HP OpenView Select Identity

Connector for Sun ONE Directory Server

Connector Version: 4.2

Installation and Configuration Guide

Document Release Date: March 2006

Software Release Date: March 2006

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

This product includes software developed by the Apache Software Foundation (http://www.apache.org/). Portions Copyright (c) 1999-2003 The Apache Software Foundation. All rights reserved.

Select Identity uses software from the Apache Jakarta Project including:

- Commons-beanutils
- Commons-collections
- Commons-logging
- Commons-digester
- Commons-httpclient
- Element Construction Set (ecs)
- Jakarta-poi
- Jakarta-regexp
- Logging Services (log4j)

Additional third party software used by Select Identity includes:

- JasperReports developed by SourceForge
- iText (for JasperReports) developed by SourceForge
- BeanShell
- Xalan from the Apache XML Project
- Xerces from the Apache XML Project
- Java API for XML Processing from the Apache XML Project
- SOAP developed by the Apache Software Foundation
- JavaMail from SUN Reference Implementation
- Java Secure Socket Extension (JSSE) from SUN Reference Implementation
- Java Cryptography Extension (JCE) from SUN Reference Implementation
- JavaBeans Activation Framework (JAF) from SUN Reference Implementation

- OpenSPML Toolkit from OpenSPML.org
- JGraph developed by JGraph
- Hibernate from Hibernate.org
- BouncyCastle engine for keystore management, bouncycastle.org

Trademark Notices

AMD and the AMD logo are trademarks of Advanced Micro Devices, Inc.

Intel and Pentium are trademarks or registered trademarks of Intel Corporation in the United States, other countries, or both.

JAVA™ is a US trademark of Sun Microsystems, Inc.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

Oracle® is a registered US trademark of Oracle Corporation, Redwood City, California

UNIX® is a registered trademark of The Open Group.

Support

Please visit the HP OpenView support web site at:

http://www.hp.com/managementsoftware/support

This web site provides contact information and details about the products, services, and support that HP OpenView offers.

HP OpenView online software support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valuable support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit enhancement requests online
- Download software patches
- Submit and track progress on support cases
- Manage a support contract
- Look up HP support contacts
- Review information about available services
- Enter discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and log in. Many also require a support contract.

To find more information about access levels, go to:

http://www.hp.com/managementsoftware/access_level

To register for an HP Passport ID, go to:

http://www.managementsoftware.hp.com/passport-registration.html

Contents

1 Introduction

This chapter gives an overview of the HP OpenView Select Identity connector for Sun ONE server. An HP OpenView Select Identity connector allows you to provision users and manage identities on Sun ONE server. At the end of this chapter, you will be able to know about:

- the benefits of HP OpenView Select Identity
- the role of a connector
- the connector for Sun ONE server

About HP OpenView Select Identity

HP OpenView Select Identity (OVSI) provides a new approach to identity management. It helps you manage the entire identity lifecycle of an enterprise application. By using OVSI, you can automate the process of provisioning and managing user accounts and access privileges across platforms, applications, and corporate boundaries. OVSI communicates with the enterprise information system through connectors, and automates the tasks of identity management. The enterprise information system, which is also referred to as **resource**, can be a database, a directory service, or an ERP package, among many others.

About Connectors

You can establish a connection between a resource and OVSI by using a connector. A connector is resource specific. It is installed on the system where OVSI is installed. The combination of OVSI and connector helps you perform a set of tasks on the resource to manage identity. A connector can be **unidirectional** or **bidirectional**. A unidirectional connector helps you manage identities from OVSI, but if any change takes place in resource, it cannot communicate that back to OVSI. On the other hand, a bidirectional connector can reflect the changes made on resource back to OVSI. This property of bidirectional connectors is known as **reverse synchronization**.

About Sun ONE LDAP Connector

The connector for Sun ONE server version 5.2 — hereafter referred to as Sun ONE LDAP connector — enables you to perform the following tasks on Sun ONE server by using OVSI.

- Add, update, and remove users

- Retrieve user attributes
- Enable and disable users
- Verify a user's existence
- Change user passwords
- Reset user passwords
- Retrieve all entitlements
- Retrieve a list of supported user attributes
- Grant and revoke entitlements to and from users, including the addition of users to multiple Operating Units
- Change log retrieval

A utility is also provided with this connector that detects changes made to Sun ONE 5.2 systems. The utility generates an SPML file that contains the changes and sends a reconciliation request to the Select Identity server.

➤ This connector can be used with OVSI version 4.0.

2 Installing the Connector

Sun ONE LDAP connector is packaged with the following files.

Table 1 Sun ONE LDAP Connector Files

Serial Number	File Name	Description
1.0	`TALDAPv3.rar`	It is the Resource Adapter Archive (RAR) file for the connector. It contains the connector binary files.
2.0	`schema.jar`	It contains the attribute mapping file (`SunOne40.xml`) for this system, which controls how the OVSI fields are mapped to Sun ONE server LDAP fields.

These files are located in the `LDAP Sun One` directory on the Select Identity Connector CD.

System Requirements

The Sun ONE LDAP connector is supported in the following environment:

Table 2 Platform Matrix for Sun ONE LDAP Connector

Select Identity Version	Application Server	Database
3.0.2	WebLogic 8.1.2 on Windows 2003	SQL Server 2000
	WebLogic 8.1.2 on Solaris 9	Oracle 9i
	WebLogic 8.1.2 on HP-UX 11i	Oracle 9i
	WebSphere 5.1.1 on Solaris 9	DB2 8.2 (or DB2 8.1 Service Pack 7)
3.3	WebLogic 8.1.4 on Windows 2003	SQL Server 2000

Table 2 Platform Matrix for Sun ONE LDAP Connector

Select Identity Version	Application Server	Database
3.3.1	WebLogic 8.1.4 on Windows 2003	SQL Server 2000
	WebSphere 5.1.1 on HP-UX 11i	Oracle 9i
4.0	The Sun ONE LDAP connector is supported on all the platform configurations of Select Identity 4.0.	

This connector is supported with Sun ONE Directory Servers 5.0 and Sun ONE Directory Servers 5.2 on Windows 2000 and Solaris 9.

Installation Procedure

The Sun ONE LDAP connector is internationalized and able to operate with languages that are supported by the Java Unicode specification. If you wish to use the connector on non-English platforms, make sure that the following prerequisites are met:

- The Select Identity server should be configured for internationalization. Refer to the *HP OpenView Select Identity Installation and Configuration Guide* for more information.
- The resource should be configured to support local language characters.

Perform the following tasks to install the Sun ONE LDAP connector on OVSI system.

1 Extract the Contents of Schema File

1 Deploy the Connector on Application Server

2 Install the Change Detection Utitlity

3 Configure the Connector with OVSIConfigure the Connector with OVSI

Extract the Contents of Schema File

Create a subdirectory in the OVSI home directory on OVSI system. Extract the contents of `schema.jar` file to this subdirectory. Ensure that the `CLASSPATH` environment variable in the application server startup script references this `Schema` subdirectory.

Deploy the Connector on Application Server

You must deploy the RAR file (`TALDAPv3.rar`) of the connector on an application server. Before deploying the RAR file, you must copy it to a local directory from the connector CD. Refer to *HP OpenView Select Identity Connector Deployment Guide* for more information on deploying a connector on an application server.

Install the Change Detection Utitlity

The Change Detection utility detects the changes made on the LDAP server and generates an SPML file for reconciliation with Select Identity. This utility works with Sun ONE 5.2. The following files are provided:

- `runagent.bat`
  A Windows batch file that runs the utility once based on the settings in the `resourceagent.properties` file. The JAVA_HOME variable is required to change according to the installation on the target host.
- `runagent.sh`
  A UNIX shell script that runs the utility once based on the settings in the `resourceagent.properties` file. The JAVA_HOME variable is required to change according to the installation on the target host.
- `ldapagent.jar`
  The utility executables.
- `ldapjdk.jar`
  The NetScape LDAP JDK executables.
- `resourceagent.properties`
  The configuration file.
- `fieldmapping.properties`
  The mapping files that provides a mapping between LDAP resource and Select Identity resource attribute names.

Also, keep the following in mind:

- The SPML file is user oriented. When the utility detects a group change on the LDAP server, the SPML file is created such that one group contains multiple users. Each user must be specified in an individual SPML request containing only one group.
- When all members of a group are removed, the Retro Plugin does not provide a list of user IDs that were removed. (The utility relies on the Retro Plugin to interact with the LDAP server.) Thus, a request to remove the empty group is not generated. To avoid this and workaround this limitation, it is recommended that you leave a user in a group or delete the least significant user from a group last.
- The password in the change log that is generated is encrypted. The utility cannot decode the password and does not provide the password field as part of the SPML file.

Installation and Configuration

Complete the following steps to install, configure, and run the utility on the LDAP server:

1 Enable the LDAP server to log changes by enabling the Retro ChangeLog Plugin:

  a Launch LDAP Directory Server.

  a Click the **Configuration** tab.

  a Select **Plugins**.

  a Locate the Retro Changelog Plugin and select **Enable plug-in**.

  b Save the changes.

2 Copy the utility's files from the `ldapagent` directory on the CD to a directory on the LDAP server. All of the files must reside in the same directory.

3. Make sure that the JRE (version 1.3.3+) is installed properly and included in the path on the LDAP server.
4. Edit the `runagent.bat` or `runagent.sh` file to specify the Java home directory on the server.
5. Edit the configuration file. The file is described in The resourceagent.properties File on page 12.
6. Run the `runagent.bat` or `runagent.sh` file. It is recomended that you execute the utility as a scheduled job.

The utility generates an SPML file that contains the user information that has changed. If the SPML file is formatted for Select Identity reconciliation through a file upload, upload the file using the Select Identity reconciliation page. Refer to the *HP OpenView Select Identity Administrator Guide* for more information. If the file is formatted for Select Identity reconciliation through Web Services, send the file to Select Identity as specified in the *HP OpenView Select Identity Web Service Developer Guide*.

The resourceagent.properties File

The following are the parameters provided by the `resourceagent.properties` file and required for reconciliation with Select Identity. All parameters are required. However, only those parameters that you can modify are explained here. *Do not modify parameters not listed here*.

- `debug`
  The audit flag, which enables you to generate debug statements. In general, set this property to **`false`**.
- `ldap_host`
  The name of the LDAP server.
- `ldap_port`
  The LDAP server's port.
- `ldap_user`
  The user name of the LDAP server; the utility will use this to log in and retrieve changes.
- `ldap_pass`
  The password of the LDAP server user.
- `s_filter`
  The filter DN for the LDAP server.
- `t_checkperiod`
  The frequency (in minutes) to check for changes in LDAP.
- `method`
  The method used to send the reconciliation request (the SPML file) to the Select Identity server. Based on this setting, the SPML will vary slightly. Specify **`fileupload`** or **`webservice`**.
- `resourcename`
  The Select Identity resource name for the LDAP server.
- `resource_key_field`
  The attribute that uniquely identifies the user on the resource.
- `si_username_field`
  The user name that will be used to log in to Select Identity.

- `si_ws_userid`
  The user name that enables the Web Service to log in to Select Identity. Set this property only is you specified **`webservice`** for the `method` property.
- si_ws_password
  The password of the user specified by `si_ws_userid`.
- `workingdir`
  The directory where the SPML files will be stored.
- `extension`
  The extension of the generated SPML files.

Configure the Connector with OVSI

After deploying the connector to an application server, you must configure it with OVSI. Before configuring the connector with OVSI, connect to the Lightweight Directory Access Protocol (LDAP) server by using an LDAP browser or any other utility. This can ensure that the LDAP resource is available and the correct parameters are known before deploying the resource in OVSI.

To configure the connector with OVSI, perform the following steps.

1. Add a new connector – Add a new connector on OVSI. Refer to *HP OpenView Select Identity Connector Deployment Guide* for information on adding a new connector. While adding the connector, under Current Resource Connectors section in Manage Connectors page, do the following:
   - In the Connector Name text box, specify a name for the connector.
   - In the Pool Name text box, enter **`eis/LDAPv3`**.
   - Under Mapper Available section, select **No**.
2. Add a resource — You must add a resource to OVSI that uses the newly added connector. Refer to *HP OpenView Select Identity Connector Deployment Guide* for the instructions to achieve this. While entering the resource parameters for Sun ONE LDAP connector, refer to the table below.

Table 3 Resource Configuration Parameters

Field Name	**Sample Values**	**Description**
Resource Name	local_sunONE	Name of the target resource.
Resource Type	Sun ONE	The connector that was deployed in step 1 on page 13.
Authoritative Source	*No*	Whether this resource is a system that is considered to be the authoritative source for user data in your environment. You must specify **No** because the connector cannot synchronize account data with the Select Identity server.
Associate to Group	*Selected*	Whether the system uses the concept of groups. For this LDAP connector, select this option.

Table 3 Resource Configuration Parameters

Field Name	Sample Values	Description
Access URL	ldap://136.168.1.20:389	URL to access the resource.
Suffix	*dc=qa, dc=hp, dc=com*	The domain(s) to which the users will be provisioned.
Login Name	cn=Administrator, cn=Users, dc=qa, dc=hp, dc=com	Login account with administrative privileges to add and delete users. This is required to log in to the resource.
Password	*Password123*	Password corresponding to the login account.
User Suffix	ou=people	Suffix of user's distinguished name. This is the location in the tree where the users will be provisioned.
User Object Class	*top, person, organizationalperson, user*	Object class for the users.
Group Suffix	ou=people	Suffix part of group's distinguished name. This is the location in the tree where the user groups will be provisioned. This parameter is optional (you can leave this field blank).
Group Object Class	*Top, group*	Object class of user groups.
Mapping File	`SunOne40.xml`	Location of the connector mapping file, which is used to map resource attributes to Select Identity attributes.
Cleanup Groups	*Selected*	Whether to delete the user's entitlements when the user is deleted from Select Identity.

3 Map the attributes — You must map the OVSI attributes to the attributes of the resource. Refer to *HP OpenView Select Identity Connector Deployment Guide* for information on mapping attributes. While mapping the attributes, refer to the following table for resource specific mapping information.

Table 4 Sun ONE LDAP Mapping Information

Select Identity Resource Attribute	Sun ONE LDAP Attribute	Description
UserName	uid	Key field on the resource
Password	userpassword	
Email	mail	
FirstName	givenname	
LastName	sn	
FirstName + LastName	cn	
Address 1	postalAddress	
Address 2	roomNumber	
City	l	
State	st	
Zip	postalCode	
Title	title	
Employee ID	employeenumber	
Business Phone	telephoneNumber	
Disable Function	Description=”disabled”	Marks the user as disabled
Enable Function	Description=”enabled”	Marks the user as enabled
mailHost	mailHost	Mail-related attributes
maildeliveryoption	mailDeliveryOption	
mailQuota	mailQuota	
nslicensedfor	nslicensedfor	
mailAlternateAddress	mailAlternateAddress	
mailForwardingAddress	mailForwardingAddress	
nscalorgunit2	nscalorgunit2	Calendar-related attributes
nscalpasswordrequired	nscalpasswordrequired	
nscalxitemid	nscalxitemid	
nscalflags	nscalflags	
nscallanguageid	nscallanguageid	
nscalsysopcanwrite password	nscalsysopcanwrite password	
nscaldefaultnotereminder	nscaldefaultnotereminder	

4 Associate the newly added resource to a service. Refer to the chapter *Service Studio* of *HP OpenView Select Identity Administrator Guide* for more information on service.

3 Uninstalling the Connector

If you want to uninstall a connector from OVSI, perform the following steps:

1. Remove all resource dependencies.
2. Delete the connector from OVSI.
3. Delete the connector from application server.

See *HP OpenView Select Identity Connector Deployment Guide* for more information on deleting the connector from OVSI and application server.