



IDP:n asennus

16-17.3.2010 Shibboleth
asennuskoulutus

Janne Lauros

CSC – Tieteen tietotekniikan keskus Oy
CSC – IT Center for Science Ltd.

Vaiheet



- Virtuaalikoneen ympäristö
- Shibboleth Idp 2.1.5:sen asennus
- Shibboleth Idp:n konfigurointi
 - Metadata provider määrittelyt
 - Käyttäjätunnistus määrittelyt
 - Attribuutti määrittelyt

Ennen asentamista



- Autentikointimetodi ja lähde
 - LDAP, SQL-tietokanta...
 - Olemassa oleva kirjautumisjärjestelmä (Pubcookie, CAS...)
 - Uusi autentikointijärjestelmä (yllämainitut, Tomcat forms...)
 - Shibbolethin oma (LDAP)
- Attribuuttivarasto
 - LDAP, SQL-tietokanta...
 - Mitä attribuutteja löytyy ja täyttyykö tarve

Asentaminen



- Idp on 2.4 Servlet, vaatii siis isännäkseen Servlet Containerin
- Ensin sovelluspalvelin toimintaan
 - Esim. Tomcat + Java
- Apachen voi laittaa Tomcatin eteen halutessaan

Verkkoyhteydet



- IdP:ssä kaksi palvelua ulospäin
 - Käyttäjille tunnistautumista varten
 - SP-palvelimille joitakin profiileja varten
- 443 auki maailmalle
 - Käyttäjät tulevat selaimilla
 - Normaali-https
- 8443 voi sallia SP-kohtaisesti
 - SP-palvelimet mm. hakevat attribuutteja tietyissä tilanteissa
 - Palvelimet tunnistavat toisensa varmenteiden avulla

Virtuaalikoneen ympäristö



- Virtuaalikoneen käyttäjätunnus on "root" ja salasana "password". Ensimmäisen käynnistyksen yhteydessä asetetaan virtuaalikoneen IP etc. asetukset kohdilleen setupVM komennolla. Osallistujanumerosi ldp:lle on 1 ja näppäimistösi on todennäköisesti suomalainen.

```
[root@idp1 ~]#
Shibboleth Inst... VM Image Setup
#####
Please enter yo... icipation number:
These and more... d layouts are avail able:
by, cf, croat, ... de_CH-latin1, dk, es, et, fi, fr_CH, gr, il, it, lt,
mk, nl, no, pl, ... , se-latin1, sg, slovene, sv-latin1, ua, uk, us
Please enter yo... oard layout [default: us]:
```

Shibboleth Idp:n asennus



- Idp asennetaan virtuaalikoneelta löytyvästä .zip tiedostosta.

```
[root@idp1 ~]# unzip -d /var/tmp/ /opt/installfest/distro/shibboleth-identityprovider-2.1.5-bin.zip
```

```
[root@idp1 ~]# cd /var/tmp/shibboleth-identityprovider-2.1.5/
```

```
[root@idp1 shibboleth-identityprovider-2.1.5]# chmod +x install.sh
```

```
[root@idp1 shibboleth-identityprovider-2.1.5]# ./install.sh
```

...

```
Where should the Shibboleth Identity Provider software be installed? [/opt/shibboleth-idp]
```

```
/opt/shibboleth-idp
```

```
What is the fully qualified hostname of the Shibboleth Identity Provider server? [idp.example.org]
```

```
idp1.example.org
```

```
A keystore is about to be generated for you. Please enter a password that will be used to protect it.
```

```
password
```

...

```
BUILD SUCCESSFUL
```

```
Total time: 1 minute 35 seconds
```

Shibboleth Idp:n asennus



- Idp asennuksen hakemistot.

```
[root@idp1 ~]# cd /opt/shibboleth-idp
```

```
[root@idp1 shibboleth-idp]# ls
```

bin	–muutama työkalu Idp:n testaamiseen
conf	- Idp:n konfigurointi tiedostot
credentials	- Idp:n private key ja vastaava sertifikaatti
lib	– kirjastot, huom. sisältää endorsed hakemiston
logs	– Idp:n logit
metadata	- Idp:n metadata hakemisto, tänne tallettuu asennuksen yhteydessä luotu metadata.
war	– Idp:n deployattava idp.war tiedosto

Konfiguraatiot



- relying-party.xml
 - Yleiset asetukset mm. miten keskustellaan eri SP:den kanssa
- handler.xml
 - Tuetut viestinvaihto- ja autentikointimekanismit
- logging.xml
 - Logien asetukset
- attribute-filter.xml
 - Mitä attribuutteja luovutetaan millekin SP:lle
- attribute-resolver.xml
 - Attribuuttien haun ja luonnin asetukset

Shibboleth Idp:n asennus



- Kerrotaan tomcatille meidän idp:stä:

```
[root@idp1 ~]# cd /opt/tomcat/conf/Catalina/localhost/
```

```
[root@idp1 localhost]# nano idp.xml
```

```
<Context
```

```
    docBase="/opt/shibboleth-idp/war/idp.war"
```

```
    privileged="true"
```

```
    antiResourceLocking="false"
```

```
    antiJARLocking="false"
```

```
    unpackWAR="false" />
```

Shibboleth Idp:n asennus



- Idp:n asetukset server.xml failissa (esiasetetut)

```
[root@idp1 ~]# more /opt/tomcat/conf/server.xml
```

```
<Service name="Catalina">  
  <Connector port="443"  
    address="10.0.1.1"  
    maxHttpHeaderSize="8192"  
    maxSpareThreads="75"  
    scheme="https"  
    secure="true"  
    sslProtocol="TLS"  
    SSLEnabled="true"  
    keystoreFile="/opt/shibboleth-idp/credentials/idp.jks"  
    keystorePass="password"  
    trustoreFile="/opt/shibboleth-idp/credentials/idp.jks"  
    trustorePass="password"  
    truststoreAlgorithm="DelegateToApplication" />
```

Shibboleth Idp:n asennus



- Idp:n asetukset server.xml failissa (esiasetetut).. jatkuu

```
[root@idp1 ~]# more /opt/tomcat/conf/server.xml
```

```
...
```

```
<Connector port="8443"
    address="10.0.1.1"
    maxHttpHeaderSize="8192"
    maxSpareThreads="75"
    scheme="https"
    secure="true"
    clientAuth="want"
    sslProtocol="TLS"
    SSLEnabled="true"
    keystoreFile="/opt/shibboleth-idp/credentials/idp.jks"
    keystorePass="password"
    truststoreFile="/opt/shibboleth-idp/credentials/idp.jks"
    truststorePass="password"
    truststoreAlgorithm="DelegateToApplication" />
```

Shibboleth Idp:n asennus



- Ohjataan tomcat käyttämään Idp:n endorsed hakemistoa

```
[root@idp1 ~]# cd /opt/tomcat/
```

```
[root@idp1 tomcat]# ln -fs /opt/shibboleth-idp/lib/endorsed endorsed
```

Shibboleth Idp:n asennus – Jälkihoito



- Kopioidaan vielä ennaltamääritellyt avaimet asennuksessa luotujen tilalle:

```
[root@idp1 ~]# cp /opt/installfest/idps/idp1/idp.* /opt/shibboleth-idp/credentials/  
cp: overwrite `/opt/shibboleth-idp/credentials/idp.crt'? y  
cp: overwrite `/opt/shibboleth-idp/credentials/idp.jks'? y  
cp: overwrite `/opt/shibboleth-idp/credentials/idp.key'? y
```

- Kopioidaan myös sp2.example.org:in metadata

```
[root@idp1 ~]# cp /opt/installfest/sps/sp2/*.xml /opt/shibboleth-idp/metadata/
```

- Käynnistä Idp uudelleen – Nyt olemme valmiit muokkaamaan Idp keskustelemaan sp2.example.org:in kanssa.

Shibboleth Idp:n konfigurointi



- Logit
- Metadata
- Käyttäjätunnistus
- Attribuutit

Logit



- Logitasot määritellään SHIB_HOME/conf/logging.xml failissa
- Logitasot ovat TRACE, DEBUG, INFO, WARN ja ERROR
- Useimmissa tapauksissa logitasot voidaan määritellä java pakettien nimien mukaan hierarkisesti
- Idp:tä ei tarvitse uudelleenkäynnistää. Idp tarkistaa logitasot 5 minuutin välein
- Logit kirjoitetaan oletuksena SHIB_HOME/logs hakemistoon
- idp-process.log – 'päälogi'. Tästä kaivetaan yleensä ongelmat esiin.
- idp-audit.log – logitus ulosmenevästä informaatiosta
- idp-access.log – logitetaan kaikki käyttäjät

Logit



- Nosta Shibbolethin logi DEBUG tasolle:

```
[root@idp1 conf]# cd /opt/shibboleth-idp/conf/
```

```
[root@idp1 conf]# nano logging.xml
```

```
<!-- Logs IdP, but not OpenSAML, messages -->
```

```
  <logger name="edu.internet2.middleware.shibboleth">
```

```
    <level value="DEBUG" />
```

```
  </logger>
```

- Uudelleenkäynnistä Idp ja ota tuntumaa logeihin

Metadata



- Tavoitteena on ottaa sp2.example.org:in metadata käyttöön
- Metadata (kertausta) kuvaa siis SAML entiteetin konfiguraation, palveluosoitteet ja käytetyt sertifikaatit
- Idp:n käyttämä metadata määrittellään SHIB_HOME/conf/relying_party.xml tiedoston MetadataProvider osiossa
- SHIB_HOME/conf/relying_party.xml:ssä määrittellään myös kommunikointiprofiilit (anonymous, default ja specific) mutta niihin palataan myöhemmin

Metadata



- Metadata luetaan ketjutetusti mahdollisesti useammasta lähteestä
- Chaining Metadata Provider
 - Sisältää yhden tai useamman Metadata Provider elementin yhdistäen ne yhdeksi kokonaisuudeksi
 - Jos yksittäinen entity löytyy useammasta lähteestä vain ensimmäinen on voimassa
- Filesystem Metadata Provider
 - Lukee metadatan tiedostojärjestelmästä.
- File Backed HTTP Metadata Provider
 - Lukee metadatan http tai https osoitteesta ja tallettaa backupin tiedostojärjestelmään. Default cachetus 48min.
- HTTP Metadata Provider
 - Lukee metadatan http tai https osoitteesta. Default cachetus 48min.
- Inline Metadata Provider
 - Copy-paste metadata provideri..

Metadata



- Metadatan lukemiseen voidaan lisätä tarkistuksia metadatan allekirjoitukselle lisäämällä Metada Filter elementti Metadata Provideriin.
- Chaining Metadata Filter
 - Sisältää yhden tai useamman Metadata Filterin suorittaen ne järjestyksessä
- Schema Validation Filter
 - Validoi metadatan annettua XML schemaa vasten
- Required validUntil Filter
 - Tarkistaa että metadatan root elementissä on validUntil attribuutti ja että sen arvo on pienempi kuin annettu arvo (valinnainen tarkastus)

Metadata



- Metadatan lukemiseen voidaan lisätä tarkistuksia metadatan allekirjoitukselle lisäämällä Metada Filter elementti Metadata Provideriin.
- Signature Validation Filter
 - Tarkistaa metadatan XML allekirjoituksen
- Entity Role WhiteList Filter
 - Mahdollisuus Idp:lle poistaa sille turhat Idp entityt metadatatista

Metadata



- Lisää sp2.example.org:in metadata relying_party.xml:ään

```
[root@idp1 ~]# cd /opt/shibboleth-idp/conf/
```

```
[root@idp1 conf]# nano relying-party.xml
```

```
<MetadataProvider id="sp2" xsi:type="FilesystemMetadataProvider"
xmlns="urn:mace:shibboleth:2.0:metadata" metadataFile="/opt/shibboleth-idp/metadata/sp2-metadata.xml"
/>
```

- Uudelleen käynnistä Idp, seuraa logeista onnistuiko sp2 metadatan käyttöönotto
- Mene selaimella osoitteeseen <https://sp2.example.org/secure> ja tutki logeista mitä tapahtuu. Mikä menee vielä pieleen?

Metadata



- Lisätehtävä: Käynnistä virtuaalikone ShibInstallFest-Test-IdP-DS.
- Määrittele File Backed Metadata Provider (<https://spaces.internet2.edu/display/SHIB2/IdPMetadataProvider>) testsp2:selle jonka metadatat voi lukea osoitteesta <http://testsp2.example.org/metadata.xml>
- Katso logeista ja levypinnalta että metadatan luku onnistuu

Käyttäjätunnistus



- RemoteUser
- Username/Password (LDAP/Kerberos)
- IP osoite
- Oma JAAS moduli

Käyttäjätunnistus



- Tavoitteena harjoituksessa on määritellä Username/Password pohjainen LDAP käyttäjätunnistus
- LoginHandler elementti määritellään SHIB_HOME/conf/handler.xml tiedostossa

```
[root@idp1 ~]# cd /opt/shibboleth-idp/conf/
```

```
[root@idp1 conf]# nano handler.xml
```

- Poista RemoteUser tyyppinen LoginHandler, aktivoi UsernamePassword LoginHandler

Käyttäjätunnistus



- Muokkaa UsernamePassword handlerin konfiguraatiota (jaasConfigurationLocation), lisätään LDAP:in tiedot:

```
edu.vt.middleware.ldap.jaas.LdapLoginModule required  
  
host="127.0.0.1"  
  
base="ou=people,dc=example,dc=org"  
  
port="10389"  
  
userField="uid";
```

- Mene selaimella osoitteeseen <https://sp2.example.org/secure> ja tutki logeista mitä tapahtuu. Käyttäjätunnus on "student1" ja salasana "password". Mitä puuttuu vielä?

Käyttäjätunnistus



- Autentikointimetodin yhteydessä voidaan määritellä authenticationDuration. Oletusarvo on 30 minuuttia.
- Käyttäjä joutuu uudelleen autentikoitumaan mennessään uudelle SP :lle jos sessio Idp:hen tai authenticationDuration on lauennut.
- SP voi ehdottaa autentikointimetoodeja. Jos voimassa oleva ei tyydytä suoritetaan uusi autentikointi käyttäen haluttua metodia.

Käyttäjätunnistus



- Lisätehtävä: Lisää IP pohjainen tunnistus. Määrittele että omasta IP osoitteestasi (10.0.3.1) tuleva käyttäjä on "student1". Lisää uusi LoginHandler LDAP handleriä 'ennen' ja koita pääsetkö kirjautumaan sivulle <https://sp2.example.org/secure> pelkän IP osoitteen perusteella.
(<https://spaces.internet2.edu/display/SHIB2/IdPAuthIP>)

Käyttäjätunnistus



- Lisätehtävä II: Muokkaa SP2:sta niin että se vaatii <https://altsp2.example.org/secure> sivulle mentäessä nimenomaan PasswordProtectedTransport tunnistuksen eikä IP pohjaista. Huom! Tehtävä 8 SP osiosta pitää olla tehtynä ensin. (<https://spaces.internet2.edu/display/SHIB2/NativeSPSessionInitiator#NativeSPSessionInitiator-CommonAttributes>)

Attribuutit



..haluamme siis yleensä kertoa käyttäjästä
muutakin kuin että hän osaa salasanansa..

..mutta emme enempää kuin pakko..

Attribuutit – In a nutshell



- Attribuutti pitää määritellä ja populoida eli muodostetaan **AttributeDefinition**
 - Määritellään tiedostoon attribute-resolver.xml sisältäen
 - **Attribuutin tyyppiin**,
 - **ID:n** eli shibin sisäisen tunnisteiden attribuutille,
 - **sourceAttributeID:n** eli attribuutin tunnisteiden käytettävälle DataConnectorille
 - **DataConnectorin** eli keinon populoida attribuutti ja
 - **AttributeEncoderin** jolla määritellään miten populoitu attribuutti esitetään SAML viestissä
- Lisäksi tarvitaan Attribuutin luovutussääntö
 - Määritellään tiedostossa attribute-filter.xml

Attribuutit – Muutama Tyyppi



- Simple – Perustyyppi. Attribuuteille jotka välitetään eteenpäin sellaisenaan
- Scoped – Kuten Simple mutta attribuutin arvoon lisätään AttributeDefinition:ssa määritelty scope
- Prescoped – Olettaa saavansa valmiiksi scopatun attribuutin
- Principalname – Käyttäjän principal name
- ad:TransientId
- SAML1NameIdentifier
- SAML2NameID
- Script – Muodostaa attribuutin esimerkiksi java scriptillä muista attribuutesita
- Mapped – Mäppää attribuutin arvon toiseksi
- ...

Attribuutit



- **Esimerkki:**

```
<resolver:AttributeDefinition id="surName" xsi:type="Simple" xmlns="urn:mace:shibboleth:2.0:resolver:ad"
  sourceAttributeID="sn">

  <resolver:Dependency ref="myLDAP" />

  <resolver:AttributeEncoder xsi:type="SAML1String"
    xmlns="urn:mace:shibboleth:2.0:attribute:encoder" name="urn:mace:dir:attribute-def:sn" />

  <resolver:AttributeEncoder xsi:type="SAML2String"
    xmlns="urn:mace:shibboleth:2.0:attribute:encoder" name="urn:oid:2.5.4.4" friendlyName="sn" />

</resolver:AttributeDefinition>
```

Attribuutit – DataConnector



- Static – Kätevä kun halutaan myöntää ”vakioarvoja” idp:n kaikille käyttäjille
- ComputedId – Hashaa määritellystä attribuutista, SP:n entity id:stä ja salt:ista uuden arvon (Deprecated)
- StoredId – Kuten ComputedId mutta tallentaa arvon tietokantaan
- RelationalDatabase – Connectori Attribuutin arvon hakemiseksi tietokannasta
- LDAPDirectory – Connectori Attribuutin arvon hakemiseksi LDAP:ista

Attribuutit – DataConnector



- **Esimerkki:**

```
<resolver:DataConnector id="myLDAP" xsi:type="LDAPDirectory" xmlns="urn:mace:shibboleth:2.0:resolver:dc"
    ldapURL="ldap://127.0.0.1:10389" baseDN="ou=people,dc=example,dc=org"
    principal="uid=myservice,ou=system">
    <FilterTemplate>
        <![CDATA[
            (uid=$requestContext.principalName)
        ]]>
    </FilterTemplate>
</resolver:DataConnector>
```

Attribuutit – Filter



- **Esimerkki:**

```
<AttributeFilterPolicy>
    <PolicyRequirementRule xsi:type="basic:AttributeRequesterString"
value="https://sp2.example.org/shibboleth" />
    <AttributeRule attributeID="surName">
        <PermitValueRule xsi:type="basic:ANY" />
    </AttributeRule>
</AttributeFilterPolicy>
```

Attribuutit



- Tehtävä: Julkaistaan ryhmä attribuutteja
- Vapauta ryhmään "Core" ja "eduPerson" kuuluvat AttributeDefinition:it kommentteista.
- Kommentoi ulos AttributeDefinition:it jotka käyttävät ComputedID DataConnectoria
- Lisää DataConnector:

```
<resolver:DataConnector id="myLDAP" xsi:type="LDAPDirectory" xmlns="urn:mace:shibboleth:2.0:resolver:dc"
    ldapURL="ldap://127.0.0.1:10389" baseDN="ou=people,dc=example,dc=org"
    principal="uid=myservice,ou=system">
    <FilterTemplate>
        <![CDATA[
            (uid=$requestContext.principalName)
        ]]>
    </FilterTemplate>
</resolver:DataConnector>
```

Attribuutit



- Lisää testi SP:lle attribuuttien rilisointisääntö:

```
<AttributeFilterPolicy>

  <PolicyRequirementRule xsi:type="basic:AttributeRequesterString" value="https://sp2.example.org/shibboleth" />

  <AttributeRule attributeID="givenName">

    <PermitValueRule xsi:type="basic:ANY" />

  </AttributeRule>

  <AttributeRule attributeID="surName">

    <PermitValueRule xsi:type="basic:ANY" />

  </AttributeRule>

  <AttributeRule attributeID="uid">

    <PermitValueRule xsi:type="basic:ANY" />

  </AttributeRule>

  ..jatkuu
```

Attribuutit



- Lisää testi SP:lle attribuuttien rilisointisääntö:

```
<AttributeRule attributeID="commonName">
    <PermitValueRule xsi:type="basic:ANY" />
</AttributeRule>
<AttributeRule attributeID="eduPersonAffiliation">
    <PermitValueRule xsi:type="basic:ANY" />
</AttributeRule>
</AttributeFilterPolicy>
```

- Uudelleenkäynnistä Idp
- Mene selaimella sivun <https://sp2.example.org/secure/> kautta tutkimaan attribuuttejasi.. Tulivatko kaikki perille SP:lle?
- Lisätehtävä: Korjaa attribuuttimääritelmät siten että kaikki rilisoidut attribuutit saapuvat SP:lle.