administrative rights, the utility displays an error message and exits.

   `WAS_GlobalSecurity_Enabled = true` and the WebSphere Application Server user name and password are relevant only for IBM Security Identity Manager 5.1. They do not apply to IBM Security Identity Manager 6.0.

Results

Consult the `Load.log` file for errors and other processing information.

The role and separation of duty constraint data is now loaded into IBM Security Identity Manager.

Running the Load tool on AIX or Linux operating systems

Run **`Load.sh`** to load the IBM Security Role and Policy Modeler role and the separation of duty constraint data into IBM Security Identity Manager.

Before you begin

Ensure IBM Security Identity Manager is running.

Complete the steps in "Installing and configuring the Load tool on AIX or Linux operating systems" on page 11.

Update the `config.properties` file which defines the parameters of the Load tool. See "Updating the Config.properties input file for the Load tool" on page 13.

Know the file and path information of the XML file for the project you exported from IBM Security Role and Policy Modeler, or copy it to the Load tool folder.

About this task

When you run **Load.sh**, the input for the tool comes from the XML file containing roles and separation of duty constraint data from IBM Security Role and Policy Modeler.

The Load utility then connects with IBM Security Identity Manager and loads the role and the separation of duty constraint data into IBM Security Identity Manager.

Procedure

1. From the command prompt, navigate to the folder where you extracted the Load tool files. For example, go to `/opt/IBM/SecurityModeler/load`.
2. Run **Load.sh** from the command prompt. Use the following optional parameters for the command:

   Load.sh [**-enableURI**] [**-PreviewMode=***value*] [**-InputFileName=**"*filename*"] [**-ConfigFileName=**"*filename*"]

   where:

   enableURI
   Enables the Load tool to use the URI information. If you do not specify this option, the distinguished name is used.

   If you specify the **enableURI** parameter for the Extract tool, you must also specify it for the Load tool. This ensures data consistency in IBM Security Identity Manager and IBM Security Role and Policy Modeler.

   Note: The **enableURI** parameter is only available with IBM Security Identity Manager version 6.0 or later. In addition, the Load tool only recognizes the URIs for roles.

   PreviewMode
   Specify `true` to preview only the statistics with the total number of roles and separation of duty constraints that are potentially to be added or modified. To perform the load action of the additions and modifications, specify `false`. The default value is `true`.

   The preview mode statistics display the number of changes that are to be performed in the IBM Security Identity Manager server without actually performing the changes. In addition, the preview displays any errors that occurred due to these operations.

   InputFileName
   Specify the path and file name of the XML file exported from IBM Security Role and Policy Modeler. This file contains role and separation of duty constraint data to be imported into IBM Security Identity Manager.

   ConfigFileName
   Specify the path and file name of the load configuration XML file.

If you do not specify this parameter, the tool uses the directory where you extracted the Load tool files from. The default input configuration file is `LoadConfig.xml`.

The values you specify on the command line override the values you specify in the `Config.properties` file. To use the parameters specified in the `Config.properties` file, run the command without any parameters.

Following are some examples of using this command:

```
Load.sh

Load.sh -enableURI -PreviewMode=true
  -InputFileName="/Adapter Installers/RaPM/Identity-Manager-Load/Project1.xml"

Load.sh -PreviewMode=true
  -InputFileName="/Adapter Installers/RaPM/Identity-Manager-Load/Project1.xml"
-ConfigFileName="/Adapter Installers/RaPM/Identity-Manager-Load/LoadConfig.xml"
```

3. If you have set `WAS_GlobalSecurity_Enabled = true` in your `Config.properties` file, then the Load tool prompts for the WebSphere Application Server user name and password. Enter the user name and password of the IBM Security Identity Manager server from where data is to be loaded. This user must be a system user with administrative rights. If the user does not have administrative rights, the utility displays an error message and exits.

   `WAS_GlobalSecurity_Enabled = true` and the WebSphere Application Server user name and password are relevant only for IBM Security Identity Manager 5.1. They do not apply to IBM Security Identity Manager 6.0.

Results

Consult the `Load.log` file for errors and other processing information.

The role and the separation of duty constraint data is now loaded into IBM Security Identity Manager.

Load tool statistics

The load tool displays statistics of the changes performed in the IBM Security Identity Manager server.

In preview mode, the load tool displays statistics of the changes to be performed in the IBM Security Identity Manager server. In normal mode, the load tool displays statistics of the actual changes performed in the IBM Security Identity Manager server.

Note: Normal mode is used when preview mode is set to false.

The changes can be due to:

- Creation or modification of roles and separation of duty constraints
- Changes to the role hierarchy
- Addition or deletion of user-to-role membership

In normal mode, the Load tool displays failure statistics if particular operations fail. For example, the total number of role modifications that failed is displayed.

Scenarios for the Load tool

The following information describes how the Load tool handles different scenarios.

- If there are separation of duty constraints created in IBM Security Role and Policy Modeler to add or modify, the Load tool takes the following actions:
  - If you run the Load tool with the **enableURI** parameter, then the search is based on the role URI under the organization defined in the `Config.properties` file. The following actions also apply to this scenario:
    - If the organization is not specified, then Load searches for it under the default organization.
    - If no roles are found, then the Load search operation is based on the role name or separation of duty constraint name.
    - If no roles or separation of duty constraints are found, then Load performs an addition operation. Otherwise, Load performs a modification operation.
    - If more than one role or separation of duty constraint exists with the same name under the same organization, then Load reports an error. This applies to each role or separation of duty constraint.
  - If you run the Load tool without the **enableURI** parameter, then the search operation is based on the role name or separation of duty constraint name under the organization defined in the `Config.properties` file. The following actions also apply to this scenario:
    - If the organization is not specified, then Load searches for it under the default organization.
    - If no roles or separation of duty constraints are found, then Load performs an addition operation. Otherwise, Load performs a modification operation.
    - If more than one role or separation of duty constraint exists with the same name under the same organization, then Load reports an error. This applies to each particular role or separation of duty constraint.
- If there are IBM Security Identity Manager roles and separation of duty constraints to modify, the Load tool takes the following actions:
  - If you run the Load tool with the **enableURI** parameter, then the Load tool performs a search operation based on the role URI. The following actions also apply to this scenario:
    - If no roles are found, Load performs a search operation based on the role or separation of duty constraint DN defined in the XML file.
    - The Load tool performs the modification only if the attribute values defined in the XML file are different from the attribute values in the IBM Security Identity Manager LDAP. This applies to each specific role or separation of duty constraint.
  - If you run the Load tool without the **enableURI** parameter, then the Load tool performs a search operation based on the role or separation of duty constraint DN mentioned in the XML file. The following action also applies to this scenario:
    - Load performs the modification only if the attribute values defined in the XML file are different from the attribute values in the IBM Security Identity Manager LDAP. This applies to each specific role or separation of duty constraint.
- If there are IBM Security Role and Policy Modeler roles and separation of duty constraints to modify, the Load tool takes the following actions:
  - Load performs a search operation based on the role or separation of duty constraint under the organization defined in the `Config.properties` file.
  - If the organization is not specified, then Load searches for it under the default organization.

– Load performs the modification only if the attribute values defined in the XML file are different from the attribute values in the IBM Security Identity Manager LDAP. This applies to each specific role or separation of duty constraint.
– If more than one role or separation of duty constraint exists with the same name under the same organization, then the utility generates an error.

Tuning the Load tool for large numbers of roles and policies

When using the Load tool with large numbers of exported roles and policies, optimize performance by increasing the Java Virtual Machine memory.

The Load tool might run out of memory in the Java Virtual Machine, even though the computer has additional physical memory. Consider increasing the JVM heap size when using the Load tool to process XML files that contain large numbers of roles and policies that have been exported from IBM Security Identity Manager.

You can increase the JVM heap size by updating the script file that launches the Load tool application.

1. In the Load tool installation directory, open the Load script file.

Table 7. Load tool filename

Operating system	File name
UNIX	Load.sh
Windows	Load.cmd

2. Edit the script code to specify the heap size parameters. Set the following values according to the needs of your deployment:

Table 8. Heap size parameter

Parameter	Description
-Xms	Initial heap size, in bytes
-Xmx	Maximum heap size, in bytes

For example, add the command line argument `-Xms254m -Xmx1024m` as shown in the tables below.

Note: The only changes to the commands are the addition of values for -Xms and -Xmx.

Table 9. Example for UNIX and Linux platforms

Default script command:

```
"$JAVA_HOME/bin/java" "-Dcom.ibm.CORBA.Debug.Output=/dev/null" $WAS_LOGGING
-classpath $CP "-Djava.security.auth.login.config=jaas.conf"
-Djava.ext.dirs="$JAVA_JRE/lib/ext:$WAS_EXT_DIRS:$WAS_HOME/plugins:$WAS_HOME/lib/WMQ/java/lib"
"$SERVER_ROOT" "$CLIENTSAS" "$CLIENTSSL" com.ibm.security.modeling.load.SODxmlParser $HOME_DIR $*
```

Updated command, with new arguments in **bold**:

```
"$JAVA_HOME/bin/java" -Xms254m -Xmx1024M "-Dcom.ibm.CORBA.Debug.Output=/dev/null"
$WAS_LOGGING -classpath $CP "-Djava.security.auth.login.config=jaas.conf"
-Djava.ext.dirs="$JAVA_JRE/lib/ext:$WAS_EXT_DIRS:$WAS_HOME/plugins:$WAS_HOME/lib/WMQ/java/lib"
"$SERVER_ROOT" "$CLIENTSAS" "$CLIENTSSL" com.ibm.security.modeling.load.SODxmlParser $HOME_DIR $*
```

Table 10. Example for Windows platforms

Default script command:

```
"%JAVA_HOME%\bin\java" "-Dcom.ibm.CORBA.Debug.Output=NUL"
%WAS_LOGGING% -Djava.endorsed.dirs="%WAS_ENDORSED_DIRS%"
"-Djava.security.auth.login.config=jaas.conf" -classpath "%CP%"
-Djava.ext.dirs="%JAVA_JRE%\lib\ext;%WAS_EXT_DIRS%;%WAS_HOME%\plugins;%WAS_HOME%\installedConnectors"
"%CLIENTSAS%" "%CLIENTSSL%" com.ibm.security.modeling.load.SODxmlParser "%HOME_DIR%" %*
```

Updated command, with new arguments in **bold**:

```
"%JAVA_HOME%\bin\java" -Xms254m -Xmx1024M "-Dcom.ibm.CORBA.Debug.Output=NUL"
%WAS_LOGGING% -Djava.endorsed.dirs="%WAS_ENDORSED_DIRS%"
"-Djava.security.auth.login.config=jaas.conf" -classpath "%CP%"
-Djava.ext.dirs="%JAVA_JRE%\lib\ext;%WAS_EXT_DIRS%;%WAS_HOME%\plugins;%WAS_HOME%\installedConnectors"
"%CLIENTSAS%" "%CLIENTSSL%" com.ibm.security.modeling.load.SODxmlParser "%HOME_DIR%" %*
```

Appendix A. Conventions used in this information

This information uses several conventions for special terms and actions and for operating system-dependent commands and paths.

Typeface conventions

This information uses the following typeface conventions.

Bold

- Lowercase commands and mixed case commands that are otherwise difficult to distinguish from surrounding text
- Interface controls (check boxes, push buttons, radio buttons, spin buttons, fields, folders, icons, list boxes, items inside list boxes, multicolumn lists, containers, menu choices, menu names, tabs, property sheets), labels (such as **Tip:**, and **Operating system considerations**:)
- Keywords and parameters in text

Italic

- Citations (examples: titles of publications, diskettes, and CDs
- Words defined in text (example: a nonswitched line is called a *point-to-point line*)
- Emphasis of words and letters (words as words example: "Use the word *that* to introduce a restrictive clause."; letters as letters example: "The LUN address must start with the letter *L*.")
- New terms in text (except in a definition list): a *view* is a frame in a workspace that contains data.
- Variables and values you must provide: ... where *myname* represents....

Monospace

- Examples and code examples
- File names, programming keywords, and other elements that are difficult to distinguish from surrounding text
- Message text and prompts addressed to the user
- Text that the user must type
- Values for arguments or command options

Bold monospace

- Command names, and names of macros and utilities that you can type as commands
- Environment variable names in text
- Keywords
- Parameter names in text: API structure parameters, command parameters and arguments, and configuration parameters
- Process names
- Registry variable names in text
- Script names

Definitions for HOME and other directory variables

The table contains default definitions that are used in IBM Security Role and Policy Modeler information center and guides. These definitions represent the HOME directory level for different product installation paths.

You can customize the HOME directory for your specific requirement. The default directory installation locations in the following table are provided for either administrator or root users.

For non-administrator or nonroot users, replace the following paths with *user_home*:

- Windows operating system: *drive*:\Program Files
- Linux: */opt*
- UNIX, or AIX: */usr*

Table 11. Home directory variable definitions

Path variable	Default definitions	Description
SM_HOME	• Windows operating system: C:\Program Files\IBM\SecurityModeler • Linux, UNIX or AIX: /opt/IBM/SecurityModeler	The base directory that contains IBM Security Role and Policy Modeler and documentation.
DB_HOME	• Windows operating system: C:\Program Files\IBM\SQLLIB • Linux: /opt/ibm/db2/V9.7 • UNIX or AIX: /opt/IBM/db2/V9.7	The default DB2 home directory.
WAS_HOME	• Windows operating system: C:\Program Files\IBM\WebSphere\AppServer • Linux: /opt/IBM/WebSphere/AppServer • UNIX or AIX: /usr/IBM/WebSphere/AppServer	The default WebSphere Application Server home directory.
TIP_PROFILE_HOME	• Windows operating system: *WAS_HOME*\profiles\TIPProfile • Linux, UNIX, or AIX: *WAS_HOME*/profiles/TIPProfile	The default Tivoli® Integrated Portal home directory.

Table 11. Home directory variable definitions (continued)

Path variable	Default definitions	Description
TCR_COMPONENT_HOME	• Windows operating system: `C:\Program Files\IBM\WebSphere\AppServerComponents\TCRComponent` • Linux: `/opt/IBM/WebSphere/AppServerComponents/TCRComponent` • UNIX or AIX: `/usr/IBM/WebSphere/AppServerComponents/TCRComponent`	The Tivoli Common Reporting home directory.

Appendix B. Accessibility features for IBM Security Role and Policy Modeler

Accessibility features help users who have a disability, such as restricted mobility, use information technology products successfully.

Accessibility features

The following list includes the major accessibility features in IBM Security Role and Policy Modeler:

- Keyboard-only operation
- Interfaces that are commonly used by screen readers
- Keys that are discernible by touch but not activated by touch
- Industry-standard devices for ports and connectors
- The attachment of alternative input and output devices

The IBM Security Role and Policy Modeler information center and its related publications are accessibility-enabled.

Keyboard navigation

This product allows operation with a keyboard.

Interface information

Hierarchical view is not keyboard accessible
The hierarchical view of the role and policy model is not keyboard accessible. However, the table view of the role and policy model is keyboard accessible. Customers who require a keyboard-accessible role and policy model can use the table view on the Roles and Policies window.

Analysis graphs are not keyboard accessible
There is an alternative representation of the same data in the form of in and out tables in the analysis windows.

Supported browsers for accessibility
Mozilla FireFox 3.6.22.

Microsoft Internet Explorer 8. For information about known accessibility issues for this browser, see the "Known limitations, problems, and workarounds" topic in the IBM Security Role and Policy Modeler information center.

Reports are accessible
Reports are accessible in HTML and PDF format. For more information, see the "Assistive technologies for reports" topic in the IBM Security Role and Policy Modeler information center.

Opening online help within IBM Security Role and Policy Modeler
For Microsoft Internet Explorer, press Alt+6+Enter.

For Mozilla FireFox, press Shift+Alt+6.

IBM and accessibility

See the IBM Human Ability and Accessibility Center for more information about the commitment that IBM has to accessibility.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features contained in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM might have patents or pending patent applications that cover subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it to enable: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
J46A/G4
555 Bailey Avenue
San Jose, CA 95141-1003
U.S.A.

Such information might be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments might vary significantly. Some measurements might have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements might have been estimated through extrapolation. Actual results might vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements, or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding the future direction or intent of IBM are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing, or distributing application programs that conform to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample

programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows: © (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. 2004, 2012. All rights reserved.

If you are viewing this information softcopy, the photographs and color illustrations might not appear.

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both: http://www.ibm.com/legal/copytrade.shtml

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

The Oracle Outside In Technology included herein is subject to a restricted use license and can only be used in conjunction with this application.

Index

Special characters

A

C

D

E

H

I

L

M

N

O

P

R

S

T

U

Printed in USA

SC27-2798-02