

HP SOA Systinet

Software Version: 2.50

Installation and Deployment

Document Release Date: May 2007
Software Release Date: May 2007



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.

Third-Party Web Sites

Mercury provides links to external third-party Web sites to help you find supplemental information. Site content and availability may change without notice. Mercury makes no representations or warranties whatsoever as to site content or availability.

Copyright Notices

Copyright © 1997-2007, Systinet Corporation. All Rights Reserved.

Trademark Notices

Java™ is a US trademark of Sun Microsystems, Inc. Microsoft®, Windows® and Windows XP® are U.S. registered trademarks of Microsoft Corporation. IBM®, AIX® and WebSphere® are trademarks or registered trademarks of International Business Machines Corporation in the United States and/or other countries. BEA® and WebLogic® are registered trademarks of BEA Systems, Inc.

Contents

| | |
|---|-----------|
| Welcome to This Guide. | 5 |
| How This Guide Is Organized. | 5 |
| Document Conventions. | 6 |
| Documentation Updates. | 7 |
| Support. | 8 |
| I Before Installing. | 11 |
| 1 Prerequisites. | 13 |
| Hardware. | 13 |
| Software. | 13 |
| 2 Supported Platforms. | 15 |
| Combined Servers and Operating Systems. | 15 |
| 3 Designing Your Deployment. | 17 |
| Development. | 17 |
| Production. | 17 |
| 4 Database Setup. | 19 |
| Setting Up DB2. | 19 |
| Setting Up Oracle. | 19 |
| II Installation Procedures. | 21 |
| 5 Installing Single Sign-On Service. | 23 |
| Running the SSO Installer. | 23 |
| Database Operations. | 26 |
| LDAP Accounts Integration. | 29 |

| | | |
|-----|---|----|
| 6 | Installing Reporting Service..... | 37 |
| 7 | Installing Platform..... | 41 |
| 8 | Installing Policy Manager..... | 45 |
| 9 | Using Silent Installation..... | 49 |
| III | After Installation..... | 51 |
| 10 | Configuring the Database for Full Text Searching..... | 53 |
| | Preparing DB2 for Full Text Search..... | 53 |
| | Preparing Oracle for Full Text Search..... | 55 |
| 11 | Launching SOA Systinet..... | 57 |
| 12 | Advanced JBoss Server Setup..... | 59 |
| | Establishing Trust..... | 59 |
| | JBoss JMS Configuration..... | 59 |
| | Setting Datasource MaxPoolSize..... | 60 |
| | JBoss Client Truststore..... | 60 |
| | JBoss Memory Allocation..... | 61 |
| | Configuring JBoss When SOA Systinet Uses Non-default Ports..... | 62 |
| | Encrypting Datasource Passwords..... | 62 |
| 13 | Importing SOA Systinet Registry Truststore..... | 63 |
| | Index..... | 65 |



Welcome to This Guide

Welcome to HP SOA Systinet, the foundation of Service Oriented Architecture, providing an enterprise with a single place to organize, understand, and manage information in its SOA. The standards-based architecture of SOA Systinet maximizes interoperability with other SOA products.

How This Guide Is Organized

HP SOA Systinet Installation Guide describes the prerequisites and process of installing HP SOA Systinet to your enterprise.

It contains the following parts:

- **Part I, “Before Installing”**. Preparing your enterprise system for HP SOA Systinet
- **Part II, “Installation Procedures”**. Detailed installation instructions
- **Part III, “After Installation”**. A guide to the likely next steps and where to find the information required

Document Conventions

The typographic conventions used in this document are:

| | |
|-----------------------------------|---|
| run.bat make | Script name or other executable command plus mandatory arguments. |
| <code>[--help]</code> | A command-line option. |
| <code>either or</code> | A choice of arguments. |
| <i>replace_value</i> | A command-line argument that should be replaced with an actual value. |
| <code>{arg1 arg2}</code> | A choice between two command-line arguments where one or the other is mandatory. |
| <code>rmdir /S /Q System32</code> | Operating system commands and other user input that you can type on the command line and press Enter to invoke. Items in <i>italics</i> should be replaced by actual values. |
| <code>C:\System.ini</code> | Filenames, directory names, paths and package names. |
| <code>a.append(b);</code> | Program source code. |
| <code>server.Version</code> | An inline Java or C++ class name. |
| <code>getVersion()</code> | An inline Java method name. |
| Shift-N | A combination of keystrokes. |
| Service View | A label, word or phrase in a GUI window, often clickable. |
| New->Service | Menu choice. |

Documentation Updates

This manual's title page contains the following identifying information:

- Software version number
- Document release date, which changes each time the document is updated
- Software release date, which indicates the release date of this version of the software

To check for recent updates, or to verify that you are using the most recent edition of a document, go to:

http://ovweb.external.hp.com/lpe/doc_serv/

Support

Mercury Product Support

You can obtain support information for products formerly produced by Mercury as follows:

- If you work with an HP Software Services Integrator (SVI) partner (www.hp.com/managementsoftware/svi_partner_list), contact your SVI agent.
- If you have an active HP Software support contract, visit the HP Software Support Web site and use the Self-Solve Knowledge Search to find answers to technical questions.
- For the latest information about support processes and tools available for products formerly produced by Mercury, we encourage you to visit the Mercury Customer Support Web site at: <http://support.mercury.com>.
- For the latest information about support processes and tools available for products formerly produced by Systinet, we encourage you to visit the Systinet Online Support Web site at: <http://www.systinet.com/support/index>.
- If you have additional questions, contact your HP Sales Representative.

HP Software Support

You can visit the HP Software Support Web site at:

www.hp.com/managementsoftware/services

HP Software 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

Part I. Before Installing

Before installing SOA Systinet, check that you meet system requirements, design your deployment and set up your database. These topics are covered in the following chapters:

- [Prerequisites on page 13](#)
- [Supported Platforms on page 15](#)
- [Designing Your Deployment on page 17](#)
- [Database Setup on page 19](#)

1 Prerequisites

The following hardware and software is required for running SOA Systinet:

Hardware

Hardware requirements vary depending on sizing and deployment type (see [Designing Your Deployment on page 17](#)). For a distributed, production environment, the suggested requirements are:

- For each physical node, an Intel Pentium Dual Core processor, 2 GB RAM, 1 GB free disk space and a network card that supports 1 Gb/sec.
- Network bandwidth of 1 Gb/sec or higher.

For development and evaluation purposes, SOA Systinet can run on a single machine, even on a notebook. The hardware requirements in this case are:

- Intel Pentium IV processor, 1 GB RAM, 1 - 2 GB free disk space and a network card that supports 100 Mb/sec.
- Network bandwidth of 100Mb/sec or higher.

Software

Each physical node must have the following software:

- A JDK and a J2EE application server from the list in [Supported Platforms on page 15](#). The application server must use this JDK.
- A `JAVA_HOME` environment variable set to point to the Java JDK used by the host J2EE application server.
- Access to a supported database from [Supported Platforms on page 15](#).

2 Supported Platforms

Combined Servers and Operating Systems

This table presents combinations of application servers, operating systems, JDKs and backend databases that were rigorously tested during the quality control phase of HP SOA Systinet development. Some combinations are supported even though they were not thoroughly tested.

We recommend only running this product on those sets which passed our quality control criteria.

| Operating System | J2EE Application Server | Java JDK | Relational Database |
|--|--------------------------------|---|------------------------------|
| Windows Server 2003, Red Hat Enterprise Linux 4.0 ES | JBoss 4.0.5 | Sun JDK 1.4.2_13 or later, 1.5.0_09 or later | Oracle 10g, DB2 version 9 |

3 Designing Your Deployment

HP SOA Systinet can be deployed on a wide range of scales. You have to design your deployment to match the scale of your network and your own J2EE application installation procedures. Broadly speaking, there are two types of deployment:

- **Development.** If you wish to evaluate the product, a simple deployment is possible on a single machine.
- **Production.** SOA Systinet used in a production environment is normally clustered and with its components installed on separate application servers.

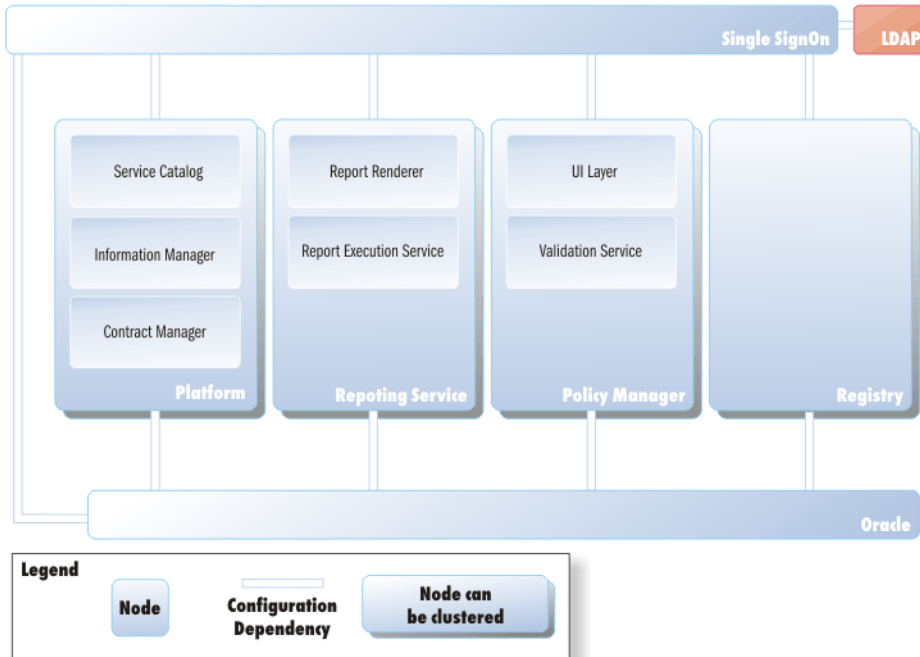
Development

If you are a developer, CIO or other IT manager who wants to learn the functions of SOA Systinet, this is the correct type of deployment for you. It should be on one machine and preferably on one J2EE server instance. We recommend using the installation wizard to deploy the product, following default settings.

Production

Deploying SOA Systinet for use in a production environment is a complex scenario. Different components of SOA Systinet are installed to different machines and are likely to be clustered as well. A schematic of such a deployment is shown in [Figure 1](#). We expect that if you are creating such a deployment, you already have a set of tools and procedures for deploying J2EE applications and managing relational databases.

Figure 1. Production Environment Deployment



When deploying SOA Systinet to a production environment you may need to install the SOA Systinet components non-interactively or install them using a reusable installation configuration. Our installation wizard generates an XML property file with the installer configuration.

Reporting, Platform and Policy Manager should share the same database.

4 Database Setup

The databases hosting SOA Systinet repository data need to be set up correctly before you install SOA Systinet components. The following sections address these issues:

- [Setting Up DB2 on page 19](#)
- [Setting Up Oracle on page 19](#)

Setting Up DB2

Configure the DB2 database as follows for use with SOA Systinet:

- Set up database to use UTF-8 Code Set.
- Install optional DB2 Net Search Extender if you plan to use SOA Systinet full text search feature.
- Make sure there is a *system temporary tablespace* with at least 16k page size. In order to create it, you will be required to create new bufferpool with minimum of 16k page size.

Setting Up Oracle

Configure the Oracle database as follows for use with SOA Systinet:

- Set up your database to use the Unicode (AL32UTF8) character set and national character set. UTF-8 is the preferred encoding.
- Include the "Oracle Text" extension when installing Oracle. Otherwise the SOA Systinet installation fails due to SOA Systinet's full text search feature. The "Oracle Text" extension is applied to Oracle by default. Only take care not to exclude it during installation.

Part II. Installation Procedures

There are several components of SOA Systinet. You need to install them in the following order, regardless of what type of deployment you have designed (see [Designing Your Deployment on page 17](#)):

- 1 Install the SSO service. See [Installing Single Sign-On Service on page 23](#).
- 2 Configure the SSO host J2EE server as necessary. See [Advanced JBoss Server Setup on page 59](#).
- 3 Launch the SSO service. See [Launching SOA Systinet on page 57](#).
- 4 Install HP SOA Systinet Reporting Service. See [Installing Reporting Service on page 37](#)
- 5 Configure the Reporting host J2EE server as necessary. See [Advanced JBoss Server Setup on page 59](#).
- 6 Launch the Reporting J2EE server. See [Launching SOA Systinet on page 57](#)
- 7 Install HP SOA Systinet Platform. See [Installing Platform on page 41](#)
- 8 Configure the Platform host J2EE server as necessary. See [Advanced JBoss Server Setup on page 59](#).
- 9 Launch the Platform. See [Launching SOA Systinet on page 57](#)
- 10 Install HP SOA Systinet Policy Manager. See [Installing Policy Manager on page 45](#)
- 11 Configure the Policy Manager host J2EE server as necessary. See [Advanced JBoss Server Setup on page 59](#).
- 12 Launch SOA Systinet. See [Launching SOA Systinet on page 57](#).

5 Installing Single Sign-On Service

This chapter contains the following sections describing the procedures of installing the Single Sign-On (SSO) Service:

[Running the SSO Installer on page 23](#). Executing the installer .jar file and the top-level procedure for installing SSO.

[Database Operations on page 26](#). The sub-procedure for setting up the SSO service's operations in the relational database. This sub-procedure is also used for installing HP SOA Systinet Platform and HP SOA Systinet Policy Manager.

[LDAP Accounts Integration on page 29](#). An explanation of the information you need to enter when you use LDAP backend accounts with the SSO service, including mapping between SOA Systinet and LDAP properties.

In the installation process, the SSO service must be running when you install the next component.


Running the SSO Installer

To install the SOA Systinet Single Sign-On (SSO) service:

- 1 Install and set up the target J2EE application server as described in [Advanced JBoss Server Setup on page 59](#).
- 2 Make sure the J2EE server is not running.
- 3 Execute the file `hp-soa-systinet-ss0-2.50.jar`, located on the installation CD or in your distribution directory. In Windows, you can double-click on it in an exploration window. On all operating systems, it launches with the command **java -jar hp-soa-systinet-ss0-2.50.jar**. Executing this file opens the installation wizard.

To see the command-line options, run **java -jar hp-soa-systinet-ss0-2.50.jar --help**. Use these options to set up and run a silent installation.

- 4 The welcome screen opens with hardware and software requirements. Read this carefully before clicking **Next**, which opens the license page.
- 5 Read and accept the license. Click **Next** to proceed to the **Installation Folder** page.
- 6 Type or browse the path to your SOA Systinet SSO server installation folder and click **Next**. The default path is C:\Program Files\Hewlett-Packard\Systinet\SSO. Each SOA Systinet component requires a separate installation subfolder. Click **Next** and the installer unpacks the distribution files to the chosen location.
- 7 Choose either advanced or default deployment. Default deployment performs all steps. If you choose advanced deployment, select which of the following steps to perform:
 - Database Setup, [Step 8](#)
 - Configuration Table Setup, [Step 9](#)
 - Endpoint Properties, [Step 10](#)
 - SSO setup, [Step 11](#)
 - Application Server Selection, see [Step 12](#)
 - Datasource Setup, [Step 13](#)
 - Deployment, [Step 14](#)
 - SSL Setup
- 8 Set up the database.
 - a Choose whether to create a new database or create a new schema in an existing database. Click **Next** to proceed. Please see [Database Operations on page 26](#) for details.
 - b Indicate which type of database you are using, such as Oracle or DB2.
 - c Type in database parameters. Please see [Table 1 on page 28](#) for details.

- d Type in or browse to the full paths of each JDBC driver .jar/.zip file to be installed to SSO, separated by commas.
 - e The installer now copies the JDBC drivers and verifies the connection to the database.
- 9 The installer now verifies that a configuration table is available.
- 10 Now specify the endpoint properties: Hostname, HTTP and HTTPS port numbers, whether or not to use HTTPS transport, and the web context. If you change any of these from the default values, you will have to enter these changes when installing the HP SOA Systinet Platform or HP SOA Systinet Policy Manager server.
-  If you change the port numbers from their default values, you also need to change the application server configuration to use these ports. See [Configuring JBoss When SOA Systinet Uses Non-default Ports](#) on page 62.
- If you change the Web Context property, also change the web context root in the `JBOSS_HOME/server/default/deploy/hp-soa-systinet-platform.ear/META-INF/application.xml`.
- 11 Set up the SSO parameters that will be used by other SOA Systinet servers to communicate with the SSO server.
- a Specify SOA Systinet administrator username and password. The default password is [changeit](#).
 - b Choose whether to keep user accounts on the database server or on an LDAP backend. If you choose the LDAP backend, enter LDAP service properties. The relationship between SOA Systinet and LDAP properties is described in [LDAP Accounts Integration](#) on page 29. Please also consult your LDAP administrator.
- 12 Indicate path and configuration type of JBoss server. JBoss should be in default configuration.
- 13 The installer now verifies the datasource.
- 14 The installer now verifies the application server connection.
- 15 The installer now verifies that the necessary client truststore is present for SSL communication.

- 16 The installer now performs the SSO server installation.
- 17 See [Launching SOA Systinet on page 57](#) about running the SSO service. If you are going to run the SSO service from the application server `run` script instead of `serverstart`, also see [Advanced JBoss Server Setup on page 59](#).

Database Operations

During installation you either create a new database or create schema in an existing empty database. After installation you can reconfigure the database with the Setup tool (see the Administration Guide). Using Setup, you can also drop a database or database schema or connect to an existing database with created schema.

- **Create Database.** For Oracle and DB2, the **Create Database** option does not create a new physical database. The process only creates a new tablespace in an existing database. Then it creates a database schema. For Oracle, a new user is also created with access to the new tablespace.
 - ▶ When creating a DB2 database, a new user must be created manually before installation. You also need a bufferpool with a 16k page size, a temporary tablespace using that bufferpool. The new user has to have a permission to access the temporary tablespace. Set this up with the DB2 Control Center.
- **Create schema (default).** Create tables and indexes in the default schema in existing database. Select this method if you have access to an existing empty database with the ability to create tables and indexes. This option is suitable when you do not know the administrator's credentials. We assume the administrator has already created a new database/user/tablespace for this option.
 - ▶ Since SSO is the very first step in the installation of whole SOA Systinet, **Create Database** now and later just repeat **Create Schema** option in the other installers.
- **Drop database.** The reverse of creating a database. Details depend on the type of database. Anything you did manually when creating the database, you must undo manually. You need an administrator's credentials.
- **Drop schema.** Drops all tables in the database but leave the empty database.

- **Configure database.** This gives you the option later in the installation of editing the configuration table. Use this method if the database already exists, for example, from a previous SOA Systinet installation of the same release number.

After selecting the operation, you need to type in database parameters. The parameters vary in some cases depending on the operation and the database type. [Table 1 on page 28](#) describes these parameters and any notes about their use.



If you install multiple SOA Systinet components to the same application server, set identical database parameters for each component.

Table 1. Database Setup Parameters

| Parameter | Description | Notes |
|---------------------------------|---|---|
| Database Server Address | The hostname or IP address where the database server is accessible. | For example, in the database connection string jdbc:oracle:thin:@dbhost42:1521:platform, the hostname is dbhost42. |
| Database Server Port | The connection port for the database. | For example, in the database connection string jdbc:oracle:thin:@dbhost42:1521:platform, the port number is 1521. |
| Existing Database Name | The name of the database. | For example, in the database connection string jdbc:oracle:thin:@dbhost42:1521:platform, the database name is platform. |
| Database Administrator Name | The user name and password of the administrator of the database. | Only required for the Create Database and Drop Database option. |
| Database Administrator Password | | |
| Database Tablespace Name | Name of the tablespace to be created for Create Database option. For DB2, this name is also used for Create Schema option . | With DB2, tablespace name is required for both Create database and Create schema options. With Oracle, it is only required to Create Database option. Tablespace name must not conflict with existing objects in the database during setup in the Create Database option. |
| Tablespace Datafile | The path to the tablespace datafile that is stored on the database host machine. | Only required to create a new database tablespace. Must not conflict with existing objects in the database. |

| Parameter | Description | Notes |
|------------------------------|--|---|
| (New) Database User | The name and password of a user who can create tables in his default schema, for Create Schema option. You must confirm a new user's password if creating a database. | If creating a new user, the name must not conflict with existing objects in the database. |
| (New) Database User Password | | |
| Confirm Password | | |

LDAP Accounts Integration

When installing the Single Sign-On (SSO) service (see [Installing Single Sign-On Service on page 23](#)), you can select to use accounts from an external LDAP server. This chapter describes how to integrate accounts from an LDAP server into SOA Systinet. It includes the following sections:

- [Automatic Service Discovery on page 30](#). A brief explanation of automatic service discovery and its implications
- [LDAP Service Properties on page 30](#). A list of JNDI properties of the LDAP server that must be known to the SSO service.
- [LDAP with a Single Search Base on page 31](#). One of two use scenarios, the other being LDAP with multiple search bases. The single search base scenario is very simple. There is only one LDAP server. All identities are stored under a single search base.
- [LDAP with Multiple Search Bases on page 33](#). One of two use scenarios, the other being LDAP with a single search base. In the multiple search base scenario there is also only one LDAP server, but it has multiple search bases mapped to a domain. The domain is a specified part of the user's login name (that is, DOMAIN/USERNAME). All users must specify the domain name in the login dialog. When managing accounts or groups, we recommend using the DOMAIN/USERNAME format for performance reasons. If no domain is set, searches are performed across all domains.
- [LDAP over SSL/TLS on page 34](#). Various scenarios for enabling communication over SSL between the SSO service and the LDAP server.



The Administrator account must not be stored in the LDAP. We strongly recommend that users stored in `account_list.xml` (by default, only administrator) should not be in LDAP. If you really need to have users from LDAP in the file `SSO_HOME/conf/system/account_list.xml`, delete password items from the file and change of all the accounts' properties according to LDAP. The

account_list.xml file contains a list of users that can be logged into SOA Systinet without connection to the database.



Sometimes SOA Systinet displays various warnings into logs. We recommend suppressing account/group LDAP integration warnings. To suppress these warnings, open the files `SSO_HOME/conf/system/directory.xml` and `SSO_HOME/conf/system/group_core.xml` and set all instances of the attribute `suppressWarnings` to `true`.

Automatic Service Discovery

The automatic discovery of LDAP servers means you do not have to hardwire the URL and port of the LDAP server. Instead you can use `ldap:///o=JNDITutorial,dc=example,dc=com` as a URL and the real URL will be deduced from the distinguished name `o=JNDITutorial,dc=example,dc=com`.

Automatic discovery of the LDAP service using the URL's distinguished name is supported only in Java 2 SDK, versions 1.4.1 and later, so be sure of the Java version you are using.

LDAP Service Properties

To integrate external accounts, during Single Sign-On (SSO) service installation select **LDAP** in the account provider panel.

SOA Systinet integration with LDAP uses a JNDI interface to connect to LDAP servers. (For more information, about the JNDI API, see <http://java.sun.com/products/jndi/tutorial/ldap/connect/create.html> and <http://java.sun.com/j2se/1.4.2/docs/guide/jndi/jndi-dns.html#URL>) The following JNDI properties must be known to the server:

| Property Name | Property Description | API Link |
|-------------------------------|---|---|
| Naming Provider URL | URL of the LDAP service | http://java.sun.com/j2se/1.4.-2/docs/api/javax/naming/Context.html#PROVIDER_URL |
| Initial Naming Factory | Java class for the initial naming factory | http://java.sun.com/j2se/1.4.-2/docs/api/javax/naming/Context.html#INITIAL_CONTEXT_FACTORY |
| Security Principal | The name of the security principal for anonymous read access to the directory service | http://java.sun.com/j2se/1.4.-2/docs/api/javax/naming/Context.html#SECURITY_PRINCIPAL |

| Property Name | Property Description | API Link |
|--------------------------|---|---|
| Password | Password of security principal | http://java.sun.com/j2se/1.4.2/docs/api/javax/naming/Context.html#SECURITY_CREDENTIALS |
| Security Protocol | Name of the security protocol. Default is "simple." | http://java.sun.com/j2se/1.4.2/docs/api/javax/naming/Context.html#SECURITY_PROTOCOL |

LDAP with a Single Search Base

The installation consists of the following steps:

- 1 Specify user/account search properties.
- 2 Map SOA Systinet user search properties to LDAP properties.
- 3 Specify group search properties.
- 4 Map SOA Systinet group search properties to LDAP properties.

Users and groups have the same properties. These properties are described in [Table 2 on page 32](#)

Table 2. SOA Systinet User and Group Search Properties

| Property | Description | |
|---------------|---|---|
| Search Filter | The notation of the search filter conforms to the LDAP search notation. You can specify the LDAP node property that matches the user account. | |
| Search Base | LDAP will be searched from this base including the current LDAP node and all possible child nodes. | |
| Search Scope | Object Scope | Only the search base node will be searched. |
| | One-level Scope | Only direct sub-nodes of the search base (entries one level below the search base) will be searched. The base entry is not included in the scope. |
| | Subtree Scope | The search base and all its sub-nodes will be searched |
| Results Limit | Number of items returned when searching LDAP. If more than this number of results are returned by an LDAP search an error occurs. | |

The following user account properties can be mapped from an LDAP server:

```

java.lang.String loginName
java.lang.String email
java.lang.String fullName
java.lang.String languageCode
java.lang.String password
java.lang.String description
java.lang.String businessName
java.lang.String phone
java.lang.String alternatePhone
java.lang.String address
java.lang.String city
java.lang.String stateProvince
java.lang.String country
java.lang.String zip
java.util.Date expiration
java.lang.Boolean expires
java.lang.Boolean external
java.lang.Boolean blocked
java.lang.Integer businessesLimit
java.lang.Integer servicesLimit
java.lang.Integer bindingsLimit
java.lang.Integer tModelsLimit


```




```
java.lang.Integer assertionsLimit
java.lang.Integer subscriptionsLimit
```

The following group properties can be mapped from an LDAP server:

```
java.lang.String name
java.lang.String owner
java.lang.String description
java.lang.Boolean privateGroup
java.lang.String member
```

 The platform account property **dn** specifies the LDAP distinguished name. The value depends on the LDAP vendor.

- On the Sun ONE Directory Server, the value is **entryDN**
- On Microsoft Active Directory, the value is **distinguishedName**

 User account properties that you specify when mapping to LDAP are treated as read-only in SOA Systinet.

If an optional property (such as email) does not exist in LDAP, then the property value is set according to the default account or group. The default account is specified in the config file `SSO_HOME/conf/system/account_core.xml`. The default group (groupInfo) is specified in the config file whose name is `group_core.xml`.

You can specify mapping between SOA Systinet group properties and LDAP properties. You can add rows by clicking **Add**. To edit an entry, double click on the value you wish to edit.

If a property (such as description) does not exist in LDAP then property value is set according to the default group.

LDAP with Multiple Search Bases

The installation consists of the following steps:

- 1 Specify the domain delimiter, domain prefix and postfix. These properties are used to dynamically specify domains.
- 2 Enable/Disable domains. In this step you can statically specify additional domains or disable domains.

- 3 Specify and map user/account search properties and group search properties as with single search bases. See [LDAP with a Single Search Base](#) on page 31.

Domain properties are described in [Table 3](#) on page 34.

Table 3. SOA Systinet Domain Properties

| Property | Description |
|-------------------------------|--|
| Domain Delimiter | Specifies the character that delimits domain and user name. |
| Domain Prefix, Domain Postfix | Allows the dynamic specification of domains. Domains are searched using the following pattern: {domain prefix}domain_name{domain postfix}{search base} where {} curly brackets indicate the value of the property whose name is contained in the brackets. |

LDAP over SSL/TLS

It is only a matter of configuration to set up LDAP over *SSL* (or *TLS*) with a directory server of your choice. We recommend that you first install SOA Systinet with a connection to LDAP that does not use SSL. You can then verify the configuration by logging in as a user defined in this directory before configuring use of SSL.

The configuration procedure assumes that you have already installed SOA Systinet with an LDAP account provider. SOA Systinet must not be running.

LDAP over SSL Without Client Authentication

In this case only LDAP server authentication is required. This is usually the case.

To change the LDAP configuration, run the Setup Tool and change **Naming Provider URL** to use the `ldaps` protocol and the port on which the directory server accepts SSL/TLS connections. An example of such a URL is `ldaps://ldap.test.com:636`.

Be sure that the hostname specified in the `java.naming.provider.url` property matches the name that is in the directory server certificate's subject common name (CN part of certificate's Subject). Otherwise you will get an exception during startup of SOA Systinet. It will inform you of a hostname verification error. The stacktrace contains the hostname that you must use.

LDAP over SSL With Mutual Authentication

SOA Systinet does not support LDAP over SSL with mutual authentication.

Ensuring Trust with the LDAP Server

The client that connects to the SSL/TLS server must trust the server certificate in order to establish communication with that server. The configuration of LDAPS described in [LDAP over SSL/TLS on page 34](#) inherits the default rule for establishing trust from JSSE (the Java implementation of SSL/TLS). This is based on trust stores.

The trust store for SOA Systinet is located in `SSO_HOME/conf/client.truststore` and the certificate for the LDAP server or its certification authority should be added to it.

To add the LDAP certificate to the SOA Systinet trust store, contact the administrator of the LDAP server and get the certificate of the server or the certificate of the authority that signed it, then Import the certificate into the SSO service trust store using the Java keytool:

```
keytool -import -trustcacerts -alias alias -file file -keystore keystore -storepass storepass
```

The parameters in the `keytool` command are as follows:

| Parameter | Description |
|------------------------|---|
| <code>alias</code> | A mandatory, unique alias for the certificate in the trust store; |
| <code>file</code> | The file containing the certificate (usually with <code>.crt</code> extension); |
| <code>keystore</code> | The SOA Systinet keystore file (<code>SSO_HOME/conf/client.truststore</code>). |
| <code>storepass</code> | A password designed to protect the keystore file from tampering. The password for the SOA Systinet keystore is the <i>SSL Certificate Password</i> set during installation. The default is changeit . |

6 Installing Reporting Service

After installing the SSO service (see [Installing Single Sign-On Service on page 23](#)), install the reporting service. The installation process is identical to reconfiguring an installed reporting service with the Setup tool (see the Administration Guide), which starts at [Step 7](#). To install the reporting service:

- 1 Install and set up the target J2EE application server as described in [Advanced JBoss Server Setup on page 59](#). You can also use the same J2EE server that hosts the SSO service.
- 2 Start the J2EE server hosting the SSO service. Use the `SSO_HOME/bin/serverstart` script.
- 3 Execute the file `hp-soa-systinet-reporting-2.50-standard.jar`, located on the installation CD or in your distribution directory. In Windows, you can double-click on it in an exploration window. On all operating systems, it launches with the command **java -jar hp-soa-systinet-reporting-2.50-standard.jar**. Executing this file opens the installation wizard.

To see the command-line options, run **java -jar hp-soa-systinet-reporting-2.50-standard.jar --help**. Use these options to set up and run a silent installation.

- 4 The welcome screen opens with hardware and software requirements. Read this carefully before clicking **Next**, which opens the license page.
- 5 Read and accept the license. Click **Next** to proceed to the **Installation Folder** page.
- 6 Type or browse the path to your SOA Systinet reporting server installation folder and click **Next**. The default path is `C:\Program Files\Hewlett-Packard\Systinet\Reporting`. Each SOA Systinet component requires a separate installation subfolder. Click **Next** and the installer unpacks the distribution files to the chosen location.
- 7 Choose either advanced or default deployment. Default deployment performs all steps. If you choose advanced deployment, select which of the following steps to perform:
 - Database Setup, [Step 8](#)

- Configuration Table Setup, [Step 9](#)
- Endpoint Properties, [Step 10](#)
- SSO Identity setup, [Step 11](#)
- Application of Reporting Service Extensions,
- Reporting Service Extensions Data Import, [Step 13](#)
- Application Server Properties, [Step 14](#)
- Datasource Setup, [Step 15](#)
- JMS Setup, [Step 16](#)
- Deployment, [Step 17](#)
- SSL Setup

8 Set up the database.

- a Choose whether to create a new database or create a new schema in an existing database. Click **Next** to proceed. Please see [Database Operations on page 26](#) for details.
- b Indicate which type of database you are using, such as Oracle or DB2.
- c Type in database parameters and click **Next**. Please see [Table 1 on page 28](#) for details.
- d Type in or browse to the full paths of each JDBC driver .jar/.zip file to be installed to Reporting, separated by commas.
- e The installer now copies the JDBC drivers and verifies the connection to the database.

9 The installer now verifies that a configuration table is available.

10 Now specify the endpoint properties: Hostname, HTTP and HTTPS port numbers, whether or not to use HTTPS transport, and the web context. If you change any of these from the default values, you

will have to enter these changes when installing the HP SOA Systinet Platform , HP SOA Systinet Policy Manager or reporting server.



If you change the port numbers from their default values, you also need to change the application server configuration to use these ports. See [Configuring JBoss When SOA Systinet Uses Non-default Ports on page 62](#).

If you change the Web Context property, also change the web context root in the `JBOSS_HOME/server/default/deploy/hp-soa-systinet-reporting.ear/META-INF/application.xml`.

11 Type in the following information:

| | |
|--------------------------------------|---|
| SSO Service URL | The URL of the SSO Service |
| Configuration Service Admin Name | Name and password of the SSO Service administrator. The default password is changeit . |
| Configuration Service Admin Password | |
| Identity Name | Arbitrary name of the identity for the reporting server you are creating on the SSO Server. Default is <code>reporting</code> . |
| Identity Password | The password of the SSO identity you are creating. The default password is changeit . |

- 12 (Advanced scenario and Setup tool only) Applies extensions from the `/extensions` directory to the `.ear` file. (This is not necessary in most cases when you first install the Reporting Server, because the default extensions are preapplied.)
- 13 The installer now imports extension data from the extension `.jar` files into the database.
- 14 Indicate path and configuration type of JBoss server. JBoss should be in `default` configuration.
- 15 The installer now verifies the datasource.
- 16 The installer now verifies JMS setup.
- 17 Installer now verifies application server properties.

- 18 The installer now verifies that the necessary client truststore is present for SSL communication.
- 19 The installer now performs the reporting server installation.
- 20 When installation is complete, run `SSO_HOME/bin/serverstop` and stop the SSO server. If you are going to run the reporting service from the application server `run` script instead of `serverstart`, see [Advanced JBoss Server Setup on page 59](#).

7 Installing Platform

After installing the SSO and reporting services (see [Installing Single Sign-On Service on page 23](#) and [Installing Reporting Service on page 37](#)), install the HP SOA Systinet Platform service. The installation process is identical to reconfiguring an installed HP SOA Systinet Platform service with the Setup tool (see the Administration Guide), which starts at [Step 7](#). To install or reconfigure the HP SOA Systinet Platform service:

- 1 Install and the target J2EE application server. You can use the same J2EE server that hosts the SSO and/or the reporting service.
- 2 Start the J2EE server hosting the SSO service. Use the `SSO_HOME/bin/serverstart` script.
- 3 Execute the file `hp-soa-systinet-platform-2.50-standard.jar`, located on the installation CD or in your distribution directory. In Windows, you can double-click on it in an exploration window. On all operating systems, it launches with the command `java -jar hp-soa-systinet-platform-2.50-standard.jar`. Executing this file opens the installation wizard.


To see the command-line options, run `java -jar hp-soa-systinet-platform-2.50-standard.jar --help`. Use these options to set up and run a silent installation.

- 4 The welcome screen opens with hardware and software requirements. Read this carefully before clicking **Next**, which opens the license page.
- 5 Read and accept the license. Click **Next** to proceed to the **Installation Folder** page.
- 6 Type or browse the path to your HP SOA Systinet Platform installation folder and click **Next**. The default path is `C:\Program Files\Hewlett-Packard\Systinet\Platform`. Each SOA Systinet component requires a separate installation subfolder. Click **Next** and the installer unpacks the distribution files to the chosen location.
- 7 Choose either advanced or default deployment. Default deployment performs all steps. If you choose advanced deployment, select which of the following steps to perform:

- Database Setup, [Step 8](#)
- Configuration Table Setup, [Step 9](#)
- Endpoint Properties, [Step 10](#)
- SSO Identity Setup, [Step 11](#)
- Repository Import, [Step 12](#)
- UI Perspective Import, [Step 13](#)
- Reporting Server Connection, [Step 14](#)
- Application Server Connection, [Step 15](#)
- Datasource Setup
- SSL Setup, [Step 17](#)
- JMS Setup, [Step 19](#)
- SMTP Properties
- Deployment, [Step 21](#)
- Client Package Creation

8 Set up the database.

- a Choose whether to create a new database, create a new schema in an existing database or configure an existing database and schema. If you are using the Setup tool, you can also drop a database or schema. Click **Next** to proceed. Please see [Database Operations on page 26](#) for details.
- b Select which type of database you are using, such as Oracle 10 or DB2.
- c Type in database parameters. Please see [Table 1 on page 28](#) for details.

- d Type in or browse to the full paths of each JDBC driver .jar/.zip file to be installed to Platform, separated by commas.
 - e The installer now copies the JDBC drivers and verifies the connection to the database.
- 9 The installer now verifies that a configuration table is available.
- 10 Now specify the endpoint properties: Hostname, HTTP and HTTPS port numbers, whether or not to use HTTPS transport, and the web context. These should be the same as the port numbers for the SSO service. Default values are the same for SSO, Policy Manager and HP SOA Systinet Platform servers.
-  If you change the port numbers from their default values, you also need to change the application server configuration to use these ports. See [Configuring JBoss When SOA Systinet Uses Non-default Ports](#) on page 62.

If you change the Web Context property, also change the web context root in the `JBOSS_HOME/server/default/deploy/hp-soa-systinet-platform.ear/META-INF/application.xml`.

- 11 Type in the following information:

| | |
|--------------------------------------|---|
| SSO Service URL | The URL of the SSO Service |
| Configuration Service Admin Name | Name and password of the SSO Service administrator. The default password is changeit . |
| Configuration Service Admin Password | |
| Identity Name | Arbitrary name of the identity for the HP SOA Systinet Platform server you are creating on the SSO Server. Default is <code>platform</code> . |
| Identity Password | The password of the SSO identity you are creating. The default password is changeit . |

- 12 Select to either install the default, initial bootstrap image or to import a custom image exported from another HP SOA Systinet Platform server.
- 13 The installer now verifies UI perspective importation.

- 14 In the **Reporting Server Properties** panel, select the SSO partner identity name of the reporting service component that you are linking to this platform component. The default partner identity name you want is **reporting**. You can also choose to use the secure SSO https URL .
- 15 Indicate path and configuration type of J2EE application server. JBoss should be in default configuration.
- 16 The installer now verifies the datasource.
- 17 The installer now verifies the existence of the necessary application server configuration files for SSL communication.
- 18 Now select the URL of the partner reporting service, or type a URL manually. If you select an https URL, HP SOA Systinet Platform communicates with the reporting service over SSL.
- 19 The installer now verifies JMS setup.
- 20 If you want SOA Systinet to send notifications over email, type in SMTP server authentication details. Mail service must be configured separately on the J2EE server.
- 21 Installer now verifies application server properties.
- 22 The installer now verifies the existence of necessary client package files.
- 23 The installer now installs HP SOA Systinet Platform. (Or the Setup tool now reconfigures HP SOA Systinet Platform.)
- 24 When installation is complete, run `SSO_HOME/bin/serverstop` and stop the SSO service. If you are going to run HP SOA Systinet Platform from the application server `run` script instead of `serverstart`, see [Advanced JBoss Server Setup on page 59](#).

8 Installing Policy Manager

After installing the SSO, reporting and HP SOA Systinet Platform services (see [Installing Single Sign-On Service on page 23](#), [Installing Reporting Service on page 37](#) and [Installing Platform on page 41](#)), install the HP SOA Systinet Policy Manager service. To install the HP SOA Systinet Policy Manager service:

- 1 Install and set up the target J2EE application server as described in [Advanced JBoss Server Setup on page 59](#). You can use the same J2EE server that hosts the SSO and/or the reporting and/or the HP SOA Systinet Platform service.
- 2 Start the J2EE server hosting the SSO service. Use the `SSO_HOME/bin/serverstart` script.
- 3 Execute the file `hp-soa-systinet-policymgr-2.50.jar`, located on the installation CD or in your distribution directory. In Windows, you can double-click on it in an exploration window. On all operating systems, it launches with the command `java -jar hp-soa-systinet-policymgr-2.50.jar`. Executing this file opens the installation wizard.

To see the command-line options, run `java -jar hp-soa-systinet-policymgr-2.50.jar --help`. Use these options to set up and run a silent installation.

- 4 The welcome screen opens with hardware and software requirements. Read this carefully before clicking **Next**, which opens the license page.
- 5 Read and accept the license. Click **Next** to proceed to the **Installation Folder** page.
- 6 Type or browse the path to your HP SOA Systinet Policy Manager installation folder and click **Next**. The default path is `C:\Program Files\Hewlett-Packard\Systinet\PolicyMgr`. Each SOA Systinet component requires a separate installation subfolder. Click **Next** and the installer unpacks the distribution files to the chosen location.
- 7 Choose either advanced or default deployment. Default deployment performs all steps. If you choose advanced deployment, select which of the following steps to perform:
 - Database Setup, [Step 8](#)

- Configuration Table Setup, [Step 9](#)
- Endpoint Properties, [Step 10](#)
- SSO Identity Setup, [Step 11](#)
- Application Server Selection, [Step 12](#)
- Datasource Setup, [Step 13](#)
- SSL Setup, [Step 14](#)
- JMS Setup, [Step 16](#)
- SMTP Properties, [Step 17](#)
- Deployment, [Step 18](#)
- Platform server properties, [Step 19](#)
- Reporting server properties, [Step 20](#)

8 Set up the database.

- a Choose whether to create a new database, create a new schema in an existing database or configure an existing database and schema. If you are using the Setup tool, you can also drop a database or schema. Click **Next** to proceed. Please see [Database Operations on page 26](#) for details.
- b Select which type of database you are using, such as Oracle 10 or DB2.
- c Type in database parameters. Please see [Table 1 on page 28](#) for details.
- d Type in or browse to the full paths of each JDBC driver .jar/.zip file to be installed to Policy Manager, separated by commas.
- e The installer now copies the JDBC drivers and verifies the connection to the database.

9 The installer now verifies that a configuration table is available.

- 10 Now specify the endpoint properties: Hostname, HTTP and HTTPS port numbers, whether or not to use HTTPS transport, and the web context. These should be the same as the port numbers for the SSO service. Default values are the same for SSO, Policy Manager and HP SOA Systinet Platform servers.

▶ If you change the port numbers from their default values, you also need to change the application server configuration to use these ports. See [Configuring JBoss When SOA Systinet Uses Non-default Ports on page 62](#).

If you change the Web Context property, also change the web context root in the `JBOSS_HOME/server/default/deploy/hp-soa-systinet-policymgr.ear/META-INF/application.xml`.

▶ Only the specific hostname entered here during installation can be used with HP SOA Systinet Policy Manager validation tools, either in the UI or on the command line. For example, if you enter the absolute address of your local machine as the hostname, you must use that absolute address and not "localhost" with validation tools.

If you change the Web Context property, also change the web context root in the `.ear` configuration.

- 11 Type in the following information:

| | |
|--------------------------------------|---|
| SSO Service URL | The URL of the SSO Service |
| Configuration Service Admin Name | Name and password of the SSO Service administrator. The default password is changeit . |
| Configuration Service Admin Password | |
| Identity Name | Arbitrary name of the identity for the HP SOA Systinet Policy Manager service you are creating on the SSO Server. Default is <code>policymgr</code> . |
| Identity Password | The password of the SSO identity you are creating. The default password is changeit . |

- 12 Indicate path and configuration type of J2EE application server. JBoss should be in `default` configuration.
- 13 The installer now verifies the datasource.

- 14 The installer now verifies the existence of the necessary application server configuration files for SSL communication.
- 15 The installer now validates that the extensions can be applied.
- 16 The installer now verifies JMS setup.
- 17 If you want the HP SOA Systinet Policy Manager component to send notifications over email, type in SMTP server authentication details. Mail service must be configured separately on the J2EE server.
- 18 The installer now verifies application server properties.
- 19 In the **Platform SSO Partner** panel, enter the SSO partner identity name of the platform component that you are linking to this HP SOA Systinet Policy Manager component. First select whether to choose from a list of known SSO identities or type in a partner name manually. Then, if you are selecting from the list, highlight the selected identity name. The default partner identity name you want is **platform**.
- 20 In the **Reporting Server Properties** panel, select the SSO partner identity name of the reporting service component that you are linking to this HP SOA Systinet Policy Manager component. The default partner identity name you want is **reporting**. You can also choose to use the secure SSO https URL .
- 21 The installer now installs HP SOA Systinet Policy Manager.
- 22 When installation is complete, run `SSO_HOME/bin/serverstop` and stop the SSO service. If you are going to run HP SOA Systinet Policy Manager from the application server run script instead of `serverstart`, see [Advanced JBoss Server Setup on page 59](#).

9 Using Silent Installation

You may need to install the SOA Systinet components non-interactively or install them using a reusable installation configuration. Our installation wizard generates an XML property file with the installer configuration. This file can be edited and can be used in non-interactive installation.

To generate a SOA Systinet installation configuration property file or install SOA Systinet non-interactively, launch the installation wizards with the **java -jar** command and various options. To see a list of all options and a brief description of each, run **java -jar *installer_jar_file* --help**. These options are the same as those for the Setup tool described in the Administration Utilities part of the Administrator Guide.

Part III. After Installation

The procedures described in After Installation are applied between installing each component in [Part II, “Installation Procedures”](#) as well as after installation is complete. These procedures are:

- [Configuring the Database for Full Text Searching on page 53](#)
- [Launching SOA Systinet on page 57](#)
- [Advanced JBoss Server Setup on page 59](#)

10 Configuring the Database for Full Text Searching

The SOA Systinet full text search is an optional feature based on relational database extensions. Enabling FTS in SOA Systinet is a two-fold process:

- 1 Enable FTS on the database server.
 - a Create an index for column "m_extension" from "ry_resource" table.
 - b Create an index for column "data" from "ry_resource" table.
 - c Schedule update of these indexes.

- 2 Activate FTS in the SOA Systinet UI.

This section describes the procedure for enabling FTS on these supported relational databases:

- [Preparing DB2 for Full Text Search on page 53](#)
- [Preparing Oracle for Full Text Search on page 55](#)

Ensure that your database server meets the system requirements described in the [Database Setup on page 19](#). See also SOA Systinet Configuration Options in the Administrator Guide.

Preparing DB2 for Full Text Search

In order to create indexes and schedule their update in DB2 you can use DB2 Net Search Extender. Connect to database using the same credentials used during installation. Please follow [Example 1 on page 54](#).

Example 1: Create Indexes for FTS and Schedule Synchronization in DB2

```
db2text START

#use sa user in this case
db2text ENABLE DATABASE FOR TEXT
CONNECT TO <database> USER sa
USING <password>

db2text CREATE INDEX idx_ry_resource_meta FOR TEXT ON
ry_resource(m_extensions)
CONNECT TO <database> USER <user>
USING <password>

db2text CREATE INDEX idx_ry_resource_data FOR TEXT ON
ry_resource(data)
CONNECT TO <database> USER <user>
USING <password>

#schedule a regular index update each day at midnight
db2text ALTER INDEX idx_ry_resource_meta FOR TEXT UPDATE FREQUENCY D(*) H(0) M(0)
CONNECT TO <database> USER <user>
USING <password>

db2text ALTER INDEX idx_ry_resource_data FOR TEXT UPDATE FREQUENCY D(*) H(0) M(0)
CONNECT TO <database> USER <user>
USING <password>
```

[Example 2 on page 55](#) shows commands how to update index manually.

Example 2: Synchronizing Indexes in DB2 Manually

```
db2text UPDATE INDEX idx_ry_resource_meta FOR TEXT
CONNECT TO <database> USER <user>
USING <password>
```

```
db2text UPDATE INDEX idx_ry_resource_data FOR TEXT
CONNECT TO <database> USER <user>
USING <password>
```

For more scheduling details see also DB2 Net Search Extender documentation.

Preparing Oracle for Full Text Search

In order to create indexes and schedule their update you can use Oracle **sqlplus** console. Connect to database using credentials used during installation.

[Example 3 on page 56](#) shows the procedure in commands. In addition, it also shows how to synchronize indexes every midnight. We assume the database user has permissions to create a scheduled job.

Example 3: Preparing Oracle For Full Text Search using the Scheduling Mechanism

```
sqlplus user/password@connect_identifier

DROP INDEX idx_ry_resource_meta;
DROP INDEX idx_ry_resource_data;

CREATE INDEX idx_ry_resource_meta ON ry_resource(m_extensions)
  INDEXTYPE IS CTXSYS.CONTEXT PARAMETERS
  ('FILTER CTXSYS.NULL_FILTER SECTION
  GROUP CTXSYS.HTML_SECTION_GROUP
  SYNC (EVERY "TRUNC(SYSDATE)+1")');

CREATE INDEX idx_ry_resource_data ON ry_resource(data)
  INDEXTYPE IS CTXSYS.CONTEXT PARAMETERS
  ('FILTER CTXSYS.NULL_FILTER SECTION
  GROUP CTXSYS.HTML_SECTION_GROUP
  SYNC (EVERY "TRUNC(SYSDATE)+1")');
```

See also Oracle documentation for details on how to create indexes at http://download-uk.oracle.com/docs/cd/B19306_01/text.102/b14218/csql.htm#i997677



Other synchronization techniques also may be used. Avoid performance issues by NOT implementing index synchronization ON COMMIT.

Example 4 on page 56 shows how to execute index synchronization manually.

Example 4: Synchronizing Indexes in Oracle Manually

```
sqlplus user/password@connect_identifier
CALL CTX_DDL.SYNC_INDEX('idx_ry_resource_meta', '2M');
CALL CTX_DDL.SYNC_INDEX('idx_ry_resource_data', '2M');
```

11 Launching SOA Systinet

The `bin` directory of every SOA Systinet component contains the scripts `serverstart`, `serverstop` and `env-jboss`. Running `serverstart` calls `env-jboss`, which gives JBoss access to the SOA Systinet client truststore and optimizes JBoss memory allocation. Using `serverstart` and `serverstop` is therefore the simplest way of launching and stopping SOA Systinet.

If all SOA Systinet components are installed to the same JBoss, it is only necessary to run one of the component `serverstart` scripts. It does not matter which one.

JBoss application server attempts to hot-deploy each ear file after every installation — no matter whether it is SSO, Reporting, Platform or Policy Manager. Don't rely on this hot-deployment feature especially in case you decided to host two J2EE servers on one JBoss installation. We highly recommend you to restart the particular JBoss node after installation ends.

In some cases, where the SOA Systinet components are widely distributed or clustered, when there are applications other than SOA Systinet on the same JBoss, or where JBoss is using non-default configuration or rmi ports, it may be preferable to use the native JBoss `run` scripts. In this case, you must first modify the `run` script of each host JBoss as described in [Advanced JBoss Server Setup on page 59](#). The contents of `serverstart` and `serverstop` are also useful guides in this case.

12 Advanced JBoss Server Setup

Before SOA Systinet is launched, `serverstart` script sets up and calls JBOSS run script so that JBOSS environment meets performance requirements good enough for evaluation or development environments. This chapter describes how you can also alter a number of application server settings due to specific deployments typical for production environments.

Establishing Trust

If the components of SOA Systinet—`sso`, `platform`, `polycmgr`—are installed to different instances or profiles of the application server, you need to set up trust between these instances/profiles/etc. Otherwise, SSL communication will fail. Please refer to your J2EE application server documentation for instructions on setting up trust.

JBoss JMS Configuration

JBoss uses JMS preconfigured for HSQLDB, which is sufficient for evaluation purposes.

For production deployments the JMS service should be configured to use Oracle or DB2.

To setup JBoss JMS to use Oracle DS:

- 1 Copy the Oracle JDBC driver `ojdbc14.jar` to `JBOSS_HOME/server/default/lib`.
- 2 Delete the `JBOSS_HOME/server/default/deploy/hsqldb-ds.xml` file.
- 3 Copy `JBOSS_HOME/docs/examples/jca/oracle-ds.xml` to `JBOSS_HOME/server/default/deploy` and update the `connection-url`, `user-name`, `password` and `jndi-name` (set `DefaultDS`) elements.
- 4 Set the `max-pool-size` element to the maximum number of parallel served execution requests (< than the number of parallel served users) plus the number of parallel processed executions (~5).
- 5 Delete the `JBOSS_HOME/server/default/deploy/jms/hsqldb-jdbc2-service.xml` file.

- 6 Copy `JBOSS_HOME/docs/examples/jms/oracle-jdbc2-service.xml` into `jboss-4.0.5.GA/server/default/deploy/jms` and replace OracleDS by DefaultDS in this file.
- 7 Set the `max-pool-size` element to maximum number of parallel served execution requests in the `JBOSS_HOME/server/default/deploy/jms/jms-ds.xml` file.
- 8 Set the `maxThreads` attribute to the maximum number of parallel served users in the `JBOSS_HOME/server/default/deploy/jbossweb-tomcat55.sar/server.xml` file.

Setting Datasource MaxPoolSize

The default JBoss datasource Maximum Pool Size is not adequate for a production environment. The default MaxPoolSize based on default Oracle configuration is only 15, for example. The Maximum Pool Size should be at least 1/4 the number of parallel requests that you require to be handled simultaneously. To increase Maximum Pool Size:

- 1 Open `JBOSS_HOME/server/default/deploy/hpssoasystinet-xa-ds.xml` in an editor.
- 2 Edit the element `max-pool-size`. Its value should be at least 1/4 of the number of simultaneous parallel requests.
- 3 Save your changes and exit.

JBoss Client Truststore

For SSL communication, each JBoss server must access the client truststore of a SOA Systinet component that is deployed to it. If more than one component is deployed to the same JBoss, that JBoss only needs to access one of the component truststores, because all truststores contain the same CA certificate.



If you intend to launch SOA Systinet from the `SOA_SYSTINET_COMPONENT_HOME/bin/serverstart` and `serverstop` scripts instead of the JBoss `run` script, it is not necessary to set truststore access, as `serverstart` sets it automatically by calling `env-jboss`. However, `serverstart` and `serverstop` may not work with complex or non-default JBoss configurations. It is still useful to refer to the contents of these scripts when modifying `JBOSS_HOME/bin/run.bat`.

After installing SOA Systinet components to one or more JBoss servers as described in [Part II, “Installation Procedures”](#), give each JBoss access to SOA Systinet client truststores. For each JBoss server:

1 Open the `JBOSS_HOME/bin/run` script in an editor.

2 Insert these lines anywhere in the script:

```
-Djavax.net.ssl.trustStore=SSO_SYSTINET_COMPONENT_HOME\conf\client.truststore  
-Djavax.net.ssl.trustStorePassword=changeit
```

3 Save and exit the script.

JBoss Memory Allocation

Increase the maximum memory limit on the JBoss server to optimize SOA Systinet performance. This is suggested for JBoss servers hosting SSO, Policy Manager and/or Platform servers. It is not necessary for the Reporting host server.



If you intend to launch SOA Systinet from the `SOA_SYSTINET_COMPONENT_HOME/bin/serverstart` scripts instead of the JBoss `run` script, you do not need to set the max memory limit, as `serverstart` sets these properties. However, `serverstart` and `serverstop` may not work with complex or non-default JBoss configurations. It is still useful to refer to the contents of these scripts when modifying `JBOSS_HOME/bin/run.bat`.

Increase the maximum memory limit to 1GB and set the `MaxPermSize` to 256m in these steps:

1 Open the `run` script in the `bin` directory of the JBoss server.

2 Find the following lines:

```
rem JVM memory allocation pool parameters. Modify as appropriate.  
set JAVA_OPTS=%JAVA_OPTS% -Xms128m...
```

3 Edit the lines to read:

```
rem JVM memory allocation pool parameters. Modify as appropriate.  
set JAVA_OPTS=%JAVA_OPTS% -Xms128m -Xmx1024m -XX:MaxPermSize=256m
```

4 Save and exit the script.

Configuring JBoss When SOA Systinet Uses Non-default Ports

SOA Systinet by default uses ports 8080 and 8443. If you select a different set of ports during installation, you have to configure JBoss after installation to use these ports. If you are using port numbers that are higher than the default, the easiest way is to edit the JBoss configuration files as follows:

- 1 Open `JBOSS_HOME\server\default\conf\jboss-service.xml` in an editor.
- 2 Search for the string `ports-01`. The search function takes you to the following commented-out MBean:

```
<!-- (comment text).....
<mbean code="org.jboss.services.binding.ServiceBindingManager"
      name="jboss.system:service=ServiceBindingManager">
  <attribute name="ServerName">ports-01</attribute>
  <attribute name="StoreURL">
    ${jboss.home.url}/docs/examples/binding-manager/sample-bindings.xml
  </attribute>
  <attribute name="StoreFactoryClassName">
    org.jboss.services.binding.XMLServicesStoreFactory
  </attribute>
</mbean>
-->
```

- 3 Remove the wrapping comment tag and comment text from the MBean.
- 4 Set the value of the element `<attribute name="ServerName">ports-01</attribute>`. This value represents the factors of 100 by which additional port numbers above the default value are enabled. For example, if you leave the value at `ports-01`, ports 8180, 8280, 8380... are enabled. If you set the value at `ports-02`, the additional ports are 8280, 8480, 8680...
- 5 Save your changes and exit the editor.

Encrypting Datasource Passwords

The SOA Systinet installer and Setup tool creates a JBoss datasource definition with the password in open (readable) form. For instructions on encrypting the datasource passwords, see [the JBoss Wiki](http://wiki.jboss.org/wiki/Wiki.jsp?page=EncryptingDataSourcePasswords) [<http://wiki.jboss.org/wiki/Wiki.jsp?page=EncryptingDataSourcePasswords>].

13 Importing SOA Systinet Registry Truststore

If you are using SOA Systinet in conjunction with HP SOA Systinet Registry and plan to import artifacts and taxonomies, you need to import the HP SOA Systinet Registry truststore. To import the truststore, run this command:

```
keytool -import -alias registry -file "C:\Program Files\Hewlett-Packard\Systinet\registry\doc\registry.crt" -keystore "C:\Program Files\Hewlett-Packard\Systinet\platform\conf\client.truststore"
```

In the syntax of that command it is assumed that SOA Systinet and HP SOA Systinet Registry are installed to the default locations. If they are installed to different locations, modify the command accordingly. It is also assumed that `JAVA_HOME/bin` is on your path, in which case it does not matter where you run the command from.

Index

A

- Active directory
 - installation, 29
- application servers
 - recommended OS, 15
- authentication
 - LDAP, 34

C

- certificate
 - LDAP, 35

D

- database
 - creation, 26
 - operations, 26
 - schema, 26
 - tablespace, 26

E

- external accounts, 29
 - LDAP, 29

H

- hostname verification error
 - LDAP, 34

I

- installation

- Active directory, 29
 - external accounts, 29
 - LDAP, 29
 - reporting server, 37
 - SSO, 23

J

- J2EE platforms
 - with recommended OS, 15
- JSSE
 - LDAP, 35

K

- keytool
 - LDAP server trust, 35

L

- LDAP
 - installation, 29
 - SSL, 34
 - TLS, 34
- ldaps, 34

O

- operating system
 - recommended application servers, 15

R

- reporting server
 - installation, 37

S

- SSL
 - LDAP, 34
- supported platforms
 - recommended application servers and OS, 15

system property
LDAP, 35

T

trust
LDAP, 35