Oracle® Identity Manager

Connector Guide for IBM RACF Advanced

Release 9.0.4

E10451-04

July 2009

ORACLE®

Oracle Identity Manager Connector Guide for IBM RACF Advanced, Release 9.0.4

E10451-04

Primary Author: Lyju Vadassery

Contributing Authors: Debapriya Datta, Devanshi Mohan, Alankrita Prakash

Contents

Preface

This guide describes the procedure to deploy the connector that is used to integrate Oracle Identity Manager with IBM RACF.

Audience

This guide is intended for resource administrators and target system integration teams.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. 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.

Deaf/Hard of Hearing Access to Oracle Support Services

To reach Oracle Support Services, use a telecommunications relay service (TRS) to call Oracle Support at 1.800.223.1711. An Oracle Support Services engineer will handle technical issues and provide customer support according to the Oracle service request process. Information about TRS is available at http://www.fcc.gov/cgb/consumerfacts/trs.html, and a list of phone numbers is available at http://www.fcc.gov/cgb/dro/trsphonebk.html.

Related Documents

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

- *Oracle Identity Manager Release Notes*
- *Oracle Identity Manager Concepts*
- *Oracle Identity Manager Installation and Configuration Guide for BEA WebLogic Server*
- *Oracle Identity Manager Installation and Configuration Guide for IBM WebSphere Application Server*
- *Oracle Identity Manager Installation and Configuration Guide for JBoss Application Server*
- *Oracle Identity Manager Installation and Configuration Guide for Oracle Application Server*
- *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 API Usage Guide*
- *Oracle Identity Manager Audit Report Developer's Guide*
- *Oracle Identity Manager Best Practices Guide*
- *Oracle Identity Manager Globalization Guide*
- *Oracle Identity Manager Integration Guide for Crystal Reports*
- *Oracle Identity Manager Tools Reference*
- *Oracle Identity Manager Reference*

The following document is available in the Oracle Identity Manager Connector Pack documentation library:

- *Oracle Identity Manager Connector Concepts Guide*

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager Connector Pack documentation library, 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.

Convention	Meaning
`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?

This chapter provides an overview of the updates made to the software and documentation for the Oracle Identity Manager Connector for IBM RACF in release 9.0.4.4.

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

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

- Software Updates

  This section describes updates made to the connector software. This section also points out the sections of this guide that have been changed in response to each software update.

- Documentation-Specific Updates

  This section describes major changes made to this guide. These changes are not related to software updates.

Software Updates

The following software updates have been made in this connector:

- Software Updates Up To Release 9.0.4.2
- Software Updates in Release 9.0.4.3
- Software Updates in Release 9.0.4.4

Software Updates Up To Release 9.0.4.2

The following are software updates up to release 9.0.4.2:

- IBM RACF user profile, group profile, and data set and resource profile commands supported by the Provisioning Agent have been added in the "Functionality Supported by the Pioneer Provisioning Agent" section.
- The list of functions supported by the Provisioning Agent has been updated in the "Functionality Supported for Provisioning" section.
- The commands supported by the Reconciliation Agent have been added in the "Functionality Supported by the Voyager Reconciliation Agent" section.

- The list of functions supported by the Reconciliation Agent has been updated in the "Functionality Supported for Reconciliation" section.
- The list of fields reconciled between IBM RACF and Oracle Identity Manager has been updated in the "Target System Attributes Used for Reconciliation and Provisioning" section.
- The IT resource parameters and their corresponding descriptions and sample values have been updated in the "Defining the IT Resource" section.
- The procedure to configure the connector for multiple installations of the target system has been added in the "Configuring the Connector for Multiple Installations of the Target System" section.
- Information about reconciliation based on user status has been added in the "Configuring Account Status Reconciliation" section.
- Known issues related to the following bugs have been added in the "Known Issues" chapter:
  - Bug 6668844
  - Bug 6904041
  - Bug 6920042
  - Bug 7033009

Software Updates in Release 9.0.4.3

The following is a software updates in release 9.0.4.3:

- Support for IBM z/OS version 1.9

Support for IBM z/OS version 1.9

From this release onward, IBM z/OS version 1.9 is one of the certified target system identity repository. This operating system version has been added in the "Certified Deployment Configurations" section.

Software Updates in Release 9.0.4.4

The following table lists issues resolved in release 9.0.4.4:

Bug Number	Issue	Resolution
7286016	On certain UK operating environments, a mainframe code page of `GB` was used instead of the default `UK`. This caused the mainframe agents to use the American pound symbol instead of the British pound symbol.	This issue has been resolved. The mainframe agents have been rebuilt to include the GB code page.

Documentation-Specific Updates

The following are documentation-specific updates in releases 9.0.4.1 through 9.0.4.4:

- Guidelines that were earlier documented in the "Known Issues" chapter have been moved to "Guidelines on Using the Connector" on page 5-2.
- Information about enabling logging on the LDAP Gateway server has been added in "Installing and Configuring the LDAP Gateway" on page 2-8.

- In "Certified Languages" on page 1-2, Arabic has been added to the list of languages that the connector supports.
- The IBM MQ Series protocol for the message transport layer is no longer supported for this connector. All content related to this protocol has been removed from the guide.
- In the "Certified Deployment Configurations" section, changes have been made in the second row. Information about certified deployment configurations has been removed from "Verifying Deployment Requirements" on page 3-1.

1

About the Connector

The Oracle Identity Manager Connector for IBM RACF provides a native interface between IBM RACF installed on a z/OS mainframe and Oracle Identity Manager. The connector functions as a trusted virtual administrator on the target system, performing tasks such as creating login IDs, suspending IDs, and changing passwords. In addition, it automates some of the functions that administrators usually perform manually.

The connector enables provisioning and reconciliation with the IBM RACF security facilities.

This chapter discusses the following topics:

1.1 Certified Deployment Configurations

Table 1–1 lists the certified deployment configurations.

Table 1–1 Certified Deployment Configurations

Item	Requirement
Oracle Identity Manager	Oracle Identity Manager release 8.5.3.1 or later
Target System	IBM RACF on z/OS V1.8, V1.9
Infrastructure Requirements: Message transport layer	TCP/IP with AES encryption
Target system user account for Oracle Identity Manager	APF-authorized account with `SystemAdministrators` privileges

Note: The LDAP Gateway uses the target system user account that you create for Oracle Identity Manager. Therefore, it has the privileges required to access and operate with the Reconciliation Agent and Provisioning Agent.

1.1.1 Message Transport Layer Requirements

Between the Oracle Identity Manager and mainframe environments, Oracle Identity Manager supports the TCP/IP message transport layer.

For the TCP/IP message transport layer, ports 5190 and 5790 are the default ports for the Reconciliation Agent and Provisioning Agent, respectively. You can change the ports for these agents.

The procedures to configure this message transport layer is described later in this guide.

1.1.2 Configuration of APF Authorization

APF stands for the IBM Authorized Program Facility. Granting the APF Authorized status to a program 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.

1.2 Certified Languages

The connector supports the following languages:

- Arabic
- Chinese (Simplified)
- Chinese (Traditional)
- Danish
- English
- French
- German
- Italian
- Japanese
- Korean
- Portuguese (Brazilian)
- Spanish

1.3 Overview of the Connector

Note: In this guide, the Oracle Identity Manager Connector for IBM RACF is referred to as the **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, which is also native to IBM RACF, is parsed into an LDAP-format response and returned to Oracle Identity Manager.
- **Pioneer Provisioning Agent**: The Pioneer Provisioning Agent is a mainframe component. It receives native mainframe IBM RACF provisioning commands from the LDAP Gateway. These requests are processed against the IBM RACF authentication repository. The response is parsed and returned to the LDAP Gateway.

  Note: At some places in this guide, the Pioneer Provisioning Agent is referred to as the **Provisioning Agent** or **Pioneer.**

- **Voyager Reconciliation Agent**: The Voyager Reconciliation Agent captures native mainframe events by using advanced exit technology for seamless reconciliation with Oracle Identity Manager through the LDAP Gateway. Exits are programs that are run after a system event in IBM RACF is processed. The Reconciliation Agent captures in real time events occurring from the TSO logins, the command prompt, batch jobs, and other native events. The Reconciliation Agent captures these events and transforms them into notification messages for Oracle Identity Manager through the LDAP Gateway.

  Note: At some places in this guide, the Voyager Reconciliation Agent is referred to as the **Reconciliation Agent** or **Voyager.**

- **Message Transport Layer**: The message transport layer enables the exchange of messages between the LDAP Gateway and the Reconciliation Agent and Provisioning Agent. You can use the TCP/IP messaging protocol for the message transport layer.

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

  See Also: Appendix B, "Connector Architecture" for more information about the connector architecture and configuration of the message transport layer

1.4 Features of the Connector

This section discusses the following topics:

- Functionality Supported by the Pioneer Provisioning Agent
- Functionality Supported for Provisioning
- Functionality Supported by the Voyager Reconciliation Agent
- Functionality Supported for Reconciliation
- Target System Attributes Used for Reconciliation and Provisioning

1.4.1 Functionality Supported by the Pioneer Provisioning Agent

The Pioneer Provisioning Agent supports the following functions:

- Standard IBM RACF user profile commands:
  - [ADDUSER]: Creates an IBM RACF user profile
  - [ALTUSER]: Modifies an existing IBM RACF user profile
  - [DELUSER]: Deletes an IBM RACF user profile
- Standard IBM RACF group profile commands:
  - [CONNECT]: Adds an IBM RACF user to a group
  - [REMOVE]: Removes an IBM RACF user from a group
- Standard IBM RACF data set and resource profile commands:
  - [PERMIT]: Provides data set or resource profile access to a user

1.4.2 Functionality Supported for Provisioning

The functions supported by the Provisioning Agent are described in the following table:

Function	Description
Change passwords	Changes user passwords on IBM RACF in response to password changes made on Oracle Identity Manager through user self-service.
Reset passwords	Resets user passwords on IBM RACF. The passwords are reset by the administrator.
Create users	Adds new users in IBM RACF.
Modify users	Modifies user information in IBM RACF.
Revoking user accounts	Sets IBM RACF users to a REVOKED state.
Resuming user accounts	Sets IBM RACF users to an ENABLED state.
Add user to group	Connects users with an IBM RACF group.
Remove user from group	Disconnects users from an IBM RACF group.
Permit user to dataset	Permits users to be part of the data set ACL and gives them access rights to the data set.
Remove user from dataset	Removes users from the data set ACL.
Permit user to general resource	Permits users to be part of the resource ACL and gives them access rights to the resource.
Remove user from general resource	Removes users from the resource ACL.
Grant user to TSO segment	Provides TSO access and information to users.
Grant user to OMVS segment	Provides OMVS information to users.

1.4.3 Functionality Supported by the Voyager Reconciliation Agent

The Voyager Reconciliation Agent supports reconciliation of changes that are made to user profiles by using commands such as ADDUSER or ALTUSER. These commands also contain users' passwords for reconciliation, if any.

1.4.4 Functionality Supported for Reconciliation

The Reconciliation Agent supports the following functions:

- Change passwords
- Reset passwords
- Create user data
- Modify user data
- Revoke users
- Resume users
- Delete users

1.4.5 Target System Attributes Used for Reconciliation and Provisioning

The following attributes are reconciled between IBM RACF and Oracle Identity Manager:

See Also: Appendix A, "Field Mapping Between IBM RACF and Oracle Identity Manager" for the descriptions of these fields

Oracle Identity Manager Gateway Attribute	IBM RACF Attribute
cn	NAME
defaultGroup	DEFAULT-GROUP
instdata	DATA
omvsHome	HOME
omvsProgram	PROGRAM
omvsUid	UID
owner	OWNER
resumeDate	RESUME DATE
revokeDate	REVOKE DATE
tsoAcctNum	ACCTNUM
tsoCommand	COMMAND
tsoDest	DEST
tsoHoldclass	HOLDCLASS
tsoJobclass	JOBCLASS
tsoMaxSize	MAXSIZE
tsoMsgclass	MSGCLASS
tsoProc	PROC

Oracle Identity Manager Gateway Attribute	IBM RACF Attribute
tsoSize	SIZE
tsoSysoutclass	SYSOUTCLASS
tsoUnit	UNIT
tsoUserdata	USERDATA
uid	USER
userPassword	PASSWORD
waaccnt	WAACCNT
waaddr1	WAADDR1
waaddr2	WAADDR2
waaddr3	WAADDR3
waaddr4	WAADDR4
wabldg	WABLDG
wadept	WADEPT
waname	WANAME
waroom	WAROOM

1.5 Roadmap for Deploying and Using the Connector

The IBM RACF Advanced connector deployment involves deploying the LDAP Gateway, Reconciliation Agent, and Provisioning Agent. This document assumes that the LDAP Gateway is deployed on the same system as Oracle Identity Manager. The Reconciliation Agent and Provisioning Agent are deployed on the mainframe.

These procedures are described in the following chapters:

- Chapter 2, "Connector Deployment on Oracle Identity Manager" provides instructions for deploying the LDAP Gateway on the Oracle Identity Manager system. This procedure involves configuring Oracle Identity Manager, importing the connector XML file, compiling adapters, installing the LDAP Gateway, and configuring the message transport layer.
- Chapter 3, "Connector Deployment on IBM RACF" describes the procedure to deploy the Reconciliation Agent and Provisioning Agent on the mainframe. It is recommended that you perform this procedure with the assistance of the systems programmer.
- Chapter 4, "Configuring Reconciliation" describes the procedure to run initial reconciliation and to configure trusted source reconciliation and account status reconciliation.
- Chapter 5, "Troubleshooting" states the problem scenarios commonly associated with the connector and the possible solutions to those problems. In addition, this chapter discusses some guidelines on using the connector.
- Chapter 6, "Known Issues" lists the known issues associated with this release of the connector.
- Appendix A, "Field Mapping Between IBM RACF and Oracle Identity Manager" describes the user field mapping, group field mapping, and resource profile field mapping between Oracle Identity Manager and IBM RACF.

2

Connector Deployment on Oracle Identity Manager

The following sections of this chapter describe the procedure to deploy the LDAP Gateway on the Oracle Identity Manager system:

- Files and Directories That Comprise the Connector
- Copying the Connector Files
- Configuring Oracle Identity Manager
- Importing the Connector XML File
- Compiling Adapters
- Installing and Configuring the LDAP Gateway
- Configuring the Connector to Work with the Oracle Identity Manager Application Server

Refer to the following section if you want to configure the connector for multiple installations of the target system:

- Configuring the Connector for Multiple Installations of the Target System

> **See Also:** Chapter 3, "Connector Deployment on IBM RACF" for the procedure to deploy the Reconciliation Agent and Provisioning Agent on the mainframe

2.1 Files and Directories That Comprise the Connector

Table 2–1 describes the contents of the connector installation media.

Table 2–1 Files and Directories That Comprise the Connector

Files and Directories	Description
etc/LDAP Gateway/ldapgateway.zip	Files required for LDAP Gateway deployment on the Oracle Identity Manager system
etc/Provisioning and Reconciliation Connector/Mainframe_RACF.zip	Files required for the installation of the Reconciliation Agent and Provisioning Agent on the target system
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 the target system and Oracle Identity Manager

Table 2–1 (Cont.) Files and Directories That Comprise the Connector

Files and Directories	Description
Files in the resources directory	Each of these resource bundles contains 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.bat scripts/run_initial_recon_provisioning.sh	Files that are used to perform first-time (initial) reconciliation with Oracle Identity Manager
scripts/initialRacfAdv.properties scripts/racf-adv-initial-recon.jar	Files that are used during the initial reconciliation run
scripts/user.txt	Sample of the file containing user data that is used during initial reconciliation This file is discussed in detail in "Running Initial Reconciliation" on page 4-2.
xml/oimRacfAdvConnector.xml	The XML file that contains component definitions for the connector
xml/racfTrustedXellerateUser.xml	The XML file that contains definitions of the connector components that are used for trusted source reconciliation

See Also:

- "Copying the Connector Files" on page 2-2
- "Uploading the Components of the Reconciliation Agent and Provisioning Agent" on page 3-2

2.2 Copying the Connector Files

Copy the following connector files to the specified destination directories on the Oracle Identity Manager system:

Note: Do not copy the files that are not listed in this table. Those files are used later in the deployment procedure. See "Files and Directories That Comprise the Connector" on page 2-1 for more information about the following files.

Table 2–2 Copying the Connector Files

Files	Destination Directory
etc/LDAP Gateway/ldapgateway.zip	*LDAP_INSTALL_DIR* This is the directory on the Oracle Identity Manager system where you want to install the LDAP Gateway. See "Installing and Configuring the LDAP Gateway" on page 2-8 for information about installing the LDAP Gateway.
lib/racf-adv-agent-recon.jar lib/racfConnection.properties	*LDAP_INSTALL_DIR*/etc
lib/idm.jar scripts/initialRacfAdv.properties scripts/run_initial_recon_provisioning.sh scripts/run_initial_recon_provisioning.bat scripts/racf-adv-initial-recon.jar	*OIM_HOME*/xellerate/JavaTasks
Files in the resources directory	*OIM_HOME*/xellerate/connectorResources
xml/oimRacfAdvConnector.xml xml/racfTrustedXellerateUser.xml	*OIM_HOME*/xellerate/XLIntegrations/racf/xml

2.3 Configuring Oracle Identity Manager

Configuring Oracle Identity Manager involves the following procedures:

- 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.

2.3.1 Clearing Content Related to Connector Resource Bundles from the Server Cache

When you deploy the connector, the resource bundles are copied from the resources directory on the installation media into the *OIM_HOME*/xellerate/connectorResources directory. Whenever you add a new resource bundle in the 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.

   Note: You must perform Step 1 before you perform Step 2. An exception is thrown if you run the command described in Step 2 as follows:

   ```
   OIM_HOME/xellerate/bin/BATCH_FILE_NAME
   ```

2. Enter one of the following commands:

- On Microsoft Windows:

  ```
  PurgeCache.bat ConnectorResourceBundle
  ```

- On UNIX:

  ```
  PurgeCache.sh ConnectorResourceBundle
  ```

Note: You can ignore the exception that is thrown when you perform Step 2. This exception is different from the one mentioned in Step 1.

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

2.3.2 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 messages that highlight the progress of the application at a 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 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:

- **BEA WebLogic Server**

  To enable logging:

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

   ```
   log4j.logger.COM.IDENTITYFORGE.ORACLE.INTEGRATION.IDFUSEROPERATIONS=LOG_LEVEL
   ```

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

   For example:

   ```
   log4j.logger.COM.IDENTITYFORGE.ORACLE.INTEGRATION.IDFUSEROPERATIONS=INFO
   ```

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

WEBLOGIC_HOME/user_projects/domains/*DOMAIN_NAME*/*SERVERr_NAME*/*SERVER_NAME*.log

- **IBM WebSphere Application Server**

  To enable logging:

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

     ```
     log4j.logger.COM.IDENTITYFORGE.ORACLE.INTEGRATION.IDFUSEROPERATIONS=LOG_LEVEL
     ```

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

     For example:

     ```
     log4j.logger.COM.IDENTITYFORGE.ORACLE.INTEGRATION.IDFUSEROPERATIONS=INFO
     ```

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

  WEBSPHERE_HOME/AppServer/logs/*SERVER_NAME*/startServer.log

- **JBoss Application Server**

  To enable logging:

  1. In the *JBOSS_HOME*/server/default/conf/log4j.xml file, locate or add the following lines:

     ```
     <category name="COM.IDENTITYFORGE.ORACLE.INTEGRATION.IDFUSEROPERATIONS">
        <priority value="LOG_LEVEL"/>
     </category>
     ```

  2. In the second XML line, replace *LOG_LEVEL* with the log level that you want to set. For example:

     ```
     <category name="COM.IDENTITYFORGE.ORACLE.INTEGRATION.IDFUSEROPERATIONS">
        <priority value="INFO"/>
     </category>
     ```

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

  JBOSS_HOME/server/default/log/server.log

- **Oracle Application Server**

  To enable logging:

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

     ```
     log4j.logger.IDENTITYFORGE.ORACLE.INTEGRATION.IDFUSEROPERATIONS=LOG_LEVEL
     ```

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

   For example:

   ```
   log4j.logger.IDENTITYFORGE.ORACLE.INTEGRATION.IDFUSEROPERATIONS=INFO
   ```

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

OAS_HOME/opmn/logs/default_group~home~default_group~1.log

2.4 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 pane.
3. Click the **Import** link under Deployment Management. A dialog box for locating files is displayed.
4. Locate and open the oimRacfAdvConnector.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 a new instance of the OIMLDAPGatewayResourceType IT resource type is displayed.
8. Create an IT resource based on the `OIMLDAPGatewayResourceType` IT resource type. Refer to "Defining the IT Resource" on page 2-6 for information about the parameters for which you must specify values.
9. Click **Next.** The Provide IT Resource Instance Data page for a new instance of the OIMLDAPGatewayResourceType 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.
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. These nodes represent Oracle Identity Manager entities that are redundant. Before you import the connector XML file, you must remove these entities by right-clicking each node and then selecting **Remove**.
12. Click **Import**. The connector file is imported into Oracle Identity Manager.

2.4.1 Defining the IT Resource

You must specify values for the IT resource parameters listed in the following table:

Parameter	Description
AtMap User	Name of the lookup definition containing attribute mappings that are used for provisioning Value: `AtMap.RACF` **Note:** You must not change the value of this parameter.
idfPrincipalDn	The administrator ID for connecting to the LDAP Gateway Sample value: `cn=idfRacfAdmin,dc=racf,dc=com`
idfPrincipalPwd	The administrator password for connecting to the LDAP Gateway
idfRootContext	The root context for IBM RACF Value: `dc=racf,dc=com` **Note:** You must not change the value of this parameter.
idfServerHost	Host name for connecting to the LDAP Gateway Value: `localhost` **Note:** You must not change the value of this parameter.
idfServerPort	The port for connecting to the LDAP Gateway Sample value: `5389`

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

2.5 Compiling Adapters

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

- AddUserToDataset
- AddUserToGroup
- AddUserToResource
- ChangePassword
- DeleteUser
- ModifyUser
- OnBoardRacfUser
- RemoveSecurityAttr
- RemoveUserFromDataset
- RemoveUserFromGroup
- RemoveUserFromResource
- ResetPassword
- ResumeUser
- RevokeUser

You must compile these adapters.

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, click **Compile All**.

   If you have created your own adapters or if a new adapter is shipped with a patch that you installed, then you might need to compile one adapter at a time. To compile multiple (but not all) adapters, select the adapters you want to compile. Then, click **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.

2.6 Installing and Configuring the LDAP Gateway

To install and configure the LDAP Gateway:

1. Extract the contents of the ldapgateway.zip file to a directory on the same server as Oracle Identity Manager. In this document, the location (and name) of the ldapgateway directory is referred to as *LDAP_INSTALL_DIR*.
2. In a text editor, open the racf.properties file. This file is located in the *LDAP_INSTALL_DIR*/conf directory. In this file, specify information for the following properties of the TCP/IP message transport layer:

   The default values are as follows. You can change these values.

```
_type_=socket
_isencrypted_=true
_timeout_=5000
_authretries_=2
_host_=HOST_NAME_OR_IP_ADDRESS_OF_MAINFRAME
_port_=5790
_agentport_=5190
```

   Note: If you are configuring the LDAP Gateway in the same server as Oracle Identity Manager, then specify `localhost` as the value of the _host_ property. If you are configuring the LDAP Gateway in a different server than Oracle Identity Manager, then specify the host name or IP address of the server as the value of the _host_ property. However, Oracle recommends that the LDAP Gateway be installed in the same server as Oracle Identity Manager.
3. In the racf.properties file, use the following property to specify whether you want to revoke access rights or delete users during Disable User provisioning operations:

```
# DEFAULT ACTION WHEN DELETE FUNCTION USED
_defaultDelete_=delete
```

   Set `revoke` as the value of this property if you want the user to be disabled on the target system as the outcome of a Delete User provisioning operation.

   Set `delete` as the value of this property if you want the user to be deleted from the target system as the outcome of a Delete User provisioning operation.

4. In the racf.properties file, use the _nameFormat_ property to specify the format of the Full Name attribute.

   You can use the following as the components of the format that you specify:

   - Use fn to represent the first name.
   - Use sp to represent the space character.
   - Use ln to represent the last name.
   - Use a comma (,) to represent the comma.
   - Use a period (.) to represent the period.
   - Use the vertical bar (|) as the separator for the other components.

   The following line shows a sample value for the _nameFormat_ property:

   ```
   _nameFormat_=fn|sp|ln
   ```

5. Open the *LDAP_INSTALL_DIR*/etc/racfConnection.properties file and edit the following property:

   Note: You must also make this change in the initialRacfAdv.properties file, which is in the *OIM_HOME*/xellerate/JavaTasks directory.

   ```
   _itResource_=NAME_OF_THE_NEW_IT_RESOURCE
   ```

   Replace *NAME_OF_THE_NEW_IT_RESOURCE* with the name of the IT resource that you create by performing Step 8 of the procedure described in "Importing the Connector XML File" on page 2-6.

6. From the *LDAP_INSTALL_DIR*/dist/idfserver.jar file, extract the beans.xml file, open it in an editor, and set values for the following:

   - Target system administrator credentials

     You must change the administrator credentials stored in the following lines of the beans.xml file:

     Note: In these lines, the values that you can change are highlighted in bold font. The values that you enter in the beans.xml file must be the same as the values that you specify for the IT resource parameters and the properties in the racfConnection.properties and initialRacfAdv.properties files.

     ```
     <property name="adminUserDN" value="cn=ximRACFAdmin,dc=RACF,dc=com"/>
     <property name="adminUserPassword" value="ximRACFPwd"/>
     ```

   - Port used for communication between the LDAP Gateway and the mainframe LPAR that you use for the connector installation

     The default value of the port property is `5389`. If you want to change this value, then edit the value of the `port` property defined in the `beans.xml` file:

     ```
     <property name="port" value="5389"/>
     ```

7. To enable logging on the LDAP Gateway server:

a. Extract the log4j.properties file from the *LDAP_INSTALL_DIR*/dist/idfserver.jar file.

b. Ensure that the log4j.rootLogger variable is set to the following:

```
log4j.rootLogger=DEBUG, A1
```

c. Save and close the file.

When you use the connector, the following LDAP Gateway log files are generated in the *LDAP_INSTALL_DIR*/logs directory:

- idfserver.log.0: This is the main log file.
- topsecret-agent-recon.log: This is ongoing reconciliation log file that stores Oracle Identity Manager reconciliation messages.
- topsagent.log.0: This file is currently redundant, and it will be removed in a later release.

8. Save the changes made to the beans.xml file, and then re-create the idfserver.jar file.

Note: When you start using the connector, the logs for the LDAP Gateway are created in the *LDAP_INSTALL_DIR*/logs directory.

2.7 Configuring the Connector to Work with the Oracle Identity Manager Application Server

To ensure that the connector works with the application server that Oracle Identity Manager is deployed on:

1. In a text editor, open the following scripts:
   - Open the run script from the *LDAP_INSTALL_DIR*/bin directory.
   - Open the run_initial_recon_provisioning script from the *OIM_HOME*/Xellerate/JavaTasks directory.
2. In the run and run_initial_recon_provisioning scripts, uncomment the lines related to the specific application server that you are using. In addition, change the paths to reflect the actual location of the application server directory.

   The following are the contents of the run.sh file:

Note: The contents of the run_initial_recon_provisioning script are similar. You must make the same change in that script.

```
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
```

In the run.sh file, the lines starting with a number sign (#) are comments. To uncomment the line, remove the number sign. For example, to ensure that the connector works with JBoss Application Server, uncomment the following line:

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

3. If you are using IBM WebSphere Application Server 6.1, then add the com.ibm.ws.wccm_6.1.0.jar file to the CLASSPATH variable in the run and run_initial_recon_provisioning scripts as shown in the following example:

```
rem
rem SET WEBSPHERE APPLICATION SERVER REQUIRED LIBRARIES
rem
set CLASSPATH=%CLASSPATH%;"%APPSERVER_HOME%"\lib\com.ibm.ws.wccm_6.1.0.jar
```

2.8 Configuring the Connector for Multiple Installations of the Target System

You can configure the connector for multiple installations of the target system. You can also configure the connector for a scenario in which multiple logical partitions (LPARs), which are not associated with the first LPAR, are configured in the target system.

For each installation of the target system, you create an IT resource and configure an additional instance of the LDAP Gateway.

To configure the connector for the second installation of the target system:

Note: Perform the same procedure for each installation of the target system.

1. Create an IT resource based on the OIMLDAPGatewayResourceType IT resource type.

   Refer to *Oracle Identity Manager Design Console Guide* for information about creating IT resources. Refer to "Defining the IT Resource" on page 2-6 for information about the parameters of the IT resource.

2. Copy the current *LDAP_INSTALL_DIR* directory, including all the subdirectories, to a new location.

   Note: In the remaining steps of this procedure, *LDAP_INSTALL_DIR* refers to the newly copied directory.

3. Extract the contents of the *LDAP_INSTALL_DIR*/dist/idfserver.jar file.

4. In the beans.xml file, change the value of the port in the <property name="port" value="xxxx"/> line to specify a port that is different from the port used for the

first instance of the LDAP Gateway. The default port number is shown in the following example:

```
<bean id="listener" class="com.identityforge.idfserver.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>
```

If you change the port number, then you must make the same change in the value of the idfServerPort parameter of the IT resource that you create.

5. Save and close the bean.xml file.
6. Open the *LDAP_INSTALL_DIR*/conf/racf.properties file and edit the following parameters:
   - _host_=*IP_ADDRESS_OR_HOST_NAME_OF_THE_MAINFRAME*
   - _port_=*PORT_OF_THE_SECOND_INSTANCE_OF_THE_PROVISIONING_AGENT*
   - _agentPort_=*PORT_OF_THE_SECOND_INSTANCE_OF_THE_RECONCILIATION_AGENT*

   Note: The value of the `_agentPort_` parameter must not be the same as that of the first instance if a second LPAR, which is not associated with the first LPAR, is configured in the target system. This value can be the same as the value of the `idfServerPort` parameter if you have two mainframe servers with IBM RACF running on each server.
7. Open the *LDAP_INSTALL_DIR*/etc/racfConnection.properties file and edit the following property:

   itResource=*NAME_OF_THE_NEW_IT_RESOURCE*

3

Connector Deployment on IBM RACF

You must install the Reconciliation Agent and Provisioning Agent components of the IBM RACF Advanced connector on the mainframe.

The following section summarizes the procedure:

- Summary of the Deployment Procedure

The following sections describe each deployment step in detail:

1. Verifying Deployment Requirements
2. Uploading the Components of the Reconciliation Agent and Provisioning Agent
3. Modifying the prclib.xmi and parmlib.xmi Files
4. Configuring the Started Tasks
5. Integrating the Exits for the Reconciliation Agent with the Target System Exits
6. Creating an IBM RACF Account
7. Starting Up and Shutting Down the Reconciliation Agent and Provisioning Agent

3.1 Summary of the Deployment Procedure

The following steps summarize the procedure to deploy the connector components on the target system:

1. Verify the deployment requirements.
2. Upload the components of the Reconciliation Agent and Provisioning Agent.
3. Modify the prclib.xmi and parmlib.xmi files according to the settings of your target system installation.
4. Configure the started tasks.
5. Integrate the connector exits with the target system exits.
6. Create an IBM RACF account for reconciliation and provisioning operations.
7. Test the setup by starting up and shutting down the Reconciliation Agent and Provisioning Agent.

3.2 Verifying Deployment Requirements

Both the Reconciliation Agent and Provisioning Agent need a started task and service account that has the privileges required to run IBM RACF system commands on the mainframe system.

In addition, these agents function under a user account on the mainframe system. This user account must be created by the systems programmer before you deploy the agents.

Note: Both the Reconciliation Agent and Provisioning Agent user accounts must be placed 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

Ensure that the following requirements are met on the mainframe:

- The Reconciliation Agent and Provisioning Agent each use memory subpools to manage peak load conditions. These subpools require 1.5 to 2.0 MB of mainframe memory for operations. You configure this while installing the Reconciliation Agent and Provisioning Agent.
- 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 configured by the systems programmer.
- Because TCP/IP is used in the message transport layer, an administrator must have authorization to create ports on the mainframe and provide security authorizations.
- The Reconciliation Agent operates by using user exit technology, outside the mainframe operating system. This means it runs on a different LPAR from the operating system.

  Maintaining a specific password format is an example of the objective for which you use custom exits. Oracle Identity Manager exits are engineered to be the last exits called in sequence, allowing existing exits to function normally. After modifying exits within an LPAR, an initial program load (IPL) of the LPAR may be required.

  Note: As the systems programmer, you must do an IPL after a system component is changed or modified.

3.3 Uploading the Components of the Reconciliation Agent and Provisioning Agent

Perform the following steps to upload the components of the Reconciliation Agent and Provisioning Agent:

1. Extract the contents of the following file from the installation media to a temporary directory on any computer:

   ```
   etc/Provisioning and Reconciliation Connector/Mainframe_RACF.zip
   ```

2. Transmit or FTP the jcl.xmi and linklib.xmi files to the mainframe, each with the following specifications: RECFM=FB, LRECL=80, BLKSIZE=3120, and DSORG=PS.

3. Log in to the TSO environment of the mainframe.
4. Expand the CNTL data sets, and then run the following command from the ISPF command line:

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

5. When prompted to specify restore parameters, enter:

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

   Note: DA is a parameter of the Restore command. It means `Dataset`.

6. To expand the LINKLIB data set, run the following command from the ISPF command line:

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

7. When prompted to enter restore parameters, enter:

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

8. Perform Steps 4 through 7 for the prclib.xmi and parmlib.xmi files included in the Mainframe_RACF.zip file.
9. Copy LOGPWX01 and LOGRIX02 to the LPA load library contained within the appropriate IEASYSxx member of SYS1.PARMLIB.

3.4 Modifying the prclib.xmi and parmlib.xmi Files

After you upload the prclib.xmi and parmlib.xmi files, edit the contents of the files so that the values of parameters in the file match the settings of your target system installation.

The following z/OS libraries are used by the connector:

- **Library = IDF.LINKLIB**

  This library contains executable modules for the Provisioning (Pioneer) and Reconciliation (Voyager) Agents and various utility programs required for their operation.

- **Library = IDF.PROCLIB**

  This library contains STC procedures for Pioneer and Voyager. There are four members in this library:

  Pioneerx: Provisioning Agent

  Voyager: Reconciliation Agent

  Startup: Procedure to create Subpool 231 to capture events for Voyager

  Wrapup: Procedure to delete the Startup created subpool

- **Library = IDF.PARMLIB**

  This library contains the following members:

  PROG01: Dynamic APF authorization member for IDF.LINKLIB

  PROG76: Dynamic EXIT member for Activation of IRREVX01

PROG77: Dynamic EXIT member for deactivation of IRREVX01

3.5 Configuring the Started Tasks

There are two different STCs (Started Task procedures) to set up and run the Reconciliation Agent and Provisioning Agent. There is a STC procedure member for each agent. RUNPIONX and RUNVOYAX are samples for you to set up the started tasks.

The parameters for RUNPIONX are:

- TCPN: The name of the TCP STC on z/OS
- IPAD: The value must always be 0.0.0.0.
- PORT: The incoming connection port for the Provisioning Agent must match the value given in the LDAP gateway properties file.
- DEBUG: The debug switch for showing diagnostic output

The parameters for RUNVOYAX are:

- `TCPN`: The name of the TCP STC on z/OS
- `IPAD`: The destination IP Address of the LDAP gateway
- `PORT`: The outgoing connection port for the Reconciliation Agent for the LDAP gateway
- `DEBUG`: The debug switch for showing diagnostic output

The source code for each program is as follows:

For RUNPIONX:

```
//PIONEER  EXEC PGM=PIONEERX,REGION=0M,TIME=1440,
//    PARM=('TCPN=TCPIP',
//          'IPAD=0.0.0.0',
//          'PORT=5799',
//          'DEBUG=Y',
//          'ESIZE=16',
//          'LPAR=ORACLE-T',
//          'JWAIT=10')
//STEPLIB  DD DISP=SHR,DSN=IDF.LINKLIB                    (1)
//* EPLIB  DD DISP=SHR,DSN=IDF.PROD.LINKLIB
//         DD DISP=SHR,DSN=TCPIP.SEZATCP
//* BATJINFO DD DISP=SHR,DSN=ADCDM.BATJCARD               (2)
//* VSAMGETU DD DISP=SHR,DSN=ADCDM.SWUSERS                (3)
//* VSAMGETO DD DISP=SHR,DSN=ADCDM.BATJCOUT               (4)
//DEBUGOUT  DD SYSOUT=*                                   (5)
//SYSPUNCH DD SYSOUT=(*,INTRDR)
//SYSPRINT DD SYSOUT=X
//SYSUDUMP DD SYSOUT=X
//
```

An explanation of some of the lines in the preceding block:

- (1) In this example, Pioneer is using a STEPLIB.
- (2) , (3) , (4) these can be commented out. They are used only for ACF2 installations.
- (5) The new DEBUG out data definition statement.

For RUNVOYAX:

```
//VOYAGER JOB SYSTEMS,MSGLEVEL=(1,1),MSGCLASS=X,CLASS=A,PRTY=8,
```

```
// NOTIFY=&SYSUID,REGION=4096K
//STEP1    EXEC PGM=VOYAGERX,REGION=0M,TIME=1440,
//  PARM=('TCPN=TCPIP',
//    'IPAD=LDAP_GATEWAY_IP_ADDRESS',
//    'PORT=5190',
//    'DEBUG=Y',
//    'ESIZE=16',
//    'DELAY=00',
//    'STARTDELAY=10',
//    'PRTNCODE=SHUTRC')
//STEPLIB  DD  DSN=IDF.LINKLIB,DISP=SHR
//CACHESAV DD  DSN=ADCDM.CACHESAV,DISP=SHR
//DEBUGOUT DD  SYSOUT=*
//SYSPRINT DD  SYSOUT=*
//SYSUDUMP DD  SYSOUT=*
```

3.6 Integrating the Exits for the Reconciliation Agent with the Target System Exits

Note: Before you perform this procedure, ensure that earlier versions of the reconciliation exits are not present.

Because two of the exit modules, ICHPWX01 and ICHRIX02, are in the z/OS Load Library that resides in the LPA, an IPL is required to complete the installation. The third exit, IRREVX01(LOGREVX01), resides in a z/OS Link List load library. This depends on whether the z/OS Load Library is added to the LinkList. To allow the LDAP Gateway to fully capture events, the Reconciliation Agent and its exits must be installed on each LPAR that shares the authentication repository.

To install the Reconciliation Agent exits:

Note: In the console commands given in the following steps, XX is the PROG suffix for the member in SYS1.PARMLIB, which is one of the libraries that are used to start up the mainframe.

1. Install LOGEVX01, the Common Command exit, by using the Dynamic Exit Facility. The LOGRIX02, LOGOWX01 and LOGEVX01 are standard Assembler-language exits for manipulation or capture of IBM RACF data.

   See Also: IBM Security Server documentation for more information about the LOGRIX02, LOGOWX01, and LOGEVX01 exits

2. For testing, it is recommended that you set up one or more PROGxx members for dynamic activation of exits in SYS1.PARMLIB (or equivalent), to allow for easy removal of the exit, if required.
3. In SYS1.PARMLIB, create a member containing the following Dynamic Exit definitions:

   ```
   EXIT ADD EXITNAME(IRREVX01) MODULE(LOGEVX01)
   ```

4. From the distribution Load Library, copy LOGRIX02 as ICHRIX02 and LOGOWX01 as ICHPWX01 into a user LPA library defined in the sys1.parmlib – IEASYSxx member (LPALSTxx). A z/OS IPL is required to activate these exits.
5. IPL z/OS with the new LPA library contained within the LPALSTxx member of SYS1.PARMLIB.

   An entry similar to the following is logged when the target system finds and activates connector exits:

   ```
   0090  ICH508I ACTIVE RACF EXITS: ICHRIX02 ICHPWX01
   ```

6. Activate LOGEVX01 as an IRREVX01 exit point by running the console command SET PROG=XX. IRREVX01 is the only dynamically activated exit.
7. Use Startup or VOYINIT to build subpool 231. Verify that the job ends with the MVS condition code 0000.

Loading Exits

If the command exit IRREVX01 is contained in a Link List library and was activated through a z/OS SET command, then the LLA (Library Lookaside Area) must be refreshed, either using ISPF through SDSF or the z/OS master console:

```
/F LLA,REFRESH
```

Verifying Exit Installation

From the z/OS master console or ISPF - SDSF, enter the following command to verify that the load library where the product is installed is APF authorized:

```
/D PROG,APF
```

By default, if the installation load library is in the linklist, then it is APF authorized. You can determine whether or not the installation load library is in the linklist at IPL time by running the following command from the IPL library:

```
SYS1.PARMLIB, member = IEASYSxx
```

Here, *xx* is a user suffix for a z/OS startup member in SYS1.PARMIB.

Verifying That the Exits Are Loaded

The following are commands to verify that the exits are loaded and sample output for these commands:

```
0290  D PROG,LPA,MODNAME=ICHPWX01
0090  CSV550I 10.07.56 LPA DISPLAY 702
0090  FLAGS  MODULE    ENTRY PT  LOAD PT   LENGTH    DIAG
0090     P   ICHPWX01  83A56730  03A56730  00000228  11AF5B80


0290  D PROG,LPA,MODNAME=ICHRIX02
0090  CSV550I 10.08.54 LPA DISPLAY 704
0090  FLAGS  MODULE    ENTRY PT  LOAD PT   LENGTH    DIAG
0090     P   ICHRIX02  8318EAE0  0318EAE0  00000228  11AFD420

D PROG,EXIT,EXITNAME=IRREVX01
CSV461I 14.46.59 PROG,EXIT DISPLAY 414
EXIT            MODULE   STATE MODULE   STATE MODULE   STATE
IRREVX01        LOGEVX01   A
```

Uninstalling the Exits

If you want to uninstall the Reconciliation Agent exits, then use one of the following methods:

- For the command exit, IRREVX01, run the SET PROG=XX console command. In this command, replace *XX* with the PROG suffix for the exit (member) in SYS1.PARMLIB.
- For ICHPWX01 and ICHRIX02, delete modules from the LPA library where they are installed. Alternatively, you can create and use two LPA libraries, one each for production and for testing purposes. The correct IEASYSxx suffix can be pointed to the appropriate LPA library. After you delete the exits, a z/OS IPL is required.
- Run the following command:

```
EXIT DELETE EXITNAME(IRREVX01) MODULE(LOGEVX01)
```

3.7 Creating an IBM RACF Account

The connector uses a target system account for reconciliation and provisioning operations performed on the target system. To create this target system account:

1. Create a RACF user account similar to the following:

   ADDUSER START2 DFLTGRP(xxxx) PASSWORD(yyyyyyyy)

   ALTUSER START2 SPECIAL OPERATIONS

2. Build the following RACF permissions:

   RDEFINE FACILITY IRR.RADMIN.* UACC(NONE)

   PERMIT IRR.RADMIN.* CLASS(FACILITY) ID(START2) ACCESS(READ)

   PERMIT BPX.DAEMON CLASS(FACILITY) ID(START2) ACCESS(READ)

3. Refresh the RACLIST as follows:

   SETROPTS RACLIST(FACILITY) REFRESH

3.8 Starting Up and Shutting Down the Reconciliation Agent and Provisioning Agent

Note: Both agents use the standard CICS Socket Interface EZASOKET. The errors returned from various calls are documented in z/OS V1R9.0 Communications Server IP CICS Sockets Guide.

To start up the Reconciliation Agent and Provisioning Agent:

1. z/OS IPLs.
2. RACF is started and the ICHPWX01 and ICHRIX02 exits are activated from the LPA.
3. JES2 is started.
4. TCP/IP and other communications-related STCs are started.
5. The VOYINIT or STARTUP procedure is executed to establish the subpool used to capture RACF events.

6. You verify that the LDAP Gateway properties have been changed to match Voyager and Pioneer properties.
7. To start Voyager, run the `S VOYAGER` command from the z/OS operator's console or SDSF in TSO.
8. To start Pioneer, run the `S PIONEER` command from the z/OS operator's console or SDSF in TSO.

To shut down the Reconciliation Agent and Provisioning Agent:

To shut down the Reconciliation Agent, run the `F VOYAGER,SHUTDOWN` command from the z/OS Operator's console or TSO/ISPF issue.

To shut down the Provisioning Agent, run the `F PIONEER,SHUTDOWN` command from the z/OS Operator's console or TSO/ISPF issue.

4

Configuring Reconciliation

This connector enables real-time reconciliation of user data from IBM RACF. After you deploy the connector and import existing user data from the target system to Oracle Identity Manager, you need not depend on a scheduled task to initiate reconciliation runs with the target system.

This chapter discusses the following topics:

4.1 Configuring Trusted Source Reconciliation

The XML file for trusted source reconciliation, racfTrustedXellerateUser.xml, contains definitions of the connector components that are used for trusted source reconciliation. To import this XML file:

> **Note:** The procedure described in this section enables trusted source reconciliation for both the initial reconciliation run and subsequent, real-time reconciliation runs.

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 opening files is displayed.
4. Locate and open the racfTrustedXellerateUser.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 **Import**.
8. In the message that is displayed, click **Import** to confirm that you want to import the **XML** file and then click **OK**.

4.2 Running Initial Reconciliation

The initial reconciliation run involves importing user data from the target system into Oracle Identity Manager, immediately after you deploy the connector.

To start the initial reconciliation run:

1. Ensure that properties that are common to both the run script and the run_initial_recon_provisioning script have the same values.

   The run script is in the *LDAP_INSTALL_DIR*/bin directory. The run_initial_recon_provisioning script is in the *OIM_HOME*/xellerate/JavaTasks directory.

2. In a text editor, open the initialRacfAdv.properties file. This file is in the following directory:

   OIM_HOME/xellerate/JavaTasks

3. In the initialRacfAdv.properties file, specify values for the properties that control the initial reconciliation script.

   Note: Ensure that properties that are common to both the initialRacfAdv.properties file and racfConnection.properties file have the same values.

   The following is a description of some of the properties in the file:

   - idfTrusted

     Enter true as the value of this property to specify that you want to perform trusted source reconciliation with the target system.

   - userFile

     Enter the name of the TXT file in which you have stored the user IDs of the target system users that you want to reconcile. This file must be placed in the following directory:

     OIM_HOME/xellerate/JavaTasks

     For more information about this file, see the sample user.txt file in the scripts directory on the installation media.

   The following is a sample set of values for the properties in the initialRacfAdv.properties file:

```
xlAdminId:xelsysadm
idfTrusted:true
_resourceObject_:OIMRacfResourceObject
_itResource_:RacfResource
_dummyPwd_:Pwd123
isFileRecon:true
userFile:user.txt
#REMOVED: sn,givenName,revoke,passwordExpire,
reconAttrs:uid,cn,userPassword,revokeDate,resumeDate,defaultGroup,owner,instdat
a,omvsUid,omvsHome,omvsProgram,waaccnt,waaddr1,waaddr2,waaddr3,waaddr4,wabldg,w
adept,waname,waroom
tsoReconAttrs:tsoAcctNum,tsoProc,tsoSize,tsoUnit,tsoUserdata,tsoCommand,tsoDest
,tsoHoldclass,tsoMsgclass,tsoMaxSize,tsoSysoutclass,tsoJobclass
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
```

4. In a text editor, open the run_initial_recon_provisioning script. This file is in the following directory:

   OIM_HOME/xellerate/JavaTasks

5. To perform trusted source reconciliation:

   Note: Ignore step 5 if you want to run target resource reconciliation only.

   a. Set the value of the JV parameter in the script to –X to reconcile Xellerate User.

   b. Run the script.

      When you run the script, it opens the file (whose name is the value of the userFile property) containing user data and reads the user IDs of the users that you want to reconcile. Then, the loader, which is the initial load script, connects to the LDAP Gateway and issues commands to fetch the required user data from the target system. This data is loaded in the LDAP Gateway cache and reconciliation events are submitted to Oracle Identity Manager. Xellerate Users are created for all the target system users identified by the userFile property in the initialRacfAdv.properties file.

   c. In the run_initial_recon_provisioning script, change the value of the JV parameter to `-R` to run target resource reconciliation.

   d. Run the script again.

      Because you have set the value of the JV parameter in the script to `-R`, target resource reconciliation is performed when you run the script. Resources are assigned to each OIM User that was created when you first ran the script.

6. To perform target resource reconciliation only:

   Note: Ignore step 6 if you want to run trusted source reconciliation.

   a. In a text editor, open the initialRacfAdv.properties file and enter `false` as the value of the idfTrusted property to specify that you want to perform target resource reconciliation with the target system.

      Make the same change in the racfConnection.properties file.

   b. In the run_initial_recon_provisioning script and change the value of the JV parameter to `-P` to run target resource reconciliation.

   c. Run the script again.

Because you have set the value of the JV parameter in the script to `-P`, target resource reconciliation is performed when you run the script.

After the initial reconciliation run ends, real-time reconciliation takes over and newly created or modified user data is automatically reconciled into Oracle Identity Manager.

4.3 Configuring Account Status Reconciliation

When a user is disabled or enabled on the target system, the user is reconciled and the changed status is reflected in Oracle Identity Manager. To reconcile a user after a change of the user's status on the mainframe system, perform the following configuration steps:

1. In the *LDAP_INSTALL_DIR* directory, add the name of the status attribute to the reconAttrs section in the racfConnection.properties.

   Make the same change in the initialRacfAdv.properties file, which is in the *OIM_HOME*/xellerate/JavaTasks directory.

2. Restart the LDAP Gateway for the changes to take effect.

3. In the Design Console:

   See Also: *Oracle Identity Manager Design Console Guide* for detailed information about the following steps

   - In the OIMRacfResourceObject resource object, create a field to represent the status attribute.
   - In the OIMRacfProvisioningProcess process definition, map the field for the status attribute to the OIM_OBJECT_STATUS field.

5 Troubleshooting

This chapter contains the following sections:

5.1 Troubleshooting

The following table lists solutions to some commonly encountered issues associated with the connector:

Problem Description	Solution
Oracle Identity Manager cannot establish a connection with IBM RACF.	■ Ensure that the mainframe is running. ■ Verify that the required ports are working. ■ Due to the nature of the Provisioning Agent, the LDAP Gateway must be started first, and then the mainframe JCL started task must be started. This is a requirement based on how TCP/IP operates. Check that the server IP that hosts the LDAP Gateway is configured in the Reconciliation Agent JCL. ■ Read the LDAP Gateway logs to determine if messages are being sent or received. ■ Verify that the IP address, administrator ID, and administrator password are correctly specified in the IT resource. Refer to *Oracle Identity Manager Design Console Guide* for information about viewing and modifying IT resources. ■ Verify that the mainframe user account and password have not been changed.
The mainframe does not appear to respond.	■ Check the connection information that you have provided in the IT resource and the *LDAP_INSTALL_DIR*`/conf/racf.properties` file. ■ Check the logs. If any of the mainframe JCL jobs have reached an abnormal end, then make the required corrections and rerun the jobs.

Problem Description	Solution
A particular use case does not work as expected.	Check for the use case event in the LDAP Gateway logs. Then check for the event in the specific log assigned to the IBM RACF Advanced connector that you are using. ■ If the event has not been recorded in either of these logs, then investigate the connection between Oracle Identity Manager and the LDAP Gateway. ■ If the event is in the log but the command has not had the intended change on a mainframe user profile, then check for configuration and connections between the LDAP Gateway and the mainframe. ■ Verify that the message transport layer is working.
The LDAP Gateway fails and stops working.	If this problem occurs, then the Reconciliation Agent stops sending messages to the LDAP Gateway. Instead, it stores them in the subpool cache. When this happens, restart the LDAP Gateway instance so that the Reconciliation Agent reads the subpool cache and resends the messages.
The LDAP Gateway is running. However, the Reconciliation Agent fails and stops working.	If this problem occurs, then all events are sent to the subpool cache. If the mainframe fails, then all messages are written to the disk. When this happens, restart the Reconciliation Agent instance so that it reads messages from the disk or subpool cache and resends the messages.

5.2 Guidelines on Using the Connector

Apply the following guidelines while using 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.
- If you configure the connector for trusted source reconciliation and set the idfTrusted property in the initialRacfAdv.properties file 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 LDAP Gateway. Otherwise, the connector will fail. This applies only to a configuration in which a single LDAP Gateway connects to multiple installations of the target system.

6

Known Issues

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

- **Bug 6668844**

  If there is any reconciliation field mapped to OIM_OBJECT_STATUS in the process definition, then the associated process form cannot be modified to create a new version. To create a new version of the process form, remove the reconciliation field mapping of OIM_OBJECT_STATUS from the process definition, update the process form, and then remap the OIM_OBJECT_STATUS field.

- **Bug 6904041**

  Group membership changes of user profiles that are updated on the target system cannot be reconciled into Oracle Identity Manager.

- **Bug 6920042**

  When you update the SIZE and MAXSIZE IBM RACF attributes during a provisioning operation, you must not include leading zeros in the value that you specify. For example, if you want to change the value of the SIZE attribute from 000001 to 000002, then enter 2 in the SIZE field on the Administrative and User Console.

  See Also: "User Field Mapping" on page A-1 for mapping information about the SIZE and MAXSIZE attributes

- **Bug 7033009**

  The number sign (#) or a space at the *beginning* of the User Profile ID string is not supported. In addition, the following characters are not supported in the User Profile ID string:

  - Comma (,)
  - Plus sign (+)
  - Double quotation mark (")
  - Slash (/)
  - Left angle bracket (<)
  - Right angle bracket (>)
  - Backslash (\)

A

Field Mapping Between IBM RACF and Oracle Identity Manager

This appendix discusses the field mapping between IBM RACF and Oracle Identity Manager. It consists of the following topics:

- User Field Mapping
- Group Field Mapping
- Resource Profile Field Mapping

A.1 User Field Mapping

Table A–1 describes the user field mapping between Oracle Identity Manager and IBM RACF.

Table A–1 User Field Mapping

Oracle Identity Manager Gateway Field	IBM RACF Field	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
omvsHome	HOME	OMVS HOME Location attribute
omvsProgram	PROGRAM	OMVS Program attribute
omvsUid	UID	OMVS UID Attribute
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

Table A–1 (Cont.) User Field Mapping

Oracle Identity Manager Gateway Field	IBM RACF Field	Description
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	Data set profile of the user
lastaccessdate	LAST-ACCESS	Last time the user accessed the system
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

A.2 Group Field Mapping

Table A–2 describes the group field mapping between Oracle Identity Manager and IBM RACF.

Table A–2 Group Field Mapping

Oracle Identity Manager Field	IBM RACF Field	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

A.3 Resource Profile Field Mapping

Table A–3 describes the resource profile field mapping between Oracle Identity Manager and IBM RACF.

Table A–3 Data Set Resource Profile Field Mapping

Oracle Identity Manager Field	IBM RACF Field	Description
cn	PROFILE NAME	The profile id
standardAccessList	ID,ACCESS,ACCESS COUNT	The standard access list of IDs and access for the data set
conditionalAccessList	ID,ACCESS,ACCESS COUNT	The conditional access list of IDs and access for the data set
owner	OWNER	The owner of the data set
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 data set

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

B.1 Oracle Identity Manager LDAP Gateway

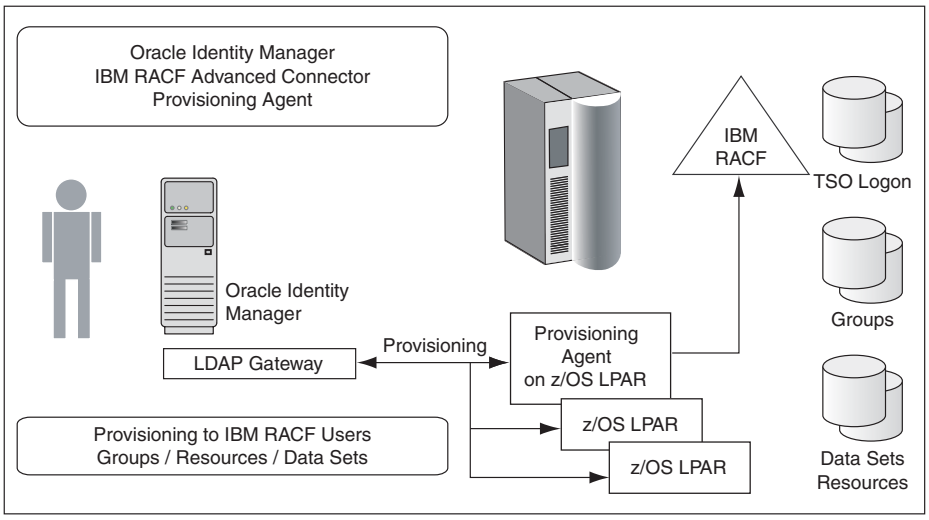
The architecture for Oracle Identity Manager Advanced connector begins with the Oracle Identity Manager LDAP Gateway. The LDAP Gateway is built on Java 1.4.2, allowing for portability across different platforms and operating systems and complete integration with the Oracle Identity Manager system.

The LDAP Gateway works transparently with Oracle Identity Manager to communicate with IBM RACF 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.

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.

B.2 Oracle Identity Manager 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.



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 building CLIST files, and working to replicate existing mainframe user profile scenarios. The Provisioning Agent can also extend authorization to data sets, groups, and resources through enterprise rules set in Oracle Identity Manager.

Mainframe architecture includes 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.

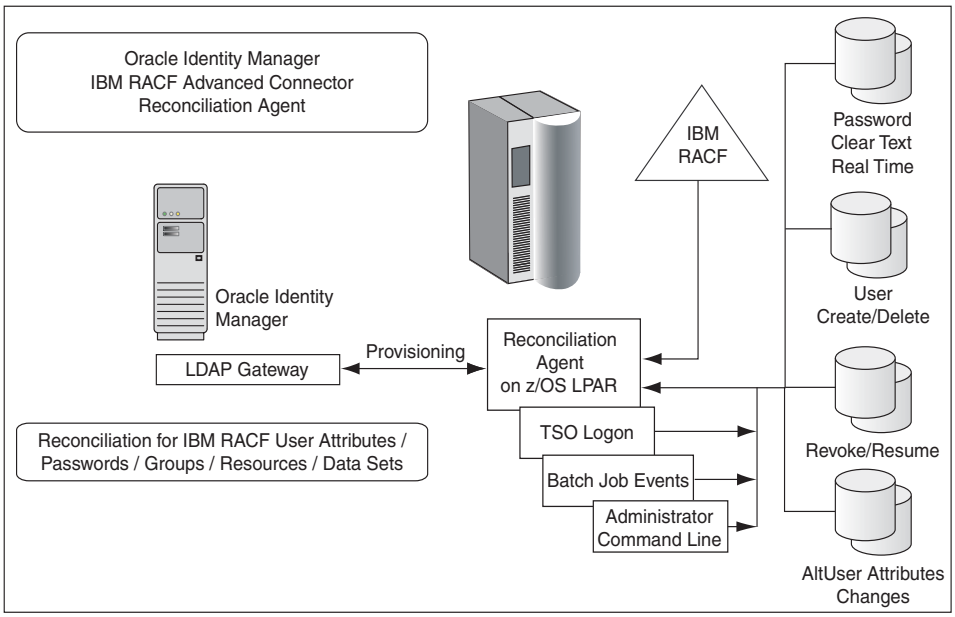
An important architectural feature of the Provisioning Agent is that provisioning updates are made from the LDAP Gateway to the IBM RACF Advanced authentication repository. As such, the Provisioning Agent needs to be installed on at least one z/OS LPAR. Provisioning commands sent from Oracle Identity 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 that 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.

B.3 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 real time. 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. If 1 MB of mainframe memory is allocated to the messaging subpools, they can hold up to 50,000 identity event messages. 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. 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 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 an LPAR exit change is only recognized after an IPL.

B.4 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.

The LDAP Gateway 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, and does not depend on platform-specific programs or libraries.

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

Messages between the LDAP Gateway 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.

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 Agent 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 Gateway, again in an encrypted format.

C

Installing Exits for Voyager

The exits that the Reconciliation Agent (Voyager) uses to capture real-time data are standard RACF exits and are all passive. They do not change data on the target system. These exits, ICHPWX01, ICHRIX02, and IRREVX01 are used in some environments and are not used in others. These exits can be installed after an initial installation of Pioneer (the Provisioning Agent).

To integrate the reconciliation exits into the target system environment, the approach illustrated by the following code block is recommended:

```
RET0     DS    0H
         L     R15,=V(USRRIX02)
         LM    R0,R12,20(R13)
         BR    R15
```

In this code block, `USRRIX02` is the connector exit called `LOGRIX02`.

You must make the required changes in the existing exit to call LOGRIX02. For example, you must re-assemble and Linkedit the exit and then IPL.

> **Caution:** Both ICHRIX02 and ICHPWX01 use MODESET macros in assembler to place themselves in supervisor mode. A test LPA and test IEASYSXX must be developed for testing the new exits. Otherwise, if a coding error occurs, you might not be able to IPL the z/OS system.

D

Reconciliation Agent (Voyager) Messages

This appendix describes messages generated by the Reconciliation Agent.

Note: All Reconciliation Agent messages are prefixed with `IDMV`.

Message: **IDMV000I** Voyager Reconciliation Agent Starting

Message-Type: Informational

Action Required: None

Message: **IDMV001I** Voyager Input Parameters are OK

Message-Type: Informational

Action Required: None

Description: All parameters passed via PARM= statement were ok no errors

Message: **IDMV002I** Voyager Build Level is at yyyymmddHHMM

Message-Type: Informational

Action Required: None

Description: Voyager Build yyyy = 4 digit year, mm = 2 digit month dd = 2 digit day, HH = 2 digit hour, MM = 2 digit month This was the year,month,day,hour and minute of the Pioneer Reconciliation Agent Production Build prior to Distribution.

Message: **IDMV004I** Voyager Detects (TCPIP) Jobname XXXXXXXX

Message-Type: Informational

Action Required: None

Description: Voyager has detected the TCPIP STC(Started Task) Name where XXXXXXXX is the STC name passed via the TCPN parameter and used for the connection to the LDAP Gateway.

Message: **IDMP005I** Pioneer Detects (TCPIP) IP Address of

xxx.xxx.xxx.xxx

Message-Type: Informational

Action Required: None

Description: Voyager will use this IP Address and PORT= to connect to the LDAP Gateway. This IP Address or Hostname is passed via PARM= , IPAD= parameter.

Message: **IDMV006I** Voyager Detects (TCPIP) IP PORT xxxx

Message-Type: Informational

Action Required: None

Description: Voyager will use the PORT= number in conjunction with The IPAD= parameter to connect to the LDAP gateway.

Message: **IDMV007I** Voyager Detects Encryption is ON

Message-Type: Informational

Action Required: None

Description: Voyager via ESIZE=16 will turn on 'enable' AES 128 encryption module for encryption of messages to/from LDAP.

Message: **IDMV008I** Voyager Detects Cache Delay Set to xx Secs

Message-Type: Informational

Action Required: None

Description: Voyager via DELAY= parameter will set a DELAY for polling Cache to xx Secs this is only applicable to CA Top-Secret users only. All other users (RACF and ACF2) should set this Parameter to DELAY=00

Message: **IDMV009I** Voyager Detects Cache File Opened OK

Message-Type: Informational

Action Required: None

Description: Voyager's external Cache file on dasd has opened ok.

Message: **IDMV010I** Voyager Computing Cache Timer Delay successful

Message-Type: Informational

Action Required: None

Description: Voyager computed the DELAY= value correctly and will use it for polling cache. This is only applicable to CA Top-Secret users only.

Message: **IDMV011I** Voyager Detects Encryption

KVER xxxxxxxxxxxxxxx

Message-Type: Informational

Action Required: None

Description: Voyager via ESIZE= parameter passed as a PARM= in the STC is using KVER xxxxxxxxxxxxxxxx for Encryption.

Message: **IDMV012I** Voyager Detects Debugging is ON

Message-Type: Informational

Action Required: None

Description: Voyager will use the DEBUG= parameter passed to provide detailed diagnostics for Oracle/IDF technical personnel. The output routes to the DEBUGOUT 'DD' statement in Voyager. Be aware if DEBUG=Y then there will be a lot of output placed into the JES2 queue.

Message: **IDMV013I** Voyager Detects Debugging is OFF

Message-Type: Informational

Action Required: None

Description: Voyager will use the DEBUG= parameter passed and no detailed diagnostics will route to the DEBUGOUT 'DD' statement in Voyager.

Message: **IDMV014I** Voyager Detects MVS retcodes of xxx

Message-Type: Informational

Action Required: None

Description: Voyager via the PRTNCODE= parameter passed will use this value for its return code when it is shutdown. The value of 'SHUTRC' will produce a 0000 return code and the value of 'TERMRC' will produce the return code greater than zero and that was contained in register 15 at time of shutdown.

Message: **IDMV015I** Voyager Detects Country Code of XX

Message-Type: Informational

Action Required: None

Description: Voyager has queried z/OS and retrieved the Country code of this system. This will be used in all conversions from EBCDIC to ASCII and ASCII to EBCDIC.

Message: **IDMV016I** Voyager Detects Hostname of xxxxxxxxxx.xxx

Message-Type: Informational

Action Required: None

Description: Voyager was passed via IPAD= parameter a Hostname instead Of an IP address and this will be used to connect to the LDAP Gateway.

Message: **IDMV016E** Voyager Detects Bad Hostname of xxxxxxxxxx.xxx

Message-Type: Error

Action Required: Investigate error

Description: Voyager was passed via IPAD= parameter a Hostname instead Of an IP address and this will be used to connect to the LDAP Gateway this Hostname was queried via the local DNS server(s) and failed to be resolved.

Message: **IDMV019I** Voyager Initialization of TCP API was Successful

Message-Type: Informational

Action Required: None

Description: Voyager has initialized the TCPIP stack successfully

Message: **IDMP019E** Voyager Initialization of TCP API Failed RC: xx

Message-Type: Error

Action Required: Investigate error

Description: Voyager's initialization of the TCPIP API interface failed. A primary cause is a missing security subsystem (RACF,ACF2, Or Top-Secret) permit for facility 'bpx.*'

Message: **IDMV020I** Voyager Initialization of GETCLIENTID was Successful

Message-Type: Informational

Action Required: None

Description: Voyager has issued a GETCLIENTID and it was successful. This is normal for the client/socket server like Voyager.

Message: **IDMV021I** Voyager Accepting Messages on xxx.xxx.xxx.xxx (OR) hostname.com

Message-Type: Informational

Action Required: None

Description: Voyager will send/receive message to/from the LDAP gateway

on IP Address xxx.xxx.xxx.xxx with PORT= or on Hostname - Hostname.com with PORT=

* Note: Hostname.com is an example, this would be the hostname

Of the LDAP gateway.

Message: **IDMV021I** Voyager Initialization of PTON was successful

Message-Type: Informational

Action Required: None

Description: Voyager successfully converted the IP address to the correct

addressing type to communicate to the LDAP gateway.

Message: **IDMV021E** Voyager Initialization of PTON failed RC: xx

Message-Type: Error

Action Required: Investigate

Description: Voyager failed during its conversion to numeric. The RC(return code) is documented in the following source. z/OS V1R9.0 Communication Server IP CICS Sockets Guide Manual – SC31-8807-04

Message: **IDMV025I** Voyager Connected to Gateway Server

was successful

Message-Type: Informational

Action Required: None

Description: Voyager successfully connected to the LDAP Gateway using either IP address = xxx.xxx.xxx.xxx or Hostname.com with PORT = xxxx.

Message: **IDMV032I** Voyager Connection Start Timer Begins

Message-Type: Informational

Action Required: None

Description: Voyager using PARM= , 'STARTDELAY=' will delay it's connection by xx secs specified in 'STARTDELAY='. The 'STARTDELAY=' timer started.

Message: **IDMV033I** Voyager Connection Start Timer Ends

Message-Type: Informational

Action Required: None

Description: Voyager using PARM= , 'STARTDELAY=' will delay it's connection by xx secs specified in 'STARTDELAY='. The 'STARTDELAY=' timer ended.

Message: **IDMV050I** Voyager Cache Polling Begins

Message-Type: Informational

Action Required: None

Description: Voyager has started polling its subpool 231 cache for events created by the installed product exits. This is a normal process for the real-time reconciliation agent.

Message: **IDMV051I** Voyager Cache Polling Ends

Message-Type: Informational

Action Required: None

Description: Voyager has ended its polling its subpool 231 cache for events created by the installed product exits. This is a normal process for the real-time reconciliation agent.

Message: **IDMV100I** Voyager Shutdown Started

Message-Type: Informational

Action Required: None

Description: Voyager Shutdown has started via a z/OS Modify command.

Message: **IDMV101I** Voyager Reconciliation Agent Has Terminated

Message-Type: Informational

Action Required: None

Description: Voyager has been terminated

Message: **IDMV102I** Voyager has Ended with Zero Return Codes

Message-Type: Informational

Action Required: None

Description: Voyager has ended with a zero MVS Condition code. This condition was set with the PRTNCODE=SHUTRC parameter.

Message: **IDMV103I** Voyager has Ended with Non-Zero Return Code

Message-Type: Informational

Action Required: None

Description: Voyager has ended with a non-zero MVS Condition code. This condition was set with the PRTNCODE=TERMRC parameter.

Message: **IDMV104I** Voyager sent messages xxxxxx received messages xxxxxx

Message-Type: Informational – Shutdown Statistic

Action Required: None

Description: Voyager shutdown statistic on amount of work done.

Message: **IDMV102E** Voyager Cache Dasd File Not be Found

Message-Type: Error

Action Required: Investigate

Description: Voyager Cache dasd file used for recovery was not found and Voyager will abend.

Message: **IDMV130I** Voyager Operator Interface now Open for 30 Seconds

Message-Type: Informational

Action Required: None

Description: Voyager Modify Operator interface is now open for commands.

Message: **IDMV130I** Voyager Operator Interface now Closed

Message-Type: Informational

Action Required: None

Description: Voyager Modify Operator interface is now closed and no more Modify commands are accepted.

Message: **IDMV151I** Voyager DNS Request hostname.com

Message-Type: Informational

Action Required: None

Description: Voyager via IPAD= has been asked to use a DNS hostname instead of an IP Address to connect to the LDAP gateway.

Message: **IDMV152I** Voyager IP Connect Request xxx.xxx.xxx.xxx

Message-Type: Informational

Action Required: None

Description: Voyager via IPAD= has been asked to use an IP address instead of a hostname to connect to the LDAP gateway.

-

Message: **IDMV200E** Voyager Startup Parameter Error xxxxxxxxxxxxxx

Message-Type: Informational

Action Required: None

Description: Voyager had a startup PARM= error , indicated by xxxxxxxxxxxxxx

-

Message: **IDMV200I** Voyager unable to connect to the Gateway

Message-Type: Informational

Action Required: None

Description: Voyager was unable to connect to the LDAP Gateway either Via hostname or IP Address, Voyager will retry the connection. This message and IDMV201I usually are together.

-

Message: **IDMV201I** Voyager connection to the Gateway failed

Message-Type: Informational

Action Required: None

Description: Voyager was unable to connect to the LDAP Gateway either Via hostname or IP Address, Voyager will retry the connection. This message and IDMV200I are usually together.

-

Message: **IDMV202E** Voyager no Storage Token Found

Message-Type: Informational

Action Required: None

Description: Voyager was unable to find the required subpool 231 storage token, Voyager will terminate.

-

Message: **IDMV202I** Voyager Unable to Connect to new IP/Port

Message-Type: Informational

Action Required: None

Description: Voyager's IP address and port were swapped via a Modify command and it could not connect to the LDAP using that combination.

Message: **IDMV203E** Voyager Quiescing Because of the subpool Not found.

Message-Type: Informational

Action Required: None

Description: Voyager is shutting down because of a missing Storage token for the subpool, required for normal operations.

Message: **IDMV204E** Voyager subpool 231 cannot be found

Message-Type: Informational

Action Required: None

Description: Voyager went to poll the subpool 231 (cache) for events And the subpool was not there. This will result in Voyager Quiescing and shutting down.

Message: **IDMV300I** *Debug* - xxxxxxxxxxxxxxxxxxxxxx

Message-Type: Error

Action Required: None

Description: Voyager will display this statement when DEBUG=Y is on and Output will route to // DEBUGOUT 'DD'.

E

Provisioning Agent (Pioneer) Messages

This appendix describes messages generated by the Provisioning Agent.

> **Note:** All Reconciliation Agent messages are prefixed with `IDMP`.

Message: **IDMP000I** Pioneer Provision Agent is Starting

Message-Type: Informational

Action Required: None

Message: **IDMP001I** Pioneer Input Parameters are OK

Message-Type: Informational

Action Required: None

Meaning: All parameters passed via PARM= statement were ok no errors

Message: **IDMP002I** Pioneer Detects Build yyyymmddHHMM

Message-Type: Informational

Action Required: None

Meaning: Pioneer Build yyyy = 4 digit year , mm = 2 digit month dd = 2 digit day, HH = 2 digit hour , MM = 2 digit month. This was the year,month,day,hour and minute of the Pioneer Provisioning Agent Production Build prior to Distribution.

Message: **IDMP003I** Pioneer Detects TCPIP Jobname XXXXXXXX

Message-Type: Informational

Action Required: None

Meaning: Pioneer has detected the TCPIP STC(Started Task) Name where XXXXXXXX is the STC name passed via the TCPN parameter and used for the connection to the LDAP Gateway.

Message: **IDMP004I** Pioneer Detects TCPIP IP Address of xxx.xxx.xxx.xxx

Message-Type: Informational

Action Required: None

Meaning: Pioneer will not use this IP Address it must be 0.0.0.0 , Pioneer is a Socket Server and is only using PORT=, passed by the IPAD= parameter.

Message: **IDMP005I** Pioneer Detects TCPIP IP PORT of xxxx

Message-Type: Informational

Action Required: None

Meaning: Pioneer will use this port passed in the PORT= parameter to accept connections from the LDAP server. This port does not need reserving in the TCPIP cpnfiguration file on z/OS.

Message: **IDMP006I** Pioneer Detects Debugging is ON

Message-Type: Informational

Action Required: None

Meaning: Pioneer will use the DEBUG= parameter passed to provide detailed diagnostics for Oracle/IDF technical personnel. The output routes to the DEBUGOUT 'DD' statement in Pioneer. Be aware if DEBUG=Y then there will be a lot of output placed into the JES2 queue.

Message: **IDMP007I** Pioneer Detects Debugging is OFF

Message-Type: Informational

Action Required: None

Meaning: Pioneer will use the DEBUG= parameter passed and no detailed diagnostics will route to the DEBUGOUT 'DD' statement in Pioneer.

Message: **IDMP008I** Pioneer Detects KVER xxxxxxxxxxxxxxxx

Message-Type: Informational

Action Required: None

Meaning: Pioneer via ESIZE= parameter passed as a PARM= in the

STC is using KVER xxxxxxxxxxxxxxxx for Encryption.

Message: **IDMP009I** Pioneer Detects Encryption Enabled

Message-Type: Informational

Action Required: None

Meaning: Pioneer via ESIZE=16 will turn on 'enable' AES 128 encryption module for encryption of messages to/from LDAP.

Message: **IDMP010I** Pioneer Detects Encryption Disabled

Message-Type: Informational

Action Required: None

Meaning: Pioneer via ESIZE=00 will turn off 'disable' AES 128 encryption module for encryption of messages to/from LDAP. Warning, Pioneer will not work in this mode of Operation.

Message: **IDMP011I** Pioneer Detects CPUID xxxxxxxxxxxx

Message-Type: Informational

Action Required: None

Meaning: Pioneer has queried z/OS and retrieved the actual CPUID of the system it is running.

Message: **IDMP012I** Pioneer Detects Sysplex Sysname xxxxxxxx

Message-Type: Informational

Action Required: None

Meaning: Pioneer has queried z/OS and retrieved the actual Sysplex Sysname it is executing on.

Message: **IDMP013I** Pioneer Detects LPARNAME xxxxxxxx

Message-Type: Informational

Action Required: None

Meaning: Pioneer via the LPAR= parameter will use the xxxxxxxx as A name for this system. This is informational only. Will be used in a later release of software.

Message: **IDMP014I** Pioneer Detects Country Code of XX

Message-Type: Informational

Action Required: None

Meaning: Pioneer has queried z/OS and retrieved the Country code of this system. This will be used in all conversions from EBCDIC to ASCII and ASCII to EBCDIC.

Message: **IDMP015I** Pioneer Detects Job Wait Time Of xx Secs

Message-Type: Informational

Action Required: None

Meaning: Pioneer has detected a Job Wait Time Of xx seconds. This is The JWAIT= PARM. Used for an optional feature not supported by all versions of Pioneer or LDAP.

Message: **IDMP015I** Pioneer Detects RECON wait time of xx Mins

Message-Type: Informational

Action Required: None

Meaning: Pioneer has detected via PARM= a RWAIT= which controls the Amount of time Pioneer waits to query RECON file completion.

Message: **IDMP020I** Pioneer Accepting Messages on xxx.xxx.xxx.xxx

Message-Type: Informational

Action Required: None

Meaning: Pioneer has initialized the TCPIP stack with its calls and has bound a socket for listening to the PORT= parameter..

Message: **IDMP020A** Pioneer Operator has Issued a Shutdown Command

Message-Type: Informational

Action Required: Action

Meaning: Pioneer has been requested to shutdown via Modify command passed from console, TSO or automation.

Message: **IDMP030I** Pioneer INITAPI was successful

Message-Type: Informational

Action Required: None

Meaning: Pioneer has Initialized the TCPIP stack successfully

Message: **IDMP031I** Pioneer GETCLIENTID was successful

Message-Type: Informational

Action Required: None

Meaning: Pioneer has issued a GETCLIENTID and it was successful.

This is normal for the socket server like Pioneer.

Message: **IDMP032I** Pioneer CLIENT NAME/ID is xxxxxxxx

Message-Type: Informational

Action Required: None

Meaning: Pioneer has successfully acquired the CLIENTID required for a socket server connection and it will use xxxxxxxx as the name.

Message: **IDMP033I** Pioneer CLIENT TASK is xxxxxxxx

Message-Type: Informational

Action Required: None

Meaning: Pioneer has successfully acquired the CLIENTID required for a socket server connection and it will use xxxxxxxx as the Task name.

Message: **IDMP034I** Pioneer CREATE SOCKET was successful

Message-Type: Informational

Action Required: None

Meaning: Pioneer has successfully created a socket for its SOCKET Server function.

Message: **IDMP035I** Pioneer BIND SOCKET was successful

Message-Type: Informational

Action Required: None

Meaning: Pioneer has successfully BINDED the Socket to the port that was passed via PORT= parameter.

Message: **IDMP036I** Pioneer Listening port is xxxx

Message-Type: Informational

Action Required: None

Meaning: Pioneer will be listening on port xxxx for incoming LDAP requests.

Message: **IDMP037I** Pioneer Listening Address is xxx.xxx.xxx.xxx

Message-Type: Informational

Action Required: None

Meaning: Pioneer will be listening on IP Address xxx.xxx.xxx.xxx for incoming LDAP requests.

Message: **IDMP038I** Pioneer Listen Socket Call was successful

Message-Type: Informational

Action Required: None

Meaning: Pioneer has successfully issued a Socket Listen call.

Message: **IDMP039I** Pioneer Read Socket Call was successful

Message-Type: Informational

Action Required: None

Meaning: Pioneer has received a message from the LDAP gateway via the Read Socket call and it was successful..

Message: **IDMP039I** Pioneer Write Socket Call was successful

Message-Type: Informational

Action Required: None

Meaning: Pioneer has sent a message to the LDAP gateway via the Write Socket call and it was successful..

Message: **IDMP040I** Pioneer Translation was successful from-to xxxxxxxxxxxxxxxxx. (ASCII-TO-EBCDIC) or (EBCDIC-TO-ASCII)

Message-Type: Informational

Action Required: None

Meaning: Pioneer successfully translated LDAP's message from

ASCII-TO-EBCDIC or translated the message going to

The LDAP gateway from EBCDIC-TO-ASCII

Message: **IDMP040E** Pioneer Translation was not successful from-to

xxxxxxxxxxxxxxxxx.(ASCII-TO-EBCDIC) or (EBCDIC-TO-ASCII)

Message-Type: Informational

Action Required: None

Meaning: Pioneer did not successfully translated LDAP's message from

ASCII-TO-EBCDIC or the message going to

The LDAP gateway from EBCDIC-TO-ASCII

Message: **IDMP040I** Pioneer Socket Accept was successful

Message-Type: Informational

Action Required: None

Meaning: Pioneer's Socket Accept call was successful.

Message: **IDMP040E** Pioneer Socket Accept was not successful RC: xxxxxxxx

Message-Type: Error

Action Required: Review Socket Accept Return Code and take required action as outlined in z/OS V1R9.0 Communication Server IP CICS Sockets Guide – SC31-8807-04

Meaning: Pioneer's Socket Accept call failed with RC: xxxxxxxx

Message: **IDMP048I** Pioneer LDAP Connection Timed out

Message-Type: Informational

Action Required: None

Meaning: Pioneer to LDAP connection timed out.

Message: **IDMP049I** Pioneer Has Been Idle for 30 Mins

Message-Type: Informational

Action Required: None

Meaning: Pioneer has not received any messages from LDAP Gateway in 30 mins.

Message: **IDMP050A** Pioneer Closing IP Connection

Message-Type: Informational

Action Required: None

Meaning: Pioneer has received or issued a Socket Close and the connection will be closed.

Message: **IDMP051I** Pioneer Close Socket Call was Successful

Message-Type: Informational

Action Required: None

Meaning: Pioneer has received or issued a Socket Close and it was successful

Message: **IDMP052I** Pioneer Shutdown Socket Call was Successful

Message-Type: Informational

Action Required: None

Meaning: Pioneer has received or issued a Socket Close and it was successful

Message: **IDMP053I** Pioneer MYRADMIN SAF call was Successful

Message-Type: Informational

Action Required: None

Meaning: Pioneer has passed the security system function call via the SAF interface (module IRRSEQ00) and it was a success.

Message: **IDMP054I** Pioneer Received TSS Recon Request from LDAP

Message-Type: Informational

Action Required: None

Meaning: Pioneer has received a Batch Recon request from the LDAP Gateway.

Message: **IDMP055I** Pioneer Recon Processing Started

Message-Type: Informational

Action Required: None

Meaning: Pioneer has received a Batch Recon request from the LDAP Gateway and has been submitted to z/OS.

Message: **IDMP056I** Pioneer Recon Processing Ended

Message-Type: Informational

Action Required: None

Meaning: Pioneer Batch Recon request has ended.

Message: **IDMP057I** Pioneer Recon Processing Successful

Message-Type: Informational

Action Required: None

Meaning: Pioneer Batch Recon Request was successful and data was retrieved and send back to the LDAP gateway..

Message: **IDMP058I** Pioneer Recon Has Processed: xxxx Userids

Message-Type: Informational

Action Required: None

Meaning: Pioneer Recon Processing status message. The xxxx is the increment and is usually 1000 userids/ACIDS.

Message: **IDMP058I** Pioneer Recon Total Processed: xxxxxx Userids

Message-Type: Informational

Action Required: None

Meaning: Pioneer Recon Processing status message. The xxxxxx is the total of the processed userids/ACIDS and is put out with the first IDMP058I message.

Message: **IDMP070I** Pioneer xxxxxxxx Is Now Open

Message-Type: Informational

Action Required: None

Meaning: Pioneer file xxxxxxxx is now Open.

Message: **IDMP071I** Pioneer xxxxxxxx Is Now Closed

Message-Type: Informational

Action Required: None

Meaning: Pioneer file xxxxxxxx is now Closed

Message: **IDMP070I** Pioneer Could Not Open xxxxxxxx RC: xx

Message-Type: Informational

Action Required: None

Meaning: Pioneer file xxxxxxxx could not be opened

Message: **IDMP080I** Pioneer Job Submitted to the Intrdr

Message-Type: Informational

Action Required: None

Meaning: Pioneer has punched a Job to the Intrdr, see JCLOUTP 'DD' in Pioneer for details.

Message: **IDMP100I** Pioneer (IN) Msgs Processed is xxxxxxxxxx

Message-Type: Informational – Shutdown Statistic

Action Required: None

Meaning: Pioneer has processed xxxxxxxxxx (IN) bound messages from LDAP gateway.

Message: **IDMP100I** Pioneer (OUT) Msgs Processed is xxxxxxxxxx

Message-Type: Informational – Shutdown Statistic

Action Required: None

Meaning: Pioneer has processed xxxxxxxxxx (OUT) bound messages To LDAP gateway.

Message: **IDMP100I** Pioneer Message (READ) Bytes xxxxxxxxxx

Message-Type: Informational – Shutdown Statistic

Action Required: None

Meaning: Pioneer has processed xxxxxxxxx (IN) bound messages bytes from LDAP gateway.

Message: **IDMP100I** Pioneer Message (WRITE) Bytes xxxxxxxxxx

Message-Type: Informational – Shutdown Statistic

Action Required: None

Meaning: Pioneer has processed xxxxxxxxx (OUT) bound messages bytes to the LDAP gateway.

Message: **IDMP200E** Pioneer Startup Parameter Error xxxxxxxxxxxxx

Message-Type: Error

Action Required: None

Meaning: Pioneer has shutdown with a PARM= error, see SYSOUT 'DD'for the details of the error.

Message: **IDMP300I** *Debug* - xxxxxxxxxxxxxxxxxxxxxxx

Message-Type: Error

Action Required: None

Meaning: Pioneer will display this statement when DEBUG=Y is on and Output will route to // DEBUGOUT 'DD'.

Index

M

O

P

R

S

T

U

V

X