Oracle® Identity Manager

Connector Guide for IBM RACF Advanced

Release 9.0.3

B32378-01

February 2007

Oracle Identity Manager Connector Guide for IBM RACF Advanced, Release 9.0.3

B32378-01

Primary Author: Deepa Aswani

Contributing Author: Lyju Vadassery

Contents

Preface

Oracle Identity Manager Connector Guide for IBM RACF Advanced provides information about integrating Oracle Identity Manager with IBM RACF.

> **Note:** This is a transitional release following Oracle's acquisition of Thor Technologies. Some parts of the product and documentation still refer to the original Thor company name and Xellerate product name and will be rebranded in future releases.

Audience

This guide is intended for users who want to deploy the Oracle Identity Manager IBM RACF Connector.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at

`http://www.oracle.com/accessibility/`

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

TTY Access to Oracle Support Services

Oracle provides dedicated Text Telephone (TTY) access to Oracle Support Services within the United States of America 24 hours a day, seven days a week. For TTY support, call 800.446.2398.

Related Documents

For more information, refer to the following documents in the Oracle Identity Manager documentation set:

- *Oracle Identity Manager Release Notes*
- *Oracle Identity Manager Installation Guide for JBoss*
- *Oracle Identity Manager Installation Guide for Oracle Containers for J2EE*
- *Oracle Identity Manager Installation Guide for WebLogic*
- *Oracle Identity Manager Installation Guide for WebSphere*
- *Oracle Identity Manager Administrative and User Console Guide*
- *Oracle Identity Manager Administrative and User Console Customization Guide*
- *Oracle Identity Manager Design Console Guide*
- *Oracle Identity Manager Tools Reference Guide*
- *Oracle Identity Manager Audit Report Developer Guide*
- *Oracle Identity Manager Best Practices Guide*
- *Oracle Identity Manager Connector Framework Guide*
- Connector guides for various third-party applications

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager 9.0.3 connector documentation set, visit Oracle Technology Network at

`http://www.oracle.com/technology/documentation/index.html`

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

What's New in the Oracle Identity Manager Connector for IBM RACF Advanced?

This chapter provides an overview of the updates made to the connector and documentation for IBM RACF in release 9.0.3 of the Oracle Identity Manager connector pack.

> **See Also:** The 9.0.2 release of this guide for information about updates that were new for the 9.0.2 release

The updates discussed in this chapter are divided into the following categories:

- Software Updates

  These include updates made to the connector software.

- Documentation-Specific Updates

  These include major changes made to the connector documentation. These changes are not related to software updates.

> **See Also:** *Oracle Identity Manager Release Notes*

Software Updates

This section discusses updates made to this release of the connector software.

Enhancement in the Multilanguage Support Feature

In addition to the three languages supported by the earlier release, this release of the connector supports seven other languages. All the supported languages are listed in the Multilanguage Support section.

Application Server Support

This release of the connector includes support for the following application servers:

- JBoss Application Server
- BEA WebLogic
- IBM WebSphere
- Oracle Containers for J2EE (OC4J)

To ensure connector compatibility with the application server, refer to the instructions specified in the Step 4: Configuring the Connector to Work with the Oracle Identity Manager Application Server section.

Scripts for Initial Reconciliation

From this release of the connector, you can perform the initial reconciliation run using the scripts provided with the connector instead of issuing commands at the command line. These files are described in the Files and Directories That Comprise the Connector section. Chapter 4, "Initial Reconciliation Run" describes the modified procedure to perform the initial reconciliation run.

Documentation-Specific Updates

The following documentation-specific update has been made in this release of the guide:

- In the Enabling Logging section, instructions are included for each of the application servers that are supported by this release of the connector.
- The LDAP Gateway installation procedure has been modified. A simpler procedure is described in the Step 7: Installing and Configuring the LDAP Gateway section.
- In the Step 6: Compiling Adapters section, the instruction about restarting the node has been removed from Step 4 of the procedure to compile adapters.

1

About the Connector

The Oracle Identity Manager IBM RACF Advanced Connector provides a native interface between IBM RACF installed on z/OS mainframe and Oracle Identity Manager. The Advanced Connector functions as a trusted virtual administrator on the targeted platform, performing tasks such as creating login IDs, suspending IDs, changing passwords, and performing other functions that administrators usually perform manually.

The IBM RACF Advanced Connector enables provisioning and reconciliation to IBM RACF security facilities. This chapter discusses the following topics:

- Overview of IBM RACF Advanced Connector
- Supported Functionality
- Multilanguage Support
- Files and Directories That Comprise the Connector
- How to Use This Guide

Overview of IBM RACF Advanced Connector

The IBM RACF Advanced Connector includes the following components:

- **LDAP Gateway**: The LDAP Gateway receives instructions from Oracle Identity Manager in the same way as any LDAP version 3 identity store. These LDAP commands are then converted into native mainframe commands for IBM RACF and sent to the Provisioning Agent. The response is also native to IBM RACF, which is then parsed into an LDAP response. After execution, an LDAP-formatted response is returned to the requesting application.
- **Provisioning Agent**: The Provisioning Agent is a mainframe component, receiving native mainframe IBM RACF provisioning commands from the LDAP Gateway. These requests are processed against the IBM RACF authentication repository with the response parsed and returned to the LDAP Gateway.
- **Reconciliation Agent**: The Oracle Identity Manager Reconciliation Agent captures native mainframe events using advanced exit technology for seamless reconciliation to Oracle Identity Manager through the LDAP Gateway. The Reconciliation Agent captures events occurring from the TSO logins, command prompt, batch jobs, and other native events in real time. The Reconciliation Agent captures these events and transforms them into notification messages for Oracle Identity Manager through the LDAP Gateway.
- **Message Transport Layer**: The message transport layer enables the exchange of messages between the LDAP Gateway and the IBM RACF Provisioning and

Reconciliation Agent. You can use the following messaging protocols for the message transport layer:

- IBM MQ Series
- TCP/IP with internal Advanced Encryption Standard (AES) encryption using 128-bit cryptographic keys. The IBM RACF Advanced connector supports a manually configured message transport layer using the TCP/IP protocol, which is functionally similar to proprietary message transport layer protocols.

In addition, the Advanced connector is engineered for high-performance environments and transactions.

> **See Also:** For more information on the IBM RACF Advanced Connector architecture and configuration of the message transport layer, refer to Appendix B, "Connector Architecture"

Supported Functionality

The following sections list the features supported by the IBM RACF Advanced Connector:

- Provisioning Agent Functionality
- Reconciliation Agent Functionality
- Reconciled Attributes

Provisioning Agent Functionality

The Provisioning Agent provides the following functionality:

- Change passwords
- Reset passwords
- Create users
- Modify users
- Revoke user accounts
- Add user to groups
- Delete users
- Resume user accounts
- List users
- List groups
- List users by groups
- List resource profiles by user
- Grant user access to data sets
- Grant user access to resource profiles
- Grant user access to TSO

Reconciliation Agent Functionality

The Reconciliation Agent provides the following functionality:

- Change passwords
- Password resets
- Create user data
- Modify user data
- Revoke users
- Add users to groups
- Delete users
- Resume users

Reconciled Attributes

This section discusses the elements that the Reconciliation Agent extracts from the target system to construct reconciliation event records. The attributes that are reconciled between the IBM RACF and Oracle Identity Manager systems are listed in the following table:

Reconciled Attributes with IBM RACF		
uid	userPassword	sn
cn	givenName	resumeDate
revokeDate	dataset	lastaccessdate
lastconnectdate	defaultgroup	owner
memberOf	attributes	tsoacctnum
tsoholdclass	tsojobclass	tsomsgclass
tsoproc	tsosize	tsomaxsize
tsosysoutclass	tsounit	tsouserdata
tsocommand	tsodest	tsoseclabel

See Also: Appendix A, "Attribute Mapping Between Oracle Identity Manager and IBM RACF"

Multilanguage Support

In addition to English, this release of the connector supports the following languages:

- English
- Brazilian Portuguese
- French
- German
- Italian
- Japanese
- Korean
- Simplified Chinese
- Spanish

- Traditional Chinese

Files and Directories That Comprise the Connector

The files and directories that comprise this connector are located in the following directory on the installation media:

```
Security Applications/IBM RACF/IBM RACF Advanced
```

Copy the contents of this file to the *`oim_home`* directory. The contents of this file are described in brief in the following table:

Files and Directories	Description of Files and Contents
`etc/LDAP Gateway/ldapgateway.zip`	Files required for LDAP Gateway deployment in the Oracle Identity Manager system.
`etc/Provisioning and Reconciliation Connector/Mainframe_RACF_version.zip`	Files required for the installation of the Provisioning Agent and Reconciliation Agent on the mainframe.
`lib/idm.jar`	The connector JAR file to be deployed on the Oracle Identity Manager system.
`lib/racf-adv-agent-recon.jar` `lib/racfConnection.properties`	Files required for real-time reconciliation between Oracle Identity Manager and the target system.
Files in the `resources` directory	Each of these files contain locale-specific information that is used by the connector. **Note:** A **resource bundle** is a file containing localized versions of the text strings that are displayed on the user interface of Oracle Identity Manager. These text strings include GUI element labels and messages displayed on the Administrative and User Console.

`scripts/run_initial_recon_provisioning.sh`
`scripts/run_initial_recon_provisioning.bat`
`scripts/racf-adv-initial-recon.jar`
`scripts/initialRacfAdv.properties`
	Files that are used for performing the initial reconciliation run.

`scripts/run_initial_recon_disable.sh` `scripts/run_initial_recon_disable.bat`	These files are scripts that perform the initial reconciliaton run. In addition, these scripts also check for users disabled on the target system and disable them on Oracle Identity Manager.
`xml/oimRacfAdvancedConnector.xml`	The XML file that contains component definitions for the connector.

See Also:

- Step 2: Copying the Connector Files in Chapter 2
- Step 2: Installing the Connector Agents in Chapter 3

How to Use This Guide

The IBM RACF Advanced connector deployment primarily consists of installing the LDAP Gateway, Reconciliation Agent, and Provisioning Agent. The LDAP Gateway is installed on the same system as the Oracle Identity Manager server. The Provisioning Agent and Reconciliation Agents are installed on the mainframe.

The deployment procedure on the Oracle Identity Manager server is different in nature from the deployment procedure on the mainframe. For simplicity, these instructions have been divided into two chapters in this guide:

- Chapter 2, "Deployment on the Oracle Identity Manager Server" covers instructions for deploying the connector on the Oracle Identity Manager system. This consists of configuring the Oracle Identity Manager server, importing the connector XML file, compiling adapters, installing the LDAP Gateway, configuring the message transport layer, and so on.
- Chapter 3, "Connector Deployment on the Target IBM RACF System" includes the second set of instructions to deploy the connector on the mainframe to interface with Oracle Identity Manager. While it may be possible for the Oracle Identity Manager administrator to perform these tasks, it is recommended that these tasks be performed with the assistance of the mainframe administrator.

2

Deployment on the Oracle Identity Manager Server

This chapter covers deploying the connector components on the Oracle Identity Manager server in the following sections:

- Step 1: Verifying Deployment Requirements
- Step 2: Copying the Connector Files
- Step 3: Configuring the Oracle Identity Manager Server
- Step 4: Configuring the Connector to Work with the Oracle Identity Manager Application Server
- Step 5: Importing the Connector XML File
- Step 6: Compiling Adapters
- Step 7: Installing and Configuring the LDAP Gateway

> **Note:** The deployment procedure for the connector components on on the mainframe is covered in Chapter 3, "Connector Deployment on the Target IBM RACF System".

Step 1: Verifying Deployment Requirements

Verify that the system requirements specified in the following table are met for deploying the IBM RACF Advanced Connector.

Item	Requirement
Oracle Identity Manager	Oracle Identity Manager release 8.5.3 or later
Target System	IBM RACF
Mainframe Repository	IBM z/OS v.1.4, with RACF updated to current patch level
Target System Host Platforms	IBM z/OS Mainframe Supports all z/OS versions
Infrastructure Requirements: message transport layer	MQ Series or TCP/IP with AES encryption
Target system user account for Oracle Identity Manager	APF-authorized account with `SystemAdministrators` privileges

Note: The LDAP Gateway works in a seamless manner with Oracle Identity Manager and operates under the user account created for Oracle Identity Manager itself. As a result, it has the same privileges as those granted to the Oracle Identity Manager user account to access and operate with the Provisioning Agent and Reconciliation Agent.

Message Transport Layer Requirements

Between the Oracle Identity Manager and mainframe environments, Oracle Identity Manager supports two different secure message transport layers, TCP/IP and IBM MQ Series.

The MQ Series comes with its own internal setup procedures, which are transparent at the LDAP Gateway level. The primary requirement is that port 1414 is used between Oracle Identity Manager and the mainframe.

Additional configuration is required for the TCP/IP message transport layer. Oracle Identity Manager reserves the following ports for standard message transport layer communication.

- In coordination with an enterprise level architecture, port 5790 is used for the Advanced Provisioning Agent.
- Between the LDAP Gateway and the Reconciliation Agent, Oracle Identity Manager reserves ports 5190 through 5199 as a range of ports for multiple LPARs.

Step 2: Copying the Connector Files

Copy the following connector files to the destinations on the Oracle Identity Manager server as indicated in the following table.

Note: The directory paths given in the first column of this table correspond to the location of the connector files in the following directory on the installation media:

```
Security Applications/IBM RACF/IBM RACF Advanced
```

Refer to the Files and Directories That Comprise the Connector section for more information about these files.

Files	Destination
`etc/LDAP Gateway/ldapgateway.zip`	*`LDAP_install_dir`* The *`LDAP_install_dir`* must be located on the Oracle Identity Manager server.
`lib/racf-adv-agent-recon.jar` `lib/racfConnection.properties`	*`LDAP_install_dir/etc`*

Files	Destination

`lib/idm.jar`
`scripts/run_initial_recon_provisioning.sh`
`scripts/run_initial_recon_provisioning.bat`
`scripts/run_initial_recon_disable.sh`
`scripts/run_initial_recon_disable.bat`
	oim_home`/xellerate/JavaTasks/`

Files in the `resources` directory	*oim_home*`/xellerate/connectorResources/`
`xml/oimRacfAdvancedConnector.xml`	*oim_home*`/xellerate/XLIntegrations/racf/xml/`

Step 3: Configuring the Oracle Identity Manager Server

Configuring the Oracle Identity Manager server involves the following procedures:

- Changing to the Required Input Locale
- Clearing Content Related to Connector Resource Bundles from the Server Cache
- Enabling Logging

> **Note:** In a clustered environment, you must perform these steps on each node of the cluster.

Changing to the Required Input Locale

Changing to the required input locale (language and country setting) involves installing the required fonts and setting the required input locale.

To set the required input locale:

> **Note:** Depending on the operating system used, you may need to perform this procedure differently.

1. Open Control Panel.
2. Double-click **Regional Options**.
3. On the Input Locales tab of the Regional Options dialog box, add the input locale that you want to use and then switch to the input locale.

Clearing Content Related to Connector Resource Bundles from the Server Cache

Whenever you add a new resource bundle in the *oim_home*`/xellerate/connectorResources` directory or make a change in an existing resource bundle, you must clear content related to connector resource bundles from the server cache.

To clear content related to connector resource bundles from the server cache:

1. In a command window, change to the *oim_home*`/xellerate/bin` directory.

2. Enter one of the following commands:

   > **Note:** You must perform Step 1 before you perform this step. If you run the command as follows, then an exception is thrown:
   >
   > *oim_home*/xellerate/bin/*batch_file_name*

   - On Microsoft Windows:

     ```
     PurgeCache.bat ConnectorResourceBundle
     ```

   - On UNIX:

     ```
     PurgeCache.sh ConnectorResourceBundle
     ```

   In this command, `ConnectorResourceBundle` is one of the content categories that you can remove from the server cache. Refer to the following file for information about the other content categories:

   oim_home/xellerate/config/xlConfig.xml

   > **Note:** You can ignore the exception that is thrown when you perform Step 2.

Enabling Logging

When you enable logging, Oracle Identity Manager automatically stores in a log file information about events that occur during the course of provisioning and reconciliation operations. To specify the type of event for which you want logging to take place, you can set the log level to one of the following:

- `ALL`

  This level enables logging for all events.

- `DEBUG`

  This level enables logging of information about fine-grained events that are useful for debugging.

- `INFO`

  This level enables logging of informational messages that highlight the progress of the application at coarse-grained level.

- `WARN`

  This level enables logging of information about potentially harmful situations.

- `ERROR`

  This level enables logging of information about error events that may still allow the application to continue running.

- `FATAL`

  This level enables logging of information about very severe error events that could cause the application to stop functioning.

- `OFF`

  This level disables logging for all events.

The file in which you set the log level and the log file path depend on the application server that you use:

- **For JBoss Application Server**

  To enable logging:

  1. Uncomment or add the following lines in the `JBoss_home/server/default/conf/log4j.xml` file:

     ```
        <category name="XELLERATE">
           <priority value="<log_level>"/>
        </category>
      log_level= WARN or DEBUG or ALL or INFO or ERROR or FATAL or OFF
     ```

  2. In the properties file, replace *`log_level`* with the log level that you want to set.

     ```
     log4j.logger.XELLERATE=log_level

     log_level= WARN or DEBUG or ALL or INFO or ERROR or FATAL or OFF
     ```

  After you enable logging, log information is written to the following file:

  ```
  JBoss_home/server/default/log/server.log
  ```

- **For IBM WebSphere:**

  To enable logging:

  1. Add the following line in the *`OIM_home`*`/xellerate/config/log.properties` file:

     ```
     log4j.logger.XELLERATE=log_level
     ```

  2. In this line, replace *`log_level`* with the log level that you want to set.

     For example:

     ```
     log4j.logger.XELLERATE=INFO
     ```

  After you enable logging, log information is written to the following file:

  ```
  WebSphere_home/AppServer/logs/server_name/startServer.log
  ```

- **For BEA WebLogic**

  To enable logging:

  1. Add the following line in the *`OIM_home`*`/xellerate/config/log.properties` file:

     ```
     log4j.logger.XELLERATE=log_level
     ```

  2. In this line, replace *`log_level`* with the log level that you want to set.

     For example:

     ```
     log4j.logger.XELLERATE=INFO
     ```

  After you enable logging, log information is written to the following file:

  ```
  WebLogic_home/user_projects/domains/domain_name/server_name/server_name.log
  ```

- **For OC4J**

  To enable logging:

1. Add the following line in the *oim_home*/xellerate/config/log.properties file:

   ```
   log4j.logger.XELLERATE=log_level
   ```

2. In this line, replace *log_level* with the log level that you want to set.

   For example:

   ```
   log4j.logger.XELLERATE=INFO
   ```

After you enable logging, log information is written to the following file:

```
OC4J_home/opmn/logs/default_group~home~default_group~1.log
```

Step 4: Configuring the Connector to Work with the Oracle Identity Manager Application Server

The IBM RACF Advanced connector is compatible with the following application servers that Oracle Identity Manager is deployed on:

- JBoss
- IBM WebSphere
- BEA WebLogic
- Oracle Containers for Java (OC4J)

To ensure that the connector works with the application server that Oracle Identity Manager is deployed on, you must the /ldapgateway/bin/run.sh file (or run.bat for Microsoft Windows) and uncomment the lines related to that particular application server. The following are the contents of the run.sh file:

```
SET CLASSPATH VARIABLES
##### SET ENVIRONMENT VARIABLES #######
APP_HOME=/opt/ldapgateway
TMPDIR=/opt/ldapgateway/temp
OIM_HOME=/opt/OIM/xellerate
OIM_CLIENT_LIB=/opt/OIM/client/xlclient/lib

##### SET JBOSS HOME ##################
# APPSERVER_HOME=/opt/ldapgateway/lib/jboss-4.0.2

##### SET WEBSPHERE HOME ##################
#APPSERVER_HOME=/opt/WebSphere/AppServer/lib

##### SET WEBLOGIC HOME ##################
# APPSERVER_HOME=/opt/bea/

##### SET OC4J HOME ##################
#APPSERVER_HOME=/opt/oracle/oc4j
```

You also need to edit the related application server-specific libraries. For more information, refer to the vendor documentation for the application server.

Step 5: Importing the Connector XML File

To import the connector XML file into Oracle Identity Manager:

1. Open the Oracle Identity Manager Administrative and User Console.

2. Click the **Deployment Management** link on the left navigation bar.
3. Click the **Import** link under Deployment Management. A dialog box for locating files is displayed.
4. Locate and open the `oimRacfAdvancedConnector.xml` file, which is in the *`oim_home`*`/xellerate/XLIntegrations/racf/xml/` directory. Details of this XML file are shown on the File Preview page.
5. Click **Add File.** The Substitutions page is displayed.
6. Click **Next**. The Confirmation page is displayed.
7. Click **Next.** The Provide IT Resource Instance Data page for the `OIMRacfResourceObject` IT resource is displayed.
8. Specify values for the parameters of the `OIMRacfResourceObject` IT resource. Refer to the table in the Defining IT Resources section for information about the values to be specified.
9. Click **Next.** The Provide IT Resource Instance Data page for a new instance of the `OIMRacfResourceObject` IT resource type is displayed.
10. Click **Skip** to specify that you do not want to define another IT resource. The Confirmation page is displayed.

    See Also: If you want to define another IT resource, then refer to *Oracle Identity Manager Tools Reference Guide* for instructions.

11. Click **View Selections**.

    The contents of the XML file are displayed on the Import page. You may see a cross-shaped icon along with some nodes. Remove these nodes by right-clicking each node and then selecting **Remove.**

12. Click **Import**. The connector file is imported into Oracle Identity Manager.

Defining IT Resources

You must specify values for the `OIMRacfResourceObject` IT resource parameters listed in the following table.

Parameter Name	Parameter Value (Default)
Resource Asset Name	`OIMRacfResourceObject`
Resource Asset Type	`LDAP Server`
Admin Id	`uid=idfRacfAdmin,ou=People,dc=racf,dc=com`
Admin Password	`idfRacfPwd`
Server Address	`localhost`
Root DN	`dc=racf,dc=com`
Port	`5389`
Is the resource asset to be used to call a method on an API, which resides on a system that is external to Xellerate?	`No`

After you specify values for these IT resource parameters, go to Step 9 of the procedure to import connector XML files.

Step 6: Compiling Adapters

The following adapters are imported into Oracle Identity Manager when you import the connector XML file:

- `CreateRacfUser`
- `ChangePassword`
- `ResetPassword`
- `DeleteUser`
- `RevokeUser`
- `ResumeUser`
- `ModifyUser`
- `GrantTsoAccess`
- `AddUserToGroup`
- `RemoveUserFromGroup`
- `AddUserToDataset`
- `RemoveUserFromDataset`
- `AddUserToResource`
- `RemoveUserFromResource`

To compile adapters by using the Adapter Manager form:

1. Open the Adapter Manager form.
2. To compile all the adapters that you have imported into the current database, select **Compile All**.

   To compile multiple (but not all) adapters, select the adapters you want to compile. Then, select **Compile Selected**.
3. Click **Start.** Oracle Identity Manager compiles the adapters that you specify.
4. If Oracle Identity Manager is installed in a clustered environment, then copy the compiled adapters from the *`oim_home`*`/xellerate/Adapter` directory to the same directory on each of the other nodes of the cluster. If required, overwrite the adapter files on the other nodes.

To view detailed information about an adapter:

1. Highlight the adapter in the Adapter Manager form.
2. Double-click the row header of the adapter, or right-click the adapter.
3. Select **Launch Adapter** from the shortcut menu that is displayed. Details of the adapter are displayed.

Note: To compile multiple adapters simultaneously, use the Adapter Manager form. To compile one adapter at a time, use the Adapter Factory form. Refer to *Oracle Identity Manager Tools Reference Guide* for information about how to use these forms.

Step 7: Installing and Configuring the LDAP Gateway

The LDAP Gateway is installed on the same system as Oracle Identity Manager. To install the LDAP Gateway, do the following:

1. Unzip the `ldapgateway.zip` file to a directory on the same system as Oracle Identity Manager. For convenience, this location is referred to as *`LDAP_install_dir`*.

   See Also: Step 2: Copying the Connector Files

2. Open the `RACF.properties` file located under the *`LDAP_install_dir`*`/conf` directory. Edit this file and specify information for the following properties, depending on whether you use TCP/IP or IBM MQ Series for the message transport layer:

   - For TCP/IP:

   ```
   _type_=socket
   _isencrypted_=true
   _timeout_=5000
   _authretries_=2
   _host_=Host IP Address of the Target RACF System
   _port_=5790
   _agentport_=5190
   ```

   - For MQ Series:

   ```
   _type_=mq
   _isencrypted_=true
   _timeout_=5000
   _authretries_=2
   _qmgr_=CSQ1
   _qhost_=Host IP Address of the Target RACF System
   _qport_=1414
   _qchannel_=CSQ1.PIONEER
   _qname_=PIONEER.REQUEST
   _qreplyname_=PIONEER.REPLY
   ```

3. Extract the `idfserver.jar` file and edit the `beans.xml` file located under *`LDAP_install_dir`*`/dist/`. Edit the `port` property of the server and specify the port used for communication between the Gateway and the mainframe LPAR that you use for the connector installation. For example, the port property is set to `5389` in the following code:

   ```
   <bean id="listener" class=
   "com.identityforge.ximserver.nio.Listener">
   <constructor-arg><ref bean="bus"/></constructor-arg>
   <property name="admin"><value>false</value></property>
   <property name="config"> <value>../conf/listener.xml</value></property>
   <property name="port" value="5389"/>
   </bean>
   ```

4. If you are using IBM MQ Series for the message transport layer, you must also copy the following files to the *`LDAP_install_dir`*`/lib` directory:

   - `com.ibm.mq.jar`
   - `com.ibm.mqbind.jar`
   - `com.ibm.mqjms.jar`

- fscontext.jar
- providerutil.jar

Configuring the LDAP Gateway for Provisioning

To configure Oracle Identity Manager LDAP Gateway for provisioning:

1. Open the `ximserver.jar` and edit the `beans.xml` file located under *`LDAP_install_dir`*`/dist/ximserver.jar`.
2. Find the `<bean name="RACF">` tag and edit the information highlighted in bold in the following code:

```
<bean name="RACF" singleton="true"
class="com.identityforge.ximserver.backend.RACF.RACFModule">

  <!-- The following change is optional. If you make this change, also
       change the metaengine.xml file. -->
  <property name="suffix" value="dc=RACF,dc=com"/>

  <property name="workingDirectory" value="../RACF"/>

  <!-- The following change is optional. -->
  <property name="adminUserDN" value="cn=ximRACFAdmin,dc=RACF,dc=com"/>

  <property name="adminUserPassword" value="ximRACFPwd"/>
  ...
  ...
  <property name="transport">
        <map>
              <!-- Set to MQ if using IBM MQ Series -->
              <entry key="_type_" value="SOCKET"/>

              <!-- Set to true for 128-bit AES encryption. -->
              <entry key="_isencrypted_" value="false"/>

              <!-- Set to IP of RACF system. -->
              <entry key="_host_"
                     value="Host IP Address of the Target RACF  System"/>
              ...
              ...
        </map>
  </property>
  <property name="Connector" value="false"/>
</bean>
```

3. If the domain partition was changed from the default `"dc=RACF,dc=com,"` open up the `metaengine.xml` file located under *`LDAP_install_dir`*`/conf`.
   a. Replace all occurrences of the domain partition "`dc=RACF,dc=com`" with the domain partition that was chosen for your installation.
   b. Save the file.

3

Connector Deployment on the Target IBM RACF System

The Provisioning and Reconciliation Agent Components of the IBM RACF Advanced Connector are installed on the mainframe. This chapter describes the installation and configuration of the Provisioning Agent and Reconciliation Agent in the following sections:

- Step 1: Verifying Deployment Requirements
- Step 2: Installing the Connector Agents
- Step 3: Installing the Exits for the Reconciliation Agent
- Step 4: Configuring the Message Transport Layer

Step 1: Verifying Deployment Requirements

The following table identifies hardware, software, and authorization prerequisites for the installing Provisioning Agent and Reconciliation Agent.

Item	Requirement
Operating System	IBM z/OS any version Verify that all current patches are in place.
Message Transport Layer	TCP/IP Network with AES encryption MQ Series v.5 or later
RACF Identity Repository	Current patch level for z/OS
Target system user account for the Provisioning Agent and Reconciliation Agent	APF-authorized user accounts with `SystemAdministrators` privileges

The Provisioning Agent and the Reconciliation Agent are installed on the mainframe. Both require the installation of a started task. In addition, these agents function under a user account on the mainframe system. This user account must be created by the mainframe administrator during the deployment of the Provisioning Agent and the Reconciliation Agent.

> **Note:** Both the Provisioning Agent and Reconciliation Agent user accounts require placement into an administrative APF-authorized library. These user accounts must have at least the permissions of the `SystemAdministrators` group on the mainframe. These user accounts have permissions above those of ordinary administrators on the mainframe, which include Read, Write, Execute, and Modify privileges.

Environmental Settings and Requirements

To deploy the IBM RACF Advanced Connector, ensure that the following requirements are met on the mainframe:

- Each agent uses memory subpools to manage peak load conditions. These subpools require 1.5 to 2.0 MB of mainframe memory for operations. This is configured at the time of Provisioning Agent and Reconciliation Agent installation.
- In addition to the program itself, the user account that a program runs under must also have authorization to access subpools on the host platform. This must be done by the mainframe administrator.
- If MQ Series is used for the message transport layer, an MQ administrator will be needed to authorize the creation of MQ queues from an automated script that comes with the connector.

  Oracle Identity Manager requires three queues: a send queue, a receive queue, and a communication queue for the Reconciliation Agent. The MQ administrator creates these queues and typically names them according to the naming conventions used in the system. These names are automatically inserted into the Provisioning Agent and Reconciliation Agent start up Job Control Language (JCL) program.
- If TCP/IP is used in the message transport layer, an administrator must have authorization to create ports on the mainframe, as well as provide security authorizations.
- The Reconciliation Agent operates using user exit technology, outside the mainframe operating system. This means it runs in a different LPAR from the operating system.

  Typical mainframe shops install custom exits, for example to maintain a certain password format. Oracle Identity Manager exits are engineered to be the last exits called in sequence, allowing existing exits to function normally. After modifying exits within a logical partition (LPAR), an initial program load (IPL) of the LPAR may be required.

Step 2: Installing the Connector Agents

These are the initial steps for installing the components of the IBM RACF Advanced connector on z/OS.

1. Transmit or FTP `JCL.XMIT` and `LINKLIB.XMIT` to the z/OS server, each with the following specifications: `RECFM=FB`, `LRECL=80`, `BLKSIZE=3120`, and `DSORG=PS`.
2. Log in to the z/OS server's TSO environment.
3. Expand the `CNTL` data sets, issue the following command from the ISPF command line:

```
TSO RECEIVE INDA('IDF.CNTL.XMIT')
```

4. When prompted to specify restore parameters, enter:

   ```
   DA('IDF.CNTL')
   ```

5. To expand the LINKLIB data set, enter the following command on the ISPF command line:

   ```
   TSO RECEIVE INDA('IDF.LINKLIB.XMIT')
   ```

6. When prompted to enter restore parameters, enter:

   ```
   DA('IDF.LINKLIB')
   ```

7. To complete the installation, follow the procedures in IDF.CNTL member #INSTVOY for the Reconciliation Agent components, and member #INSTPIO for the Provisioning Agent component.

Step 3: Installing the Exits for the Reconciliation Agent

Because the exits reside in LPARs, an IPL is required to complete the installation. To allow the LDAP Gateway to fully capture events, the Reconciliation Agent and its exits should be installed on each LPAR that shares the IBM RACF authentication repository.

To install the Reconciliation Agent exits:

1. Install LOGRIX02, LOGPWX01, and LOGEVX01, the Common Command exits, using the Dynamic Exit Facility.
2. For testing, it is recommended that you set up one or more PROGxx members in SYS1.PARMLIB (or equivalent), to allow for easy removal of the exit if desired.
3. The following commands comprise the PARMLIB list. These commands can also be added with operator console commands. The following sample command is used to append the Reconciliation Agent exits to the appropriate IBM RACF exits.

   ```
   EXIT ADD EXITNAME(ICHRIX02) MODULE(LOGRIX02)
   EXIT ADD EXITNAME(ICHPWX01) MODULE(LOGPWX01)
   EXIT ADD EXITNAME(IRREVX01) MODULE(LOGEVX01)
   ```

4. Copy these three members to your system PARMLIB data set.
5. If you already have a PROGAD or PROGDL member, rename the LOG members to a PROGxx name that is not in use.
6. When ready, use the console command SET PROG=XX to activate LOGPWX01 as an ICHPWX01 exit point.
7. When Ready, use the console command SET PROG=XX to activate LOGRIX02 as an ICHRIX02 exit point.
8. When ready, use the console command SET PROG=XX to activate LOGEVX01 as an IRREVX01 exit point.

Permanent Installation

For permanent installation, do one of the following:

- Add the EXIT ADD statement in PROGAD to your production PROGxx PARMLIB member.
- Add a SET PROG=XX command to CONSOL00 or an automation script, so that it is issued during your IPL procedure.

- Install ICHRIX02, the RACROUTE REQUEST=VERIFY(X) (RACINIT) post processing exit.

> **Note:** If you do not have an existing ICHRIX02 exit, run the job in the samples library member RIX0A. This job uses SMP/E to linkedit LDXRIX02 into SYS1.LPALIB as exit ICHRIX02.

Loading Exits

To load the exits:

- Command done from the Operator Log (ISPF menu option SDSF then option LOG)

```
/F LLA,REFRESH
/T PROG=XX Where XX is the Parmlib list name created EX. PROG75
/T PROG=75
```

Viewing Exits

To look at the exits:

```
/D PROG,LPA,MODNAME=ICHPWX01
/D PROG,LPA,MODNAME=ICHRIX02
/D PROG,LPA,MODNAME=IRREVX01
```

Sample output of the display command:

```
15:47:38 D PROG,LPA,MODNAME=ICHPWX01
15:47:38 CSV550I 15.47.38 LPA DISPLAY 321
15:47:38 FLAGS MODULE  ENTRY PT LOAD PT  LENGTH  DIAG
15:47:38  P  ICHPWX01 85024C68 05024C68 00000398 0DA015F8

15:47:38 D PROG,LPA,MODNAME=ICHPWX01
15:47:38 CSV550I 15.47.38 LPA DISPLAY 321
15:47:38 FLAGS MODULE  ENTRY PT LOAD PT  LENGTH  DIAG
15:47:38  P  ICHPWX01 85024C68 05024C68 00000398 0DA015F8
```

Uninstalling the Exits

If you need to uninstall the Reconciliation Agent exits, enter SET PROG=XY as a console command or enter the following commands.

```
EXIT DELETE EXITNAME(ICHRIX02) MODULE(LOGRIX02)
EXIT DELETE EXITNAME(ICHPWX01) MODULE(LOGPWX01)
EXIT DELETE EXITNAME(IRREVX01) MODULE(LOGEVX01)
```

Step 4: Configuring the Message Transport Layer

This section describes the following Message Transport Layer configuration tasks for both TCP/IP and MQ Series:

- Configuring TCP/IP
- Using MQ Series
- Building and Operation of the Starter Tasks

Configuring TCP/IP

This section describes configuring TCP/IP as the message transport layer for the IBM RACF Advanced connector on the z/OS system. The rules for using TCP/IP are beyond the scope of this document, but affect the startup and communication sequences. The goal is to establish a stateful connection, allowing the pooling of messages and significantly reducing the load on both the mainframe and the LDAP Gateway server.

1. Start up the Oracle Identity Manager LDAP Gateway. This must be previously configured to connect to the mainframe using a given IP address and port number.
2. Start the Provisioning Agent started task, which is also preset to establish the TCP/IP connection to the LDAP Gateway on a specified IP address and port number.

   The same procedure applies to the Reconciliation Agent. Start the LDAP Gateway, and then initiate the Reconciliation Agent started task.

To use TCP/IP for the message transport layer, you will need the following IP addresses:

- IP address to be used by z/OS
- IP address for the router
- IP addresses for domain name servers

For using TCP/IP as the message transport layer, you might need the help of a mainframe administrator to allow for the creation of ports on the mainframe, as well as providing security authorizations for the data structures.

To edit the Provisioning Agent and Reconciliation Agent JCL:

1. Insert an installation-approved job card.
2. Change the value for `PARM` =('`TCPN=TCPIP`' to the name of the running TCP/IP started task).
3. Change the IP address to the address of the LPAR (z/OS System that Provisioning Agent will be started from).
4. Change the port number to the port assigned in the LPAR (z/OS System that Provisioning Agent will be started from).
5. If your installation requires batch feeds then insert the proper `VSAMGETU` statement. The following code shows the batch loading of IBM RACF ACIDs:

```
//USR98S01 JOB (,xxxxxxxx,,'PROVISIONING AGENT UPLOAD PROCESS FOR ACIDS'),
//       'UPLOAD CATS TO XELLTE',
//       REGION=2M,CLASS=6,MSGCLASS=Q,
//       USER=XXXXXXXX,TIME=1440,
//       NOTIFY=&SYSUID,TYPRUN=HOLD
//*
/*ROUTE PRINT CLE
//*
//PIONEERX EXEC PGM=PIONEERX,REGION=0M,TIME=1440,
//       PARM=('TCPN=TCPIP',
//       'IPAD=Host IP Address of the IBM RACF System',
//       'PORT=6500',
//       'DEBUG=Y')
//STEPLIB DD DISP=SHR,DSN=PPRD.IDF.LINKLIB
//     DD DISP=SHR,DSN=SYS2.TCPACCES.V60.LINK
//     DD DISP=SHR,DSN=TCPIP.SEZATCP
//SYSOUT  DD SYSOUT=*
```

```
//SYSPRINT DD SYSOUT=*
//SYSDBOUT DD SYSOUT=*
//SYSABOUT DD SYSOUT=*
//ABENDAID DD SYSOUT=*
//SYSUDUMP DD SYSOUT=*
//VSAMGETU DD DISP=SHR,DSN=LXT99S.FEEDFILE.SORTED
//*
```

For the Reconciliation Agent, the Job Control is the same with the exception of the execute card, which is shown here:

```
 //VOYAGERX EXEC PGM=VOYAGERX,
//   PARM=('TCPN=TCPIP',
//      'IPAD=Host IP Address of the IBM RACF System',
//      'PORT=5791',
//      'DEBUG=Y')
```

For both Reconciliation Agent and Provisioning Agent the following DEBUG parameter field equivalents can be used:

```
* VALID DEBUG PARMS ARE: N, Y, Z
*  N IS FOR NO DEBUGGING OUTPUT
*  Y IS FOR DEBUGGING OUTPUT
*  Z IS FOR DEBUGGING OUTPUT, BUT DO NOT WRITE TO MQ.
```

> **Note:** If you get the "data set in use" message when attempting to edit a member, use the F1 key to see the member in question that you are trying to edit. You will have to press the F1 key twice. The second time will actually give the name of the job using the file that you are trying to edit. You can then go to the z/OS console and remove it by using the p or c command.

Using MQ Series

This section describes the installation of the Provisioning and Reconciliation Agents and configuring them to use IBM MQ Series.

Provisioning Agent Installation for MQ Series

Provisioning Agent uses the following members for MQ installation:

- PIONEER: The Provisioning Agent start task job control
- PIOCOPY: Copies the Provisioning Agent-started task to your installation procedure library.
- PIODEF: Defines the Provisioning Agent MQ definitions
- PIOMQ: Provisioning Agent MQ definition input

To install the Provisioning Agent:

1. Edit member PIONEER:

   a. Change "QMGR" in the QMGR PARM field to the name of your queue manager. Your Queue manager is the actual task name given to the MQ Queue manager in the system.

   b. If required, enable the debug option by setting Debug=N (the default) to Y.

Caution: This will generate a large amount of output. This should only be done for testing.

---

c. Change `Idf.Linklib` to the name you have given the Oracle Identity Manager Authorized Load Module Library.

2. Edit member `PIOCOPY` and submit:

   a. Insert your installation approved job card.

   b. Change `IDF.CNTL` to the name you have given the Oracle Identity Manager Control Library. See Step 2: Installing the Connector Agents.

   c. Change `SYS1.PROCLIB` to the name of the `JES PROCLIB` you would like to use.

   d. Change the Reconciliation Agent-started task to initiate as a started task.

   e. Submit `PIOCOPY`. Ensure that the member `VOYAGER` is present in your selected `JES PROCLIB`.

3. Edit member `PIOMQ`:

   a. Change all occurrences of "`QMGR`" to the name of your queue manager. Your Queue manager is the actual task name given to the MQ Queue manager in the system.

   b. Change all occurrences of "`STGCLASS`" to the name of the storage class for the two Provisioning Agent queues.

Note: For performance reasons, your installation may want to define the two Provisioning Agent queues to different storage classes. If you are also using the Reconciliation Agent, you may want to use separate storage classes for the Reconciliation Agent queue.

---

4. Edit member `PIODEF` and submit:

   a. Insert your jobcard.

   b. Change "`QMGR`" in the PARM to the name of your queue manager.

   c. Change "`MQMHLQ`" to the high level qualifier of your MQ System datasets.

   d. Change `IDF.CNTL` to the name you have given the Oracle Identity Manager control library.

Note: Depending on your security environment, you may need to define Provisioning Agent as a started task and grant access to the dataset and MQ resources.

The Provisioning Agent is ready to start.

Note: The Provisioning Agent is dependent on MQ series, so you must ensure that the queue manager is active before starting the Provisioning Agent.

If the Provisioning Agent is a started task, then start Provisioning Agent by issuing `S PIONEER` from the console. If Provisioning Agent is a batch task, then submit the `PIONEER JCL`.

Reconciliation Agent Installation for MQ series

The Reconciliation Agent installation members in the control library are:

- `VOYAGER`: Reconciliation Agent started task job control
- `VOYCOPY`: Copies the `VOYAGER` Reconciliation Agent started tasks to the procedure library
- `VOYDEF`: Defines the Reconciliation Agent MQ definitions
- `VOYINIT`: Reconciliation Agent initialization started task
- `VOYKILL`: Reconciliation Agent subpool removal started task
- `VOYMQ`: Reconciliation Agent MQ definition input
- `VOYSTOP`: Reconciliation Agent stop started task

To install the Reconciliation Agent:

1. Edit member `VOYAGER`:

   a. Change "`QMGR`" in the `QMGR PARM` field to the name of your queue manager. Your queue manager is the actual task name given to the MQ Queue manager in the system.

   b. If required, enable the debug option by changing `Debug=N` to `Y`.

   Caution: This will generate a large amount of output. This should only be performed for testing purposes.

   c. Change `IDF.LINKLIB` to the name you have given the Oracle Identity Manager Authorized Load Module Library.

2. Edit members `VOYINIT`, `VOYKILL`, and `VOYSTOP`:

   Change `IDF.LINKLIB` to the name you have given the Oracle Identity Manager Authorized Load Module Library.

3. Edit member `VOYCOPY` and submit.

   a. Insert your installation approved job card.

   b. Change `IDF.CNTL` to the name you have given the Oracle Identity Manager control library.

   c. Change `SYS1PROCLIB` to the name of the `JESPROCLIB` proclib you would like Voyager to be started from as a started task.

   d. Ensure that members `VOYAGER`, `VOYINIT`, `VOYKILL`, and `VOYSTOP` are present in selected `JES PROCLIB`.

4. For installation with MQ Series: edit member `VOYMQ`.

a. Change all occurrences of "`QMGR`" to the name of your queue manager. Your queue manager is the actual task name given to the MQ Queue manager in the system.

b. Change all occurrences of `+STGCLASS+` to the name of the storage class for the Reconciliation Agent queue.

> **Note:** You may want to assign the Reconciliation Agent to a different storage class than the one used by the Provisioning Agent queues.

5. Edit member `VOYDEF` and submit.

   a. Insert your job card.

   b. Change "`QMGR`" in the parameter to the name of your queue manager. Your queue manager is the actual task name given to the MQ Queue manager in the system.

   c. Change `+MQMHLQ+` to the high level qualifier of your MQ system datasets.

   d. Change `IDF.CNTL` to the name you have given the Oracle Identity Manager Control Library.

   e. Ensure that the three objects are defined without errors.

> **Note:** Depending on your security environment, you may need to define `VOYAGER`, `VOYINIT`, `VOYKILL`, and `VOYSTOP` as started tasks and grant access to the dataset and MQ resources.

The Reconciliation Agent is ready to start.

Additional Notes

- The Reconciliation Agent is dependent on MQ. Therefore, ensure that the queue manager is active before starting the Reconciliation Agent.
- Start the `VOYINIT` task by issuing "`S VOYINIT`" from the console to create the subpool (this only needs to be done once, unless `VOYKILL` is run).
- Once `VOYINIT` ends, then start Reconciliation Agent by issuing "`S VOYAGER`" from the console.
- To quiesce `VOYAGER` while leaving the subpool intact, start `VOYSTOP` by issuing "`S VOYSTOP`" from the console. To quiesce Reconciliation Agent and destroy the subpool, start `VOYKILL` by issuing "`S VOYKILL`" from the console. Use of `VOYKILL` will cause any messages stored in the subpool to be lost.

Note: Events detected by the Reconciliation Agent through exit technology are transformed into messages and passed to the LDAP Gateway.

If MQ Series is used as the message transport layer, these messages are secured internally within the MQ system for delivery.

If the TCP/IP message transport layer is used, the messages are securely sent to the Gateway. If the Gateway is down, messages are held until the Gateway is returned to service, but also secured in an AES encrypted file on the mainframe. When the Gateway resumes, the messages are then sent.

If the subpool is stopped by an administrator, it shuts down the Provisioning Agent, destroying any messages not transmitted. However, the messages in the secured AES-encrypted file are not affected and can be recovered.

Configuration of APF Authorization

APF stands for the IBM Authorized Program Facility. Granting a program the APF Authorized status is similar to giving superuser status. This process will allow a program to run without allowing normal system administrators to query or interfere with its operation. Both the program that runs on the mainframe system and the user account it runs under must have APF authorization. For example, the Provisioning Agent user account must also have APF authorization.

Note: APF authorization is usually done by a mainframe administrator. If you do not have the required authority to perform such tasks, you should arrange to enlist the assistance of someone who is qualified to perform these tasks.

For APF authorization, you need to create the necessary definitions.

- Logon to TSO by using a user account that has the requisite authority to execute IBM RACF commands and modify the IBM RACF database. For example, IBMUSER normally has such authority.
- From a TSO command line (or Option 6 of ISPF), issue the following IBM RACF command:

  ```
  RDEFINE FACILITY IRR.RADMIN.* UACC(NONE)
  ```

  This command defines a IBM RACF resource named `IRR.RADMIN.*` in the `FACILITY` class.
- From a TSO command line (or Option 6 of ISPF), issue the following IBM RACF command:

  ```
  PERMIT IRR.RADMIN.* CLASS(FACILITY) ID(STARTER) ACCESS(READ)
  ```

  This command grants READ access to the resource `IRR.RADMIN.*` for user account `STARTER` (an example of the user account for the starter task). This allows the starter task to issue RACF commands.
- From a TSO command line (or Option 6 of ISPF), issue the following IBM RACF command:

```
ALTUSER STARTER SPECIAL
```

This command grants the `SPECIAL` attribute to user account `STARTER`, which allows the started task to access and modify IBM RACF User Profiles.

- Issue the following command from a TSO command line (or Option 6 of ISPF):

  ```
  SETROPTS RACLIST(FACILITY) REFRESH
  ```

  This command updates the in-storage tables of IBM RACF to immediately activate the definitions that you create.

- Exit from ISPF.

Building and Operation of the Starter Tasks

There are two different JCLs to set up and run the Provisioning Agent and Reconciliation Agent. You can use these two JCL files for the basis of a starter task definition.

The parameters for `RUNPIONX.txt` are:

- `TCPN`, the name of the TCP process
- `IPAD`, the IP address of the system that the Provisioning Agent is running on
- `PORT`, the incoming connection port for the Provisioning Agent
- `DEBUG`, the debug switch for showing the extra output

The parameters for `RUNVOYAX.txt` are:

- `TCPN`, the name of the TCP process
- `IPAD`, the IP address of the system that the Reconciliation Agent is connected to
- `PORT`, the outgoing connection port for the Reconciliation Agent
- `DEBUG`, the debug switch for showing the extra output

Source code for each program is:

```
RUNPIONX:

//ADCDMPPT JOB SYSTEMS,MSGLEVEL=(1,1),MSGCLASS=X,CLASS=A,PRTY=8,
//  NOTIFY=&SYSUID,REGION=4096K
//PIONEERX EXEC PGM=PIONEERX,REGION=0M,TIME=1440,
//  PARM=('TCPN=TCPIP',
//     'IPAD=Host IP Address of the IBM RACF System',
//     'PORT=5790',
//     'DEBUG=Y')
//STEPLIB DD DISP=SHR,DSN=IDF.LINKLIB
//     DD DISP=SHR,DSN=TCPIP.SEZATCP
//SYSPRINT DD SYSOUT=X
//SYSUDUMP DD SYSOUT=X
//


RUNVOYAx:

//ADCDMRVX JOB SYSTEMS,MSGLEVEL=(1,1),MSGCLASS=X,CLASS=A,PRTY=8,
//  NOTIFY=&SYSUID,REGION=4096K
//VOYAGERX EXEC PGM=VOYAGERX,REGION=0M,TIME=1440,
//  PARM=('TCPN=TCPIP',
//     'IPAD=Host IP Address of the IBM RACF System',
```

```
//     'PORT=5190',
//     'DEBUG=Y')
//STEPLIB DD DISP=SHR,DSN=IDF.LINKLIB
//     DD DISP=SHR,DSN=TCPIP.SEZATCP
//SYSPRINT DD SYSOUT=X
//SYSUDUMP DD SYSOUT=X
//
```

4 Initial Reconciliation Run

Reconciliation with the IBM RACF Advanced connector is carried out in real time. This implies that after you have imported the initial load of user information, you need not perform reconciliation as a scheduled task. The initial reconciliation run involves obtaining user information from the target system into the Oracle Identity Manager server. This allows for the extension of enterprise user management of profiles and authorization of resources.

The initialization process is run from the command line on the Oracle Identity Manager server. The commands are run from the *oim_home*/xellerate/JavaTasks directory. There are non-trusted example scripts for initial provisioning and initial disabling at the following location:

```
IBM RACF Advanced Rev 9.0.3/scripts
```

These non-trusted scripts are:

```
run_initial_recon_provisioning.bat
run_initial_recon_disable.bat
```

The controls for the commands in these files are specified in the initialRacfAdv.properties file. The following is a sample set of values for these parameters:

```
xlAdminId:xelsysadm
xlAdminPwd:xelsysadm
xlJndiUrl:jnp://IP Address of the OIM Server:1099
idfTrusted:true
idfServerUrl:ldap://localhost:5389
idfAdminDn:cn=idfRacfAdmin, dc=racf,dc=com
idfAdminPwd:idfRacfPwd
ouPeople:ou=People
ouGroups:ou=Groups
ouDatasets:ou=Datasets
ouResources:ou=Resources
ouFacilities:ou=Facilities
ouBaseDn:dc=racf,dc=com
idfSystemAdminDn:cn=Directory Manager, dc=system,dc=backend
idfSystemAdminPwd:testpass
idfSystemDn:dc=system,dc=backend
idfIgnoreIdList:start1,start2,private
idfDoOnlyIdList:martin81,martin82,martin83
idList=do
```

To include or exclude specific users during initial reconciliation, modify the following lines:

```
idfIgnoreIdList:start1,start2,private
idfDoOnlyIdList:jdoe81,jdoe82,jdoe83
```

Note: This control does not support wildcards and is designed for processing or excluding a limited number of users.

Configuring Trusted Source Reconciliation

To configure the connector to perform trusted source reconciliation, set the `idfTrusted` control in the `initialRacfAdv.properties` file to `true`, as follows:

```
idfTrusted:true
```

This control toggles trusted source reconciliation in the connector. Set this to `false` if you are not performing reconciliation with a trusted source.

In addition, you must make a copy of the non-trusted scripts and change the `JV` parameter first to `-X`, and then to `-R`.

5 Testing and Troubleshooting

After you deploy the connector, you must test it to ensure that it functions as expected. This chapter contains information on the following types of testing:

- **Connectivity testing**: All message transport layers have a dependency on open ports, allowing application data to be to be passed between applications and between systems. This test checks for open ports on the mainframe system from the Oracle Identity Manager system. Both the IBM MQ Series and TCP/IP depend on open ports to communicate.
- **Provisioning Testing:** This type of test involves using Oracle Identity Manager for provisioning or de-provisioning one of its users or organizations with a target resource. In other words, Oracle Identity Manager is the starting point of the connector, and the target resource is the end point.
- **Reconciliation Testing:** In this type of test, you reconcile Oracle Identity Manager with the target resource. In other words, the target resource is the starting point of the connector, and Oracle Identity Manager is the end point.

This chapter contains the following sections:

- Port Connectivity Testing
- Running Test Cases
- Troubleshooting
- Performance Tests

Port Connectivity Testing

This section discusses open port testing for the connector. Testing of open ports is done on the Oracle Identity Manager server system.

The following tests assume that the test will be conducted on the Oracle Identity Manager server, with required ports open to the mainframe.

1. For IBM MQ Series messaging, the standard port is 1414. Connectivity to this port is tested from the Oracle Identity Manager server.
2. The TCP/IP message transport layer relies on several different ports. The ports should be checked from the Oracle Identity Manager server to the mainframe. For provisioning to IBM RACF, check for open ports between the two systems for port 5791. The reconciliation agent uses port 5190.

Note:

- Check your specific setup configuration files for the actual provisioning and reconciliation agent port numbers used in your deployment.
- It is common for the mainframe TCP/IP configuration and the IBM RACF Advanced Connector Adapter JCLs to have the same code set, even if multiple LPARs and connectors are used. As the port traffic passes through a router, the public IP address then becomes different from the private locally assigned system IP address. This conversion of the private and public IP address can also extend to remapping to the ports.

Running Test Cases

This section focuses on the functional and performance test cases that are associated with this connector. The following table includes information on running test cases on the IBM RACF Advanced connector:

Test Case	Test Type	Description/Comment
Test to change IBM RACF Password	Provisioning	A user password is changed, with the change posted to the mainframe through the connector.
Test to reset IBM RACF Password	Provisioning	A user password is reset, with the change posted to the mainframe through the connector.
Test to create IBM RACF User	Provisioning	A user is created, with the change posted to the mainframe through the connector.
Test to revoke/disable IBM RACF User Account	Provisioning	A user account is revoked, with the change posted to the mainframe through the connector.
Test to resume IBM RACF User Account	Provisioning	A user account is resumed from a revoked status, with the change posted to the mainframe through the connector.
Test to List IBM RACF Users	Provisioning	A list of users is retrieved from the mainframe IBM RACF repository.
Test to Permit IBM RACF User Access to Resource Profile	Provisioning	A user is authorized to access mainframe resources, with change posted to the mainframe through the connector.
Test to permit IBM RACF User Access to TSO	Provisioning	A user is provisioned to log on to the mainframe through TSO, with the change posted to the mainframe through the connector.
Test to remove IBM RACF User Access to Dataset	Provisioning	A user is removed from access to a mainframe dataset, with the change posted to the mainframe through the connector.
Test to remove IBM RACF User Access to Resource Profile	Provisioning	A user is removed from access to a mainframe resource, with the change posted to the mainframe through the connector.

Test Case	Test Type	Description/Comment
Test to detect and report Native IBM RACF Password Change Event	Reconciliation	A native password change is made on the mainframe and subsequently detected by the connector.
Test to detect and report Native IBM RACF Password Reset Event	Reconciliation	A native password reset is made on the mainframe and subsequently detected by the connector.
Test to detect and report Native IBM RACF Create User Data Event	Reconciliation	User creation is done by an administrator natively on the mainframe and subsequently detected by the connector.
Test to detect and report Native IBM RACF Revoke User Event	Reconciliation	A user account password is revoked through native mainframe events, which is subsequently detected by the connector.
Test to detect and report Native IBM RACF Delete User Event	Reconciliation	A user account is deleted through native mainframe events, which is subsequently detected by the connector.
Test to detect and report Native IBM RACF Resume User Event	Reconciliation	A user account is resumed from a revoke status through native mainframe events, which is subsequently detected by the connector.

Troubleshooting

The following table lists solutions to some commonly encountered issues associated with the IBM RACF Advanced Connector.

Problem Description	Solution
Oracle Identity Manager cannot establish a connection to the IBM RACF Server.	■ Ensure that the mainframe server is up and running. ■ Check that the necessary ports are working. ■ Due to the nature of the Provisioning Adapter, the Gateway must be started first, and then the mainframe JCL started task must be initiated. This is a requirement based on how TCP/IP operates. Check that the server IP which hosts the Gateway is configured in the Reconciliation Agent JCL. ■ View the Gateway logs to determine if messages are being sent or received. ■ Examine the Oracle Identity Manager configuration to verify that the IP address, admin ID, and admin password are correct. ■ Check with the mainframe platform manager to verify that the mainframe user account and password have not been changed.
The mainframe does not appear to respond.	■ Ensure that the Oracle Identity Manager mappings are correct. ■ Check the configuration mappings for the Advanced Adapter Gateway. ■ Check that the mainframe JCL jobs have not ABENDED. If so, determine the reason for the ABEND and ask the mainframe administrator to restart the jobs.

Problem Description	Solution
A particular use case does not appear to be functioning.	■ Check for the use case event in question on the Gateway Server Log. Then check for the event in the specific log assigned to that Advanced Connector. ■ If the event does not register in either of these two logs, investigate the connection between Oracle Identity Manager and the Advanced Connector Gateway. ■ If the event is in the log but the command has not had the intended change on a mainframe user profile, check for configuration and connections between the Gateway and the mainframe. ■ Check that TCP/IP is turned on or that the IBM MQ series is operational, depending on the particular message transport layer chosen.

Performance Tests

The IBM RACF Advanced Connector architecture has been engineered for enterprise-level performance. When an identity event passes through an exit, the Reconciliation Agent analyzes the event, and then creates a message, allowing the command to complete its routine without loss of time.

A given event will typically fire multiple exits at the same time. For example, a batch job that generates a password change identity event will fire both a batch exit and a password change exit. The Reconciliation Agent captures both events, filters duplicate entries, and passes the result to the Oracle Identity Manager LDAP Gateway.

A batch job to change 50,000 passwords has been tested on a single LPAR to complete within 10 minutes. Because two exits were involved, 100,000 messages were created, filtered, and transformed into MQ messages. The LDAP Gateway then took 30 minutes to retrieve and update the Oracle Identity Manager identity store, with most of that time consumed by the LDAP database.

The LDAP Gateway is engineered to detect when a given event originates from Oracle Identity Manager, when it passes through the Reconciliation Connector. Provisioning Agent events also create a native exit event that is detected. To prevent a feedback loop, events that originate from the LDAP Gateway are logged, but are not reported again to Oracle Identity Manager. By contrast, events that originate outside Oracle Identity Manager are treated as native events, and recorded for future auditing.

The LDAP Gateway and Reconciliation securely capture, filter, and log the identity events from the host system, publishing them for use by Oracle Identity Manager.

6

Known Issues

The following are known issues associated with this release of the connector:

- The IBM RACF Advanced Connector can accept and transmit any non-ASCII data to the mainframe, but the mainframe does not accept non-ASCII characters. As a result, any task that requires non-ASCII data transfer fails. In addition, there is no provision in the connector to indicate that the task has failed or that an error has occurred on the mainframe. You must exercise caution when providing inputs to the connector for the target system, especially when using a regional language interface.
- Passwords used on the mainframe must conform to stringent rules related to passwords on mainframes. These passwords are also subject to restrictions imposed by corporate policies and rules about mainframe passwords. While creating user accounts for target systems on the mainframe, you must take these requirements into account before assigning passwords for these accounts.
- This only applies to a configuration where a single LDAP Gateway connects to multiple installations of the target system. If you configure the connector for trusted source reconciliation and set the `idfTrusted` parameter to true in one of the target system installations on the mainframe, then it must be set to true in all installations that connect to the same Gateway. Otherwise, the connector will fail to work.

A

Attribute Mapping Between Oracle Identity Manager and IBM RACF

The following tables describe the schema used by the Oracle Identity Manager LDAP Gateway.

- Table A–1, " User Attribute Descriptions"
- Table A–2, " Group Attribute Descriptions"
- Table A–3, " Dataset Resource Profile Attribute Descriptions"

Table A–1 User Attribute Descriptions

Oracle Identity Manager Gateway Attribute	IBM RACF Attribute	Description
uid	USER	User login ID
cn	NAME	User full name
sn	NAME	User last name
givenName	NAME	User first name
userPassword	PASSWORD	Password used to login
attributes	SPECIAL, AUDITOR, GPRACC, OPERATIONS	Attributes for the user
owner	OWNER	The owner of the user profile
defaultGroup	DEFAULT-GROUP	Default group for the user
instdata	DATA	Installation-defined data for the user
createdate	CREATED	Date user was created
passwordDate	PASSDATE	Date the user password expires
passwordInterval	PASS-INTERVAL	The number of days a password remains valid for the user
revokeDate	REVOKE DATE	Future date the user will be prevented from accessing the system
resumeDate	RESUME DATE	Future date the user will be allowed access to the system again
memberOf	GROUP	Group information for the user
dataset	MODEL	Dataset profile of the user
lastaccessdate	LAST-ACCESS	Last time the user accessed the system

Table A–1 (Cont.) User Attribute Descriptions

Oracle Identity Manager Gateway Attribute	IBM RACF Attribute	Description
lastconnectdate	LAST-CONNECT	Last time the user connected
tsocommand	COMMAND	Command to be run during TSO/E logon
tsodest	DEST	Default SYSOUT destination
tsoseclabel	SECLABEL	User's security label
tsounit	UNIT	Default UNIT name for allocations
tsouserdata	USERDATA	Installation-defined data for the user
tsoacctnum	ACCTNUM	Default TSO account number on the TSO/E logon panel
tsoholdclass	HOLDCLASS	Default hold class
tsojobclass	JOBCLASS	Default job class
tsomaxsize	MAXSIZE	The maximum region size the user can request at logon
tsomsgclass	MSGCLASS	Default message class
tsoproc	PROC	Default logon procedure on the TSO/E logon panel
tsosize	SIZE	Minimum region size if not requested at logon
tsosysoutclass	SYSOUTCLASS	Default SYSOUT class
revoke	NA	Value 'Y' if user is revoked or 'N' if user is resumed
waaccnt	WAACCNT	Account number for APPC/z/OS processing
waaddr1	WAADDR1	Address line 1 for SYSOUT delivery
waaddr2	WAADDR2	Address line 2 for SYSOUT delivery
waaddr3	WAADDR3	Address line 3 for SYSOUT delivery
waaddr4	WAADDR4	Address line 4 for SYSOUT delivery
wabldg	WABLDG	Building for SYSOUT delivery
wadept	WADEPT	Department for SYSOUT delivery
waname	WANAME	User name for SYSOUT delivery
waroom	WAROOM	Room for SYSOUT delivery

Table A–2 Group Attribute Descriptions

Oracle Identity Manager Attribute	IBM RACF Atribute	Description
cn	GROUP	The group ID
uniqueMember	USERS	The users associated to the group
owner	OWNER	The owner of the group
subgroups	SUBGROUPS	All groups associated with this group
instdata	DATA	The installation data for the group

Table A–3 Dataset Resource Profile Attribute Descriptions

Oracle Identity Manager Attribute	IBM RACF Attribute	Description
cn	PROFILE NAME	The profile id
standardAccessList	ID,ACCESS,ACCESS COUNT	The standard access list of IDs and access for the dataset
conditionalAccessList	ID,ACCESS,ACCESS COUNT	The conditional access list of IDs and access for the dataset
owner	OWNER	The owner of the dataset
auditing	AUDITING	Indicates whether auditing should be enabled
notify	NOTIFY	Indicates whether notification is enabled for any changes to resource profiles
instdata	DATA	The installation data for the dataset

B

Connector Architecture

This appendix describes the IBM RACF Advanced Connector functionality in detail in the following sections:

- Oracle Identity Manager LDAP Gateway
- Oracle Identity Manager Provisioning Agent
- Oracle Identity Manager Reconciliation Agent
- Message Transport Layer

Oracle Identity Manager LDAP Gateway

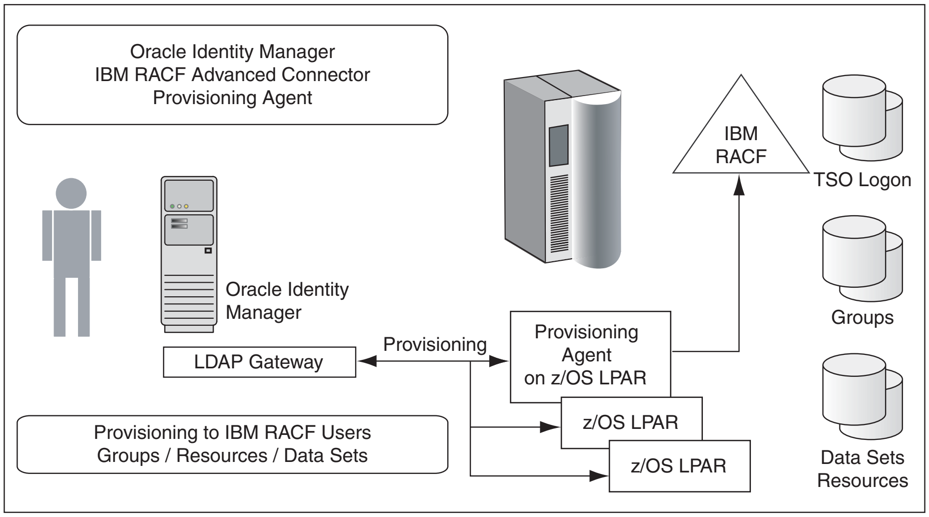
The architecture for Oracle Identity Manager Advanced Connector begins with the Oracle Identity Manager LDAP Gateway. The LDAP Gateway is built on Java 1.4.2, allowing for portability across different platforms and operating systems and complete integration with the Oracle Identity Manager system.

The LDAP Gateway works transparently with Oracle Identity Manager to communicate with IBM RACF Advanced facilities in a z/OS environment. The LDAP Gateway is installed along with Oracle Identity Manager on the same server. In addition, the Reconciliation Agent enables the LDAP Gateway server to become a subscriber to security and identity events from IBM RACF Advanced.

Oracle Identity Manager maps mainframe authentication repositories by the LDAP DN. By changing the LDAP DN, different authentication repositories and different mainframe resources can be addressed.

Oracle Identity Manager Provisioning Agent

The Provisioning Agent is a mainframe component, receiving native mainframe IBM RACF Advanced provisioning commands from the LDAP Gateway. These requests are processed against the IBM RACF Advanced authentication repository with the response parsed and returned to the LDAP Gateway.



The Provisioning Agent includes LDAP bind and authorization requests. In addition to traditional provisioning functions, the Provisioning Agent can also build the necessary TSO logon functions, including the building CLIST files, and working to replicate existing mainframe user profile scenarios. Provisioning Agent can also extend authorization to data sets, groups, and resources through enterprise rules set in by Oracle Identity Manager.

Internal to mainframe architecture is significant communication of connector resources and internal mainframe memory subpools for enterprise loads at peak times, supporting over a million transactions per day. The entire Provisioning Agent is protected by AES 128 encryption and APF authorized resources.

The Provisioning Agent receives Identity and Authorization change events, and effects requested changes on the z/OS mainframe authentication repository, IBM RACF Advanced. The Provisioning Agent is a mainframe-installed component that receives native mainframe requests from the LDAP Gateway.

An important architectural feature of the Provisioning Agent is that provisioning updates are made from the LDAP Gateway to the IBM RACF Advanced authentication repository. As such, the Provisioning Agent needs to be installed on at least one z/OS LPAR. Provisioning commands sent from Oracle Identity Manager then change authentication and authorization across all LPARS serviced by the IBM RACF Advanced authentication repository. Within this framework, multiple IBM RACF Advanced systems which are not externally synchronized will require a second Provisioning Connector.

While most provisioning commands are designed around direct access to IBM RACF Advanced, some LDAP provisioning commands are executed in multiple mainframe commands. For example, to provision for TSO access, some systems require modification to a CLIST profile. The type of command depends on which mainframe process is to be accessed.

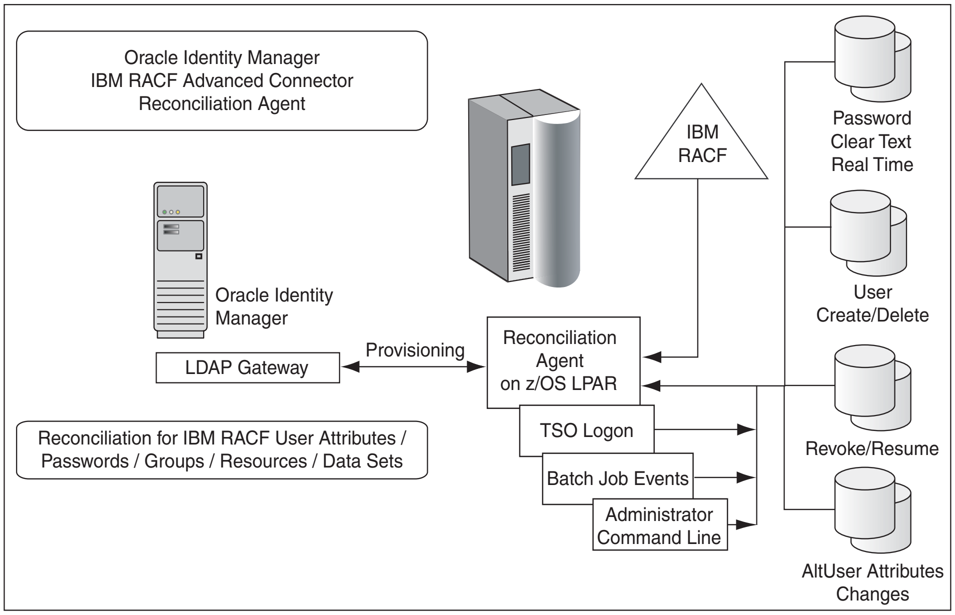
While not within the scope of standard Oracle Identity Management provisioning, the Provisioning Agent can extend control to TSO commands, CICS commands, batch jobs, and other mainframe resources.

Oracle Identity Manager Reconciliation Agent

When an event occurs on the mainframe, independent of any custom installed technology, the event is processed through an appropriate mainframe exit. Because the

Reconciliation Agent uses exit technology, there are no hooks in the z/OS mainframe operating system.

Identity events that arise from a user at TSO login, changes by an administrator from the command prompt, or events resulting from batch jobs are detected and notification messages are securely sent in real time. The Reconciliation Agent captures changes to user attributes (any ALTUSER change), changes to a user account (REVOKE, RESUME), and certain changes to user authorization for groups and resources. If a user account is created or deleted on the mainframe, the Reconciliation Agent will notify Oracle Identity Manager and even create a corresponding account in Oracle Identity Manager.



Passwords fall into a special category. If business rules permit, a password change will be passed to Oracle Identity Manager in clear text and real time. In a testing environment, it is almost immediate. Within other business rules, only a notification that the password has been changed will be passed.

Internal to mainframe architecture is significant communication of connector resources and internal mainframe memory subpools for enterprise loads at peak times. The Reconciliation Agent was specifically designed to handle peak loads from a mainframe batch job. By allocating one meg mainframe memory to the messaging subpools, 50,000 identity event messages can be held as fast as the batch job can produce them (about 8 minutes). These messages are then spooled to the LDAP Gateway, which supplies the messages to Oracle Identity Manager for subsequent processing (typically over the next hour). The entire Reconciliation Agent is protected by AES 128 encryption and APF authorized resources.

The Reconciliation Agent sends notification events to the Oracle Identity Manager LDAP Gateway from the z/OS mainframe. This architecture does not originate with IBM RACF Advanced, but captures the events just outside the operating system using exit technology, in real time.

A command execution is passed through an exit, just before full completion of the native mainframe command. A common use of this technology is to require user accounts or passwords to be formatted to a proper length or that they must contain at least one letter and one number. If the exit fails, the command fails and returns an error message. By capturing identity or authentication events at an exit, the

Reconciliation Agent captures these events outside the operating system, just prior to completing the command and storing the results in the IBM RACF Advanced authentication repository.

As with the Provisioning Agent, there is an architectural dependence based on the LPAR. When a user account is created, is authorized to something, or works on the mainframe, they do this on an LPAR. Since all actions are within the LPAR and the Reconciliation Agent detected events from an LPAR exit, the Reconciliation Agent must be installed on each LPAR. This is a scheduled event, usually done with a maintenance schedule, because the an LPAR exit change is only recognized after an IPL.

Message Transport Layer

The message transport layer is the process where the messages are exchanged between the LDAP Gateway and the IBM RACF Advanced Provisioning and Reconciliation Agent.

- IBM MQ Series

  Some IBM shops use the IBM MQ Series messaging system as their primary digital communication system. MQ Series is a secure and reliable message transport layer, utilizing internal encryption, conservation of resources, and guaranteed message delivery. The LDAP Gateway supports this message protocol.

- TCP/IP

  The LDAP Gateway also uses TCP/IP as a message transport layer to the Provisioning and Reconciliation Agent. This protocol is layered with an internal Advanced Encryption Standard (AES) encryption using 128-bit cryptographic keys. This encryption protocol is internal between the LDAP Gateway and Provisioning / Reconciliation Agent, not depending platform-specific programs or libraries.

  The LDAP Gateway, Provisioning Agent, and Reconciliation Agent all coordinate bidirectional synchronization to a single IBM RACF Advanced authentication repository. Internally, the LDAP Gateway has 20 AES cryptographic keys which are randomly selected for a given message, 10 of which are dedicate for bidirectional messages between the Provisioning Agent and the other 10 are used for the Reconciliation Agent.

  Messages between the LDAP Connector and the Provisioning Agent have a very short life span. The provisioning process that arises for Oracle Identity Manager expects a pass or fail LDAP message quickly. Typical logging and auditing protocols exist here and are usually all that are required.

  Messages originating from the Reconciliation Agent require the same level of security and guaranteed delivery as MQ Series provides. Within this context, the Reconciliation Agent has been engineered for the following:

  - If the TCP/IP connection has not been established between the Reconciliation Agent and the LDAP Gateway, up to 50,000 messages are kept in a secure mainframe memory subpool prior to message processing.
  - During the message generation process, the Reconciliation Connector places both a time stamp and a sequential serial number to each message. An archive of the message is kept in an encrypted format in an APF authorized VSIM file, with both serial and time/date stamps.

  - Once transmitted, the messages are logged internally within the LDAP Connector, again in an encrypted format.

Overall, the entire TCP/IP message transport layer approaches the performance and security level of the IBM MQ Series. The Oracle Identity Manager TCP/IP message transport layer is included at no additional charge.

Index