Shibboleth Topics

Paul Caskey

March 8, 2021

Overview

Shibboleth Overview

- Open source, from the Shibboleth Consortium
- SAML, both IdP and SP
  - IdP + CAS
  - IdP + OIDC
- Very mature/Solid code base
- Deployed by the 1000s worldwide!
- The InCommon Trusted Access Platform packages Shibboleth as docker containers
  - Container source

IdP quick install

Bringing up an IDP container (and SP too)

- Start with a Linux VM with Docker-CE installed.
- mkdir ~/shib-train
- cd ~/shib-train
- curl -s -L -o shib_files.zip https://github.internet2.edu/docker/shib-idp/archive/master.zip
- unzip shib_files.zip
- cd shib-idp-master/
- rm -rf bin container_files tests *file common.bash README.md test-compose/README.md test-compose/idp/container_files/*
- mv test-compose/* ..
- cd ..
-

Bringing up an IDP container (cont)

- rm -rf shib-idp-master/
- rm -f shib_files.zip
- cd ~/shib-train/idp/container_files
- docker run -it -v $PWD:/output -e "BUILD_ENV=LINUX" tier/shibbidp_configbuilder_container
  - my.idp.name (in /etc/hosts)
  - ldap://data:389
  - ou=People, dc=internet2, dc=edu
  - cn=admin, dc=internet2, dc=edu
  - password
- rm -f Dockerfile

Bringing up an IDP container (cont)

- #Launch the container!
- cd ~/shib-train/idp/
- ./compose.sh
- # this takes a few minutes
- #check the output of 'docker ps' - look for status = healthy
- View the IdP's status page:
  - docker-compose exec idp curl -k https://127.0.0.1/idp/status

- The IdP is now operational, but can't really do anything yet...

Basic configuration of an IDP - Supplying Metadata

- This is similar to what you would do when you join a federation so that others could trust your IdP.
- Save the file from https://my.idp.name/idp/shibboleth to your local drive. That is the IdP's basic metadata.
- Navigate to http://sp.training.incommon.org/mdupload and upload the file form the previous step.
- Wait a few minutes...

Basic configuration of an IDP - Configuring Trusted Metadata

- This is similar to what you would do when you join a federation so that your IdP would trust federated SPs.
- Add to config/shib-idp/conf/metadata-providers.xml
  - <MetadataProvider id='ShibbTrainMD' xsi:type='FileBackedHTTPMetadataProvider' xmlns='urn:mace:shibboleth:2.0:metadata'

    metadataURL='http://md.training.incommon.org/downloads/ShibTrain1-metadata.xml'

    backingFile='/opt/shibboleth-idp/metadata/ShibTrain1-metadata.xml'/>
-

Basic configuration of an IDP - Configuring Attribute Release

- In config/shib-idp/conf/attribute-filter.xml
- <AttributeFilterPolicy id='releaseForClassroomSP'>
  <PolicyRequirementRule xsi:type='Requester' value='https://sp.training.incommon.org/shibboleth' />
- <AttributeRule attributeID='eduPersonPrincipalName'>
- <PermitValueRule xsi:type='ANY' />
- </AttributeRule>
- <AttributeRule attributeID='displayName'>
- <PermitValueRule xsi:type='ANY' />
- </AttributeRule>

Basic configuration of an IDP - Configuring Attribute Release (cont)

```
<AttributeRule attributeID='mail'>
    <PermitValueRule xsi:type='ANY' />
</AttributeRule>
<AttributeRule attributeID='surname'>
    <PermitValueRule xsi:type='ANY' />
</AttributeRule>
<AttributeRule attributeID='givenName'>
    <PermitValueRule xsi:type='ANY' />
</AttributeRule>
```

Basic configuration of an IDP - Configuring Attribute Release (cont)

```
    <AttributeRule attributeID='eduPersonAffiliation'>
        <PermitValueRule xsi:type='ANY' />
    </AttributeRule>
    <AttributeRule attributeID='uid'>
        <PermitValueRule xsi:type='ANY' />
    </AttributeRule>
</AttributeFilterPolicy>
```

Basic configuration of an IDP - Testing

- Navigate to https://sp.training.incommon.org/secure
- Select the new IdP from the list (my.idp.name)
- Login as kwhite/password
- Verify released attributes

The InCommon Federation

The InCommon Federation

- Trust federation for higher-education and research in the US
  - IdPs and SPs
  - Global: partnered with over 60 other federations
- Publishes trusted SAML metadata
- Metadata is well-curated
  - Strong vetting of institutions/contacts
  - Strong vetting of SAML entityID/endpoints
- InCommon Federation Manager
- On-demand metadata: MDQ

Open Discussion