Oracle® Identity Manager

Connector Guide for CA ACF2 Advanced

Release 9.0.4

E10423-17

August 2018

ORACLE

Oracle Identity Manager Connector Guide for CA ACF2 Advanced, Release 9.0.4

E10423-17

Primary Author: Balakrishnan Nanjan

Contributing Author: Prakash Hulikere

Contents

Preface ix

Audience ix
Documentation Accessibility ix
Related Documents ix
Documentation Updates ix
Conventions x

What's New in the Oracle Identity Manager Connector for CA ACF2? xi

Software Updates xi
Documentation-Specific Updates xxi

1 About the Connector

1.1 Certified Components 1-1
1.2 Certified Languages 1-2
1.3 Connector Architecture 1-2
1.3.1 Connector Components 1-3
1.3.2 Connector Operations 1-3
1.3.2.1 Full Reconciliation Process 1-3
1.3.2.2 Incremental (Real-Time) Reconciliation Process 1-4
1.3.2.3 Provisioning Process 1-6
1.4 Features of the Connector 1-7
1.4.1 Target Resource and Trusted Source Reconciliation 1-8
1.4.2 Full and Incremental Reconciliation 1-8
1.4.3 Encrypted Communication Between the Target System and Oracle Identity Manager ... 1-8
1.4.4 High Availability Feature of the Connector 1-8
1.5 Connector Objects Used During Reconciliation and Provisioning 1-9
1.5.1 Supported Functions for Reconciliation 1-9
1.5.2 Supported Functions for Provisioning 1-9
1.5.3 User Attributes for Target Resource Reconciliation and Provisioning 1-10
1.5.3.1 Resource Rule Attributes for Target Resource Reconciliation and Provisioning 1-13
1.5.3.2 Access Rule Attributes for Target Resource Reconciliation and Provisioning. 1-13
1.5.4 User Attributes for Trusted Source Reconciliation 1-14
1.5.5 Reconciliation Rule 1-14

1.5.6 Reconciliation Action Rules 1-15

2 Deploying the IdF Advanced Adapter for ACF2

2.1 IDF Mainframe Adapters Functional Characteristics 2-1
2.1.1 Alias Post-Processing 2-1
2.1.2 Other Post-Processing 2-1
2.2 Prerequisites 2-3
2.2.1 Message Transport Requirements 2-3
2.2.2 APF Authorization 2-3
2.3 Mainframe Adapter Installation 2-3
2.3.1 Extracting the Files from the Distribution Zip Archive File 2-4
2.3.2 Uploading the Files 2-4
2.3.3 Extracting the XMIT Files 2-7
2.3.4 Editing the Mainframe Batch Job Files to Match the Settings for the Customer's Site 2-11
2.3.5 Submitting Batch Job Streams 2-16
2.3.6 Loading and Activating the Exits 2-17
2.3.7 Creating an ACF2 LID for Pioneer and Voyager with Permissions 2-18
2.3.8 Adding Pioneer/Voyager to the Resource Rule Facilities (BPX and IRR) 2-19
2.3.9 Testing the Installation 2-22

3 Connector Deployment on Oracle Identity Manager

3.1 Files and Directories that Comprise the Connector 3-1
3.2 Determining the Release Number of the Connector 3-2
3.3 Before Running the Connector Installer 3-3
3.4 Running the Connector Installer 3-3
3.5 Configuring the IT Resource 3-5
3.6 Configuring Oracle Identity Manager 3-7
3.6.1 Clearing Content Related to Connector Resource Bundles from the Server Cache 3-7
3.6.2 Enabling Logging 3-9
3.7 Configuring Trusted Source Reconciliation 3-10
3.8 Configuring Oracle Identity Manager for Request-Based Provisioning 3-11
3.8.1 Copying Predefined Request Datasets 3-11
3.8.2 Importing Request Datasets into the MDS 3-12
3.8.3 Enabling the Auto Save Form Feature 3-13
3.8.4 Running the PurgeCache Utility 3-13
3.9 Installing and Configuring the LDAP Gateway 3-13

4 Configuring the Connector

4.1 Performing Full Reconciliation 4-1
4.2 Configuring Account Status Reconciliation 4-4
4.3 Configuring Filtered Reconciliation to Multiple Resource Objects 4-4
4.4 Guidelines on Using the Connector 4-5
4.5 Performing Provisioning Operations 4-6
4.5.1 Provisioning Users 4-6
4.5.1.1 Direct Provisioning 4-6

4.5.1.2 Request-Based Provisioning 4-8
4.5.1.2.1 End User's Role in Request-Based Provisioning..... 4-8
4.5.1.2.2 Approver's Role in Request-Based Provisioning..... 4-9
4.6 Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1 4-9
4.7 Configuring Resource and Access Rule Pre-Population Scheduled Tasks 4-10

5 Extending the Functionality of the Connector

5.1 Adding New Attributes for Target Resource Reconciliation 5-1
5.2 Adding New Attributes for Provisioning 5-2
5.3 Removing Attributes Mapped for Target Resource Reconciliation and Provisioning..... 5-3
5.4 Configuring the Connector for Provisioning to Multiple Installations of the Target System . 5-4
5.5 Configuring the Connector for Reconciliation of Multiple Installations of the Target System 5-5
5.6 Reconciling Deleted Users to Oracle Identity Manager 5-6
5.7 Reconciling Users to the Internal LDAP..... 5-9
5.8 Reconciling Internal LDAP Users to Oracle Identity Manager..... 5-11

6 Troubleshooting

7 Known Issues

A Reconciliation Agent (Voyager) Messages

B Provisioning Agent (Pioneer) Messages

C Authorized Libraries

D Relationship between the Pioneer (DDs), Voyager (DDs) and the INDDs

E LOADDSN1 Member and the File Contents

F Voyager and Pioneer Control File Parameters

G Mainframe Language Environment Runtime Options

Index

List of Tables

1–1	Certified Components	1-2
1–2	Supported Functions for Provisioning	1-10
1–3	User Attributes for Target Resource Reconciliation and Provisioning	1-10
1–4	Resource Rule Attribute Mappings	1-13
1–5	Access Rule Attribute Mappings	1-13
1–6	User Attributes for Trusted Source Reconciliation	1-14
1–7	Reconciliation Action Rules	1-15
2–1	File Names on Client Machine and Mainframe Host	2-7
2–2	XMIT File Names and PDS Names	2-7
2–3	YOURHLQ	2-14
2–4	LOADDSN1	2-15
2–5	Pioneer Commands and Descriptions	2-27
2–6	Voyager Commands via Operator Interface	2-27
3–1	Files and Directories that Comprise the Connector	3-1
3–2	IT Resource Parameters	3-6
3–3	Logger Parameters	3-10
3–4	Properties in the acf2.properties File	3-14
4–1	Attributes of the Reconcile All Users Scheduled Task	4-3
4–2	Attributes of the FindAllAccessRules and FindAllResourceRules Scheduled Tasks	4-12
5–1	Attributes of the Deleted User Reconciliation to OIM Scheduled Task	5-8
5–2	Attributes of the Reconcile User to internal LDAP Scheduled Task	5-10
5–3	Attributes of the Reconcile LDAP Users Scheduled Task	5-12
6–1	Troubleshooting Tips	6-1
6–2	Three Options Settings and their Effects	6-2
D–1	Relationship between the Pioneer (DDs) and the INDDs in CREATDSN Member	D-1
D–2	Relationship between the Voyager (DDs) and the INDDs in CREATDSN Member	D-2
D–3	Purpose of the Pioneer (DDs)	D-2
E–1	Steps of LOADDSN1 Member and File Contents	E-2
F–1	Voyager Control File Parameters	F-1
F–2	Pioneer Control File Parameters	F-2
G–1	Language Environment Run Time Options, Defaults and Recommendations	G-2

List of Figures

1–1 Incremental Reconciliation Process 1-5
1–2 Provisioning Process 1-7

Preface

This guide provides information about integrating Oracle Identity Manager with CA ACF2.

Audience

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

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Documents

For information about installing and using Oracle Identity Manager, see the Oracle Identity Manager documentation library.

For generic information about connectors, see *Oracle Fusion Middleware User's Guide for Oracle Identity Manage*r.

The following Oracle Technology Network page provides links to Oracle Identity Manager documentation:

http://docs.oracle.com/cd/E11223_01/index.htm

Documentation Updates

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

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

Conventions

The following text conventions are used in this document:

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

What's New in the Oracle Identity Manager Connector for CA ACF2?

This chapter provides an overview of the updates made to the software and documentation for the Oracle Identity Manager Connector for CA ACF2 in release 9.0.4.20.

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 sections discuss software updates:

- Software Updates in Release 9.0.4.20
- Software Updates in Release 9.0.4.19
- Software Updates in Release 9.0.4.18
- Software Updates in Release 9.0.4.17
- Software Updates in Release 9.0.4.16
- Software Updates in Release 9.0.4.15
- Software Updates in Release 9.0.4.14
- Software Updates in Release 9.0.4.13
- Software Updates in Release 9.0.4.12
- Software Updates in Release 9.0.4.11
- Software Updates in Releases 9.0.4.1 Through 9.0.4.4

Software Updates in Release 9.0.4.20

The following are the software updates in release 9.0.4.20:

- Removal of clistlib.xmi - this function is now internal to Pioneer.

- Removal of batch submitted IDCAM's Alias functions - now internal to Pioneer.
- Removal of batch submitted ACF2 rules - now internal to Pioneer.
- Removal of batch submitted ACF2 - LDAP searches - see clistlib.xmi above.

Software Updates in Release 9.0.4.19

The following are the software updates in release 9.0.4.19:

- **Support for Pioneer changes**

  From this release onward the following changes are applicable to Pioneer:

1. Parameter Changes:

   Removal of MVS PARM= parameters, the following parameters are now being added to the control file.

   a. TCPN=

   b. IPAD=

   c. PORT=

   d. DEBUG=

   See Section 2.3.9, "Testing the Installation" for more details.

2. Obsolete Parameters:

   The following control file parameters are now obsolete (required for batch processing):

   a. RWAIT=

   b. JWAIT=

   c. QUEUE_DSN=

3. Obsolete DDNAMES:

   In conjunction with the parameters in Step 2, the following Pioneer DDNAMES are now obsolete:

   a. //RECONJCL = For external batch ACF2 searches

   b. //INJCLR = For external batch ALIAS functions

4. Search Functions:

   All ACF2 search functions and ALIAS functions are now handled by Pioneer internally. To support this functionally, the following three new DDNAMES are added:

   a. //IDCAMSD - IDCAMS controls records from LDAP

   b. //ACF2CTL -ACF2 control records from LDAP

   c. //ACF2OUT -ACF2 Sysprint output

   Note: IDCAMS control parameters are DEFINE/DELETE ALIAS and LISTC functions only. The ACF2 control file will only contain ACF2 LIST functions no passwords. All three of these files are small in size. Please see the connector guide more information.

   See Appendix D for more details.

- **Support for Voyager Changes**

  From this release onward the following changes have been made to Voyager:

  1. Additional New Parameters:

     a. SUBPOOL_SIZE=7500K - values are 0200K to 7500K and is the size of Subpool requested. See Appendix F for more details.

     b. STARTUP to create the subpool is now obsolete and WRAPUP for delete the subpool is now also obsoleted. Voyager will now create the subpool and build the storage token based on the new SUBPOOL_SIZE= parameter. When a normal shutdown occurs the Voyager will delete the storage token and delete the subpool storage allocated. See Chapter 2, "Deploying the IdF Advanced Adapter for ACF2" for more details.

     c. The following Voyager Parameters have been removed and are no longer supported:

        - STARTDELAY=

        - DELAY=

        - PRTNCODE=

- **Support for Scheduled Task – Delete User Reconciliation Using Oracle Identity Manager**

  From this release onward, the connector supports an additional scheduled task for reconciling deleted users on the target system. This task retrieves a list of users from the target system and compares that list with a list of users from Oracle Identity Manager. If a user is found to exist within OIM, but not on the target system, then a delete reconciliation event for the user is sent to Oracle Identity Manager. See Section 4.3.3.2, "ACF2 Reconcile Deleted Users" for more details.

- **Support for Scheduled Task – Reconcile Users to Internal LDAP**

  From this release onward, the connector supports an additional scheduled task for reconciling users on the target system to the internal LDAP store. This task retrieves a list of users and their profiles from the target system and reconciles each user to the internal LDAP gateway metastore. See Section 4.3.3.3, "ACF2 Reconcile Users to the Internal LDAP" for more details.

- **Support for Scheduled Task – Reconcile LDAP Users**

  From this release onward, the connector supports an additional scheduled task for reconciling users from the internal LDAP store to Oracle Identity Manager. This task retrieves a list of users from the internal LDAP store and reconciles those users to Oracle Identity Manager. The task can reconcile either all users, or only users that have changed since the Last Modified Time Stamp (LMTS) IT resource property. See Section 4.3.3.4, "ACF2 Reconcile Internal LDAP Users to Oracle Identity Manager" for more details.

Resolved Issues in Release 9.0.4.19

The following table lists issues resolved in release 9.0.4.19:

Bug Number	Issue	Resolution
15845201	CN and givenName attributes are parsing incorrectly, depending on whether UID NUMBER comes before or after NAME.	This issue has been resolved. CN and givenName attributes now parse correctly.
13968611	Real-time reconciliation throwing an error: "tt13yct: duplicated key detected for oimcp_main_generic _120415.2000".	This issue has been resolved. New LDAP reconciliation scheduled tasks no longer cause this error.
14178184	Real-time reconciliation throwing an error: "t13yct: duplicated key detected for oimcp_main_generic _120603.2001".	This issue has been resolved. New LDAP reconciliation scheduled tasks no longer cause this error.
15890816	Delete reconciliation events are stuck in "Data Received" state.	This issue has been resolved. Delete reconciliation events now includes a call to finishReconciliationE vent() to close the event.
13653082	Pioneer/Voyager unable to filter events based on user privileges.	This issue has been resolved. Pioneer and Voyager can now filter processing of events based on user attributes (such as privileges).
15914553	While adding custom CICS-related privileges, no ACF2 command is generated from OIM to the target system.	This issue has been resolved. Custom privileges that include the CICS-prefix are no longer ignored.

Software Updates in Release 9.0.4.18

The following are the software updates in release 9.0.4.18:

Support for Pioneer and Voyager Filtering and New Parameters

From this release onwards, the connector supports new Pioneer and Voyager filtering, new Pioneer for shutdown statistics, and new parameters to support the filtering in both applications. See Chapter 2, "Deploying the IdF Advanced Adapter for ACF2" for more details.

Support for New JCL Members and Pioneer/Voyager Audit Log

From this release onwards, the connector supports new JCL members and Pioneer/Voyager Audit Log. See Chapter 2, "Deploying the IdF Advanced Adapter for ACF2" for more details.

Resolved Issues in Release 9.0.4.18

The following table lists issues resolved in release 9.0.4.18:

Bug Number	Issue	Resolution
13968611	SGT T13Y scan tool reports few duplicated keys defined in the resource bundle.	This issue has been resolved. The duplicated keys have been removed.
12921588	The current version of the CA-AFC2 Oracle Identity Manager connector does not support the ability to filter data in shared mainframe application.	This issue has been resolved. Now the connector supports the ability to filter data in both types of application.
14167389	When trying to reconcile users from the target system an exception is thrown.	This issue has been resolved. Now the reconciliation of the users from the target system is successful.

Software Updates in Release 9.0.4.17

The following is a software update in release 9.0.4.17:

Support for Multiple Target Resource Reconciliation Through a Single LPAR

From this release onward, change-based reconciliation using a single LDAP gateway installation from multiple target resource systems is supported. As part of this update, the VOYAGER_ID.properties file (previously known as acf2Connection.properties) must be renamed to match the Voyager server's VOYAGER_ID control file property.

See Section 5.5, "Configuring the Connector for Reconciliation of Multiple Installations of the Target System," and Section 4.3.3.2, "ACF2 Reconcile Deleted Users".

Resolved Issues in Release 9.0.4.17

The following table lists issues resolved in release 9.0.4.17:

Bug Number	Issue	Resolution
13147557	ACF2 connector restricts DSN to either Pioneer or Voyager	This issue has been resolved. Procedures and parameters for Pioneer and Voyager have been updated.

Software Updates in Release 9.0.4.16

The following are the software updates in release 9.0.4.16:

- New LDAP Search for Pioneer
- RWAIT= Control Parameter Removed from Control File
- New SYSOUT Data Definition JCL Statements Added
- New Permission Required for Voyager
- Voyager Uses Control File Similar to Pioneer

- Voyager Supports New Parameter for Control File

New LDAP Search for Pioneer

All batch submitted "Searchalls" that are LDAP initiated to Pioneer are now internal to Pioneer by calling ACF2 directly. See the Chapter 2, "Deploying the IdF Advanced Adapter for ACF2" for more details.

RWAIT= Control Parameter Removed from Control File

RWAIT= control parameter has now been removed from the control file. This parameter was used for the external batch "Searchall" submissions.

New SYSOUT Data Definition JCL Statements Added

New SYSOUT "DD" (data definition) JCL statements have been added for the internal ACF2 call. See the Chapter 2, "Deploying the IdF Advanced Adapter for ACF2" for more details.

New Permission Required for Voyager

Voyager now requires a new facility permission, "IRR.RADMIN.LISTUSER". <For guideline examples, see the Chapter 2, "Deploying the IdF Advanced Adapter for ACF2," and Chapter 2, "Deploying the IdF Advanced Adapter for ACF2" for moe information. Voyager also requires an additional ACF2 permissions.

Voyager Uses Control File Similar to Pioneer

Voyager now uses a control file, which is similar to Pioneer. All parameters are passed via the control file.

Voyager Supports New Parameter for Control File

Voyager has a new parameter for the control file, "FILTER=YES/NO". The new parameter permits filtering of ACF2 events being read from the subpool. See Chapter 2, "Deploying the IdF Advanced Adapter for ACF2" for more information.

Software Updates in Release 9.0.4.15

The following are the software updates in release 9.0.4.15:

- Support for Initial Reconciliation Via Scheduled Task
- New Subpool Record Size for Voyager from 20 bytes to 100 bytes
- New Searches Initiated from LDAP and Submitted from Pioneer All in Rexx and Output Being Send Back to LDAP
- Enhanced Message Control (Suppression) in Both Pioneer and Voyager
- Pioneer Passes Parameters Via Control File
- Pioneer Performs Post-Processing on ACF2 Commands Initiated Through the LDAP Gateway (INSERT, CHANGE, and DELETE)
- Resolved Issues in Release 9.0.4.15

Support for Initial Reconciliation Via Scheduled Task

From this release onward, initial reconciliation is no longer performed using the acf2-initial-recon-adapter deployment. Instead, initial reconciliation is supported via the ACF2 Reconcile All Users scheduled task. See Section 4.3.2, "Full Reconciliation" for details about this scheduled task.

New Subpool Record Size for Voyager from 20 bytes to 100 bytes

In this release of the connector, auditing data to the subpool has been included. The data consists the details about who made the change to the user, the user affected by the change, timestamp, IP address, and ACF2 command issued.

New Searches Initiated from LDAP and Submitted from Pioneer All in Rexx and Output Being Send Back to LDAP

This feature gives the ability to search all users, which allows the use of the scheduled tasks.

Enhanced Message Control (Suppression) in Both Pioneer and Voyager

If DEBUG=N, then unnecessary output is removed to the log. If DEBUG=Y, then full messages will flow to SYSOUT and z/OS master console. See Chapter 2, "Deploying the IdF Advanced Adapter for ACF2," for more information.

Pioneer Passes Parameters Via Control File

This feature provides the STC parameters for Pioneer. See Chapter 2, "Deploying the IdF Advanced Adapter for ACF2" for more information.

Pioneer Performs Post-Processing on ACF2 Commands Initiated Through the LDAP Gateway (INSERT, CHANGE, and DELETE)

This feature enables Pioneer for post processing. See Chapter 2, "Deploying the IdF Advanced Adapter for ACF2" for more information.

Resolved Issues in Release 9.0.4.15

The following table lists issues resolved in release 9.0.4.15:

Bug Number	Issue	Resolution
5566654	Hardcoded and uppercase string when provisioning ACF2 resource	This issue has been resolved. There are no hardcoded and uppercase string when provisioning ACF2 resource in this release.
6800001	Active_Date is not a data type in the process form	This issue has been resolved. Active_Date is now a data type in the process form.
6846000	Too many unnecessary reconciliation events	This issue has been resolved. ignoreEvent() is used to avoid some of the reconciliation events in this release.
7201072	Multiple alias user catalogs	This issue has been resolved by running Pioneer on each LPAR.

Bug Number	Issue	Resolution
10378079	Oracle Identity Manager Voyager task does not prefix two (2) messages with message prefix for automation	This issue has been resolved. The correct prefix and date/time to missing automation messages have been added in this release.
11659466	ACF2 9.0.4.14 FAILS - IDMP200E	This issue has been resolved. The connector guide has been updated for Mainframe configurations.
11924937	UID string information is not being parsed and/or sent down to Open Systems component	This issue has been resolved. UID string information is now being parsed and/or sent down to Open Systems component.
12367608	The 9.0.4.14 version of the CA ACF2 Advanced connector cannot be installed without certain intervention in the installation kit	This issue has been resolved. A new installation kit has been included that no longer causes an installation error.

Software Updates in Release 9.0.4.14

The following are the software updates in release 9.0.4.14:

- Support for New Script for Oracle Identity Manager 11g Release (11.1.1)
- Support for CICS Login ID Record Attributes

Support for New Script for Oracle Identity Manager 11g Release (11.1.1)

From this release onward, new script and lib directories are provided for Oracle Identity Manager 11*g* release 1 (11.1.1) to enable jar and property files to be picked up directly from this new location. See Section 3.1, "Files and Directories that Comprise the Connector" for usage instructions.

Support for CICS Login ID Record Attributes

From this release onward, all CICS-related login ID record attributes are supported by the provisioning agent. The list of functions supported by the provisioning agent has been updated in the Section 1.5.2, "Supported Functions for Provisioning".

Software Updates in Release 9.0.4.13

The following are the software updates in release 9.0.4.13:

- Support for New Oracle Identity Manager Release
- Support for Request-Based Provisioning

Support for New Oracle Identity Manager Release

From this release onward, the connector can be installed and used on Oracle Identity Manager 11*g* release 1 (11.1.1). Where applicable, instructions specific to this Oracle Identity Manager release have been added in the guide.

See Section 1.1, "Certified Components" for the full list of certified Oracle Identity Manager releases.

Support for Request-Based Provisioning

From this release onward, the connector provides support for request-based provisioning on Oracle Identity Manager 11*g* release 1 (11.1.1).

See Section 4.5.1.2, "Request-Based Provisioning" for more information.

Software Updates in Release 9.0.4.12

The following are issues resolved in release 9.0.4.12:

Bug Number	Issue	Resolution
7282209	During reconciliation, if the value of the Name attribute fetched from the target system did not match the format specified in the nameFormat property in the acf2.properties file, then the Index Out Of Range error was encountered.	This issue has been resolved. If the format of the Name attribute does not match the specified format, then a message is recorded in the log file.
7375999	If the file system did not have sufficient disk space, then the LDAP Gateway threw an error when you tried to start it up.	To resolve this issue, ensure that there is sufficient disk space and then retry starting the LDAP Gateway.
7478625	During initial (full) reconciliation, an error was encountered when the record of a user with no privileges was processed.	This issue has been resolved. Records of users with no privileges are correctly processed.
9005394	Users' passwords were stored in clear text in reconciliation events created during a target resource reconciliation run.	This issue has been resolved. Passwords are not stored in reconciliation events created during a target resource reconciliation run.
9921954	When a user logs in to Oracle Identity Manager and changes the password, the Update Password operation is triggered on the target system. However, this operation fails on the target system.	This issue has been resolved. The Update Password operation is successfully completed on the target system.

Software Updates in Release 9.0.4.11

The following are software updates in release 9.0.4.11:

- Support for a New Version of the Target System
- Resolved Issues in Release 9.0.4.11

Support for a New Version of the Target System

CA ACF2 r14 has been added to the list of supported target system versions. See Section 1.1, "Certified Components" for the full list of certified target system versions.

Resolved Issues in Release 9.0.4.11

The following are issues resolved in release 9.0.4.11:

Bug Number	Issue	Resolution
6802885	Provisioning a user using MODEL made data related to that user inconsistent in the target system and Oracle Identity Manager.	This issue has been resolved. Provisioning using MODEL is not supported anymore.
7189194	Some of the comments in the run.sh file were not correct.	This issue has been resolved.

Bug Number	Issue	Resolution
7209124	Reconciliation of the Revoke User operation did not work.	This issue has been resolved. Reconciliation of the Revoke User operation now works as expected.
9176318	During reconciliation, StringIndexOutOfBoundsException was encountered if user profile data contained reserved CA ACF2 keywords. Reconciliation events were not created for such user profiles.	This issue has been resolved. A reconciliation event is created for a user profile even if any of the user profile attributes contain reserved keywords.
9317037	The following issue was observed on Oracle Identity Manager installed on Oracle3 WebLogic Server 10.3.0: When Oracle Identity Manager was upgraded from release 9.1.0 to 9.1.0.1 or 9.1.0.2 with JDK upgrade to jre1.6_16, the LDAP Gateway stopped responding and had to be restarted.	This issue has been resolved.

Software Updates in Releases 9.0.4.1 Through 9.0.4.4

The following are software updates in releases 9.0.4.1 through 9.0.4.4:

- CA ACF2 user profile, group profile, and data set and resource profile commands supported by the Provisioning Agent have been added in "Functionality Supported by the Pioneer Provisioning Agent" on page 1-6.
- The list of functions supported by the Provisioning Agent has been updated in "Supported Functions for Provisioning" on page 1-9.
- The commands supported by the Reconciliation Agent have been added in "Functionality Supported by the Voyager Reconciliation Agent" on page 1-7.
- The list of functions supported by the Reconciliation Agent has been updated in "Functionality Supported for Reconciliation" on page 1-7.
- The list of fields reconciled between CA ACF2 and Oracle Identity Manager has been updated in "User Attributes for Target Resource Reconciliation and Provisioning" on page 1-10.
- The IT resource parameters and their corresponding descriptions and sample values have been updated in "Importing the Connector XML File" on page 2-6.
- The procedure to configure the connector for multiple installations of the target system has been added in "Configuring the Connector for Multiple Installations of the Target System" on page 2-11.
- Information about reconciliation based on user status has been added in "Configuring Account Status Reconciliation" on page 4-4.
- The steps to add a new field for provisioning have been added in "Adding New Fields for Provisioning" on page 4-4.
- Known issues related to the following bugs have been added in Chapter 7, "Known Issues":
  - Bug 6668844
  - Bug 6904041
  - Bug 7189194
  - Bug 7033009

Documentation-Specific Updates

The following sections discuss documentation-specific updates:

- Documentation-Specific Updates in Release 9.0.4.21
- Documentation-Specific Updates in Release 9.0.4.20
- Documentation-Specific Updates in Release 9.0.4.19
- Documentation-Specific Updates in Release 9.0.4.18
- Documentation-Specific Updates in Release 9.0.4.17
- Documentation-Specific Updates in Release 9.0.4.16
- Documentation-Specific Updates in Release 9.0.4.15
- Documentation-Specific Updates in Release 9.0.4.14
- Documentation-Specific Updates in Release 9.0.4.13
- Documentation-Specific Updates in Release 9.0.4.12
- Documentation-Specific Updates in Release 9.0.4.11
- Documentation-Specific Updates in Releases 9.0.4.1 Through 9.0.4.4

Documentation-Specific Updates in Release 9.0.4.21

The following documentation-specific updates have been made in revision "17" of release 9.0.4.21:

- Section 2.1, "IDF Mainframe Adapters Functional Characteristics" has been added.
- Information about setting the 'SECURITY SERVER' to disabled state has been added to the "Note" in Section 2.3.8, "Adding Pioneer/Voyager to the Resource Rule Facilities (BPX and IRR)".
- The entire Section 3.6.2, "Enabling Logging" has been modified to include updated content regarding log levels and loggers.
- Table 6–1, " Troubleshooting Tips" has been updated to include the solution when The PIONEER STC fails.
- Table 6–1, " Troubleshooting Tips" has been updated to include the solution when CA-ACF2 connector requires RACF API to make calls to R_ADMIN.
- The sample value of "IPAD" row of Table F–1, " Voyager Control File Parameters" has been updated.
- Appendix G, "Mainframe Language Environment Runtime Options" has been added.

Documentation-Specific Updates in Release 9.0.4.20

The following documentation-specific update has been made in revision "16" of this guide:

The "Target System" row of Table 1–1, " Certified Components" has been updated to include r15.

The following documentation-specific updates have been made in the earlier revision of release 9.0.4.20:

- Section 2.3.6, "Loading and Activating the Exits" has been updated for new screenshot.

- From this release onward, "Connector Deployment on the Mainframe" chapter has been removed.
- The PDS IDF.JCLLIB member "IEBCOPYP" has been removed from the members list and information on "YOURHLQ" has been updated. See Section 2.3.4, "Editing the Mainframe Batch Job Files to Match the Settings for the Customer's Site."
- Chapter 6, "Troubleshooting" has been updated with new troubleshooting tips.
- Table 6–2, " Three Options Settings and their Effects" has been added for the three options settings and their effects.
- Appendix C, "Provisioning Agent (Startup) Messages has been removed from the connector guide.
- Table F–2, " Pioneer Control File Parameters" has been updated with new parameters.

Documentation-Specific Updates in Release 9.0.4.19

The following are the documentation-specific updates in this release:

- Table 3–2, " IT Resource Parameters" has been updated with new parameter.
- Table 3–4, " Properties in the acf2.properties File" has been updated with new parameter.
- Section 4.3.3.2, "ACF2 Reconcile Deleted Users" has been updated for information on deleted user reconciliation to Oracle Identity Manager.

Documentation-Specific Updates in Release 9.0.4.18

The following is a documentation-specific update in this release:

Table 3–4 has been updated with new parameters.

Documentation-Specific Updates in Release 9.0.4.17

The following are the documentation-specific updates in this release:

- In the entire guide, acf2Connection.properties has been changed to VOYAGER_ID.properties.
- Parmfle Parameters has been added. See Chapter 2, "Deploying the IdF Advanced Adapter for ACF2,"
- Pioneer 'DD's (Data Definition statements) has been added. See Chapter 2, "Deploying the IdF Advanced Adapter for ACF2"
- A note on lost message recovery has been added. See Chapter 2, "Deploying the IdF Advanced Adapter for ACF2"
- Procedure for Pioneer STC has been updated, and procedure for Pioneer reconciliation search flow has been added. See Chapter 2, "Deploying the IdF Advanced Adapter for ACF2"
- Procedure for Integrating exits has been added. See Chapter 2, "Deploying the IdF Advanced Adapter for ACF2"
- Section 5.1, "Adding New Attributes for Target Resource Reconciliation" has been modified for the information on reconAttrs property and full reconciliation.
- Section 5.3, "Removing Attributes Mapped for Target Resource Reconciliation and Provisioning" has been updated for the information on reconAttrs property and its attributes.

Documentation-Specific Updates in Release 9.0.4.16

The following are the documentation-specific updates in this release:

Configuring Scheduled Tasks for Resource/Access Keys on the Target System for Reconciliation

A new section is added in Chapter 4, which provides details about configuring FindAllAccessRules and FindAllResourceRules scheduled tasks populate lookup tables with resource or access rule keys that can be assigned during user provisioning. See Section 4.2, "Scheduled Tasks for Lookup Field Synchronization" and Section 4.5, "Configuring Scheduled Tasks" for more details.

Configuring SSL in the LDAP Gateway

A new step (8) has been added in the Section 3.9, "Installing and Configuring the LDAP Gateway" providing information about the configurations for setting up SSL in the LDAP Gateway.

New Attribute Name

Data Set Resource Profile name has been changed to Resource Rule Attributes in this release. See Section 1.5.2, "Supported Functions for Provisioning" and Section 1.5.3.1, "Resource Rule Attributes for Target Resource Reconciliation and Provisioning" for details.

Access Rule Attribute Mappings

A new section providing information about Access Rule attribute mappings has been added in this release. See Section 1.5.3.2, "Access Rule Attributes for Target Resource Reconciliation and Provisioning" for details.

Documentation-Specific Updates in Release 9.0.4.15

There are no documentation-specific updates in release 9.0.4.15.

Documentation-Specific Updates in Release 9.0.4.14

There are no documentation-specific updates in release 9.0.4.14.

Documentation-Specific Updates in Release 9.0.4.13

There are no documentation-specific updates in this release.

Documentation-Specific Updates in Release 9.0.4.12

There are no documentation-specific updates in this release.

Documentation-Specific Updates in Release 9.0.4.11

Major changes have been made in the structure of the guide.

Documentation-Specific Updates in Releases 9.0.4.1 Through 9.0.4.4

- The user profile field mappings and resource profile field mappings between Oracle Identity Manager and the target system have been added in "User Attributes for Target Resource Reconciliation and Provisioning" on page 1-10. "Appendix A: Attribute Mapping Between CA ACF2 and Oracle Identity Manager" has been removed.
- The components of the CA ACF2 Advanced connector and the connector architecture for reconciliation and provisioning have been added in "Connector

Architecture" on page 1-3. "Appendix B: Connector Architecture" has been removed.

- Guidelines that were earlier documented in Chapter 7, "Known Issues" have been moved to "Guidelines on Using the Connector" on page 5-2.
- In "Certified Languages" on page 1-2, Arabic has been added to the list of languages that the connector supports.
- In "Certified Components" on page 1-2, major changes have been made in the "Target System" row. Information about certified deployment configurations has been removed from "Reviewing Deployment Requirements" on page 3-2.
- 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 "Certified Components" on page 1-2, the minimum Oracle Identity Manager release has been changed to 9.1.0.1 and the JDK requirement of release 1.5 or later has been added.

1

About the Connector

Oracle Identity Manager automates access rights management, security, and provisioning of IT resources. Oracle Identity Manager connectors are used to integrate Oracle Identity Manager with external, identity-aware applications. This guide discusses the connector that enables you to use CA ACF2 either as a managed (target) resource or as an authoritative (trusted) source of identity data for Oracle Identity Manager.

The advanced connector for CA ACF2 provides a native interface between Oracle Identity Manager and CA ACF2 installed on an IBM z/OS mainframe. The connector functions as a trusted virtual administrator on the target system, performing tasks related to creating and managing user profiles.

In the account management (target resource) mode of the connector, information about users created or modified directly on the target system can be reconciled into Oracle Identity Manager. In addition, you can use Oracle Identity Manager to perform provisioning operations on the target system.

In the identity reconciliation (trusted source) configuration of the connector, users are created or modified only on the target system and information about these users is reconciled into Oracle Identity Manager.

If you configure CA ACF2 as a target resource, then user profiles on CA ACF2 correspond to accounts or resources assigned to OIM Users. In contrast, if you configure CA ACF2 as a trusted source, then user profiles on CA ACF2 correspond to OIM Users.

This chapter is divided into the following sections:

- Section 1.1, "Certified Components"
- Section 1.2, "Certified Languages"
- Section 1.3, "Connector Architecture"
- Section 1.4, "Features of the Connector"
- Section 1.5, "Connector Objects Used During Reconciliation and Provisioning"

1.1 Certified Components

Table 1–1 lists the certified components.

Table 1–1 Certified Components

Item	Requirement
Oracle Identity Manager	■ Oracle Identity Manager Release 9.1.0.1 or later **Note:** In this guide, **Oracle Identity Manager Release 9.1.0.*x*** has been used to denote Oracle Identity Manager Release 9.1.0.1 and future releases in the 9.1.0.*x* series that the connector will support. ■ Oracle Identity Manager 11*g* Release 1 (11.1.1) or later **Note:** In this guide, **Oracle Identity Manager Release 11.1.1** has been used to denote Oracle Identity Manager 11*g* Release 1 (11.1.1).
Target system	CA ACF2 r6.2, r8.0 SP4 or later, r9.0 SP1 or later, r12, r14, r15
JDK	The JDK version can be one of the following: ■ For Oracle Identity Manager Release 9.1.0.*x*, use JDK 1.5 or later. ■ For Oracle Identity Manager Release 11.1.1, use JDK 1.6 update 18 or later.
Infrastructure Requirements: Message transport layer between the Oracle Identity Manager and the mainframe environment	TCP/IP with Advanced Encryption Standard (AES) encryption

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

See Also: On Oracle Identity Manager Release 9.1.0.*x*, see *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

On Oracle Identity Manager Release 11.1.1, see *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

1.3 Connector Architecture

The connector architecture is described in the following sections:

- Section 1.3.1, "Connector Components"

- Section 1.3.2, "Connector Operations"

1.3.1 Connector Components

The CA ACF2 Advanced connector contains 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 converted into native commands for CA ACF2, encrypted using AES-128 encryption, and then sent to the Provisioning Agent. The response, which is also native to CA ACF2, is parsed into an LDAP-format response and returned to Oracle Identity Manager.

  During reconciliation, the LDAP Gateway receives event notification, converts the events to LDAP format, and then forwards them to Oracle Identity Manager.

- **Provisioning Agent (Pioneer):** The Provisioning Agent, running as an IBM z/OS STC (Started Task), is a mainframe component. It receives native mainframe CA ACF2 provisioning commands from the LDAP Gateway. These requests are decrypted, converted from ASCII to EBCDIC, passed to CA ACF2 through the standard RACF Sub System Interface API, and then posted to the CA ACF2 database. The response is parsed and returned to the LDAP Gateway.

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

- **Reconciliation Agent (Voyager):** The Reconciliation Agent captures mainframe events by using exits, which are programs run after events in CA ACF2 are processed. These events include the ones generated at the TSO logins, the command prompt, batch jobs, and other native events. The Reconciliation Agent captures these events, transforms them into notification messages, and then sends them to Oracle Identity Manager through the LDAP Gateway.

  Note: At some places in this guide, the Reconciliation Agent is referred to as **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 is supported by the connector.

1.3.2 Connector Operations

This section provides an overview of the following processes:

- Section 1.3.2.1, "Full Reconciliation Process"
- Section 1.3.2.2, "Incremental (Real-Time) Reconciliation Process"
- Section 1.3.2.3, "Provisioning Process"

1.3.2.1 Full Reconciliation Process

Full reconciliation involves fetching all existing user profile data from the mainframe to Oracle Identity Manager. If you configure the target system as a target resource,

then this user profile data is converted into accounts or resources for OIM Users. If you configure the target system as a trusted source, then the user profile data is used to create OIM Users.

The following is a summary of the full reconciliation process:

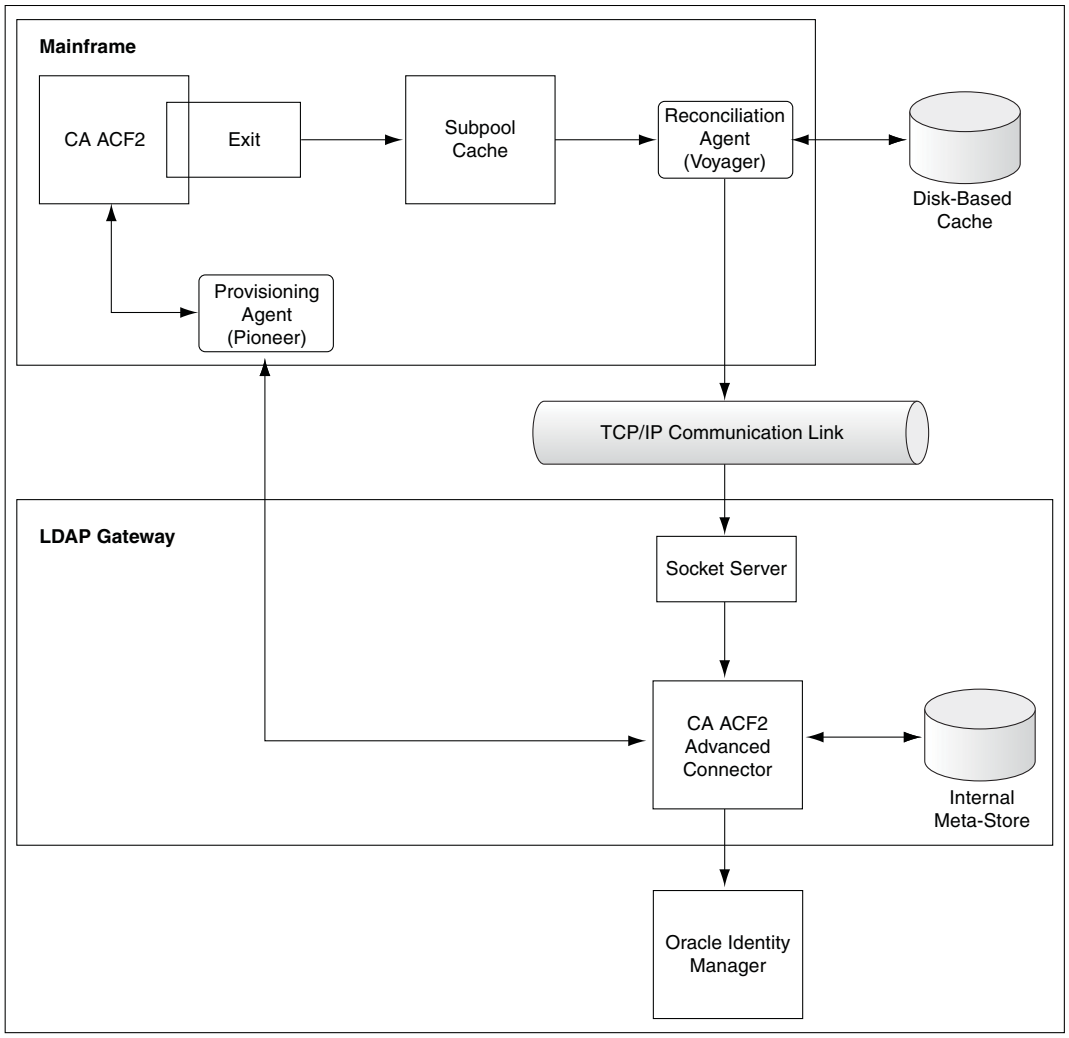
Note: Detailed instructions are provided later in this guide.

1. You specify the full reconciliation configuration in the ACF2 Reconcile All Users scheduled task.
2. In the scheduled task form UsersList property, you enter a list of user IDs of the user profiles that you want to reconcile. If no users are specified, then all existing users on the target system will be reconciled.
3. You specify whether you want to configure ACF2 as a target resource or trusted source of Oracle Identity Manager.
4. You set a start time for the task and run the scheduled task. The task sends the list of user IDs to the LDAP Gateway.
5. The LDAP Gateway encrypts the list of user IDs and then sends it to the Provisioning Agent on the mainframe.
6. You run the scheduled task. The task sends a search request to the LDAP Gateway.
7. The LDAP Gateway encrypts the search request and then sends it to the Provisioning Agent on the mainframe.
8. The Provisioning Agent encrypts the user profile data received from ACF2 and then passes this data to the LDAP Gateway.
9. The LDAP Gateway decrypts the user profile data and passes it to Oracle Identity Manager.
10. The next step depends on the setting in the scheduled task:
    - If you configure the target system as a target resource, then this user profile data is converted into accounts or resources for OIM Users.
    - If you configure the target system as a trusted source, then the user profile data is used to create OIM Users.

1.3.2.2 Incremental (Real-Time) Reconciliation Process

Incremental or real-time reconciliation is initiated by one of the exits that work in conjunction with the Reconciliation Agent. Figure 1–1 shows the flow of data during this form of reconciliation.

Figure 1–1 Incremental Reconciliation Process



This figure shows the incremental or real-time reconciliation process of the connector. The description of the process is given in the same section.

****

The following is a summary of the incremental or real-time reconciliation process:

1. Incremental reconciliation begins when a user is created, updated, or deleted on CA ACF2. This event might take place either directly on the mainframe or in response to a provisioning operation on Oracle Identity Manager.
2. The Reconciliation Agent gathers data captured by one of three CA ACF2 exits: LIDPOST, NEWPXIT, or EXPPXIT. The exit detects the event and sends a message containing user data to Subpool 231 (cache). This message contains the minimum number of data items, such as the user ID and password, required to reconcile the event.
3. The Reconciliation Agent polls Subpool 231. When it finds a message in the subpool, it reads the message into its buffer. This frees up the subpool entry.
4. The Reconciliation Agent opens up a connection with the LDAP Gateway, and then sends the message to the gateway over TCP/IP.

Note: Messages sent to the LDAP Gateway are encrypted using AES-128 encryption.

5. The LDAP Gateway decrypts the message, if it is a Create User or Change User event, or if the STC ID matches the Pioneer STC it will ignore events and not send them to Oracle Identity Manager.

   If the event does not meet conditions, then the LDAP Gateway determines that the source of the event is not Oracle Identity Manager. The gateway then sends the message to Oracle Identity Manager.

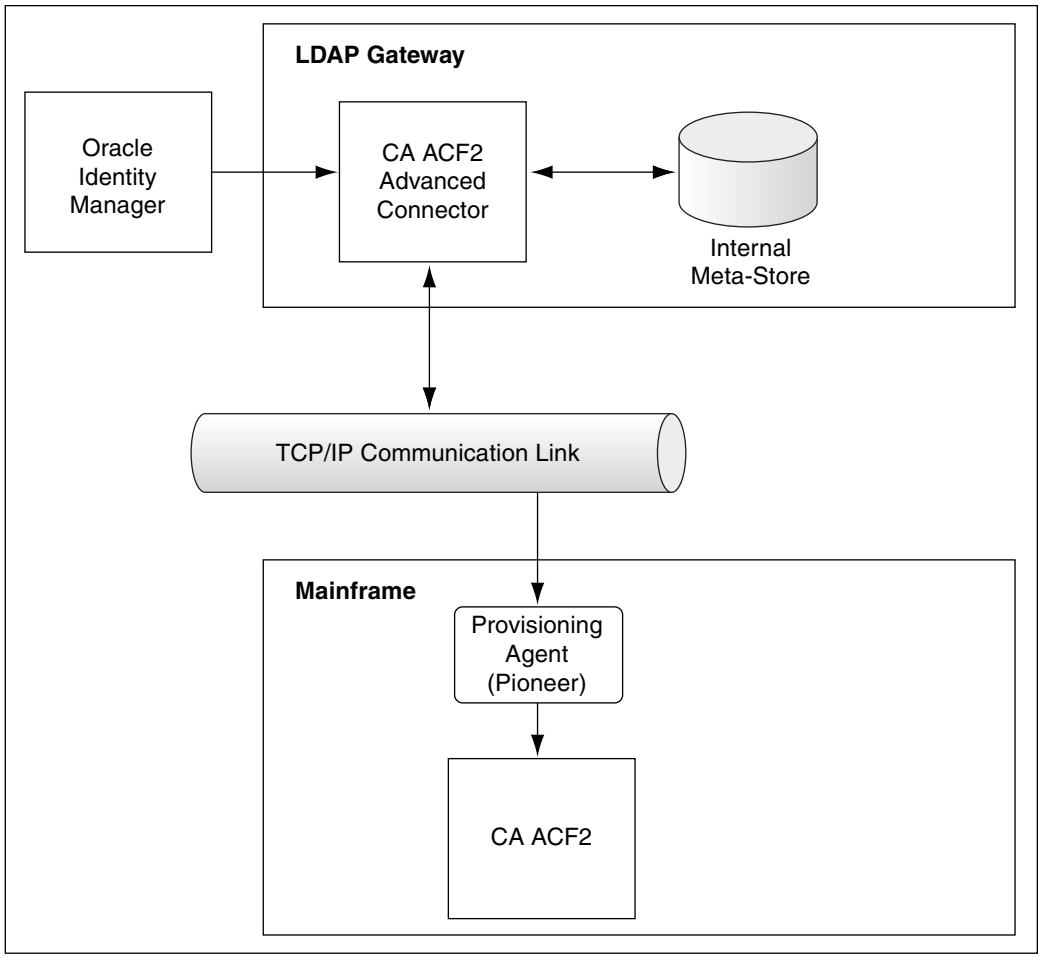
   Note: As mentioned in Step 2, the message sent by the Reconciliation Agent contains only a minimum amount of data. The LDAP Gateway sends a request to the Provisioning Agent to fetch the remaining user data from the target system.

6. Oracle Identity Manager processes the message and creates or updates either the corresponding CA ACF2 resource or the OIM User.

1.3.2.3 Provisioning Process

Figure 1–2 shows the flow of data during provisioning.

Figure 1–2 Provisioning Process



This figure shows the provisioning process of the connector. The description of the process is given in the same section.

****

The following is a summary of the provisioning process:

1. Provisioning data is sent from Oracle Identity Manager to the LDAP Gateway.
2. The LDAP Gateway converts the provisioning data into mainframe commands, encrypts the commands, and then sends them to the mainframe over TCP/IP.
3. The Provisioning Agent installed on the mainframe decrypts the commands and then runs them on the mainframe.
4. The Provisioning Agent sends the output of the commands back to the LDAP Gateway.
5. The outcome of the operation on the mainframe is displayed on the Oracle Identity Manager console. A more detailed message is recorded in the connector log file.

1.4 Features of the Connector

The following are features of the connector:

- Section 1.4.1, "Target Resource and Trusted Source Reconciliation"
- Section 1.4.2, "Full and Incremental Reconciliation"
- Section 1.4.3, "Encrypted Communication Between the Target System and Oracle Identity Manager"
- Section 1.4.4, "High Availability Feature of the Connector"

1.4.1 Target Resource and Trusted Source Reconciliation

You can use the connector to configure CA ACF2 as either a target resource or trusted source of Oracle Identity Manager.

1.4.2 Full and Incremental Reconciliation

After you deploy the connector, you perform full reconciliation to bring all existing user data from the target system to Oracle Identity Manager. After the first full reconciliation run, change-based or incremental reconciliation is automatically enabled and active. Incremental reconciliation is a real-time process. User changes on the target system are directly sent to Oracle Identity Manager.

You can perform a full reconciliation run at any time.

1.4.3 Encrypted Communication Between the Target System and Oracle Identity Manager

AES-128 encryption is used to encrypt data that is exchanged between the LDAP Gateway and the Reconciliation Agent and Provisioning Agent on the mainframe.

1.4.4 High Availability Feature of the Connector

The following are component-failure scenarios and the response of the connector to each scenario:

- **Scenario 1: The Reconciliation Agent is running and the LDAP Gateway stops responding**

  1. The Reconciliation Agent stops sending messages (event data) to the LDAP Gateway.
  2. Messages that are not sent are stored in the subpool cache.

     Note: The subpool cache cannot grow beyond the allocated limit. If the LDAP Gateway does not start responding before the allocated limit is reached, then new messages that come in are lost.

  3. When the LDAP Gateway is brought back online, the Reconciliation Agent reads data from the subpool cache and then sends messages to the LDAP Gateway.

- **Scenario 2: The LDAP Gateway is running and the Reconciliation Agent stops responding**

  1. Event data is sent to the subpool cache.
  2. When the Reconciliation Agent is brought back online, it reads data from the subpool cache and then sends messages to the LDAP Gateway.

- **Scenario 3: The LDAP Gateway is running and the mainframe stops responding**
  1. Messages that are in the subpool cache are written to disk.
  2. When the mainframe is brought back online, event data written to disk is again stored in the subpool cache.
  3. The Reconciliation Agent reads data from the subpool cache and then sends messages to the LDAP Gateway.
- **Scenario 4: The LDAP Gateway is running and the Provisioning Agent or mainframe stops responding**

  The process task that sends provisioning data to the LDAP Gateway retries the task.
- **Scenario 5: The subpool is stopped by an administrator**

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

1.5 Connector Objects Used During Reconciliation and Provisioning

The following sections provide information about connector objects used during reconciliation and provisioning:

- Section 1.5.1, "Supported Functions for Reconciliation"
- Section 1.5.2, "Supported Functions for Provisioning"
- Section 1.5.3, "User Attributes for Target Resource Reconciliation and Provisioning"
- Section 1.5.4, "User Attributes for Trusted Source Reconciliation"
- Section 1.5.5, "Reconciliation Rule"
- Section 1.5.6, "Reconciliation Action Rules"

1.5.1 Supported Functions for Reconciliation

The connector supports reconciliation of user profile data from the following events:

- Create user
- Modify user
- Change password
- Reset password
- Reset password no expire
- Disable user
- Delete user
- Enable user

1.5.2 Supported Functions for Provisioning

Table 1–2 lists the provisioning functions supported by the connector.

Table 1–2 Supported Functions for Provisioning

Function	Description	Mainframe Command
Create user	Adds new login ID record on CA ACF2	INSERT
Modify user	Modifies login ID record information on CA ACF2	CHANGE
Change password	Changes user password on CA ACF2 in response to password changes made on Oracle Identity Manager through user self-service.	CHANGE
Reset password	Resets user password on CA ACF2 The passwords are reset by the administrator.	CHANGE
Disable user	Disables user on CA ACF2	CHANGE
Enable user	Enables user on CA ACF2	CHANGE
Delete user	Removes user from CA ACF2	DELETE
Grant user access to rule	Creates a CA ACF2 resource or access rule for the CA ACF2 user	SET RULE
Grant user access to privileges (TSO)	Provides user access to CA ACF2 security fields (including custom fields)	CHANGE
Grant user access to privileges (CICS)	Provides user access to CA ACF2 CICS login ID record fields	CHANGE

1.5.3 User Attributes for Target Resource Reconciliation and Provisioning

Table 1–3 lists attribute mappings between CA ACF2 and Oracle Identity Manager for target resource reconciliation and provisioning. The OnBoardAcf2User and ModifyAcf2User adapters are used for the Create User and Modify User provisioning operations, respectively.

Table 1–3 User Attributes for Target Resource Reconciliation and Provisioning

Process Form Field	CA ACF2 Attribute	Description
accessCnt	ACC-CNT	Count of number of times the user accessed the system
accessDate	ACC-DATE	Date when the user last accessed the system
activeDate	ACTIVE	Privilege to allow or deny access based on a date
accessSrce	ACC-SRCE	System component accessed by the user
accessTime	ACC-TIME	Time when the user last accessed the system
cn	NAME	Full name of the user You can specify the format in which Full Name values are stored on the target system. Step 3 of Section 3.9, "Installing and Configuring the LDAP Gateway" describes the procedure.
sn	NAME	Last name of the user
expire	EXPIRE	Privilege to allow or deny access based on a date
givenName	NAME	First name of the user
defaultGroup	GROUP	Default group for the user
cicsid	CICSID	Indicates the CICS operator ID (3 characters)
cicsPri	CICSPRI	Indicates the CICS operator priority (1-byte binary)

Table 1–3 (Cont.) User Attributes for Target Resource Reconciliation and Provisioning

Process Form Field	CA ACF2 Attribute	Description
cicsIdle	IDLE	Maximum number of minutes permitted between terminal transactions for this user (1-byte binary)
cicsCl	CICSCL	Indicates the CICS operator class (3 hexadecimal bytes)
cicsRsl	CICSRLS	Indicates the CICS resource access key (3 hexadecimal bytes)
cicsOpt	CICSOPT	Specifies the SYSID of the C-CIC records to use at initialization time (8-characters)
cicsAcf2Cics	ACF2CICS	ACF2CICS or NOACF2CICS Indicates that CA ACF2 CICS security is to be initialized in any CTS 1.2 or later region running with this address space logonid (bit field)
kerbVio	KERB-VIO	Number of Kerberos key violations
kerbCurv	KERBCURV	Kerberos key version
minDays	MINDAYS	Minimum number of days that must elapse before a user can change the password 0 indicates no limit.
maxDays	MAXDAYS	Maximum number of days (based on the date specified in the PSWD-TOD field) that the user is permitted to change password before the password expires 0 indicates no limit.
passwordExpire	PSWD-EXP | NOPSWD-EXP	Indicates that a user's password has been manually expired This field lets a security administrator force this user to change the password.
privileges	SECURITY fields	Privileges assigned to the user **Note:** This is a multivalued attribute. All standard SECURITY fields are mapped by default. You can also map custom fields.
prefix	PREFIX	0- to 8-character key of the rule used to validate access to a data set.
pswdDate	PSWD-DAT	Date of last invalid password attempt The date is displayed in the `mm/dd/yy`, `dd/mm/yy`, or `yy/mm/dd` formats depending on the DATE field of the GSO OPTS record. Year designations of 70-99 assume a date in the 20th century (1970-1999). Year designations of 00-69 assume a date in the 21st century (2000-2069). **Note:** See the target system documentation for detailed information about GSO.
pswdInv	PWSD-INV	Number of password violations that occurred since the last successful logon This field can be reset to 0 by a security administrator.
pswdTod	PWSD-TOD	Date and time when a user changed the password The date is displayed in the `mm/dd/yy`, `dd/mm/yy`, or `yy/mm/dd` formats depending on the DATE field of the GSO OPTS record. You cannot set this field. CA ACF2 maintains and displays it. Year designations of 70-99 assume a date in the twentieth century (1970-1999). Year designations of 00-69 assume a date in the 21st century (2000-2069).
pswdVio	PWSD-VIO	Number of password violations that occurred on PSWD-DAT
revoke	NA	Value is `Y` if user is revoked or `N` if user is resumed

Table 1–3 (Cont.) User Attributes for Target Resource Reconciliation and Provisioning

Process Form Field	CA ACF2 Attribute	Description
secVio	SEC-VIO	Indicates the number of cumulative security violations for a user
tsoDest	DFT-DEST	Default SYSOUT destination
tsoDftPfx	DFT-PFX	0- to 8-character default TSO prefix that is set in the user's profile at logon time
tsoUnit	TSOUNIT	Default UNIT name for allocations.
tsoRba	TSORBA	Mail Index Record Pointer (MIRP) for the user
tsoAcctnum	TSOACCT	Default TSO account number on the TSO/E logon panel
tsoHoldclass	DFT-SUBH	Default hold class
tsoSubmitclass	DFT-SUBC	Default submit class
tsoMaxSize	TSOSIZE	Maximum region size the user can request at logon
tsoMsgclass	DFT-SUBM	Default message class
tsoProc	TSOPROC	Default login procedure on the TSO/E logon panel
tsoSize	TSORGN	Minimum region size if not requested at logon
tsoSysoutclass	DFT-SOUT	Default SYSOUT class
tsoPerf	TSOPERF	User's default TSO performance group
tsoMail	MAIL	Indicates that a user can receive mail messages from TSO at logon time
tsoAcctPriv	ACCTPRIV	Indicates that the user has TSO accounting privileges
tsoAllCmds	ALLCMDS	Indicates the ability to bypass the CA ACF2 restricted command lists by entering a special prefix character
tsoJcl	JCL	Indicates the ability to submit batch jobs from TSO and to use SUBMIT, STATUS, CANCEL, and OUTPUT commands
tsoWtp	WTP	Indicates that CA ACF2 displays write-to-programmer messages
tsoFscrn	TSOFSCRN	Indicates that a user can use the full-screen logon display
tsoMount	MOUNT	Indicates permission to issue mounts for devices
tsoOperator	OPERATOR	Indicates that a user has TSO operator privileges
tsoNotices	NOTICES	Indicates that a user can receive TSO notices at logon time
tsoPrompt	PROMPT	Indicates that CA ACF2 prompts a user if parameters are missing or incorrect
tsoLgnAcct	LGN-ACCT	Indicates the permission to specify an account number at logon time
tsoLgnMsg	LGN-MSG	Indicates that the user has permission to specify a message class at logon time
tsoLgnPerf	LGN-PERF	Indicates the permission to specify a performance group at logon time
tsoLgnProc	LGN-PROC	Indicates the permission to specify a TSO procedure name at logon time
tsoLgnTime	LGN-TIME	Indicates the permission to specify a TSO session time limit at logon time

Table 1–3 (Cont.) User Attributes for Target Resource Reconciliation and Provisioning

Process Form Field	CA ACF2 Attribute	Description
tsoLgnRcvr	LGN-RCVR	Indicates the permission to use the recover option of the TSO or TSO/E command package
tsoLgnSize	LGN-SIZE	Indicates that the user is authorized to specify a region size at logon time by overriding TSOSIZE
tsoLgnUnit	LGN-UNIT	Indicates the permission to specify a TSO unit name at logon time
tsoIntercom	INTERCOM	Indicates that the user is willing to accept messages from other users through the TSO SEND command
uid	USER	Login ID of the user
updTod	UPD-TOD	Indicates the date and time when a login ID record was last updated
userPassword	PASSWORD	Password

1.5.3.1 Resource Rule Attributes for Target Resource Reconciliation and Provisioning

Table 1–4 lists resource rule attribute mappings between CA ACF2 and Oracle Identity Manager. The AssignUserToResourceRule and RemoveUserFromResourceRule adapters are used for resource rule provisioning operations.

Table 1–4 Resource Rule Attribute Mappings

Child Form Field	CA ACF2 Attribute	Description
RULE KEY	KEY	The high-level index of the data set name for which this rule is being written
TYPE	TYPE	The type of resource rule
ACCESS	ACESS	System mode CA ACF2 should take when it validates access for this rule

1.5.3.2 Access Rule Attributes for Target Resource Reconciliation and Provisioning

Table 1–5 lists access rule attribute mappings between CA ACF2 and Oracle Identity Manager. The AssignUserToAccessRule and RemoveUserFromAccessRule adapters are used for access rule provisioning operations.

Table 1–5 Access Rule Attribute Mappings

Child Form Field	CA ACF2 Attribute	Description
DATASET ID	dsnmask	The name of the data set or a mask
RULE KEY	$KEY	The high-level index of the data set name for which this rule is being written, or the VSM key of the rule set.
ACCESS READ	Read	Specifies read access and the action CA ACF2 should take when the environment matches
ACCESS WRITE	Write	Specifies write access and the action CA ACF2 should take when the environment matches
ACCESS EXECUTE	Execute	Specifies execute access and the action CA ACF2 should take when the environment matches
ACCESS ALLOCATE	Allocate	Specifies allocate access and the action CA ACF2 should take when the environment matches

1.5.4 User Attributes for Trusted Source Reconciliation

Table 1–6 lists attribute mappings between CA ACF2 and Oracle Identity Manager for trusted source reconciliation.

Table 1–6 User Attributes for Trusted Source Reconciliation

OIM User Field	CA ACF2 Attribute	Description
uid	USER	Login ID of the user
cn	NAME	Full name of the user
sn	NAME	Last name of the user
givenName	NAME	First name of the user
userPassword	PASSWORD	Password

1.5.5 Reconciliation Rule

See Also: *Oracle Fusion Middleware User's Guide for Oracle Identity Manager* for generic information about reconciliation matching and action rules

During target resource reconciliation, Oracle Identity Manager tries to match each user profile fetched from CA ACF2 with existing CA ACF2 resources provisioned to OIM Users. This is known as process matching. A reconciliation rule is applied for process matching. If a process match is found, then changes made to the user profile on the target system are copied to the resource on Oracle Identity Manager. If no match is found, then Oracle Identity Manager tries to match the user profile against existing OIM Users. This is known as entity matching. The same reconciliation rule is applied during this process. If an entity match is found, then a CA ACF2 resource is provisioned to the OIM User. Data for the newly provisioned resource is copied from the user.

During trusted reconciliation, the same reconciliation rule is applied for entity matching. If an entity match is found, then an OIM User is created out of the data in the reconciliation event.

The following is the reconciliation rule for both target resource and trusted source reconciliation:

Rule name: IdfReconUserRule

Rule element: User Login Equals uid

In this rule element:

- User Login is the User ID field on the process form and the OIM User form.
- uid is the USER attribute on CA ACF2.

After you deploy the connector, you can view this reconciliation rule by performing the following steps:

1. On the Design Console, expand **Development Tools** and then double-click **Reconciliation Rules**.
2. Search for and open the **IdfReconUserRule** rule.

1.5.6 Reconciliation Action Rules

Reconciliation action rules specify actions that must be taken depending on whether or not matching CA ACF2 resources or OIM Users are found on Oracle Identity Manager when the reconciliation rule is applied. Table 1–7 lists the reconciliation action rules.

Table 1–7 Reconciliation Action Rules

Rule Condition	Action
No Matches Found	Assign to Administrator With Least Load
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

Note: No action is performed for rule conditions that are not predefined for this connector. You can define your own action rule for such rule conditions. See *Oracle Fusion Middleware User's Guide for Oracle Identity Manager* for information about modifying or creating reconciliation action rules.

After you deploy the connector, you can view the reconciliation action rules for target resource reconciliation by performing the following steps:

1. On the Design Console, expand **Resource Management** and then double-click **Resource Objects**.
2. Search for and open the **OIMAcf2ResourceObject** resource object.
3. Click the **Object Reconciliation** tab, and then click the **Reconciliation Action Rules** tab. The Reconciliation Action Rules tab displays the action rules defined for this connector.

2

Deploying the IdF Advanced Adapter for ACF2

The IdF Mainframe Adapter is composed of the following main components:

Pioneer: As discussed in one of the earlier chapters, Pioneer (also known as the Provisioning Agent) receives native mainframe identity and authorization change events from the LDAP Gateway. These events are processed against the mainframe authentication repository, in which all provisioning updates from the LDAP Gateway are stored. The response is parsed and returned to the LDAP Gateway.

Voyager: This component is also known as the Reconciliation Agent. The Voyager captures native mainframe events by using System Exits. The Voyager transforms these events into LDAPv3 protocol notification messages through the LDAP Gateway.

System Exits: These are programs that are run after system events in IBM RACF have been detected. System Exits capture these events in real time. They are events occurring from the TSO logins, the command prompt, batch jobs, and other native mainframe events.

Note: Before you install the mainframe components of the RACF Advanced Adapter on a Production environment, Oracle recommends that you install the product on a Test and/or Development environment for testing, prior to installing on a Production environment.

2.1 IDF Mainframe Adapters Functional Characteristics

Pioneer can post-process ACF2 commands initiated through the LDAP gateway (INSERT, CHANGE, and DELETE). The following topics provide more information on post-processing:

- Section 2.1.1, "Alias Post-Processing"
- Section 2.1.2, "Other Post-Processing"

2.1.1 Alias Post-Processing

The Alias processing is controlled by the usage of a Pioneer parameter in its control file. If the "POST_PROC_ALIAS" parameter is set to 'T' or true, then it enables post-processing. If set to 'F' or false, then it disables ALIAS post-processing.

2.1.2 Other Post-Processing

Post-processing is invoked by using an entry in the Pioneer control file to submit a z/OS JCL Stream to the internal reader for processing.

- C=function, m=member name, L=PDS Library name

  function can be INSERT, CHANGE, or DELETE

  ```
  Example1, C=INSERT,M=INSERT10,L=TEST.CNTL.LIB
  Example2, C=CHANGE,M=CHANGE33,L=TEST.CNTL.LIB
  Example3, C=DELETE,M=DELETE99,L=TEST.CNTL.LIB
  ```

  Example 1

  Pioneer dynamically allocates 'TEST.CNTL.LIB', member = INSERT10 and reads and punches it to the z/OS INTRDR. The ACF2 command for the INSERT also occurs. This process occurs for every INSERT.

  Example 2

  Pioneer dynamically allocates 'TEST.CNTL.LIB', member = CHANGE33 and reads and punches it to the z/OS INTRDR. The ACF2 command for the CHANGE also occurs. This process occurs for every CHANGE.

  Example 3

  Pioneer dynamically allocates 'TEST.CNTL.LIB', member = INSERT10 and reads and punches it to the z/OS INTRDR. The ACF2 command for the INSERT also occurs. This process occurs for every INSERT.

  If Pioneer finds no 'C=' commands in the control file, then post-processing does not occur.

  Pioneer does NOT check the result of the JCL Stream submitted to z/OS. Any actions performed by the submitted stream are independent of Pioneer processing.

- Utilize PIONEER ACF2 Control cards
  - POST_PROC_ALIAS=T
  - FILTER=NO

  Also, note that what this allows is for example A REXX script named M=INSERT10 to be executed for SYSTSIN &mbrname lid.

  You can also look at using COBOL, PL/I, ASSEMBER or other mainframe languages to process them.

- C=function, m=member name, L=PDS Library name

  Function can be INSERT, CHANGE, or DELETE

  ```
  Example1: C=INSERT,M=INSERT10,L=TEST.CNTL.LIB
  Example2: C=CHANGE,M=CHANGE33,L=TEST.CNTL.LIB
  Example3: C=DELETE,M=DELETE99,L=TEST.CNTL.LIB
  ```

  1. The M= is the PDS or PDSE member name and L= is the PDS or PDSE library dataset name.
  2. For example when C=INSERT is found, Pioneer dynamically allocates the library name in "L=" and its member name in "M=".
  3. Pioneer reads the PDS or PDSE member name and inserts a %mbrname and ACF2 LID into the read job stream, as shown in the following JLC example:

     ```
     //Yourjobn JOB ,SYSTEMS,CLASS=A,MSGCLASS=X,
     //           MSGLEVEL=(1,1),REGION=4096K,NOTIFY=&SYSUID
     //STEP1 EXEC PGM=IKJEFT01,DYNAMNBR=20
     //SYSEXEC DD DSN=yourhlq.CLIST.LIBRARY,DISP=SHR
     //SYSPRINT DD SYSOUT=*
     //SYSTSPRT DD SYSOUT=*
     ```

```
//SYSTSIN DD *
&mbrname lid
```

Note that this job stream is executed for every INSERT sent to Pioneer.

4. Pioneer submits the preceding job-stream to the internal reader for z/OS execution.
5. The PDS or PDSE is then "Freed".

2.2 Prerequisites

The prerequisites for installing the IdF Advanced adapter as follows:

- Section 2.2.1, "Message Transport Requirements"
- Section 2.2.2, "APF Authorization"

2.2.1 Message Transport Requirements

Between the LDAPv3 server and mainframe environments, the software supports TCP/IP. For the TCP/IP message transport layer, ports 5190 and 5790 are the default ports for the Voyager Agent and Pioneer Agent, respectively. You can change the ports for these agents. The procedures to configure these message transport layers are described later in this guide.

2.2.2 APF Authorization

Authorized Program Facility(APF). Granting the APF Authorized status to a program is similar to giving super user 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. The IdF Agent user account must have APF authorization.

2.3 Mainframe Adapter Installation

The following sections of this chapter describe the procedure to install the adapter.

- Section 2.3.1, "Extracting the Files from the Distribution Zip Archive File"
- Section 2.3.2, "Uploading the Files"
- Section 2.3.3, "Extracting the XMIT Files"
- Section 2.3.4, "Editing the Mainframe Batch Job Files to Match the Settings for the Customer's Site"
- Section 2.3.5, "Submitting Batch Job Streams"
- Section 2.3.6, "Loading and Activating the Exits"
- Section 2.3.7, "Creating an ACF2 LID for Pioneer and Voyager with Permissions"
- Section 2.3.8, "Adding Pioneer/Voyager to the Resource Rule Facilities (BPX and IRR)"
- Section 2.3.9, "Testing the Installation"

2.3.1 Extracting the Files from the Distribution Zip Archive File

To extract the files from the distribution zip file:

Extract the contents of the following file to a temporary directory, distribution zip archive file.

The following are the contents of the zip file:

- acf2-readme.txt
- linklib.xmi
- proclib.xmi
- parmlib.xmi
- jclib.xmi

2.3.2 Uploading the Files

You must upload the files that are extracted with the .xmi extension to the computer that is hosting the mainframe. See Section 2.3.1, "Extracting the Files from the Distribution Zip Archive File" for information about extracting the files for deployment.

You can upload the files either by using a QWS3270P emulator or FTP. The following is the procedure to upload files by using the QWS3270P emulator:

1. Log in to the TSO environment of the mainframe, type ISPF at the READY prompt, and then press **Enter.**
2. From the `ISPF` menu, on the Option line, enter `"6"`. The Command entry screen to enter TSO commands is displayed.

3. Use the IND$FILE command to upload files to the computer hosting the mainframe. The upload option of the QWS3270P program enters a formatted command.

   In this example the host file name is LINKLIB.XMIT' and the sending or local file name is as follows:

   The Upload File dialog box is displayed with the following options:

   `C:\Users\My_Name\Desktop\test-acf2\linklib.xmi.`

   The upload options are in the upload window for QWS3270P are:

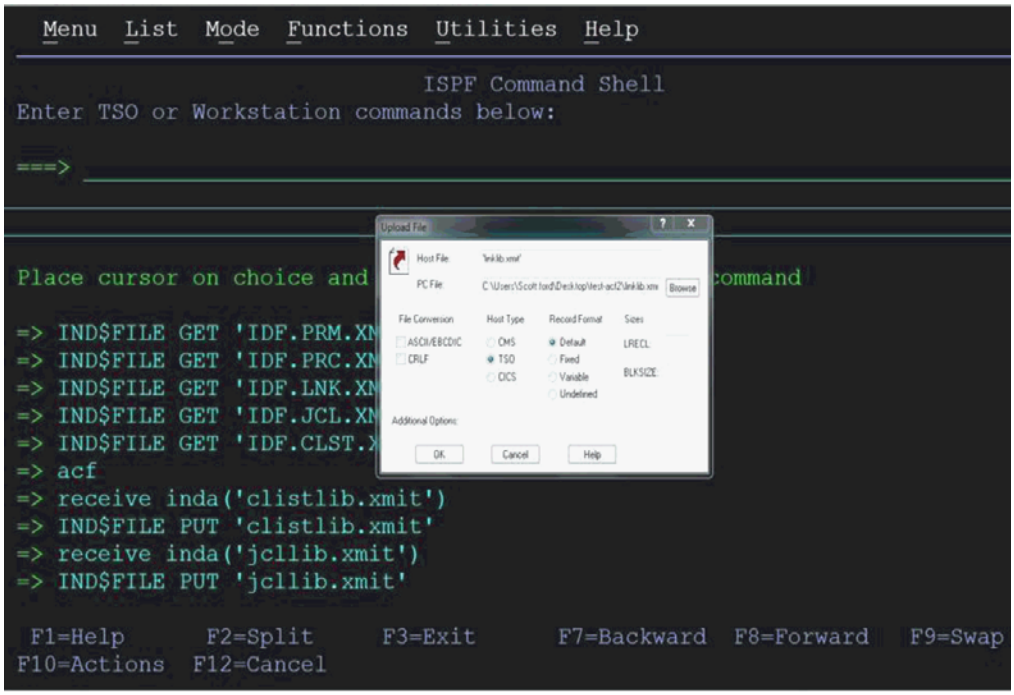
   File Conversion: Nothing selected (No ASCII/EBCDIC translation and no CRLF).

   Host Type: TSO

   Record Format: Default selected.

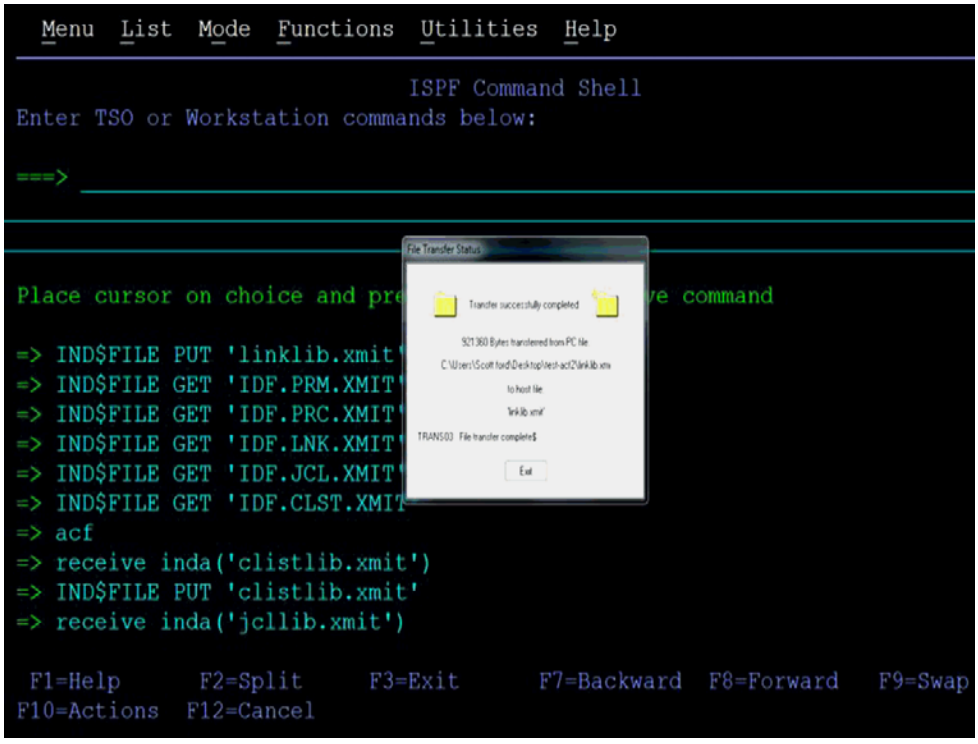
   Sizes: LRECL and **BLKSIZE** are left blank.

   Alternatively you can set the LRECL to `80` and the BLKSIZE set to `3120`.



4. Click **OK** to initiate file upload.

   The File Transfer Status dialog box with a message that the transfer was successfully completed is displayed.



5. Click **Exit** to dismiss the dialog box.
6. Repeat Steps 3 through 6 to upload the rest of the .XMI files.

Table 2–1 lists the uploaded files:

Table 2–1 File Names on Client Machine and Mainframe Host

Filename on Client Machine	Recommended File name on Mainframe Host
linklib.xmi	LINKLIB.XMIT
proclib.xmi	PROCLIB.XMIT
parmlib.xmi	PARMLIB.XMIT
jcllib.xmi	JCLLIB.XMIT

2.3.3 Extracting the XMIT Files

The files uploaded to the computer hosting the mainframe (by using the procedure described in Section 2.3.2, "Uploading the Files") are XMIT files. An XMIT file is an archived file format used on the mainframe.

To extract the files or Partition Datasets (PDS) in the XMIT file:

1. Enter the **RECEIVE c**ommand in the area designated to enter commands.

   For example, enter the following command:

   ```
   receive inda('linklib.xmit')
   ```

   Note: Filenames in mainframe are case insensitive.

2. When prompted, enter the following to complete running the RECEIVE command:

   ```
   Enter restore parameters or "DELETE" or "END" +
   ```

3. Enter the name of the PDS that the XMIT file will expand into. In this case, enter the following:

   ```
   dataset('USER_NAME.idf.FILE_NAME')
   ```

In this command, replace:

- USER_NAME with the user name on the system you have access to.
- FILE_NAME with the name of the XMIT file to be extracted.

For example:

```
dataset('IDF.LINKLIB.XMIT')
```

In this example, the prefix IDF is the user name that is being used in this section. In your environment, replace the prefix IDF with the user name on the system you have access to. If you specify the PDS name within single quotation marks, then the PDS name with a user name. That is the fully qualified name.

If single quotation marks are not used, then the PDS is created with a prefix of the user name that you are logged on with. In this case, the response is as follows:

```
dataset(idf.linklib)
```

Table 2–2 lists the XMIT file names and the corresponding PDS names:

Table 2–2 XMIT File Names and PDS Names

XMIT File Name on Mainframe Host	Recommended PDS Name on Mainframe Host
LINKLIB.XMIT	IDF.LINKLIB

Table 2–2 (Cont.) XMIT File Names and PDS Names

XMIT File Name on Mainframe Host	Recommended PDS Name on Mainframe Host
PROCLIB.XMIT	IDF.PROCLIB
PARMLIB.XMIT	IDF.PARMLIB
JCLLIB.XMIT	DF.JCLLIB

```
receive inda('idf.linklib.xmit')
 INMR901I Dataset IDF.LINKLIB from SFORD on NODENAME
 INMR906A Enter restore parameters or 'DELETE' or 'END' +
data('idf.prod.linklib')
                                        IEBCOPY MESSAGES AND CONTROL STATEMENT
S                               PAGE     1
 IEB1135I IEBCOPY  FMID HDZ1C10  SERVICE LEVEL NONE     DATED 20100402 DFSMS 01.
12.00 z/OS    01.12.00 HBB7770  CPU 1090
 IEB1035I SFORD    ISPFPROC ISPFPROC 12:27:25 TUE 08 JAN 2013 PARM='WORK=4M,SIZE
=1M'
  COPY INDD=((SYS00004,R)),OUTDD=SYS00003
 IEB1013I COPYING FROM PDSU  INDD=SYS00004 VOL=ZCSYS1 DSN=SYS13008.T122724.RA000
.SFORD.R0100214
 IEB1014I          TO PDS  OUTDD=SYS00003 VOL=ZCSYS1 DSN=IDF.PROD.LINKLIB
 IEB167I FOLLOWING MEMBER(S) LOADED FROM INPUT DATA SET REFERENCED BY SYS00004
 IEB154I ADDSP231 HAS BEEN SUCCESSFULLY LOADED
 IEB154I AESDEC16 HAS BEEN SUCCESSFULLY LOADED
 IEB154I AESDKX16 HAS BEEN SUCCESSFULLY LOADED
 IEB154I AESEKX16 HAS BEEN SUCCESSFULLY LOADED
 IEB154I AESENC16 HAS BEEN SUCCESSFULLY LOADED
 IEB154I CATNAP   HAS BEEN SUCCESSFULLY LOADED
 IEB154I CHKUSRPW HAS BEEN SUCCESSFULLY LOADED
 IEB154I DELSP231 HAS BEEN SUCCESSFULLY LOADED
 ***
```

Enter the response and follow the given steps:

1. Press **Enter** again for the **RECEIVE** command to continue.

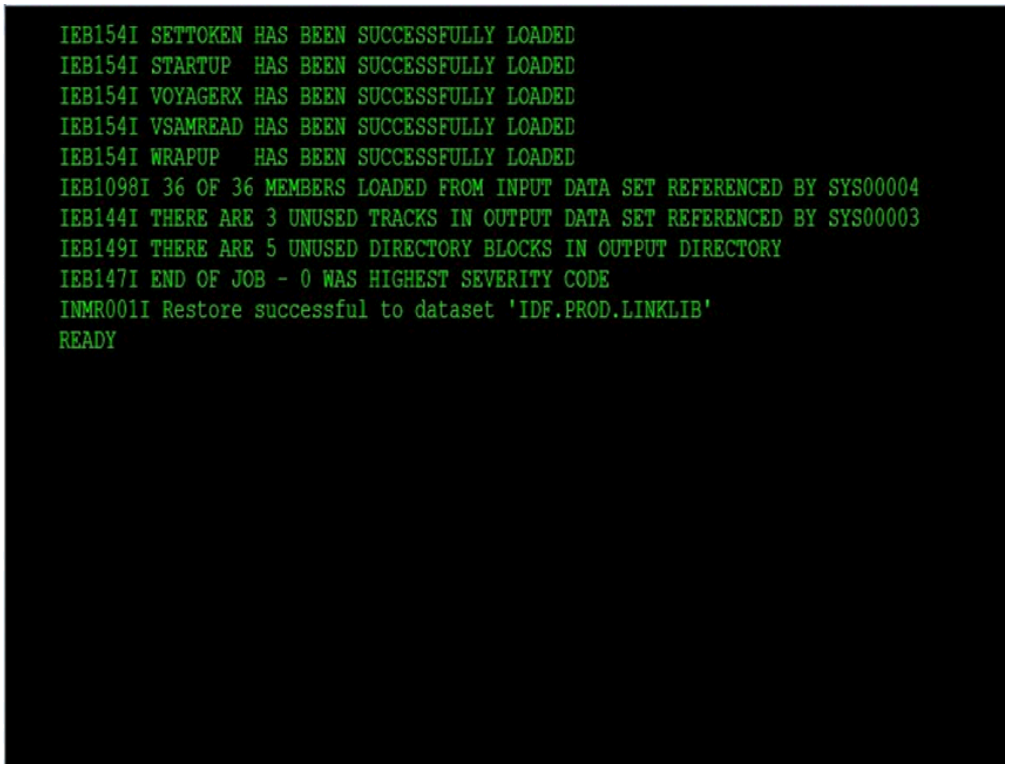
   The following two screen shots shows the output from the execution of the RECEIVE command.

2. Press **Enter** for each screen displayed since the output stops when the screen is full. The Receive command completes when the Restore successful message has been displayed on the screen.

3. Press **Enter** one last time to bring back the command entry screen.

4. Enter the **RECEIVE** command for each of the uploaded files using the host files name you selected for them.

5. Enter the **restore parameters** in response to each Receive command you enter.

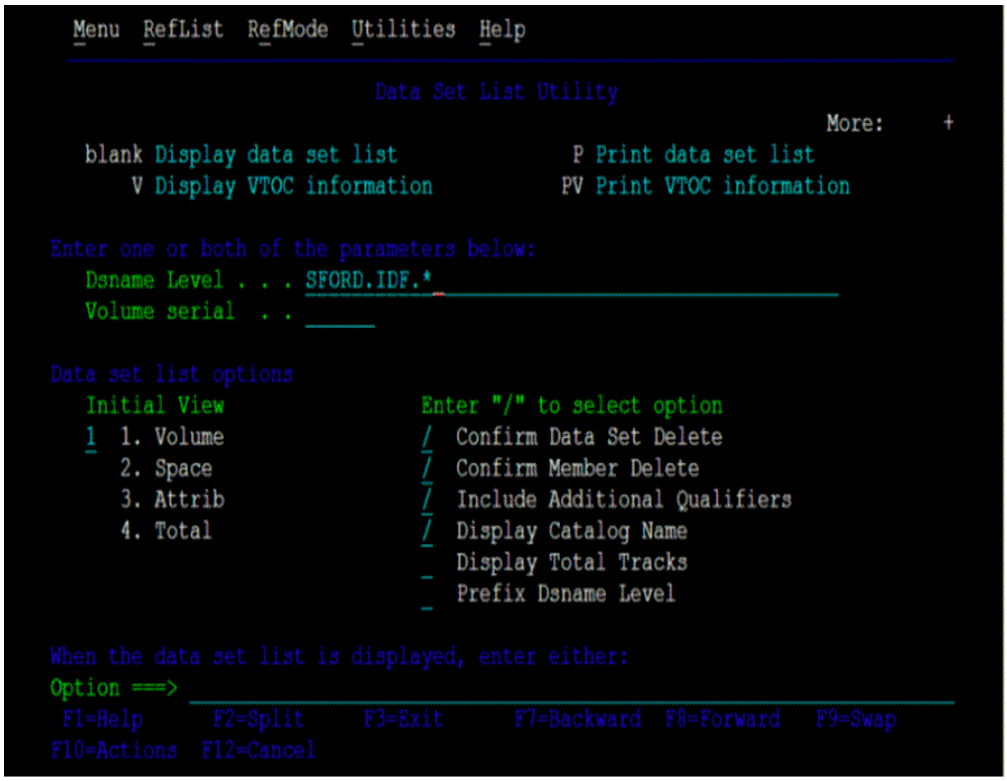


Note: The IDF.LINKLIB once "RECEIVED" can be either a STEPLIB or added to the environments existing Linklist. This library MUST be APF authorized.

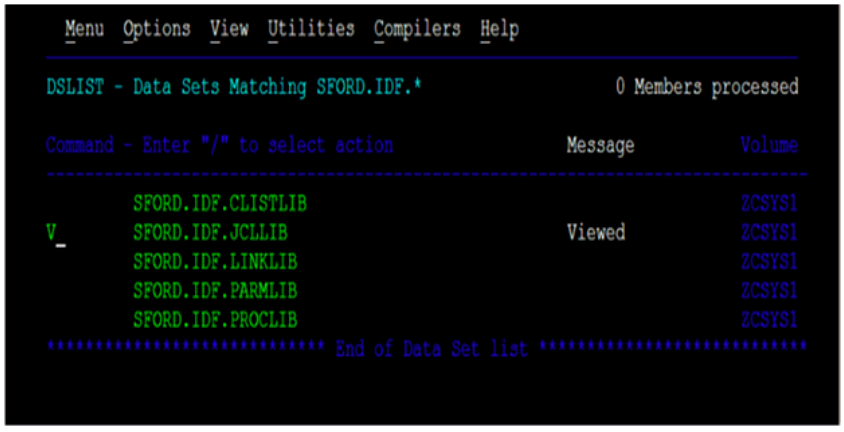
6. After all the files have been processed (extracted from the XMIT file with the Receive command), look at the members of each PDS using the Data Set List Utility which is ISPF option **3.4.**
7. Enter =**3.4** on the command line to go there from the command entry screen.

Note: The IDF.LINKLIB must be APF authorized. It can be a steplib or added to the systems existing Linklist. See Appendix C to see how to find the APF authorized files on your system.

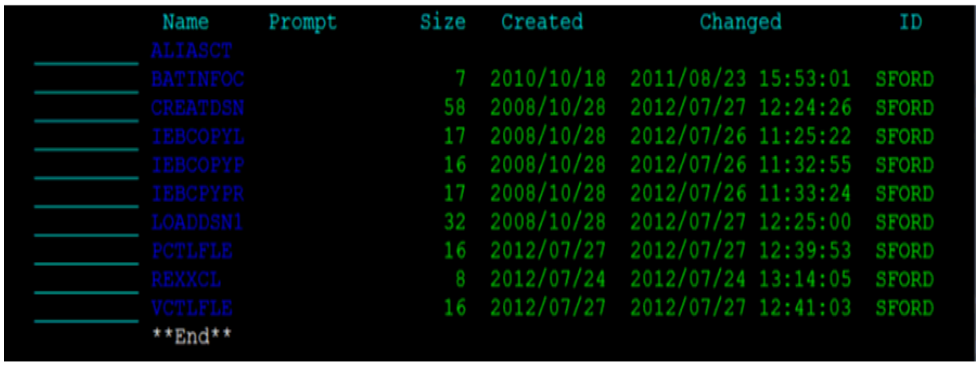
8. In the Data Set List Screen we entered **SFORD.IDF.*** in the Dsname Level field on the screen, because the user name that we used was SFORD. This will display a list of the files that match.



9. Press **Enter** to bring up the list. Here is the list of the files which matched what you entered.



10. Enter **V** (for view) to the left of one file names, and press the **Enter** to view the members in the PDS.
11. Enter **E** (for edit) to edit the members in the list.



Name	Prompt	Size	Created	Changed	ID
ALIASCT					
BATINFOC		7	2010/10/18	2011/08/23 15:53:01	SFORD
CREATDSN		58	2008/10/28	2012/07/27 12:24:26	SFORD
IEBCOPYL		17	2008/10/28	2012/07/26 11:25:22	SFORD
IEBCOPYP		16	2008/10/28	2012/07/26 11:32:55	SFORD
IEBCPYPR		17	2008/10/28	2012/07/26 11:33:24	SFORD
LOADDSN1		32	2008/10/28	2012/07/27 12:25:00	SFORD
PCTLFLE		16	2012/07/27	2012/07/27 12:39:53	SFORD
REXXCL		8	2012/07/24	2012/07/24 13:14:05	SFORD
VCTLFLE		16	2012/07/27	2012/07/27 12:41:03	SFORD
End					

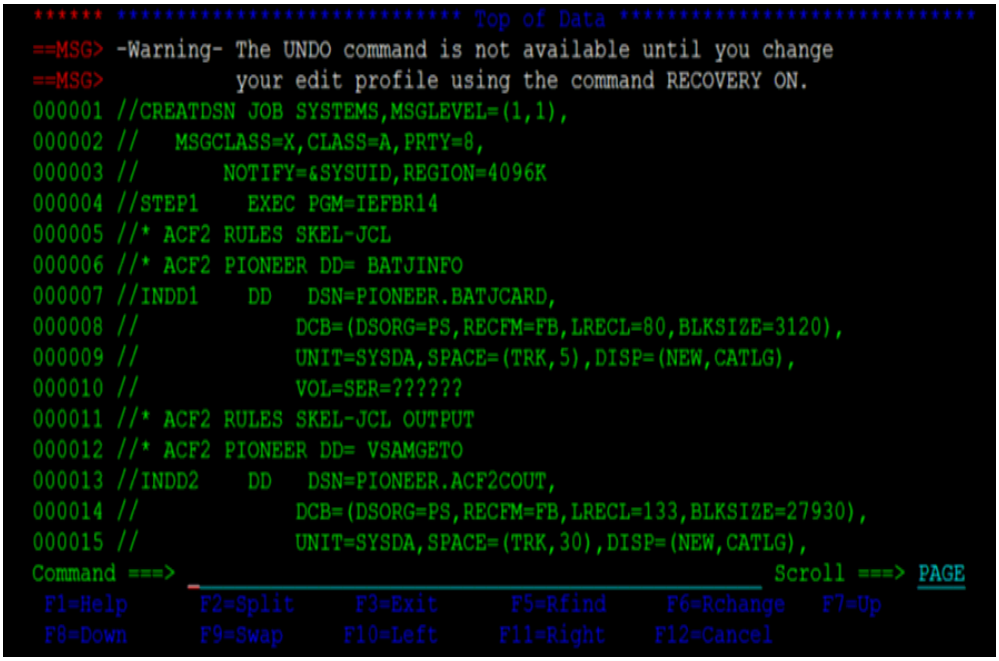
12. Place the cursor to the left of one of the member names on this screen to bring up the editor.
13. Click **EDIT** mode to make changes.

2.3.4 Editing the Mainframe Batch Job Files to Match the Settings for the Customer's Site

The **PDS IDF.JCLLIB** contains the following members: **CREATEDSN, IEBCOPYL, IEBCPYRP,** and **LOADDSN** which will have to be edited to change file names, volsers, and job names to match your installation specifications. Modify the jobcard for each batch job to meet your installation specifications. The job card will usually be the first three lines of the batch file.

To make changes to the batch job files:

1. Click **Edit** mode.
2. Open the CREATDSN member in the editor s to make changes.



```
****** ***************************** Top of Data ******************************
==MSG> -Warning- The UNDO command is not available until you change
==MSG>           your edit profile using the command RECOVERY ON.
000001 //CREATDSN JOB SYSTEMS,MSGLEVEL=(1,1),
000002 //    MSGCLASS=X,CLASS=A,PRTY=8,
000003 //         NOTIFY=&SYSUID,REGION=4096K
000004 //STEP1     EXEC PGM=IEFBR14
000005 //* ACF2 RULES SKEL-JCL
000006 //* ACF2 PIONEER DD= BATJINFO
000007 //INDD1     DD   DSN=PIONEER.BATJCARD,
000008 //              DCB=(DSORG=PS,RECFM=FB,LRECL=80,BLKSIZE=3120),
000009 //              UNIT=SYSDA,SPACE=(TRK,5),DISP=(NEW,CATLG),
000010 //              VOL=SER=??????
000011 //* ACF2 RULES SKEL-JCL OUTPUT
000012 //* ACF2 PIONEER DD= VSAMGETO
000013 //INDD2     DD   DSN=PIONEER.ACF2COUT,
000014 //              DCB=(DSORG=PS,RECFM=FB,LRECL=133,BLKSIZE=27930),
000015 //              UNIT=SYSDA,SPACE=(TRK,30),DISP=(NEW,CATLG),
Command ===> _                                          Scroll ===> PAGE
 F1=Help      F2=Split     F3=Exit      F5=Rfind     F6=Rchange   F7=Up
 F8=Down      F9=Swap      F10=Left     F11=Right    F12=Cancel
```

3. To change existing text in the file, type over the existing text with new text.
4. The editor will respond and provide a line to enter the text.

5. Press **Enter** before entering the text to remove the line.
6. Press **Enter** to add another line.
7. Press **Enter** to finish.

```
000005 //* ACF2 RULES SKEL-JCL
010006 //* ACF2 PIONEER DD= BATJINFO
000007 //INDD1    DD   DSN=PIONEER.BATJCARD,
```

There are also variations to the insert line command. A common variation is to enter a number after the **"I".**

To indicate the number of lines to insert:

- Use the arrow keys or the mouse to position the cursor to the line to enter text.

  If you press the **Enter** before you have finished entering text in your lines, then the lines that you didn't enter text into will disappear.

```
i50006 //* ACF2 PIONEER DD= BATJINFO
000007 //INDD1    DD   DSN=PIONEER.BATJCARD,
000008 //           DCB=(DSORG=PS,RECFM=FB,LRECL=80,BLKSIZE=3120),
```

```
000006 //* ACF2 PIONEER DD= BATJINFO
''''''
''''''
''''''
''''''
''''''
000007 //INDD1    DD   DSN=PIONEER.BATJCARD,
```

To delete lines in the file:

1. Enter **D** in the number area on the line that you want to delete.
2. Press **Enter** to delete the line.

   You can see that after entering a "D" in the first screen and in the second screen the line has been deleted.

```
000006 //* ACF2 PIONEER DD= BATJINFO
0d0007 //* A TEST TEXTLINE
000008 //INDD1    DD   DSN=PIONEER.BATJCARD,
000009 //           DCB=(DSORG=PS,RECFM=FB,LRECL=80,BLKSIZE=3120),
```

```
000006 //* ACF2 PIONEER DD= BATJINFO
000007 //INDD1    DD   DSN=PIONEER.BATJCARD,
000008 //           DCB=(DSORG=PS,RECFM=FB,LRECL=80,BLKSIZE=3120),
```

There are variations of the delete line command. A common variation is to enter a number after D to indicate the number of lines to delete. For example:

- Enter **D3** to delete 3 lines.

```
000006 //* ACF2 PIONEER DD= BATJINFO
d30007 //* TEST LINE 1
000008 //* TEST LINE 2
000009 //* TEST LINE 3
000010 //INDD1    DD   DSN=PIONEER.BATJCARD,
```

```
000006 //* ACF2 PIONEER DD= BATJINFO
000007 //INDD1    DD   DSN=PIONEER.BATJCARD,
000008 //            DCB=(DSORG=PS,RECFM=FB,LRECL=80,BLKSIZE=3120),
```

To navigate through the file you need to use the function keys as follows:

- Press **F7** to scroll the edit screen up a screen to the beginning of the file.
- Press **F8** to scroll the edit screen down a screen to the end of the file.
- Press **F3** to finish editing the file.

```
Command ===>                                              Scroll ===> PAGE
 F1=Help      F2=Split     F3=Exit      F5=Rfind     F6=Rchange   F7=Up
 F8=Down      F9=Swap      F10=Left     F11=Right    F12=Cancel
```

The Following are the Members of PDS IDF.JCLLIB:

- The **CREATDSN** member is an IEFBR14 file creation stream that will build the files required for Pioneer and Voyager. For each dataset name (DSN), PIONEER is used for the High-Level qualifier (HLQ) for Pioneer files and VOYAGER is used for the HLQ for Voyager files. The HLQ will have to be changed to meet installation standards. The VOL=SER= should be changed to point to the installation dasd volumes. The allocations are adequate. Once this member has been reviewed and changed, submit this job and review the output. The return code (RC) should be 0000.
- The **LOADDSN 1** member loads the files created by CREATDSN to the defined load area. For each DSN, PIONEER is used for the HLQ for Pioneer files and VOYAGER is used for the HLQ for Voyager files. The HLQ will have to be changed to meet installation standards. The SYSUT1 value defines the member to be loaded and SYSUT2 value defines the sequential or flat file it is being loaded into. Submit the job and review the output. The RC should be 0000.
- The **IEBCOPYL** member copies the ACF2 exits (LIDPOST, NEWPXIT, and EXPPXIT) and the called caching routine IDFCACHE to an installation LPA library that ACF2 has access to. Review and change the LPA library name to meet installation standards. Submit the job and review the output. The RC should be 0000.

  If your host mainframe has any of the exits already in place that IdF ships (LIDPOST, NEWPXIT, and EXPPXIT), then it is your responsibility to integrate these exits. If the customer does not have the staff or knowledge then IdF can be contacted and they will provide assistance via a Professional Services contract.
- The **IEBCPYPR** member is an IEBCOPY file copy stream for the STC procedures and procedures used by the product. Pioneer and Voyager are STC procedures. Startup and Wrapup are **emergency only** procedures to build the subpool (STARTUP) and delete the subpool(WRAPUP) for Voyager. Normally, when z/OS

is shutdown the subpool storage area is released. Review the names and change to meet installation specifications. Change the procedure library name to the installation procedure library name. Submit the JOB stream and review the output. The RC should be 0000.

Remember that the jobcard for each of the above batch jobs will have to be changed to meet installation specifications. Files must not be shared in a SYSPLEX. Each Pioneer and Voyager must have their own set of files.

Below is shown the "Createdsn" supplied in the JCLLIB PDS. The "YOURHLQ" is the installation Highlevel qualifier used for the Pioneer and Voyager datasets. The second portion of the dataset name is only a reference to illustrate the correspondence between the STC Pioneer and Voyager to the datasets. The VOL=SER=?????? is the dasd volume where the files are to be created. If SMS is being used this JCL will have to be changed to match installation definitions for these type and size datasets.

Table 2–3 YOURHLQ

YOURHLQ
//CREATDSN JOB SYSTEMS,MSGLEVEL=(1,1), // MSGCLASS=X,CLASS=A,PRTY=8, // NOTIFY=&SYSUID,REGION=4096K //*---* //* CHANGE YOURHLQ TO THE INSTALLATION HLQ //* CHANGE VOL=SER=?????? TO YOUR INSTALLATION VOL=SER //* STEP 1 = PIONEER DDNAME=LISTINR //* STEP 2 = PIONEER DDNAME=IDCAMSD //* STEP 3 = PIONEER DDNAME=ACF2CTL //* STEP 4 = PIONEER DDNAME=ACF2OUT //* STEP 5 = VOYAGER DDNAME=CACHESAV //* STEP 6 = VOYAGER DDNAME=PARMFLE //* STEP 7 = PIONEER DDNAME=PARMFLE //*---*

//STEP1 EXEC PGM=IEFBR14
//INDD1 DD DSN=YOURHLQ.ALIASOUT,
// DCB=(DSORG=PS,RECFM=VBA,LRECL=133,BLKSIZE=0),
// UNIT=SYSDA,SPACE=(CYL,5),DISP=(NEW,CATLG),
// VOL=SER=??????

//STEP2 EXEC PGM=IEFBR14
//INDD2 DD DSN=YOURHLQ.IDCAMSD.FILE,
// DCB=(DSORG=PS,RECFM=F,LRECL=80,BLKSIZE=80),
// UNIT=SYSDA,SPACE=(TRK,2),DISP=(NEW,CATLG),
// VOL=SER=??????

//STEP3 EXEC PGM=IEFBR14
//INDD3 DD DSN=YOURHLQ.ACF2.CTL,
// DCB=(DSORG=PS,RECFM=F,LRECL=80,BLKSIZE=80),
// UNIT=SYSDA,SPACE=(TRK,2),DISP=(NEW,CATLG),
// VOL=SER=??????

Table 2–3 (Cont.) YOURHLQ

YOURHLQ
//STEP4 EXEC PGM=IEFBR14
//INDD4 DD DSN=YOURHLQ.ACF2OUT,
// DCB=(DSORG=PS,RECFM=VBA,LRECL=133,BLKSIZE=0),
// UNIT=SYSDA,SPACE=(CYL,30),DISP=(NEW,CATLG),
// VOL=SER=??????
//STEP5 EXEC PGM=IEFBR14
//INDD5 DD DSN=YOURHLQ.CACHESAV,
// DCB=(DSORG=PS,RECFM=FB,LRECL=112,BLKSIZE=27888),
// UNIT=SYSDA,SPACE=(CYL,10),DISP=(NEW,CATLG),
// VOL=SER=??????
//STEP6 EXEC PGM=IEFBR14
//INDD6 DD DSN=YOURHLQ.CONTROL.FILE,
// DCB=(DSORG=PS,RECFM=F,LRECL=80,BLKSIZE=80),
// UNIT=SYSDA,SPACE=(TRK,1),DISP=(NEW,CATLG),
// VOL=SER=??????
//STEP7 EXEC PGM=IEFBR14
//INDD7 DD DSN=YOURHLQ.CONTROL.FILE,
// DCB=(DSORG=PS,RECFM=F,LRECL=80,BLKSIZE=80),
// UNIT=SYSDA,SPACE=(TRK,1),DISP=(NEW,CATLG),
// VOL=SER=??????

Table 2–4 shows the LOADDSN1.

Pioneer and Voyager were used below as High Level Qualifiers to illustrate the job stream below.

Table 2–4 LOADDSN1

LOADDSN1
//LOADDSN JOB SYSTEMS,MSGLEVEL=(1,1),
// MSGCLASS=X,CLASS=A,PRTY=8,
// NOTIFY=&SYSUID,REGION=4096K
//STEP1 EXEC PGM=IEBGENER
//SYSUT1 DD DSN=IDF.PROD.JCLLIB(PCTLFLE),DISP=SHR
//SYSUT2 DD DSN=PIONEER.CONTROL.FILE,DISP=SHR
//SYSPRINT DD SYSOUT=*
//SYSIN DD DUMMY
/*
//STEP2 EXEC PGM=IEBGENER
//SYSUT1 DD DSN=IDF.PROD.JCLLIB(VCTLFLE),DISP=SHR
//SYSUT2 DD DSN=VOYAGER.CONTROL.FILE,DISP=SHR
//SYSPRINT DD SYSOUT=*
//SYSIN DD DUMMY

The "YOURHLQ" is the installation Highlevel qualifier used for the Pioneer and Voyager datasets. The second portion of the dataset name is only a reference to illustrate the correspondance between the STC Pioneer and Voyager to the datasets. The VOL=SER=?????? is the dasd volume where the files are to be created. If SMS is being used this JCL will have to be changed to match installation definitions for these type and size datasets.

See Appendix E for information about the relationships between the DSNs in each step in the LOADDSN1 member and the file contents that are loaded into Pioneer's datasets.

The following is the IEBCOPYL member:

```
//IEBCOPYL JOB SYSTEMS,MSGLEVEL=(1,1),
// MSGCLASS=X,CLASS=A,PRTY=8,
// NOTIFY=&SYSUID,REGION=4096K
//*
---------------------------------------
//* COPY EXITS TO LPA LOADLIB
//*
---------------------------------------
//MODUCPY1 EXEC PGM=IEBCOPY
//INDD DD DSN=IDF.TEST.LINKLIB,DISP=SHR
//OUTDD DD DSN=USER.ACF2.LPALIB,DISP=SHR
//SYSPRINT DD SYSOUT=*
//SYSIN DD * COPY INDD=((INDD,R)),OUTDD=OUTDD
S M=((IDFACF2E,,R))
S M=((IDFACF2P,,R))
S M=((IDFACF2X,,R))
S M=((IDFCACHE,,R))
/*
```

The following is the IEBCPYPR member:

```
//IEBCPYPR JOB SYSTEMS,MSGLEVEL=(1,1),
// MSGCLASS=X,CLASS=A,PRTY=8,
// NOTIFY=&SYSUID,REGION=4096K
//*
-------------------------------------------
//* COPY STC PROCEDURES TO PROCLIB--------------
//*-------------------------------------------
//JCLCPY EXEC PGM=IEBCOPY
//INDD2 DD DSN=IDF.TEST.PROCLIB,DISP=SHR
//OUTDD2 DD DSN=IDF.TEST.PPPRC,DISP=SHR
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
COPY INDD=((INDD2,R)),OUTDD=OUTDD2
S M=((VOYAGER,,R))
S M=((PIONEER,,R))
```

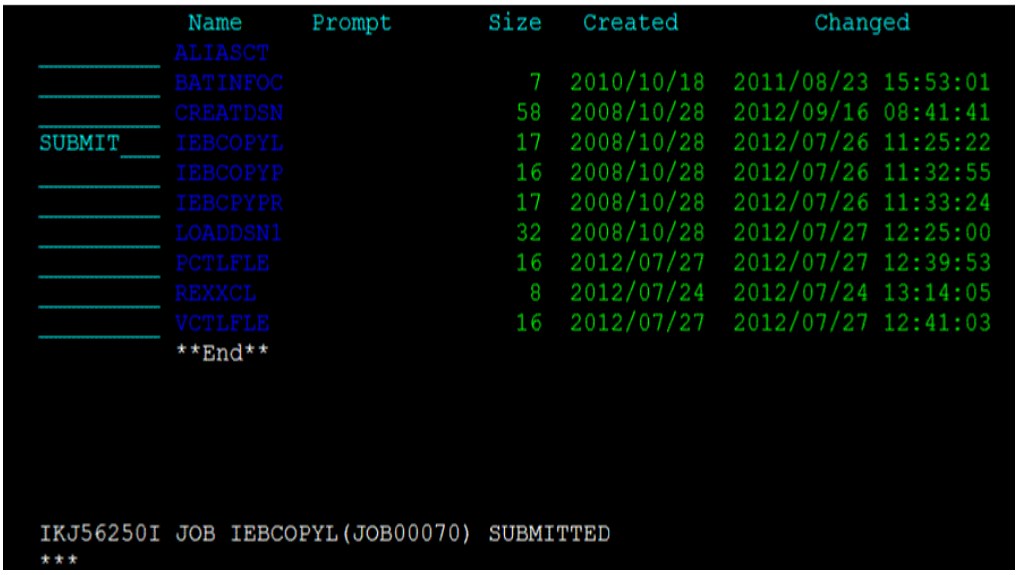
2.3.5 Submitting Batch Job Streams

For submitting batch job streams to z/OS for execution and verify jobs completed successfully, after the jcl files have been edited to reflect the settings for the target environment, the jcl needs to be submitted for batch processing, perform the following steps:

1. Submit the jobs from the screen where the members of the JCLLIB were displayed.
2. Type **SUBMIT** to the left of the member you want to submit for processing.

3. Press **Enter** to verify that the jobs have completed successfully.

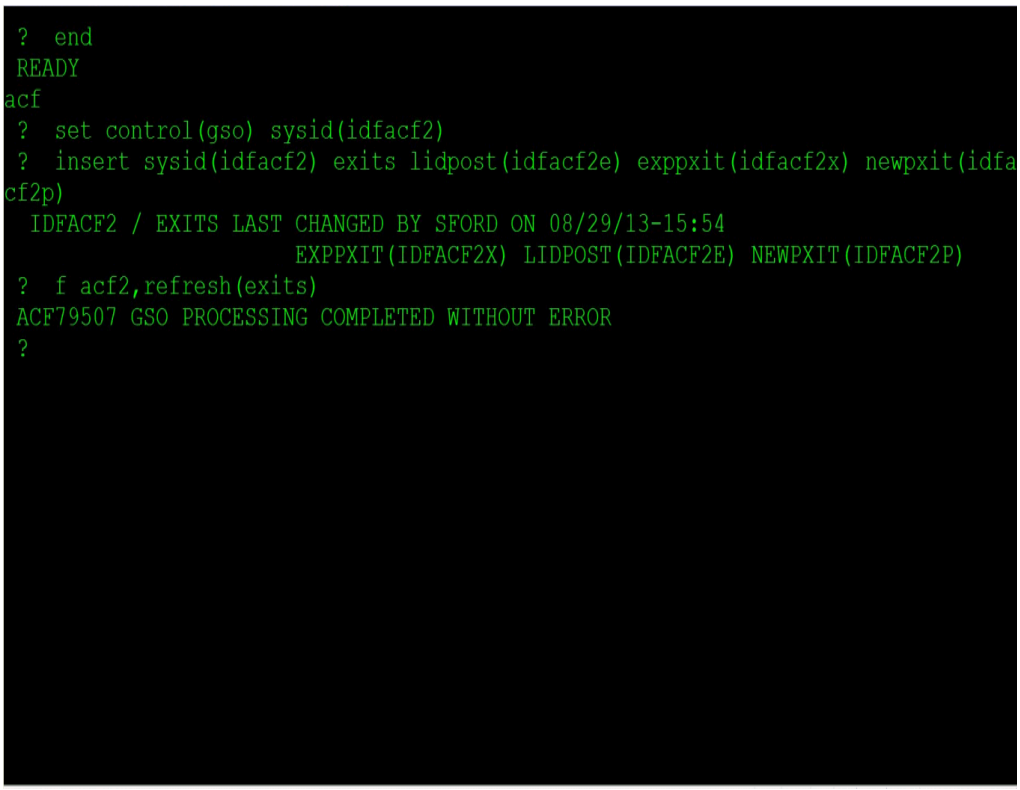
   If there are any errors when submitting a job, fix the errors in the job and resubmit the job.



2.3.6 Loading and Activating the Exits

To load and activate the exits (new install):

1. In TSO enter the ACF environment by entering ACF in the option `#6` command line. The text in green is entered by the user.



2. If an exit has been loaded already and you want to change it, then a CHANGE SYSID (xxxx) EXITS with the exit name and module name will have to be performed. If the exits don't exist then an INSERT SYSID (xxx) exit name and module names will have to be performed.

   Display the exits that are loaded.

```
 READY
ACF
 ?  SET CONTROL(GSO) SYSID(ADCD)
 ?  LIST EXITS
  ADCD / EXITS LAST CHANGED BY SFORD ON 07/26/12-13:35
                      EXPPXIT(IDFACF2X) LIDPOST(IDFACF2E) NEWPXIT(IDFACF2P)
 ?  QUIT
 READY
```

3. Set APF authorization for Pioneer and Voyager with progID as follows:

   a. Verify that the LPA library containing the exits are in the LPA, IEASYSXX. Start member of Z/OS, usually contained within the SYS1.PARMLIB.

   b. The executable code (IBM z/OS loadlibs) of Pioneer and Voyager must be APF authorized. This can be achieved by running a dynamic set command (T PROG=ID) or by placing the installation loadlib containing Pioneer and Voyager in the IBM z/OS link list. In order to refresh the LPA library, IPL the IBM z/OS system.

      IBM® provides the PROGxx parmlib member as an alternative to IEAAPFxx, which allows you to update the APF list dynamically and specify an unlimited number of APF-authorized libraries. IBM suggests that you use PROGxx to specify the APF list (regardless of whether you plan to take advantage of the dynamic update capability). The system will process IEAAPFxx and PROGxx if both parameters are specified. If you decide to use PROGxx only, remove APF=xx system parameters from IEASYSxx and IEASYS00.

Note: Voyager also needs AUDIT to list. So it will be `INSERT VOYAGER NAME(VOYAGER) AUDIT STC`.

2.3.7 Creating an ACF2 LID for Pioneer and Voyager with Permissions

To create an ACF 2 LID for Pioneer and Voyager with permissions:

```
 READY
ACF
 ? SET LID
 ? INSERT PIONEER NAME(PIONEER) ACCOUNT STC SECURITY
 ? INSERT VOYAGER NAME(VOYAGER) AUDIT STC
 ? QUIT
 READY
```

After the LIDs have been created an ACF LIST should show this output:

```
READY
ACF
 ? LIST PIONEER
  PIONEER              PIONEER  PIONEER PROVISIONING
  PRIVILEGES           ACCOUNT SECURITY STC
  ACCESS               ACC-CNT(39) ACC-DATE(07/27/12) ACC-TIME(10:48)
  PASSWORD             KERB-VIO(0) KERBCURV() PSWA1TOD(00/00/00-00:00)
                       PSWD-DAT(00/00/00) PSWD-INV(0) PSWD-TOD(00/00/00-00:00)
                       PSWD-VIO(0) PSWDCVIO(0) PWP-DATE(00/00/00) PWP-VIO(0)
  TSO                  DFT-PFX(PIONEER)
  STATISTICS           CRE-TOD(05/02/10-22:41) SEC-VIO(0)
                       UPD-TOD(07/27/12-10:48)
  RESTRICTIONS         PREFIX(PIONEER)
 ? QUIT
 READY
```

```
READY
ACF
 ? LIST VOYAGER
  VOYAGER              VOYAGER  VOYAGER
  PRIVILEGES           AUDIT STC
  ACCESS               ACC-CNT(0) ACC-DATE(00/00/00) ACC-TIME(00:00)
  PASSWORD             KERB-VIO(0) KERBCURV() PSWA1TOD(00/00/00-00:00)
                       PSWD-DAT(00/00/00) PSWD-INV(0) PSWD-TOD(00/00/00-00:00)
                       PSWD-VIO(0) PSWDCVIO(0) PWP-DATE(00/00/00) PWP-VIO(0)
  TSO                  DFT-PFX(VOYAGER)
  STATISTICS           CRE-TOD(05/02/10-22:40) SEC-VIO(0)
                       UPD-TOD(09/16/12-09:00)
  RESTRICTIONS         PREFIX(VOYAGER)
 ? QUIT
 READY
```

2.3.8 Adding Pioneer/Voyager to the Resource Rule Facilities (BPX and IRR)

To add Pioneer or Voyager to the resource rule facilities:

```
 READY
ACF
 ?  SET RESOURCE(FAC)
 ?  COMPILE
 ACF70010 ACF COMPILER ENTERED

 .  $KEY(BPX) TYPE(FAC)
 .  DAEMON UID(PIONEER) SERVICE(READ) LOG
 .  DAEMON UID(VOYAGER) SERVICE(READ) LOG
 .
 ACF70051 TOTAL RECORD LENGTH= 220 BYTES, 5 PERCENT UTILIZED
 ?  STORE
 ACF60028 RESOURCE  BPX REPLACED
 ACF60039 Issue the F ACF2,REBUILD(FAC) command to activate the rule
 ?  F ACF2,REBUILD(FAC)
 ACF8A036 DIRECTORY RFAC HAS BEEN REBUILT
 ?  QUIT
 READY
```

```
 READY
ACF
 ?  SET RESOURCE(FAC)
 ?  COMPILE
 ACF70010 ACF COMPILER ENTERED

 .  $KEY(IRR) TYPE(FAC)
 .  IRR.RADMIN.* UID(PIONEER) SERVICE(READ) LOG
```

List the new rules.

```
 READY
ACF
 ?  SET RESOURCE(FAC)
 ?  LIST BPX
 ACF75052 RESOURCE RULE BPX STORED BY MLIGHT ON 09/06/12-20:55
 $KEY(BPX) TYPE(FAC)
  DAEMON UID(PIONEER) SERVICE(READ) LOG
  DAEMON UID(VOYAGER) SERVICE(READ) LOG
 ACF75051 TOTAL RECORD LENGTH= 220 BYTES, 5 PERCENT UTILIZED
 ?  LIST IRR
 ACF75052 RESOURCE RULE IRR STORED BY MLIGHT ON 09/06/12-21:20
 $KEY(IRR) TYPE(FAC)
  IRR.RADMIN.LISTUSER UID(VOYAGER) SERVICE(READ) LOG
  IRR.RADMIN.* UID(PIONEER) SERVICE(READ) LOG
 ACF75051 TOTAL RECORD LENGTH= 262 BYTES, 6 PERCENT UTILIZED
 ?  QUIT
 READY
```

Note:

- Pioneer must have SECURITY privileges, which acts as a central site security administrator and must be able to add lids, change lids, delete lids as well as resources, rules. Voyager does not need this level of security. Pioneer needs to be able to perform all functions for IRR.RADMIN so we will use **IRR.RADMIN.*.**
- Voyager only needs to be able to perform IRR.RADMIN.LISTUSER.
- All IRR.RADMIN calls are through the standard IBM module IRRSEQ00. Verify that the RACF subsystem interface is activated at IPL time.
- The SYS1.PARMLIB member is IEFSSNxx, where xx is the user's suffix. The required parameters for the RACF API are as follows: **SUBSYS SUBNAME(RACF) /* RACF SUBSYSTEM */ INITRTN(IRRSSI00) INITPARM('#')** (Or) **SUBSYS SUBNAME(RACF)**. All ACF2 commands are passed through the RACF API interface (service Radmin, program = IRRSEQ00).
- The SYS1.PARMLIB member (IFAPRDnn) must be updated to set the 'SECURITY SERVER' to a disabled state:

  For example:

  ```
  (not the "STATE(DISABLED)")
  PRODUCT OWNER('IBM CORP')
  NAME('z/OS')
  VERSION(*) RELEASE(*) MOD(*)
  STATE(DISABLED)
  ```

  You can ignore the "IRR418I RACF product disabled: IRRSSI00 ended." message that appears.

The INITPARM can contain any character that IBM z/OS supports. There may be more than one character in the list such as INITPARM('#,X'). Even though the Security Subsystem is ACF2, this RACF API is still used by Pioneer when it makes the call to R_admin (IRRSEQ00) API.

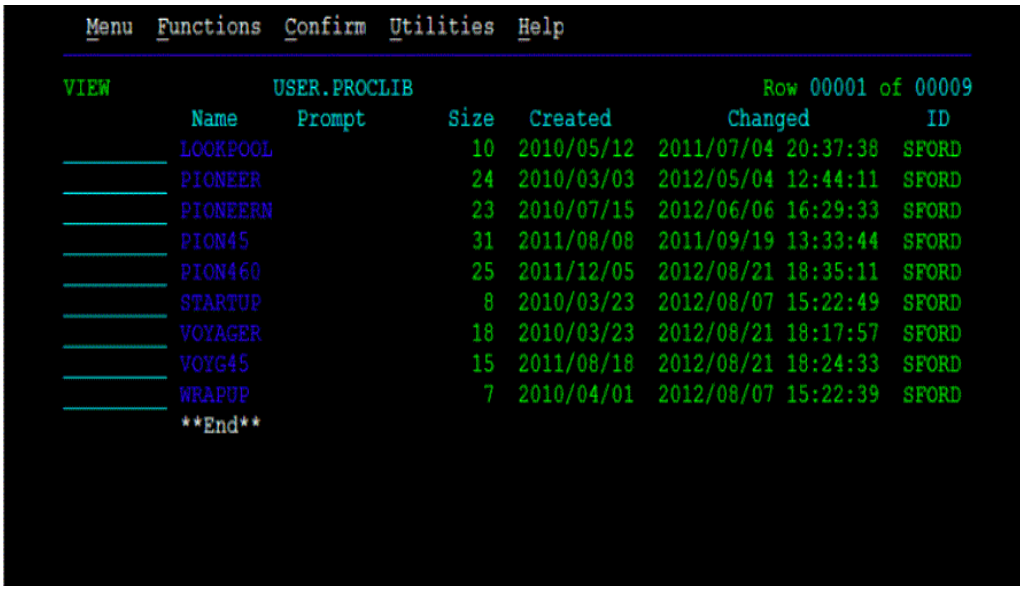
2.3.9 Testing the Installation

Review this connector guide for the control file parameters for Voyager and Pioneer and change the configuration files (Pioneer and Voyager STC PARMFLE DDs) for the installation. Consult the Identity Manage Installation Staff for TCPIP PORT addresses and TCPIP Addresses for both Voyager and Pioneer. Also consult the IDM staff for the VOYAGER_ID= variable explained later in this connector guide in the Voyager parameters section.

To test the installation:

1. IPL the system to bring in the new LPA library modules.
2. Check that the exit modules have been loaded.

   The following are the list of the members in **USER.PROCLIB.**



3. Execute Voyager.

Note: STARTUP and WRAPUP are not required any more. Voyager performs their functions.

Start the Voyager Agent by running "S VOYAGER" from the console or SDSF in TSO. By adding the STC procedure for VOYAGER inside a Job Scheduler is another way you can start the task. To quiesce VOYAGER:

```
"F VOYAGER,SHUTDOWN"
```

Upon entering the "F VOYAGER,SHUTDOWN", Voyager closes the IP connection the LDAP and then closes all open files. The last task that is performed is deletion of a storage subpool token and deletion of the subpool.

Voyager Control File Used for Testing:

```
* COMMENT FOR VOYAGER
SUBPOOL_SIZE=1000K
TCPN=TCPIP
IPAD=xxx.xxx.xxx.xxx
PORT=5197
DEBUG=N
ESIZE=16
DEBUGOUT=SYSOUT,CLAS(K)
VOYAGER_ID=TESTACF2
FILTER1=NO
FILTER2=NO
FILTER3=NO
CACHE_DELAY=005
AUDIT=YES,SYSOUT,CLASS(S)
```

JCL for the Voyager Started Task (STC):

Voyager STC:

```
//VOYAGER  PROC
//STEP1    EXEC PGM=VOYAGERX,REGION=0M,TIME=1440
//STEPLIB  DD DISP=SHR,DSN=IDF.LINKLIB     <--- IF NOT IN LINKLIST
```

```
//CACHESAV DD DSN=VOYAGER.CACHSAV,DISP=SHR
//DEBUGOUT DD SYSOUT=*
//SYSOUT   DD SYSOUT=*
//AUDTLOG  DD SYSOUT=*
//PARMOUT  DD SYSOUT=*
//PARMFLE  DD DISP=SHR,DSN=VOYAGER.CONTROL.FILE
//SYSPRINT DD SYSOUT=*
//SYSUDUMP DD SYSOUT=X
//
```

To Execute Voyager (STC log):

```
0290  S  VOYAGER
0281  $HASP100 VOYAGER  ON STCINRDR
0290  IEF695I START VOYAGER  WITH JOBNAME VOYAGER  IS ASSIGNED TO USER
VOYAGER
0090  $HASP373 VOYAGER  STARTED
0090  ACF9CCCD USERID VOYAGER  IS ASSIGNED TO THIS JOB - VOYAGER
0281  IEF403I VOYAGER - STARTED - TIME=13.08.42
0090  IDMV000I - VOYAGER RECONCILATION  AGENT STARTING
0090  IDMV000I - VOYAGER IS EXECUTING  FROM AN APF AUTHORIZED LIBRARY
0090  IDMV000I - VOYAGER FOUND          ACF2 SECURITY SUBSYSTEM
0090  IDMV202E - VOYAGER NO STORAGE TOKEN     FOUND
0090  IDMV000I - VOYAGER SUBPOOL  INITIALIZATION OK
0090  IDMV003I - VOYAGER SP231  ALLOCATED OK
0090  IDMV001I - VOYAGER SUBPOOL  SIZE IS:    1000 K
0090  IDMV002I - VOYAGER SUBPOOL  WILL HOLD :   10240 MESSAGES
0090  IDMV004I - VOYAGER STORAGE TOKEN BUILT OK
0090  IDMV152I - VOYAGER IP CONNECT REQUEST 71.14.2.190
0090  IDMV002I - VOYAGER BUILD          LEVEL IS AT
201301081402-4.7.0.5
0090  IDMV003I - VOYAGER SUBPOOL        100 BYTE VERSION
0090  IDMV004I - VOYAGER DETECTS       (TCPIP)JOBNAME      TCPIP
0090  IDMV005I - VOYAGER DETECTS       (TCPIP)IP ADDRESS   71.14.2.190
0090  IDMV002I - ORACLE BUILD           LEVEL IS AT        09.00.04.19.0
0090  IDMV006I - VOYAGER DETECTS       (TCPIP)IP PORT      5097
0090  IDMV013I - VOYAGER DETECTS        DEBUGGING IS       OFF
0090  IDMV017  - VOYAGER DETECTS AUDLOG IS NOW : ACTIVE
0090  IDMV015I - VOYAGER DETECTS        COUNTRY CODE OF    US
0090  IDMV007I - VOYAGER DETECTS        ENCRYPTION IS      ON
0090  IDMV011I - VOYAGER DETECTS        ENCRYPTION KVER    200610261425
0090  IDMV019I - VOYAGER INITIALIZATION OF TCP API WAS     SUCCESSFUL
0090  IDMV022I - VOYAGER INITIALIZATION OF PTON WAS SUCCESSFUL
0090  IDMV009I - VOYAGER DETECTS        CACHE FILE OPENED  OK
0090  IDMV155I - VOYAGER CACHESAVE WAS READ        0  MESSAGES
```

To Execute Voyager (PARMSOUT log):

```
01/08/13 13:08:43:11 * PARMFLE * OPEN
01/08/13 13:08:43:11 VOYAGER PARMS FOUND:
01/08/13 13:08:43:11 SUBPOOL_SIZE=1000K
01/08/13 13:08:43:11 TCPN=TCPIP
01/08/13 13:08:43:11 IPAD=xxx.xxx.xxx.xxx
01/08/13 13:08:43:11 * IPAD=RACF.LEGACYIDM.COM
01/08/13 13:08:43:11 PORT=5097
01/08/13 13:08:43:11 DEBUG=N
01/08/13 13:08:43:11 ESIZE=16
01/08/13 13:08:43:11 VOYAGER_ID=TESTVGER
01/08/13 13:08:43:11 FILTER1=NO
01/08/13 13:08:43:11 FILTER2=NO
```

```
01/08/13 13:08:43:11 CACHE_DELAY=002
01/08/13 13:08:43:11 AUDIT=YES,SYSOUT,CLASS(S)
01/08/13 13:08:43:14 ALL PARMS GOOD
------------------------------------------------------------
```

4. Starting Pioneer:

   Start the Pioneer Agent by running "S PIONEER" from the console or by running /S PIONEER in SDSF under TSO. Adding the STC procedure for PIONEER inside a Job Scheduler is another way you can start the task.

   Pioneer Control File Used for Testing:

```
* CONTROL FILE COMMENT
TCPN=TCPIP
IPAD=0.0.0.0
PORT=5190
DEBUG=N
LPAR=ACF2-100BYTE-SYS
POST_PROC_ALIAS=F
IDLEMSG=N
DEBUGOUT=SYSOUT,CLASS(X)
SPIN_CLASS=K
FILTER=NO
AUDIT=YES,SYSOUT,CLASS(S)
STATS=NO
```

   The "YOURHLQ" is the installation Highlevel qualifier used for the Pioneer and Voyager datasets. The second portion of the dataset name is only a reference to illustrate the correspondence between the STC Pioneer and Voyager to the datasets. The VOL=SER=?????? is the dasd volume where the files are to be created. If SMS is being used this JCL will have to be changed to match installation definitions for these type and size datasets.

   See Appendix F for information about Pioneer control file parameter descriptions.

   JCL for the Pioneer Started Task (STC):

   Pioneer STC:

```
//PIONEER  EXEC PGM=PIONEERX,REGION=0M,TIME=1440
//JCLOUTP  DD SYSOUT=*
//DEBUGOUT DD SYSOUT=*
//PARMOUT  DD SYSOUT=*
//RULELOG  DD SYSOUT=*
//SYSOUT   DD SYSOUT=*
//AUDTLOG  DD SYSOUT=*
//PARMFLE  DD DISP=SHR,DSN=YOURHLQ.CONTROL.FILE
//LISTINR  DD DISP=SHR,DSN=YOURHLQ.ALIASOUT,
//            DCB=(RECFM=VB,LRECL=137)
//IDCAMSD  DD DISP=SHR,DSN=YOURHLQ.IDCAMSD.FILE
//ACF2CTL  DD DISP=SHR,DSN=PIONEER.ACF2.CTL
//ACF2OUT  DD DISP=SHR,DSN=PIONEER.ACF2OUT,
//            DCB=(RECFM=VB,LRECL=137)
//SYSPUNCH DD SYSOUT=(*,INTRDR)
//SYSPRINT DD SYSOUT=*
//SYSUDUMP DD SYSOUT=X
//
```

To Execute Pioneer (STC log):

```
0290  S PIONEER
0281  $HASP100 PIONEER  ON STCINRDR
0290  IEF695I START PIONEER  WITH JOBNAME PIONEER  IS ASSIGNED TO USER PIONEER
0090  $HASP373 PIONEER  STARTED
0090  ACF9CCCD USERID PIONEER  IS ASSIGNED TO THIS JOB - PIONEER
0281  IEF403I PIONEER - STARTED - TIME=14.36.28
0090  IDMP201I - PIONEER ALL POST PARMS WERE GOOD  STATUS = GOOD
0090  IDMP071I - PIONEER  PARMFLE    IS NOW CLOSED
0090  IDMP201I - PIONEER ALL PARMS WERE GOOD       STATUS = GOOD
0090  IDMP000I - PIONEER STARTING
0090  IDMP001I - PIONEER INPUT    PARAMETERS ARE   OK
0090  IDMP002I - PIONEER DETECTS  IDF-BUILD        201201081531-4.7.0.5
0090  IDMP002I - PIONEER DETECTS  AUDIT LOG IS NOW: ACTIVE
0090  IDMP002I - PIONEER DETECTS  ORACLE BUILD     09.00.04.19
0090  IDMP003I - PIONEER DETECTS  TCPIP JOBNAME    TCPIP
0090  IDMP004I - PIONEER DETECTS  TCPIP IP ADDRESS 0.0.0.0
0090  IDMP005I - PIONEER DETECTS  TCPIP IP PORT    5697
0090  IDMP006I - PIONEER DETECTS  DEBUGGING IS     ACTIVE
0090  IDMP011I - PIONEER DETECTS  CPUID            01B0DB1090
0090  IDMP012I - PIONEER DETECTS  SYSPLEX SYSNAME  ADCD
0090  IDMP013I - PIONEER DETECTS  LPARNAME AS      ACF2-QA-ZOS112
0090  IDMP014I - PIONEER DETECTS  COUNTRY CODE OF  US
0090  IDMP009I - PIONEER DETECTS  ENCRYPTION       ENABLED
0090  IDMA000I - PIONEER EXECUTING FROM APF AUTHORIZED LIBRARY
0090  IDMP030I - PIONEER INITAPI   WAS SUCCESSFUL
0090  IDMP031I - PIONEER GETCLIENTID WAS SUCCESSFUL
0090  IDMP032I - CLIENT  NAME IS PIONEER
0090  IDMP033I - CLIENT  TASK IS PIONEERX
0090  IDMP035I - PIONEER BIND SOCKET WAS SUCCESSFUL
0090  IDMP036I - PIONEER LISTENING PORT IS  5697
0090  IDMP037I - PIONEER LISTENING ADDRESS IS 0.0.0.0
0090  IDMP038I - PIONEER LISTEN SOCKET CALL WAS  SUCCESSFUL
0090  ** PIONEER LISTENING READY FOR MESSAGES **
```

To Execute Pioneer (PARMSOUT):

```
01/08/13 14:36:29.32 IDMP400I  *PARMS* - TCPN=TCPIP
01/08/13 14:36:29.32 IDMP400I  *PARMS* - IPAD=0.0.0.0
01/08/13 14:36:29.32 IDMP400I  *PARMS* - PORT=5697
01/08/13 14:36:29.32 IDMP400I  *PARMS* - DEBUG=Y
01/08/13 14:36:29.32 IDMP400I  *PARMS* - ESIZE=16
01/08/13 14:36:29.32 IDMP400I  *PARMS* - LPAR=ACF2-QA-ZOS112
01/08/13 14:36:29.32 IDMP400I  *PARMS* - POST_PROC_ALIAS=T
01/08/13 14:36:29.33 IDMP400I  *PARMS* - IDLEMSG=N
01/08/13 14:36:29.33 IDMP400I  *PARMS* - DEBUGOUT=SYSOUT,CLASS(S)
01/08/13 14:36:29.33 IDMP400I  *PARMS* - SPIN_CLASS=K
01/08/13 14:36:29.33 IDMP400I  *PARMS* - FILTER=NO
01/08/13 14:36:29.33 IDMP400I  *PARMS* - AUDIT=YES,SYSOUT,CLASS(S)
01/08/13 14:36:29.33 IDMP400I  *PARMS* - STATS=NO
01/08/13 14:36:29.33 IDMP400I  *PARMS* - PARMOUT CLOSED
```

5. Stopping the started tasks.

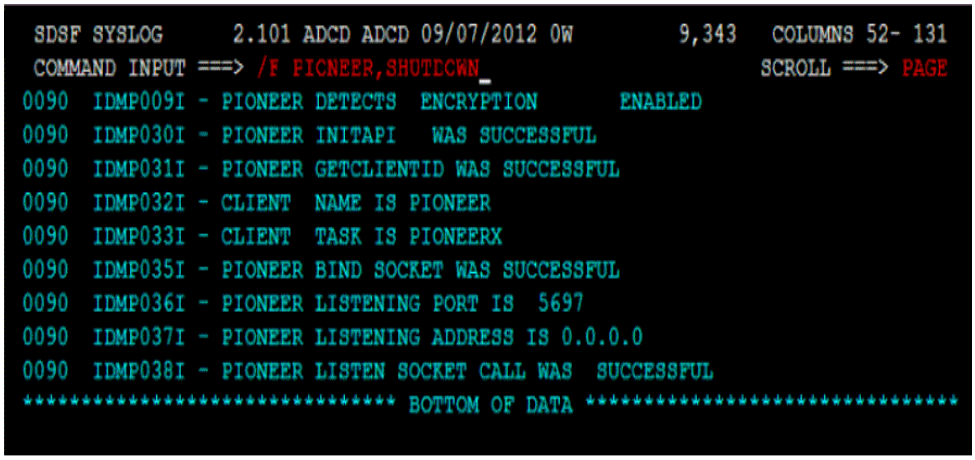
   The operator interface is named **POLLOPER** in both Voyager and Pioneer. Both STCs are single thread and commands are passed to them via a z/OS modify("F") command.

Pioneer can be controlled by commands via Operator Interface with the commands given in Table 2–5.

Table 2–5 Pioneer Commands and Descriptions

Pioneer Commands	Description
F PIONEER,SHUTDOWN	Shuts Down Pioneer
F PIONEER,STATUS	Heartbeat message
F PIONEER,DEBUG=Y	Turns on Debugging
F PIONEER,DEBUG=N	Turns off Debugging

Functions:



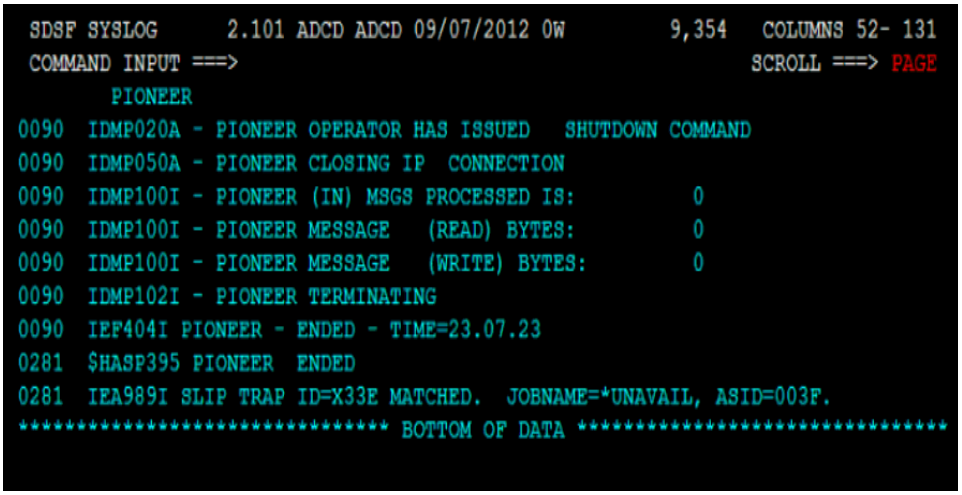


Table 2–6 lists Voyager Commands via Operator Interface:

Table 2–6 Voyager Commands via Operator Interface

Voyager commands	Description
F VOYAGER,SHUTDOWN	Shuts Down Voyager
F VOYAGER,STATUS	Heartbeat message
F VOYAGER,DEBUG=Y	Turns on Debugging
F VOYAGER,DEBUG=N	Turns off Debugging

Table 2–6 (Cont.) Voyager Commands via Operator Interface

Voyager commands	Description
F VOYAGER,IPAD=999.999.999.999,PORT=99999	Swaps LDAP Gateway

Note: The commands in the following screen shots are not required if DNS is used.

```
 SDSF SYSLOG      2.101 ADCD ADCD 09/07/2012 0W         9,354   COLUMNS 52- 131
 COMMAND INPUT ===>                                            SCROLL ===> PAGE
       PIONEER
0090  IDMP020A - PIONEER OPERATOR HAS ISSUED   SHUTDOWN COMMAND
0090  IDMP050A - PIONEER CLOSING IP  CONNECTION
0090  IDMP100I - PIONEER (IN) MSGS PROCESSED IS:          0
0090  IDMP100I - PIONEER MESSAGE   (READ) BYTES:          0
0090  IDMP100I - PIONEER MESSAGE   (WRITE) BYTES:         0
0090  IDMP102I - PIONEER TERMINATING
0090  IEF404I PIONEER - ENDED - TIME=23.07.23
0281  $HASP395 PIONEER  ENDED
0281  IEA989I SLIP TRAP ID=X33E MATCHED.  JOBNAME=*UNAVAIL, ASID=003F.
******************************** BOTTOM OF DATA ********************************
```

```
 SDSF SYSLOG      2.101 ADCD ADCD 09/07/2012 0W         9,450   COLUMNS 52- 131
 COMMAND INPUT ===> /F VOYAGER,SHUTDOWN                        SCROLL ===> PAGE
0090  IDMV008I - VOYAGER DETECTS        CACHE READ DELAY   002 SECS
0090  IDMV011I - VOYAGER DETECTS        ENCRYPTION KVER    200610261425
0090  IDMV019I - VOYAGER INITIALIZATION OF TCP API WAS     SUCCESSFUL
0090  IDMV021I - VOYAGER INITIALIZATION OF PTON WAS SUCCESSFUL
0090  IDMV025I - VOYAGER CONNECTED      TO GATEWAY SERVER WAS SUCCESSFUL
0090  IDMV021I - VOYAGER ACCEPTING      MESSAGES ON        71.14.2.190
0090  IDMV009I - VOYAGER DETECTS        CACHE FILE OPENED  OK
0281  IKT100I USERID MLIGHT    CANCELED DUE TO UNCONDITIONAL LOGOFF
```

3

Connector Deployment on Oracle Identity Manager

The LDAP Gateway acts as the intermediary between Oracle Identity Manager and the connector components on the mainframe. The following sections of this chapter describe the procedure to deploy some components of the connector, including the LDAP Gateway, on the Oracle Identity Manager host computer:

> **Note:** The procedure to deploy the mainframe components of the connector is described in the next chapter.

- Section 3.1, "Files and Directories that Comprise the Connector"
- Section 3.2, "Determining the Release Number of the Connector"
- Section 3.3, "Before Running the Connector Installer"
- Section 3.4, "Running the Connector Installer"
- Section 3.5, "Configuring the IT Resource"
- Section 3.6, "Configuring Oracle Identity Manager"
- Section 3.7, "Configuring Trusted Source Reconciliation"
- Section 3.8, "Configuring Oracle Identity Manager for Request-Based Provisioning"
- Section 3.9, "Installing and Configuring the LDAP Gateway"

3.1 Files and Directories that Comprise the Connector

Table 3–1 describes the contents of the connector installation media.

Table 3–1 Files and Directories that Comprise the Connector

Files and Directories	Description
configuration/ACF2Adv.xml	This XML file contains configuration information that is used during connector installation.
DataSets/ProvisionResource_OIMACF2ResourceObject.xml DataSets/ModifyResource_OIMACF2ResourceObject.xml	This XML file specifies the information to be submitted by the requester during a request-based provisioning operation. Section 3.8, "Configuring Oracle Identity Manager for Request-Based Provisioning" provides more information.
etc/LDAP Gateway/ldapgateway.zip	This ZIP file contains the files required to deploy the LDAP Gateway.

Table 3–1 (Cont.) Files and Directories that Comprise the Connector

Files and Directories	Description
etc/Provisioning and Reconciliation Connector/Mainframe_ACF2.zip	This ZIP file contains the files required to deploy the Reconciliation and Provisioning Agents on the mainframe.
Files in the resources directory	Each of these resource bundles contains locale-specific information that is used by the connector. During connector installation, this file is copied to the following location: ■ For Oracle Identity Manager Release 9.1.0.*x*: *OIM_HOME*/xellerate/connectorResources ■ For Oracle Identity Manager Release 11.1.1: Oracle Identity Manager database **Note:** A **resource bundle** is a file containing localized versions of text strings that are displayed on the Administrative and User Console. These text strings include GUI element labels and messages.
For Oracle Identity Manager Release 9.1.0.*x:* lib/acf2-provisioning-adapter.jar For Oracle Identity Manager Release 11.1.1: lib-11G/acf2-provisioning-adapter.jar	This JAR file contains the code for the adapters that are used during connector operations. During connector installation, this file is copied to the following location: ■ For Oracle Identity Manager Release 9.1.0.*x:* *OIM_HOME*/xellerate/JavaTasks ■ For Oracle Identity Manager Release 11.1.1: Oracle Identity Manager database
For Oracle Identity Manager Release 9.1.0.*x:* lib/acf2-scheduled-tasks.jar For Oracle Identity Manager Release 11.1.1: lib-11G/acf2-scheduled-tasks.jar	This JAR file contains the code for the scheduled task that is used during full reconciliation. During connector installation, this file is copied to the following location: ■ For Oracle Identity Manager Release 9.1.0.*x:* *OIM_HOME*/xellerate/ScheduledTask ■ For Oracle Identity Manager Release 11.1.1: Oracle Identity Manager database
For Oracle Identity Manager Release 9.1.0.*x:* scripts/propertyEncrypt.bat scripts/propertyEncrypt.sh For Oracle Identity Manager Release 11.1.1: scripts-11G/propertyEncrypt.bat scripts-11G/propertyEncrypt.sh	This script is used to encrypt the password of the user account that you create for the LDAP Gateway.
xml/oimAcf2AdvConnector.xml	This XML file contains definitions of the connector components, such as the IT resource and resource object. These objects are created in Oracle Identity Manager when you import the XML file.
xml/Acf2TrustedXellerateUser.xml	This XML file contains definitions of the connector components that are used for trusted source reconciliation.

3.2 Determining the Release Number of the Connector

Note: If you are using Oracle Identity Manager Release 9.1.0.*x*, then the procedure described in this section is optional.

If you are using Oracle Identity Manager Release 11.1.1, then skip this section.

You might have a deployment of an earlier release of the connector. While deploying the latest release, you might want to know the release number of the earlier release. To determine the release number of the connector that has already been deployed:

1. In a temporary directory, extract the contents of the connector JAR file that is in the *OIM_HOME*/xellerate/JavaTasks directory.
2. Open the Manifest.mf file in a text editor. The Manifest.mf file is one of the files bundled inside the connector JAR file.

   In the Manifest.mf file, the release number of the connector is displayed as the value of the Version property.

3.3 Before Running the Connector Installer

Prior to running the Connector Installer, you will need to delete the script and lib directories that do not pertain to your Oracle Identity Manager release version.

If running Oracle Identity Manager Release 9.1.0.*x:*

- Delete the "scripts-11G" directory from the connector package.
- Delete the "lib-11G" directory from the connector package.

If running Oracle Identity Manager Release 11.1.1:

- Delete the "scripts" directory from the connector package.
- Delete the "lib" directory from the connector package.
- Rename the "scripts-11G" directory to "scripts".
- Rename the "lib-11G" directory to "lib".

3.4 Running the Connector Installer

To run the Connector Installer:

1. Copy the contents of the connector installation media directory into the following directory:

   Note: In an Oracle Identity Manager cluster, copy this JAR file to each node of the cluster.

   - For Oracle Identity Manager Release 9.1.0.*x*: *OIM_HOME*/xellerate/ConnectorDefaultDirectory
   - For Oracle Identity Manager Release 11.1.1: *OIM_HOME*/server/ConnectorDefaultDirectory
2. Log in to the Administrative and User Console by using the user account described in the "Creating the User Account for Installing Connectors" section of the following guide:
   - For Oracle Identity Manager Release 9.1.0.*x*:

     Oracle Identity Manager Administrative and User Console Guide
   - For Oracle Identity Manager Release 11.1.1:

     Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager

3. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:

   - For Oracle Identity Manager Release 9.1.0.*x*:

     Click **Deployment Management**, and then click **Install Connector**.

   - For Oracle Identity Manager Release 11.1.1:

     On the Welcome to Identity Manager Advanced Administration page, in the System Management region, click **Install Connector**.

4. From the Connector List list, select **CA ACF2 Advanced *RELEASE_NUMBER***. This list displays the names and release numbers of connectors whose installation files you copy into the default connector installation directory in Step 1.

   If you have copied the installation files into a different directory, then:

   a. In the **Alternative Directory** field, enter the full path and name of that directory.

   b. To repopulate the list of connectors in the Connector List list, click **Refresh**.

   c. From the Connector List list, select **CA ACF2 Advanced *RELEASE_NUMBER***.

5. Click **Load**.

6. To start the installation process, click **Continue**.

   The following tasks are performed in sequence:

   a. Configuration of connector libraries

   b. Import of the connector Target Resource user configuration XML file (by using the Deployment Manager). If you want to import the target system as a trusted source for reconciliation, then see Section 3.7, "Configuring Trusted Source Reconciliation."

   c. Compilation of adapters

   On successful completion of a task, a check mark is displayed for the task. If a task fails, then an X mark and a message stating the reason for failure are displayed. Depending on the reason for the failure, make the required correction and then perform one of the following steps:

   - Retry the installation by clicking **Retry.**
   - Cancel the installation and begin again from Step 1.

7. If all three tasks of the connector installation process are successful, then a message indicating successful installation is displayed. In addition, a list of the steps that you must perform after the installation is displayed. These steps are as follows:

   a. Ensuring that the prerequisites for using the connector are addressed

   Note: At this stage, run the Oracle Identity Manager PurgeCache utility to load the server cache with content from the connector resource bundle in order to view the list of prerequisites. See Section 3.6.1, "Clearing Content Related to Connector Resource Bundles from the Server Cache" for information about running the PurgeCache utility.

   There are no prerequisites for some predefined connectors.

b. Configuring the IT resource for the connector

Record the name of the IT resource displayed on this page. The procedure to configure the IT resource is described later in this guide.

c. Configuring the scheduled task that is created when you installed the connector

---

Note: In Oracle Identity Manager Release 11.1.1, a scheduled job is an instance of a scheduled task. In this guide, the term **scheduled task** used in the context of Oracle Identity Manager Release 9.1.0.*x* is the same as the term **scheduled job** in the context of Oracle Identity Manager Release 11.1.1.

See *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager* for more information about scheduled tasks and scheduled jobs.

Record the name of the scheduled task displayed on this page. The procedure to configure this scheduled task is described later in this guide.

When you run the Connector Installer, it copies the connector files and external code files to destination directories on the Oracle Identity Manager host computer. These files are listed in Table 3–1.

Installing the Connector in an Oracle Identity Manager Cluster

While installing Oracle Identity Manager in a cluster, you must copy all the JAR files and the contents of the `connectorResources` directory into the corresponding directories on each node of the cluster. See Section 3.1, "Files and Directories that Comprise the Connector" for information about the files that you must copy and their destination locations on the Oracle Identity Manager server.

3.5 Configuring the IT Resource

You must specify values for the parameters of the Acf2Resource IT resource as follows:

1. Log in to the Administrative and User Console.
2. If you are using Oracle Identity Manager Release 9.1.0.*x*, expand **Resource Management,** and then click **Manage IT Resource**.
3. If you are using Oracle Identity Manager Release 11.1.1, then:
   - On the Welcome page, click **Advanced** in the upper-right corner of the page.
   - On the Welcome to Oracle Identity Manager Advanced Administration page, in the Configuration region, click **Manage IT Resource**.
4. In the IT Resource Name field on the Manage IT Resource page, enter `Acf2Resource` and then click **Search**.
5. Click the edit icon for the IT resource.
6. From the list at the top of the page, select **Details and Parameters**.
7. Specify values for the parameters of the IT resource. Table 3–2 describes each parameter.

Table 3–2 IT Resource Parameters

Parameter	Description
AtMap User	This parameter holds the name of the lookup definition containing attribute mappings that are used for provisioning. Value: `AtMap.ACF2` **Note:** You must not change the value of this parameter.
idfPrincipalDn	Set a user ID for an account that the connector will use to connect to the LDAP Gateway. Format: `cn=`*`USER_ID`*`,dc=acf2,dc=com` Sample value: `cn=idfAcf2Admin,dc=acf2,dc=com` You also set this user ID in the following files: ■ beans.xml inside the idfserver.jar file. See Step 6 in Section 3.9, "Installing and Configuring the LDAP Gateway." ■ initialAcf2Adv.properties. See Section 4.1, "Performing Full Reconciliation."
idfPrincipalPwd	Set a password for the account that the connector will use to connect to the LDAP Gateway. You also set this password in the files listed in the description of the idfPrincipalDn parameter.
idfRootContext	This parameter holds the root context for CA ACF2. Value: `dc=acf2,dc=com` **Note:** You must not change the value of this parameter.
idfServerHost	This parameter holds the host name of the computer on which you install the LDAP Gateway. For this release of the connector, you install the LDAP Gateway on the Oracle Identity Manager host computer. Value: `localhost` **Note:** You must not change the value of this parameter.
idfServerPort	Enter the number of the port for connecting to the LDAP Gateway. Sample value: `5389` You also set this port number in the beans.xml inside the idfserver.jar file. See Step 6 in Section 3.9, "Installing and Configuring the LDAP Gateway."
idfSsl	This parameter determines whether the LDAP Gateway will use SSL to connect to the target system. Enter 'true' if using SSL; otherwise enter 'false'. Value: `true`
idfTrustStore	This parameter holds the directory location of the trust store containing the SSL certificate. This parameter is optional, and should only be entered when using SSL authentication. Sample value: `../conf/idf.jks`

Table 3–2 (Cont.) IT Resource Parameters

Parameter	Description
idfTrustStorePassword	This parameter holds the password for the SSL trust store. This parameter is optional, and should only be entered when using SSL authentication.
idfTrustStoreType	This parameter holds the trust store type for the SSL trust store. This parameter is optional, and should only be entered when using SSL authentication. Sample value: `jks`
Last Modified Time Stamp	The most recent start time of the Reconcile LDAP Users reconciliation scheduled task is stored in this parameter. See Section 6.8, "Reconciling Internal LDAP Users to Oracle Identity Manager" for more information about this scheduled task. The format of the value stored in this parameter is as follows: `MM/dd/yy hh:mm:ss a` In this format: ▪ MM is the month of the year. ▪ dd is the day of the month. ▪ yy is the year. ▪ hh is the hour in am/pm (01-12). ▪ mm is the minute in the hour. ▪ ss is the second in the minute. ▪ a is the marker for AM or PM. ▪ Sample value: `05/07/10 02:46:52 PM` The default value is 0. The reconciliation task will perform full LDAP user reconciliation when the value is 0. If the value is a non-zero, standard time-stamp value in the format given above, then incremental reconciliation is performed. Only records that have been created or modified after the specified time stamp are brought to Oracle Identity Manager for reconciliation. **Note:** When required, you can manually enter a time-stamp value in the specified format.

8. To save the values, click **Update**.

3.6 Configuring Oracle Identity Manager

Configuring Oracle Identity Manager involves the following procedures:

Note: In an Oracle Identity Manager cluster, perform these steps on each node of the cluster.

- Section 3.6.1, "Clearing Content Related to Connector Resource Bundles from the Server Cache"
- Section 3.6.2, "Enabling Logging"

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

Note: In an Oracle Identity Manager cluster, you must perform this step on each node of the cluster. Then, restart each node.

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 for Oracle Identity Manager Release 9.1.0.*x*, and Oracle Identity Manager database for Oracle Identity Manager Release 11.1.1. Whenever you add a new resource bundle to 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, perform one of the following steps:
   - If you are using Oracle Identity Manager Release 9.1.0.*x*, then switch to the *OIM_HOME*/xellerate/bin directory.
   - If you are using Oracle Identity Manager Release 11.1.1, then switch to the *OIM_HOME*/server/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:

   For Oracle Identity Manager Release 9.1.0.*x*:

   OIM_HOME/xellerate/bin/*SCRIPT_FILE_NAME*

   For Oracle Identity Manager Release 11.1.1:

   OIM_HOME/server/bin/*SCRIPT_FILE_NAME*

2. Enter one of the following commands:

   Note: You can use the PurgeCache utility to purge the cache for any content category. Run `PurgeCache.bat` *`CATEGORY_NAME`* on Microsoft Windows or `PurgeCache.sh` *`CATEGORY_NAME`* on UNIX. The *`CATEGORY_NAME`* argument represents the name of the content category that must be purged.

   For example, the following commands purge Metadata entries from the server cache:

   ```
   PurgeCache.bat MetaData
   ```

   ```
   PurgeCache.sh MetaData
   ```

   - For Oracle Identity Manager Release 9.1.0.*x*:

     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 delete from the server cache. See the following file for information about the other content categories:

OIM_HOME/xellerate/config/xlconfig.xml

- For Oracle Identity Manager Release 11.1.1:

  On Microsoft Windows: `PurgeCache.bat All`

  On UNIX: `PurgeCache.sh All`

  When prompted, enter the user name and password of an account belonging to the SYSTEM ADMINISTRATORS group. In addition, you are prompted to enter the service URL in the following format:

  `t3://OIM_HOST_NAME:OIM_PORT_NUMBER`

  In this format:

  – Replace *OIM_HOST_NAME* with the host name or IP address of the Oracle Identity Manager host computer.

  – Replace *OIM_PORT_NUMBER* with the port on which Oracle Identity Manager is listening.

See *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager* for more information about the PurgeCache utility.

3.6.2 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. Oracle Identity Manager uses Oracle Java Diagnostic Logging (OJDL) for logging. OJDL is based on java.util.logger.

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:

- ERROR:1
- WARNING:1
- NOTIFICATION:1
- NOTIFICATION:16
- TRACE:1
- TRACE:16
- TRACE:32

See Message Types and Levels in *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information about the log levels.

Oracle Identity Manager level logging operations are managed by the logging.xml file which is located in the following directory:

DOMAIN_NAME/config/fmwconfig/servers/*SERVER_NAME*/

Loggers are used to configure logging operations for the Oracle Identity Manager functions of the connector.

To configure loggers:

1. In a text editor, open the *DOMAIN_NAME*/config/fmwconfig/servers/*SERVER_NAME*/logging.xml file.

2. Locate the logger you want to configure. If you are adding a logger for the first time, you must create the logger definition. Table 3–3, " Logger Parameters" lists the Oracle Identity Manager loggers for this connector.

Table 3–3 Logger Parameters

Logger	Description
com.identityforge.util.acf2.LdapOperationsImpl	Logs events related to basic LDAP functions, including connecting to and disconnecting from the LDAP gateway.
com.identityforge.util.acf2.tasks.DeleteReconcileOIMUsersTask	Logs events related to the ACF2 Delete OIM Users scheduled task.
com.identityforge.util.acf2.tasks.FindAllAccessRulesTask	Logs events related to the ACF2 Find All Access Rules scheduled task.
com.identityforge.util.acf2.tasks.FindAllResourcesTask	Logs events related to the ACF2 Find All Resources scheduled task.
com.identityforge.util.acf2.tasks.ReconcileAllLdapUsersTask	Logs events related to the ACF2 Resources scheduled task.
com.identityforge.util.acf2.tasks.ReconcileAllUsersTask	Logs events related to the ACF2 Reconcile All Users scheduled task.
com.identityforge.util.acf2.tasks.ReconcileUsersToInternalLdapTask	Logs events related to the ACF2 Reconcile Users to Internal LDAP scheduled task.

3.7 Configuring Trusted Source Reconciliation

Note: This section describes an optional procedure. Perform this procedure only if you want to configure CA ACF2 as a trusted source for identity data. By performing this procedure, you enable trusted source reconciliation for both full reconciliation runs and incremental reconciliation.

Section 4.1, "Performing Full Reconciliation" describe the remaining steps for configuring trusted source reconciliation.

The XML file for trusted source reconciliation, Acf2TrustedXellerateUser.xml, contains definitions of the connector components that are used for trusted source reconciliation. To import this XML file:

1. Open the Oracle Identity Manager Administrative and User Console.
2. If you are using Oracle Identity Manager Release 9.1.0.*x*, then:
   a. Click the **Deployment Management** link on the left navigation pane.
   b. Click the **Import** link under Deployment Management. A dialog box for opening files is displayed.
3. If you are using Oracle Identity Manager Release 11.1.1, then:
   a. On the Welcome page, click **Advanced** in the upper-right corner of the page.
   b. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Import Deployment Manager File**. A dialog box for opening files is displayed.

4. Locate and open the Acf2TrustedXellerateUser.xml file from the xml directory on the installation media. 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**.

3.8 Configuring Oracle Identity Manager for Request-Based Provisioning

Note: Perform the procedure described in this section only if you are using Oracle Identity Manager Release 11.1.1 and you want to configure request-based provisioning.

In request-based provisioning, an end user creates a request for a resource by using the Administrative and User Console. Administrators or other users can also create requests for a particular user. Requests for a particular resource on the resource can be viewed and approved by approvers designated in Oracle Identity Manager.

The following are features of request-based provisioning:

- A user can be provisioned only one resource (account) on the target system.

  Note: Direct provisioning allows the provisioning of multiple target system accounts on the target system.

- Direct provisioning cannot be used if you enable request-based provisioning.

To configure request-based provisioning, perform the following procedures:

- Section 3.8.1, "Copying Predefined Request Datasets"
- Section 3.8.2, "Importing Request Datasets into the MDS"
- Section 3.8.3, "Enabling the Auto Save Form Feature"
- Section 3.8.4, "Running the PurgeCache Utility"

3.8.1 Copying Predefined Request Datasets

A request dataset is an XML file that specifies the information to be submitted by the requester during a provisioning operation. Predefined request datasets are shipped with this connector. These request datasets specify information about the default set of attributes for which the requester must submit information during a request-based provisioning operation. The following predefined request datasets are available in the DataSets directory on the installation media:

ProvisionResource_OIMACF2ResourceObject.xml

ModifyResource_OIMACF2ResourceObject.xml

Copy these files from the installation media to any directory on the Oracle Identity Manager host computer. It is recommended that you create a directory structure as follows:

/custom/connector/*RESOURCE_NAME*

For example:

E:\MyDatasets\custom\connector\acf2Adv

> **Note:** Until you complete the procedure to configure request-based provisioning, ensure that there are no other files or directories inside the parent directory in which you create the directory structure. In the preceding example, ensure that there are no other files or directories inside the E:\MyDatasets directory.

The directory structure to which you copy the dataset files is the MDS location into which these files are imported after you run the Oracle Identity Manager MDS Import utility. The procedure to import dataset files is described in the next section.

Depending on your requirement, you can modify the file names of the request datasets. In addition, you can modify the information in the request datasets. See *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for information on modifying request datasets.

3.8.2 Importing Request Datasets into the MDS

All request datasets must be imported into the metadata store (MDS), which can be done by using the Oracle Identity Manager MDS Import utility.

To import a request dataset definition into MDS:

1. Ensure that you have set the environment for running the MDS Import utility. See *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for detailed information about setting up the environment for MDS utilities.

   > **Note:** While setting up the properties in the weblogic.properties file, ensure that the value of the metadata_from_loc property is the parent directory of the /custom/connector/*RESOURCE_NAME* directory. For example, while performing the procedure in Section 3.8.1, "Copying Predefined Request Datasets," if you copy the files to the E:\MyDatasets\custom\connector\acf2Adv directory, then set the value of the metada_from_loc property to `E:\MyDatasets`.

2. In a command window, change to the *OIM_HOME*\server\bin directory.
3. Run one of the following commands:
   - On Microsoft Windows

     ```
     weblogicImportMetadata.bat
     ```

   - On UNIX

     ```
     weblogicImportMetadata.sh
     ```

4. When prompted, enter the following values:
   - `Please enter your username [weblogic]`

     Enter the username used to log in to the WebLogic server

     Sample value: `WL_User`

- `Please enter your password [weblogic]`

  Enter the password used to log in to the WebLogic server.

- `Please enter your server URL [t3://localhost:7001]`

  Enter the URL of the application server in the following format:

  `t3://`*`HOST_NAME_IP_ADDRESS`*`:`*`PORT`*

  In this format, replace:

  – *HOST_NAME_IP_ADDRESS* with the host name or IP address of the computer on which Oracle Identity Manager is installed.

  – *PORT* with the port on which Oracle Identity Manager is listening.

The request dataset is imported into MDS at the following location:

/custom/connector/*RESOURCE_NAME*

3.8.3 Enabling the Auto Save Form Feature

To enable the Auto Save Form feature:

1. Log in to the Design Console.
2. Expand **Process Management,** and then double-click **Process Definition.**
3. Search for and open the **OIMACF2ProvisioningProcess** process definition.
4. Select the **Auto Save Form** check box.
5. Click the **Save** icon.

3.8.4 Running the PurgeCache Utility

Run the PurgeCache utility to clear content belonging to the Metadata category from the server cache. See Section 3.6.1, "Clearing Content Related to Connector Resource Bundles from the Server Cache" for instructions.

The procedure to configure request-based provisioning ends with this step.

3.9 Installing and Configuring the LDAP Gateway

The IT resource contains connection information for Oracle Identity Manager to connect to the LDAP Gateway. The acf2.properties file is one of the components of the gateway. This file contains information used by the gateway to connect to the mainframe. Configuring the gateway involves setting values in the acf2.properties file and the other files that constitute the gateway.

Note: In addition to the following procedure, see Section 5.4, "Configuring the Connector for Provisioning to Multiple Installations of the Target System" if you want to configure the connector to work with multiple LPARs on the IBM z/OS system.

To install and configure the LDAP Gateway:

1. Extract the contents of the ldapgateway.zip file to a directory on the computer on which you want to install the LDAP Gateway. This ZIP file is in the etc/LDAP Gateway directory on the installation media.

Note: In this document, the location (and name) of the ldapgateway directory on the Oracle Identity Manager host computer is referred to as *LDAP_INSTALL_DIR*.

2. Copy the acf2-adv-agent-recon.jar andVOYAGER_ID.properties files from the lib directory on the installation media to the *LDAP_INSTALL_DIR*/etc directory.
3. In a text editor, open the *LDAP_INSTALL_DIR*/conf/acf2.properties file. Enter values for the properties listed in this file. Table 3–4 describes these properties.

Table 3–4 Properties in the acf2.properties File

Property	Description
agentPort	Enter the number of the port on the LDAP Gateway host computer from which the Reconciliation Agent sends messages.
configAttrs	If you create a custom attribute on the target system, then add the name of that attribute to the value of the _configAttrs_ property. These attributes assume NAME (VALUE) format. This step is mentioned in the following sections: Section 5.1, "Adding New Attributes for Target Resource Reconciliation" Section 5.2, "Adding New Attributes for Provisioning"
defaultDelete	Enter one of the following as the value of this property: Set `revoke` as the value 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 if you want the user to be deleted from the target system as the outcome of a Delete User provisioning operation. For example: `# DEFAULT ACTION WHEN DELETE FUNCTION USED` `_defaultDelete_=`**`delete`**
host	Set the host name or IP address of the mainframe as the value of this property.
uidNumberBefore	Set this to "true" if using standard ACF2 header definition that has the UID NUMBER located before the NAME field. (true | false)
uidNumberLength	The length of the UID NUMBER. Default is 8 (LOGIN ID).
customListFormat	Used only for custom header attributes that have no attribute name and located after the NAME.
customListSpaces	Does custom header attribute contain spaces between value (true | false).
stcID	Set this to the Pioneer STC: This will allow to ignoreEvents that were already sent from Oracle Identity Manager.
port	Enter the number of the port on the mainframe that you are going to reserve for the provisioning agent. The LDAP Gateway will send provisioning messages to this port.
internalEnt	Enter one of the following as the value of this property: ■ Set true as the value of this property if you want the LDAP Gateway to use the internal LDAP store. ■ Set false as the value of this property if you do not want the LDAP Gateway to use the internal LDAP store.

4. Save and close the acf2.properties file.

5. Open the *LDAP_INSTALL_DIR*/etc/VOYAGER_ID.properties file and set a value for the following property:

   - _itResource_

     Enter the name of the IT resource that you define by performing the procedure described in Section 3.5, "Configuring the IT Resource."

   - _xlAdminId_

     Use the xlAdminId property to specify the user ID of a user belonging to the SYSTEM ADMINISTRATORS group.

   - _xlAdminPwd_

     Use the xlAdminPwd property to specify the password of the user whose user ID you specify as the value of the xlAdminId property. This property is used only on Oracle Identity Manager Release 11.1.1. If required, you can encrypt the password for security purposes. You can use the propertyEncrypt script to encrypt passwords. This script is in the scripts directory on the installation media. The procedure to use the script is given in Step 6. After you run the script, copy the encrypted password as the value of the xlAdminPwd property.

   - _xlAdminPwdEncrypt_

     Enter `true` as the value of the xlAdminPwdEncrypt property if you have set an encrypted password as the value of the xlAdminPwd property. Otherwise, enter `false`. This property is used only on Oracle Identity Manager Release 11.1.1.

   - _xlJndiUrl_

     This property is used only on Oracle Identity Manager Release 11.1.1.

     To determine the JNDI URL:

     a. In a text editor, open the following file:

        OIM_DC_HOME/xlclient/Config/xlconfig.xml

        Here, *OIM_DC_HOME* is the name and full path of the directory in which you install the Oracle Identity Manager Design Console.

     b. Copy the value of the java.naming.provider.url element.

     c. Set the value for the xlJndiUrl property.

     Sample value: `t3://localhost:14000/oim`

   - _xlJndiFactory_

     The default value is `weblogic.jndi.WLInitialContextFactory`. Do not change this default value. This property is used only on Oracle Identity Manager Release 11.1.1.

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:

   - **LDAP Gateway user credentials**

     You use the beans.xml file to store the credentials of the account used by Oracle Identity Manager to connect to the LDAP Gateway. You also enter these credentials as parameters of the IT resource. During provisioning and reconciliation, credentials passed through the IT resource are authenticated against the credentials stored in the beans.xml file. The LDAP Gateway

exchanges data with the other connector components only after this authentication succeeds.

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 values that you specify in the IT resource parameters.

You enter the credentials of the LDAP Gateway user in the following lines of the beans.xml file:

```
<property name="adminUserDN" value="cn=idfAcf2Admin,dc=acf2,dc=com"/>
<property name="adminUserPassword" value="idfAcf2Pwd"/>
```

In the first line, replace the sample value **cn=idfAcf2Admin,dc=acf2,dc=com** with the value that you set for the idfPrincipalDn parameter of the IT resource. In the second line, replace the sample value **idfAcf2Pwd** with the value that you set for the idfPrincipalPwd parameter of the IT resource. Table 3–2, " IT Resource Parameters" describes both parameters. If you want to encrypt the password before you enter it in the beans.xml file, then:

Note: It is optional to encrypt the password that you set in the beans.xml file. However, it is recommended that you encrypt the password for security reasons.

You must enter the unencrypted password as the value of the idfPrincipalPwd IT resource parameter. This is regardless of whether you enter the encrypted password in the beans.xml file.

a. In a text editor, copy one of the following script files from the installation media into a temporary directory and then open the script file in a text editor:

For Microsoft Windows:

```
/scripts/propertyEncrypt.bat
```

For UNIX:

```
/scripts/propertyEncrypt.sh
```

b. Specify values for the following properties in the file:

SET CLASSPATH=*DIRECTORY_LOCATION*\idfserver.jar

Replace *DIRECTORY_LOCATION* with the full path of the directory into which you copied the idfserver.jar file while deploying the connector.

For example:

```
SET CLASSPATH=C:\software\ldapgateway\dist\idfserver.jar
```

%JAVACMD% %JVM_OPTS% -cp %CLASSPATH%
com.identityforge.idfserver.util.AESCipherUtil *PLAINTEXT_PASSWORD*

Replace *PLAINTEXT_PASSWORD* with the password that you want to encrypt.

For example:

```
%JAVACMD%  %JVM_OPTS%  -cp %CLASSPATH%
```

```
com.identityforge.idfserver.util.AESCipherUtil idfAcf2Pwd
```

c. Save the changes made to the propertyEncrypt.bat or propertyEncrypt.sh script.

d. Run the script.

The script encrypts the password that you provide and displays it in the command window.

e. In the beans.xml file, search for the following string:

```
<property name="adminUserPassword"
```

f. Replace the value of this property with the encrypted password.

For example:

```
<property name="adminUserPassword"
value="468018DD1CDBE82E515EBF78A41C428E"/>
```

- **Port used for communication between the LDAP Gateway and the mainframe LPAR on which you install the Reconciliation and Provisioning Agents**

Note: The procedure to install the Reconciliation and Provisioning Agents is described in the next chapter.

As shown in the following line, the default value of the port property is `5389` in the beans.xml file. You can change this default value to any port of your choice.

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

Note: The port number must be the same as the port number that you specify as the value of the idfServerPort IT resource parameter. See Table 3–2, " IT Resource Parameters" for more information.

7. To enable logging for the LDAP Gateway:

a. Copy the log4j JAR file from the application server directory in which it is placed to the *LDAP_INSTALL_DIR*/lib directory.

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

c. Enter a log level as the value of the log4j.rootLogger variable. For example:

```
log4j.rootLogger=ERROR, A1
```

d. Save and close the file.

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

- idfserver.log.0: This is the main log file.
- acf2-agent-recon.log: This is the real-time, incremental reconciliation log file that stores Oracle Identity Manager reconciliation messages.

8. To configure the SSL in the LDAP Gateway:

   a. Edit the /ldapgateway/idfserver.jar beans.xml directory for the following:

```
<bean id="sslChannelFactory"
class="com.identityforge.idfserver.nio.ssl.SSLChannelFactory">
<constructor-arg><value>false</value></constructor-arg>
<constructor-arg><value>./conf/idf.jks</value></constructor-arg>
<constructor-arg><value>abc123</value></constructor-arg>
<constructor-arg><value>false</value></constructor-arg>
</bean>
```

   The first argument indicates we are not in client mode.

   Note: Do not change this argument.

   The second argument is the path to the keystore. Either change this path to your keystore or add your certificate to this keystore.

   The third argument is the keystore password that you used to generate your keystore.

   b. Edit a listener using the SSLChannelFactory for only "port", which is the only item you can change in the listener:

```
<bean id="sslListener" class="com.identityforge.idfserver.nio.Listener">
constructor-arg><ref bean="bus"/></constructor-arg>
<constructor-arg><ref bean="sslChannelFactory"/></constructor-arg>
<property name="admin"><value>false</value></property>
<property name="config"><value>./conf/listener.xml</value></property>
<property name="port" value="7389"/>
<property name="threadName" value="SSLLDAPListener"/>
</bean>
```

   c. Add the listener to the server by uncommenting the following line:

```
<bean id="server" class="com.identityforge.idfserver.Server">
<property name="tasks">
<list>
<ref bean="bus"/>
<ref bean="decoder"/>
<ref bean="listener"/>
<!-- <ref bean="sslListener"/>  ? <!-- added here -->
<ref bean="client"/>
<ref bean="protocol"/>
<ref bean="encoder"/>
<ref bean="output"/>
</list>
</property>
<property name="nexus" ref="nexus"/>
<property name="logPath" value="../logs/idfserver.log"/>
</bean>
```

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

10. To configure the LDAP Gateway for the application server that Oracle Identity Manager is running on:

    a. In a text editor, open the run script from the *LDAP_INSTALL_DIR*/bin directory.

b. In the run script, uncomment the lines related to the 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 instructions given in this step apply to Oracle Identity Manager Release 9.1.0.*x*. For Oracle Identity Manager Release 11.1.1, follow the instructions given in the run script itself. Remove un-needed # commented lines in the file and make sure .sh file CP is contained in double quotes " "

```
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 enable the connector to work with JBoss Application Server, uncomment the line for that application server as follows:

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

c. 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 follows:

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

11. In the run script, set the JAVA_HOME property as follows:

```
JAVA_HOME=DIRECTORY_LOCATION\jdk1.5.0_22
```

Replace *DIRECTORY_LOCATION* with the full path of the directory.

12. Save and close the run script.

Starting and Stopping the LDAP Gateway

To start the LDAP Gateway on UNIX, run the following command:

bin> ./run.sh

To stop the LDAP Gateway on UNIX, run the following command:

bin> ./stop_idf.sh

To start the LDAP Gateway on Microsoft Windows, run the run.bat file.

To stop the LDAP Gateway on Microsoft Windows, close the command window in which the gateway is running.

4

Configuring the Connector

This chapter discusses the following topics:

- Section 4.1, "Performing Full Reconciliation"
- Section 4.2, "Configuring Account Status Reconciliation"
- Section 4.3, "Configuring Filtered Reconciliation to Multiple Resource Objects"
- Section 4.4, "Guidelines on Using the Connector"
- Section 4.5, "Performing Provisioning Operations"
- Section 4.6, "Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1"
- Section 4.7, "Configuring Resource and Access Rule Pre-Population Scheduled Tasks"

4.1 Performing Full Reconciliation

The ACF2 Reconcile All Users scheduled task performs full reconciliation. When you configure this scheduled task, it runs at specified intervals and fetches create and modify events on the target system for reconciliation.

To configure the Reconcile All Users scheduled task:

1. Log in to the Oracle Identity Manager Administrative and User Console.
2. Perform one of the following steps.
   a. If you are using Oracle Identity Manager Release 9.1.0.*x*, expand **Resource Management**, and then click **Manage Scheduled Task**.
   b. If you are using Oracle Identity Manager Release 11.1.1, then on the Welcome to Oracle Identity Manager Self Service page, click **Advanced** in the upper-right corner of the page.
3. Search for and open the scheduled task as follows:

   If you are using Oracle Identity Manager Release 9.1.0.*x*, then:

   a. On the Scheduled Task Management page, enter the name of the scheduled task as the search criteria and then click **Search**.
   b. In the search results table, click **Edit** the edit column for the scheduled task.\
   c. On the Scheduled Task Details page, where the details of the scheduled task that you selected are displayed, click **Edit**.

   If you are using Oracle Identity Manager Release 11.1.1, then:

a. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Search Scheduled Jobs**.

b. On the left pane, in the Search field, enter the name of the scheduled job as the search criterion. Alternatively, you can click **Advanced Search** and specify the search criterion.

c. In the search results table on the left pane, click the **scheduled job** in the Job Name column.

4. Modify the details of the scheduled task as follows:

a. If you are using Oracle Identity Manager Release 9.1.0.*x*, then on the Edit Scheduled Task Details page, modify the following parameters, and then click **Continue**:

Status: Specify whether you want to leave the task in the enabled state. In the enabled state, the task is ready for use.

Max Retries: Enter an integer value in this field. This number represents the number of times Oracle Identity Manager must attempt to complete the task before assigning the ERROR status to the task. The default value is 0.

Next Start: Use the date editor to specify the date when you want the task to run. After you select a date value in the date editor, you can modify the time value that is automatically displayed in the Next Start field.

Frequency: Specify the frequency at which you want the task to run.

b. If you are using Oracle Identity Manager Release 11.1.1, then on the Job Details tab, you can modify the following parameters:

Retries: Enter an integer value in this field. This number represents the number of times the scheduler tries to start the job before assigning the Stopped status to the job.

Schedule Type: Depending on the frequency at which you want the job to run, select the appropriate schedule type.

See Also: *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager* for detailed information about schedule types

In addition to modifying the job details, you can enable or disable a job.

5. Specify values for the attributes of the scheduled task as follows:

Note: Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.

- If you are using Oracle Identity Manager Release 9.1.0.*x*, then on the Attributes page, select the attribute from the Attribute list, specify a value in the field provided, and then click **Update**.
- If you are using Oracle Identity Manager Release 11.1.1, then on the Job Details tab, in the Parameters region, specify values for the attributes of the scheduled task. Table 4–1 describes the attributes of the scheduled task.

Table 4–1 Attributes of the Reconcile All Users Scheduled Task

Attribute	Description
IT Resource	Enter the name of the IT resource that was configured for the target system. Sample value: `Acf2Resource`
Resource Object	Enter the name of the resource object against which reconciliation runs must be performed. Sample value: `OIMAcf2ResourceObject`
Trusted Resource Object	Enter the name of the resource object against which trusted reconciliation runs must be performed. Sample value: `Xellerate User`
MultiValuedAttributes	Enter a comma-separated list of multi-valued attributes that you want to reconcile. Do not include a space after each comma. Sample value: `attributes,memberOf`
SingleValueAttributes	Enter a comma-separated list of single-valued attributes that you want to reconcile. Do not include a space after each comma. Do not include attributes already listed in the MultiValueAttributes field. Sample value: `uid,owner,defaultGroup,waddr1,tsoMaxSize` **Note:** By default, Oracle Identity Manager's design form only allows entering up to 150 characters in a text field. To increase this limit, change the value of the TSA_VALUE column in the Oracle Identity Manager database.
TrustedReconciliation	Enter whether the target system should be treated as a trusted source. Sample value: `true`
UsersList	Enter a comma-separated list of user IDs to be reconciled. **Note:** This field is optional. If no user IDs are listed, then full reconciliation will be performed. Sample value: `testusr1,testusr2,testusr3`

6. After specifying the attributes, perform one of the following steps:

   a. If you are using Oracle Identity Manager Release 9.1.0.*x,* then click **Save Changes** to save the changes.

   Note: The Stop Execution option is not available in the *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*. If you want to stop a task, then click Stop Execution on the Task Scheduler form of the Design Console.

   b. If you are using Oracle Identity Manager Release 11.1.1, then click **Apply** to save the changes.

   Note: The Stop Execution option is available in the *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*. You can use the Scheduler Status page to either start, stop, or re-initialize the scheduler.

4.2 Configuring Account Status Reconciliation

Note: This section describes an optional procedure. Perform this procedure only if you want to enable reconciliation of user status changes on CA ACF2.

When a user is disabled or enabled on the target system, the status of the user can be reconciled into Oracle Identity Manager. To configure reconciliation of user status changes made on CA ACF2:

1. In the *LDAP_INSTALL_DIR*/etc/VOYAGER_ID.properties file, add the name of the Status field to the reconAttrs section.
2. Restart the LDAP Gateway for the changes to take effect.
3. In the Design Console:

   See Also: *Oracle Fusion Middleware User's Guide for Oracle Identity Manager* for detailed information about the following steps

   - In the OIMAcf2ResourceObject resource object, create the Status reconciliation field.
   - In the OIMAcf2ProvisioningProcess process definition, map the field for the Status field to the OIM_OBJECT_STATUS field.

4.3 Configuring Filtered Reconciliation to Multiple Resource Objects

You might have created multiple resource objects to represent multiple user types in your organization. You use the Resource Object property of the Reconcile All Users scheduled task to specify the resource object that you want to use during reconciliation. You can enter more than one resource object in the value of the Resource Object property. In addition, you can include CA ACF2 attribute-value pairs to filter records for each resource object.

See Also: Section 4.1, "Performing Full Reconciliation" for information about the Reconcile All Users scheduled task

The following is a sample format of the value for the Resource Object property:

```
(ATTRIBUTE1:VALUE1)RESOURCE_OBJECT1,RESOURCE_OBJECT2
```

As shown in the sample format, specifying a filter attribute is optional, but if more than one resource object is specified, you must specify a filter for each additional resource object. If you do not specify a filter attribute, then all records are reconciled to the first resource object. Further, the filters are checked in order, so the resource object without a filter attribute should be included last in the list.

Filter attributes should be surrounded by parentheses.

Apply the following guidelines while specifying a value for the Object property:

- The names of the resource objects must be the same as the names that you specified while creating the resource objects by using the Design Console.
- The CA ACF2 attribute names must be the same as the names used in the LDAP Gateway configuration files.

See Also: Section 3.9, "Installing and Configuring the LDAP Gateway" for information about the LDAP Gateway configuration files

- The value must be a regular expression as defined in the java.util.regex Java package. Note that the `find` methodology of the regex matcher is used rather than the `matches` methodology. This means that a substring matching rule can be specified in the pattern, rather than requiring the entire string matching rule.

  Further, substring matching is case-sensitive. A "(tso)" filter will not match a user with the user ID "TSOUSER1"

- Multiple values can be matched. Use a vertical bar (`|`) for a separator as shown in the following example:

  `(`*`ATTRIBUTE`*`:`*`VALUE1`*`|`*`VALUE2`*`|`*`VALUE3`*`)`*`RESOURCE_OBJECT`*

- Multiple filters can be applied to the attribute and to the same resource object. For example:

  `(`*`ATTRIBUTE1`*`:`*`VALUE1`*`)&(`*`ATTRIBUTE2`*`:`*`VALUE2`*`)`*`RESOURCE_OBJECT`*

The following is a sample value for the Object property:

```
(tsoProc:X)ACF2R01,(active:value1|value2|value3)ACF2ResourceObject2,(tso)ACF2Resou
rceObject24000,Resource
```

In this sample value:

- `(tsoProc:X)ACF2RO1` represents a user with `X` as the attribute value for the TSO Proc segment. Records that meet this criterion are reconciled with the ACF2RO1 resource object.
- `(active:value1|value2|value3)ACF2ResourceObject2` represents a user with `value1`, `value2`, or `value3` as their active date. Records that meet this criterion are reconciled with the ACF2ResourceObject2 resource object.
- `(tso)ACF2ResourceObject24000` represents a user with TSO privileges. A TSO attribute value is not specified. Records that meet this criterion are reconciled with the ACF2ResourceObject24000 resource object.
- All other records are reconciled with the Resource resource object.

4.4 Guidelines on Using the Connector

Apply the following guidelines while using the connector:

- The subpool and the LDAP Gateway must be started before starting the Reconciliation Agent. If the LDAP Gateway is not available when the Reconciliation Agent is started, then an error is generated with `RETCODE=-01` and `ERRORNO=61`.
- The 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. To avoid errors of this type, 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. Keep in mind these requirements when you create or modify target system user profiles through provisioning operations on Oracle Identity Manager.
- The following guideline applies only to a configuration in which a single LDAP Gateway connects to multiple installations of the target system:

  If you configure the connector for trusted source reconciliation and set the idfTrusted property in the Reconcile All Users scheduled task 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.

4.5 Performing Provisioning Operations

Provisioning involves creating or modifying a user's account information on the target system through Oracle Identity Manager.

This section discusses the following topics related to configuring provisioning:

4.5.1 Provisioning Users

Provisioning a resource for an OIM User involves using Oracle Identity Manager to create a target system account for the user.

When you install the connector on Oracle Identity Manager Release 11.1.1, the direct provisioning feature is automatically enabled. This means that the process form is enabled when you install the connector.

If you have configured the connector for request-based provisioning, then the process form is suppressed and the object form is displayed. In other words, direct provisioning is disabled when you configure the connector for request-based provisioning. If you want to revert to direct provisioning, then perform the steps described in Section 4.6, "Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1."

This following are types of provisioning operations:

- Direct provisioning
- Request-based provisioning
- Provisioning triggered by policy changes

> **See Also:** *Oracle Fusion Middleware User's Guide for Oracle Identity Manager* for information about the types of provisioning

This section discusses the following topics:

- Section 4.5.1.1, "Direct Provisioning"
- Section 4.5.1.2, "Request-Based Provisioning"

4.5.1.1 Direct Provisioning

To provision a resource by using the direct provisioning approach:

1. Log in to the Administrative and User Console.

2. If you want to first create an OIM User and then provision a target system account, then:
   - If you are using Oracle Identity Manager Release 9.1.0.*x*, then:
     - From the Users menu, select **Create**.
     - On the Create User page, enter values for the OIM User fields and then click **Create User**.
   - If you are using Oracle Identity Manager Release 11.1.1, then:
     - On the Welcome to Identity Administration page, in the Users region, click **Create User**.
     - On the Create User page, enter values for the OIM User fields, and then click Save.
3. If you want to provision a target system account to an existing OIM User, then:
   - If you are using Oracle Identity Manager Release 9.1.0.*x*, then:
     - From the Users menu, select **Manage**.
     - Search for the OIM User and select the link for the user from the list of users displayed in the search results.
   - If you are using Oracle Identity Manager Release 11.1.1, then:
     - On the Welcome to Identity Administration page, search for the OIM User by selecting **Users** from the list on the left pane.
     - From the list of users displayed in the search results, select the OIM User. The user details page is displayed on the right pane.
4. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - If you are using Oracle Identity Manager Release 9.1.0.*x*, then:
     - On the User Detail page, select **Resource Profile** from the list at the top of the page.
     - On the Resource Profile page, click **Provision New Resource**.
   - If you are using Oracle Identity Manager Release 11.1.1, then:
     - On the user details page, click the **Resources** tab.
     - From the Action menu, select **Add Resource**. Alternatively, you can click the add resource icon with the plus (+) sign. The Provision Resource to User page is displayed in a new window.
5. On the Step 1: Select a Resource page, select **OIMACF2ResourceObject** from the list and then click **Continue**.
6. On the Step 2: Verify Resource Selection page, click **Continue**.
7. On the Step 5: Provide Process Data for ACF2 Advanced Details page, enter the details of the account that you want to create on the target system and then click **Continue**.
8. On the Step 6: Verify Process Data page, verify the data that you have provided and then click **Continue**.
9. The "Provisioning has been initiated" message is displayed. Perform one of the following steps:

- If you are using Oracle Identity Manager Release 9.1.0.*x*, click **Back to User Resource Profile.** The Resource Profile page shows that the resource has been provisioned to the user.
- If you are using Oracle Identity Manager Release 11.1.1, then:
  - Close the window displaying the "Provisioning has been initiated" message.
  - On the Resources tab, click **Refresh** to view the newly provisioned resource.

4.5.1.2 Request-Based Provisioning

Note: The information provided in this section is applicable only if you are using Oracle Identity Manager Release 11.1.1.

A request-based provisioning operation involves both end users and approvers. Typically, these approvers are in the management chain of the requesters. The following sections discuss the steps to be performed by end users and approvers during a request-based provisioning operation:

Note: The procedures described in these sections are built on an example in which the end user raises or creates a request for provisioning a target system account. This request is then approved by the approver.

- Section 4.5.1.2.1, "End User's Role in Request-Based Provisioning"
- Section 4.5.1.2.2, "Approver's Role in Request-Based Provisioning"

4.5.1.2.1 End User's Role in Request-Based Provisioning

The following steps are performed by the end user in a request-based provisioning operation:

See Also: *Oracle Fusion Middleware User's Guide for Oracle Identity Manager* for detailed information about these steps

1. Log in to the Administrative and User Console.
2. On the Welcome page, click **Advanced** in the upper-right corner of the page.
3. On the Welcome to Identity Administration page, click the **Administration** tab, and then click the **Requests** tab.
4. From the Actions menu on the left pane, select **Create Request**.

   The Select Request Template page is displayed.
5. From the Request Template list, select **Provision Resource** and click **Next**.
6. On the Select Users page, specify a search criterion in the fields to search for the user that you want to provision the resource, and then click **Search**. A list of users that match the search criterion you specify is displayed in the Available Users list.
7. From the **Available Users** list, select the user to whom you want to provision the account.

If you want to create a provisioning request for more than one user, then from the **Available Users** list, select users to whom you want to provision the account.

8. Click **Move** or **Move All** to include your selection in the Selected Users list, and then click **Next**.
9. On the Select Resources page, click the arrow button next to the Resource Name field to display the list of all available resources.
10. From the Available Resources list, select **OIMACF2ResourceObject**, move it to the Selected Resources list, and then click **Next**.
11. On the Resource Details page, enter details of the account that must be created on the target system, and then click **Next**.
12. On the Justification page, you can specify values for the following fields, and then click **Finish**.
    - Effective Date
    - Justification

    On the resulting page, a message confirming that your request has been sent successfully is displayed along with the Request ID.
13. If you click the request ID, then the Request Details page is displayed.
14. To view details of the approval, on the Request Details page, click the **Request History** tab.

4.5.1.2.2 Approver's Role in Request-Based Provisioning

The following are steps performed by the approver in a request-based provisioning operation:

The following are steps that the approver can perform:

1. Log in to the Administrative and User Console.
2. On the Welcome page, click **Self-Service** in the upper-right corner of the page.
3. On the Welcome to Identity Manager Self Service page, click the **Tasks** tab.
4. On the **Approvals** tab, in the first section, you can specify a search criterion for request task that is assigned to you.
5. From the search results table, select the row containing the request you want to approve, and then click **Approve Task**.

   A message confirming that the task was approved is displayed.

4.6 Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1

Note: It is assumed that you have performed the procedure described in Section 3.8, "Configuring Oracle Identity Manager for Request-Based Provisioning."

On Oracle Identity Manager Release 11.1.1, if you want to switch from request-based provisioning to direct provisioning, then:

1. Log in to the Design Console.

2. Disable the Auto Save Form feature as follows:
   a. Expand **Process Management**, and then double-click **Process Definition**.
   b. Search for and open the **OIMACF2ProvisioningProcess** process definition.
   c. Deselect the Auto Save Form check box.
   d. Click the **Save** icon.
3. If the Self Request Allowed feature is enabled, then:
   a. Expand **Resource Management**, and then double-click **Resource Objects**.
   b. Search for and open the **OIMAcf2ResourceObject** resource object.
   c. Deselect the **Self Request Allowed** check box.
   d. Click the **Save** icon.

On Oracle Identity Manager Release 11.1.1, if you want to switch from direct provisioning back to request-based provisioning, then:

1. Log in to the Design Console.
2. Enable the Auto Save Form feature as follows:
   a. Expand **Process Management**, and then double-click **Process Definition**.
   b. Search for and open the **OIMAcf2ProvisioningProcess** process definition.
   c. Select the **Auto Save Form** check box.
   d. Click the **Save** icon.
3. If you want to enable end users to raise requests for themselves, then:
   a. Expand **Resource Management**, and then double-click **Resource Objects**.
   b. Search for and open the **OIMAcf2ResourceObject** resource object.
   c. Select the Self Request Allowed check box.
   d. Click the **Save** icon.

4.7 Configuring Resource and Access Rule Pre-Population Scheduled Tasks

The FindAllAccessRules and FindAllResourceRules scheduled tasks populate lookup tables with resource or access rule keys that can be assigned during user provisioning. When you configure these scheduled tasks, they run at specified intervals and fetch a listing of all resource or access keys on the target system for reconciliation.

To configure the FindAllAccessRules or FindAllResourceRules scheduled task:

1. Log in to Oracle Identity Manager Administrative and User Console.
2. Perform one of the following steps:
   a. If you are using Oracle Identity Manager Release 9.1.0.*x*, expand **Resource Management**, and then click **Manage Scheduled Task**.
   b. If you are using Oracle Identity Manager Release 11.1.1, then on the Welcome to Oracle Identity Manager Self Service page, click **Advanced** in the upper-right corner of the page.
3. Search for and open the scheduled task as follows:

If you are using Oracle Identity Manager Release 9.1.0.*x*, then:

a. On the Scheduled Task Management page, enter the name of the scheduled task as the search criteria and then click **Search**.

b. In the search results table, click **Edit** the edit column for the scheduled task.

c. On the Scheduled Task Details page, where the details of the scheduled task that you selected are displayed, click **Edit**.

If you are using Oracle Identity Manager Release 11.1.1, then:

a. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Search Scheduled Jobs**.

b. On the left pane, in the Search field, enter the name of the scheduled job as the search criterion. Alternatively, you can click **Advanced Search** and specify the search criterion.

c. In the search results table on the left pane, click the scheduled job in the Job Name column.

4. Modify the details of the scheduled task as follows:

a. If you are using Oracle Identity Manager Release 9.1.0.*x*, then on the Edit Scheduled Task Details page, modify the following parameters, and then click **Continue**:

Status: Specify whether you want to leave the task in the enabled state. In the enabled state, the task is ready for use.

Max Retries: Enter an integer value in this field. This number represents the number of times Oracle Identity Manager must attempt to complete the task before assigning the ERROR status to the task. The default value is 0.

Next Start: Use the date editor to specify the date when you want the task to run. After you select a date value in the date editor, you can modify the time value that is automatically displayed in the Next Start field.

Frequency: Specify the frequency at which you want the task to run.

b. If you are using Oracle Identity Manager Release 11.1.1, then on the Job Details tab, you can modify the following parameters:

Retries: Enter an integer value in this field. This number represents the number of times the scheduler tries to start the job before assigning the Stopped status to the job.

Schedule Type: Depending on the frequency at which you want the job to run, select the appropriate schedule type.

See Also: *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager* for detailed information about schedule types

In addition to modifying the job details, you can enable or disable a job.

5. Specify values for the attributes of the scheduled task as follows:

Note: Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.

If you are using Oracle Identity Manager Release 9.1.0.*x*, then on the Attributes page, select the attribute from the Attribute list, specify a value in the field provided, and then click **Update**.

If you are using Oracle Identity Manager Release 11.1.1, then on the Job Details tab, in the Parameters region, specify values for the attributes of the scheduled task. Table 4–2 describes the attributes of the scheduled task.

Table 4–2 Attributes of the FindAllAccessRules and FindAllResourceRules Scheduled Tasks

Attribute	Description
IT Resource	Enter the name of the IT resource that was configured for the target system. Sample value: `Acf2Resource`
Resource Object	Enter the name of the resource object against which provisioning runs must be performed. Sample value: `OIMAcf2ResourceObject`
Lookup Code Name	Enter the name of the lookup code where OIM will store the names of any resources to which the user belongs. Sample value: `Lookup.Users.ResourceMemberships`
Recon Type	Enter "Append" or "Replace". This attribute determines whether located memberships should be appended to the lookup, or replace the lookup values. If set to "Replace", existing lookup code values will be deleted. Sample value: `Append`

6. After specifying the attributes, perform one of the following steps:

   a. If you are using Oracle Identity Manager Release 9.1.0.*x*, then click **Save Changes** to save the changes.

   Note: The Stop Execution option is not available in the *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*. If you want to stop a task, then click Stop Execution on the Task Scheduler form of the Design Console.

   b. If you are using Oracle Identity Manager Release 11.1.1, then click **Apply** to save the changes.

   Note: The Stop Execution option is available in the *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*. You can use the Scheduler Status page to start, stop, or reinitialize the scheduler.

5

Extending the Functionality of the Connector

This chapter discusses the following optional procedures that you can perform to extend the functionality of the connector for addressing your business requirements:

- Section 5.1, "Adding New Attributes for Target Resource Reconciliation"
- Section 5.2, "Adding New Attributes for Provisioning"
- Section 5.3, "Removing Attributes Mapped for Target Resource Reconciliation and Provisioning"
- Section 5.4, "Configuring the Connector for Provisioning to Multiple Installations of the Target System"
- Section 5.5, "Configuring the Connector for Reconciliation of Multiple Installations of the Target System"
- Section 5.6, "Reconciling Deleted Users to Oracle Identity Manager"
- Section 5.7, "Reconciling Users to the Internal LDAP"
- Section 5.8, "Reconciling Internal LDAP Users to Oracle Identity Manager"

5.1 Adding New Attributes for Target Resource Reconciliation

Note: You must ensure that new attributes you add for reconciliation contain only string-format data. Binary attributes must not be brought into Oracle Identity Manager natively.

By default, the attributes listed in Table 1–3 are mapped for reconciliation between Oracle Identity Manager and the target system. If required, you can add new attributes for target resource reconciliation.

For real-time/incremental reconciliation, the reconAttrs property contains the list of target system attributes that are mapped for real-time reconciliation with Oracle Identity Manager. This property found in the VOYAGER_ID.properties file. Attributes mapped for reconciliation are listed as the value of the reconAttrs property. If you want to add an attribute for reconciliation, then copy it from the "removed" list to the list in the reconAttrs property.

For full reconciliation, the reconciliation scheduled task contains two sections: SingleValueAttributes and MultiValuedAttributes. Attributes that can have multiple values (such as MEMBER_OF containing multiple group names) should be entered as a comma-separated list in the MultiValuedAttributes property. All other attributes should be entered in the SingleValueAttributes property. Attributes entered in the

MultiValuedAttributes property should not be included in the SingleValueAttributes property and vice versa.

If you are adding a custom target system attribute, then you must also add it to the list of attributes specified as the value of the configAttrs property in the acf2.properties file. See Section 3.9, "Installing and Configuring the LDAP Gateway" for information about this property.

5.2 Adding New Attributes for Provisioning

By default, the attributes listed in Table 1–3 are mapped for provisioning between Oracle Identity Manager and the target system. If required, you can map additional attributes for provisioning.

To add a new attribute for provisioning:

> **See Also:** *Oracle Fusion Middleware User's Guide for Oracle Identity Manager* for detailed information about these steps

1. Log in to the Oracle Identity Manager Design Console.
2. Add the new attribute on the process form as follows:
   a. Expand **Development Tools**.
   b. Double-click **Form Designer.**
   c. Search for and open the **UD_IDF_ACF2** process form.
   d. Click **Create New Version**, and then click **Add**.
   e. Enter the details of the attribute.
   f. Click Save and then click **Make Version Active.**
3. Create an entry for the attribute in the lookup definition for provisioning as follows:
   a. Expand **Administration**.
   b. Double-click **Lookup Definition.**
   c. Search for and open the **AtMap.ACF2** lookup definition.
   d. Click **Add** and then enter the Code Key and Decode values for the attribute.

      The Code Key value must be the name of the field on the process form. The Decode value is the name of the attribute on the target system.
4. To enable update of the attribute during provisioning operations, create a process task as follows:

   > **See Also:** *Oracle Fusion Middleware User's Guide for Oracle Identity Manager* for detailed information about these steps

   a. Expand **Process Management**, and double-click **Process Definition**.
   b. Search for and open the **OIMAcf2ProvisioningProcess** process definition.
   c. Click **Add**.
   d. On the General tab of the Creating New Task dialog box, enter a name and description for the task and then select the following:

      Conditional

Required for Completion

Allow Cancellation while Pending

Allow Multiple Instances

e. Click Save.

f. On the Integration tab of the Creating New Task dialog box, click **Add**.

g. In the Handler Selection dialog box, select **Adapter**, click **adpMODIFYACF2USER**, and then click the **Save** icon.

The list of adapter variables is displayed on the Integration tab.

h. To create the mapping for the first adapter variable:

Double-click the number of the first row.

In the Edit Data Mapping for Variable dialog box, enter the following values:

Variable Name: Adapter return value

Data Type: Object

Map To: Response code

Click the **Save** icon

i. To create mappings for the remaining adapter variables, use the data given in the following table:

Variable Number	Variable Name	Map To	Qualifier
Second	idfResource	IT Resource	Not applicable
Third	uid	Process Data	LoginId
Fourth	attrName	Literal	`cn` string
Fifth	attrValue	Process Data	`UD_ACF2_ADV_NAME` string

j. Click the **Save** icon in the Editing Task dialog box, and then close the dialog box.

k. Click the **Save** icon to save changes to the process definition.

5. If you are adding a custom attribute, then add it to the list of attributes specified as the value of the configAttrs property in the Properties in the acf2.properties file. See Step 3 of Section 3.9, "Installing and Configuring the LDAP Gateway" for information about this property.

5.3 Removing Attributes Mapped for Target Resource Reconciliation and Provisioning

Note: You must not remove the uid, cn, sn, givenName, or userPassword attribute. These attributes are mandatory on the target system.

The reconAttrs property contains the list of target system attributes that are mapped for real-time reconciliation and provisioning. This property is found in the

VOYAGER_ID.properties file. If you want to remove an attribute mapped for real-time reconciliation and provisioning, then remove it from the reconAttrs property.

The SingleValueAttributes and MultiValuedAttributes properties contain the list of target system attributes that are mapped for initial reconciliation. These properties are found in the Reconcile All Users scheduled task. If you want to remove an attribute mapped for initial reconciliation, then remove it from the SingleValueAttributes or MultiValuedAttributes property.

5.4 Configuring the Connector for Provisioning to 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 all installations of the target system.

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

   See *Oracle Fusion Middleware User's Guide for Oracle Identity Manager* for information about creating IT resources. See Section 3.5, "Configuring the IT Resource" 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>
   ```

   When you change the port number, 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 beans.xml file.

6. Open the *LDAP_INSTALL_DIR*/conf/acf2.properties file and set values for the following parameters:
   - _agentPort_= Enter the port number for 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 CA ACF2 running on each server.

   - _host_= Enter the IP address or host name of the mainframe.
   - _port_= Enter the port number for the second instance of the Provisioning agent.
7. Save and close the acf2.properties file.
8. Open the *LDAP_INSTALL_DIR*/etc/VOYAGER_ID.properties file, and set a value for the following property:

   itResource: Enter the name of the IT resource for the second LDAP Gateway.
9. Save and close the VOYAGER_ID.properties file.
10. In a Linux or Solaris environment, if there are not enough socket file descriptors to open up all the ports needed for the server, then:
    a. In a text editor, open the run script from the *LDAP_INSTALL_DIR*/bin directory.
    b. Add the following line in the file:

       ```
       -Djava.nio.channels.spi.SelectorProvider=sun.nio.ch.PollSelectorProvider
       ```

    c. Save and close the file.

When you perform provisioning operations:

When you use the Administrative and User Console to perform provisioning, you can specify the IT resource corresponding to the CA ACF2 installation to which you want to provision the user.

5.5 Configuring the Connector for Reconciliation of Multiple Installations of the Target System

You can configure the connector for reconciling multiple installations of the target system. For each installation of the target system, you create a corresponding .properties file in the `/ldapgateway/etc/ directory`.

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

Note: Perform the same procedure for all installations of the target system.

1. Make of copy of the current LDAP_INSTALL_DIR/etc/.properties file, saving it in the /etc/ directory. The default name for this file is VOYAGER_ID.propeties; otherwise, select the .properties file whose name matches the VOYAGER_ID of the

target system you would like to configure for reconciliation. See Chapter 2, "Deploying the IdF Advanced Adapter for ACF2" for information about the VOYAGER_ID property.

2. Open the copied file and set a value for the following properties:
   - _itResource__= Enter the name of the IT resource.
   - _userStatus_ _= Enter either Provisioned or Enabled depending on the status that must be set for accounts that are created through target resource reconciliation.
   - _xlAdminId_ = Enter the user ID of a user belonging to the SYSTEM ADMINISTRATORS group.
   - _xlAdminPwdEncrypt_ = Enter the password of the user whose user ID you specified as the value of the xlAdminId property. This property is used only on Oracle Identity Manager Release 11.1.1. If required, you can encrypt the password for security purposes using the propertyEncrypt script located in the scripts directory of the installation media. The procedure to use the script is given in Section 3.9, "Installing and Configuring the LDAP Gateway". After you run the script, copy the encrypted password as the value of the xladminPwd property.
   - _xlAdminPwdEncrypt_ = Enter true as the value of the xlAdminPwdEncrypt property if you have set an encrypted password as the value of the xlAdminPwd property. Otherwise, enter false. This property is used only on Oracle Identity Manager Release 11.1.1.
   - _xlJndiUrl_ = This property is only used on Oracle Identity Manager Release 11.1.1.
3. To determine the JNDI URL:

   In a text editor, open the following file:

   OIM_DR_HOME/xlclient/Config/xlconfig.xml

   Here, OIM_DC_HOME is the name and full path of the directory in which you install the Oracle Identity Manager Design Console.
   - Copy the value of the java.naming.provider.url element. Set the value for the xlJndiUrl property, Sample value: t3://localhost:14000/oim.
   - _xlJndiFactory_ = The default value is weblogic.jndi.WLInitialContextFactory. Do not change this default value. This property is used only on Oracle Identity Manager Release 11.1.1.
4. The Voyager reconciliation agent sends a unique identifier value, called VOYAGER_ID, each time a reconciliation event occurs. This value must match the name of the .properties file being used by the acf2-adv-agent-recon.jar for reconciliation.

   Rename the copied field to match the VOYAGER_ID property. For example, if the target system has VOYAGER_ID = VOYAGER14, then the .properties file should be named VOYAGER14.properties.

5.6 Reconciling Deleted Users to Oracle Identity Manager

The ACF2 Deleted User Reconciliation to OIM scheduled task allows the administrator to reconcile deleted users from the target system to Oracle Identity Manager. When you configure this scheduled task, it runs at specified intervals and fetches a list of

users on the target system. These user names are then compared with provisioned users in Oracle Identity Manager. Any user profiles that exist within Oracle Identity Manager, but not in the target system, are deleted from Oracle Identity Manager.

To configure the Deleted User Reconciliation to OIM scheduled task:

1. Log in to the Oracle Identity Manager Administrative and User Console.
2. Perform one of the following steps:

   a.) If you are using Oracle Identity Manager Release 9.1.0.*x*, expand Resource Management, and then click **Manage Scheduled Task**.

   b.) If you are using Oracle Identity Manager Release 11.1.1, then on the Welcome to Oracle Identity Manager Self Service page, click **Advanced** in the upper-right corner of the page.
3. Search for and open the scheduled task as follows:

   If you are using Oracle Identity Manager Release 9.1.0.*x*, then:

   a.) On the Scheduled Task Management page, enter the name of the scheduled task as the search criteria and then click **Search**.

   b.) In the search results table, click **Edit** column for the scheduled task.

   c.) On the Scheduled Task Details page, where the details of the scheduled task that you selected are displayed, click **Edit**.

   If you are using Oracle Identity Manager Release 11.1.1, then:

   a.) On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Search Scheduled Jobs**.

   b.) On the left pane, in the Search field, enter the name of the scheduled job as the search criterion. Alternatively, you can click **Advanced Search** and specify the search criterion.

   c.) In the search results table on the left pane, click the **scheduled job** in the Job Name column.
4. Modify the details of the scheduled task as follows:

   a.) If you are using Oracle Identity Manager Release 9.1.0.*x*, then on the Edit Scheduled Task Details page, modify the following parameters, and then click **Continue**:

   Status: Specify whether you want to leave the task in the enabled state. In the enabled state, the task is ready for use.

   Max Retries: Enter an integer value in this field. This number represents the number of times Oracle Identity Manager must attempt to complete the task before assigning the ERROR status to the task. The default value is 0.

   Next Start: Use the date editor to specify the date when you want the task to run. After you select a date value in the date editor, you can modify the time value that is automatically displayed in the Next Start field.

   Frequency: Specify the frequency at which you want the task to run.

   b.) If you are using Oracle Identity Manager Release 11.1.1, then on the Job Details tab, you can modify the following parameters:

   Retries: Enter an integer value in this field. This number represents the number of times the scheduler tries to start the job before assigning the Stopped status to the job.

Schedule Type: Depending on the frequency at which you want the job to run, select the appropriate schedule type.

Note: See *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager* for detailed information about schedule types.

In addition to modifying the job details, you can enable or disable a job.

5. Specify values for the attributes of the scheduled task as follows:

Note:
- Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.
- Values (either default or user-defined) must be assigned to all the attributes. If even a single attribute value is left empty, then reconciliation is not performed.

Table 5–1 describes the attributes of the scheduled task.

Table 5–1 Attributes of the Deleted User Reconciliation to OIM Scheduled Task

Attribute	Description
IT Resource	Enter the name of the IT resource that was configured for the target system. Sample value: `Acf2Resource`
Resource Object	Enter the name of the resource object against which the delete reconciliation runs must be performed. Sample value: `OIMAcf2ResourceObject`
Domain OU	Enter the name of the internally-configured directory in the LDAP where the contents of event changes will be stored. Sample value: `acf2`
UsersList	Enter a comma-separated list of user IDs that will be evaluated for delete reconciliation. **Note:** This field is optional. If no user IDs are listed, then all users will be evaluated. Sample value: `testusr1,testusr2,testusr3`

6. After specifying the attributes, perform one of the following steps:

a.) If you are using Oracle Identity Manager Release 9.1.0.*x*, then click **Save Changes** to save the changes.

Note: The Stop Execution option is not available in the *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*. If you want to stop a task, then click Stop Execution on the Task Scheduler form of the Design Console.

b.) If you are using Oracle Identity Manager Release 11.1.1, then click **Apply** to save the changes.

5.7 Reconciling Users to the Internal LDAP

The ACF2 Reconcile Users to Internal LDAP scheduled task allows the administrator to reconcile users from the target system to the internal LDAP store. When you configure this scheduled task, it runs at specified intervals and fetches a list of users and their profiles on the target system. Each of these users is then reconciled to the internal LDAP store. No reconciliation to Oracle Identity Manager is performed.

To configure the Reconcile Users to Internal LDAP scheduled task:

1. Log in to the Oracle Identity Manager Administrative and User Console.
2. Perform one of the following steps:
   a. If you are using Oracle Identity Manager Release 9.1.0.*x*, expand Resource Management, and then click **Manage Scheduled Task.**
   b. If you are using Oracle Identity Manager Release 11.1.1, then on the Welcome to Oracle Identity Manager Self Service page, click **Advanced** in the upper-right corner of the page.
3. Search for and open the scheduled task as follows:

   If you are using Oracle Identity Manager Release 9.1.0.*x*, then:

   a. On the Scheduled Task Management page, enter the name of the scheduled task as the search criteria and then click **Search.**
   b. In the search results table, click **Edit c**olumn for the scheduled task.
   c. On the Scheduled Task Details page, where the details of the scheduled task that you selected are displayed, click **Edit.**

   If you are using Oracle Identity Manager Release 11.1.1, then:

   a. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Search Scheduled Jobs.**
   b. On the left pane, in the Search field, enter the name of the scheduled job as the search criterion. Alternatively, you can click **Advanced Search** and specify the search criterion.
   c. In the search results table on the left pane, click the **scheduled job** in the Job Name column.
4. Modify the details of the scheduled task as follows:
   a. If you are using Oracle Identity Manager Release 9.1.0.*x*, then on the Edit Scheduled Task Details page, modify the following parameters, and then click **Continue:**

      Status: Specify whether you want to leave the task in the enabled state. In the enabled state, the task is ready for use.

      Max Retries: Enter an integer value in this field. This number represents the number of times Oracle Identity Manager must attempt to complete the task before assigning the ERROR status to the task. The default value is 0.

      Next Start: Use the date editor to specify the date when you want the task to run. After you select a date value in the date editor, you can modify the time value that is automatically displayed in the Next Start field.

      Frequency: Specify the frequency at which you want the task to run.

   b. If you are using Oracle Identity Manager Release 11.1.1, then on the Job Details tab, you can modify the following parameters:

Retries: Enter an integer value in this field. This number represents the number of times the scheduler tries to start the job before assigning the Stopped status to the job.

Schedule Type: Depending on the frequency at which you want the job to run, select the appropriate schedule type.

Note: See Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager for detailed information about schedule types.

In addition to modifying the job details, you can enable or disable a job.

5. Specify values for the attributes of the scheduled task as follows:

Note:

- Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.
- Values (either default or user-defined) must be assigned to all the attributes. If even a single attribute value is left empty, then reconciliation is not performed.

Table 5–2 describes the attributes of the scheduled task.

Table 5–2 Attributes of the Reconcile User to internal LDAP Scheduled Task

Attribute	Description
IT Resource	Enter the name of the IT resource that was configured for the target system. Sample value: `Acf2Resource`
Domain OU	Enter the name of the internally-configured directory in the LDAP where the contents of event changes will be stored. Sample value: `acf2`

6. After specifying the attributes, perform one of the following steps:

   a. If you are using Oracle Identity Manager Release 9.1.0.*x*, then click **Save Changes** to save the changes.

   Note: The Stop Execution option is not available in the Oracle Fusion Middleware User's Guide for Oracle Identity Manager. If you want to stop a task, then click Stop Execution on the Task Scheduler form of the Design Console.

   b. If you are using Oracle Identity Manager Release 11.1.1, then click **Apply** to save the changes.

5.8 Reconciling Internal LDAP Users to Oracle Identity Manager

The ACF2 Reconcile LDAP Users scheduled task allows the administrator to reconcile users from the internal LDAP store to Oracle Identity Manager. When you configure this scheduled task, it runs at specified intervals and fetches a list of users within the internal LDAP store and reconciles these users to Oracle Identity Manager.

To configure the Deleted User Reconciliation to OIM scheduled task:

1. Log in to the Oracle Identity Manager Administrative and User Console.
2. Perform one of the following steps:
   a. If you are using Oracle Identity Manager Release 9.1.0.*x*, expand Resource Management, and then click **Manage Scheduled Task.**
   b. If you are using Oracle Identity Manager Release 11.1.1, then on the Welcome to Oracle Identity Manager Self Service page, click **Advanced** in the upper-right corner of the page.
3. Search for and open the scheduled task as follows:

   If you are using Oracle Identity Manager Release 9.1.0.*x*, then:

   a. On the Scheduled Task Management page, enter the name of the scheduled task as the search criteria and then click **Search.**
   b. In the search results table, click **Edit c**olumn for the scheduled task.
   c. On the Scheduled Task Details page, where the details of the scheduled task that you selected are displayed, click **Edit.**

   If you are using Oracle Identity Manager Release 11.1.1, then:

   a. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Search Scheduled Jobs.**
   b. On the left pane, in the Search field, enter the name of the scheduled job as the search criterion. Alternatively, you can click **Advanced Search** and specify the search criterion.
   c. In the search results table on the left pane, click the **scheduled job** in the Job Name column.
4. Modify the details of the scheduled task as follows:
   a. If you are using Oracle Identity Manager Release 9.1.0.*x*, then on the Edit Scheduled Task Details page, modify the following parameters, and then click **Continue:**

      Status: Specify whether you want to leave the task in the enabled state. In the enabled state, the task is ready for use.

      Max Retries: Enter an integer value in this field. This number represents the number of times Oracle Identity Manager must attempt to complete the task before assigning the ERROR status to the task. The default value is 0.

      Next Start: Use the date editor to specify the date when you want the task to run. After you select a date value in the date editor, you can modify the time value that is automatically displayed in the Next Start field.

      Frequency: Specify the frequency at which you want the task to run.

   b. If you are using Oracle Identity Manager Release 11.1.1, then on the Job Details tab, you can modify the following parameters:

Retries: Enter an integer value in this field. This number represents the number of times the scheduler tries to start the job before assigning the Stopped status to the job.

Schedule Type: Depending on the frequency at which you want the job to run, select the appropriate schedule type.

Note: See Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager for detailed information about schedule types.

In addition to modifying the job details, you can enable or disable a job.

5. Specify values for the attributes of the scheduled task as follows:

Note:

- Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.
- Values (either default or user-defined) must be assigned to all the attributes. If even a single attribute value is left empty, then reconciliation is not performed.

Table 5–3 describes the attributes of the scheduled task.

Table 5–3 Attributes of the Reconcile LDAP Users Scheduled Task

Attribute	Description
IT Resource	Enter the name of the IT resource that was configured for the target system. Sample value: `Acf2Resource`
Resource Object	Enter the name of the resource object against which the delete reconciliation runs must be performed. Sample value: `OIMAcf2ResourceObject`
Domain OU	Enter the name of the internally-configured directory in the LDAP where the contents of event changes will be stored. Sample value: `acf2`
Trusted Resource Object	Enter the name of the resource object against which trusted reconciliation runs must be performed. Sample value: `Xellerate User`
MultiValuedAttributes	Enter a comma-separated list of multi-valued attributes that you want to reconcile. Do not include a space after each comma. Sample value: `attributes,memberOf`

Table 5–3 (Cont.) Attributes of the Reconcile LDAP Users Scheduled Task

Attribute	Description
SingleValueAttributes	Enter a comma-separated list of single-valued attributes that you want to reconcile. Do not include a space after each comma. Do not include attributes already listed in the MultiValueAttributes field. Sample value: `uid,owner,defaultGroup,waddr1,tsoMaxSize` **Note:** By default, Oracle Identity Manager's design form only allows entering up to 150 characters in a text field. To increase this limit, change the value of the TSA_VALUE column in the Oracle Identity Manager database.
TrustedReconciliation	Enter whether the target system should be treated as a trusted source. Sample value: `true`
LDAP Time Zone	Enter the time zone ID for the server on which the LDAP gateway is hosted. Sample value: `America/New_York`
uidcase	Enter whether the user ID should be displayed in uppercase or lowercase. Sample value: `upper`

6. After specifying the attributes, perform one of the following steps:

   a. If you are using Oracle Identity Manager Release 9.1.0.*x*, then click **Save Changes** to save the changes.

   Note: The Stop Execution option is not available in the Oracle Fusion Middleware User's Guide for Oracle Identity Manager. If you want to stop a task, then click Stop Execution on the Task Scheduler form of the Design Console.

   b. If you are using Oracle Identity Manager Release 11.1.1, then click **Apply** to save the changes.

6

Troubleshooting

Table 6–1 describes solutions to some problems that you might encounter while using the connector.

Table 6–1 Troubleshooting Tips

Problem Description	Solution
Oracle Identity Manager cannot establish a connection with CA ACF2.	■ 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 IP address of the server that hosts the LDAP Gateway is configured in the Reconciliation Agent JCL. ■ Read the LDAP Gateway logs to determine if messages are being sent and received. ■ Examine the Oracle Identity Manager configuration to verify that the IP address, admin ID, and admin password are correct. ■ Check with the mainframe platform manager to verify that the mainframe user account and password have not been changed.
The mainframe does not appear to respond.	■ Check the connection information that you have provided in the IT resource and the acf2Connection.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.
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 connector: ■ 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.

Table 6–1 (Cont.) Troubleshooting Tips

Problem Description	Solution
The Pioneer STC exits with a SD37 abend	This problem occurred because the dataset sizing for ACF2OUT is incorrect for the number of resource rules used in your environment. This is not a problem with the Pioneer STC, but with your sizing estimates. ACFCMD writes its output to ACF2OUT. As a sizing guideline, a blocksize of 27400 will yield 206 records of 133 bytes each.
The Pioneer STC exits with a S0C4 abend.	This problem possibly occurred because of a conflict between the system settings for the Language Environment (LE) options and what is needed. The LE options that maybe involved are ALL31, HEAP, and STACK. Using a CEEOPTS DD in the job stream may be necessary to over ride set defaults. See Table 6–2 for the three options settings and their effects.
The PIONEER STC exits with S722 abend when DEBUG=Y is set.	This happens because the debugging output from PIONEER can exceed limits that maybe set for JES2/JES3 SYSOUT files. Running with DEBUG=Y is meant to be used only on our request for a short duration to troubleshoot an issue. In all other cases DEBUG=N should be used.
Pioneer requires RACF to make calls to R_ADMIN API when the security subsystem is CA-ACF2.	All ACF2 commands are passed through the RACF API interface (service RADMIN, program = IRRSEQ00). Even though the Security Subsystem is CA-ACF2, the RACF API is still used by Pioneer for making calls to R_ADMIN API. Ensure that you have performed the steps described in the following sections: ■ Section 2.3.6, "Loading and Activating the Exits" ■ Section 2.3.7, "Creating an ACF2 LID for Pioneer and Voyager with Permissions" ■ Section 2.3.8, "Adding Pioneer/Voyager to the Resource Rule Facilities (BPX and IRR)"

The PIONEER STC fails with the following error message:
`IKJ56231I FILE AUDTLOG NOT ALLOCATED, SYSTEM OR INSTALLATION ERROR+`
`IKJ56231I TEXT UNIT X'0018' CONTAINS INVALID PARAMETER`
`AUDIT LOG FAILED TO ALLOC`
`RC: 0056360984`
`BPXWDYN PARMSTR: ALLOC DD(AUDTLOG) SYSOUT(*) MSG(WTP)`
	Ensure that you specify a SYSOUT value in the PIONEER CONTROL CARD Setting:
	`AUDIT=YES,SYSOUT,CLASS(*)`
	`For example: AUDIT=YES,SYSOUT,CLASS(S)`

Table 6–2 shows the three options settings and their effects:

Table 6–2 Three Options Settings and their Effects

ALL31	HEAP	STACK	RESULT
OFF	BELOW	BELOW	RC=0
OFF	BELOW	ANYWHERE	Loop
OFF	ANYWHERE	BELOW	S0C4
OFF	ANYWHERE	ANYWHERE	RC=0
ON	BELOW	BELOW	RC=0
ON	BELOW	ANYWHERE	RC=0
ON	ANYWHERE	BELOW	S0C4

Table 6–2 (Cont.) Three Options Settings and their Effects

ALL31	HEAP	STACK	RESULT
ON	ANYWHERE	ANYWHERE	RC=0

7

Known Issues

There are no known issues associated with this release of the connector.

A

Reconciliation Agent (Voyager) Messages

This appendix describes log 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: **IDMV000I** Voyager Executing From and APF Authorized Library

Message-Type: Informational

Action Required: None

Description: Module IDFAUTH verified that Voyager is executing out of a APF Authorized Library.

Message: **IDMV000E** Voyager Not Executing From a APF Authorized Library

Message-Type: Severe

Action Required: Voyager Abends

Description:Voyager is being executed from a library that is not APF authorized. To resolve this, APF authorize the Library that Voyager is executing from.

Message: **IDMV000I** Voyager Found RACF | ACF2 | TSS Security Subsystem

Message-Type: Informational

Action Required: None

Description: Module IDFIQSEC queried the Security Control Block in Storage And found RACF or ACF2 or Top-Secret, Voyager continues execution.

Message: **IDMV000I** Voyager Found Required Storage Subpool

Message-Type: Informational

Action Required: None

Description: Voyager found the Storage subpool built by STARTUP, Voyager Continues execution.

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 - v.r.r.m

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: **IDMV002I** Oracle Build Level 9.9.9.9.9

Message-Type: Informational

Action Required: None

Description: This is the Oracle Release of Voyager

Message: **IDMV003I** Voyager Subpool 100 BYTE Version

Message-Type: Informational

Action Required: None

Description: This Voyager supports only the 100 Byte version of the Subpool That STARTUP builds.

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: **IDMV060I** Voyager is OK and Working

Message-Type: Informational

Action Required: None

Description: The Operator queried Voyager's status with a "F stcid,STATUS" command. This message is usually coupled.

Message: **IDMV061I** Voyager is Setting DEBUG to YES

Message-Type: Informational

Action Required: None

Description: The Operator issued a 'F stcid,DEBUG=Y' command to Voyager

Message: **IDMV062I** Voyager is OK and Working

Message-Type: Informational

Action Required: None

Description: The Operator issued a 'F stcid,DEBUG=N' command to Voyager

Message: **IDMV063I** Voyager DEBUG is ALL READY ACTIVE

Message-Type: Informational

Action Required: None

Description: The Operator issued a 'F stcid,DEBUG=Y' and DEBUGGING was All ready active.

Message: **IDMV064I** Voyager DEBUG Will Be Activated

Message-Type: Informational

Action Required: None

Description: The Operator issued a 'F stcid,DEBUG=Y' and Voyager has turned on DEBUGGING.

Message: **IDMV065I** Voyager Debugging is not Active

Message-Type: Informational

Action Required: None

Description: The Operator issued a "F stcid,DEBUG=N" and debugging was already off.

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: **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** VoyagerConnection to the Gateway Failed IP=999.999.999.999

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, the IP= is the IP Address or Hostname of the LDAP

Gateway that Voyager is trying to connect to. Voyager will attempt retries ever 15-20 seconds.

-

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* - xxxxxxxxxxxxxxxxxxxxxxx

Message-Type: Error

Action Required: None

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

Message:	IDMV400I *Status* - xxxxxxxxxxxxxxxxxxxxxxx
Message-Type:	Informational
Action Required:	None
Description:	Voyager will display a status as it processes RACF events from the subpool.

B

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

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

Message: **IDMP002I** Pioneer Detects Build yyyymmddHHMM

Message-Type: Informational

Action Required: None

Description: 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

Description: 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

Description: 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

Description: 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

Description: 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 xxxxxxxxxxxxxxx

Message-Type: Informational

Action Required: None

Description: 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

Description: 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

Description: 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

Description: 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

Description: 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

Description: 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

Description: 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

Description: 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

Description: 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 ACF2 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 xxxxxxxxxxx

Message-Type: Informational – Shutdown Statistic

Action Required: None

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

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

Message-Type: Informational – Shutdown Statistic

Action Required: None

Meaning: Pioneer has processed xxxxxxxxxx (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'.

C

Authorized Libraries

APF means "Authorized Program Facility". In a z/OS environment, APF is a facility that permits the identification of programs that are authorized to use restricted functions. APF-authorized programs must reside in one of the following authorized libraries:

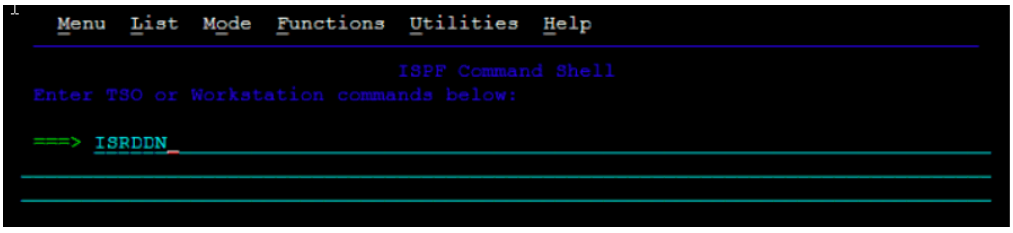
- SYS1.LINKLIB
- SYS1.SVCLIB
- SYS1.LPALIB
- Authorized libraries specified by your installation

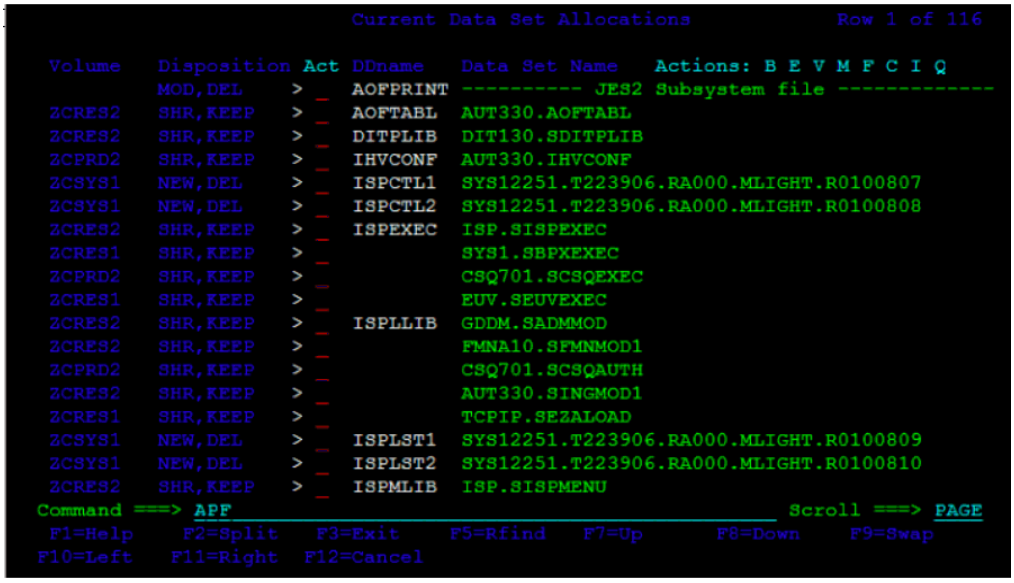
Authorized libraries are defined in an APF list, or in the link pack area (LPA). Any module in the LPA (pageable, modified, fixed, or dynamic) will be treated by the system as though it came from an APF-authorized library. The installation must ensure that it has properly protected SYS1.LPALIB and any other library that contributes modules to the link pack area to avoid system security and integrity exposures, just as it would protect any APF-authorized library. APF also prevents authorized programs (supervisor state, APF-authorized, PSW key 0-7, or PKM 0-7) from accessing a load module that is not in an APF-authorized library.

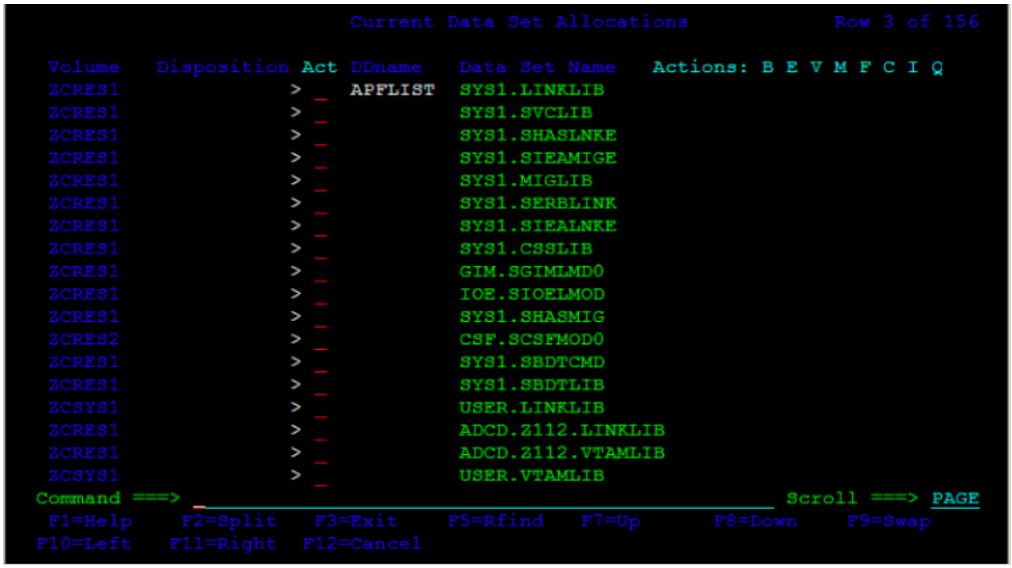
To find the datasets that are APF authorized:

1. Type TSO ISRDDN in your ISPF session (some shops need just ISRDDN with no TSO prefix) and hit enter.
2. Type APF and hit enter. It'll bring up a list of all datasets that are APF authorized.

Remember that, if you like to use an APF authorized dataset in a job STEPLIB, make sure all the datasets in the STEPLIB are APF authorized.




Current Data Set Allocations Row 1 of 116
Volume Disposition Act DDname Data Set Name Actions: B E V M F C I Q
MOD,DEL > AOFPRINT ---------- JES2 Subsystem file ----------
ZCRES2 SHR,KEEP > AOFTABL AUT330.AOFTABL
ZCRES2 SHR,KEEP > DITPLIB DIT130.SDITPLIB
ZCPRD2 SHR,KEEP > IHVCONF AUT330.IHVCONF
ZCSYS1 NEW,DEL > ISPCTL1 SYS12251.T223906.RA000.MLIGHT.R0100807
ZCSYS1 NEW,DEL > ISPCTL2 SYS12251.T223906.RA000.MLIGHT.R0100808
ZCRES2 SHR,KEEP > ISPEXEC ISP.SISPEXEC
ZCRES1 SHR,KEEP > SYS1.SBPXEXEC
ZCPRD2 SHR,KEEP > CSQ701.SCSQEXEC
ZCRES1 SHR,KEEP > EUV.SEUVEXEC
ZCRES2 SHR,KEEP > ISPLLIB GDDM.SADMMOD
ZCRES2 SHR,KEEP > FMNA10.SFMNMOD1
ZCPRD2 SHR,KEEP > CSQ701.SCSQAUTH
ZCRES2 SHR,KEEP > AUT330.SINGMOD1
ZCRES1 SHR,KEEP > TCPIP.SEZALOAD
ZCSYS1 NEW,DEL > ISPLST1 SYS12251.T223906.RA000.MLIGHT.R0100809
ZCSYS1 NEW,DEL > ISPLST2 SYS12251.T223906.RA000.MLIGHT.R0100810
ZCRES2 SHR,KEEP > ISPMLIB ISP.SISPMENU
Command ===> APF Scroll ===> PAGE
F1=Help F2=Split F3=Exit F5=Rfind F7=Up F8=Down F9=Swap
F10=Left F11=Right F12=Cancel


Current Data Set Allocations Row 3 of 156
Volume Disposition Act DDname Data Set Name Actions: B E V M F C I Q
ZCRES1 > APFLIST SYS1.LINKLIB
ZCRES1 > SYS1.SVCLIB
ZCRES1 > SYS1.SHASLNKE
ZCRES1 > SYS1.SIEAMIGE
ZCRES1 > SYS1.MIGLIB
ZCRES1 > SYS1.SERBLINK
ZCRES1 > SYS1.SIEALNKE
ZCRES1 > SYS1.CSSLIB
ZCRES1 > GIM.SGIMLMD0
ZCRES1 > IOE.SIOELMOD
ZCRES1 > SYS1.SHASMIG
ZCRES2 > CSF.SCSFMOD0
ZCRES1 > SYS1.SBDTCMD
ZCRES1 > SYS1.SBDTLIB
ZCSYS1 > USER.LINKLIB
ZCRES1 > ADCD.Z112.LINKLIB
ZCRES1 > ADCD.Z112.VTAMLIB
ZCSYS1 > USER.VTAMLIB
Command ===> Scroll ===> PAGE
F1=Help F2=Split F3=Exit F5=Rfind F7=Up F8=Down F9=Swap
F10=Left F11=Right F12=Cancel

D

Relationship between the Pioneer (DDs), Voyager (DDs) and the INDDs

The Table D–1 shows the relationship between the Pioneer (DDs) and the INDDs in CREATDSN member. The Table D–2 shows the relationship between the Voyager (DDs) and the INDDs in CREATDSN. Pioneer was used as a High-Level Qualifier to illustrate only

Table D–1 Relationship between the Pioneer (DDs) and the INDDs in CREATDSN Member

Pioneer DD:	CREATDSN DD:

LISTINR	//INDD1 DD DSN=PIONEER.ALIASOUT,
	//DCB=(DSORG=PS,RECFM=VBA,LRECL=133,BLKSIZE=0),
	// UNIT=SYSDA,SPACE=(CYL,5),DISP=(NEW,CATLG),
	// VOL=SER=??????

IDCAMSD	//INDD2 DD DSN=PIONEER.IDCAMSD.FILE,
	//DCB=(DSORG=PS,RECFM=F,LRECL=80,BLKSIZE=80
	// UNIT=SYSDA,SPACE=(TRK,5),DISP=(NEW,CATLG),
	// VOL=SER=??????

ACF2CTL	//INDD3 DD DSN=PIONEER.ACF2.CTL,
	//DCB=(DSORG=PS,RECFM=F,LRECL=80,BLKSIZE=80
	// UNIT=SYSDA,SPACE=(TRK,5),DISP=(NEW,CATLG),
	// VOL=SER=??????

ACF2OUT	//INDD4 DD DSN=PIONEER.ACF2OUT,
	//DCB=(DSORG=PS,RECFM=VBA,LRECL=133,BLKSIZE=0),
	// UNIT=SYSDA,SPACE=(CYL,5),DISP=(NEW,CATLG),
	// VOL=SER=??????

PARMFLE	//INDD7 DD DSN=PIONEER.CONTROL.FILE,
	//DCB=(DSORG=PS,RECFM=F,LRECL=80,BLKSIZE=80
	// UNIT=SYSDA,SPACE=(TRK,5),DISP=(NEW,CATLG),
	// VOL=SER=??????

NOTES:	Set VOL=SER=?????? to the location of the datasets. If customer is not using SMS to manage space.

Note: Voyager was used as a High-Level Qualifier to illustrate only.

Table D–2 Relationship between the Voyager (DDs) and the INDDs in CREATDSN Member

Voyager DD:	CREATDSN DD:

CACHESAV	//INDD5 DD DSN=VOYAGER.CACHESAV,
	//DCB=(DSORG=PS,RECFM=FB,LRECL=112,BLKSIZE=27888),
	// UNIT=SYSDA,SPACE=(CYL,10),DISP=(NEW,CATLG),
	// VOL=SER=??????

PARMFLE	//INDD6 DD DSN=VOYAGER.CONTROL.FILE,
	// DCB=(DSORG=PS,RECFM=F,LRECL=80,BLKSIZE=80),
	// UNIT=SYSDA,SPACE=(TRK,1),DISP=(NEW,CATLG),
	// VOL=SER=??????

NOTES:	Change vol=ser to the location of the datasets. If customer is not using SMS to manage space.

The Table D–3 describes the purpose of the Pioneer (DDs) and the files that were loaded by CREATDSN.

Table D–3 Purpose of the Pioneer (DDs)

Pioneer (DD):	Purpose:	Size Requirement:
LISTINR	Output file of the INJCLR JCL execution. Pioneer reads this file and sends it back to the LDAP.	None, this file is large enough.
IDCAMSD	IBM's IDCAMS control file Parameters sent by the LDAP.	No more than 2 Trks.
ACF2CTL	CA ACF2's internal SYSIN file For parameters sent by LDAP Input into the ACF2 call.	No more than 2 Trks.
ACF2OUT	CA ACF2's internal SYSPRINT file output of ACF2 calls.	No more than 2 Trks.
JCLOUTP	Output SYSOUT file for all listings of submitted JCL	N/A
AUDTLOG	Output SYSOUT file for AUDIT listings when the PARMFLE parameter AUDIT=YES is on.	N/A

E

LOADDSN1 Member and the File Contents

The Table E–1 shows the relationship between the steps in the LOADDSN1 member and the file contents that are loaded into Pioneer's datasets. In these example datasets, PIONEER is used for the High-Level qualifier for Pioneer files and VOYAGER is used for the High-Level qualifier for Voyager files. The HLQ will have to be changed to meet installation standards.

Table E–1 Steps of LOADDSN1 Member and File Contents

Steps	File Contents

Step #1	//STEP1 EXEC PGM=IEBGENER
	//SYSUT1 DD DSN=IDF.PROD.JCLLIB(PCTLFLE),DISP=SHR
	//SYSUT2 DD DSN=PIONEER.CONTROL.FILE,DISP=SHR
	//SYSPRINT DD SYSOUT=*
	//SYSIN DD DUMMY

PCTLFLE	* THIS IS A VALID COMMENT * CHANGE?? TO INSTALLATION VALUES * SEE MANUAL FOR PARAMETER VALUES * CONTROL FILE COMMENT TCPN=TCPIP IPAD=0.0.0.0 PORT=????? DEBUG=N ESIZE=16 LPAR=ACF2-100BYTE-SYS POST_PROC_ALIAS=F IDLEMSG=N DEBUGOUT=SYSOUT,CLASS(X) SPIN_CLASS=K FILTER=NO AUDIT=YES,SYSOUT,CLASS(S) STATS=NO C=INSERT,M=??????,L=????.???.???? C=CHANGE,M=??????,L=????.???.???? C=DELETE,M=??????,L=????.???.????
Note:	These are sample control file parameters. Please review this connector guide for details. The control file example illustrated shows all parameters.

Table E–1 (Cont.) Steps of LOADDSN1 Member and File Contents

Steps	File Contents

Step #2	//STEP2 EXEC PGM=IEBGENER
	//SYSUT1 DD DSN=IDF.PROD.JCLLIB(VCTLFLE),DISP=SHR
	//SYSUT2 DD DSN=VOYAGER.CONTROL.FILE,DISP=SHR
	//SYSPRINT DD SYSOUT=*
	//SYSIN DD DUMMY
	* COMMENT FOR VOYAGER
	SUBPOOL_SIZE=xxxxK
	TCPN=TCPIP
	IPAD=???.???.???.???
	PORT=5197
	DEBUG=Y
	ESIZE=16
	VOYAGER_ID=TESTACF2
	FILTER1=NO
	FILTER2=NO
	AUDIT=YES,SYSOUT,CLASS(S)

Note:	These are sample control file parameters. Please review the connector guide for details. .

F

Voyager and Pioneer Control File Parameters

The following table lists the Voyager control file parameter and corresponding descriptions:

Table F–1 Voyager Control File Parameters

Voyager Control File Parameter	Descriptions
SUBPOOL_SIZE=	Size of Subpool being requested, values are 0200K to 7500K 1000K will hold 10240 messages.
TCPN=	Name of the TCPIP STC in the LPAR where Voyager is executing.
IPAD=	IP address or hostname of the LDAP Gateway Host computer. Sample value: 192.168.1.109 myhost.com
PORT=	99999, the port LPAD is listening on.
DEBUG=	N = no debugging and Y = yes debugging. Running DEBUG=Y is meant to be used only by request and for a short duration to troubleshoot an issue.
ESIZE=	16 is the only valid parameter for encryption/decryption
DEBUGOUT=	SYSOUT,CLASS(K) the class of output to JES2 when DEBUG=Y is specified
VOYAGER_ID=	8 character unique name that will be passed with each Voyager message to the LDAP gateway. If for example 8 Lpars all running Voyager, each Voyager control file must have the same VOYAGER_ID= coded.

Table F–1 (Cont.) Voyager Control File Parameters

Voyager Control File Parameter	Descriptions
FILTER1	NO, no filtering, FILTER1=YES,A=TSO PROC,V=DSNUPROC,DBSPROC9,ABCPROC Any ACF2 LIDS Created or Changed with the ACF2 Attribute 'TSOPROC' in it with one of the values described will not be passed to the LDAP. It will be deleted. If AUDIT=YES is specified the Filters will be shown and actions taken FILTER2=YES,A=TSOAACT,V=ABCD,DEFGG,POIUYT Any ACF2 LIDS created or changed with the ACF2 attribute 'TSOACCT' in it and with one of the values described will not be passed to the LDAP. It will be deleted. If AUDIT=YES is specified the Filters will be shown and actions taken. The A= field or attribute is maximum of 10 characters. The V= variable field is a maximum of 10 characters each.
FILTER2	Same as FILTER1
FILTER3	Same as FILTER1
CACHE-DELAY=	999 this value is in seconds. Only used for installations running Oracle OIM. If the installation does not have OIM installed code CACHE_DELAY=002, this delay is the amount of time that Voyager waits before it issues a write socket to the LDAP gateway.
AUDIT=	No Audit Log is to be created. YES,SYSOUT,CLASS (x), AUDIT log is required and sent to //AUDTLOG DD

The following table lists the Pioneer control file parameter and corresponding descriptions:

Table F–2 Pioneer Control File Parameters

Pioneer Control File Parameter	Descriptions
TCPN=	Name of the TCPIP STC in the LPAR where Voyager is executing
IPAD=	The address will always be 0.0.0.0, do not change
PORT=	Port that Pioneer will listen on for LDAP messages
DEBUG=	Y or N, Normal operation is "N"
ESIZE=	16 is the only valid parameter for encryption/decryption
LPAR=	A 20 character unique identifier for customer usage
IDLEMSG=	Y or N, Y = idle message is displayed every 60 minutes N = no idle messages will be displayed
DEBUGOUT=	SYSOUT,CLASS(K) the class of output to JES2 when DEBUG=Y is specified
SPIN_CLASS=K	Used in conjunction with DEBUG=Y and DEBUGOUT,SYSOUT,CLASS(X), when DEBUG is closed manually via Operator command, then the output is send to the SPIN_CLASS specified

Table F–2 (Cont.) Pioneer Control File Parameters

Pioneer Control File Parameter	Descriptions
FILTER=	NO, no filtering inbound LDAP requests YES. If YES is specified then a F1= with filter values are required. F2 and F3 are also supported for a large number of values.
CACHE-DELAY=	999 this value is in seconds. Only used for Installations running Oracle OIM. If the installation does not have OIM installed code CACHE_DELAY=002, this delay is the amount of time that Voyager waits before it issues a write socket to the LDAP gateway.
AUDIT=	No Audit Log is to be created. YES, SYSOUT, CLASS (x), AUDIT log is required and sent to //AUDTLOG DD
STATS=	NO, no shutdown statistics, messages processed or bytes read/write YES, provide shutdown statistics
POST_PROC_ALIAS=	If you set the value of this parameter to T, then Pioneer will honor all DEFINE/DELETE alias requests from the LDAP. If you set the value of this parameter to F, Pioneer will ignore all requests for DEFINE or DELETE aliases. Sample value: T C=function, m=member name, L=PDS Library name Function can be INSERT, CHANGE or DELETE example1, C=INSERT,M=INSERT10,L=TEST.CNTL.LIB example2, C=CHANGE,M=CHANGE33,L=TEST.CNTL.LIB example3, C=DELETE,M=DELETE99,L=TEST.CNTL.LIB

Running DEBUG=Y is meant to be used only by request and for a short duration to troubleshoot an issue.

G

Mainframe Language Environment Runtime Options

If the following settings are not properly set, they can cause random S806 or S0C4 conditions.

1. Add the following CEEOPTS DD to your PIONEER and or VOYAGER Task (or other modules through STC/JCL) as needed.

   Example (this may vary by site requirements):

   ```
   //CEEOPTS DD DISP=SHR,
   //DSN=&SYSPLEX.OIDM.VOYAGER.CONTROL.PARMLIB(CEEPRM00)
   ```

2. Where the CEEPRM00 PDS member contains:
   a. RPTOPT(ON)
   b. RPTSTG(ON)
3. When you run the offending STC/JCL again you will get a list of the options in affect.
4. Compare the output of the current JES LOG and look for one of the following literals, so one may review the current options in place.
   a. "LAST WHERE SET"
   b. "IBM-supplied default"
   c. "ALL31"
5. Note that all LE options should all be reviewed (not only ALL31) as noted in step 8 of this section.
6. The options can be overridden within the CEEOPTS DD through the CEEPRM00 PDS member (or site specific implementation), as follows:
   - Where CEEPRM00
   - ALL31(ON)
   - RPTOPT(ON)
   - RPTSTG(ON)
   - STACK(128K,128K,ANYWHERE,KEEP,512K,512K)
7. When the anomaly is addressed, the RPT* lines can be removed, if desired:
   - Where CEEPRM00
   - ALL31(ON)

- STACK(128K,128K,ANYWHERE,KEEP,512K,512K)

8. Customizing Language Environment run time options Z/OS Language Environment Customization: Info gathered from IBM Manual # SA22-7564-13.

Table G–1 lists Language Environment run time options, defaults and recommendations.

Table G–1 Language Environment Run Time Options, Defaults and Recommendations

Option	Default	Recommended	IDF's
ABPERC	NONE	NONE	NONE
ABTERMENC	ABEND	ABEND	ABEND
AIXBLD	OFF	OFF	OFF
ALL31	ON	ON	ON
ANYHEAP	16K,8K,ANY,FREE	16K,8K,ANY,FREE	16K,8K,ANY,FREE
ARGPARSE	ARGPARSE	ARGPARSE	ARGPARSE
AUTOTASK	NOAUTOTASK	NOAUTOTASK	NOAUTOTASK
BELOWHEAP	8K,4K,FREE	8K,4K,FREE	8K,4K,FREE
CBLOPTS	ON	ON	ON
CBLPSHPOP	ON	N/A	ON
CBLQDA	OFF	OFF	OFF
CEEDUMP	60,SYSOUT=*,FREE-END,SPIN-UNALLOC	60,SYSOUT=*,FREE-END,SPIN-UNALLOC	60,SYSOUT=*,FREE-END,SPIN-UNALLOC
CHECK	ON	ON	ON
COUNTRY	US	User defined	US
DEBUG	OFF	OFF	OFF
DEPTHCONDLMT	10	0	10
DYNDMP	*USERID,NODYNAMIC,TDUMP	*USERID,NODYNAMIC,TDUMP	*USERID,NODYNAMIC,TDUMP
ENV	No default	User default	No default
ENVAR	"	"	"
ERRCOUNT	0	0	0
ERRUNIT	6	6	6
EXECOPS	EXECOPS	EXECOPS	EXECOPS
FILEHIST	ON	ON	ON
FILETAG	NOAUTOCVT, NOAUTOTAG	NOAUTOCVT, NOAUTOTAG	NOAUTOCVT, NOAUTOTAG
HEAP	32K,32K,ANY,KEEP,8K,4K	32K,32K,ANY,KEEP,8K,4K	32K,32K,ANY,KEEP,8K,4K
HEAP64	1M,1M,KEEP,32K,32K,KEEP,4k,4K,FREE	N/A	N/A
STACK	128K,128K,ANY,KEEP,512K,128K	128K,128K,ANY,KEEP,512K,128K	128K,128K,ANY,KEEP,512K,128K

There are many more run time options that are not applicable to this situation.

Index

A

Administrative and User Console, 3-10
Advanced Encryption Standard, 1-3
AES, 1-3

C

certified deployment configurations, 1-1
certified languages, 1-2
changing input locale, 3-7
clearing server cache, 3-7
configuring
  Oracle Identity Manager, 3-7
configuring account status reconciliation, 4-4
connector
  deployment, 3-1
  files and directories, 3-1
connector deployment, 3-1
  configuring Oracle Identity Manager, 3-7
  installing and configuring the LDAP Gateway, 3-13
connector release number, determining, 3-2
CREATEDSN, 2-11

D

data set resource profile attribute descriptions, 1-13
defining
  IT resources, 3-5
deploying, connector, 3-1
deployment
  Oracle Identity Manager system, 3-1
determining release number of connector, 3-2

E

enabling logging, 3-9

F

Filtered, 4-4
full reconciliation, 4-1

G

globalization features, 1-2

I

identity repository, supported, 1-2
IEBCOPYL, 2-11
IEBCPYRP, 2-11
input locale changing, 3-7
installation
  LDAP Gateway, 3-13
issues, 7-1
IT resources
  Acf2Resource, 3-5
  defining, 3-5
  parameters, 3-5

L

LDAP Gateway, 1-3
  installing, 3-13
limitations, 7-1
LOADDSN, 2-11
logging enabling, 3-9

M

Members of PDS IDF.JCLLIB, 2-13
message transport layer, 1-3
  TCP/IP with Advanced Encryption Standard, 1-3
multilanguage support, 1-2

O

Oracle Identity Manager Administrative and User Console, 3-10
Oracle Identity Manager server, configuring, 3-7

P

parameters of IT resources, 3-5
PDS IDF.JCLLIB, 2-11
Pioneer Provisioning Agent, 1-3
POLLOPER, 2-26
provisioned target system attributes, 1-14
provisioning, 4-6
  direct provisioning, 4-6
  provisioning triggered by policy changes, 4-6
  request-based provisioning, 4-6
  supported functions, 1-9

Provisioning Agent
provisioned target system attributes, 1-14

R

reconciled target system attributes, 1-14
reconciliation
account status reconciliation, 4-4
real-time reconciliation, 3-10
trusted source, 3-10
reconciliation action rules, 1-15
Reconciliation Agent, 1-3, 1-9
functionality, 1-9
reconciled target system attributes, 1-14
reconciliation rule, 1-14
release number of connector, determining, 3-2

S

server cache, clearing, 3-7
supported
mainframe identity repository, 1-2
Oracle Identity Manager versions, 1-2

T

target resource reconciliation
adding new fields, 5-1
target system, multiple installations, 5-4
TCP/IP with Advanced Encryption Standard, 1-3
trusted source reconciliation, 3-10

V

Voyager Reconciliation Agent, 1-3