Oracle ® Entitlements Server 10*g* (10.1.4.3)

Securing OES Production Environments

September 2008

ORACLE

Securing OES Production Environments, Oracle ® Entitlements Server 10*g* (10.1.4.3)

CHAPTER 1

Introduction

This section describes the contents and organization of this guide.

Note: Oracle Entitlements Server was previously known as BEA Aqualogic Enterprise Security. Some items, such as schema objects, paths, and so on may still use the term “ALES."

Document Scope and Audience

This document is a resource for system administrators and others who deploy Oracle Entitlements Server in production environments. It contains information about security practices that should be considered when moving OES from a development to a production system.

Guide to this Document

This document is organized as follows:

- “Configuring SSL” on page 2-1 describes how to implement SSL for connections between Oracle Entitlements Server components.
- “Configuring SSL in the Web Services SSM” on page 3-1 describes how to enable one-way SSL between a Web Services SSM and its client.

- "Configuring SSL in the RMI SSM" on page 4-1 describes how to enable one-way SSL between a RMI SSM and a remote SSM.
- "Resetting the Administrator Password" on page 5-1 describes how to change the OES administrator password.
- "Additional Recommendations" on page 6-1 provides information about other security practices.

Related Documentation

For information about other aspects of Oracle Entitlements Server, see the following documents:

- *Introduction to Oracle Entitlements Server* provides overview, conceptual, and architectural information of this product.
- *Administration Server Installation Guide* provides instructions for installing the Administration Server on supported platforms.
- *SSM Installation and Configuration Guide* provides instructions for setting up SSMs.
- *Getting Started with Oracle Entitlements Server* provides a number of tutorials that show how to use the Entitlements Administration Application to secure application resources.
- *Policy Managers Guide d*efines the policy model and describes how to manage, generate, import, and export policy data.
- *Programming Security for Java Applications* describes how to implement security in Java applications. It includes descriptions of the security service APIs and provides programming instructions.
- *Developing Security Providers* provides security vendors, administrators, and application developers with information needed to develop custom security providers.
- For API documentation in Javadoc format, see the documentation home page.

CHAPTER 2

Configuring SSL

OES uses SSL for communications between the Administration Server, remote OES components, and external clients. Installation of OES includes demonstration certificates that can be used get the system up and running in non-production environments.

This document describes how OES uses SSL and provides instructions for replacing the demonstration certificates with those signed by a recognized Certificate Authority. It contains the following topics:

OES Component Connections

OES uses one-way or two-way SSL as follows:

- **Administration Server and Remote OES Components**

  Once the enrollment process is performed on a remote machine, all OES components on that machine (SCM, SSM) are bound into the internal OES trust structure based on the internal CA, residing on the Administration Server. All communication with the server is performed using two-way SSL.

- **SSM Enrollment Clients**

  A single set of keys located in *BEA_HOME*\ales32-shared\keys is used by all OES components on that machine. When enrollment is initiated on a remote machine, communication between the enrollment client and the Administration Server is one-way SSL.

  NOTE: For step-by-step enrollment instructions, see the SSM Installation and Configuration Guide.

  If enrollment is performed in demo mode, the Administration Server presents its certificate signed by the Demo ALES CA that is supplied with the installation that enrollment clients are configured to trust. In secure mode, the client verifies the CA certificate against its list of trusted certificate authorities in $JAVA_HOME/lib/security/cacerts.

- **Internet Explorer Browsers**

  One-way SSL is used for browser connections with the Administration Console or the Entitlements Management Tool. When a browser client initiates the connection, the Administration Server sends the client its certificate. If the CA authority that signed the certificate of Administration web server (WebLogic or Tomcat) is in the browser's trust store, the browser proceeds to establish the one-way SSL connection. If not, the browser issues a warning that allows the user to trust the certificate.

NOTE: The OES administration tools themselves use two-way SSL when communicating with other internal OES components.

- **External Business Logic Manager (BLM) Clients**

  Instead of using the provided Java wrapper for the BLM SOAP interface, external clients may directly access BLM interfaces.

Demo Keystores and Certificates

Upon installation, two keystores containing demo certificates are used to establish trust between the Administration Server and clients:

– **`Webserver.jks`**—The Administration Server uses `BEA_HOME\ales32-shared\keys\webserver.jks`. This keystore contains a demonstration private key for the Administration Server, the server's identity in a public certificate that is signed by the Demo ALES CA, and a public certificate for the internal CA itself.

– **DemoTrust.jks**— SSM enrollment clients use this keystore when enrolling in demo mode. Because this keystore also contains the Demo CA certificate, clients will trust the Administration Server. This keystore is located in the BEA_HOME\ales32-shared\keys directory.

Replacing the Demo Certificates

For production environments, first configure the Administration Server must be configured to use a keystore containing its private key and corresponding certificate signed by a well-know certificate authority. After this, SSMs can be bound into internal OES 2-way SSL framework by enrolling in secure mode.

Note: Some certificates issued by CA authorities do not strictly comply with Certicom's Internet X.509 Public Key Infrastructure standard. To use these certificates, you must disable constraints extension checking by adding information to the the enrollment and unenrollment scripts. For instructions, see "Certificates" on page 3-6 of the *SSM Installation and Configuration Guide*.

Clients enrolling in secure mode will verify the CA certificate against its list of trusted certificate authorities in $JAVA_HOME/lib/security/cacerts and determine that it was signed by a trusted CA by checking for its presence in the cacerts keystore. If the certificate authority is not in the list of trusted CAs, the CA's certificate must be imported into cacerts.

1. Rename BEA_HOME\ales32-shared\keys\webserver.jks to demowebserver.jks or a similar name.

   Note: This allows you to create the new keystore named webserver.jks. Doing so will minimize modifications that must be made to existing Administration Server config files.

2. Using the Keytool utility, enter:

   ```
   keytool -genkey -alias ales-webserver -keyalg RSA -keystore Webserver.jks
   ```

3. When prompted, enter the keystore password and other information about the certificate, (company, contact name, etc.).

4. When prompted for the key password, enter the same password used for the keystore itself. This can be accomplished by pressing ENTER.

5. Create a Certificate Signing Request (CSR) as shown below and submit it to the Certificate Authority:

   ```
   keytool -certreq -alias ales-webserver -keyalg RSA -file certreq.csr
   -keystore Webserver.jks
   ```

6. When you receive the signed certificate, download a chain certificate from the CA.
7. Import the chain certificate and new CA certificate into the keystore:

   `keytool -import -alias AlesCA -keystore Webserver.jks -trustcacerts -file <chain_certificate_filename>`

   `keytool -import -alias ales-webserver -keystore Webserver.jks -trustcacerts -file <certificate_filename>`
8. Copy the new `Webserver.jks` to the `BEA_HOME\ales32-shared\keys` directory.
9. Modify the server's configuration file as described in the table below.

Container Type	Instructions
WebLogic Server	In `BEA_HOME/asiDomain/config.xml`, replace the existing `<server-private-key-pass-phrase-encrypted>` value with the encrypted value of the keystore password used when new `webserver.jks` keystore was created (see step 3 on page 2-4). To encrypt the password, you may use the `encrypt` tool provided with WebLogic Server.
Tomcat	Modify `TOMCAT_HOME/config/server.xml` as follows: Add `keystorePass=<encrypted_keystore_password>` next to the `keystoreFile` attribute.

10. Restart the Administration Server.

Configuring BLM Clients for One-Way SSL

SSL connections between BLM clients and the BLM server are two-way SSL by default. You can change this to one-way SSL using the following steps:

1. Open `BEA_HOME/ales32-admin/config/WLESblm.properties` in an editor and add the following parameter to the bottom of the file:

   `BLM.sslType=one-way`

   Note: If you are using the default properties file, this is already entered as a commented line at the bottom of the file. Simply remove the comment symbol (#).
2. Restart the server using the following command:

```
BEA_HOME/ales32-admin/bin/WLESadmin.sh restart
```

This is all that is required if the BLM client is on the same machine and the server. You do not need to perform the remaining steps.

3. If the BLM client is on a separate machine, make a copy of `trust.jks` in the `BEA_HOME/ales32-shared/keys` directory and move the copy to an appropriate directory on the BLM client machine.
4. On the BLM client machine, add the following parameter to the BLM client application:

   ```
   -Dwles.ssl.trustedCAKeyStore=/<directory_name>/trust.jks
   ```

   where

   <`directory_name`>—name of the directory containing `trust.jks`.

   Note: No keys are distributed with `trust.jks`. It contains only the CA public certificate.

SSL Diagnosis Utility

The SSL diagnosis tool in a SSM's `ales32-shared/bin` directory can be used to troubleshoot SSL connectivity problems between the SSM and the administration server. The tool checks the SSM's SSL configuration and shows detailed handshake information.

To use the tool:

1. Make sure the Administration Server is running and using the following debugging settings. If necessary, modify the settings and restart the server.

Server	File	Setting

WebLogic	WLESWebLogic.conf	Add or modify these settings in the **# Java Additional Parameters** section of the file:
		`wrapper.java.additional.<n>=-Dssl.debug=true`
		`wrapper.java.additional.<n>=-Dweblogic.StdoutDebugEnabled=true`
		Where:
		<*n*> — the incremental property number

	log4j.properties	Add or modify this setting in the file: `log4j.logger.com.bea.security.ssl = debug`

Server	File	Setting
Tomcat	WLESTomcat.conf	Add or modify this setting in the file:: `-Djavax.net.debug=ssl`
	log4j.properties	Add or modify this setting in the file: `log4j.logger.com.bea.security.ssl = debug`

2. Launch the utility in the SSM's `ales32-shared/bin` directory as follows:

   `ssldiagnosis.bat|sh <demo|secure>`

   where

   – `demo` — use this entry if you are using certificates created by the demo CA certificate

   – `secure` — use this entry if you are using certificates created by a CA certificate from the cacerts file in `BEA_HOME/jdk-version/jre/lib/security`.

3. At the enrollment prompt, enter the Administration Server administrator username and password. (The defaults are `admin` and `password` respectively)

4. Check DEMO CA: the default password for demo CA is "password" and the default ca alias name is "alesdemoca".

5. Check OES Certificates in keystore files

6. Check OES components, PD and SCM belongs to SM: give directory of any SSM. For example, Java-SSM location value is BEA_HOME/ales32-ssm/java-ssm

```
C:\bea_ssms\ales32-shared\bin>ssldiagnosis.bat demo
================================================================================
=====
AquaLogic Enterprise Security Enrollment/Unenrollment Utility
================================================================================
=====
Enter admin username :> admin
Enter admin password :>
checking keystore:C:\bea_ssms\ales32-shared/keys/DemoTrust.jks
Enter Demo Trust CA keystore password :>
checking Demo Trust CA Alias
```

```
Enter Demo Trust CA Alias:>alesdemoca
checking keystore:C:\bea_ssms\ales32-shared/keys\trust.jks
Enter password of C:\bea_ssms\ales32-shared/keys\trust.jks:>
checking keystore:C:\bea_ssms\ales32-shared/keys\identity.jceks
Enter password of C:\bea_ssms\ales32-shared/keys\identity.jceks:>
checking keystore:C:\bea_ssms\ales32-shared/keys\peer.jks
Enter password of C:\bea_ssms\ales32-shared/keys\peer.jks:>
checking Demo Trust CA certificate
the CA certificate with alias name: alesdemoca is compatible with OES
requirement

Checking Admin server: blougee-lap and port number is: 7010
Sending SSL Diagnosis request
Processing ssl diagnosis result
found qualified certificate for certficate with tag:cacert
found qualified certificate for certficate with tag:ssmcert
found qualified certificate for certficate with tag:admincert
found qualified certificate for certficate with tag:trustedcert
check OES component: PD & SCM status
input one of installed SSMs' Location:>C:\bea_ssms\ales32-ssm\java-ssm
PD is working on blougee-lap and port number is 7011
SCM is working on localhost and port number is 7005

C:\bea_ssms\ales32-shared\bin>
```

Configuring SSL in the Web Services SSM

When you create a Web Services SSM instance, it accessible via HTTP. This is appropriate for development and for debugging purposes, but production environments should use SSL.

This section describes how to enable one-way SSL communication between a Web Services SSM and its client. It is assumed that the reader has basic knowledge of the SSL protocol, Certificate Authorities (CA), X.509 certificates and Java Key Stores (JKS).

In this section, `%SSM_INST_HOME%` represents the installation folder of the Web Services SSM, for example, `c:\bea\ales32-ssm\webservice-ssm\instance\wsssm`.

Configuring One-Way SSL

With one-way SSL, the SSM sends its identity certificate to the client, therefore the client must trust the CA that signed the identity certificate. (The client does not have to have its own certificate, because it is not authenticated by the Web Services SSM.)

To configure a Web Services SSM to use one-way SSL:

1. Stop the Web Services SSM if it is running.
2. Delete the contents of the `%SSM_INST_HOME%\apps` directory.
3. Run the following command to regenerate the content of the `apps` directory:

   ```
   %SSM_INST_HOME%\adm\ssmwsInstance.bat -m
   ```

4. Restart the Web Services SSM.

After performing the above, copy the trusted JKS to the client. Then specify the following system properties when running the client:

```
-Djavax.net.ssl.trustStore=C:\jks\trust.jks
-Djavax.net.ssl.trustStorePassword="secretword"
```

Configuring SSL in the RMI SSM

This section describes the steps needed to configure the RMI SSM to use SSL for coommunication with a remote SSM.

Note: This information assumes the RMI SSM has already been set up without SSL as described in "Configuring a Remote SSM and Proxy" within the *SSM Installation and Configuration Guide*.

Procedure

To configure the RMI SSM for SSL, do the following:

1. Copy the trust keystore file from the `BEA_HOME\ales32-shared\keys` directory on the remote SSM to a directory on the application client where the SSM proxy is located.

   Note: The trust keystore provided during installation is **DemoTrust.jks**.

2. Make sure the keystore file is included in the classpath.

3. On the application client, open `PDPProxyConfiguration.properties` in a text editor and set the following parameters:

   PDPAddress
   Make sure the URLs begin with `rmis://` rather than `rmi://`.

   TrustStore
   The fully-qualified path to the trust keystore (use forward slashes). for example, `c:/bea3_2/ales32-shared/keys/<filename>.jks`.

CHAPTER 5

Resetting the Administrator Password

OES is installed using an administrative account that has a username and password of `admin` and `password` respectively. For security purposes, the account's password should be changed immediately after installation is complete or if it is compromised or lost.

Follow these steps to reset the OES administrator password:

1. To generate a hashed version of the new administrator password, open a command window in *BEA_HOME*`/ales32-admin/bin` and enter the following:

   `generatePasswordHash.bat <`*new_password*`>`

   This generates a hashed password. In the following example, the hashed password is shown inside square brackets.

   `hash result is[{SHA1}pvGBjCW7IS5jCM1e9dYR/EtCTojHjqk=]`

2. To update the database table for administration user, do the following:

   a. Connect to the database and the schema defined during OES installation.
   Note: This can be obtained by examining the following file:

   `BEA_HOME\ales32-admin\config\database.properties`.

   b. Enter the following:

   ```
   SQL> update adminuser set password = '<hash_password>' where userid =
   '//user/asi/system/';
   ```

   where
   <*hash_password*> is the hashed password generated in step 1.

Example:

```
SQL> update adminuser set password =
'{SHA1}pvGBjCW7IS5jCM1e9dYR/EtCTojHjqk=' where userid =
'//user/asi/system/';
```

3. To establish the new password and update the `password.xml/password.key` file, open a command window in *`BEA_HOME`*`/ales32-admin/bin` and execute the following on one line:

   ```
   asipassword.bat <admin_username>
   <BEA_Home>\ales32-shared>\keys\password.xml
   <BEA_Home>\ales32-shared>\keys\password.key
   ```

   where

   `<admin_username>` is the OES administrator username (be default, `system`)
   <BEA_Home> is BEA_HOME, for example `c:\bea`.

   Note: A number of administrative utilities use the password stored in `password.xml` to connect to the database.

4. Start the Administration Server.

CHAPTER 6

Additional Recommendations

Use SSL for Communications with the Database

SSL should be used for communication between Administration Server and the OES database server. This can be accomplished by enabling SSL communication on the JDBC driver.

For instructions, contact your JDBC driver vender or Oracle support.

Remove the Demonstration Examples

Installation of OES 3.2 automatically provides a number of demonstration examples that should be removed when no longer needed. The demonstration examples are provided in separate sub-directories located under the following directories:

Administration Server

- BEA_HOME/ales32-admin/examples

SSMs

- BEA_HOME/ales32-ssm/java-ssm/examples
- BEA_HOME/ales32-ssm/oracle-ssm/examples
- BEA_HOME/ales32-ssm/webservice-ssm/examples
- BEA_HOME/ales32-ssm/websphere-ssm/examples