

Oracle® Identity Manager

Connector Guide for UNIX SSH

Release 9.0.4

E10447-12

September 2013

Oracle Identity Manager Connector Guide for UNIX SSH, Release 9.0.4

E10447-12

Copyright © 2011, 2013, Oracle and/or its affiliates. All rights reserved.

Primary Author: Gauhar Khan

Contributing Authors: Sridhar Machani, Alankrita Prakash, Gowri G. R, Deena Purushothaman

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate failsafe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Contents

| | |
|--|------|
| Preface | ix |
| Audience | ix |
| Documentation Accessibility | ix |
| Related Documents | ix |
| Documentation Updates | ix |
| Conventions | x |
| | |
| What's New in Oracle Identity Manager Connector for UNIX SSH? | xi |
| Software Updates | xi |
| Documentation-Specific Updates..... | xix |
| | |
| 1 About the Connector | |
| 1.1 Certified Components | 1-1 |
| 1.2 Certified Languages..... | 1-3 |
| 1.3 Connector Architecture..... | 1-3 |
| 1.3.1 Reconciliation Process..... | 1-4 |
| 1.3.2 Provisioning Process | 1-5 |
| 1.4 Features of the Connector..... | 1-6 |
| 1.4.1 Support for Both Target Resource and Trusted Source Reconciliation | 1-6 |
| 1.4.2 Support for Limited Reconciliation..... | 1-6 |
| 1.4.3 Support for Batched Reconciliation | 1-7 |
| 1.4.4 Support for Both Full and Incremental Reconciliation | 1-7 |
| 1.4.5 Support for Adding Custom Attributes for Reconciliation and Provisioning | 1-7 |
| 1.4.6 Transformation of Account Data..... | 1-7 |
| 1.4.7 Support for Reconciliation of User Status from the Target System | 1-7 |
| 1.5 Lookup Definitions Used During Connector Operations..... | 1-7 |
| 1.5.1 Lookup Definitions Synchronized with the Target System | 1-7 |
| 1.5.2 Other Lookup Definitions | 1-8 |
| 1.6 Connector Objects Used During Target Resource Reconciliation and Provisioning..... | 1-8 |
| 1.6.1 User Attributes for Target Resource Reconciliation and Provisioning..... | 1-8 |
| 1.6.2 Reconciliation Rule for Target Resource Reconciliation | 1-10 |
| 1.6.3 Reconciliation Action Rules for Target Resource Reconciliation..... | 1-10 |
| 1.6.4 Provisioning Functions | 1-12 |
| 1.7 Connector Objects Used During Trusted Source Reconciliation | 1-12 |
| 1.7.1 User Attributes for Trusted Source Reconciliation..... | 1-12 |

| | | |
|-------|---|------|
| 1.7.2 | Reconciliation Rule for Trusted Source Reconciliation | 1-13 |
| 1.7.3 | Reconciliation Action Rules for Trusted Source Reconciliation | 1-14 |
| 1.8 | Roadmap for Deploying and Using the Connector | 1-15 |

2 Deploying the Connector

| | | |
|-----------|--|------|
| 2.1 | Files and Directories on the Installation Media | 2-1 |
| 2.2 | Determining the Release Number of the Connector | 2-3 |
| 2.3 | Configuring the Target System | 2-3 |
| 2.3.1 | Platform-Specific Configuration Steps | 2-3 |
| 2.3.1.1 | Configuration Steps for Solaris and Linux | 2-3 |
| 2.3.1.2 | Configuration Steps for AIX | 2-4 |
| 2.3.1.3 | Configuration Steps for HP-UX | 2-4 |
| 2.3.2 | Installing OpenSSH | 2-5 |
| 2.3.3 | Creating a Target System User Account for Connector Operations | 2-7 |
| 2.3.3.1 | Creating a Target System User Account for Connector Operations on Solaris... | 2-7 |
| 2.3.3.1.1 | Creating a Sudo User for Connector Operations | 2-7 |
| 2.3.3.1.2 | Creating an RBAC User Account for Connector Operations | 2-9 |
| 2.3.3.2 | Creating a Target System User Account for Connector Operations on HP-UX | 2-10 |
| 2.3.3.3 | Creating a Target System User Account for Connector Operations on AIX | 2-12 |
| 2.3.3.4 | Creating a Target System User Account for Connector Operations on Red Hat Advanced Server 2.1 | 2-13 |
| 2.3.3.5 | Creating a Target System User Account for Connector Operations on Red Hat Enterprise Linux 3.x or Red Hat Linux 4.x | 2-15 |
| 2.3.4 | Public Key Authentication (SSH Key Generation) | 2-17 |
| 2.3.4.1 | Configuring Public Key Authentication | 2-17 |
| 2.3.4.2 | Configuring SSH Public Key Authentication | 2-18 |
| 2.4 | Installing the Connector on Oracle Identity Manager Release 9.1.0.x or Release 11.1.1 | 2-21 |
| 2.4.1 | Running the Connector Installer | 2-21 |
| 2.4.2 | Copying the sshfactory.jar File | 2-23 |
| 2.4.3 | Configuring the IT Resource | 2-24 |
| 2.4.4 | Copying the Configuration Files | 2-26 |
| 2.5 | Configuring the Oracle Identity Manager Server | 2-26 |
| 2.5.1 | Configuring the Target System As a Trusted Source | 2-27 |
| 2.5.2 | Changing to the Required Input Locale | 2-28 |
| 2.5.3 | Clearing Content Related to Connector Resource Bundles from the Server Cache | 2-28 |
| 2.5.4 | Enabling Logging | 2-30 |
| 2.5.4.1 | Enabling Logging on Oracle Identity Manager Release 9.1.0.x | 2-30 |
| 2.5.4.2 | Enabling Logging on Oracle Identity Manager Release 11.1.1 | 2-32 |
| 2.5.5 | Configuring Oracle Identity Manager for Request-Based Provisioning | 2-34 |
| 2.5.5.1 | Importing Request Datasets Using Deployment Manager | 2-35 |
| 2.5.5.2 | Copying Predefined Request Datasets | 2-35 |
| 2.5.5.3 | Importing Request Datasets into MDS | 2-36 |
| 2.5.5.4 | Enabling the Auto Save Form Feature | 2-37 |
| 2.5.5.5 | Running the PurgeCache Utility | 2-37 |

3 Using the Connector

| | | |
|-----|--|-----|
| 3.1 | Performing First-Time Reconciliation | 3-1 |
|-----|--|-----|

| | | |
|---------|--|------|
| 3.2 | Scheduled Task for Lookup Field Synchronization..... | 3-2 |
| 3.3 | Configuring Reconciliation..... | 3-3 |
| 3.3.1 | Full Reconciliation | 3-3 |
| 3.3.2 | Limited Reconciliation | 3-4 |
| 3.3.3 | Batched Reconciliation | 3-4 |
| 3.3.4 | Reconciliation Scheduled Tasks..... | 3-4 |
| 3.4 | Configuring Scheduled Tasks | 3-6 |
| 3.4.1 | Configuring Scheduled Tasks on Oracle Identity Manager Release 9.1.0.x or Release 11.1.1 | 3-7 |
| 3.5 | Guidelines on Performing Provisioning Operations | 3-8 |
| 3.6 | Performing Provisioning Operations..... | 3-9 |
| 3.6.1 | Direct Provisioning..... | 3-10 |
| 3.6.2 | Request-Based Provisioning..... | 3-11 |
| 3.6.2.1 | End User's Role in Request-Based Provisioning | 3-12 |
| 3.6.2.2 | Approver's Role in Request-Based Provisioning | 3-13 |
| 3.7 | Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1 | 3-13 |

4 Extending the Functionality of the Connector

| | | |
|-----|---|-----|
| 4.1 | Adding Custom Attributes for Target Resource Reconciliation..... | 4-1 |
| 4.2 | Adding Custom Attributes for Provisioning | 4-3 |
| 4.3 | Configuring the Connector for Multiple Installations of the Target System | 4-7 |
| 4.4 | Transforming Data Reconciled Into Oracle Identity Manager..... | 4-8 |

5 Testing and Troubleshooting

6 Known Issues

A Privileges Required for Performing Provisioning and Reconciliation

| | | |
|-----|--|-----|
| A.1 | Privileges Required for Running Commands on Non-AIX..... | A-1 |
| A.2 | Privileges Required for Running Commands on HP-UX | A-1 |
| A.3 | Privileges Required for Running Commands on AIX..... | A-1 |

B Sample Transformation Class

Index

List of Figures

| | | |
|-----|---|------|
| 1-1 | Architecture of the Connector | 1-3 |
| 1-2 | Reconciliation Rule for Target Resource Reconciliation | 1-10 |
| 1-3 | Reconciliation Action Rules for Target Resource Reconciliation..... | 1-11 |
| 1-4 | Reconciliation Rule for Trusted Source Reconciliation | 1-14 |
| 1-5 | Reconciliation Action Rules for Trusted Source Reconciliation..... | 1-15 |

List of Tables

| | | |
|-----|---|------|
| 1-1 | Certified Components | 1-2 |
| 1-2 | Other Lookup Definitions..... | 1-8 |
| 1-3 | User Attributes for Target Resource Reconciliation and Provisioning | 1-9 |
| 1-4 | Action Rules for Target Resource Reconciliation..... | 1-11 |
| 1-5 | Provisioning Functions | 1-12 |
| 1-6 | User Attributes for Trusted Source Reconciliation | 1-12 |
| 1-7 | Action Rules for Target Source Reconciliation | 1-14 |
| 2-1 | Files and Directories on the Installation Media..... | 2-1 |
| 2-2 | Log Levels and ODL Message Type:Level Combinations..... | 2-32 |
| 3-1 | Attributes of the Scheduled Tasks for Lookup Field Synchronization..... | 3-3 |
| 3-2 | Attributes of the User Reconciliation Scheduled Tasks | 3-5 |
| 3-3 | Scheduled Tasks for Lookup Field Synchronization and Reconciliation | 3-6 |

Preface

This guide describes the connector that is used to integrate Oracle Identity Manager with UNIX SSH.

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 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 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. |
| <i>italic</i> | 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 Oracle Identity Manager Connector for UNIX SSH?

This chapter provides an overview of the updates made to the software and documentation for the UNIX SSH connector in release 9.0.4.15.

Note: Release 9.0.4.15 of the connector comes after release 9.0.4.12. Release numbers 9.0.4.13 and 9.0.4.14 have not been used.

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

- [Software Updates](#)
This section describes updates made to the connector software.
- [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 9.0.4.15](#)
- [Software Updates in Release 9.0.4.12](#)
- [Software Updates in Release 9.0.4.11](#)
- [Software Updates in Release 9.0.4.7](#)
- [Software Updates in Release 9.0.4.6](#)
- [Software Updates in Release 9.0.4.5](#)
- [Software Updates in Release 9.0.4.4](#)
- [Software Updates in Release 9.0.4.3](#)
- [Software Updates in Release 9.0.4.2](#)

Software Updates in Release 9.0.4.15

The following are software updates implemented in release 9.0.4.15:

- [Support for New Target System](#)
- [Support for Importing Request Dataset XML Files](#)

- [Resolved Issues in Release 9.0.4.15](#)

Support for New Target System

From this release onward, the connector adds support for HP-UX version 11iv3 (11.31) as the target system.

See [Section 1.1, "Certified Components"](#) for the full list of certified target systems.

Support for Importing Request Dataset XML Files

From this release onward, the connector provides support for importing a request dataset XML file into Oracle Identity Manager by using the Deployment Manager on Oracle Identity Manager 11g release 1 (11.1.1).

The installation media of this release includes a request dataset file, SSHConnectorRequestDatasets.xml, which is available in the xml directory.

See [Section 2.5.5.1, "Importing Request Datasets Using Deployment Manager"](#) for more information.

Resolved Issues in Release 9.0.4.15

The following table describes issues resolved in release 9.0.4.15:

| Bug Number | Issue | Resolution |
|------------|--|--|
| 12547932 | The performance of the connector was slow. | This issue has been resolved. The reconciliation of records can now be initiated in parallel, which reduces the time taken for reconciliation. |
| 9314911 | The connector did not support AIX 6.1 as a target resource. | This issue has been resolved. AIX 6.1 is now supported as a target resource. |
| 11737066 | When running the SSH User Target Resource Reconciliation Task, if the number of users to be reconciled is greater than the batch size, an exception is thrown. | This issue has been resolved. The reconciliation task runs successfully for multiple batches. |
| 7498112 | The connector did not support HP-UX11i V2,V3 as a target resource. | This issue has been resolved. HP-UX11i V2,V3 is now supported as a target resource. |

Software Updates in Release 9.0.4.12

The following are the software updates in release 9.0.4.12:

- [Support for New Oracle Identity Manager Release](#)
- [Support for Request-Based Provisioning](#)
- [Support for New Target System](#)
- [Support for User Account Status Reconciliation](#)
- [Resolved Issues in Release 9.0.4.12](#)

Support for New Oracle Identity Manager Release

From this release onward, the connector can be installed and used on Oracle Identity Manager 11g 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 11g release 1 (11.1.1).

See [Section 3.6.2, "Request-Based Provisioning"](#) for more information.

Support for New Target System

From this release onward, the connector adds support for IBM AIX 5L Version 6.1 as the target system.

See [Section 1.1, "Certified Components"](#) for the full list of certified target systems.

Support for User Account Status Reconciliation

From this release onward, the connector can reconcile user account status information from the target system

Resolved Issues in Release 9.0.4.12

The following table lists issues resolved in release 9.0.4.12:

| Bug Number | Issue | Resolution |
|------------|--|---|
| 7374688 | Reconciliation of user records in the sudo mode failed because the connector attempted to run a shell. | This issue has been resolved. |
| 9295029 | When an update task failed, the status of the corresponding process task adapters changed from Provisioned to Provisioning. | This issue has been resolved. The status of the process task adapters do not change when the corresponding update task fails. |
| 9611960 | When performing a Create User provisioning operation on AIX, the group name must be specified as the value of the Primary Group Name lookup field. However, instead of displaying group names, the Primary Group Name lookup field displayed group IDs. The happened due to the following reason: After performing lookup field synchronization by running the TelnetSSHGroupLookupReconTask scheduled task, the Code Key column of the UD_Lookup_SSH_PrimaryGroupNames lookup definition contained the group IDs, and the Decode column contained the group names. | This issue has been resolved. After you perform lookup field synchronization, the connector now reconciles group names into the Code Key column, and group IDs into the Decode column of the UD_Lookup_SSH_PrimaryGroupNames lookup definition. Therefore, for AIX and the other target systems, the connector passes the group name instead of the group ID. |
| 9611211 | The Confirm Password field on the process form required users to enter their passwords 2 times. | The Confirm Password field has been removed from the process form. |

Software Updates in Release 9.0.4.11

The following table lists issues resolved in release 9.0.4.11:

| Bug Number | Issue | Resolution |
|------------|--|---|
| 9100879 | The Delete User provisioning operation did not work. | This issue has been resolved. The Delete User provisioning operation now works correctly. |

| Bug Number | Issue | Resolution |
|-------------------|--|--|
| 9195323 | The Create User provisioning operation failed when it was retried. | This issue has been resolved. The Create User provisioning operation can be retried. |

Software Updates in Release 9.0.4.7

The following table lists issues resolved in release 9.0.4.7:

| Bug Number | Issue | Resolution |
|-------------------|--|---|
| 7520249 | During reconciliation, you could not transform values of the target system field before they were stored in Oracle Identity Manager. | This issue has been resolved. You can now transform the values of the target system fields before they are stored in Oracle Identity Manager. See the "Transforming Data Reconciled Into Oracle Identity Manager" chapter in the connector guide for more information. |
| 7563415 | During reconciliation, the Group Name field was reconciled as a number and not as the exact name because it was stored directly as the group ID in the target system. | This issue has been resolved. During reconciliation, the exact name of the Group Name field is reconciled. |
| 8341984 | In the Create User process task, the default value of the Map To variable was IT Resource. This value was incorrect. | This issue has been resolved. The Map To variable in the Create User process task displays the correct default value. The default value of Map To variable is now Process Data. |
| 8396795 | During connector deployment, the lib/xliSSH.jar file on the installation media was not automatically copied into the <i>OIM_HOME/xellerate/ScheduleTask</i> directory. | This issue has been resolved. The lib/xliSSH.jar file is now automatically copied to the <i>OIM_HOME/xellerate/ScheduleTask</i> directory. |

Software Updates in Release 9.0.4.6

The following table lists issues resolved in release 9.0.4.6:

| Bug Number | Issue | Resolution |
|-------------------|---|---|
| 7478452 | You use the IT resource to specify the credentials of the SUDO user that you want to use for connector operations. If this SUDO user did not have the required permissions, then the target system did not allow you to perform Disable User provisioning operations. This is expected behavior. However, the status of the user was set to Disabled on Oracle Identity Manager even though the status of the user on the target system remained unchanged. | This issue has been resolved. If the SUDO user does not have the permissions required to disable users on the target system, then an appropriate message is displayed on the Administrative and User Console. |

| Bug Number | Issue | Resolution |
|------------|--|--|
| 7503701 | The target system does not allow you to delete a user who is logged in to the system. This is expected behavior. However, even when the target system did not allow the deletion of a user, the status of the user (resource) on Oracle Identity Manager was changed to Deleted (Revoked). | This issue has been resolved. If the target system does not allow the deletion of a user, then an appropriate message is displayed as the outcome of the Delete User provisioning operation. The item describing this issue has been removed from Chapter 6, "Known Issues" . |

Software Updates in Release 9.0.4.5

The following are software updates in release 9.0.4.5:

- [Support for Role-Based Access Control \(RBAC\) on Solaris](#)
- [Resolved Issues in Release 9.0.4.5](#)

Support for Role-Based Access Control (RBAC) on Solaris

In earlier releases, you had to provide the credentials of the root or sudo user for letting Oracle Identity Manager communicate with the Solaris target system. This release supports the role-based access control (RBAC) feature of Solaris. From this release onward, Oracle Identity Manager can communicate with Solaris by using a user account to which you assign the minimum required privileges.

See [Section 2.3.3.1.2, "Creating an RBAC User Account for Connector Operations"](#) on for more information.

The following are some of the changes made in the IT resource:

- The `Whether SUDO Admin Mode` parameter has been renamed to `Sudo Or RBAC`.
- Descriptions of the `Admin UserId` and `Admin Password/Private file Pwd` parameters have been modified.
- The `RBAC Role Name` and `RBAC Role Passwd` parameters have been added.

See [Chapter 2, "Deploying the Connector"](#) for information about these parameters.

Resolved Issues in Release 9.0.4.5

The following table lists issues resolved in release 9.0.4.5:

| Bug Number | Issue | Resolution |
|------------|--|---|
| 5503263 | The "Create Home Directory" field is a check box on the Administrative and User Console. If you selected this check box, the numeral 1 was displayed on the page that summarizes input you provide during provisioning operations. | The check box has been changed to a radio button. If you select the "Create Home Directory" option, then the word "Yes" is displayed on the page that summarizes input. If you do not select the option, then the word "No" is displayed. |
| 7133380 | A user for whom an SSH account was created on AIX through a provisioning operation was forced to change the password at first login. | Password change at first login is not enforced for newly created SSH accounts on AIX. |

| Bug Number | Issue | Resolution |
|------------|---|---|
| 7225692 | To stop a scheduled task, you use the Stop Execution option in the Design Console. This option did not work in earlier releases. | You can now use the Stop Execution option to stop scheduled tasks. Note: When you stop a batched reconciliation run, reconciliation stops at the end of the batch being reconciled. |
| 7345302 | During a provisioning operation, the home directory was not created if you specified an invalid path on the target system host computer. However, the status of the process task was Completed. | If an invalid home directory path is specified, then the "Invalid Home directory" error message is displayed on the Administrative and User Console. |
| 7347256 | An error was thrown when a user connected to an HP-UX target system was updated through a provisioning operation performed on Oracle Identity Manager. The response from the target system was not correctly parsed and displayed as an error message on the Administrative and User Console. | The "User currently in use" message is displayed if you try to update any attribute of a user who is currently logged in to the target system. |

Software Updates in Release 9.0.4.4

The following are software updates in release 9.0.4.4:

- [Using the Connector Installer](#)

Using the Connector Installer

From Oracle Identity Manager release 9.1.0 onward, the Administrative and User Console provides the Connector Installer feature. This feature can be used to automate the connector installation procedure.

See [Section 2.4, "Installing the Connector on Oracle Identity Manager Release 9.1.0.x or Release 11.1.1"](#) for details.

Software Updates in Release 9.0.4.3

The following are software updates in release 9.0.4.3:

- The `Primary Group Name` field on the process form has been converted into a lookup field. During a provisioning operation, you can now select a primary group instead of entering the name of the group. The `TelnetSSHGroupLookupReconTask` scheduled task has been added to reconcile (synchronize) the values in the lookup definition with primary group names in the target system.
- The name of the target resource reconciliation scheduled task has been changed from `SSH User Non Trusted Reconciliation task` to `SSH Target Resource User Reconciliation Task`.
- The level of detail has been increased for data logged when you set the log level to `DEBUG`. With this log level, it is now easier to track down the cause of an error recorded in the log file.
- The following table lists issues resolved in release 9.0.4.3:

| Bug Number | Issue | Resolution |
|------------|---|--|
| 7121688 | On AIX 5.3, the SSH_USERUID_SIZE_FAIL or SSH_USER_FAIL exception was thrown if you tried to update the User Login attribute through a provisioning operation. | This issue has been resolved. You can now update the User Login attribute through a provisioning operation. Note: The Update User Login provisioning operation is not supported by default on AIX 4.x and 5.1. However, if you upgrade these versions of AIX to support the useradd, usermod, and userdel commands, then you can perform the Update User Login provisioning operation. |
| 7143460 | During a reconciliation run on AIX, the ArrayIndexOutOfBounds exception was thrown if the number of deleted records fetched from the target system was more than the number of newly created or updated records fetched from the target system. | This issue has been resolved. An exception is not thrown if the number of deleted records fetched from the target system is more than the number of newly created or updated records fetched from the target system. |
| 7143486 | If a reconciliation run ended in an exception, then the connection with the target system was not closed. | This issue has been resolved. The connection with the target system is closed even if a reconciliation run ends in an exception. |

Software Updates in Release 9.0.4.2

The following are software updates in release 9.0.4.2:

- In Step 2 of the "Installing and Configuring SUDO" section for Solaris, the usermod command has been added to the list of commands used by the target system.
- In [Section 2.5.4, "Enabling Logging,"](#) the name of the adapter for this connector has been changed from ADAPTERS.TELNETSSH to OIMCP.TELNETSSH.
- In the "Compiling Adapters" section, the SSH updateHomeDir adapter has been added to the list of adapters.
- In the IT resource definition, the following parameters have been removed:
 - Login Prompt
 - Password Prompt
 - Target Locale
 - Supported Character Encoding (en_US) - Target

The following scheduled task attributes have been converted into IT resource parameters:

- Passwd Mirror File/User Mirror File
- Shadow Mirror File
- Target Date Format
- The following table lists issues resolved in release 9.0.4.2:

| Bug Number | Issue | Resolution |
|------------|--|--|
| 6375896 | Target resource reconciliation threw exceptions when users were reconciled from Linux using a SUDO admin user. | Target resource reconciliation issues related to Linux used in the SUDO mode have been resolved. |

| Bug Number | Issue | Resolution |
|---------------------|--|--|
| 6609731 | The Supported Character Encoding and Target Locale IT resource parameters were not used by the connector. | The Supported Character Encoding and Target Locale IT resource parameters have been removed. |
| 6642345 | The connection retry feature of the connector was not working correctly. | Issues related to the connection retry feature have been resolved. |
| 6680047 | If a connection retry attempt was made, then previous sessions were not released and new sessions were established each time. | Connectivity issues related to session leakage have been resolved. |
| 6728741 | An incorrect response was received from the connector if the username value was greater than 8 characters and the Create Home directory check box was checked. | The responses received from the connector have been corrected. |
| 6742869 | A user could not be provisioned if there were spaces in value of the GECOS field. | Spaces are now allowed in the GECOS field. |
| 6766705 and 6801405 | The status of the resource object stayed at Provisioned even when provisioning tasks were rejected. | Issues related to the resource object status and response during provisioning have been resolved. |
| 6786399 | The connector was unable to handle responses from target systems running a non-English locale. | Responses from target systems running a non-English locale are now handled correctly. |
| 6801537 | During reconciliation, temporary files were created in the /etc directory. | During reconciliation, temporary files are now created in the /tmp folder. |
| 6837471 | A user could not be provisioned with spaces in the values of any of the user attributes. | Spaces are now allowed in many of the user attributes. |
| 5180204 | On AIX computers, the connector was not able to reconcile a large number of records. | Issues related to the reconciliation of a large number of users on AIX have been resolved. |
| 5502324 | Date format parsing errors were encountered during reconciliation. | The date format parsing error that was encountered during the user reconciliation has been resolved. |
| 5503100 | The message displayed when the user name had multibyte characters during a Create User provisioning operation was incorrect. | The message displayed when the user name has multibyte characters during a Create User provisioning operation has been modified. |
| 5647992 | On Linux, Solaris, and AIX computers, the Home Directory attribute could not be updated. | The Home Directory attribute is updated correctly on Linux, Solaris, and AIX targets. |
| 5180227 | The IT Resources contained two redundant parameters, Login Prompt and Password Prompt. | The Login Prompt and Password Prompt IT resource parameters have been deleted. |
| 6604117 | The Password and Confirm Password fields on the process form were not encrypted. | The Password and Confirm Password fields have been modified to accept encrypted values. |

| Bug Number | Issue | Resolution |
|------------|--|--|
| 6310073 | During provisioning, if user creation on the target system failed at some stage, then the user was not cleaned up from the target system although the status of the resource was Provisioning. When this happened, another user with the same name could not be provisioned. | During provisioning, if the user is not created properly on the target, then the user is deleted from the target system and the resource object status is set to Provisioning. |

Documentation-Specific Updates

The following sections discuss documentation-specific updates:

- [Documentation-Specific Updates in Release 9.0.4.15](#)
- [Documentation-Specific Updates in Release 9.0.4.12](#)
- [Documentation-Specific Updates in Release 9.0.4.11](#)
- [Documentation-Specific Updates in Release 9.0.4.7](#)
- [Documentation-Specific Updates in Release 9.0.4.6](#)
- [Documentation-Specific Updates in Release 9.0.4.5](#)
- [Documentation-Specific Updates in Releases 9.0.4.1 Through 9.0.4.4](#)

Documentation-Specific Updates in Release 9.0.4.15

The following are documentation-specific updates in release 9.0.4.15:

- In [Chapter 1, "About the Connector,"](#) in [Section 1–1, "Certified Components,"](#) HP-UX 11.31 has been added to the list of target systems.
- In [Chapter 2, "Deploying the Connector,"](#) [Table 2–1, "Files and Directories on the Installation Media"](#) has been modified.
- In [Chapter 2, "Deploying the Connector,"](#) a note on converting the system to trusted system has been added to [Section 2.3.1.3, "Configuration Steps for HP-UX."](#)
- In [Chapter 2, "Deploying the Connector,"](#) [Section 2.3.4.2, "Configuring SSH Public Key Authentication"](#) has been modified.
- In [Chapter 2, "Deploying the Connector,"](#) [Section 2.4.2, "Copying the sshfactory.jar File"](#) has been added.
- In [Chapter 3, "Using the Connector,"](#) the following changes have been made to [Table 3–2, "Attributes of the User Reconciliation Scheduled Tasks"](#):
 - The description of the Server attribute has been changed.
 - A new attribute IsRoRecon has been added.
- In [Chapter 5, "Testing and Troubleshooting,"](#) the following changes have been made: a note on the testing utility has been added.
 - A note on the testing utility has been added.
 - The expiry date format has been added in the table.
- Information specific to Oracle Identity Manager release 11.1.1 has been added to the following sections:

- [Section 4.2, "Adding Custom Attributes for Provisioning."](#)
- [Section 2.3.4.1, "Configuring Public Key Authentication."](#)
- [Section 2.3.4.2, "Configuring SSH Public Key Authentication."](#)

Documentation-Specific Updates in Release 9.0.4.12

Major changes have been made to the structure of the guide. The objective of these changes is to synchronize the guide with the changes made to the connector and to improve the usability of the information provided by the guide.

Documentation-Specific Updates in Release 9.0.4.11

The following are documentation-specific updates in release 9.0.4.11:

- The minimum certified release of Oracle Identity Manager is release 9.1.0.x.
- The minimum certified release of JDK is release 1.4.2.
See [Section 1.1, "Certified Components"](#) for the full list of certified target systems.

Documentation-Specific Updates in Release 9.0.4.7

The following are documentation-specific updates in release 9.0.4.7:

- Changes have been made in the following sections:
 - [Section 2.3.2, "Installing OpenSSH"](#)
 - [Section 2.3.4.2, "Configuring SSH Public Key Authentication"](#)
- [Section 4.4, "Transforming Data Reconciled Into Oracle Identity Manager"](#) has been added.
- The following point has been removed from [Chapter 6, "Known Issues"](#):
During reconciliation, the Group Name field is reconciled as a number and not as the exact name because it is stored directly as the group ID in the target system.
- The following appendixes have been added:
 - [Appendix A, "Privileges Required for Performing Provisioning and Reconciliation"](#)
 - [Appendix B, "Sample Transformation Class"](#)

Documentation-Specific Updates in Release 9.0.4.6

At some places in this guide, corrections have been made to address some documentation issues.

Documentation-Specific Updates in Release 9.0.4.5

The following are documentation-specific updates in release 9.0.4.5:

- In [Chapter 2, "Deploying the Connector,"](#) the `Protocol` parameter has been added in the table that describes the IT resource parameters.
- In [Chapter 6, "Known Issues"](#):
 - Bug numbers have been added for all the known issues.
 - The following guidelines have been moved from [Chapter 6, "Known Issues"](#) to other parts of this guide:

- This connector does not support logins that differ by case only. It also requires all logins to be distinct considering that their values are automatically converted to uppercase by Oracle Identity Manager.

For example, the user logins `jdoe` and `JDOE` would be considered different on a UNIX server. However, from Oracle Identity Manager, the input would always be passed as `JDOE`, because user ID values are stored only in uppercase in Oracle Identity Manager.

- During provisioning, the maximum permitted date value for account expiry is 31/12/2099.
- The following point has been removed from [Chapter 6, "Known Issues"](#):
 - The Update Secondary Group Names and Update User Login functions do not work simultaneously.

Documentation-Specific Updates in Releases 9.0.4.1 Through 9.0.4.4

The following documentation-specific updates have been made in releases 9.0.4.1 through 9.0.4.4:

- Changes have been made in the following sections:
 - Adding Custom Attributes for Reconciliation
 - Adding Custom Attributes for Provisioning
- In [Chapter 6, "Known Issues,"](#) the following items have been added:
 - "The Update User Login function is not supported on most versions of AIX."
 - A reconciliation run stops if the scheduled task code encounters target system user data containing the character or characters that are same as the shell prompt of the target system.

- In [Chapter 6, "Known Issues,"](#) the following item has been removed:

When you configure an IT resource for an SSH user account and then directly provision it to a user, the Create User Task function is rejected. The user account is not created on the target system. The following message is displayed:

```
"SSH_USERCREATION_NOTCONNECTED_FAIL not able to connect  
successfully to the Target System Server".
```

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 integrate Oracle Identity Manager with target systems running AIX, HP-UX, Linux, and Solaris, using the SSH protocol. This connector enables you to use the target system as a managed (target) resource or as an authoritative (trusted) source of identity data for Oracle Identity Manager.

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.

This chapter contains 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, "Lookup Definitions Used During Connector Operations"](#)
- [Section 1.6, "Connector Objects Used During Target Resource Reconciliation and Provisioning"](#)
- [Section 1.7, "Connector Objects Used During Trusted Source Reconciliation"](#)
- [Section 1.8, "Roadmap for Deploying and Using the Connector"](#)

Note: In this guide, the term *Oracle Identity Manager server* refers to the computer on which Oracle Identity Manager is installed.

1.1 Certified Components

[Table 1–1](#) lists the certified components for this connector.

Table 1–1 Certified Components

| Item | Requirement |
|---|--|
| Oracle Identity Manager | <p>You can use one of the following releases of Oracle Identity Manager:</p> <ul style="list-style-type: none"> ■ Oracle Identity Manager release 9.1.0.x 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 11g release 1 (11.1.1) Note: In this guide, Oracle Identity Manager release 11.1.1 has been used to denote Oracle Identity Manager 11g release 1 (11.1.1). |
| Target systems | <p>The target system can be any one of the following operating systems that support SSH 2.0:</p> <ul style="list-style-type: none"> ■ HP-UX 11.11, 11.20, 11.31 ■ IBM AIX 5L Version 5.2, 5.3, 6.1 ■ Oracle Enterprise Linux 5.2 ■ Red Hat Enterprise Linux AS 2.1, 3, 4.x, Red Hat Enterprise Linux ES 3, 4.x ■ Solaris 8, 9, 10 <p>Note: See "Supported Shell Types" for information about the supported shell type for the preceding operating systems.</p> |
| Target system user account | <p>Depending on the target system that you are using, the target system user account can be one of the following:</p> <ul style="list-style-type: none"> ■ For AIX, HP-UX, and Linux environments: root user or sudo user ■ For Solaris: root user, sudo user, RBAC user <p>You provide the credentials of this user account while configuring the IT resource. The procedure is described later in this guide.</p> <p>If you do not use a target system user account of the specified type, then an error message similar to the following would be displayed when Oracle Identity Manager tries to exchange data with the target system:</p> <pre>SSH_USER_NORIGHTS_FAIL</pre> |
| External code | <p>JSCAPE SSH/SSH Libraries (SSH factory)</p> |
| Character encoding supported by the target system | <p>The target system must support the default C (POSIX) locale.</p> <p>Use the following command to check the locale that the target system supports:</p> <pre>locale -a</pre> |
| Other systems | <p>OpenSSH, OpenSSL, operating system patches (HP-UX), and SUDO software (only if the SUDO Admin mode is required)</p> |
| JDK | <p>The JDK version can be one of the following:</p> <ul style="list-style-type: none"> ■ For Oracle Identity Manager release 9.1.0.x, use JDK 1.5 or later in the 1.5 series. ■ For Oracle Identity Manager release 11.1.1, use JDK 1.6 update 18 or later, or JRockit JDK 1.6 update 17 or later. |

Supported Shell Types

The supported shell types for various operating systems are given in the following table.

| Solaris | HP-UX | Linux | AIX |
|---------|-------|-------|------|
| sh | csch | ksh | csch |
| csch | ksh | bash | ksh |
| - | sh | sh | sh |
| - | - | csch | - |

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

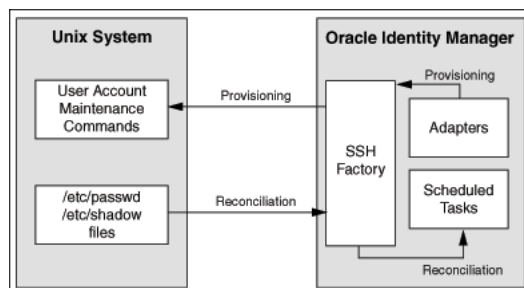
Note: However, the connector does not support the entry of multibyte characters in some of the fields.

See Also: *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for information about supported special characters

1.3 Connector Architecture

This connector enables management of target system accounts through Oracle Identity Manager. [Figure 1-1](#) shows the architecture of the connector.

Figure 1-1 Architecture of the Connector



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

- [Section 1.3.1, "Reconciliation Process"](#)
- [Section 1.3.2, "Provisioning Process"](#)

1.3.1 Reconciliation Process

This connector can be configured to perform either trusted source reconciliation or target resource reconciliation.

When you configure the target system as a target resource, the connector enables you to create and manage target accounts for OIM Users through provisioning. In addition, data related to newly created and modified target system accounts can be reconciled and linked with existing OIM Users and provisioned resources.

When you configure the target system as a trusted source, the connector fetches into Oracle Identity Manager, data about newly created or modified target system accounts. This data is used to create or update OIM Users.

See Also: For conceptual information about target resource reconciliation and trusted source reconciliation, see one of the following guides:

- For Oracle Identity Manager release 9.1.0.x: *Oracle Identity Manager Connector Concepts*
- For Oracle Identity Manager release 11.1.1: *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*

The following is an overview of the steps involved in reconciliation:

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.

1. The scheduled task is run at the time or frequency that you specify. This scheduled task contains details of the mode of reconciliation (trusted source or target resource) that you want to perform.
2. The scheduled task establishes a connection with the target system by using the SSH Factory.
3. The scheduled task performs the following tasks:
 - Reads the values that you set for the task attributes.
 - Reads the differences in the `etc/passwd`, `/etc/shadow` and their corresponding mirror files to determine user records to be fetched into Oracle Identity Manager.
 - Fetches user records into Oracle Identity Manager.

4. If you have configured your target system as a trusted source, then:
 - a. Each user record fetched from the target system is compared with existing OIM Users. The reconciliation rule is applied during the comparison process. See [Section 1.7.2, "Reconciliation Rule for Trusted Source Reconciliation"](#) for information about the reconciliation rule.
 - b. The next step of the process depends on the outcome of the matching operation:
 - If a match is found between the target system record and the OIM User, then the OIM User attributes are updated with changes made to the target system record.
 - If no match is found, then the target system record is used to create an OIM User.
5. If you have configured your target system as a target resource, then:
 - a. Each user record fetched from the target system is compared with existing target system resources assigned to OIM Users. The reconciliation rule is applied during the comparison process. See [Section 1.6.2, "Reconciliation Rule for Target Resource Reconciliation"](#) for information about the reconciliation rule.
 - b. The next step of the process depends on the outcome of the matching operation:
 - If a match is found between the target system record and a resource provisioned to an OIM User, then the database user resource is updated with changes made to the target system record.
 - If no match is found, then the target system user record is compared with existing OIM Users. The next step depends on the outcome of the matching operation:
 - If a match is found, then the target system record is used to provision a resource for the OIM User.
 - If no match is found, then the status of the reconciliation event is set to No Match Found.

1.3.2 Provisioning Process

See Also: For conceptual information about provisioning, see one of the following guides:

- For Oracle Identity Manager release 9.1.0.x: *Oracle Identity Manager Connector Concepts*
- For Oracle Identity Manager release 11.1.1: *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*

Provisioning involves creating and managing user accounts. When you allocate (or provision) a UNIX SSH resource to an OIM User, the operation results in the creation of an account on the target system for that user. Similarly, when you update the resource on Oracle Identity Manager, the same update is made to the account on the target system.

The provisioning process can be started through one of the following events:

- Direct provisioning

The Oracle Identity Manager administrator uses the Administrative and User Console to create a target system account for a user.

- Provisioning triggered by access policy changes
An access policy related to accounts on the target system is modified. When an access policy is modified, it is reevaluated for all users to which it applies.
- Request-based provisioning

Note: Request-based provisioning can be performed only on Oracle Identity Manager release 11.1.1.

In request-based provisioning, an individual creates a request for a target system account. The provisioning process is completed when an OIM User with the required privileges approves the request and provisions the target system account to the requester.

During provisioning operations, adapters carry provisioning data submitted through the process form to the SSH factory, which in turn submits the provisioning data to the target system. The user account maintenance commands accept provisioning data from the adapters, carry out the required operation on the target system, and return the response from the target system to the adapters. The adapters return the response to Oracle Identity Manager.

1.4 Features of the Connector

- [Section 1.4.1, "Support for Both Target Resource and Trusted Source Reconciliation"](#)
- [Section 1.4.2, "Support for Limited Reconciliation"](#)
- [Section 1.4.3, "Support for Batched Reconciliation"](#)
- [Section 1.4.4, "Support for Both Full and Incremental Reconciliation"](#)
- [Section 1.4.5, "Support for Adding Custom Attributes for Reconciliation and Provisioning"](#)
- [Section 1.4.6, "Transformation of Account Data"](#)
- [Section 1.4.7, "Support for Reconciliation of User Status from the Target System"](#)

1.4.1 Support for Both Target Resource and Trusted Source Reconciliation

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

See [Section 3.3, "Configuring Reconciliation"](#) for more information.

1.4.2 Support for Limited Reconciliation

You can set a reconciliation filter as the value of the `UserNameFilter` attribute of the scheduled tasks. This filter specifies the subset of newly added and modified target system records that must be reconciled.

See [Section 3.3.2, "Limited Reconciliation"](#) for more information.

1.4.3 Support for Batched Reconciliation

You can break down a reconciliation run into batches by specifying the number of records that must be included in each batch.

See [Section 3.3.3, "Batched Reconciliation"](#) for more information.

1.4.4 Support for Both Full and Incremental Reconciliation

After you deploy the connector, you can perform full reconciliation to bring all existing user data from the target system to Oracle Identity Manager. After the first full reconciliation run, incremental reconciliation is automatically enabled from the next run of the user reconciliation.

You can perform a full reconciliation run at any time. See [Section 3.3.1, "Full Reconciliation"](#) for more information.

1.4.5 Support for Adding Custom Attributes for Reconciliation and Provisioning

If you want to add custom attributes for reconciliation and provisioning, then perform the procedures described in [Chapter 4, "Extending the Functionality of the Connector."](#)

1.4.6 Transformation of Account Data

You can configure transformation of account data that is brought into Oracle Identity Manager during reconciliation.

See [Section 4.4, "Transforming Data Reconciled Into Oracle Identity Manager"](#) for more information.

1.4.7 Support for Reconciliation of User Status from the Target System

From this release onward, the connector can reconcile user account status information from the target system

1.5 Lookup Definitions Used During Connector Operations

Lookup definitions used during connector operations can be divided into the following categories:

- [Section 1.5.1, "Lookup Definitions Synchronized with the Target System"](#)
- [Section 1.5.2, "Other Lookup Definitions"](#)

1.5.1 Lookup Definitions Synchronized with the Target System

During a provisioning operation, you use a lookup field on the process form to specify a single value from a set of values. For example, you use the Primary Group Name lookup field to select a group name for the user's initial login group. When you deploy the connector, lookup definitions corresponding to the lookup fields on the target system are automatically created in Oracle Identity Manager. Lookup field synchronization involves copying additions or changes made to the target system lookup fields into the lookup definitions in Oracle Identity Manager.

The UD_Lookup_SSH_PrimaryGroupNames lookup definition is populated with group names fetched from the target system by the scheduled task for lookup field synchronization.

See Also: [Section 3.2, "Scheduled Task for Lookup Field Synchronization"](#) for information about this scheduled task

1.5.2 Other Lookup Definitions

[Table 1–2](#) describes the other lookup definitions that are created in Oracle Identity Manager when you deploy the connector. These lookup definitions are either prepopulated with values or values must be manually entered in them after the connector is deployed.

Table 1–2 Other Lookup Definitions

| Lookup Definition | Description of Values | Method to Specify Values for the Lookup Definition |
|---|---|---|
| Lookup.Unix.Configuration | This lookup definition maps statuses of users accounts in the target system with the corresponding statuses to be displayed in the Status field of the OIM User form. | This lookup definition is preconfigured. It is used for performing user account status reconciliation. You cannot add or modify entries in this lookup definition. |
| Lookup.Reconciliation.TransformationMap | This lookup definition is used to configure transformation of attribute values that are fetched from the target system during user reconciliation. | You manually create entries in this lookup definition. See Section 4.4, "Transforming Data Reconciled Into Oracle Identity Manager" for more information. |

1.6 Connector Objects Used During Target Resource Reconciliation and Provisioning

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

See Also: The "Reconciliation" section in *Oracle Identity Manager Connector Concepts* for conceptual information about reconciliation

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

- [Section 1.6.1, "User Attributes for Target Resource Reconciliation and Provisioning"](#)
- [Section 1.6.2, "Reconciliation Rule for Target Resource Reconciliation"](#)
- [Section 1.6.3, "Reconciliation Action Rules for Target Resource Reconciliation"](#)
- [Section 1.6.4, "Provisioning Functions"](#)

1.6.1 User Attributes for Target Resource Reconciliation and Provisioning

[Table 1–3](#) provides information about user attribute mappings for target resource reconciliation and provisioning.

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

| Process Form Field | Target System Field | Description |
|-----------------------|----------------------|--|
| User Login | User Login | New login name, specified as a string of printable characters |
| Password | passwd | Password |
| Secondary Group Names | supplementary groups | List of supplementary groups, of which the user is also a member |
| User UID | uid | Numeric value of the user ID This value must be unique and nonnegative. The default is to use the smallest ID value greater than 99 and greater than the number used for any other user. Values between 0 and 99 are typically reserved for system accounts. |
| Primary Group Name | initial group | The group name or number of the user's initial login group. |
| Default Shell | shell | User's login shell |
| GECOS | comment | Generally, a short description of the login It is used as the field for the user's full name. This information is stored in the user's /etc/passwd file entry. Note: The entry of multibyte characters is supported for this attribute. |
| Home Directory | home directory | Login directory of the new user The default directory name is obtained by appending the login name to the default home directory. For example, if the login name is jdoe, then the default home directory is /home/jdoe. Note: The entry of multibyte characters is supported for this attribute. |
| Account Expiry Date | expire date | Date on which the user account is disabled Note: For a trusted configuration, such as the HP-UX (trusted) mode, the Password Change Time and Account Expiry Date fields are not reconciled. |
| Password Change Time | maxdays | Maximum number of days for which a password is valid |
| Skeleton Directory | skeleton directory | Specifies the skeleton directory that contains information that can be copied to the new login's home directory An existing directory must be specified. The system provides a skeleton directory, /etc/skel, that can be used for this purpose. Note: The entry of multibyte characters is supported for this attribute. |
| Inactive Days | inactive days | Number of days after a password has expired before the account is disabled |

1.6.2 Reconciliation Rule for Target Resource Reconciliation

See Also: For generic information about reconciliation matching and action rules, see one of the following guides:

- For Oracle Identity Manager release 9.1.0.x: *Oracle Identity Manager Connector Concepts*
- For Oracle Identity Manager release 11.1.1: *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*

The following is the process-matching rule:

Rule name: SSH User Rule

Rule element: User Login equals Users.UserLogin

In this rule:

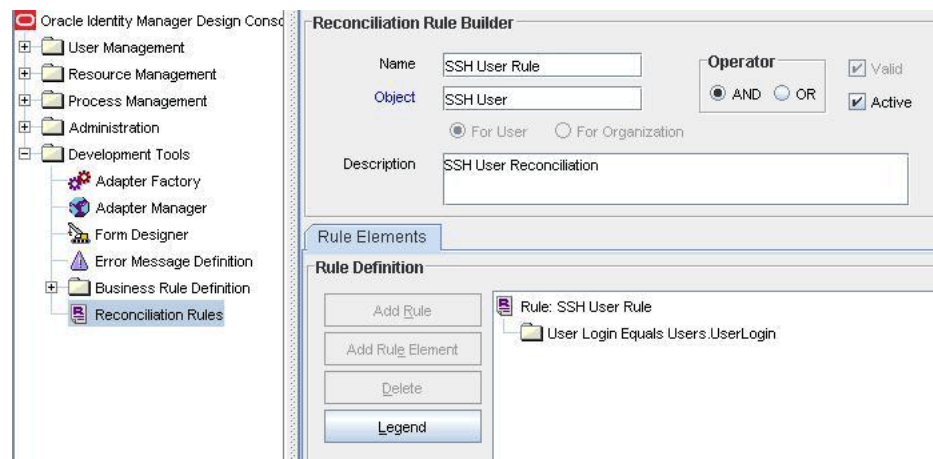
- User Login is the User ID attribute on the OIM User form.
- Users.UserLogin is the User Login attribute of the target system.

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

Note: Perform the following procedure only after the connector is deployed.

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Development Tools**.
3. Search for **SSH User Rule**. [Figure 1–2](#) shows the reconciliation rule for target resource reconciliation.

Figure 1–2 Reconciliation Rule for Target Resource Reconciliation



1.6.3 Reconciliation Action Rules for Target Resource Reconciliation

[Table 1–4](#) lists the action rules for target resource reconciliation.

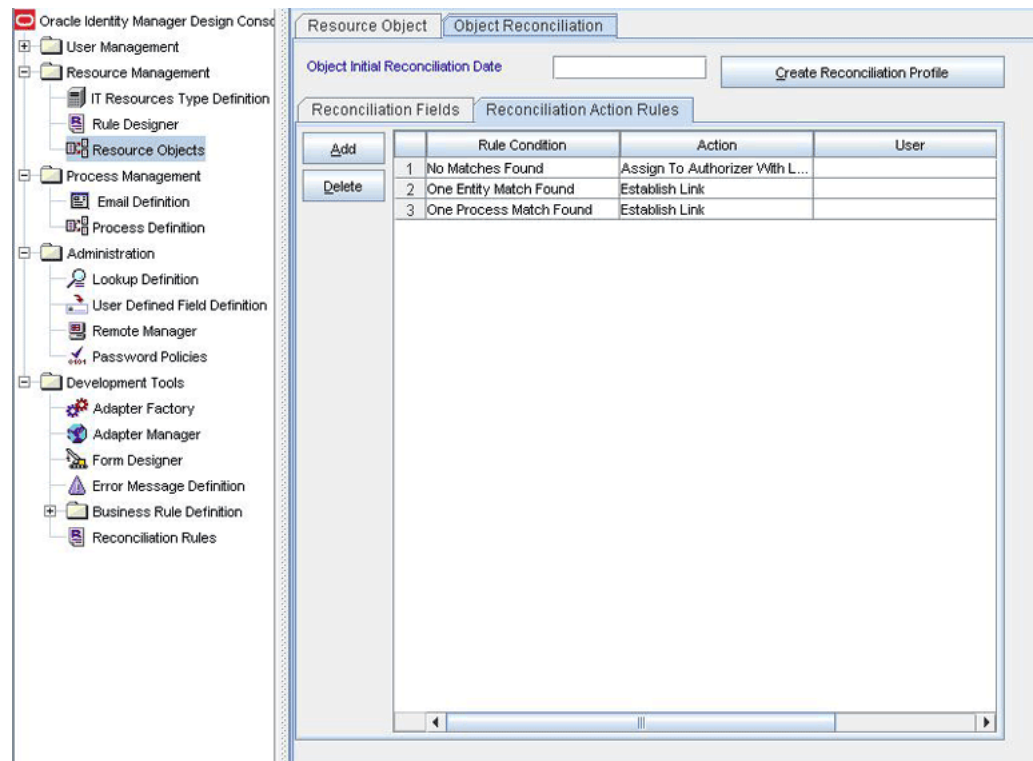
Table 1–4 Action Rules for Target Resource Reconciliation

| Rule Condition | Action |
|-------------------------|--------------------------------------|
| No Matches Found | Assign to Authorizer 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 Developer'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. Log in to the Oracle Identity Manager Design Console.
2. Expand **Resource Management**.
3. Double-click **Resource Objects**.
4. Search for and open the **SSH User** resource object.
5. 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. [Figure 1–3](#) shows the reconciliation action rule for target resource reconciliation.

Figure 1–3 Reconciliation Action Rules for Target Resource Reconciliation

1.6.4 Provisioning Functions

Table 1–5 lists the provisioning functions that are supported by the connector. The Adapter column gives the name of the adapter that is used when the function is performed.

Table 1–5 Provisioning Functions

| Function | Adapter |
|---|-----------------------|
| Create User | adpSSHCreateUser |
| Delete User | adpSSHDeleteUser |
| Update User UID | adpSSHupdateIntField |
| Update User Group | adpSSHupdateStrField |
| Update User Password Change Time | adpSSHupdateIntField |
| Update Shell | adpSSHupdateStrField |
| Update Home Directory | adpSSHupdateHomeDir |
| Update Account Expiry Date | adpSSHupdateDateField |
| Update User GECOS | adpSSHupdateStrField |
| Set Password | adpSSHsetpassword |
| Update Secondary Group Names | adpSSHupdateStrField |
| Update Inactive Days | adpSSHupdateIntField |
| Note: This function is not supported on AIX 5.2. | |
| Update User Login | adpSSHupdateStrField |
| Disable User | adpSSHdisableUser |
| Enable User | adpSSHenableUser |

1.7 Connector Objects Used During Trusted Source Reconciliation

The following sections provide information about connector objects used during trusted source reconciliation:

- [Section 1.7.1, "User Attributes for Trusted Source Reconciliation"](#)
- [Section 1.7.2, "Reconciliation Rule for Trusted Source Reconciliation"](#)
- [Section 1.7.3, "Reconciliation Action Rules for Trusted Source Reconciliation"](#)

1.7.1 User Attributes for Trusted Source Reconciliation

Table 1–6 lists user attributes for trusted source reconciliation.

Table 1–6 User Attributes for Trusted Source Reconciliation

| OIM User Form Field | Target System Attribute | Description |
|---------------------|-------------------------|-------------|
| User ID | UserLogin | Common name |
| First Name | UserLogin | Given name |
| Last Name | UserLogin | Last name |

Table 1–6 (Cont.) User Attributes for Trusted Source Reconciliation

| OIM User Form Field | Target System Attribute | Description |
|---------------------|-------------------------|---------------------------------------|
| Employee Type | NA | Default value: Consultant |
| User Type | NA | Default value: End-User Administrator |
| Organization | NA | Default value: Xellerate Users |

1.7.2 Reconciliation Rule for Trusted Source Reconciliation

See Also: For generic information about reconciliation matching and action rules, see one of the following guides:

- For Oracle Identity Manager release 9.1.0.x: *Oracle Identity Manager Connector Concepts*
- For Oracle Identity Manager release 11.1.1: *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*

The following is the process matching rule:

Rule name: SSH Xellerate User Rule

Rule element: User Login equals Users.UserLogin

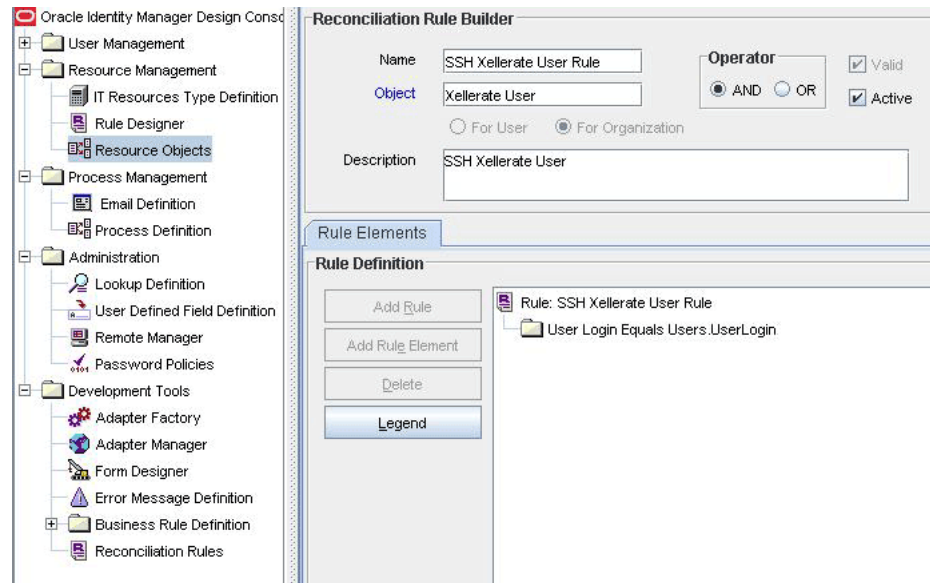
In this rule element:

- User Login is the User ID attribute on the OIM User form.
- Users.UserLogin is the User Login attribute of the target system.

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

Note: Perform the following procedure only after the connector is deployed.

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Development Tools**.
3. Double-click **Reconciliation Rules**.
4. Search for **SSH Xellerate User Rule**. [Figure 1–5](#) shows the reconciliation rule for trusted source reconciliation.

Figure 1–4 Reconciliation Rule for Trusted Source Reconciliation

1.7.3 Reconciliation Action Rules for Trusted Source Reconciliation

Table 1–7 lists the action rules for target resource reconciliation.

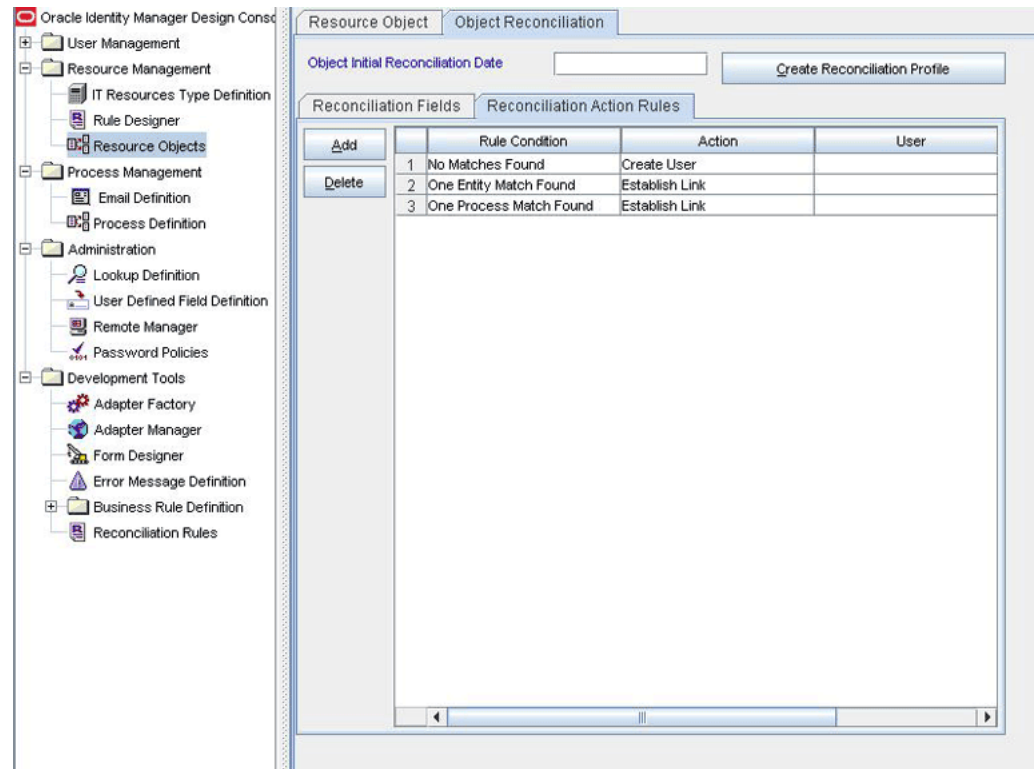
Table 1–7 Action Rules for Target Source Reconciliation

| Rule Condition | Action |
|-------------------------|----------------|
| No Matches Found | Create User |
| 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 Developer'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. Log in to the Oracle Identity Manager Design Console.
2. Expand **Resource Management**.
3. Double-click **Resource Objects**.
4. Search for and open the **Xellerate User** resource object.
5. 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. Figure 1–5 shows the reconciliation action rules for trusted source reconciliation.

Figure 1–5 Reconciliation Action Rules for Trusted Source Reconciliation

1.8 Roadmap for Deploying and Using the Connector

The following is the organization of information in the rest of this guide:

- [Chapter 2, "Deploying the Connector"](#) describes procedures that you must perform on Oracle Identity Manager and the target system during each stage of connector deployment.
- [Chapter 3, "Using the Connector"](#) describes guidelines on using the connector and the procedure to configure reconciliation runs and perform provisioning operations.
- [Chapter 4, "Extending the Functionality of the Connector"](#) describes procedures that you can perform if you want to extend the functionality of the connector.
- [Chapter 5, "Testing and Troubleshooting"](#) describes the procedure to use the connector testing utility for testing the connector.
- [Chapter 6, "Known Issues"](#) lists known issues associated with this release of the connector.
- [Appendix A, "Privileges Required for Performing Provisioning and Reconciliation"](#) provides information about privileges required for successful provisioning operations and reconciliation runs.
- [Appendix B, "Sample Transformation Class"](#) provides the code for a sample Java class. You can use this sample class to create a class for transforming reconciled data according to your requirements.

Deploying the Connector

This chapter is divided into the following sections:

- [Section 2.1, "Files and Directories on the Installation Media"](#)
- [Section 2.2, "Determining the Release Number of the Connector"](#)
- [Section 2.3, "Configuring the Target System"](#)
- [Section 2.4, "Installing the Connector on Oracle Identity Manager Release 9.1.0.x or Release 11.1.1"](#)
- [Section 2.5, "Configuring the Oracle Identity Manager Server"](#)

2.1 Files and Directories on the Installation Media

The files and directories on the installation media are listed and described in [Table 2-1](#).

Table 2-1 Files and Directories on the Installation Media

| File in the Installation Media Directory | Description |
|--|---|
| configuration/UNIX SSH-CI.xml | This XML file contains configuration information that is used during connector installation. |
| ext/sshfactory.jar | This file contains the JSCTAPE libraries. These libraries are used to open an SSH session with the target server. During connector deployment, this file is copied to the following location: <ul style="list-style-type: none"> ■ For Oracle Identity Manager release 9.1.0.x: <i>OIM_HOME/xellerate/ThirdParty</i> ■ For Oracle Identity Manager release 11.1.1: Oracle Identity Manager database |
| lib/xliSSH.jar | This JAR file contains the Java classes that are required for provisioning and reconciliation in SSH. During connector deployment, this file is copied to the following location: <ul style="list-style-type: none"> ■ For Oracle Identity Manager release 9.1.0.x: <i>OIM_HOME/xellerate/JavaTasks</i> <i>OIM_HOME/xellerate/ScheduleTask</i> ■ For Oracle Identity Manager release 11.1.1: Oracle Identity Manager database |

Table 2–1 (Cont.) Files and Directories on the Installation Media

| File in the Installation Media Directory | Description |
|--|---|
| Files in the resources directory | <p>Each of these resource bundles contains language-specific information that is used by the connector. During connector installation, these resource bundles are copied to the following location:</p> <ul style="list-style-type: none"> ■ For Oracle Identity Manager release 9.1.0.x: <i>OIM_HOME/xellerate/connectorResources</i> ■ For Oracle Identity Manager release 11.1.1: Oracle Identity Manager database <p>Note: A resource bundle is a file containing localized versions of the text strings that are displayed on the Administrative and User Console. These text strings include GUI element labels and messages.</p> |
| scripts/privateKeyGen.sh | This file is used to generate the private key in SSH. |
| scripts/sudoers | This file contains the SUDO user specifications and configurations. |
| test/config/config.properties | This file is used to specify the parameters and settings required to connect to the target system by using the testing utility. |
| test/config/log.properties | This file is used to specify the log level and the directory in which the log file is to be created when you run the testing utility. |
| config/userAttribute_NonAIX_prov.properties | This file contains the parameters required for dynamic provisioning on non-AIX platforms. |
| config/userAttribute_AIX_prov.properties | This file contains the parameters required for dynamic provisioning on AIX platform. |
| config/userAttribute_NonAIX_recon.properties | This file contains the parameters required for dynamic reconciliation on non-AIX platforms. |
| config/userAttribute_AIX_recon.properties | This file contains the parameters required for dynamic reconciliation on AIX platform. |
| test/scripts/SSH.bat test/scripts/SSH.sh | This file contains the script required to run the client for running test calls from the Oracle Identity Manager server. |
| xml/SSHNonTrustedUser.xml | <p>This XML file contains definitions for the following SSH User components of the connector:</p> <ul style="list-style-type: none"> ■ IT resource type ■ IT resource ■ Resource object ■ Process definition ■ Process tasks ■ Adapters ■ Process form ■ Reconciliation scheduled task |
| xml/XellSSHUser.xml | This XML file contains the configuration for the Xellerate User (OIM User) and the definition of the trusted source reconciliation schedule task. You must import this file only if you plan to use the connector for trusted source reconciliation. |
| xml/SSHConnectorRequestDatasets.xml | This file contains the request datasets for the connector. You import this file by using the Deployment Manager. |

2.2 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 following JAR file:
OIM_HOME/xellerate/JavaTasks/xliSSH.jar
2. Open the manifest.mf file in a text editor. The manifest.mf file is one of the files bundled inside the xliSSH.jar file.

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

2.3 Configuring the Target System

Configuring the target system involves the steps described in the following sections:

- [Section 2.3.1, "Platform-Specific Configuration Steps"](#)
- [Section 2.3.2, "Installing OpenSSH"](#)
- [Section 2.3.3, "Creating a Target System User Account for Connector Operations"](#)
- [Section 2.3.4, "Public Key Authentication \(SSH Key Generation\)"](#)

2.3.1 Platform-Specific Configuration Steps

This section provides instructions to configure the target system on the following platforms:

- [Section 2.3.1.1, "Configuration Steps for Solaris and Linux"](#)
- [Section 2.3.1.2, "Configuration Steps for AIX"](#)
- [Section 2.3.1.3, "Configuration Steps for HP-UX"](#)

2.3.1.1 Configuration Steps for Solaris and Linux

Perform the following steps for Solaris and Linux environments:

1. Ensure that the `/etc/passwd` and `/etc/shadow` files are available on the UNIX server.
2. Create a passwd mirror file on the target server by using a command similar to the following:

```
cp /etc/passwd /etc/passwd1
```

You can specify any destination directory and file name when you run the command. While configuring the IT resource, you specify the name and path of this file as the value of the `Passwd Mirror File/User Mirror File` parameter of the IT resource for Solaris and Linux.

Note: The administrator account whose credentials you provide as part of the IT resource definition must have read and write permissions on this file.

3. Create a shadow mirror file on the target server by using a command similar to the following:

```
cp /etc/shadow /etc/shadow1
```

You can specify any destination directory and file name when you run the command. While configuring the IT resource, you specify the name and path of this file as the value of the Shadow Mirror File parameter of the IT resource.

Note: The administrator account whose credentials you provide as part of the IT resource definition must have read and write permissions on this file.

2.3.1.2 Configuration Steps for AIX

Perform the following steps for AIX environments:

1. Ensure that the `/etc/passwd` and `/etc/security/user` files are available on the server.
2. Create a user mirror file on the server by using a command similar to the following:

```
> /etc/mainUserFile1
```

You can specify any destination directory and file name when you run the command. While configuring the IT resource, you specify the name and path of this file as the value of the `Passwd Mirror File/User Mirror File (AIX)` parameter of the IT resource for AIX.

Note:

- The administrator account whose credentials you provide as part of the IT resource definition must have read and write permissions on this file.
 - The Update User Login provisioning operation is not supported by default on AIX 4.x and 5.1. However, if you upgrade these versions of AIX to support the `useradd`, `usermod`, and `userdel` commands, then you can perform the Update User Login provisioning operation.
-
-

2.3.1.3 Configuration Steps for HP-UX

Perform the following steps for HP-UX environments:

1. If you want to switch to HP-UX Trusted mode, then:

Note: If you are converting the target system to the trusted system, then please make sure that no shadow file exists on the target after it is converted to trusted system. You can use `pwunconv` command to get rid of the shadow file, if it exists.

- a. Log in as root and then run the following command:

```
/usr/bin/sam
```

```
/usr/sbin/sam
```

- b. Select **Auditing and Security** and then select **System Security Policies**. A message is displayed asking if you want to switch to the trusted mode.
- c. Click **Yes**. The following message is displayed:

```
System changed successfully to trusted system
```

2. Ensure that the `/etc/passwd` and `/etc/shadow` directories are available on the target server.
3. Create a passwd mirror file on the target server by using a command similar to the following:

```
cp /etc/passwd /etc/passwd1
```

You can specify any destination directory and file name when you run the command. While configuring the IT resource, you specify the name and path of this file as the value of the `Passwd Mirror File/User Mirror File` parameter of the IT resource for HP-UX.

Note: The administrator account whose credentials you provide as part of the IT resource definition must have read and write permissions on this file.

4. Create a shadow mirror file on the target server by using a command similar to the following:

```
cp /etc/shadow /etc/shadow1
```

You can specify any destination directory and file name when you run the command. While configuring the IT resource, you specify the name and path of this file as the value of the `Shadow Mirror File` parameter of the IT resource.

Note: The administrator account whose credentials you provide as part of the IT resource definition must have read and write permissions on this file.

2.3.2 Installing OpenSSH

Follow these steps to install OpenSSH on Solaris 9 or HP-UX.

For Solaris 8 and 9

1. If SSH is not installed on the Solaris server, then install the appropriate OpenSSH.

2. Create a group with the name `sshd` and group ID 27. Add a user with the name `sshadmin` to this group.
3. To enable root logins, change the value of `PermitRootLogin` in the `/etc/ssh/sshd_config` file as follows:

```
PermitRootLogin yes
```

Note: Implement this change only if it does not violate local security policies. If Public Key Authentication is enabled, then you can change the value of `PermitRootLogin` to `without-password`.

Instead of using the root account, if you can use a user account with sudo privileges, then you do not need to perform this step.

For Solaris 10

By default, OpenSSH is installed on Solaris 10. If it is not installed, then install the OpenSSH server from the operating system installation CD. To enable SSH on Solaris 10, make the following changes in the `/etc/ssh/sshd_config` file:

1. Remove the comment character from the `Host *` line.
2. To enable root logins, change the value of `PermitRootLogin` in the `/etc/ssh/sshd_config` file as follows:

```
PermitRootLogin yes
```

Note: Implement this change only if it does not violate local security policies. If Public Key Authentication is enabled, then you can change the value of `PermitRootLogin` to `without-password`.

Instead of using the root account, if you can use a user account with sudo privileges, then you do not need to perform this step.

For HP-UX

If SSH is not installed on the UNIX server, then install the appropriate OpenSSH from the installation media.

For Linux

By default, OpenSSH is installed on Red Hat Advanced Server 2.1 and Red Hat Enterprise Linux 3. If it is not installed, then install the OpenSSH server from the operating system installation CD.

For AIX

If SSH is not installed on the AIX 5.2 server, then from the installation media:

1. Install OpenSSL.
2. Install PRNG.
3. Install OpenSSH.
4. To enable root logins, change the value of `PermitRootLogin` in the `/etc/ssh/sshd_config` file as follows:

```
PermitRootLogin yes
```

Note: Implement this change only if it does not violate local security policies. If Public Key Authentication is enabled, then you can change the value of `PermitRootLogin` to `without-password`.

Instead of using the root account, if you can use a user account with sudo privileges, then you do not need to perform this step.

2.3.3 Creating a Target System User Account for Connector Operations

Oracle Identity Manager uses a target system account for performing reconciliation and provisioning operations. On all supported target systems, this account must be either the root user or sudo user. However, on Solaris, you can either create a sudo user or apply the role-based access control (RBAC) feature to create an account and assign to it the minimum privileges required for connector operations.

To create a target system user account with the minimum permissions required to perform connector operations, perform the procedure described in one of the following sections:

- [Section 2.3.3.1, "Creating a Target System User Account for Connector Operations on Solaris"](#)
- [Section 2.3.3.2, "Creating a Target System User Account for Connector Operations on HP-UX"](#)
- [Section 2.3.3.3, "Creating a Target System User Account for Connector Operations on AIX"](#)
- [Section 2.3.3.4, "Creating a Target System User Account for Connector Operations on Red Hat Advanced Server 2.1"](#)
- [Section 2.3.3.5, "Creating a Target System User Account for Connector Operations on Red Hat Enterprise Linux 3.x or Red Hat Linux 4.x"](#)

2.3.3.1 Creating a Target System User Account for Connector Operations on Solaris

As mentioned earlier, on Solaris, you can either create a sudo user or apply the RBAC feature to create an account and assign to it the minimum privileges required for connector operations. Depending on your requirement, perform the instructions described in one of the following sections:

- [Section 2.3.3.1.1, "Creating a Sudo User for Connector Operations"](#)
- [Section 2.3.3.1.2, "Creating an RBAC User Account for Connector Operations"](#)

2.3.3.1.1 Creating a Sudo User for Connector Operations

If you want to create a sudo user and use the SSH connector in the SUDO Admin mode, then perform the following steps:

1. If SUDO is not installed on the Solaris server, then install it from the installation media.
2. Edit the `sudoers` file on the Solaris server to customize it according to your requirements. This file is located in the following directory:

```
/usr/local/etc/
```

For example, if a group named `mqm` exists on the Solaris server, and you require all members of the group to act as SUDO users with all possible privileges, then the sudoers file must contain a line similar to the following:

```
%mqm ALL= (ALL) ALL
```

This is only a sample configuration. If you require some other group members or individual users to be SUDO users with specific privileges, then you must edit this file as you did for the sample value `mqm`.

This connector uses the following commands:

- `useradd`
- `usermod`
- `userdel`
- `passwd`
- `sh`
- `cat`
- `diff`
- `sort`
- `rm`
- `grep`
- `echo`

Therefore, the SUDO user must have privileges to run these commands.

Caution: Do not use the `NOPASSWD: ALL` option for any SUDO user or group. The connector will not work correctly if the `NOPASSWD: ALL` is set.

For information about customizing the sudoers file, refer to:

<http://www.courtesan.com/sudo/man/sudoers.html>

3. Edit the same `sudoers` file so that every time a command is run in SUDO Admin mode, the SUDO user is prompted for the password. Add the following line under the `# Defaults` specification header:

```
Defaults timestamp_timeout=0
```

This is a prerequisite for this connector to work successfully.

4. Log in to the Solaris computer as `root`, and enter the following commands:

```
chmod 440 /usr/local/etc/sudoers
chgrp root /usr/local/etc/sudoers
chmod 4111 /usr/local/bin/sudo
```

5. Create a SUDO user. The SUDO user must be created according to the constraints specified in the `sudoers` file.

The SUDO user must always be created with its home directory by using a command similar to the following:

```
useradd -g group_name -d /export/home/directory_name -m user_name
```

6. In the sudo user's .profile file, which is created in the sudo user's home directory, add the following lines to set the value of the PATH environment variable:

```
PATH=/usr/sbin:/usr/local/bin:/usr/local/etc:/var/adm/sw/products:$PATH
export PATH
```

7. In the sudo user's .bashrc, .cshrc, or .kshrc file, which is created in the sudo user's home directory, add the following line to change the prompt end character from \$ (dollar sign) to # (pound sign):

```
PS1="[\\u@\\h:\\w]#"
```

The encrypted passwords in the shadow file contain # (dollar sign), which matches the default prompt end character. You must change the prompt end character to ensure that changes made to the shadow file are reconciled correctly.

2.3.3.1.2 Creating an RBAC User Account for Connector Operations

Note: You use the IT resource to specify whether or not you want to use an RBAC user. Parameters of the IT resource are described later in this chapter.

To create an RBAC user account:

1. Run the following command to create a role for the user.

```
roleadd -d /export/home/ROLE_NAME -m ROLE_NAME
```

In this command, replace *ROLE_NAME* with the name that you want to assign to the role, for example, OIMRole.

2. Run the following command to assign a password to the role:

```
passwd ROLE_NAME
```

At the prompt, enter a password for the role.

See Also: [Appendix A, "Privileges Required for Performing Provisioning and Reconciliation"](#) for information about the privileges required to run the commands that are used for provisioning and reconciliation

3. Create a profile for the user as follows:
 - a. Open the /etc/security/prof_attr file in a text editor and insert the following line in the file:

```
PROFILE_NAME::Oracle Identity Manager Profile:
```

In this line, replace *PROFILE_NAME* with the name that you want to assign to the profile, for example, OIMProf.

- b. Save and close the file.
4. Add execution attribute entries in the /etc/security/exec_attr file. Each entry defines a task to be run and the uid that the role will assume when running the task.

Open the `/etc/security/exec_attr` file in a text editor, and insert the following lines:

Note: There are seven fields in this file, and the colon (:) is used as the delimiting character.

On Solaris 10, the value `suser` can be replaced with `solaris`.

Some of the entries contain `eid`. These instances of `eid` can be replaced with `uid`.

```
PROFILE_NAME:suser:cmd::/usr/sbin/usermod:uid=0
PROFILE_NAME:suser:cmd::/usr/sbin/useradd:uid=0
PROFILE_NAME:suser:cmd::/usr/sbin/userdel:uid=0
PROFILE_NAME:suser:cmd::/usr/bin/passwd:uid=0
PROFILE_NAME:suser:cmd::/usr/bin/cat:uid=0
PROFILE_NAME:suser:cmd::/usr/bin/diff:uid=0
PROFILE_NAME:suser:cmd::/usr/bin/sort:uid=0
PROFILE_NAME:suser:cmd::/usr/bin/rm:uid=0
PROFILE_NAME:suser:cmd::/usr/bin/grep:uid=0
PROFILE_NAME:suser:cmd::/usr/bin/egrep:uid=0
PROFILE_NAME:suser:cmd::/bin/echo:uid=0
PROFILE_NAME:suser:cmd::/bin/sed:uid=0
```

5. Run the following command to associate the profile with the role:

```
rolemod -P PROFILE_NAME ROLE_NAME
```

6. Run the following command to create the user:

```
useradd -d /export/home/USER_NAME -m USER_NAME
```

7. Run the following command to assign a password to the user:

```
passwd USER_NAME
```

8. Run the following command to grant the role to the user:

```
usermod -R ROLE_NAME USER_NAME
```

9. To verify the changes that you have made, open the `/etc/user_attr` file in a text editor and verify that the following entries are present in the file:

```
ROLE_NAME:::type=role;profiles=PROFILE_NAME
USER_NAME:::type=normal;roles=ROLE_NAME
```

2.3.3.2 Creating a Target System User Account for Connector Operations on HP-UX

If you want to create a sudo user and use the SSH connector in the SUDO Admin mode, then perform the following steps:

1. If SUDO is not installed on the HP-UX server, then install the appropriate SUDO from the installation media.
2. Edit the `sudoers` file to customize it according to your requirements. This file is located in the following directory:

```
/usr/local/etc/
```


For example, if you have a group named `mcm` on the HP-UX server and you want all members of the group to act as SUDO users with all possible privileges, then the `sudoers` file must contain the following line:

```
%mcm ALL= (ALL) ALL
```

This is only a sample configuration. If you want to make SUDO users with specific privileges out of other group members or individual users, then edit this file as you did for the sample value `mcm`.

This connector uses the following commands:

- `useradd`
- `usermod`
- `userdel`
- `passwd`
- `sh`
- `cat`
- `diff`
- `sort`
- `rm`
- `grep`
- `echo`
- `modprpw (/usr/sbin/modprpw)`

Therefore, the SUDO user must have the privileges required to run these commands.

Caution: Do not use the `NOPASSWD: ALL` option for any SUDO user or group. The connector will not work correctly if the `NOPASSWD: ALL` is set.

For information about customizing the `sudoers` file, refer to

<http://www.courtesan.com/sudo/man/sudoers.html>

3. Edit the same `sudoers` file so that every time a command is run in SUDO Admin mode, the SUDO user is prompted for a password. Add the following line under the `# Defaults` specification header:

```
Defaults timestamp_timeout=0
```

This is an essential prerequisite for the connector to work successfully.

4. Copy the `sudoers` file that you edited into the `/etc` directory of the target system. After copying the file, enter the following command:

```
dos2ux /etc/sudoers > /etc/sudoers1
```

Then, change the name of the file from `sudoers1` to `sudoers`.

5. Log in as root, and enter the following commands on the HP-UX computer:

```
chmod 440 /etc/sudoers
chgrp root /etc/sudoers
```

```
chmod 4111 /usr/local/bin/sudo
```

6. Create a SUDO user. The SUDO user should be created according to the constraints specified in the sudoers file.

The SUDO user should always be created with its home directory by using a command similar to the following:

```
useradd -g group_name -d /home/directory_name -m user_name
```

In addition, in the `.profile` file, which is created in the home directory, add the following lines to set the appropriate PATH:

```
PATH=/usr/sbin:/usr/local/bin:/usr/local/etc:/var/adm/sw/products:$PATH
export PATH
```

7. In the sudo user's `.bashrc`, `.cshrc`, or `.kshrc` file, which is created in the sudo user's home directory, add the following line to change the prompt end character from \$ (dollar sign) to # (pound sign):

```
PS1="[\\u@\\h:\\w]#"
```

The encrypted passwords in the shadow file contain # (dollar sign), which matches the default prompt end character. You must change the prompt end character to ensure that changes made to the shadow file are reconciled correctly.

2.3.3.3 Creating a Target System User Account for Connector Operations on AIX

If you want to create a sudo user and use the SSH connector in the SUDO Admin mode, then perform the following steps:

1. If SUDO is not installed on AIX 5.2, then install the appropriate SUDO AIX 5.2 version from the installation media.
2. Edit the sudoers file, which is in the `/etc` directory on the AIX server, to customize the file according to your requirements.

For example, if you have a group named `mqm` in the AIX server and require all members of the group to act as SUDO users with all possible privileges, then the sudoers file must contain the following line:

```
%mqm ALL= (ALL) ALL
```

This is only a sample configuration. If you need other group members or individual users to be SUDO users with specific privileges, then edit this file as was done for the sample value `mqm`.

This connector uses the following commands:

- `mkuser`
- `chuser`
- `rmuser`
- `lsuser`
- `sh`
- `cat`
- `diff`
- `sort`
- `rm`

- `grep`
- `echo`
- `sed`
- `usermod`

Therefore, the SUDO user must have the privileges required to run these commands.

Caution: Do not use the `NOPASSWD: ALL` option for any SUDO user or group. The connector will not work correctly if the `NOPASSWD: ALL` is set.

For information about customizing the `sudoers` file, refer to:

<http://www.courtesan.com/sudo/man/sudoers.html>

3. Edit the same `sudoers` file to configure the system, so that every time a command is run through SUDO Admin mode, the SUDO user is prompted for a password. Add the following line under the `# Defaults specification` header:

```
Defaults timestamp_timeout=0
```

This is a prerequisite for this connector to work successfully.

4. Create a SUDO user. The SUDO user should be created according to the constraints specified in the `sudoers` file.
5. In the sudo user's `.bashrc`, `.cshrc`, or `.kshrc` file, which is created in the sudo user's home directory, add the following line to change the prompt end character from `$` (dollar sign) to `#` (pound sign):

```
PS1="[\\u@\\h:\\w]#"
```

The encrypted passwords in the shadow file contain `#` (dollar sign), which matches the default prompt end character. You must change the prompt end character to ensure that changes made to the shadow file are reconciled correctly.

2.3.3.4 Creating a Target System User Account for Connector Operations on Red Hat Advanced Server 2.1

If you want to create a sudo user and use the SSH connector in the SUDO Admin mode, then perform the following steps:

1. If SUDO is not installed on the Red Hat Advanced Server 2.1 server, then install the appropriate SUDO. from the installation media.
2. Use the `visudo` command to edit and customize the `/etc/sudoers` file according to your requirements.

Note: If you cannot use the `visudo` command to edit the `sudoers` file, then:

1. Enter the following command:

```
chmod 777 /etc/sudoers
```
 2. Make the required changes in the `sudoers` file.
 3. Enter the following command:

```
chmod 440 /etc/sudoers
```
-
-

For example, if you have a group named `mqm` on the Linux server and require all members of the group to act as SUDO users with all possible privileges, then the `sudoers` file must contain the following line:

```
mqm ALL= (ALL) ALL
```

This example is only a sample configuration. If you need other group members or individual users to be SUDO users with specific privileges, then edit this file as was done for the sample value `mqm`.

This connector uses the following commands:

- `useradd`
- `usermod`
- `userdel`
- `passwd`
- `sh`
- `cat`
- `diff`
- `sort`
- `rm`
- `grep`
- `echo`
- `chage`

Therefore, the SUDO user must have the privileges required to run these commands.

Caution: Do not use the `NOPASSWD: ALL` option for any SUDO user or group. The connector will not work correctly if the `NOPASSWD: ALL` is set.

For information about customizing the `sudoers` file, refer to:

<http://www.courtesan.com/sudo/man/sudoers.html>

3. Edit the same `sudoers` file to configure the system, so that every time a command is run in SUDO Admin mode, the SUDO user is prompted for a password. Under the `# Defaults` specification header, add the following line:

```
Defaults timestamp_timeout=0
```

This is a prerequisite for this connector to work successfully.

4. Create a SUDO user as follows:

a. Enter the following command:

```
useradd -g group_name -d /home/directory_name -m user_name
```

In this command:

- *group_name* is the SUDO users group for which there is an entry in the `/etc/sudoers` file.

- *directory_name* is the name of the directory in which you want to create the default directory for the user.

b. In the `.bash_profile` file, which is created in the `/home/directory_name` directory, add the following lines to set the `PATH` environment variable:

```
PATH=/usr/sbin:$PATH
export PATH
```

5. In the sudo user's `.bashrc`, `.cshrc`, or `.kshrc` file, which is created in the sudo user's home directory, add the following line to change the prompt end character from \$ (dollar sign) to # (pound sign):

```
PS1="[\\u@\\h:\\w]#"
```

The encrypted passwords in the shadow file contain # (dollar sign), which matches the default prompt end character. You must change the prompt end character to ensure that changes made to the shadow file are reconciled correctly.

2.3.3.5 Creating a Target System User Account for Connector Operations on Red Hat Enterprise Linux 3.x or Red Hat Linux 4.x

If you want to create a sudo user and use the SSH connector in the SUDO Admin mode, then perform the following steps:

1. If SUDO is not installed on the Red Hat Enterprise Linux 3.x or 4.x server, then install the appropriate SUDO from the installation media.
2. Use the `visudo` command to edit and customize the `/etc/sudoers` file according to your requirements.

Note: If you cannot use the `visudo` command to edit the `sudoers` file, then:

1. Enter the following command:

```
chmod 777 /etc/sudoers
```

2. Make the required changes in the `sudoers` file.

3. Enter the following command:

```
chmod 440 /etc/sudoers
```

For example, if you have a group named `mqm` on the Linux server and want all of the members of the group to act as SUDO users with all possible privileges, then the `sudoers` file must contain the following line:

```
%mqm ALL= (ALL) ALL
```

This is only a sample configuration. If you want some other group members or individual users to be SUDO users with specific privileges, you must edit this file as was done for the sample value `mqm`.

This connector uses the following commands:

- `useradd`
- `usermod`
- `userdel`
- `passwd`
- `sh`
- `cat`
- `diff`
- `sort`
- `rm`
- `grep`
- `echo`
- `chage`

Therefore, the SUDO user must have the privileges required to run these commands.

Caution: Do not use the `NOPASSWD: ALL` option for any SUDO user or group. The connector will not work correctly if the `NOPASSWD: ALL` is set.

For information about customizing the `sudoers` file, refer to

<http://www.courtesan.com/sudo/man/sudoers.html>

3. Edit the same `sudoers` file to configure the system, so that every time a command is run in SUDO Admin mode, the SUDO user is prompted for a password. Under the `# Defaults` specification header, add the following line:

```
Defaults timestamp_timeout=0
```

This is a prerequisite for this connector to work successfully.

4. Create a SUDO user as follows:
 - a. Enter the following command:

```
useradd -g group_name -d /home/directory_name -m user_name
```

In this command:

- *group_name* is the SUDO users group for which there is an entry in the `/etc/sudoers` file.

- *directory_name* is the name of the directory in which you want to create the default directory for the user.

- b. In the `.bash_profile` file, which is created in the `/home/directory_name` directory, add the following lines to set the `PATH` environment variable:

```
PATH=/usr/sbin:$PATH
export PATH
```

5. In the sudo user's `.bashrc`, `.cshrc`, or `.kshrc` file, which is created in the sudo user's home directory, add the following line to change the prompt end character from `$` (dollar sign) to `#` (pound sign):

```
PS1="[\\u@\\h:\\w]#"
```

The encrypted passwords in the shadow file contain `#` (dollar sign), which matches the default prompt end character. You must change the prompt end character to ensure that changes made to the shadow file are reconciled correctly.

2.3.4 Public Key Authentication (SSH Key Generation)

This section discusses the following topics:

- [Section 2.3.4.1, "Configuring Public Key Authentication"](#)
- [Section 2.3.4.2, "Configuring SSH Public Key Authentication"](#)

2.3.4.1 Configuring Public Key Authentication

To configure Public Key Authentication:

Note: If Public Key Authentication is used, then an RBAC user for a Solaris target mode and the SUDO user for the remaining target systems cannot be used.

1. Copy the `scripts/privateKeyGen.sh` file from the installation media directory to any directory on the target system server.
2. Open this script file in a text editor and specify a working directory path other than the default value given in the file.
3. If required, enter the following command:

For Solaris or Linux:

```
dos2unix privateKeyGen.sh privateKeyGen.sh
```

For HP-UX:

```
dos2ux privateKeyGen.sh
```

4. Run the `privateKeyGen.sh` script on the UNIX server. Provide a secure pass phrase when prompted.

When these commands are run, the following files are created in the `$HOME/.ssh` directory:

- `id_rsa`: This is a private key file.
 - `authorized_keys`: This file lists public keys that can be used to log in.
5. When the keys are generated successfully, edit the `sshd_config` file for Public Key Authentication and test login.

6. After successfully testing login, depending on the Oracle Identity Manager release that you are using, copy the `id_rsa` file to one of the following directories:

- For Oracle Identity Manager release 9.1.0.x:
`OIM_HOME/xellerate/XLIntegrations/SSH/config`
- For Oracle Identity Manager release 11.1.1:
`OIM_HOME/server/XLIntegrations/SSH/config`

Note: This release of the connector has been tested and certified only for RSA keys, and not DSA. In addition, this connector has been tested and certified for only single key configuration and not multiple keys.

2.3.4.2 Configuring SSH Public Key Authentication

To configure SSH Public Key Authentication:

For Solaris

1. Set the following parameters in the `/etc/ssh/sshd_config` file:

```
PubKeyAuthorization yes
PasswordAuthentication no
PermitRootLogin yes
```

Note: Change the value of `PermitRootLogin` to `yes` only if it does not violate local security policies. If Public Key Authentication is enabled, then you can change the value of `PermitRootLogin` to `without-password`.

Instead of using the root account, if you can use a user account with sudo privileges, then you do not need to perform this step.

2. To restart the SSH server, enter the following commands:

- `/etc/init.d/sshd stop`
- `/etc/init.d/sshd start`

3. To test login:

```
ssh -i /.ssh/id_rsa -l root server_IP_address
```

This command prompts you for the passkey before setting up the connection.

For HP-UX

1. Uncomment the following lines in the `/etc/ssh/sshd_config` file:

```
PermitRootLogin yes
PubkeyAuthentication yes
AuthorizedKeysFile .ssh/authorized_keys
```

Note: Change the value of `PermitRootLogin` to `yes` only if it does not violate local security policies. If Public Key Authentication is enabled, then you can change the value of `PermitRootLogin` to `without-password`.

Instead of using the root account, if you can use a user account with sudo privileges, then you do not need to perform this step.

2. To restart the SSH Server, enter the following command:

```
/opt/ssh/sbin/sshd
```

3. To test login, enter the following command:

```
ssh -i /.ssh/id_rsa -l root server_IP_address
```

When prompted, enter the passkey to connect to the server.

For Linux

1. Enter the following commands at the UNIX server prompt:

```
ssh-keygen -q -f $HOME/.ssh/id_rsa -t rsa
cd $HOME/.ssh
cat id_rsa.pub >> authorized_keys
chmod 700 authorized_keys
```

You are prompted to enter a passphrase when you enter these commands. You can press **Enter** if you do not want to use a passphrase.

2. Add the following line in the `/etc/ssh/sshd_config` file:

```
AuthorizedKeysFile      /.ssh/id_rsa.pub
```

3. Enter the following commands to restart the UNIX server:

```
/etc/init.d/sshd stop
/etc/init.d/sshd start
```

4. Depending on the Oracle Identity Manager release that you are using, copy the `/.ssh/id_rsa` file to the following directory:

- For Oracle Identity Manager release 9.1.0.x:

```
OIM_HOME/xellerate/XLIntegrations/SSH/config
```

- For Oracle Identity Manager release 11.1.1:

```
OIM_HOME/server/XLIntegrations/SSH/config
```

5. To check if you can connect to the target system using the SSH protocol, directly from the command prompt and without using a password, depending on the Oracle Identity Manager release that you are using, enter the following command:

Note: The account used to run the OIM application server on UNIX should have the ownership of the `id_rsa` file.

- For Oracle Identity Manager release 9.1.0.x:

```
ssh -i OIM_HOME/xellerate/XLIntegrations/SSH/config/id_rsa root -i
localhost_ip_address
```

- For Oracle Identity Manager release 11.1.1:

```
ssh -i OIM_HOME/server/XLIntegrations/SSH/config/id_rsa root - i
lhost_ip_address
```

6. When you configure the IT resource, provide the name and full path of the `id_rsa` file as the value of the `Private Key` parameter:

- For Oracle Identity Manager release 9.1.0.x:

```
OIM_HOME/xellerate/XLIntegrations/SSH/config/id_rsa
```

- For Oracle Identity Manager release 11.1.1:

```
OIM_HOME/server/XLIntegrations/SSH/config/id_rsa
```

For AIX

1. The first step of this procedure depends on the version of AIX that you are using:

- For AIX 4.3, use the `/etc/openssh/sshd_config` file to set the following parameters:

```
export PATH=$PATH: /usr/local/bin
Installation path: /etc/openssh/
sshd -- /usr/local/bin/
```

- For AIX 5.2, use the `/etc/ssh/sshd_config` file to set the following parameters:

```
export PATH=$PATH: /usr/sbin
Installation path: /etc/ssh/
sshd -- /usr/sbin/
```

2. Open the `/etc/ssh/sshd_config` file, and uncomment the following lines:

```
AuthorizedKeysFile .ssh/authorized_keys
PermitRootLogin yes
PubkeyAuthentication yes
```

Note: Change the value of `PermitRootLogin` to `yes` only if it does not violate local security policies. If Public Key Authentication is enabled, then you can change the value of `PermitRootLogin` to `without-password`.

Instead of using the root account, if you can use a user account with sudo privileges, then you do not need to perform this step.

3. To restart the SSH server, enter the following commands:

- `/opt/ssh/sbin/sshd` (For AIX 4.3)
- `/usr/sbin/sshd` (For AIX 5.2)
- `/usr/sbin/sshd` (For AIX 6.1)

4. To test the login, enter the following command:

```
ssh -i /.ssh/id_rsa -l root server_IP_address
```

When prompted, enter the passkey to connect to the server.

Note: This release of the connector does not support Public Key Authentication provisioning if it is implemented through the SUDO Admin mode. The Public Key Authentication used for system access is available for the root user. This point is also mentioned in the Known Issues list in [Chapter 6, "Known Issues."](#)

2.4 Installing the Connector on Oracle Identity Manager Release 9.1.0.x or Release 11.1.1

Note: In this guide, the term **Connector Installer** has been used to refer to the Connector Installer feature of the Oracle Identity Manager Administrative and User Console.

Installing the connector on Oracle Identity Manager release 9.1.0.x or release 11.1.1 involves the following procedures:

- [Section 2.4.1, "Running the Connector Installer"](#)
- [Section 2.4.2, "Copying the sshfactory.jar File"](#)
- [Section 2.4.3, "Configuring the IT Resource"](#)
- [Section 2.4.4, "Copying the Configuration Files"](#)

2.4.1 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 System 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 **UNIX SSH 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 **UNIX SSH 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 2.5.1, "Configuring the Target System As a Trusted Source."](#)
- 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 2.5.3, "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 tasks that are 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 System Administrator's Guide for Oracle Identity Manager* for more information about scheduled tasks and scheduled jobs.

Record the names of the scheduled tasks displayed on this page. The procedure to configure these scheduled tasks 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 2-1](#).

Installing the Connector in an Oracle Identity Manager Cluster

While installing Oracle Identity Manager in a clustered environment, 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 2.1, "Files and Directories on the Installation Media"](#) for information about the files that you must copy and their destination locations on the Oracle Identity Manager server.

2.4.2 Copying the sshfactory.jar File

The sshfactory.jar file contains the JSCAPE libraries. These libraries are used to open an SSH session with the target server. To copy the sshfactory.jar file, perform one of the following procedures depending on the version of Oracle Identity Manager:

- If you are using Oracle Identity Manager release 9.1.0.x, then copy the ext/sshfactory.jar file from the installation media to the `OIM_HOME/xellerate/ThirdParty` directory.

Note: In an Oracle Identity Manager cluster, copy this JAR file into the ThirdParty directory on each node of the cluster.

- If you are using Oracle Identity Manager release 11.1.1, then:

Run the Upload JARs utility to post the ext/sshfactory.jar file from the installation media to the Oracle Identity Manager database. This utility is copied into the following location when you install Oracle Identity Manager:

Note: Before you run this utility, verify that the WL_HOME environment variable is set to the directory in which Oracle WebLogic Server is installed.

For Microsoft Windows:

`OIM_HOME/server/bin/UploadJars.bat`

For UNIX:

`OIM_HOME/server/bin/UploadJars.sh`

When you run the utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, URL of the Oracle Identity Manager host computer, context factory value, type of JAR file being uploaded, and the location from which the JAR file is to be uploaded. To upload the `sshfactory.jar` file, specify 3 as the value of the JAR type.

See Also: *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for detailed information about the Upload JARs utility.

2.4.3 Configuring the IT Resource

You must specify values for the parameters of the SSH LINUX 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 `SSH LINUX` 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. The following table describes each parameter:

| Parameter | Description and Sample Value |
|---------------------------------|--|
| Admin UserId | User ID of the administrator root or jdoe Here, <code>jdoe</code> can be the SUDO user ID, for the SUDO Admin mode. Alternatively, on Solaris, it can be the user ID of the account to which you assign the minimum privileges required to perform connector operations. See Section 2.3.3, "Creating a Target System User Account for Connector Operations" for more information. |
| Admin Password/Private file Pwd | Password of the administrator Note: For the SUDO Admin mode, the private key is not supported. Specify a password for this mode as the value of the parameter. If a private key is used, then enter the private key passphrase as the value of the parameter. For the Solaris target system, if an RBAC user is used, then enter the RBAC user's password as the value of the parameter. |
| Server IP Address | Server IP address |

| Parameter | Description and Sample Value |
|-------------------------------------|--|
| Port | The port at which the SSH service is running on the server Default value: 22 |
| Private Key | Private key file name with full path Note: For SUDO Admin administrator, this parameter must be left blank. |
| Server OS | Specify one of the following: <ul style="list-style-type: none"> ▪ AIX ▪ HP-UX ▪ SOLARIS ▪ LINUX |
| Shell Prompt | # or \$ |
| Whether Trusted System (HP-UX) | YES (for trusted HP-UX System) or NO (for non-trusted HP-UX system) |
| Sudo Or RBAC | Enter one of the following values: <ul style="list-style-type: none"> ▪ None: Specifies the root user. ▪ Sudo: Specifies the sudo user. ▪ RBAC: Specifies the RBAC user. See Section 2.3.3, "Creating a Target System User Account for Connector Operations" for more information. |
| Max Retries | Number of times that the connector must retry connecting to the target server if the connection fails Default value: 2 |
| Delay | Delay (in milliseconds) before the connector attempts to retry connecting to the target system, if the connection fails Default value: 10000 |
| Timeout | Value of the timeout (in milliseconds) for the connection to the target server Default value: 20000 |
| Passwd Mirror File/User Mirror File | Name and full path of the password mirror file/user mirror file The SUDO user must have read and write permissions on this file. For example, suppose you run the following command to view the permissions on the mirror file: <pre>\$ ls -ltr passwd1</pre> The command generates the following output: <pre>-rwxr--r-- 1 janedoe mqm 9972 Mar 11 20:35 passwd1</pre> In this output, janedoe is the SUDO user. Sample value for this attribute: /etc/passwd1 |

| Parameter | Description and Sample Value |
|--------------------|--|
| Shadow Mirror File | <p>Name of the shadow mirror file</p> <p>The SUDO user must have read and write permissions on this file.</p> <p>For example, suppose you run the following command to view the permissions on the mirror file:</p> <pre>\$ ls -ltr shadow1</pre> <p>The command generates the following output:</p> <pre>-rwxr--r-- 1 janedoe mqm 9972 Mar 11 20:35 shadow1</pre> <p>In this output, janedoe is the SUDO user.</p> <p>Note:</p> <p>This attribute is not required on AIX.</p> <p>The value of this attribute must not be null or blank, even for an HP-UX trusted system. However, the reconciliation process on an HP-UX trusted system ignores this attribute.</p> <p>Sample value: <code>/etc/shadow1</code></p> |
| Target Date Format | <p>This parameter is used to specify the date format of the target UNIX computer. The default value for this parameter is:</p> <pre>MMddhhmmyy</pre> <p>This parameter is used for user reconciliation.</p> |
| Protocol | <p>Default value: SSH</p> <p>Do not change this default value.</p> |
| RBAC Role Name | <p>If you specify RBAC as the value of the <code>Sudo Or RBAC</code> parameter, then enter the name of the role assigned to the RBAC user. Otherwise, do not specify a value for this parameter. See Section 2.3.3, "Creating a Target System User Account for Connector Operations" for more information.</p> |
| RBAC Role Passwd | <p>If you specify RBAC as the value of the <code>Sudo Or RBAC</code> parameter, then enter the password of the role assigned to the RBAC user. Otherwise, do not specify a value for this parameter. See Section 2.3.3, "Creating a Target System User Account for Connector Operations" for more information.</p> |

- To save the values, click **Save**.

2.4.4 Copying the Configuration Files

Depending on the Oracle Identity Manager that you are using, copy the files in the **config** directory of the installation media to the following directory on the Oracle Identity Manager host computer:

- For Oracle Identity Manager release 9.1.0.x:
`OIM_HOME/xellerate/XLIntegrations/SSH/config`
- For Oracle Identity Manager release 11.1.1:
`OIM_HOME/server/XLIntegrations/SSH/config`

2.5 Configuring the Oracle Identity Manager Server

Configuring the Oracle Identity Manager server involves the following procedures:

- [Section 2.5.1, "Configuring the Target System As a Trusted Source"](#)

- [Section 2.5.2, "Changing to the Required Input Locale"](#)
- [Section 2.5.3, "Clearing Content Related to Connector Resource Bundles from the Server Cache"](#)
- [Section 2.5.4, "Enabling Logging"](#)
- [Section 2.5.5, "Configuring Oracle Identity Manager for Request-Based Provisioning"](#)

2.5.1 Configuring the Target System As a Trusted Source

While configuring the connector, the target system can be designated as a trusted source or target resource. If you designate the target system as a **trusted source**, then during a reconciliation run:

- For each newly created user on the target system, an OIM User is created.
- Updates made to each user on the target system are propagated to the corresponding OIM User.

If you designate the target system as a **target resource**, then during a reconciliation run:

- For each account created on the target system, a resource is assigned to the corresponding OIM User.
- Updates made to each account on the target system are propagated to the corresponding resource.

Note: Skip this section if you do not want to designate the target system as a trusted source for reconciliation.

Configuring trusted source reconciliation involves the following steps:

1. Import the XML file for trusted source reconciliation, XellSSHUser.xml, by using the Deployment Manager. This section describes the procedure to import the XML file.

Note: Only one target system can be designated as a trusted source. If you import the XellSSHUser.xml file while you have another trusted source configured, then both connector reconciliations would stop working.

2. Specify values for the attributes of the SSH UserTrusted Reconciliation task scheduled task. This procedure is described later in this guide.

To import the XML file for trusted source reconciliation:

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 bar.
 - 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.

- 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 XellSSHUser.xml file, which is in the xml directory of 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**.

2.5.2 Changing to the Required Input Locale

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

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

You may require the assistance of the system administrator to change to the required input locale.

2.5.3 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 System Administrator's Guide for Oracle Identity Manager* for more information about the PurgeCache utility.

2.5.4 Enabling Logging

Depending on the Oracle Identity Manager release you are using, perform the procedure described in one of the following sections:

- [Section 2.5.4.1, "Enabling Logging on Oracle Identity Manager Release 9.1.0.x"](#)
- [Section 2.5.4.2, "Enabling Logging on Oracle Identity Manager Release 11.1.1"](#)

2.5.4.1 Enabling Logging on Oracle Identity Manager Release 9.1.0.x

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

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 might 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 depends on the application server that you use:

- **IBM WebSphere Application Server**

To enable logging:

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

```
log4j.logger.OIMCP.TELNETSSH=log_level
```

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

For example:

```
log4j.logger.OIMCP.TELNETSSH=INFO
```

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

```
WEBSPHERE_HOME/AppServer/logs/SERVER_NAME/SystemOut.log
```

■ JBoss Application Server

To enable logging:

1. In the *JBOSS_HOME/server/default/conf/log4j.xml* file, add the following lines if they are not already present in the file:

```
<category name="OIMCP.TELNETSSH">
  <priority value="log_level"/>
</category>
```

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

```
<category name="OIMCP.TELNETSSH">
  <priority value="INFO"/>
</category>
```

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

```
JBOSS_HOME/server/default/log/server.log
```

■ Oracle Application Server

To enable logging:

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

```
log4j.logger.OIMCP.TELNETSSH=log_level
```

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

For example:

```
log4j.logger.OIMCP.TELNETSSH=INFO
```

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

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

■ Oracle WebLogic Server

To enable logging:

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

```
log4j.logger.OIMCP.TELNETSSH=log_level
```

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

For example:

```
log4j.logger.OIMCP.TELNETSSH=INFO
```

After you enable logging, log information is displayed on the server console.

2.5.4.2 Enabling Logging on Oracle Identity Manager Release 11.1.1

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

Oracle Identity Manager release 11.1.1 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:

- `SEVERE.intValue()+100`
This level enables logging of information about fatal errors.
- `SEVERE`
This level enables logging of information about errors that might allow Oracle Identity Manager to continue running.
- `WARNING`
This level enables logging of information about potentially harmful situations.
- `INFO`
This level enables logging of messages that highlight the progress of the application.
- `CONFIG`
This level enables logging of information about fine-grained events that are useful for debugging.
- `FINE, FINER, FINEST`
These levels enable logging of information about fine-grained events, where `FINEST` logs information about all events.

These log levels are mapped to ODL message type and level combinations as shown in [Table 2-2](#).

Table 2-2 Log Levels and ODL Message Type:Level Combinations

| Log Level | ODL Message Type:Level |
|------------------------------------|-------------------------------|
| <code>SEVERE.intValue()+100</code> | <code>INCIDENT_ERROR:1</code> |
| <code>SEVERE</code> | <code>ERROR:1</code> |
| <code>WARNING</code> | <code>WARNING:1</code> |
| <code>INFO</code> | <code>NOTIFICATION:1</code> |
| <code>CONFIG</code> | <code>NOTIFICATION:16</code> |
| <code>FINE</code> | <code>TRACE:1</code> |
| <code>FINER</code> | <code>TRACE:16</code> |

Table 2–2 (Cont.) Log Levels and ODL Message Type:Level Combinations

| Log Level | ODL Message Type:Level |
|-----------|------------------------|
| FINEST | TRACE:32 |

The configuration file for OJDL is logging.xml, which is located at the following path:

DOMAIN_HOME/config/fmwconfig/servers/*OIM_SERVER*/logging.xml

Here, *DOMAIN_HOME* and *OIM_SERVER* are the domain name and server name specified during the installation of Oracle Identity Manager.

To enable logging in Oracle WebLogic Server:

1. Edit the logging.xml file as follows:

a. Add the following blocks in the file:

```
<log_handler name='telnetssh-handler' level='[LOG_LEVEL]'
class='oracle.core.ojdl.logging.ODLHandlerFactory'>
<property name='logreader:' value='off' />
  <property name='path' value='[FILE_NAME]' />
  <property name='format' value='ODL-Text' />
  <property name='useThreadName' value='true' />
  <property name='locale' value='en' />
  <property name='maxFileSize' value='5242880' />
  <property name='maxLogSize' value='52428800' />
  <property name='encoding' value='UTF-8' />
</log_handler>

<logger name="OIMCP.TELNETSSH" level="[LOG_LEVEL]"
useParentHandlers="false">
  <handler name="telnetssh-handler" />
  <handler name="console-handler" />
</logger>
```

b. Replace both occurrences of **[LOG_LEVEL]** with the ODL message type and level combination that you require. Table 2–2 lists the supported message type and level combinations.

Similarly, replace **[FILE_NAME]** with the full path and name of the log file in which you want log messages to be recorded.

The following blocks show sample values for **[LOG_LEVEL]** and **[FILE_NAME]**:

```
<log_handler name='telnetssh-handler' level='NOTIFICATION:1'
class='oracle.core.ojdl.logging.ODLHandlerFactory'>
<property name='logreader:' value='off' />
  <property name='path'
value='F:\MyMachine\middleware\user_projects\domains\base_domain1\servers\o
im_server1\logs\oim_server1-diagnostic-1.log' />
  <property name='format' value='ODL-Text' />
  <property name='useThreadName' value='true' />
  <property name='locale' value='en' />
  <property name='maxFileSize' value='5242880' />
  <property name='maxLogSize' value='52428800' />
  <property name='encoding' value='UTF-8' />
</log_handler>

<logger name="OIMCP.TELNETSSH" level="NOTIFICATION:1"
useParentHandlers="false">
```

```
<handler name="telnetssh-handler" />
<handler name="console-handler" />
</logger>
```

With these sample values, when you use Oracle Identity Manager, all messages generated for this connector that are of a log level equal to or higher than the NOTIFICATION: 1 level are recorded in the specified file.

2. Save and close the file.
3. Set the following environment variable to redirect the server logs to a file:

For Microsoft Windows:

```
set WLS_REDIRECT_LOG=FILENAME
```

For UNIX:

```
export WLS_REDIRECT_LOG=FILENAME
```

Replace **FILENAME** with the location and name of the file to which you want to redirect the output.

4. Restart the application server.

2.5.5 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 2.5.5.1, "Importing Request Datasets Using Deployment Manager"](#)
- [Section 2.5.5.2, "Copying Predefined Request Datasets"](#)
- [Section 2.5.5.3, "Importing Request Datasets into MDS"](#)
- [Section 2.5.5.4, "Enabling the Auto Save Form Feature"](#)
- [Section 2.5.5.5, "Running the PurgeCache Utility"](#)

2.5.5.1 Importing Request Datasets Using Deployment Manager

Note:

- You can perform this procedure instead of the procedures described in [Section 2.5.5.2, "Copying Predefined Request Datasets"](#) and [Section 2.5.5.3, "Importing Request Datasets into MDS"](#).
 - See *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager* for detailed information about importing objects from an XML file using the Deployment Manager.
-
-

A request dataset is an XML file that specifies the information to be submitted by the requester during a provisioning operation. These request datasets specify information about the default set of attributes for which the requester must submit information during a request-based provisioning operation.

To import a request dataset XML file by using the Deployment Manager:

1. Log in to the Oracle Identity Manager Administrative and User Console.
2. Click the **Deployment Management** link on the left navigation bar.
3. Click the **Import** link under Deployment Management.

A dialog box for opening files is displayed.

4. Locate and open the request dataset XML file, `SSHConnectorRequestDatasets.xml`, which is in the `xml` directory of 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. Close the Deployment Manager dialog box.

The request dataset is imported into Oracle Identity Manager.

2.5.5.2 Copying Predefined Request Datasets

Predefined request datasets are shipped with this connector. The following are the predefined request dataset available in the `DataSets` directory on the installation media:

- `ProvisionResourceSSH User.xml`
- `ModifyResourceSSH User.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\SSHStd

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.

2.5.5.3 Importing Request Datasets into MDS

You can configure request-based provisioning by importing the request datasets into the metadata store (MDS) 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 2.5.5.2, "Copying Predefined Request Datasets,"](#) if you copy the files to the E:\MyDatasets\custom\connector\SSHStd directory, then set the value of the `metadata_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.

2.5.5.4 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 **SSH User** process definition.
4. Select the **Auto Save Form** check box.
5. Click **Save**.

2.5.5.5 Running the PurgeCache Utility

Run the PurgeCache utility to clear content belonging to the Metadata category from the server cache. See [Section 2.5.3, "Clearing Content Related to Connector Resource Bundles from the Server Cache"](#) for instructions.

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

Using the Connector

After you deploy the connector, you must configure it to meet your requirements. This chapter discusses the following connector configuration procedures:

Note: These sections provide both conceptual and procedural information about configuring the connector. It is recommended that you read the conceptual information before you perform the procedures.

- [Section 3.1, "Performing First-Time Reconciliation"](#)
- [Section 3.2, "Scheduled Task for Lookup Field Synchronization"](#)
- [Section 3.3, "Configuring Reconciliation"](#)
- [Section 3.4, "Configuring Scheduled Tasks"](#)
- [Section 3.5, "Guidelines on Performing Provisioning Operations"](#)
- [Section 3.6, "Performing Provisioning Operations"](#)
- [Section 3.7, "Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1"](#)

3.1 Performing First-Time Reconciliation

First-time reconciliation involves synchronizing lookup definitions in Oracle Identity Manager with the lookup fields of the target system, and performing full reconciliation. In full reconciliation, all existing user records from the target system are brought into Oracle Identity Manager.

The following is the sequence of steps involved in reconciling all existing user records:

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

1. Perform lookup field synchronization by running the scheduled tasks provided for this operation.
See [Section 3.2, "Scheduled Task for Lookup Field Synchronization"](#) for information about the attributes of the scheduled tasks for lookup field synchronization.
See [Section 3.4, "Configuring Scheduled Tasks"](#) for information about running scheduled tasks.
2. Perform user reconciliation by running the scheduled task for user reconciliation.
See [Section 3.3.4, "Reconciliation Scheduled Tasks"](#) for information about the attributes of this scheduled task.
See [Section 3.4, "Configuring Scheduled Tasks"](#) for information about running scheduled tasks.

The Pwshd Mirror File/User Mirror File and Shadow Mirror File parameters of the SSH IT resource contain the name and full path of the password mirror and shadow mirror files, respectively. Before you perform first-time reconciliation, the passwd mirror and shadow mirror files are empty (do not contain any user records).

After first-time reconciliation, the user records in the passwd and passwd mirror files are the same. Similarly, the user records in the shadow and shadow mirror files are the same.

From the next reconciliation run onward, only target system user records that are added or modified after the last reconciliation run are considered for incremental reconciliation. This is done by examining differences between the /etc/passwd, /etc/shadow files and their corresponding mirror files."

Note: For AIX, first-time reconciliation involves reconciliation of all the users present in the target system. This functionality is different from that of other target systems. On other target systems, records of all existing users are fetched from the target system only if you have created the passwd mirror file and the shadow mirror file as empty files.

See Also: [Section 2.4.3, "Configuring the IT Resource"](#) for information about the parameters of the IT resource

3.2 Scheduled Task for Lookup Field Synchronization

The TelnetSSHGroupLookupReconTask scheduled task is used for lookup fields reconciliation.

[Table 3–1](#) describes the attributes of this scheduled task. See [Section 3.4, "Configuring Scheduled Tasks"](#) for information about configuring scheduled tasks.

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 were left empty, then reconciliation would not be performed.

Table 3–1 Attributes of the Scheduled Tasks for Lookup Field Synchronization

| Attribute | Description |
|-------------------|--|
| Server | Enter the name of the target system IT resource. Sample value: SSH Server |
| Lookup Field Name | Enter the name of the lookup field (on the process form) to be used in lookup reconciliation. Default value: UD_Lookup_SSH_PrimaryGroupNames. |
| Exclusion List | Enter a comma-delimited list of the names of groups on the target system that you do not want to reconcile. Sample value: jdoe, ssam, jsmith |

3.3 Configuring Reconciliation

As mentioned earlier in this guide, reconciliation involves duplicating in Oracle Identity Manager the creation of and modifications to user accounts on the target system. This section discusses the following topics related to configuring reconciliation:

- [Section 3.3.1, "Full Reconciliation"](#)
- [Section 3.3.2, "Limited Reconciliation"](#)
- [Section 3.3.3, "Batched Reconciliation"](#)
- [Section 3.3.4, "Reconciliation Scheduled Tasks"](#)

3.3.1 Full Reconciliation

Full reconciliation involves reconciling all existing user records from the target system into Oracle Identity Manager. After you deploy the connector, you must first perform full reconciliation. In addition, you can switch from incremental reconciliation to full reconciliation whenever you want to ensure that all target system records are reconciled in Oracle Identity Manager.

To perform a full reconciliation run:

- Run the following commands on the target system before you run the scheduled tasks:


```
> etc/passwd1
> etc/shadow1
```
- Specify `All` as the value of the `NumberOfBatches` attribute of the user reconciliation scheduled task.

At the end of the reconciliation run, the user records in the passwd mirror and shadow mirror files are the same as in the passwd and shadow files, respectively. From the next reconciliation run onward, only records created or modified after the last reconciliation run are considered for reconciliation. This is incremental reconciliation.

3.3.2 Limited Reconciliation

By default, all target system records that are added or modified after the last reconciliation run are reconciled during the current reconciliation run. You can customize this process by specifying the subset of added or modified target system records that must be reconciled. You do this by creating a reconciliation filter.

For this connector, you create a filter by specifying a value for the `UserNameFilter` scheduled task attribute, which will be used in the query `SELECT` criteria to retrieve the records to be reconciled. For example, if you specify the value `JDoe` for this attribute, then all target system user records with the user name `JDoe` are reconciled.

3.3.3 Batched Reconciliation

During a reconciliation run, all changes in the target system records are reconciled into Oracle Identity Manager. Depending on the number of records to be reconciled, this process may require a large amount of time. In addition, if the connection breaks during reconciliation, then the process would take longer to complete.

You can configure batched reconciliation to avoid these problems.

To configure batched reconciliation, you must specify values for the following user reconciliation scheduled task attributes:

- `BatchSize`: Use this attribute to specify the number of records that must be included in each batch. The default value is `1000`.
- `NumberOfBatches`: Use this attribute to specify the total number of batches that must be reconciled. The default value is `All`.

If you specify a value other than `All`, then some of the newly added or modified user records may not get reconciled during the current reconciliation run. The following example illustrates this:

Suppose you specify the following values while configuring the scheduled tasks:

- `BatchSize`: `20`
- `NumberOfBatches`: `10`

Suppose that 314 user records were created or modified after the last reconciliation run. Of these 314 records, only 200 records would be reconciled during the current reconciliation run. The remaining 114 records would be reconciled during the next reconciliation run.

You specify values for the `BatchSize` and `NumberOfBatches` attributes by following the instructions described in [Section 3.4, "Configuring Scheduled Tasks."](#)

3.3.4 Reconciliation Scheduled Tasks

When you run the Connector Installer or import the connector XML file, the following reconciliation scheduled tasks are automatically created in Oracle Identity Manager:

- SSH User Trusted Source Reconciliation Task

This scheduled task is used to reconcile user data in the trusted source (identity management) mode of the connector.

- SSH User Target Resource Reconciliation Task

This scheduled task is used to reconcile user data in the target resource (account management) mode of the connector.

[Table 3–2](#) describes the attributes of both scheduled tasks. See [Section 3.4, "Configuring Scheduled Tasks"](#) for information about configuring scheduled tasks.

Table 3–2 Attributes of the User Reconciliation Scheduled Tasks

| Attribute | Description |
|---|---|
| Server | <p>If the parameter <code>IsRoRecon</code> is set to <code>No</code> then, enter the name of the IT resources as comma separated value for the UNIX SSH installation from which you want to reconcile user records.</p> <p>If the parameter <code>IsRoRecon</code> is set to <code>Yes</code>, then enter the name of the Server type under the IT Resource type definition for the RO which you want to reconcile user records.</p> |
| IsTrusted | <p>A value of <code>Yes</code> implies that you want to configure the connector for trusted source reconciliation.</p> <p>A value of <code>No</code> implies that you want to configure the connector for target resource reconciliation.</p> <p>The default value of this attribute in the SSH User Target Resource Reconciliation Task scheduled task is <code>No</code>.</p> <p>The default value of this attribute in the SSH User Trusted Source Reconciliation Task scheduled task is <code>Yes</code>.</p> <p>Note: It is recommended that you do not change the value of this attribute.</p> |
| Target System Recon - Resource Object name | <p>Enter the name of the resource object against which target resource reconciliation runs must be performed.</p> <p>Default value: <code>SSH User</code></p> |
| Trusted Source Recon - Resource Object name | <p>Enter the name of the resource object against which trusted source reconciliation runs must be performed.</p> <p>Default value: <code>xellerate User</code></p> <p>Note: Enter <code>false</code> (in lowercase) if you do not want to configure trusted source reconciliation</p> |
| BatchSize | <p>Enter the number of records that must be included in each batch fetched from the target system.</p> <p>If you do not want to implement batched reconciliation, then specify <code>nodata</code>.</p> <p>Default value: <code>1000</code></p> <p>See Also: Section 3.3.3, "Batched Reconciliation"</p> |
| NoOfBatches | <p>This attribute specifies the number of batches to be reconciled. Enter <code>All</code> if you want to reconcile all the batches. This is the default value.</p> <p>Enter an integer value if you want to reconcile only a fixed number of batches.</p> <p>Default value: <code>All</code></p> <p>Sample value: <code>50</code></p> <p>The number of records in each batch is specified by the <code>BatchSize</code> attribute.</p> <p>See Also: Section 3.3.3, "Batched Reconciliation"</p> |

Table 3–2 (Cont.) Attributes of the User Reconciliation Scheduled Tasks

| Attribute | Description |
|---------------------|--|
| UserNameFilter | <p>This is a filter attribute. Use this attribute to specify the user name (User Login) for which you want to reconcile user records.</p> <p>If you do not want to use this filter attribute, then specify <code>Nodata</code>.</p> <p>Default value: <code>Nodata</code></p> <p>See Also: Section 3.3.2, "Limited Reconciliation"</p> |
| TransformLookupName | <p>Enter <code>Lookup.Reconciliation.TransformationMap</code>, which is the name of the lookup definition used for the transformation class map that is stored in the lookup tables.</p> <p>This attribute is valid only when the <code>UseTransformMapping</code> attribute is set to <code>Yes</code>.</p> <p>Note: You must not change the value of this attribute.</p> <p>See Section 4.4, "Transforming Data Reconciled Into Oracle Identity Manager" for detailed information about using the <code>TransformLookupName</code> attribute.</p> |
| UseTransformMapping | <p>Enter <code>Yes</code> if you want the transform mappings accessed by the <code>TransformLookupName</code> attribute to be used. Otherwise, enter <code>No</code>.</p> <p>The default value is <code>No</code>.</p> <p>See Section 4.4, "Transforming Data Reconciled Into Oracle Identity Manager" for detailed information about using the <code>UseTransformMapping</code> attribute.</p> |
| IsRoRecon | <p>A value of <code>Yes</code> implies that you want to configure the connector to perform reconciliation for the all <code>ITResources</code> under the given resource object.</p> <p>A value of <code>No</code> implies that you want to configure the connector to perform reconciliation for the <code>ITResources</code> provided in the <code>Server</code> attribute.</p> <p>The default value of this attribute in the SSH User Target Resource Reconciliation Task scheduled task is <code>No</code>.</p> |

3.4 Configuring Scheduled Tasks

You can apply this procedure to configure the scheduled tasks for lookup field synchronization and reconciliation.

[Table 3–3](#) lists the scheduled tasks that form part of the connector.

Table 3–3 Scheduled Tasks for Lookup Field Synchronization and Reconciliation

| Scheduled Task | Description |
|--|---|
| TelnetSSHGroupLookupReconTask | This scheduled task is used to synchronize the values of group lookup fields between Oracle Identity Manager and the target system. See Section 3.2, "Scheduled Task for Lookup Field Synchronization" for information about this scheduled task. |
| SSH User Trusted Source Reconciliation Task | This scheduled task is used for reconciling user data when the target system is configured as a trusted source. See Section 3.3.4, "Reconciliation Scheduled Tasks" for information about this scheduled task. |
| SSH User Target Resource Reconciliation Task | This scheduled task is used for reconciling user data when the target system is configured as a target resource. See Section 3.3.4, "Reconciliation Scheduled Tasks" for information about this scheduled task. |

Depending on the Oracle Identity Manager release that you are using, perform the procedure described in the following sections:

- [Section 3.4.1, "Configuring Scheduled Tasks on Oracle Identity Manager Release 9.1.0.x or Release 11.1.1"](#)

3.4.1 Configuring Scheduled Tasks on Oracle Identity Manager Release 9.1.0.x or Release 11.1.1

To configure a scheduled task:

1. Log in to the Administrative and User Console.
2. Perform one of the following:
 - 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 the edit icon in the Edit column for the scheduled task.
 - c. On the Scheduled Task Details page where the details of the scheduled task that you selected is 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. To do so:
 - 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 1.
 - **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 System 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. To do so:

Note:

- Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.
 - Attributes of the scheduled task are discussed in [Section 3.3.4, "Reconciliation Scheduled Tasks."](#)
-
-

- 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.
6. After specifying the attributes, perform one of the following:
 - 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 Administrative and User Console. If you want to stop a task, then click **Stop Execution** on the Task Scheduler form of the Design Console.

- 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 Administrative and User Console. You can use the Scheduler Status page to either start, stop, or reinitialize the scheduler.

3.5 Guidelines on Performing Provisioning Operations

Apply the following guidelines while performing provisioning operations:

- When you perform the Disable User provisioning operation, the connector disables a user account by prefixing the value in the password field of the shadow

file with two exclamation points (!!). When you perform the Enable User provisioning operation, the connector enables a user account by removing the two exclamation points (!!) that were prefixed to the value in the password field. After the user account is enabled, to log in to the target system, the user can use the password that was last used before the user account was disabled.

Therefore, to ensure that the user uses a new password after the account is enabled, you must perform the Set Password provisioning operation before you perform the Enable User provisioning operation.

- The Set Password provisioning operation resets the password of a target system user account.

If the Set Password provisioning operation is performed on a user account that has been disabled, then the account is automatically reenabled. This is because information on whether a user account is disabled is stored in the password field of the shadow file. Therefore, when you perform the Set Password provisioning operation, the value in the password field is reset, which causes information on whether or not a user account is disabled to be lost.

- While performing a Create User provisioning operation, before populating the Skeleton directory field, data must be populated in the Home Directory field and the Create Home Directory check box must also be selected.
- The value in the User Login field must not contain a colon (:) or a newline (\n) character.
- The value of the GECOS field must not contain a ' (single apostrophe) or . (period) character.
- The group names that you specify in the Secondary Group Names field must be separated by commas, with no intervening whitespace between them.
- The value in the Home Directory field must not contain spaces.
- The maximum permitted date value for account expiry is 31-Dec-2099.
- When you specify the secondary group name for the first time and then run the Update Secondary Group Names provisioning operation, the primary group name is assigned the same value as the secondary group name. However, after the value of the primary group name is changed, you cannot set the secondary group name to the same value.
- On AIX 5.2, while performing an Update User Login provisioning operation, the GECOS field value must not contain spaces.
- On HP-UX, while performing a Create User provisioning operation, the Inactive Days field must be populated only when the UNIX server is configured in trusted mode.
- On Solaris, the value of the Secondary Group Names field in the User Defined process form must always be different from the value of the Primary Group Name field.
- On Solaris, while performing a Create User provisioning operation, the value in the Secondary Group Names field must be different from the value in the Primary Group Name field.

3.6 Performing Provisioning Operations

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 3.7, "Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1."](#)

The following are types of provisioning operations:

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

See Also: *Oracle Identity Manager Connector Concepts* for information about the types of provisioning

This section discusses the following topics:

- [Section 3.6.1, "Direct Provisioning"](#)
- [Section 3.6.2, "Request-Based Provisioning"](#)

3.6.1 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:
 - a. From the Users menu, select **Create**.
 - b. 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:
 - a. On the Welcome to Identity Administration page, in the Users region, click **Create User**.
 - b. 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:
 - a. From the Users menu, select **Manage**.
 - b. 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:
 - a. On the Welcome to Identity Administration page, search for the OIM User by selecting **Users** from the list on the left pane.

- b. 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:
 - a. On the User Detail page, select **Resource Profile** from the list at the top of the page.
 - b. On the Resource Profile page, click **Provision New Resource**.
 - If you are using Oracle Identity Manager release 11.1.1, then:
 - a. On the user details page, click the **Resources** tab.
 - b. 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 **SSH User** 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 SSH User 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:
 - a. Close the window displaying the "Provisioning has been initiated" message.
 - b. On the Resources tab, click **Refresh** to view the newly provisioned resource.

3.6.2 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 3.6.2.1, "End User's Role in Request-Based Provisioning"](#)
- [Section 3.6.2.2, "Approver's Role in Request-Based Provisioning"](#)

3.6.2.1 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 **SSH User**, 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.

3.6.2.2 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.

3.7 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 2.5.5, "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 **SSH User** 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 **SSH User** 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 **SSH User** 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 **SSH User** resource object.
 - c. Select the **Self Request Allowed** check box.
 - d. Click the Save icon.

Extending the Functionality of the Connector

After you deploy the connector, you must configure it to meet your requirements. This chapter discusses the following connector configuration procedures:

- [Section 4.1, "Adding Custom Attributes for Target Resource Reconciliation"](#)
- [Section 4.2, "Adding Custom Attributes for Provisioning"](#)
- [Section 4.3, "Configuring the Connector for Multiple Installations of the Target System"](#)
- [Section 4.4, "Transforming Data Reconciled Into Oracle Identity Manager"](#)

4.1 Adding Custom Attributes for Target Resource Reconciliation

Note:

- In this section, the term "attribute" refers to the identity data fields that store user data.
 - You need not perform this procedure if you do not want to add custom attributes for reconciliation.
-
-

By default, the attributes listed in [Section 1.6, "Connector Objects Used During Target Resource Reconciliation and Provisioning"](#) are mapped for reconciliation between Oracle Identity Manager and the target system. If required, you can map additional attributes for reconciliation as follows:

See Also: *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for detailed instructions on performing the following steps

1. Depending on the Oracle Identity Manager release that you are using, for Oracle Identity Manager release 9.1.0.x, open the following file in the `OIM_HOME/xellerate/XLIntegrations/SSH/config` directory, and for Oracle Identity Manager release 11.1.1, open the following file in the `OIM_HOME/xellerate/XLIntegrations/SSH/config` directory:

For AIX:

`userAttribute_AIX_recon.properties`

For non-AIX platforms:

`userAttribute_NonAIX_recon.properties`

2. At the end of this file, some of the attribute definitions are preceded by comment characters. You can uncomment the definition of an attribute to make it a part of the list of reconciliation attributes. If required, you can also add new attributes in this file. The format that you must use is as follows:

For AIX:

```
Target_System_Attribute=OIM_Server_Attribute
```

For example:

```
maxage=Users.AccountExpiryDate
```

In this example, `AccountExpiryDate` is the reconciliation field and `maxage` is the equivalent server command parameter. As a standard, the prefix "Users ." is added at the start of all reconciliation field names.

For non-AIX platforms:

```
OIM_Server_Attribute=Target_System_Attribute_index
```

For example:

```
Users.DefaultShell=6
```

In this example, `DefaultShell` is the reconciliation field and `6` is the equivalent server Target Server Attributes index. As a standard, the prefix "Users ." is added at the start of all reconciliation field names.

3. In the resource object definition, add a reconciliation field corresponding to the new attribute as follows:
 - a. Open the Resource Objects form. This form is in the Resource Management folder.
 - b. Click **Query for Records**.
 - c. On the Resource Objects Table tab, double-click the `SSH User` resource object to open it for editing.
 - d. On the Object Reconciliation tab, click **Add Field** to open the Add Reconciliation Field dialog box.
 - e. Specify a value for the field name.

For AIX:

You must specify the name that is to the right of the equal sign in the line that you uncomment or add while performing Step 2.

For example, if you uncomment the `maxage=Users.AccountExpiryDate` line in Step 2, then you must specify `Users.AccountExpiryDate` as the attribute name.

For non-AIX platforms:

You must specify the name that is to the left of the equal sign in the line that you uncomment or add while performing Step 2.

For example, if you uncomment the `Users.DefaultShell=6` line in Step 2, then you must specify `Users.DefaultShell` as the attribute name.

- f. From the **Field Type** list, select a data type for the field.

For example: `String`

- g. Save the values that you enter, and then close the dialog box.
 - h. If required, repeat Steps d through g to map more fields.
 - i. If you are using Oracle Identity Manager release 11.1.1, then click **Create Reconciliation Profile**. This copies changes made to the resource object into the MDS.
4. Add a new field in the process form.
 - a. Open the **UD_SSH** process form. This form is in the Development Tools folder of the Oracle Identity Manager Design Console.
 - b. Click **Create New Version**.
 - c. In the Create a New Version dialog box, specify the version name in the **Label** field, save the changes, and then close the dialog box.
 - d. From the **Current Version** list, select the newly created version.
 - e. On the Additional Columns tab, click **Add**.
 - f. Specify the new field name and other values. For the example described in Step 3 in the connector guide, you enter the value `UD_SSH_DEFAULTSHELL`.
 - g. Click **Make Version Active** and then save the changes.
 5. Modify the provisioning process to include the mapping between the newly added attribute and the corresponding reconciliation field as follows:
 - a. Open the **SSH User** provisioning process. The provisioning process form is in the Process Management folder.
 - b. On the Reconciliation Field Mappings tab, click **Add Field Map** to open the Add Reconciliation Field Mapping dialog box.
 - c. Enter the required values, save the values that you enter, and then close the dialog box.

For the example described in Step 3 in the connector guide, you enter the values `Users.DefaultShell [String]` and `UD_SSH_DEFAULTSHELL`.
 - d. If required, repeat Steps b and c to map more fields.

4.2 Adding Custom Attributes for Provisioning

Note: In this section, the term "attribute" refers to the identity data fields that store user data.

By default, the attributes listed in [Section 1.6, "Connector Objects Used During Target Resource Reconciliation and Provisioning"](#) are mapped for provisioning between Oracle Identity Manager and the target system. If required, you can map additional attributes for provisioning as follows:

See Also: *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*

1. Modify the attribute entries in the following files:
 - For Oracle Identity Manager 9.1.0.x:
On the AIX platform:

`OIM_HOME/xellerate/XLIntegrations/SSH/config/userAttribute_AIX_prov.properties`

On the non-AIX platforms:

`OIM_HOME/xellerate/XLIntegrations/SSH/config/userAttribute_NonAIX_prov.properties`

If required, you can add new attributes in this file. The format that you must use is as follows:

`OimAttributeName=TargetAttributeName`

For example:

`homeDir=-d`

- For Oracle Identity Manager 11.1.1:

On the AIX platform:

`OIM_HOME/server/XLIntegrations/SSH/config/userAttribute_AIX_prov.properties`

On the non-AIX platforms:

`OIM_HOME/server/XLIntegrations/SSH/config/userAttribute_NonAIX_prov.properties`

If required, you can add new attributes in this file. The format that you must use is as follows:

`OimAttributeName=TargetAttributeName`

For example:

`homeDir=-d`

2. Add a new column in the process form.

Note: If you have already performed Step 4 of [Section 4.1, "Adding Custom Attributes for Target Resource Reconciliation,"](#) then directly proceed to Step 3.

- a. Open the process form. This form is in the Development Tools folder of the Oracle Identity Manager Design Console.
 - b. Click **Create New Version**.
 - c. In the Create a New Version dialog box, specify the version name in the **Label** field, save the changes, and then close the dialog box.
 - d. From the **Current Version** list, select the newly created version.
 - e. On the Additional Columns tab, click **Add**.
 - f. Specify the new field name and other values.
 - g. Click **Make Version Active** and save the changes.
3. Add a new variable in the variable list.
 - a. Open the Adapter Factory form. This form is in the Development Tools folder of the Oracle Identity Manager Design Console.

- b. Click the **Query for Records** icon.
 - c. On the Adapter Factory Table tab, double-click the **adpSSHCREATEUSER** adapter from the list.
 - d. On the Variable List tab, click **Add**.
 - e. In the Add a Variable dialog box, specify the required values and then save and close the dialog box.
4. Define an additional adapter task for the newly added variable in the **adpSSHCREATEUSER** adapter.
- a. On the Adapter Tasks tab of the Adapter Factory form, click **Add**.
 - b. In the Adapter Task Selection dialog box, select **Functional Task**, select **Java** from the list of functional task types, and then click **Continue**.
 - c. In the Object Instance Selection dialog box, select **Persistent Instance** and then click **Continue**.
 - d. In the Add an Adapter Factory Task dialog box, specify the task name, select the **setProperty** method from the **Method** list, and then click **Save**.
 - e. Map the application method parameters, and then save and close the dialog box. To map the application method parameters:
 - For the "Output: String Return variable (Adapter Variable)" parameter:
 - i. From the **Map to** list, select **Literal**.
 - ii. From the **Name** list, select **Return variable**.
 - For the "Input: String input (Adapter Variable)" parameter:
 - i. From the **Map to** list, select **Adapter Variables**.
 - ii. From the **Name** list, select **Input**.
 - For the "Input: String (Literal)" parameter:
 - i. From the **Map to** list, select **Literal**.
 - ii. From the **Name** list, select **String**.
 - iii. In the **Value** field, specify the name that is to the left of the equal sign in the line that you uncomment or add while performing Step 1.

For example, if you uncomment the `homeDir=-d` line in Step 1, then you must specify `homeDir` as the attribute name.
 - For the "Input: String (Adapter Variable)" parameter:
 - i. From the **Map to** list, select **Adapter Variables**.
 - ii. From the **Name** list, select the newly added adapter variable.
 - f. Repeat Steps b through g to create more adapter tasks.
5. Create an additional adapter task to set the input variable.
- a. Open the Adapter Factory form. This form is in the Development Tools folder in the Oracle Identity Manager Design Console.
 - b. On the Adapter Tasks tab, click **Add**.
 - c. In the Adapter Task Selection dialog box, select **Logic Task**, select **SET VARIABLE** from the list, and then click **Continue**.

- d. In the Edit Set Variable Task Parameters dialog box, select **input** from the **Variable Name** list, select **Adapter Task** from the **Operand Type** list, and the Operand Qualifier as the Adapter Task that you have created in the previous step. Then, click **Save**.
6. Map the process form columns and adapter variables for the Create User process task as follows:
 - a. Open the Process Definition form. This form is in the Process Management folder of the Design Console.
 - b. Click the **Query for Records** icon.
 - c. On the Process Definition Table tab, double-click the **SSH User** process.
 - d. On the Tasks tab, double-click the **Create User** task.
 - e. In the Closing Form dialog box, click **Yes**.
 - f. On the Integration tab of the Editing Task Columns Create User dialog box, map the unmapped variables, and then save and close the dialog box. To map an unmapped variable:
 - i. Double-click the row in which **N** is displayed in the Status column. The value **N** signifies that the variable is not mapped.
 - ii. From the **Map to** list in the Edit Data Mapping for Variables dialog box, select **Process Data**.
 - iii. From the **Qualifier** list, select the name of the variable.
 Repeat Steps i through iii for all unmapped variables.
 Repeat Steps 1 through 6 if you want to add more attributes.
 7. Update the request datasets.

Note: Perform steps 7 through 9 only if you want to perform request-based provisioning.

When you add an attribute on the process form, you also update the XML files containing the request dataset definitions. To update a request dataset:

- a. In a text editor, open the XML file located in the `OIM_HOME/DataSet/file` directory for editing.
- b. Add the `AttributeReference` element and specify values for the mandatory attributes of this element.

See Also: The "Configuring Requests" chapter of the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* guide for more information about creating and updating request datasets

For example, while performing Step 2 of this procedure, if you added Employee ID as an attribute on the process form, then enter the following line:

```
<AttributeReference
name = "Employee ID"
attr-ref = "Employee ID"
type = "String"
widget = "text"
length = "50"
available-in-bulk = "false"/>
```


In this `AttributeReference` element:

- For the `name` attribute, enter the value in the `Name` column of the process form without the `tablename` prefix.
For example, if `UD_SSH_EMP_ID` is the value in the `Name` column of the process form, then you must specify `Employee ID` as the value of the `name` attribute in the `AttributeReference` element.
- For the `attr-ref` attribute, enter the value that you entered in the `Field Label` column of the process form while performing Step 2.
- For the `type` attribute, enter the value that you entered in the `Variant Type` column of the process form while performing Step 2.
- For the `widget` attribute, enter the value that you entered in the `Field Type` column of the process form, while performing Step 2.
- For the `length` attribute, enter the value that you entered in the `Length` column of the process form while performing Step 2.
- For the `available-in-bulk` attribute, specify `true` if the attribute must be available during bulk request creation or modification. Otherwise, specify `false`.

If you added more than one attribute on the process form, then repeat this step for each attribute added.

c. Save and close the XML file.

8. Run the `PurgeCache` utility to clear content related to request datasets from the server cache.

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

9. Import into MDS the request dataset definitions in XML format.

See [Section 2.5.5.3, "Importing Request Datasets into MDS"](#) for detailed information about the procedure.

4.3 Configuring the Connector for Multiple Installations of the Target System

Note: Perform this procedure only if you want to configure the connector for multiple installations of the target system.

You may want to configure the connector for multiple installations of the target system. The following example illustrates this requirement:

The Tokyo, London, and New York offices of Example Multinational Inc. have their own installations of the target system. The company has recently installed Oracle Identity Manager, and they want to configure Oracle Identity Manager to link all the installations of the target system.

To meet the requirement posed by such a scenario, you must configure the connector for multiple installations of the target system.

To configure the connector for multiple installations of the target system:

See Also: *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for detailed instructions on performing each step of this procedure

1. Create and configure one IT resource for each target system installation.
The IT Resources form is in the Resource Management folder. An IT resource is created when you import the connector XML file. You can use this IT resource as the template for creating the remaining IT resources, of the same resource type.
2. Configure reconciliation for each target system installation. See [Section 3.4, "Configuring Scheduled Tasks"](#) for instructions. Note that you only need to modify the attributes that are used to specify the IT resource and to specify whether or not the target system installation is to be set up as a trusted source.
3. If required, modify the fields to be reconciled for the **Xellerate User** resource object.

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

4.4 Transforming Data Reconciled Into Oracle Identity Manager

Note: If you are using Oracle Identity Manager release 9.1.0.x or release 11.1.1, then the procedure described in this section is optional.

This section discusses the `TransformLookupName` and `UseTransformMapping` attributes of the scheduled tasks for target resource reconciliation (SSH User Target Resource Reconciliation) and trusted source reconciliation (SSH User Trusted Source Reconciliation Task).

During reconciliation, you may want to transform the values of some target system fields before they are stored in Oracle Identity Manager. Appending a number at the end of the user ID is an example of a data transformation.

The `TransformLookupName` and `UseTransformMapping` attributes provide a method for implementing such transformations. To use these attributes

1. Identify the fields that you want to transform.
2. Create the Java file containing the code implementation of the transformation that must be performed during reconciliation. See [Appendix B, "Sample Transformation Class"](#) for information about creating a transformation class.
3. Note: Transformation will not work on the field `User`. `UserLogin`
4. Compile the Java file. While compiling the file, you must reference the `xliSSH.jar` file. See [Section 2.1, "Files and Directories on the Installation Media"](#) for information about the `xliSSH.jar` file.
5. Create JAR files containing the code to implement the required transformations on the fields.
6. If you are using Oracle Identity Manager release 9.1.0.x, then copy the JAR files into the following directory:

`OIM_HOME/xellerate/ScheduleTask`

7. If you are using Oracle Identity Manager release 11.1.1, then run the Oracle Identity Manager Upload JARs utility to post the JAR file to the Oracle Identity Manager database. This utility is copied into the following location when you install Oracle Identity Manager:

Note: Verify that the WL_HOME environment variable is set to the directory in which Oracle WebLogic Server is installed.

For Microsoft Windows:

`OIM_HOME/server/bin/UploadJars.bat`

For UNIX:

`OIM_HOME/server/bin/UploadJars.sh`

When you run the utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, URL of the Oracle Identity Manager host computer, context factory value, type of JAR file being uploaded, and the location from which the JAR file is to be uploaded. Specify 2 as the value of the JAR type.

See Also: *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for detailed information about the Upload JARs utility

8. In the Lookup.Reconciliation.TransformationMap lookup definition, add an entry for the transformation. In the Code Key column, enter the name of the reconciliation field (in the resource object) on which you want the transformation to be performed. In the Decode column, enter the name of the class file. For example:

Note: You can use this lookup definition for both UNIX SSH and SSH Telnet.

Code Key: `User.UserLogin`

Decode:

`com.thortech.xl.schedule.telnetssh.tasks.AppendTransformer`

See Also: *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for information about creating lookup definitions

9. While configuring the SSH User Target Resource Reconciliation Task and SSH User Trusted Source Reconciliation Task scheduled tasks by performing the procedure described in [Section 3.4, "Configuring Scheduled Tasks"](#):
 - Enter the name of the lookup definition as the value of the TransformLookupName attribute.
 - Enter Yes as the value of the UseTransformMapping attribute to specify that you want transformations to be applied. If you enter No as the value, then the transformations are not applied.

Testing and Troubleshooting

Note:

- Before running the test utility for 11.1.1, make sure that you have copied the required jar files (xliTelnet.jar or xliSSH.jar) into the folders JavaTasks and ScheduleTask, and sshfactory.jar is copied to ThirdParty folder.
 - If the SSHVersion of the target resource is client, then the connector may not work expectedly. In this case, you need to replace the sshfactory.jar file in Thirdparty with the latest version of sshafactory.jar file.
-
-

You can use the testing utility to identify the cause of problems associated with connecting to the target system and performing basic operations on the target system.

Before you use the testing utility, copy the files in the test directory on the installation media to one of the following directories:

- For Oracle Identity Manager release 9.1.0.x:
OIM_HOME/xellerate/XLIntegrations/SSH
- For Oracle Identity Manager release 11.1.1:
OIM_HOME/server/XLIntegrations/SSH

Set the required values in the config.properties file. This file is in one of the following directories:

- For Oracle Identity Manager release 9.1.0.x:
OIM_HOME/xellerate/XLIntegrations/SSH/config/config.properties
- For Oracle Identity Manager release 11.1.1:
OIM_HOME/server/XLIntegrations/SSH/config/config.properties

Use the information in the following table to modify the default attributes of the config.properties file.

| Attribute | Description | Default/Sample Value |
|-----------|---|----------------------|
| hostname | IP address of the target server on which user provisioning is to be performed | 10.1.1.114 |

| Attribute | Description | Default/Sample Value |
|-----------------------|---|---|
| shellPrompt | Default shell prompt of the target server: # for Solaris, Linux, and HP-UX \$ for AIX | # |
| port | Port at which the SSH server is listening | 22 |
| osType | Operating system type of the UNIX server Accepted values are SOLARIS, LINUX, HP-UX, and AIX. | SOLARIS |
| adminpassword | Admin user password | password1 |
| admin | UNIX server administrator credentials for the SSH server | root |
| action | Action to be tested The value can be one of the following: <ul style="list-style-type: none"> ■ CONNECT ■ CREATE ■ CHANGEPASSWORD ■ MODIFY ■ DELETE ■ DISABLE ■ ENABLE ■ ENABLETRUSTED (only for HP-UX trusted mode) | CREATE |
| userName | User attribute | jdoe |
| privateKey | Key for Public Key authentication | The value can be blank, or it can be the name and path of the private key file. |
| sudoFlag | Sudo Admin Mode flag | The value is YES for the SUDO Admin mode. It must be NO if the SUDO Admin mode is not used. |
| Max Retries | Number of times that the UNIX SSH connector should retry connecting to the target server if the connection fails | 2 |
| Delay | Delay (in milliseconds) before the connector attempts to retry connecting to the target system, in case the connection fails | 2000 |
| Timeout | Value of the timeout (in milliseconds) for the connection to the target server | 10000 |
| passwdMirrorFile Path | This parameter is used to specify the passwd mirror file path for reconciliation. | /etc/passwd1 |
| shadowMirrorFile Path | This parameter is used to specify the shadow mirror file path for reconciliation. | /etc/shadow1 |
| targetDateFormat | This parameter is used to specify the date format of the target UNIX computer. | MMddhhmmyy |
| expiryDateFormat | This parameter is used to specify the expiry date format of the target UNIX computer. | yyyy-MM-ddHH:mm:ss |

After you specify values in the config.properties file, perform one of the following steps:

-
- If you are using Oracle Identity Manager release 9.1.0.x, then run the following script:

For UNIX:

OIM_HOME/xellerate/XLIntegrations/SSH/scripts/SSH.sh

For Microsoft Windows:

OIM_HOME\xellerate\XLIntegrations\SSH\scripts\SSH.bat

- If you are using Oracle Identity Manager release 11.1.1, then run the following script:

For UNIX:

OIM_HOME/server/XLIntegrations/SSH/scripts/SSH.sh

For Microsoft Windows:

OIM_HOME\server\XLIntegrations\SSH\scripts\SSH.bat

Known Issues

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

- **Bug 6923238**

During provisioning, the data in the User Defined form fields must not contain the shell prompt character. Because there is a variation in shell prompt character depending on the target UNIX server, it should be checked in the target system.

A reconciliation run stops if the scheduled task code encounters target system user data containing the character or characters that are same as the shell prompt of the target system.

- **Bug 13362791**

Incremental reconciliation on a HPUX 11.31 target system in trusted mode fails in SUDO Admin mode.

A

Privileges Required for Performing Provisioning and Reconciliation

This appendix lists the privileges required for successful provisioning operations and reconciliation runs.

This appendix includes the following topics:

- [Appendix A.1, "Privileges Required for Running Commands on Non-AIX"](#)
- [Appendix A.2, "Privileges Required for Running Commands on HP-UX"](#)
- [Appendix A.3, "Privileges Required for Running Commands on AIX"](#)

A.1 Privileges Required for Running Commands on Non-AIX

Users must have privileges to run the following commands:

`usermod, useradd, userdel, passwd, chage`

In addition, the users must have execute permissions for the following commands:

`sed, cat, diff, sort, rm, grep, egrep, echo, /usr/bin/sh, /bin/sh`

Users must have read and write permissions on the `/etc`, `/home`, and `/tmp` directories.

A.2 Privileges Required for Running Commands on HP-UX

Users must have privileges to execute the `modprpw` command.

In addition, users must have read and write permissions on the `/etc`, `/home`, and `/tmp` directories.

A.3 Privileges Required for Running Commands on AIX

User must have privileges to execute the following commands:

`mkuser, chuser, rmuser, lsuser, /usr/bin/usermod, /usr/chuser`

In addition, the users must have execute permissions for the following commands:

`/usr/bin/bdiff, sh, cat, /usr/bin/sort, /usr/bin/rm, /usr/bin/grep, /bin/echo, /bin/sed, command.`

Users must have read and write permissions on the `/home`, `/ (root)`, and `/tmp` directories.

Sample Transformation Class

When you use this connector, you can transform reconciled data according to your requirements. This feature has been described in [Section 4.4, "Transforming Data Reconciled Into Oracle Identity Manager,"](#) along with the discussion on the `TransformLookupName` and `UseTransformMapping` attributes.

If you want to transform the value of a target system field that is fetched during reconciliation, then the first step is to implement the required transformation logic in a Java class. This transformation class must implement the `com.thortech.xl.schedule.telnetssh.tasks.AttributeTransformer` interface and the `transform` method.

The following is a sample transformation class:

```
package com.thortech.xl.schedule.telnetssh.tasks;
import java.util.Hashtable;
import com.thortech.util.logging.Logger;
import com.thortech.xl.integration.telnetssh.util.TelnetSSHConstants;
public class AppendTransformer implements AttributeTransformer
{
    /**
     * sample transformation method
     * it appends '123' to the key if present in the data to be reconciled
     * @param sKeyToBeTransformed - key to be transformed for example: Users.GECOS
     * @param htReconData - hash table of the data to be reconciled
     */
    public Hashtable transform(String sKeyToBeTransformed, Hashtable htReconData)
    {
        if(htReconData != null && sKeyToBeTransformed != null ) {
            if(htReconData.get(sKeyToBeTransformed) != null) {
                String sValue = (String)htReconData.get(sKeyToBeTransformed) ;
                sValue+="123";
                htReconData.put(sKeyToBeTransformed, sValue);
            }
        }
        return htReconData;
    }
}
```

The method defined in this class accepts the value of the field to be transformed, appends the string 123 to it, and returns the transformed string value.

Index

A

additional files, 1-2
Administrative and User Console, 2-27

C

certified components, 1-1
changing input locale, 2-26, 2-28
clearing server cache, 2-28
configuring
 connector for multiple installations of the target system, 4-7
 Oracle Identity Manager server, 2-26
configuring connector, 3-1
connector configuration, 3-1
connector files and directories
 description, 2-1
connector installer, 2-21
connector version number, determining, 2-3

D

defining
 IT resources, 2-24
determining version number of connector, 2-3

E

enabling logging, 2-30
external code files, 1-2

F

files
 additional, 1-2
 external code, 1-2
 See also XML files
files and directories of the connector
 See connector files and directories

G

globalization features, 1-3

I

input locale, changing, 2-26, 2-28
installing connector, 2-21
issues, 6-1
IT resources
 defining, 2-24
 parameters, 2-24

L

limitations, 6-1
logging enabling, 2-30
lookup field synchronization, 1-8
lookup fields, 1-8

M

multilanguage support, 1-3

O

Oracle Identity Manager Administrative and User Console, 2-27
Oracle Identity Manager server, configuring, 2-26

P

parameters of IT resources, 2-24
provisioning, 3-9
 direct provisioning, 3-10
 provisioning triggered by policy changes, 3-10
 request-based provisioning, 3-10
provisioning functions, 1-12

R

Reconciliation, 1-4
reconciliation
 module, 1-8
 scheduled tasks, 3-6
reconciliation rule
 target resource reconciliation, 1-10, 1-13

S

scheduled tasks, 3-6

- attributes, 3-4
- server cache, clearing, 2-28
- supported
 - releases of Oracle Identity Manager, 1-2
 - target systems, 1-2
- supported languages, 1-3

T

- target resource reconciliation
 - reconciliation action rules, 1-10, 1-14
 - reconciliation rule, 1-10, 1-13
- target system, multiple installations, 4-7
- target systems supported, 1-2
- testing, 5-1
- troubleshooting, 5-1

V

- version number of connector, determining, 2-3