HP OpenView Select Identity

Connector for Linux (with BSH Scripts)

Software Version: 1.1

Installation and Configuration Guide

Document Release Date: July 2006
Software Release Date: July 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

This product includes software developed by Teodor Danciu http://jasperreports.sourceforge.net). Portions Copyright (C) 2001-2004 Teodor Danciu (teodord@users.sourceforge.net). All rights reserved.

Portions Copyright 1994-2004 Sun Microsystems, Inc. All Rights Reserved.

This product includes software developed by the Waveset Technologies, Inc. (www.waveset.com). Portions Copyright © 2003 Waveset Technologies, Inc. 6034 West Courtyard Drive, Suite 210, Austin, Texas 78730. All rights reserved.

Portions Copyright (c) 2001-2004, Gaudenz Alder. All rights reserved.

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

You can visit the HP OpenView Support web site at:

www.hp.com/managementsoftware/support

HP OpenView online support provides an efficient way to access interactive technical support tools. As a valued support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into 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 sign in. Many also require a support contract.

To find more information about access levels, go to:

www.hp.com/managementsoftware/access_level

To register for an HP Passport ID, go to:

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

Contents

1 Documentation Map

This chapter describes the organization of HP OpenView Select Identity connector documentation and provides necessary information on how to use the documentation set to install and configure the connectors.

Figure 1 illustrates the documentation map for HP OpenView Select Identity connector. For a list of available product documentation, refer to the table 1.

Figure 1 Documentation Map

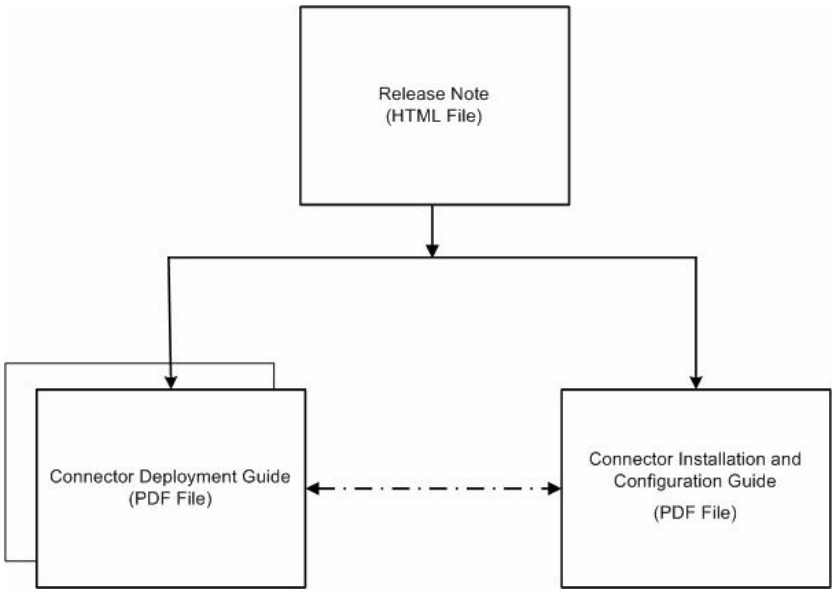

Table 1 Connector Documentation

Document Title and Filename	Contents	Location
Release Note `Linux_bsh Connector v1.1 Release Note.htm`	This file contains necessary information on new features of the connector, enhancements, known problems or limitations, and support information.	`/Docs/` subdirectory under the connector directory.
Connector Deployment Guide (for Select Identity 4.0/4.01.000) `connector_deploy_SI4.pdf`	Connector deployment guides provide detailed information on: • Deploying a connector on an application server. • Configuring a connector with Select Identity. Refer to these guides when you need generic information on connector installation.	`/Docs/` subdirectory under the connector directory.
Connector Installation and Configuration Guide `Linux_bsh_install.pdf`	Connector installation and configuration guide provides installation instructions for a specific connector. It contains resource specific configuration details.	`/Docs/` subdirectory under the connector directory.

2 Introduction

This chapter gives an overview of the HP OpenView Select Identity connector for Linux. An HP OpenView Select Identity connector enables you to provision users and manage identities on Linux 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 Linux.

About HP OpenView Select Identity

HP OpenView Select Identity provides a new approach to identity management. It helps you manage the entire identity lifecycle of an enterprise application. Select Identity helps you automate the process of provisioning and managing user accounts and access privileges across platforms, applications, and corporate boundaries. Select Identity 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 Select Identity by using a connector. A connector is resource specific. It is installed on the system where Select Identity is installed. The combination of Select Identity 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 Select Identity, but if any change takes place in resource, it cannot communicate that back to Select Identity. On the other hand, a bidirectional connector can reflect the changes made on resource back to Select Identity. This property of bidirectional connectors is known as **reverse synchronization**.

About the Linux Connector with BeanShell (BSH) Scripts

The Linux connector with BeanShell (BSH) scripts enables HP OpenView Select Identity to perform the following tasks on Linux server:

- Add, update, and remove users
- 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

The Linux connector with BSH is a unidirectional connector and pushes changes made to user data in the Select Identity database to a target server. The mapping file controls how Select Identity fields are mapped to Linux fields.

This connector can be used with Select Identity 4.01.000 and 4.0.

Overview of Installation Tasks

Before you start installing the connector, you must ensure that system requirements and all the installation prerequisites are met. Refer to the Table 2 for an overview of installation tasks.

Table 2 Organization of Tasks

Task Number	Task Name	Reference
1	Install the connector on the Select Identity server.	See Installing the Connector on page 11.
	— Meet the system requirements.	See System Requirements on page 11.
	— Extract the contents of the Schema file (file that contains the mapping files for the connector) to location on the Select Identity server.	See Extracting Contents of the Schema File on page 12.
	— Install the Resource Adapter Archive (RAR) of the connector on an application server.	See Installing the Connector RAR on page 12.
2	Configure the connector with the Select Identity server.	See Configuring the Connector with Select Identity on page 15.

3 Installing the Connector

This chapter elaborates the procedure to install Linux on Select Identity server and agent on Linux server. At the end of this chapter, you will know about

- Software requirements to install the Linux connector.
- Prerequisite conditions to install Linux connector.
- Procedure to install Linux connector.

Linux Connector Files

The Linux connector is packaged in the following files in the `Linux - BSH` directory on the Select Identity Connector CD:

Table 3 Linux Connector Files

Serial Number	File Name	Description
1	`UnixBshConnector.rar`	The Resource Adapter Archive (RAR) file contains the connector binaries.
2	`unixBshSchema.jar`	The Schema file contains the mapping files that contain attribute information of Linux.
3	`unix-bsh-scripts.zip`	The zip file contains the BSH scripts.

System Requirements

The Linux connector is supported in the following environment:

Table 4 Platform Matrix for the Linux Connector

Select Identity Version	Operating System, Application Server, and Database
4.0/4.01.000	The Linux connector is supported on all the platform configurations of Select Identity 4.0/4.01.000.

The connector can communicate with UNIX by using Secure Shel (SSH) or Telnet.

If you are using SSH method you must ensure that the SSH daemon is running on the Linux server to which you will provision users by using the connector.

The Linux connector with BSH is supported on Red Hat Linux AS 3.0.

Extracting Contents of the Schema File

The Schema file of the connector contains necessary mapping information to map resource attributes to Select Identity. Extract contents of the `unixBshSchema.jar` file to a directory that is in the application server `CLASSPATH`. Refer to the *HP OpenView Select Identity Connector Deployment Guide* for detailed instruction to extract contents of the Schema file.

Installing the Connector RAR

To install the RAR file of the connector (`UnixBshConnector.rar`) on the Select Identity server, you must copy the file to a local subdirectory on the Select Identity server, and then deploy on the application server. Refer to the *HP OpenView Select Identity Connector Deployment Guide* for detailed information on deploying a RAR file on an application server.

While deploying the RAR on WebSphere, enter the JNDI Pool Name as **`eis/UnixBshConnector`**.

Installing the Scripts on the Application Server

The Linux connector with BSH uses a Java-based scripting called BeanShell (**http://www.beanshell.org**). The BeanShell scripts control the interactions between the UNIX machine and the Select Identity server.

Copy the `unix-bsh-scripts.zip` file from the Select Identity connector CD and extract the scripts onto a local folder where Select Identity is installed. You must enter the location of this folder in Script Location field while entering the resource configuration parameters in Resource Access Information page.

Creating a Known Hosts File for Linux with SSH

If you use SSH, you must create a text file (for example, `known_hosts.txt`) that contains the names and public keys of all the trusted Linux machines to which you can provision users. You must provide the name of this file Ssh Known Hosts field while entering resource access parameters

One way of obtaining this information is to use PuTTY (`putty.exe`) to connect to the machine. When you connect to the Linux machine for the first time by using PuTTY, a pop up appears. This pop up displays the host key of the machine. You can connect to trusted Linux

machines individually from a Windows system by using PuTTY, capture this information, and put it in a text file, which can be used as known hosts file. PuTTY can be downloaded from **www.putty.nl/download**.

Sample contents of known_hosts.txt file:

```
16.73.17.88 ssh-rsa 1024 57993be4462bc4a536e8e58cad40f5ae
16.73.17.91 ssh-rsa 1024 664c2580121e2e06f702c195ae4e8885
```

4 Configuring the Connector with Select Identity

This chapter describes the procedure to configure the Linux connector with Select Identity. At the end of this chapter, you will know the procedure to configure the Linux connector with Select Identity.

Configuration Procedure

After you deploy the connector RAR on application server, you must configure the connector with Select Identity. Perform the following steps to configure the Linux connector with Select Identity.

1 Add a New Connector

2 Add a New Resource

3 Map Attributes

Add a New Connector

Add a new connector in Select Identity by using the user interface. While adding the connector, do the following:

- In the Connector Name text box, specify a name for the connector.
- In the Pool Name text box, enter **`eis/UnixBshConnector`**.
- Select No for the Mapper Available section.

Refer to the *HP OpenView Select Identity Connector Deployment Guide* for detailed information on adding a new connector in Select Identity.

Add a New Resource

Add a new resource in Select Identity that uses the newly added connector. Refer to the *HP OpenView Select Identity Connector Deployment Guide* for detailed instructions on adding a resource in Select Identity.

Refer to the following table while entering the parameters in the Basic Information and the Access Information pages:

Table 5 Resource Configuration Parameters

Field Name	Sample Values	Description
Resource Name	Linux_Server	Name given to the resource. If you enabled reverse synchronization, this must be the same as the value provided for the urn:trulog- ica:concero:2.0#resourceId attribute on the agent console.
Connector Name	Linux	The newly deployed connector.
Authoritative Source*	No	Whether this resource is a system that is considered to be the authoritative source for user data in your environment. Specify **No** if the connector is not enabled for reverse synchronization. Specify **Yes** if you want to add users through reverse synchronization. If the resource is not authoritative, the resource can only modify user entitlements during reverse synchronization.
Host Name	server.company.com	IP address or the hostname of the Linux machine.
User Name	ovsi (name must be less than 8 characters long)	Login account of the Linux machine.
User Password	Password123	Password for the user name ovsi.
Admin Password	rootPassword	Password of the super user that has the privilege to provision users on this system.
Unix Type	Linux	The type of the UNIX operating system.
Use ssh	True or False	Whether to use SSH while connecting to the resource. If you specify false, telnet is used.
Ssh known hosts	known_hosts.txt	This is needed only for SSH communication and indicates the name of a text file on the application server that contains the list of host and their host keys for the SSH protocol.
Port	22	The TCP/IP port to use to connect to the server. This is optional and if you use SSH, the default is 22. Otherwise, the default is 23.
Script Location	connectorScripts/ Linuxssh/	Location of the BSH scripts that are used by the connector. These are the ones extracted from `unix-bsh-scripts.zip` file.

Table 5 Resource Configuration Parameters

Field Name	Sample Values	Description
Timeout (sec)	300	Number of seconds to wait for a request to complete.
Max Retries	5	Number of times the request has to be retried upon a connection timeout given in the above parameter.
Mapping File	`UnixConnector.xml`	Location of the connector mapping file used to map resource attributes to Select Identity attributes.

Instead of creating an authoritative resource, you can create authoritative attributes (in the next step) for the attributes that will be synchronized. Entitlements are authoritative by default in a non-authoritative resource but other attributes are not.

Map Attributes

After successfully adding a resource for the Linux connector, you must map the resource attributes to Select Identity attributes. Refer to the *HP OpenView Select Identity Connector Deployment Guide* for information on mapping and creating attributes. While mapping attributes, refer to the following table for resource specific mapping information

Table 6 Linux Mapping Information

Select Identity Resource Attribute	Connector Attribute	Attribute on Linux Resource	Description
User Name	username	username (login argument)	UNIX logon name.
Password	password	password	Logon password
Full Name	comment	comment	Comment section in /etc/passwd
Directory	directory	home directory	User's home directory
Shell	shell	shell	UNIX logon shell
defaultgroup	defaultgroup	login primary group	Default group membership
Description**	description	description	A value from 1-100 alphanumeric characters in length.

After mapping the attributes, you can use the connector to create a service, or you can associate the connector with an existing service. Refer to the *Service Studio* chapter of the *HP OpenView Select Identity Administrator Guide* for information on Select Identity services.

5 Uninstalling the Connector

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

- Remove all resource dependencies.
- Delete the connector from Select Identity Connectors page.
- Delete the connector from application server.

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

A Understanding the Scripts

This connector uses a Java-based scripting engine called BeanShell (**http://www.beanshell.org**). The BeanShell scripts control the interactions between the Linux machine and the Select Identity server. There are some special variables and classes available to the BeanShell script when executing in the Linux connector. Each is described in this chapter.

The bean shell scripts control how the interaction with the UNIX system is to be made. You can customize the scripts if you want to customize the interaction for provisioning. The `comon.inc` script has all the common variables and methods. Other individual scripts have operation specific variables and methods.

Table 7 Scripts in unix-bsh-scripts.zip

Script Name	Description	Parameters Passed
`common.inc`	Commonly used variables and methods. Defines the UNIX prompt that the connector expects and the UNIX commands to be used for provisioning	
`dotest.bsh`	Test the initial connectivity to Linux, including login as regular user, super user and check for the existence of /etc/passwd file	`login, loginPassword, rootPassword, connection_timeout`
`finduser.bsh`	Checks for existence of user in Linux	`username, connection_timeout`
`adduser.bsh`	Adds a new user to Linux by preparing all the options needed for the UNIX command	`args` (semi-colon-separated name=value pairs), `username, connection_timeout`
`modifyuser.bsh`	Modify the comment, shell, primary or secondary groups of the user	`args` (semi-colon-separated name=value pairs), `username, connection_timeout`
`expirepasswd.bsh`	Locks the password entry for the user	`username, connection_timeout`
`changepasswd.bsh`	Changes the user's password	`username, password, connection_timeout`

Table 7 Scripts in unix-bsh-scripts.zip

Script Name	Description	Parameters Passed
changestatus.bsh	Change the status of the user	args (semi-colon-separated name=value pairs), username, connection_timeout
deleteuser.bsh	Delete the user	username, connection_timeout
findgroup.bsh	Get details of a UNIX group	group, connection_timeout
listgroups.bsh	Get all UNIX groups, Get groups of a specific user, Get users of a specific group	connection_timeout, username, connection_timeout, gname, connection_timeout
listusers.bsh	Get all users in system	connection_timeout