OFBiz Single Sign On using CAS and LDAP

Version trunk

Table of Contents

Chapter 1. Setup the Java Key Store

From the directory in which you want to create the keystore, run keytool with the following parameters.

1. Generate the server certificate.

```
    $ keytool -genkey -alias tomcat -keyalg RSA -keypass changeit -storepass
changeit -keystore keystore.jks
```

   When you press Enter, keytool prompts you to enter the server name, organizational unit, organization, locality, state, and country code.

   Note that you must enter the server name in response to keytool's first prompt, in which it asks for first and last names.

   For testing purposes, this can be localhost.

2. Export the generated server certificate in keystore.jks into the file server.cer.

```
    $ keytool -export -alias tomcat -storepass changeit -file server.cer -keystore
keystore.jks
```

3. To create the trust-store file cacerts.jks and add the server certificate to the trust-store, run keytool from the directory where you created the keystore and server certificate. Use the following parameters:

```
    $ keytool -import -v -trustcacerts -alias tomcat -file server.cer -keystore
cacerts.jks -keypass changeit -storepass changeit
```

4. Information on the certificate, such as that shown next, will display.

```
    $ keytool -import -v -trustcacerts -alias tomcat -file server.cer -keystore
cacerts.jks -keypass changeit -storepass changeit

    Owner: CN=localhost, OU=Sun Micro, O=Docs, L=Santa Clara, ST=CA, C=US
    Issuer: CN=localhost, OU=Sun Micro, O=Docs, L=Santa Clara, ST=CA, C=US
    Serial number: 3e932169
    Valid from: Tue Apr 08
    Certificate fingerprints:
    MD5: 52:9F:49:68:ED:78:6F:39:87:F3:98:B3:6A:6B:0F:90
    SHA1: EE:2E:2A:A6:9E:03:9A:3A:1C:17:4A:28:5E:97:20:78:3F:
    Trust this certificate? [no]:
```

5. Enter yes, and then press the Enter or Return key. The following information displays:

```
    Certificate was added to keystore
    [Saving cacerts.jks]
```

Chapter 2. CAS Server

1. Download CAS server from the CAS web site.
2. Deploy cas-server-webapp-[version].war to Tomcat
3. Set key store file to Tomcat

```
    keystoreFile="path/to/keystore.jks"
```

4. Start Tomcat

Chapter 3. OFBiz Certificate

Set trust store's file to Java Virtual Machine (JVM) before start OFBiz.

```
    -Djavax.net.ssl.trustStore=path/to/cacerts.jks
```

Chapter 4. LDAP Component

OFBiz uses the LDAP component in the plugins to check the security in a web application.

4.1. LDAP Properties

LDAP properties file is plugins/ldap/config/ldap.xml.
You can change a filter condition you want.

4.1.1. Attributes

1. Attribute : LDAP attbitue for filter e.g. uid=%u
2. AuthenType : LDAP authentication method e.g. simple
3. AuthenticaionHandler : CAS handler class e.g. org.apache.ofbiz.ldap.cas.OFBizCasAuthenticationHandler
4. AutoPartyId : Party's id for user login e.g. admin
5. AutoSecurityGroupId : Security group's id for user login e.g. FULLADMIN
6. BaseDN : The top level ofbiz LDAP directory tree e.g. dc=example,dc=com
7. Filter : LDAP search filter e.g. (objectclass=*)
8. Scope : LDAP search scope parameter e.g. sub,one, etc.
9. URL : LDAP server's url e.g. ldap://localhost:389
10. UserOFBizLoginWhenLDAPFail : indicate that if LDAP fail then login with normal OFBiz's user or not. (true/false)

4.1.2. CAS

1. CasLoginUri : URI to CAS login e.g. /login
2. CasLogoutUri : URI to CAS logout e.g. /logout
3. CasUrl : CAS Server's URL e.g. https://localhost:8443/cas
4. CasValidateUri : URI to CAS validate e.g. /validate
5. CasLdapHandler : LDAP hanlder class e.g. org.apache.ofbiz.ldap.openldap.OFBizLdapAuthenticationHandler
6. CasTGTCookieName : CAS TGT's cookie name e.g. CASTGC

Chapter 5. OpenLDAP

The LDAP component need data from LDAP server (OpenLDAP). The server needs to install, configure and populate OpenLDAP: see at the OpenLDAP web site.

Chapter 6. Web Application Security Mapping

Every web application you need to use LDAP (single sign on) feature, you need to change the event's path of some the security request mappings to org.apache.ofbiz.ldap.LdapLoginWorker class.

6.1. checkLogin

```
    <request-map uri="checkLogin" edit="false">
        <description>Verify a user is logged in.</description>
        <security https="true" auth="false"/>
        <event type="java" path="org.apache.ofbiz.ldap.LdapLoginWorker"
invoke="checkLogin"/>
        <response name="success" type="view" value="main"/>
        <response name="error" type="view" value="login"/>
    </request-map>
```

6.2. login

```
    <request-map uri="login">
        <security https="true" auth="false"/>
        <event type="java" path="org.apache.ofbiz.ldap.LdapLoginWorker"
invoke="login"/>
        <response name="success" type="view" value="main"/>
        <response name="requirePasswordChange" type="view"
value="requirePasswordChange"/>
        <response name="error" type="view" value="login"/>
    </request-map>
```

6.3. logout

```
    <request-map uri="logout">
            <security https="true" auth="true"/>
            <event type="java" path="org.apache.ofbiz.ldap.LdapLoginWorker"
invoke="logout"/>
            <response name="success" type="request-redirect" value="main"/>
            <response name="error" type="view" value="main"/>
    </request-map>
```