Oracle® Identity Manager

Connector Guide for CA ACF2 Advanced

Release 9.0.4

E10423-03

July 2009

ORACLE®

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

E10423-03

Primary Author: Lyju Vadassery

Contributing Authors: Debapriya Datta, Devanshi Mohan, Alankrita Prakash

Contents

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

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

Deaf/Hard of Hearing Access to Oracle Support Services

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

Related Documents

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

For generic information about connectors, see *Oracle Identity Manager Connector Concepts*.

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

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

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/oim.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 9.0.4.4.

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

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

- Software Updates

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

- Documentation-Specific Updates

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

Software Updates

The following software updates have been made in 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 "Functionality Supported for Provisioning" on page 1-6.
- 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 "Target System Fields Used for Reconciliation and Provisioning" on page 1-7.
- 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 6, "Known Issues":
  - Bug 6668844
  - Bug 6904041
  - Bug 7189194
  - Bug 7033009

Documentation-Specific Updates

The following documentation-specific updates have been made from release 9.0.4 onward:

- The user profile field mappings and resource profile field mappings between Oracle Identity Manager and the target system have been added in "Target System Fields Used for Reconciliation and Provisioning" on page 1-7. "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 6, "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 Deployment Configurations" on page 1-1, major changes have been made in the "Target System" row. Information about certified deployment configurations has been removed from "Verifying Deployment Requirements" on page 3-1.
- 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.

1

About the Connector

The Oracle Identity Manager CA ACF2 Advanced connector provides a native interface between Oracle Identity Manager and CA ACF2 installed on a z/OS mainframe. The connector functions as a trusted virtual administrator on the target system, performing tasks, such as creating login IDs and changing passwords. In addition, it automates some of the functions that administrators usually perform manually.

The connector enables provisioning and reconciliation with CA ACF2. 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 user information for Oracle Identity Manager.

This chapter discusses the following topics:

1.1 Certified Deployment Configurations

Table 1–1 lists the certified deployment configurations.

Table 1–1 Certified Deployment Configurations

Item	Requirement
Oracle Identity Manager	Oracle Identity Manager release 8.5.3.1 or later
Target System	CA ACF2 r6.2, r8.0 SP4 or later, r9.0 SP1 or later, r12
Infrastructure Requirements: message transport layer	TCP/IP with Advanced Encryption Standard (AES) encryption
Target system user account for Oracle Identity Manager	IBM Authorized Program Facility (APF)-authorized account with SystemAdministrators privileges

Note: The LDAP Gateway uses the target system user account that you create for Oracle Identity Manager. Therefore, it has the privileges required to access and operate with the Reconciliation Agent and Provisioning Agent. See "Connector Architecture" on page 1-3 for information about the Reconciliation Agent and Provisioning Agent.

1.1.1 Message Transport Layer Requirements

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

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

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

1.1.2 Configuration of APF Authorization

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

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

1.2 Certified Languages

The connector supports the following languages:

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

1.3 Features of the Connector

This section discusses the following topics:

- Connector Architecture
- Functionality Supported by the Pioneer Provisioning Agent
- Functionality Supported for Provisioning

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

1.3.1 Connector Architecture

The CA ACF2 Advanced connector consists of the following components:

- **LDAP Gateway:** The LDAP Gateway is built on Java 1.4 and allows portability across various platforms and operating systems. The LDAP Gateway receives LDAP protocol commands from distributed applications and translates them to native mainframe commands. After the commands are run, LDAP-formatted responses are returned to the requesting application. It is recommended that you install the LDAP Gateway on the same computer as Oracle Identity Manager.
- **Pioneer Provisioning Agent:** The CA ACF2 Advanced connector provides the provisioning functionality through the Pioneer Provisioning Agent, which is a mainframe component. 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 Reconciliation Agent:** The CA ACF2 Advanced connector provides the reconciliation functionality through the Voyager Reconciliation Agent, which is a mainframe component. The Reconciliation Agent captures native mainframe events by using exit technology. Exits are programs that are run after a system event in the mainframe is processed. The Reconciliation Agent captures in real time events occurring from the TSO logins, the command prompt, batch jobs, and other native mainframe events. The Reconciliation Agent transforms these events into notification messages for Oracle Identity Manager through the LDAP Gateway.
- **Message Transport Layer:** The message transport layer enables the exchange of messages between the LDAP Gateway and the Reconciliation Agent and Provisioning Agent. You can use the following messaging protocol for the message transport layer:

  TCP/IP with AES encryption: This uses 128-bit cryptographic keys. The CA- ACF2 Advanced connector supports a message transport layer by using the TCP/IP protocol, which is functionally similar to proprietary message transport layer protocols.

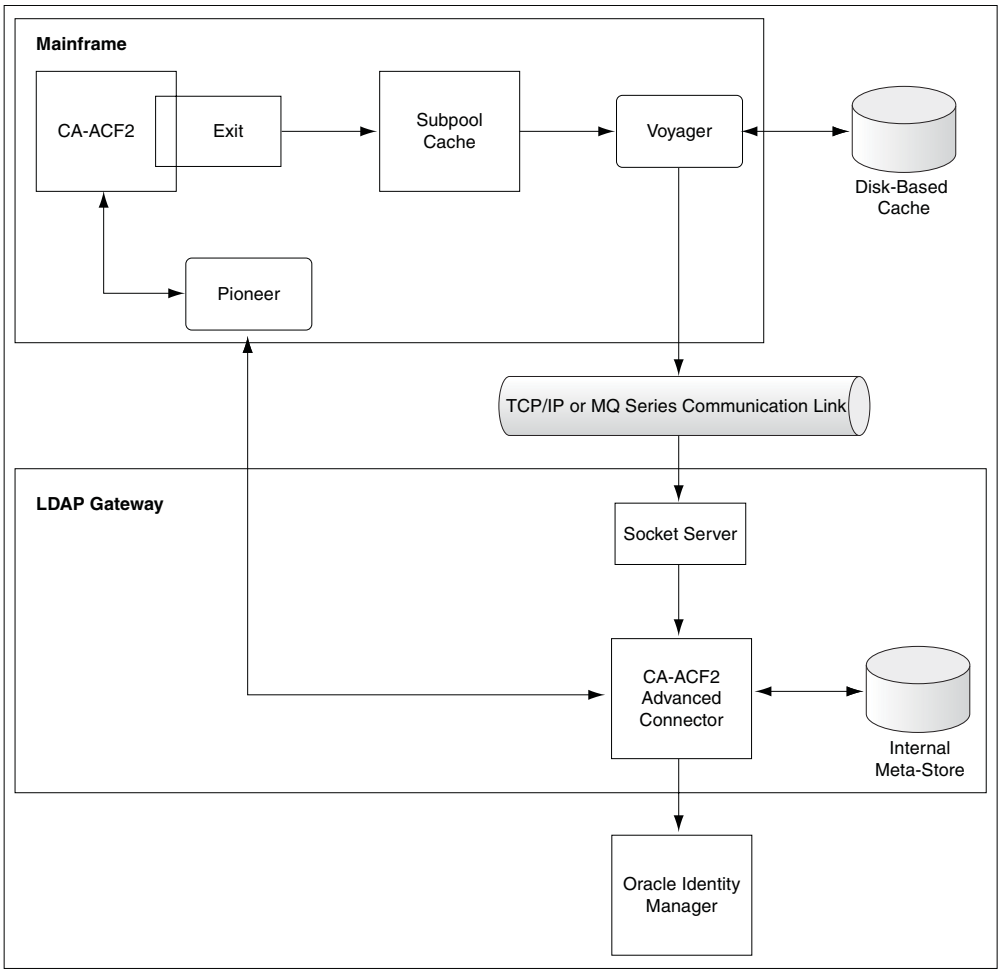
The architecture of the connector can be explained in terms of the connector operations it supports:

- Reconciliation
- Provisioning

1.3.1.1 Reconciliation

Figure 1–1 shows the flow of data during reconciliation.

Figure 1–1 Reconciliation Process



Reconciliation involves the following steps:

1. Mainframe identity and authorization events take place in the mainframe target system. The mainframe events are processed through appropriate exits.

   Note: Identity and authorization events in the mainframe system consist of TSO logon, running of a command, real-time password synchronization, creation or deletion of a user, or a change in the user attributes.

2. The mainframe events are stored in the subpool 231 cache of the Voyager Reconciliation Agent. Subpool 231 is an area of z/OS storage that the Reconciliation Agent uses to temporarily store CA ACF2 events. The subpool 231 cache enables the Reconciliation Agent to handle a large number of events from the mainframe.

3. The Reconciliation Agent reads these events and transforms them into notification messages for the LDAP Gateway. Reconciliation Agent opens a new socket to the LDAP Gateway and sends the notification messages. The messages are sent to the LDAP Gateway through the message transport layer. These messages contain the minimum amount of data required to reconcile the event, such as message type, user id, and password (for a password change event).

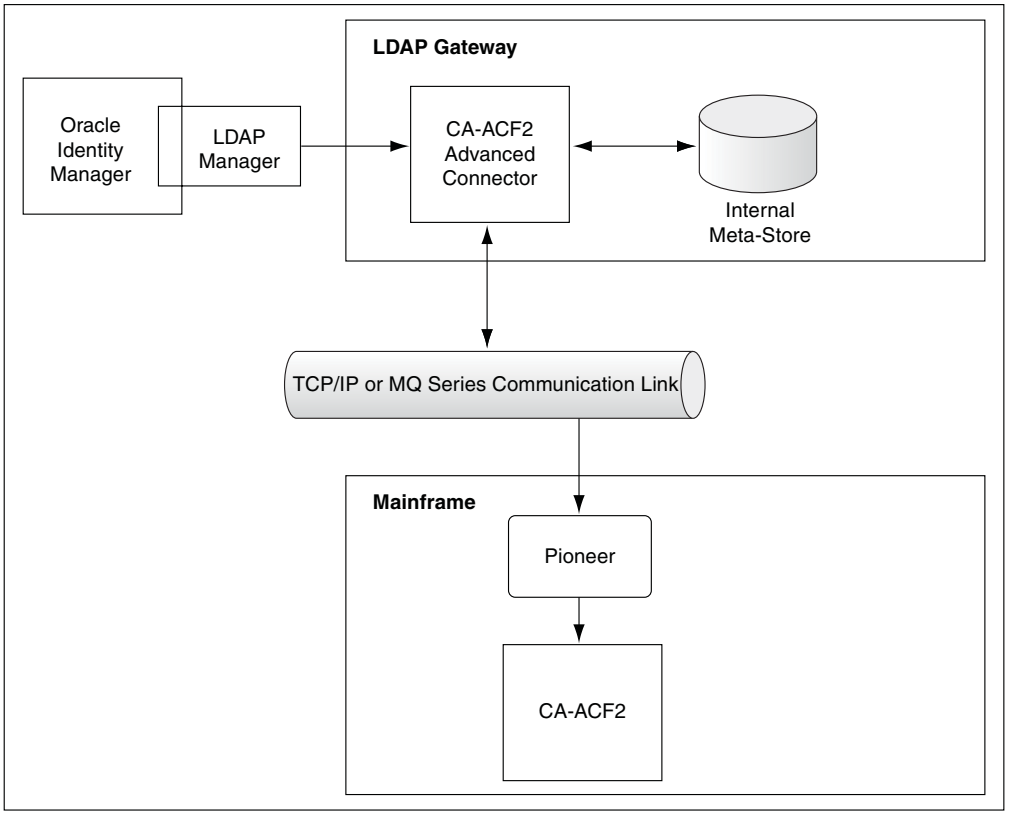
Note: When the mainframe system is shut down, event records are stored offline. These offline events are reloaded in the Reconciliation Agent when the mainframe is started up.

4. The LDAP Gateway receives the messages from the Reconciliation Agent and decrypts them for the connector.
5. The connector sends a request to the Provisioning Agent to retrieve all the current user data that is generated as a result of the mainframe identity and authorization events.
6. If an event fetched from the target system matches with the notification data, then the connector returns an error and the process stops. If the event does not match, then the connector sends the event to Oracle Identity Manager for reconciliation processing and updates the internal meta-store of event records. This process is repeated for all the events that are fetched from the target system.

1.3.1.2 Provisioning

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

Figure 1–2 Provisioning Process



Provisioning involves the following steps:

1. A user is created, updated, or deleted in Oracle Identity Manager.
2. The Oracle Identity Manager process task adapter for CA ACF2 forwards the change request to the LDAP Gateway.

3. The LDAP Gateway translates the change request from the LDAP Gateway to mainframe commands. The CA ACF2 Advanced connector encrypts the data, and sends it to the Provisioning Agent through the message transport layer.
4. The connector also updates the internal meta-store of the LDAP Gateway with the changes in user data.
5. On the target system, the Provisioning Agent decrypts the data, sends the data to the mainframe repository, and returns success or error messages back to the LDAP Gateway.

1.3.2 Functionality Supported by the Pioneer Provisioning Agent

The Pioneer Provisioning Agent supports the following functions:

- Standard CA ACF2 user profile commands:
  - [INSERT]: Creates a CA ACF2 user profile
  - [CHANGE]: Modifies a CA ACF2 user profile
  - [DELETE]: Deletes a CA ACF2 user profile
- Standard CA ACF2 group profile commands:
  - [CHANGE]: Adds a CA ACF2 user to a group. This command works based on the variables that set access rights. To add a CA ACF2 user to a group, the variables are R(A), W(A), EXEC(A), and ALLOC(A).
  - [CHANGE]: Removes a CA ACF2 user from a group. To remove a CA ACF2 user from a group, the variables are R(P), W(P), EXEC(P), and ALLOC(P).
- Standard CA ACF2 data set and resource profile commands:
  - [SET RULE]: Provides data set or resource profile access to a user

1.3.3 Functionality Supported for Provisioning

Table 1–2 describes the functions supported by the Provisioning Agent:

Table 1–2 Functionality Supported for Provisioning

Function	Description
Create Users	Adds new users in CA ACF2.
Modify Users	Modifies user information in CA ACF2.
Change Passwords	Changes user passwords on CA ACF2 in response to password changes made on Oracle Identity Manager through user self-service.
Reset Passwords	Resets user passwords on CA ACF2. The passwords are reset by the administrator.
Disable User Accounts	Disables users in CA ACF2.
Enable User Accounts	Enables users in CA ACF2.
Delete Users	Removes users from CA ACF2.
Grant Users Access To Data Sets	Sets ACF2 rule by adding the user to a ACF2 resource.
Grant Users Access To Privileges (TSO)	Provides TSO login access to users.

1.3.4 Functionality Supported by the Voyager Reconciliation Agent

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

1.3.5 Functionality Supported for Reconciliation

The Reconciliation Agent supports the following functions:

- Change passwords
- Password resets
- Create user data
- Modify user data
- Disable users
- Delete users
- Enable users

1.3.6 Target System Fields Used for Reconciliation and Provisioning

This section discusses the following topics:

- User Field Mapping
- Resource Profile Field Mapping

1.3.6.1 User Field Mapping

Table 1–3 lists the user field mappings that are reconciled between Oracle Identity Manager and the target system:

Table 1–3 Field Mapping Between Oracle Identity Manager and CA ACF2

Oracle Identity Manager Field	CA ACF2 Field	Description
uid	USER	User's login ID.
cn	NAME	User full name.
sn	NAME	User last name.
givenName	NAME	User first name.
userPassword	PASSWORD	Password used to login.
privileges	SECURITY (Including custom privileges)	Privileges for the user, including custom privileges.
activeDate	ACTIVE	Privilege to allow or deny access based on a date.
group	GROUP (Restriction Group)	Default restriction group for the user.
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 password.
cicsid	CICSID	CICS operator ID.
accessCnt	ACC-CNT	Count of times a user accessed the system.
accessDate	ACC-DATE	Date when the user accessed the system for the last time.

Table 1–3 (Cont.) Field Mapping Between Oracle Identity Manager and CA ACF2

Oracle Identity Manager Field	CA ACF2 Field	Description
accessSrce	ACC-SRCE	The system component accessed by the user.
accessTime	ACC-TIME	Time when the user accessed the system for the last time.
prefix	PREFIX	The zero to eight character key of the rule used to validate access to a data set.
kerbVio	KERB-VIO	The number of Kerberos key violations.
kerbCurv	KERBCURV	The Kerberos key version.
pwsdDate	PSWD-DAT	The date of the 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:** Refer to the target system documentation for information about GSO.
pwsdInv	PWSD-INV	The number of password violations that occurred since the last successful logon. This field can be reset to zero by a security administrator.
pwsdTod	PWSD-TOD	The date and time when a user changed password. CA ACF2 lists the date 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 20th century (1970-1999). Year designations of 00-69 assume a date in the 21st century (2000-2069).
pwsdVio	PWSD-VIO	The number of password violations that occurred on PSWD-DAT.
minDays	MINDAYS	The minimum number of days that must elapse before a user can change password. Zero indicates no limit.
maxDays	MAXDAYS	The 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. Zero indicates no limit.
tsocommand	TSOCMDS	Command to be run during TSO/E logon.
tsodest	DFT-DEST	Default SYSOUT destination.
tsoDefaultPrefix	DFT-PFX	The one to eight character default TSO prefix that is set in the user's profile at logon time.
tsounit	TSOUNIT	Default UNIT name for allocations.
tsoRba	TSORBA	The 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	The maximum region size the user can request at logon.

Table 1–3 (Cont.) Field Mapping Between Oracle Identity Manager and CA ACF2

Oracle Identity Manager Field	CA ACF2 Field	Description
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.
revoke	NA	Value is `Y` if user is revoked or `N` if user is resumed.
tsoPerf	TSOPERF	The 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 for missing or incorrect parameters.
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 the TSO procedure name at logon time.
tsoLgnTime	LGN-TIME	Indicates the permission to specify the TSO session time limit at logon time.
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 any region size at logon time by overriding TSOSIZE.
tsoLgnUnit	LGN-UNIT	Indicates permission to specify the TSO unit name at logon time.

Table 1–3 (Cont.) Field Mapping Between Oracle Identity Manager and CA ACF2

Oracle Identity Manager Field	CA ACF2 Field	Description
tsoIntercom	INTERCOM	Indicates that the user is willing to accept messages from other users through the TSO SEND command.
secVio	SEC-VIO	Indicates the number of cumulative security violations for a user.
updTod	UPD-TOD	Indicates the date and time when a login ID record was last updated.

1.3.6.2 Resource Profile Field Mapping

Table 1–4 lists resource profile field mappings between Oracle Identity Manager and the target system.

Table 1–4 Dataset Resource Profile Field Descriptions

Oracle Identity Manager Field	CA ACF2 Field	Description
cn	PROFILE NAME	The profile id
standardAccessList	ID,ACCESS,ACCESS COUNT	The standard access list of ID and access for the dataset
conditionalAccessList	ID,ACCESS,ACCESS COUNT	The condition access list of ID and access for the dataset
owner	OWNER	The owner of the dataset
auditing	AUDITING	Indicates whether auditing should be enabled
notify	NOTIFY	Indicates whether notification is enabled for any changes to resource profiles
instdata	DATA	The installation data for the dataset

1.4 Roadmap for Deploying and Using the Connector

The CA ACF2 Advanced connector deployment involves deploying the LDAP Gateway, Reconciliation Agent, and Provisioning Agent. The Reconciliation Agent and Provisioning Agent are deployed on the mainframe.

These procedures are described in the following chapters:

- Chapter 2, "Connector Deployment on Oracle Identity Manager" provides instructions for deploying the connector on the Oracle Identity Manager system. This procedure involves configuring Oracle Identity Manager, importing the connector XML file, compiling adapters, installing the LDAP Gateway, and configuring the message transport layer.
- Chapter 3, "Connector Deployment on CA ACF2" describes the procedure to deploy the Reconciliation Agent and Provisioning Agent on the mainframe. It is recommended that you perform this procedure with the assistance of the systems programmer.
- Chapter 4, "Configuring the Connector" describes the procedure to run initial reconciliation and to configure trusted source reconciliation and account status reconciliation. In addition, this chapter describes how to add a new field for provisioning.

- Chapter 5, "Troubleshooting" discusses the problems that you might encounter while using the connector. In addition, this chapter discusses guidelines on using the connector.
- Chapter 6, "Known Issues" lists the known issues associated with this release of the connector.

2

Connector Deployment on Oracle Identity Manager

The following sections in this chapter describe the procedure to deploy the LDAP Gateway on the Oracle Identity Manager host computer:

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

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

- Configuring the Connector for Multiple Installations of the Target System

> **See Also:** Chapter 3, "Connector Deployment on CA ACF2" for the procedure to deploy the Reconciliation Agent and Provisioning Agent on the mainframe

2.1 Files and Directories That Comprise the Connector

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

Table 2–1 Files and Directories That Comprise the Connector

Files and Directories	Description of Files and Contents
etc/LDAP Gateway/ldapgateway.zip	Files required to deploy the LDAP Gateway.
Files in the etc/Provisioning and Reconciliation Connector/ directory: ■ Jcl.xmit ■ linklib.xmi	Files required to deploy the Provisioning Agent and the Reconciliation Agent on the mainframe.
lib/idm.jar	The connector JAR file to be deployed on the Oracle Identity Manager system. It contains the Oracle Identity Manager process tasks adapter code.
lib/acf2-adv-agent-recon.jar lib/acf2Connection.properties	Files required to enable real-time reconciliation between the target system and Oracle Identity Manager.

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

Files and Directories	Description of Files and Contents
Files in the resources directory	Each of these resource bundles contains locale-specific information that is used by the connector. **Note:** A **resource bundle** is a file containing localized versions of the text strings that are displayed on the user interface of Oracle Identity Manager. These text strings include GUI element labels and messages displayed on the Administrative and User Console.
Files in the scripts directory: ■ run_initial_recon_provisioning.sh ■ run_initial_recon_provisioning.bat ■ acf2-adv-initial-recon.jar ■ initialAcf2Adv.properties	Files that are used to perform first-time (initial) reconciliation with Oracle Identity Manager.
scripts/user.txt	Sample of the file containing user data that is used during initial reconciliation. This file is discussed in detail in "Running Initial Reconciliation" on page 4-2.
xml/oimAcf2AdvancedConnector.xml	This XML file contains definitions for the connector components related to reconciliation and provisioning. These components include: ■ Resource objects ■ IT resource types ■ Process forms ■ Process tasks and adapters ■ Provisioning process ■ Lookup definitions ■ Prepopulate rules ■ Scheduled tasks
Xml/oimAcf2TrustedXellerateUser.xml	The XML file that contains component definitions for the connector for trusted source reconciliation.

See Also:

- "Copying the Connector Files" on page 2-2
- "Deploying the Reconciliation Agent and Provisioning Agent" on page 3-2

2.2 Copying the Connector Files

Copy the following connector files to the destination directories on the Oracle Identity Manager host computer as indicated in Table 2–2.

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

Table 2–2 Copying the Connector Files

Files	Destination
etc/LDAP Gateway/ldapgateway.zip	*LDAP_INSTALL_DIR* This is the directory on the Oracle Identity Manager system where you want to install the LDAP Gateway. See "Installing and Configuring the LDAP Gateway" on page 2-8 for information about installing the LDAP Gateway.
lib/acf2-adv-agent-recon.jar lib/acf2Connection.properties	*LDAP_INSTALL_DIR*/etc
lib/idm.jar Files in the scripts directory: ▪ run_initial_recon_provisioning.sh ▪ run_initial_recon_provisioning.bat ▪ acf2-adv-initial-recon.jar ▪ user.txt ▪ initialAcf2Adv.properties	*OIM_HOME*/xellerate/JavaTasks
Files in the resources directory	*OIM_HOME*/xellerate/connectorResources/
xml/oimAcf2AdvancedConnector.xml xml/oimAcf2TrustedXellerateUser.xml	*OIM_HOME*/xellerate/XLIntegrations/acf2/xml/

Note: While installing Oracle Identity Manager in a clustered environment, you copy the contents of the installation directory to each node of the cluster. Similarly, you must copy the files in the connectorResources directory and the JAR files to the corresponding directories on each node of the cluster.

2.3 Configuring Oracle Identity Manager

Configuring Oracle Identity Manager involves the following procedures:

- Clearing Content Related to Connector Resource Bundles from the Server Cache
- Enabling Logging

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

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

When you perform the procedure described in "Copying the Connector Files" on page 2-2, you copy the resource bundles for this connector into the *OIM_HOME*/xellerate/connectorResources directory. Whenever you add a new resource bundle in the connectorResources directory or make a change in an existing resource bundle, you must clear content related to connector resource bundles from the server cache.

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

1. In a command window, go to the *OIM_HOME*/xellerate/bin/ directory.

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

OIM_HOME/xellerate/bin/*BATCH_FILE_NAME*

2. Enter one of the following commands:

   - On Microsoft Windows:

     ```
     PurgeCache.bat ConnectorResourceBundle
     ```

   - On UNIX:

     ```
     PurgeCache.sh ConnectorResourceBundle
     ```

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

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

OIM_HOME/xellerate/config/xlConfig.xml

2.3.2 Enabling Logging

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

- ALL

  This level enables logging for all events.

- DEBUG

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

- INFO

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

- WARN

  This level enables logging of information about potentially harmful situations.

- ERROR

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

- FATAL

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

- OFF

  This level disables logging for all events.

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

- **JBoss Application Server**

  To enable logging:

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

     ```
     <category
     name="COM.IDENTITYFORGE.ORACLE.INTEGRATION.IDFACF2USEROPERATIONS">
           <priority value="LOG_LEVEL"/>
     </category>
     ```

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

     ```
     <category
     name="COM.IDENTITYFORGE.ORACLE.INTEGRATION.IDFACF2USEROPERATIONS">
        <priority value="INFO"/>
     </category>
     ```

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

  JBOSS_HOME/server/default/log/server.log

- **IBM WebSphere Application Server**

  To enable logging:

  1. In the *OIM_HOME*/xellerate/config/log.properties file, add the following line:

     ```
     log4j.logger.COM.IDENTITYFORGE.ORACLE.INTEGRATION.IDFACF2USEROPERATIONS=LOG
     _LEVEL
     ```

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

     ```
     log4j.logger.COM.IDENTITYFORGE.ORACLE.INTEGRATION.IDFACF2USEROPERATIONS=INF
     O
     ```

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

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

- **BEA WebLogic Server**

  To enable logging:

  1. In the *OIM_HOME*/xellerate/config/log.properties file, add the following line:

     ```
     log4j.logger.COM.IDENTITYFORGE.ORACLE.INTEGRATION.IDFACF2USEROPERATIONS=LOG
     _LEVEL
     ```

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

     ```
     log4j.logger.COM.IDENTITYFORGE.ORACLE.INTEGRATION.IDFACF2USEROPERATIONS=INF
     O
     ```

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

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

- **Oracle Application Server**

  To enable logging:

  1. In the *OIM_HOME*/xellerate/config/log.properties file, add the following line:

     log4j.logger.COM.IDENTITYFORGE.ORACLE.INTEGRATION.IDFACF2USEROPERATIONS=*LOG_LEVEL*

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

     log4j.logger.COM.IDENTITYFORGE.ORACLE.INTEGRATION.IDFACF2USEROPERATIONS=INFO

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

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

2.4 Importing the Connector XML File

To import the connector XML file into Oracle Identity Manager:

1. Open the Oracle Identity Manager Administrative and User Console.
2. Click the **Deployment Management** link on the left navigation pane.
3. Click the **Import** link under Deployment Management. A dialog box for locating files is displayed.
4. Locate and open the oimAcf2AdvancedConnector.xml file, which is in the *OIM_HOME*/xellerate/XLIntegrations/acf2/xml/ directory. Details of this XML file are shown on the File Preview page.

   You must import the XML file for trusted source reconciliation, acf2TrustedXellerateUser.xml, after the other XML file is imported. In other words, you must import oimAcf2AdvancedConnector.xml regardless of whether you want to implement target resource or trusted source reconciliation. If you want to implement trusted source reconciliation, then import the acf2TrustedXellerateUser.xml file after the first one is imported.
5. Click **Add File.** The Substitutions page is displayed.
6. Click **Next**. The Confirmation page is displayed.
7. Click **Next.** The Provide IT Resource Instance Data page is displayed.
8. Create an IT resource based on the OIMLDAPGatewayResourceType IT resource type. You must specify values for the IT resource parameters listed in Table 2–3.

Table 2–3 Defining IT Resources

Parameter	Description
AtMap User	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	The administrator ID for connecting to the LDAP Gateway Sample value: `cn=idfAcf2Admin,dc=acf2,dc=com`
idfPrincipalPwd	The administrator password for connecting to the LDAP Gateway Sample value: `password` See step 9 of "Installing and Configuring the LDAP Gateway" on page 2-8 for information about changing the password.
idfRootContext	The root context for CA ACF2 Value: dc=acf2,dc=com **Note:** You must not change the value of this parameter.
idfServerHost	Host name for connecting to the LDAP Gateway Sample value: `localhost` **Note:** You must not change the value of this parameter if you install the LDAP Gateway on the host computer as the one on which Oracle Identity Manager is installed. If you install the LDAP Gateway on a different computer, then specify the host name or IP address of that computer.
idfServerPort	The port for connecting to the LDAP Gateway Sample value: `5389`

9. Click **Next**. The Provide IT Resource Instance Data page for a new instance of the OIMLDAPGatewayResourceType IT resource type is displayed.
10. Click **Skip** to specify that you do not want to define another IT resource. The Confirmation page is displayed.
11. Click **View Selections**.

    The contents of the XML file are displayed on the Import page. You may see a cross-shaped icon along with some nodes. These nodes represent Oracle Identity Manager entities that are redundant. Before you import the connector XML file, you must remove these entities by right-clicking each node and then selecting **Remove**.
12. Click **Import**. The connector file is imported into Oracle Identity Manager.

2.5 Compiling Adapters

Adapters are used to implement provisioning functions. The following adapters are imported into Oracle Identity Manager when you import the connector XML file:

- CreateUserAcf2
- OnBoardAcf2User
- ResetAcf2Password
- ChangeAcf2UserPassword
- DeleteAcf2User

- RevokeAcf2User
- ResumeAcf2User
- ModifyAcf2User
- ModifyAcf2UserRemove
- AssignACF2UserToDataset
- UnAssignAcf2UserFromDataset

You must compile these adapters before they can be used in provisioning operations. To compile adapters by using the Adapter Manager form:

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

   If you have created your own adapters or if a new adapter is shipped with a patch that you installed, then you might need to compile one adapter at a time. To compile multiple (but not all) adapters, select the adapters you want to compile. Then, click **Compile Selected**.
3. Click **Start.** Oracle Identity Manager compiles the adapters that you specify.
4. If Oracle Identity Manager is installed in a clustered environment, then copy the compiled adapters from the *OIM_HOME*/xellerate/Adapter directory to the same directory on each of the other nodes of the cluster. If required, overwrite the adapter files on the other nodes.

2.6 Installing and Configuring the LDAP Gateway

To install and configure the LDAP Gateway:

1. Extract the contents of the ldapgateway.zip file to a directory on the computer on which Oracle Identity Manager is installed.

   Note: In this document, the location (and name) of the ldapgateway directory is referred to as *LDAP_INSTALL_DIR*.

2. In a text editor, open the following scripts:
   - Open the run.sh or run.bat script from the *LDAP_INSTALL_DIR*/bin/ directory.
   - Open the run_initial_recon_provisioning script from the *OIM_HOME*/Xellerate/JavaTasks directory.
3. In the run script:
   - Set the JAVA_HOME property as follows:

     ```
     JAVA_HOME=DIRECTORY_LOCATION\j2sdj1.4.2_13
     ```

     Replace *DIRECTORY_LOCATION* with the full path of the directory.
   - If you plan to run multiple LDAP Gateways on a Linux or Solaris environment and there are not enough socket file descriptors to open up all the ports needed for the server, then add the following line:

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

4. In the run and run_initial_recon_provisioning scripts, uncomment the line related to the application server directory. In addition, change the path to reflect the actual location of the application server directory.

   Note: The contents of the run and run_initial_recon_provisioning scripts are similar. You must make the same change in both the scripts.

   The lines starting with a number sign (#) are comments, as shown:

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

   To uncomment the line, remove the number sign. For example, to ensure that the connector works with JBoss Application Server, change the line to the following:

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

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

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

6. In a text editor, open the *LDAP_INSTALL_DIR*/conf/acf2.properties file. In this file, specify information for the following properties of the message transport layer that you use:

   - For TCP/IP, the default values are as follows:

     ```
     _type_=socket
     _isencrypted_=true
     _timeout_=5000
     _authretries_=1
     _host_=HOST_NAME_OR_IP_ADDRESS_OF_MAINFRAME
     _port_=5790
     _agentport_=5190
     ```

     The configurable properties are:

     – _type_: The transport type, which is TCP/IP (socket)

     – _host_: The host name of IP Address of the mainframe

     Note: If you are configuring the LDAP Gateway on the computer on which Oracle Identity Manager is installed, then specify `localhost` as the value of the _host_ property. If you are configuring the LDAP Gateway on a different computer, then specify the host name or IP address of the computer as the value of the _host_ property. However, it is recommended that you install the LDAP Gateway on the same computer on which Oracle Identity Manager is installed.

     – _port_: The port of the Pioneer Provisioning Agent

– _agentport_: The port that the Voyager Reconciliation Agent needs to send messages

7. In the acf2.properties file, use the following property to specify whether you want to revoke access rights or delete users during Disable User provisioning operations:

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

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

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

8. In the acf2.properties file, use the _nameFormat_ property to specify the format of the Full Name attribute.

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

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

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

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

9. Open the *LDAP_INSTALL_DIR*/etc/acf2Connection.properties file and edit the following property:

Note: You must also make this change in the initialAcf2Adv.properties file, which is in the *OIM_HOME*/xellerate/JavaTasks directory.

```
_itResource_=NAME_OF_THE_NEW_IT_RESOURCE
```

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

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

- Target system administrator credentials

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

Note: In these lines, the values that you can change are highlighted in bold font. The values that you enter in the beans.xml file must be the same as the values that you specify for the IT resource parameters and the properties in the acf2Connection.properties and initialAcf2Adv.properties files.

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

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

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

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

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

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

2.7 Configuring the Connector for Multiple Installations of the Target System

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

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

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

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

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

   See Also:

   - *Oracle Identity Manager Design Console Guide* for information about creating IT resources
   - Step 8 of "Importing the Connector XML File" on page 2-6 for information about the parameters of the IT resource

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

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

3. Extract the contents of the *LDAP_INSTALL_DIR*/dist/idfserver.jar file.
4. In the beans.xml file, change the value of the port in the <property name="port" value="xxxx"/> line to specify a port that is different from the port used for the first instance of the LDAP Gateway. The default port number is shown in the following example:

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

   If you change the port number, then you must make the same change in the value of the idfServerPort parameter of the IT resource that you create.
5. Save and close the bean.xml file.
6. Open the *LDAP_INSTALL_DIR*/conf/acf2.properties file and edit the following properties:
   - _host_=*IP_ADDRESS_OR_HOST_NAME_OF_THE_MAINFRAME*
   - _port_=*PORT_OF_THE_SECOND_INSTANCE_OF_THE_PROVISIONING_AGENT*
   - _agentPort_=*PORT_OF_THE_SECOND_INSTANCE_OF_THE_RECONCILIATION_AGENT*

   Note: The value of the _agentPort_ property 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 property if you have two mainframe servers with CA ACF2 running on each server.
7. Open the *LDAP_INSTALL_DIR*/etc/acf2Connection.properties file and edit the following property:

   itResource=*NAME_OF_THE_NEW_IT_RESOURCE*

3

Connector Deployment on CA ACF2

You must install the Reconciliation Agent and Provisioning Agent components of the CA ACF2 Advanced connector on the mainframe. The following sections describe the installation and configuration of these agents:

- Verifying Deployment Requirements
- Deploying the Reconciliation Agent and Provisioning Agent
- Installing the Exits for the Reconciliation Agent
- Configuring the Message Transport Layer

3.1 Verifying Deployment Requirements

Both the Reconciliation Agent and Provisioning Agent need a started task and service account that has the privileges required to run CA ACF2 system commands on the mainframe system.

In addition, these agents are accessed by a user account with privileges on the mainframe system. This user account must be created by the systems programmer before you deploy the agents.

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

3.1.1 Environmental Settings and Requirements

Ensure that the following requirements are met on the mainframe:

- The Provisioning Agent and Reconciliation Agent use their own memory subpools to manage peak load conditions. These subpools require 1.5 to 2.0 MB of mainframe memory for operations. You configure this while installing the Provisioning Agent and Reconciliation Agent.
- In addition to the program itself, the user account that a program runs under must also have authorization to access subpools on the host platform. This must be configured by the systems programmer.

- If TCP/IP is used for the message transport layer, then an administrator must have authorization to create ports on the mainframe and provide security authorizations.
- The Reconciliation Agent operates by using user exit technology, outside the mainframe operating system. This means that it runs in a different LPAR from the operating system.

  A command execution is validated through an exit, just before full completion of the native mainframe command. If the exit fails, then the command fails and returns an error message. Maintaining a specific password format is an example of the objective for which you use custom exits. Oracle Identity Manager exits are engineered to be the last exits called in sequence, which allows the existing exits to function normally. After modifying exits within an LPAR, an initial program load (IPL) of the LPAR may be required.

  Note: You must perform an IPL operation after a system component, such as an exit, is modified.

3.2 Deploying the Reconciliation Agent and Provisioning Agent

To deploy the Reconciliation Agent and Provisioning Agent:

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

   `etc/Provisioning and Reconciliation Connector/Mainframe_ACF2.zip`

2. Transmit or FTP the Jcl.xmit and linklib.xmi files to the mainframe, each with the following specifications:

   `RECFM=FB`, `LRECL=80`, `BLKSIZE=3120`, and `DSORG=PS`

3. Log in to the TSO environment of the mainframe.
4. Run the following command from the ISPF command line to expand the CNTL data set and create the output dataset for installation:

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

5. When prompted to specify restore parameters, enter:

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

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

6. To expand the LINKLIB dataset, enter the following command from the ISPF command line:

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

7. When prompted to enter restore parameters, enter:

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

8. To complete the installation, follow the procedures in IDF.CNTL member #INSTVOY for the Reconciliation Agent, and member #INSTPIO for the

Provisioning Agent. For detailed information about these procedures, see #README in the connector installation media.

3.3 Installing the Exits for the Reconciliation Agent

Because the exit modules are in the z/OS Load Library, an IPL may or may not be required to complete the installation. This depends on whether the z/OS Load Library is added to the LinkList, which is a z/OS storage area defined at the time of an IPL. To allow the LDAP Gateway to capture events, the Reconciliation Agent and its exits must be installed on each LPAR that shares the authentication repository.

To install the Reconciliation Agent exits:

1. Ensure that the exits are modules in a LINKLIB, and the SYS1.PARMLIB activates the exits. For example, a typical system would have an entry in OIMACF2.PARMLIB(LPALSTCA).
2. Copy the exits into the appropriate LPAR for the system. Copy the modules IDFACF2E, IDFACF2P, IDFACF2X into CAI.CAILPA. In addition, copy a utility module called IDFCACHE into CAI.CAILPA. The exit modules are in LINKLIB PDS and must be copied to the appropriate LPAR for the system. For detailed information about this step, see the #README in the connector installation media.
3. Modify the control GSO record for system to add the exits. If the GSO record already exists, then change it to activate the exits, or else add a new record. The CA ACF2 exit activation through z/OS is as shown:

   See Also: Target system documentation for information about GSO

```
READY ,

ACF

 ?  SET CONTROL(GSO) SYSID(SYSTEMNAME)

 ?  INSERT SYSID(SYSTEMNAME) EXITS LIDPOST(IDFACF2E) EXITS EXPPXIT(IDFACF2X)
NEWPXIT(IDFACF2P)

 ACF0A026 RECORD ALREADY EXISTS,

 ?  CHANGE SYSID(SYSTEMNAME) EXITS LIDPOST(IDFACF2E) EXPPXIT(IDFACF2X)
NEWPXIT(IDFACF2P)

  SYSTEMNAME / EXITS LAST CHANGED BY MLIGHT ON 03/22/06-23:24,

  NEWPXIT(IDFACF2P) EXPPXIT(IDFACF2X) LIDPOST(IDFACF2E)

 ? QUIT
```

   Note: SYSTEMNAME mentioned in the code is the name of the deployment system.

4. Refresh the GSO to add in the new values by running the following command:

```
 READY

ACF
```

```
?  F ACF2,REFRESH(EXITS)

ACF79507 GSO PROCESSING COMPLETED WITHOUT ERROR

?  QUIT

READY
```

5. Perform a re-IPL of the system to the make the exits operational.

To load the exits:

1. APF-authorize the LOADLIB, which contains the installation code. Alternatively, you can run the LINKLST to authorize the LOADLIB. To authorize the LOADLIB manually, run the following command:

```
'T PROG=01'
     SYS1.PARMLIB(PROG01)
     APF FORMAT(DYNAMIC)
     APF ADD
             DSNAME(yyyyyyyyyyyyyyy)
             VOLUME(xxxxxx)
```

   Where yyyyyyyyyyyyyyyyyyy is the data set name of the installation load library, and xxxxxx is volume serial.

2. To dynamically activate CA ACF2 adapter exits:

   a. Run the following:

```
SYS1.PARMLIB(PROG78)
EXIT ADD EXITNAME(LIDPOST)   MODULE(IDFACF2E)  STATE(ACTIVE)
EXIT ADD EXITNAME(NEWPXIT)  MODULE(IDFACF2P)  STATE(ACTIVE)
EXIT ADD EXITNAME(EXPPXIT)   MODULE(IDFACF2X)  STATE(ACTIVE)
```

   b. To activate the exits, set the following value form the z/OS master console:

```
T PROG=78
```

3. To dynamically deactivate CA ACF2 adapter exits:

   a. Create a dynamic member as shown:

```
SYS1.PARMLIB(PROG79)
EXIT DELETE ,EXITNAME(LIDPOST), MODULE(IDFACF2E),FORCE=YES
EXIT DELETE ,EXITNAME(NEWPXIT),MODULE(IDFACF2P),FORCE=YES
EXIT DELETE, EXITNAME(EXPPXIT) , MODULE(IDFACF2X),FORCE=YES
```

   b. To deactivate the exits, set the following value form the z/OS master console:

```
T PROG=79
```

3.4 Configuring the Message Transport Layer

This section describes the following message transport layer configuration tasks for TCP/IP:

Note: You must configure TCP/IP as the message transport layer protocol. In this section, perform only the steps that are specific to the protocol that you want to use.

- Configuring TCP/IP
- Building and Operation of the Started Tasks

Note:

- Events detected by the Reconciliation Agent through exit technology are transformed into messages and passed to the LDAP Gateway.
- Because TCP/IP is used, the messages are securely sent to the LDAP Gateway.
- If the LDAP Gateway is not running, then messages are held until the Gateway is returned to service and also secured in an AES-encrypted file on the mainframe. The messages are sent when the LDAP Gateway resumes running.
- If the subpool is stopped by an administrator, then it shuts down the Provisioning Agent, thereby destroying any messages that are not transmitted. However, the messages in the AES-encrypted file are not affected and can be recovered.

3.4.1 Configuring TCP/IP

This section describes how to configure TCP/IP as the message transport layer. Check with the systems programmer for detailed information about using TCP/IP. When you configure TCP/IP, the objective is to establish a stateful connection, allowing the pooling of messages and significantly reducing the load on both the mainframe and the LDAP Gateway server.

To establish a TCP/IP connection with the LDAP Gateway:

1. Start the LDAP Gateway.
2. Start the Provisioning Agent started task, which is also preset to establish a TCP/IP connection to the LDAP Gateway on the specified IP address and port number.
3. Start the Reconciliation Agent started task.

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

- IP address to be used by the mainframe
- IP address for the router
- IP addresses for the domain name servers

Note: To use TCP/IP as the message transport layer, you might need the help of a systems programmer to create ports on the mainframe and to provide security authorizations.

The Provisioning Agent and Reconciliation Agent JCL shipped with the connector must be edited to specify the user parameters that are specific to the environment. To edit the Provisioning Agent and Reconciliation Agent JCL:

1. Insert an installation-approved job card.
2. Change the value for PARM='TCPN=TCPIP' to the name of the running TCP/IP started task. See the code for batch loading of CA ACF2 user IDs in step 5.
3. Change the IP address to the address of the LPAR from where the Provisioning Agent will be started.
4. Change the port number to the port assigned to the LPAR from where the Provisioning Agent will be started from.
5. If your mainframe installation environment requires batch feeds, then run the required VSAMGETU statement. The following is the code and VSAMGETU statement for batch loading of CA ACF2 user IDs:

```
//USR98S01 JOB (,xxxxxxxx,,'PROVISIONING AGENT UPLOAD PROCESS FOR ACIDS'),
//       'UPLOAD CATS TO XELLTE',
//       REGION=2M,CLASS=6,MSGCLASS=Q,
//       USER=ACF2_USER_ID,TIME=1440,
//       NOTIFY=&SYSUID,TYPRUN=HOLD
//*
/*ROUTE PRINT CLE
//*
//PIONEERX EXEC PGM=PIONEERX,REGION=0M,TIME=1440,
//       PARM=('TCPN=TCPIP',
//       'IPAD=HOST_IP_ADDRESS_OF_ACF2',
//       'PORT=6500',
//       'DEBUG=Y')
//STEPLIB DD DISP=SHR,DSN=PPRD.IDF.LINKLIB
//     DD DISP=SHR,DSN=SYS2.TCPACCES.V60.LINK
//     DD DISP=SHR,DSN=TCPIP.SEZATCP
//SYSOUT  DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
//SYSDBOUT DD SYSOUT=*
//SYSABOUT DD SYSOUT=*
//ABENDAID DD SYSOUT=*
//SYSUDUMP DD SYSOUT=*
//VSAMGETU DD DISP=SHR,DSN=LXT99S.FEEDFILE.SORTED
//*
```

For the Reconciliation Agent, this is the same with the exception of the PARM card, which is shown here:

```
//VOYAGERX EXEC PGM=VOYAGERX,REGION=0M,TIME=1440,
//    PARM=('TCPN=TCPIP',
//          'IPAD=&SERVER',
//          'PORT=&PORT',
//          'DEBUG=Y',
//          'ESIZE=16',
//          'DELAY=00',
//          'STARTDELAY=10',
//          'PRTNCODE=SHUTRC')
//STEPLIB  DD DISP=SHR,DSN=IDF.LINKLIB
//         DD DISP=SHR,DSN=TCPIP.SEZATCP
//CACHESAV DD DSN=VOYAGER.CACHESAV,DISP=SHR
//SYSPRINT DD SYSOUT=X
//SYSUDUMP DD SYSOUT=X
//
```

In these lines of code:

- ESIZE=16 is used to denote AES encryption.
- DELAY is not used for this connector. Do not change the default value (00) of this property.
- STARTDELAY=10 is the recommended value (in seconds).
- PRTNCODE=SHUTRC shows all MVS condition codes after the Reconciliation Agent shuts down. Alternatively, PRTNCODE=TERMRC shows an MVS condition code of 0000 (signifying successful completion) after the Reconciliation Agent shuts down.

  Note: To shut down the Reconciliation Agent, run the following command from the z/OS operator's console:

  ```
  'F VOYAGER,SHUTDOWN'
  ```

  To shut down the Provisioning Agent, run the following command from the z/OS operator's console:

  ```
  'F PIONEER,SHUTDOWN'
  ```

- DEBUG can be one of the following for both the Reconciliation Agent and Provisioning Agent:
  - N is for no debugging output.
  - Y is for debugging output.
  - Z is for detailed debugging output.

  Note: If the "data set in use" message is displayed when you attempt to edit a member, then press the F1 key twice to see the member that you are trying to edit. The name of the job that is causing the exception is displayed. On the z/OS console, you can remove the job by using the `p` or the `c` command.

Apply the following guidelines while working with the Reconciliation Agent:

- The subpool (RUNSTART.JCL) must be started before starting the Reconciliation Agent. The subpool is used as an in-memory storage for message creation.
- Because you are using TCP/IP, the LDAP Gateway must be started first. If the Reconciliation Agent is started first, then it will throw an error with RETCODE=-01 and ERRORNO=61 because the LDAP Gateway will not be available.
- When the LDAP Gateway is not available, the Reconciliation Agent does not shut down when you run the `'F VOYAGER,SHUTDOWN'` command. In this scenario, refer to the following:
  - The following log entry:

    ```
    0090  IDMV201I - VOYAGER CONNECTION TO GATEWAY FAILED
    ```

  - The following error message is generated:

    ```
    0090  IEE342I MODIFY   REJECTED-TASK BUSY
    ```

When these error messages are generated, you must run CANCEL to force the Reconciliation Agent to shut down.

3.4.2 Building and Operation of the Started Tasks

There are two different JCLs to set up and run the Provisioning Agent and Reconciliation Agent. RUNPIONX and RUNVOYAX are samples to set up the started tasks.

The parameters for RUNPIONX are:

- TCPN: The name of the TCP process
- IPAD: The IP address of the computer on which the Provisioning Agent is running
- PORT: The incoming connection port for the Provisioning Agent
- DEBUG: The debug switch for showing the extra output
- ESIZE: The AES encryption used

The parameters for RUNVOYAX are:

- TCPN: The name of the TCP process
- IPAD: The IP address of the computer on which the Reconciliation Agent is connected
- PORT: The outgoing connection port for the Reconciliation Agent
- DEBUG: The debug switch for showing the extra output
- ESIZE: The AES encryption used

The RUNPIONX and RUNVOYAX are started tasks (STC). The source code for each started task procedure is as follows:

For RUNPIONX:

```
//ADCDMPPT JOB SYSTEMS,MSGLEVEL=(1,1),MSGCLASS=X,CLASS=A,PRTY=8,
//  NOTIFY=&SYSUID,REGION=4096K
//PIONEERX EXEC PGM=PIONEERX,REGION=0M,TIME=1440,
//  PARM=('TCPN=TCPIP',
//     'IPAD=&SERVER',
//     'PORT=&PORT'
//     'DEBUG=Y',
//     'ESIZE=16',
//     'LPAR=ACF2-SYS')

//    'LPAR= name ')
//STEPLIB DD DISP=SHR,DSN=IDF.LINKLIB
//     DD DISP=SHR,DSN=TCPIP.SEZATCP
//BATJINFO DD DISP=SHR,DSN=hlq.BATJCARD
//VSAMGETU DD DISP=SHR ,DSN=hlq.SWUSERS
//VSAMGETO DD DISP=SHR,DSN=hlq.ACF2COUT
//SYSPRINT DD SYSOUT=X
//SYSUDUMP DD SYSOUT=X
//
```

Note: In the code, hlq stands for installation high-level qualifier.

For RUNVOYAX:

```
//ADCDMRVX JOB SYSTEMS,MSGLEVEL=(1,1),MSGCLASS=X,CLASS=A,PRTY=8,
//  NOTIFY=&SYSUID,REGION=4096K
//VOYAGERX EXEC PGM=VOYAGERX,REGION=0M,TIME=1440,
//  PARM=('TCPN=TCPIP',
//     'IPAD=IP_ADDRESS_OF_ACF2_SYSTEM',
//     'PORT=5190',
//     'DEBUG=Y')
//CACHESAV DD DISP=SHR,DSN=VOYAGER.CACHESAV
//SYSPRINT DD SYSOUT=X
//SYSUDUMP DD SYSOUT=X
//
```

For the Reconciliation Agent:

The dataset attributes for Cachesav are:

> **Note:** Cachesav is a data set (file) that is required for Voyager startup. The attributes are the necessary file parameters and must be specified by the administrator performing the installation.

```
DSORG(PS),LRECL=(32),RECFM=(FB),BLKSIZE=(27968)
```

The dataset attributes for each of the Pioneer required data sets are:

```
BATJCARD - DSORG=(PS),LRECL=(80),RECFM=(FB),BLKSIZE=(8000)
VSAMGETU - DSORG=(PS),LRECL=(80),RECFM=(FB),BLKSIZE=(8000)
VSAMGETO - DSORG=((PS),LRECL=(133),RECFM=(FB),BLKSIZE=(27930)
```

VSAMGETU needs to be allocated if it is not used.

For the Provisioning Agent:

The BATJCARD data set contents required for ACF2 rule processing, which means adding users to data sets, are as shown:

```
//QACF0001 JOB SYSTEMS,MSGLEVEL=(1,1),MSGCLASS=X,
//     CLASS=A,PRTY=8,NOTIFY=&SYSUID,REGION=4096K,USER=abcdef
//ACFJOB  EXEC  PGM=IKJEFT01,DYNAMNBR=25
//SYSTSPRT DD DISP=SHR,DSN=ADCDM.ACF2COUT
//SYSHELP DD DISP=SHR,DSN=SYS1.HELP
//SYSLBC  DD DISP=SHR,DSN=SYS1.BRODCAST
//STEPLIB DD DISP=SHR,DSN=IDF.LINKLIB
```

In the second line of code, note `user=abcdef`. This must be a system level UID with ACF2 privileges to create, modify, and delete users. The SYSTSPRT 'DD' data set name must match the Pioneer 'DD' name in the VSAMGETO 'DD'.

4

Configuring the Connector

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

This chapter discusses the following topics:

4.1 Configuring Trusted Source Reconciliation

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

The XML file for trusted source reconciliation, oimAcf2TrustedXellerateUser.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. Click the **Deployment Management** link on the left navigation pane.
3. Click the **Import** link under Deployment Management. A dialog box for opening files is displayed.
4. Locate and open the oimAcf2TrustedXellerateUser.xml file, which is in the *OIM_HOME*/xellerate/XLIntegrations/acf2/xml directory. Details of this XML file are shown on the File Preview page.
5. Click **Add File**. The Substitutions page is displayed.
6. Click **Next**. The Confirmation page is displayed.
7. Click **Import**.
8. In the message that is displayed, click **Import** to confirm that you want to import the XML file, and then click **OK**.

4.2 Running Initial Reconciliation

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

To start the initial reconciliation run:

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

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

2. In a text editor, open the *OIM_HOME*/xellerate/JavaTasks/initialAcf2Adv.properties file.

3. In the initialAcf2Adv.properties file, specify values for the properties that control the initial reconciliation script.

   Note: Ensure that properties that are common to both the initialAcf2Adv.properties file and lib/acf2Connection.properties file have the same values.

   The properties in the file that control initial reconciliation are:

   - xlAdminId: Oracle Identity Manager administrator ID.
   - idfTrusted: Enter `true` as the value of this property to specify that you want to perform trusted source reconciliation with the target system. Enter `false` to specify target resource reconciliation.
   - _resourceObject_: Resource object for reconciliation.
   - _itResource_: IT resource for target resource reconciliation.
   - _dummyPwd_: Dummy password for initial reconciliation.
   - isFileRecon: The value for this is `true`, which specifies file-based initial reconciliation. You cannot change this value.
   - userFile: Enter the name of the TXT file in which you have stored the user IDs of the target system users that you want to reconcile. This file must be placed in the following directory:

     OIM_HOME/xellerate/JavaTasks

     For more information about this file, see the sample user.txt file in the `scripts` directory on the installation media.
   - #REMOVED: Ignore this property.
   - reconAttrs: Fields that are reconciled.
   - tsoReconAttrs: TSO fields that are reconciled.
   - idfServerUrl: Enter the LDAP Gateway host and port.

   You are not allowed to change the values of the rest of the properties in the initialAcf2Adv.properties file.

   The following is a sample set of values for the properties in the initialAcf2Adv.properties file:

```
xlAdminId:xelsysadm
idfTrusted:false
_resourceObject_:OIMAcf2ResourceObject
_itResource_:Acf2Resource
_dummyPwd_:Pwd123
isFileRecon:true
userFile:user.txt
#REMOVED: sn,givenName,revoke,identificationUID,cicsid,minDays,maxDays,prefix,
reconAttrs:uid,cn,userPassword,activeDate,passwordExpire,accessCnt,accessDate,a
ccessSrce,accessTime,kerbVio,kerbCurv,pswdDate,pswdInv,pswdTod,pswdVio,defaultG
roup,secVio,updTod
tsoReconAttrs:tsoDftPfx,tsoAcctNum,tsoProc,tsoSize,tsoRba,tsoUnit,tsoPerf,tsoCo
mmand,tsoDest,tsoHoldclass,tsoMsgclass,tsoMaxSize,tsoSysoutclass,tsoSubmitclass
,tsoMail,tsoAcctPriv,tsoAllCmds,tsoJcl,tsoWtp,tsoFscrn,tsoMount,tsoOperator,tso
Notices,tsoPrompt,tsoLgnAcct,tsoLgnMsg,tsoLgnPerf,tsoLgnProc,tsoLgnTime,tsoLgnR
cvr,tsoLgnSize,tsoLgnUnit,tsoIntercom
idfServerUrl:ldap://localhost:5389
idfAdminDn:cn=idfAcf2Admin, dc=acf2,dc=com
idfAdminPwd:idfAcf2Pwd
ouPeople:ou=People
ouGroups:ou=Groups
ouDatasets:ou=Datasets
ouResources:ou=Resources
ouFacilities:ou=Facilities
ouBaseDn:dc=acf2,dc=com
idfSystemAdminDn:cn=Directory Manager, dc=system,dc=backend
idfSystemAdminPwd:testpass
idfSystemDn:dc=system,dc=backend
```

4. In a text editor, open the *OIM_HOME*/xellerate/JavaTasks/run_initial_recon_provisioning script.
5. To perform trusted source reconciliation:

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

   a. Set the value of the JV parameter in the script to `-X` to reconcile Xellerate User.
   b. Run the script.

      When you run the script, it opens the file (whose name is the value of the userFile property) containing user data and reads the user IDs of the users that you want to reconcile. Then, the loader, which is the initial load script, connects to the LDAP Gateway and issues commands to fetch the required user data from the target system. This data is loaded in the LDAP Gateway cache and reconciliation events are submitted to Oracle Identity Manager. Xellerate Users are created for all the target system users identified by the userFile property in the initialAcf2Adv.properties file.
   c. In the run_initial_recon_provisioning script, change the value of the JV parameter to `-R` to run target resource reconciliation.
   d. Run the script again.

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

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

a. In a text editor, open the initialAcf2Adv.properties file and enter `false` as the value of the idfTrusted property to specify that you want to perform target resource reconciliation with the target system.

   Make the same change in the acf2Connection.properties file.

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

c. Run the script again.

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

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

If a problem exists with fault tolerance and the LDAP Gateway and Reconciliation Agent are down for a long time, and there is a possibility of losing user data, then run full reconciliation.

4.3 Configuring Account Status Reconciliation

When a user's account is disabled or enabled on the target system, the user is reconciled and the changed status is reflected in Oracle Identity Manager. To configure the reconciliation of account status data:

1. In the *LDAP_INSTALL_DIR*/acf2Connection.properties file, add the name of the Status field to the reconAttrs section.

   Make the same change in the initialAcf2Adv.properties file, which is in the *OIM_HOME*/xellerate/JavaTasks directory.

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

3. In the Design Console:

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

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

4.4 Adding New Fields for Provisioning

To add a new field for provisioning to CA ACF2:

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

1. Log in to the Oracle Identity Manager Design Console.
2. Expand the **Development Tools** folder.

3. Double-click **Form Designer**.
4. Search for and open the CA ACF2 main process form, such as the UD_ACF2_ADV_MODEL process form.
5. Click **Create New Version**, and then click **Add**.
6. Enter the details of the field. For example, if you are adding the uid field, then enter USER in the Name field, and then enter the rest of the details of this field.
7. Click Save, and then click **Make Version Active**.
8. Expand the **Administration** folder.
9. Double-click **Lookup Definition**.
10. Add the new Attribute Form Column Name to the AtMap.ACF2 lookup definition. For example, Code Key value is UD_ACF2_ADV_MODEL and Decode value is model. The Code Key value is the column name in the ACF2 main process form, and the Decode value is the name of the field on the target CA ACF2 system, which maps to the corresponding LDAP field name.
11. If you want to add a update process task for a new custom field in Oracle Identity Manager, create a new process task associated with the Oracle Identity Manager field by using the adpMODIFYUSER adapter for CA ACF2.

5 Troubleshooting

This chapter contains the following sections:

5.1 Troubleshooting

Table 5–1 lists solutions to some commonly encountered issues associated with the CA ACF2 Advanced connector.

Table 5–1 Troubleshooting

Problem Description	Solution
Oracle Identity Manager cannot establish a connection to the CA ACF2 server.	■ Ensure that the mainframe server is up and running. ■ Check that the necessary ports are working. ■ Start the LDAP Gateway first and then the mainframe JCL started task. This is a requirement based on how TCP/IP operates. Check that the server IP, which hosts the Gateway is configured in the Reconciliation Agent JCL. ■ View the Gateway logs to determine if messages are being sent or received. ■ Examine the Oracle Identity Manager configuration to verify that the IP address, admin ID, and admin password are correct. ■ Check with the mainframe platform manager to verify that the mainframe user account and password have not been changed.
The mainframe does not appear to respond.	■ Ensure that the Oracle Identity Manager mappings are correct. ■ Check the configuration mappings for the Advanced Adapter Gateway.
A particular use case does not appear to be functioning.	■ Check for the use case event in question on the Gateway Server Log. Then check for the event in the specific log assigned to that Advanced Connector. ■ If the event does not register in either of these two logs, then investigate the connection between Oracle Identity Manager and the connector Gateway. ■ If the event is in the log but the command failed to make the intended change on a mainframe user profile, then check for configuration and connections between the Gateway and the mainframe. ■ Check that TCP/IP is turned on.
The LDAP Gateway fails and stops working	If this problem occurs, then the Reconciliation Agent stops sending messages to the LDAP Gateway. Instead, it stores them in the subpool cache. When this happens, restart the LDAP Gateway instance so that the Reconciliation Agent reads the subpool cache and resends the messages.
The LDAP Gateway is running. However, the Reconciliation Agent fails and stops working	If this problem occurs, then all events are sent to the subpool cache. If the mainframe fails, then all messages are written to the disk. When this happens, restart the Reconciliation Agent instance so that it reads messages from the disk or subpool cache and resends the messages.

5.2 Guidelines on Using the Connector

Apply the following guidelines while using the connector:

- The CA ACF2 Advanced connector can accept and transmit any non-ASCII data to the mainframe, but the mainframe does not accept non-ASCII characters. As a result, any task that requires non-ASCII data transfer fails. In addition, there is no provision in the connector to indicate that the task has failed or that an error has occurred on the mainframe. You must exercise caution when providing non-ASCII data to the connector.

- 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.

6

Known Issues

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

- **Bug 6668844**

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

- **Bug 6904041**

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

- **Bug 7189194**

  In the run.sh and run.bat files, the following lines suggest that the application server home directory, APPSERVER_HOME, is for JBoss Application Server and Oracle Application Server only:

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

  And:

  ```
  ##### OC4J  ##################
  #APPSERVER_HOME=/u01/app/oracle/product/10.1.3.1/oimas
  ```

  Correct the first comment to set APPSERVER_HOME to the home directory for the application server that Oracle Identity Manager is running on. And remove the lines for Oracle Application Server.

- **Bug 7033009**

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

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

– Backslash (\)

Index