Jericho Systems Corporation

EnterSpace Community Edition 2.0

Read-Me

6600 LBJ Freeway

Suite 250

Dallas, TX 75240

(972) 231-2000

CONTENTS

EXECUTIVE SUMMARY

EnterSpace Community Edition (CE) 2.0 is an open-source XACML-based Policy Decision Point (PDP) offering from Jericho Systems Corporation. This PDP will evaluate XACML 2.0 policies and support XACML 2.0 authorization query request. In addition, there is also support for a SAML protocol bound XACML request. This PDP is packaged as a J2EE-compliant Web application Archive (WAR) and will run on any J2EE-compliant web container that has support for JAX-WS.

EnterSpace CE is being released with an Apache 2.0 License agreement. For more information on the license, please read the license.txt available in the package.

Jericho Systems also offers a more advanced and robust decisioning engine (EnterSpace Decisioning Service Enterprise Edition). Please contact a Jericho Systems representative at (800)231-2000 for more information.

INSTALLATION

ASSUMPTIONS

The following are a list of requirements:

1. Setup instructions will assume that Tomcat 6.0 will be used as the Web-container on a LINUX OS.
2. Tomcat 6.0 is installed at some folder like */opt/EnterSpace/apache.* Instructions below refer to this directory as *TOMCAT_INSTALL*. Please check apache website for additional instructions.

SETUP & CONFIGURATION

1. Shut down Tomcat (If they are already running).

```
cd TOMCAT_INSTALL/bin

./catalina.sh stop
```

2. Install the *EnterSpaceCE.war* in the $*TOMCAT_INSTALL/webapps* folder.

```
cp EnterSpaceCE.war $TOMCAT_INSTALL/webapps
```

3. Restart Tomcat

   ```
   cd $TOMCAT_INSTALL/bin
   ./catalina.sh start
   ```

   Check the logs to make sure Tomcat started fine.

4. Update XACML Policy location

   ```
   cd $TOMCAT_INSTALL/webapps/EnterSpaceCE/WEB-INF/classes
   ```

   Edit *configuration.xml* and update *@ISSUER_VALUE*@ for SAML issuer value, *@LOGPATH@* for log path and *@POLICYPATH@* for the policy location.

```
<?xml version="1.0" encoding="UTF-8"?>
<Configuration xmlns="http://an.com/configuration"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://an.com/configuration configuration.xsd">
    <DefaultLog path="@LOGPATH@/pdpsample.log" an.log.Logger="an.log.DefaultLogger"
rolloverSize="-1" level="all" />

    <PDP issuer="@ISSUER_VALUE@" domainName="pdpSample"
multiPoliciesCombineAlg="an:multiple-policies-deny-overrides"
supportMustBePresent="true">
        <FileDataStore path="@POLICYPATH@" pattern=".*xml"
an.xacml.engine.DataStore="an.xacml.adapter.file.XMLFileDataStore" />
        <DefaultContextFactory />
        <CacheManager>
            <PolicyCache size="20000" />
            <EvaluationResultCache />
        </CacheManager>
        <PolicyResolverRegistry>
            <DefaultDataStorePolicyResolver
an.xacml.engine.PolicyResolver="jericho.esx.xacml.service.PrivatePolicyReferenceResolv
er" />
        </PolicyResolverRegistry>
    </PDP>
</Configuration>
```

   Note: XACML policies should be placed in the policy location specified in the *configuration.xml*. Additionally, all policy files that are shared or referenced by other policies can be placed in a sub-directory called *private*.

5. Restart Tomcat

   ```
   cd $TOMCAT_INSTALL/bin
   ```

```
      ./catalina.sh start
```

APPENDIX

SERVICE WSDL

```
<definitions xmlns="http://schemas.xmlsoap.org/wsdl/"
xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
xmlns:tns="urn:jerichosystems:service:saml:3.0.1:security"
    xmlns:xacml-context="urn:oasis:names:tc:xacml:2.0:context:schema:os"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
targetNamespace="urn:jericho:systems:5.0:xacml:service">
    <types>
        <xs:schema>
            <xs:import namespace="urn:oasis:names:tc:xacml:2.0:context:schema:os"
schemaLocation="http://docs.oasis-open.org/xacml/access_control-xacml-2.0-context-
schema-cd-04.xsd" />
        </xs:schema>
    </types>
    <!--
        Authorization Requests
    -->
    <message name="AuthorizeRequest">
        <part element="xacml-context:Request" name="Request" />
    </message>
    <message name="AuthorizeResponse">
        <part element="xacml-context:Response" name="Response" />
    </message>


    <!--
      Operation Types
    -->
    <portType name="XACMLServicePortType">
        <operation name="Authorize">
            <input message="tns:AuthorizeRequest" />
            <output message="tns:AuthorizeResponse" />
        </operation>
    </portType>
    <!--
       Bindings
    -->
    <binding name="XACMLServiceSOAPBinding" type="tns:XACMLServicePortType">
        <soap:binding style="document"
transport="http://schemas.xmlsoap.org/soap/http" />
        <operation name="Authorize">
            <input>
                <soap:body use="literal" />
            </input>
            <output>
                <soap:body use="literal" />
            </output>
        </operation>
    </binding>
    <service name="XACMLService">
        <port binding="tns:XACMLServiceSOAPBinding" name="XACMLService">
            <soap:address location="http://localhost:11013/NHINConnect" />
        </port>
    </service>
</definitions>
```

SAMPLE XACML 2.0 REQUEST & RESPONSE

Request:

```
<Request xmlns="urn:oasis:names:tc:xacml:2.0:context:schema:os">
    <Subject>
        <Attribute AttributeId="urn:oasis:names:tc:xacml:2.0:subject:subject-id"
DataType="http://www.w3.org/2001/XMLSchema#string">
            <AttributeValue>John Smith</AttributeValue>
        </Attribute>
        <Attribute AttributeId="urn:oasis:names:tc:xacml:2.0:subject:locality"
DataType="http://www.w3.org/2001/XMLSchema#string">
            <AttributeValue>1.2</AttributeValue>
        </Attribute>
        <Attribute AttributeId="urn:oasis:names:tc:xspa:1.0:subject:purposeofuse"
DataType="http://www.w3.org/2001/XMLSchema#string">
            <AttributeValue>Purpose for Use code not provided</AttributeValue>
        </Attribute>
    </Subject>
    <Resource>
        <Attribute AttributeId="urn:gov:hhs:fha:nhinc:service-type"
DataType="http://www.w3.org/2001/XMLSchema#string">
            <AttributeValue>DocumentRetrieveIn</AttributeValue>
        </Attribute>
        <Attribute AttributeId="urn:gov:hhs:fha:nhinc:patient-opt-in"
DataType="http://www.w3.org/2001/XMLSchema#string">
            <AttributeValue>Yes</AttributeValue>
        </Attribute>
    </Resource>
    <Action>
        <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
DataType="http://www.w3.org/2001/XMLSchema#string">
            <AttributeValue>read</AttributeValue>
        </Attribute>
    </Action>
    <Environment />
</Request>
```

Response:

```
<Response ns0:schemaLocation="urn:oasis:names:tc:xacml:2.0:context:schema:os
http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-context-schema-os.xsd"
    xmlns="urn:oasis:names:tc:xacml:2.0:context:schema:os"
xmlns:ns0="http://www.w3.org/2001/XMLSchema-instance">
    <Result>
        <Decision>Permit</Decision>
        <Status>
            <StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok" />
        </Status>
    </Result>
</Response>
```

SAMPLE SAML PROTOCOL BOUND XACML REQUEST & RESPONSE

Request:

```
<samlp:RequestAbstract xsi:type="xacml-samlp:XACMLAuthzDecisionQueryType" xacml-
samlp:InputContextOnly="true"
    xacml-samlp:ReturnContext="true" ID="s2f1681b32577f2203b7e5b852c1b7e58930eb351f"
Version="2.0" IssueInstant="2009-06-11T19:32:42Z" Destination="destination-uri"
    Consent="consent-uri" xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xacml-
samlp="urn:oasis:xacml:2.0:saml:protocol:schema:os">
    <saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">ConnectOpenSSOPepEntity</saml:Issue
r>
    <Request xmlns="urn:oasis:names:tc:xacml:2.0:context:schema:os">
        <Subject>
            <Attribute AttributeId="urn:oasis:names:tc:xacml:2.0:subject:subject-id"
DataType="http://www.w3.org/2001/XMLSchema#string">
                <AttributeValue>John Smith</AttributeValue>
            </Attribute>
            <Attribute AttributeId="urn:oasis:names:tc:xacml:2.0:subject:locality"
DataType="http://www.w3.org/2001/XMLSchema#string">
                <AttributeValue>1.2</AttributeValue>
            </Attribute>
            <Attribute AttributeId="urn:oasis:names:tc:xspa:1.0:subject:purposeofuse"
DataType="http://www.w3.org/2001/XMLSchema#string">
                <AttributeValue>Purpose for Use code not provided</AttributeValue>
            </Attribute>
        </Subject>
        <Resource>
            <Attribute AttributeId="urn:gov:hhs:fha:nhinc:service-type"
DataType="http://www.w3.org/2001/XMLSchema#string">
                <AttributeValue>DocumentRetrieveIn</AttributeValue>
            </Attribute>
            <Attribute AttributeId="urn:gov:hhs:fha:nhinc:patient-opt-in"
DataType="http://www.w3.org/2001/XMLSchema#string">
                <AttributeValue>Yes</AttributeValue>
            </Attribute>
        </Resource>
        <Action>
            <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
DataType="http://www.w3.org/2001/XMLSchema#string">
                <AttributeValue>read</AttributeValue>
            </Attribute>
        </Action>
        <Environment />
    </Request>
</samlp:RequestAbstract>
```

Response:

```
<samlp:Response ID="response-id:1" Version="2.0" IssueInstant="2009-06-
17T15:31:43.454Z" xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
    <samlp:Issuer>jerichoPdpEntity</samlp:Issuer>
    <samlp:Status>
```

```
        <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
    </samlp:Status>
    <saml:Assertion Version="2.0" ID="response-id:1" IssueInstant="2009-06-
17T15:31:43.454Z" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
        <saml:Issuer>jerichoPdpEntity</saml:Issuer>
        <saml:Statement xsi:type="xacml-samlp:XACMLAuthzDecisionStatement"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <Response
                ns0:schemaLocation="urn:oasis:names:tc:xacml:2.0:context:schema:os
http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-context-schema-os.xsd"
                xmlns:ns0="http://www.w3.org/2001/XMLSchema-instance"
xmlns="urn:oasis:names:tc:xacml:2.0:context:schema:os">
                <Result>
                    <Decision>Permit</Decision>
                    <Status>
                        <StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok" />
                    </Status>
                </Result>
            </Response>
        </saml:Statement>
    </saml:Assertion>
</samlp:Response>
```

XACML POLICY

Sample XACML Policy:

```
<?xml version="1.0" encoding="utf-8"?>
<PolicySet xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:policy:schema:os http://docs.oasis-
open.org/xacml/access_control-xacml-2.0-policy-schema-os.xsd"
PolicySetId="urn:oasis:names:tc:xspa:1.0"
PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-
overrides">
  <Target />
  <Policy PolicyId="always:permit:policy"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-
applicable">
    <Target></Target>
    <Rule RuleId="always:permit:rule" Effect="Permit"></Rule>
  </Policy>
</PolicySet>
```