191023-24 @ Sunet Dagarna - Shibboleth OIDC

Agenda

Time	Contents
13.00-14.30	Introduction H, logistics A, installation A
15.00-17.00	Trust OP H, Trust RP A, Authentication A
9.00-10.15	Attribute resolving and filtering, Subject
10.45-12.00	Profile configuration, Summary and conclusions

Introduction

Section Topics

- Introduction to OAuth2 and OIDC
- Project resources (releases, documentation and source code)
- Support channels
- Tutorial logistics

Introduction to OAuth2 and OIDC

Introduction to OAuth2 and OIDC

- OAuth2 specifications
  - The OAuth 2.0 Authorization Framework: https://tools.ietf.org/html/rfc6749
  - The OAuth 2.0 Authorization Framework: Bearer Token Usage: https://tools.ietf.org/html/rfc6750
- OIDC specifications
  - https://openid.net/connect/
  - Core: http://openid.net/specs/openid-connect-core-1_0.html
  - Discovery: http://openid.net/specs/openid-connect-discovery-1_0.html
  - Dynamic registration: http://openid.net/specs/openid-connect-registration-1_0.html
- Certification tool + programme
  - https://openid.net/certification/

Project resources

Releases and Documentation
▪ https://github.com/CSCfi/shibboleth-idp-oidc-extension/releases ▪ https://github.com/CSCfi/shibboleth-idp-oidc-extension/wiki

Support channels

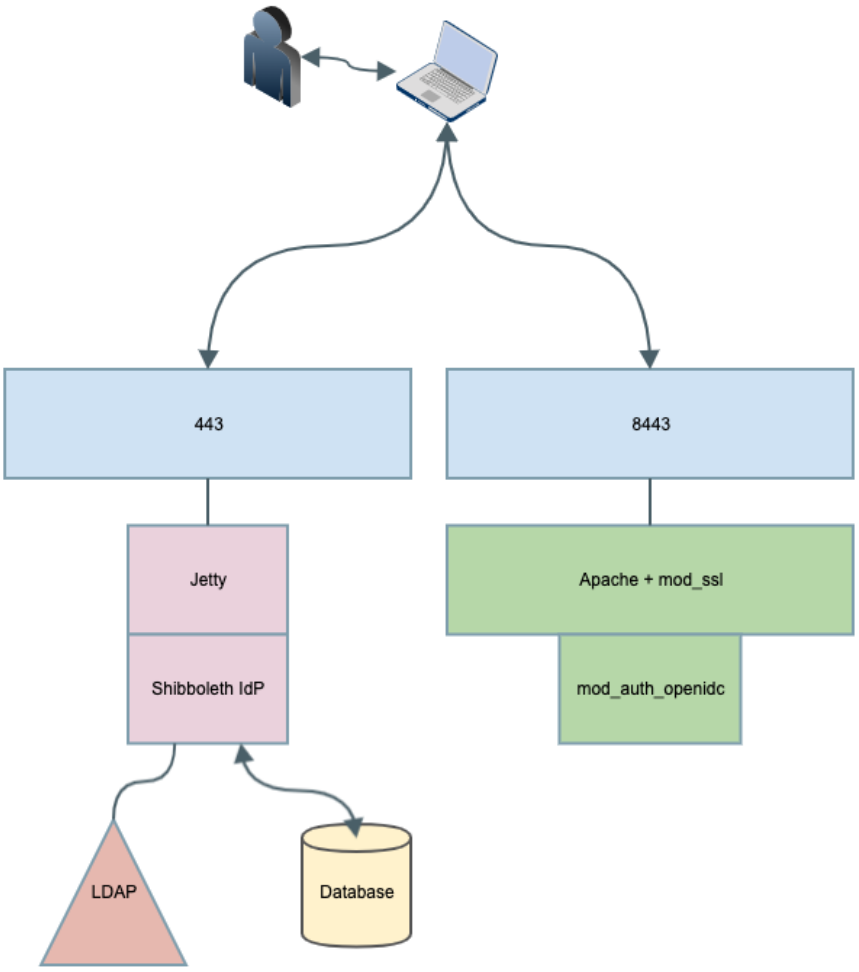
Support channels
Shibboleth mailing lists: https://www.shibboleth.net/community/lists/ GitHub issues ▪ https://github.com/CSCfi/shibboleth-idp-oidc-extension/issues

Tutorial logistics

Virtual machines
Everybody should have a paper note containing **IP address** and a **password** for *cloud-user*

The virtual machines are running CentOS 7 with the following software already installed

- OpenJDK 8 JRE
  - JAVA_HOME = /usr/lib/jvm/jre-1.8.0
- Apache 2
  - Running on ports 80 and 8443
  - OICD RP module mod_auth_openidc
  - Log files */var/log/httpd*
- Jetty v9.4.2
  - Running on ports 8080 and 443
  - /opt/jetty
  - /opt/shibboleth-idp/jetty-base
- MariaDB
  - Database name for IdP: 'idp'
  - Username 'idp' password: 'not_set_yet'
- 389 Directory Server
  - Admin 'cn=Directory Manager' and pwd 'testpword'
  - End-user ***teppo***, password ***testaaja***
- Shibboleth IdP 3.4
  - service name ***shibboleth-idp***
  - IDP home directory */opt/shibboleth-idp*
  - Log files */opt/shibboleth-idp/logs/*



Exercises

Exercise 1.1 - Check VM connection

1. Verify that you can log in to your virtual machine
    a. SSH-connection to the IP address as *cloud-user* with the given password

Hints, Tips and Result

```
# ssh cloud-user@IP_ADDRESS
```

2. Restart the *shibboleth-idp* service

Hints, Tips and Result

```
[vagrant@gn43-oidcshibop-devel ~]$ sudo su
[root@gn43-oidcshibop-devel vagrant]# systemctl stop shibboleth-idp
[root@gn43-oidcshibop-devel vagrant]# systemctl start shibboleth-idp
```

1. Verify from the logs that it starts up without errors

Hints, Tips and Result

```
[root@gn43-oidcshibop-devel vagrant]# tail -f /opt/shibboleth-idp/logs/idp-process.log
2018-09-28 22:35:50,509 - INFO [net.shibboleth.ext.spring.context.FilesystemGenericApplicationContext:
583] - Refreshing shibboleth.ReloadableAccessControlService: startup date [Fri Sep 28 22:35:50 UTC
2018]; parent: Root WebApplicationContext
2018-09-28 22:35:50,562 - INFO [net.shibboleth.ext.spring.service.ReloadableSpringService:421] -
Service 'shibboleth.ReloadableAccessControlService': Completed reload and swapped in latest
configuration for service 'shibboleth.ReloadableAccessControlService'
2018-09-28 22:35:50,562 - INFO [net.shibboleth.ext.spring.service.ReloadableSpringService:428] -
Service 'shibboleth.ReloadableAccessControlService': Reload complete
2018-09-28 22:35:50,576 - INFO [net.shibboleth.utilities.java.support.service.
AbstractReloadableService:199] - Service 'shibboleth.ReloadableAccessControlService': Reload time set
to: 300000, starting refresh thread
2018-09-28 22:35:50,585 - INFO [net.shibboleth.utilities.java.support.service.
AbstractReloadableService:173] - Service 'shibboleth.ReloadableCASServiceRegistry': Performing initial
load
2018-09-28 22:35:50,585 - INFO [net.shibboleth.utilities.java.support.service.
AbstractReloadableService:258] - Service 'shibboleth.ReloadableCASServiceRegistry': Reloading service
configuration
2018-09-28 22:35:50,587 - INFO [net.shibboleth.ext.spring.util.SchemaTypeAwareXMLBeanDefinitionReader:
317] - Loading XML bean definitions from file [/opt/shibboleth-idp/conf/cas-protocol.xml]
2018-09-28 22:35:50,596 - INFO [net.shibboleth.ext.spring.context.FilesystemGenericApplicationContext:
583] - Refreshing shibboleth.ReloadableCASServiceRegistry: startup date [Fri Sep 28 22:35:50 UTC
2018]; parent: Root WebApplicationContext
2018-09-28 22:35:50,647 - INFO [net.shibboleth.ext.spring.service.ReloadableSpringService:421] -
Service 'shibboleth.ReloadableCASServiceRegistry': Completed reload and swapped in latest
configuration for service 'shibboleth.ReloadableCASServiceRegistry'
2018-09-28 22:35:50,660 - INFO [net.shibboleth.ext.spring.service.ReloadableSpringService:428] -
Service 'shibboleth.ReloadableCASServiceRegistry': Reload complete
2018-09-28 22:35:50,672 - INFO [net.shibboleth.utilities.java.support.service.
AbstractReloadableService:199] - Service 'shibboleth.ReloadableCASServiceRegistry': Reload time set
to: 900000, starting refresh thread
2018-09-28 22:35:51,184 - WARN [net.shibboleth.utilities.java.support.net.CookieManager:171] - Use of
secure and httpOnly properties are strongly advisable, currently one or both are false
2018-09-28 22:35:51,911 - INFO [net.shibboleth.ext.spring.context.DelimiterAwareApplicationContext:
583] - Refreshing WebApplicationContext for namespace 'idp-servlet': startup date [Fri Sep 28 22:35:51
UTC 2018]; parent: Root WebApplicationContext
2018-09-28 22:35:51,943 - INFO [net.shibboleth.ext.spring.resource.ConditionalResource:87] -
ConditionalResource conditional:/opt/shibboleth-idp/conf/mvc-beans.xml: getInputStream failed on
wrapped resource
2018-09-28 22:35:51,944 - INFO [net.shibboleth.ext.spring.resource.ConditionalResource:87] -
ConditionalResource conditional:/opt/shibboleth-idp/conf/mvc-beans.xml: getInputStream failed on
wrapped resource
2018-09-28 22:35:52,832 - INFO [net.shibboleth.idp.authn.impl.RemoteUserAuthServlet:215] -
RemoteUserAuthServlet will process REMOTE_USER, along with attributes [] and headers []
```