Configuring CAS-based SSO with ActiveVOS on Apache Tomcat

Technical Note

Version: 1.3
Dated: August 2013

Content

Introduction

This technical note describes how to configure ActiveVOS 9.2.1 running on Apache Tomcat configured to use the Jasig CAS Single Sign-on (SSO) provider.

Overview of ActiveVOS Integration

Business process applications need to integrate seamlessly within an enterprise's application framework. The ability to provide a single sign-on user experience is important if an application is to gain quick acceptance by its end users.

ActiveVOS SSO lets you integrate your application with the SSO authentication and authorization framework in place such as Jasig's CAS, Sun's OpenSSO, and the SSO frameworks built into applications servers. Using ActiveVOS SSO capabilities lets you:

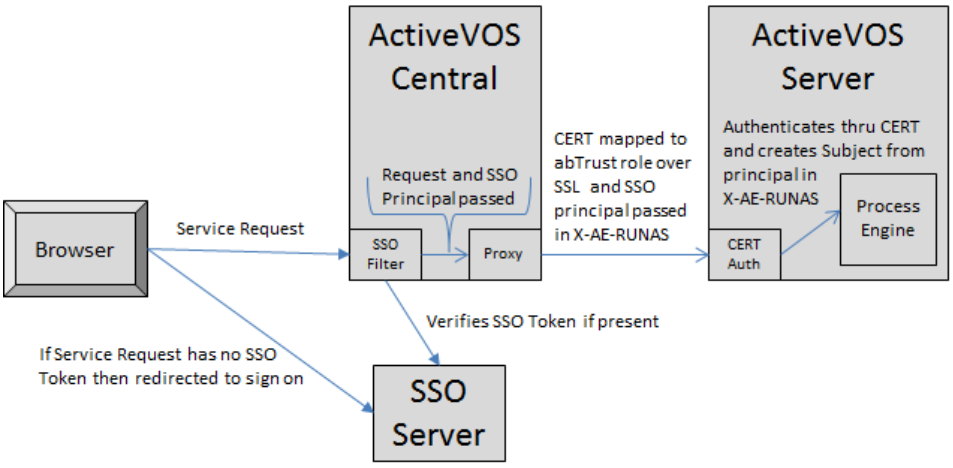
- Configure ActiveVOS Central and ActiveVOS Console to use the same SSO environment used elsewhere within the enterprise.
- Integrate ActiveVOS Central forms embedded in a user's web-based application with SSO capabilities.
- Integrate ActiveVOS Central as an integrated part of a portal-based application.

ActiveVOS

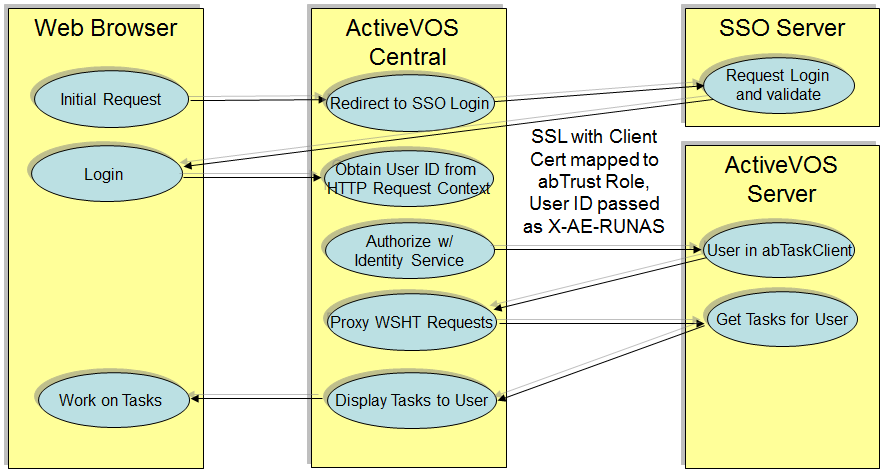
- Allows the separation of container authentication and the identification of the user for WS-HumanTask purposes.
- Provides support for secure, trusted communication between ActiveVOS Central and ActiveVOS Server via SSL/Certificate authentication.
- Integration of SSO providers only requires customization of the ActiveVOS Central application descriptors that are specific to the provider.
- The ActiveVOS server allows for requests to be proxied on behalf of a user without having access to the user's private credentials, provided that the request comes from a trusted source – ActiveVOS Central.

The ActiveVOS SSO Architecture

The following picture shows the ActiveVOS SSO architecture.



Also, here is the interaction pattern of the Web browser, ActiveVOS Central, ActiveVOS Server, and the SSO service.



Jasig CAS SSO Provider

The Jasig **Central Authentication Service** project, more commonly referred to as CAS is an authentication system originally created by Yale University to provide a trusted way for an application to authenticate a user. CAS became a Jasig project in December 2004.

The CAS is a single sign-on service that provides:

- An open and well-documented protocol
- An open-source Java server component
- A library of clients for Java, .Net, PHP, Perl, Apache, uPortal, and others
- Integrates with uPortal, BlueSocket, TikiWiki, Mule, Liferay, Moodle and others
- Community documentation and implementation support
- An extensive community of adopters

To learn more about Jasig CAS, go to http://www.jasig.org/cas

Configuring CAS for ActiveVOS Central

This section is a general overview of the installation and configuration steps that you will perform to integrate a generic SSO provider with ActiveVOS. The following section describes specific steps for the Jasig CAS provider.

Install and Configure SSO Server Component

Users should rely primarily on the documentation and support resources provided by the SSO Vendor for coverage of the entire possible configuration parameters. Users should also consult with their internal security team for recommendations.

Customize ActiveVOS Central WAR to enable the SSO Client

SSO support in ActiveVOS Central is enabled using configuring options set in the `aeWorkFlow-Config.xml` file contained in the ActiveVOS Central WAR file.

Many providers also require that you update the `web.xml` file to add servlet filters and additional configuration that is specific to the SSO provider.

Configure SSL between ActiveVOS Central and the ActiveVOS Server

- Configure a keystore containing a certificate with a private key on each server.
- Import the certificates for the other servers into each server's trust store.
- Configure the SSL connector for ActiveVOS Server to issue challenges for client certificates.
- Assign certificate principals to the required roles (`abTrust` and `abTaskClient`) .

Updating the aeWorkFlow-Config.xml file

- Provide a URL for certificate requests to ActiveVOS Server by specifying it in this location:

```
<!-- WS-HT Task Client operations service URL -->
<!-- This endpoint must be secured with roles abTaskClient
     and abTrust-->
<entry name="HtTaskClientServiceCertUrl"
value="https://host:port/activebpel-cert/services/AeB4PTaskClient-taskOperations" />
```

- Enable SSO Mode by enabling it in this location:

```
<!-- Enable single sign-on mode (requires CAS or similar SSO framework) -->
<entry name="SingleSignOnMode" value="client-cert" />
<entry name="SingleSignOnLogoutUrl" value="https://host:port/cas/logout" />
```

Steps

1. ActiveVOS Central and ActiveVOS Server 9.2.1 must be installed on Apache Tomcat 7.

2. Tomcat must be SSL-enabled using the `server.xml` file. The certificates must be set up for the communication between the ActiveVOS Central and ActiveVOS Server.

3. CAS 3.x must be installed and configured for use with Tomcat.

4. Add the following CAS client files to the `tomcat\lib` directory:

    - `cas-client-core-3.2.1.jar`
    - `cas-client-integration-tomcat-common-3.2.1.jar`
    - `cas-client-integration-tomcat-v7-3.2.1.jar`

5. In the `tomcat\conf` directory, create a file called `activevos-user-roles.properties`. This file maps users to roles. Here is an example of what you might enter:

```
# user to role mapping, password handled by CAS default implementation
would be same as username
aeadmin=abAdmin
qaOperator=abOperator
qaDeveloper=abDeveloper
qaDeployer=abDeployer
qaBusinessMgr=abBusinessManager
```

6. In the `tomcat\conf\Catalina\localhost` directory, modify the configurations for `activevos.xml` and `activevos-central.xml` to include the following declaration, which assumes an install of CAS server 3.5.2 on localhost. You will need to alter this so that it names your installation directories.

```
<Context …>
  …
   <Realm className="org.jasig.cas.client.tomcat.v7.PropertiesCasRealm"
```

```
        propertiesFilePath="conf/activevos-user-roles.properties"/>

    <Valve
        className="org.jasig.cas.client.tomcat.v7.Cas20CasAuthenticator"
                    encoding="UTF-8"
        casServerLoginUrl=
           https://localhost:8443/cas-server-webapp-3.5.2/login
        casServerUrlPrefix=
           https://localhost:8443/cas-server-webapp-3.5.2/
                    serverName="https://localhost:8443"/>

    <!-- Single sign-out support -->
    <Valve className="org.jasig.cas.client.tomcat.v7.SingleSignOutValve"
         artifactParameterName="SAMLart"/>

    <Valve
       className="org.jasig.cas.client.tomcat.v7.RegexUriLogoutValve"
       redirectUrl=https://localhost:8443/cas-server-webapp-3.5.2/logout
                   logoutUriRegex="/activevos/logout.*"/>
</Context>
```

7. Start your server.