SWAMID

# Shibboleth SP-installation

## Linux Redhat, CentOS, SUSE med Apache httpd

## Windows Server med IIS7

# Länkar till beskrivning av installation

Grundmaterialet för hur man installerar en Shibboleth SP finns här:

- https://wiki.shibboleth.net/confluence/display/SHIB2/Installation
- https://wiki.swamid.se/pages/viewpage.action?pageId=31201449

På dessa platser hittar man också en massa tips och trix för att kunna installera på plattformar som inte täcks i denna webinar.

# Linux-installation (Rhel, CentOS, SUSE)

- Shibboleth stöder bara installation på ovanstående OS-distributioner, men det går utmärkt att installera på ex.vis ubuntu, debian etc.
- Jag har valt att redovisa hur man kan installera shibboleth ”out of the box” (rpm och yum) med RHEL6 64-bitars och apache httpd 2.x
- Man bör notera att RHEL6.x (och CentOS6.x) inte har en för shibboleth fungerande libcurl-version. Installationen kommer att skapa ett bibliotek med en fungerande libcurl i /opt/shibboleth/-katalogen
- Denna installation fungerar inte om man har SELinux ”enforced” (standard i RHEL, CentOS), sätt den i disabled eller permissive.

# Installera…

- Installera httpd med yum:
  # yum install httpd.x86_64
  # yum install mod_ssl
- Installera repos:
  # wget -P /etc/yum.repos.d
  http://download.opensuse.org/repositories/security://shibboleth/RHEL_6/security:shibboleth.repo
- Installera senaste shibboleth:
  # yum install shibboleth.x86_64
- KLART – Resten är konfiguration av httpd och shibboleth2, den senare är samma för windows så det tar vi sen

# Konfigurera apache httpd 2.x

Installeras Shibboleth med yum, så kommer automatiskt Apache-modulen mod_shib att installeras och aktiveras.

Det som sedan behöver göras är att ta reda på hur den aktuella tjänsten behöver skyddas:

1. Ska hela siten skyddas, så att ingen del an tjänsten är tillgänglig utan inloggning?

2. Ska en viss del (path) av siten skyddas, så att vissa delar av tjänsten kan besökas utan inloggning, medan en viss del kommer kräva inloggning?

I din <VirtualHost> lägger du till en <Location>-tagg för det du vill skydda (/etc/httpd/conf.d/shib.conf):

```
<Location />
        AuthType shibboleth
        ShibRequestSetting requireSession 1
        Require valid-user
</Location>
```

Det som behöver ändras baserat på hur tjänsten ska skyddas är vilken path man anger. Vid alternativ 1 och 2, anger man root-pathen (som i exemplet) eller den path som ska skyddas

# Konfigurera apache httpd (forts.)

- **Inloggningshantering i Tjänsten/Applikationen**
- Inloggningsinformation (användarnamn och ev. namn eller andra attribut om den inloggade användaren) sätts som HTTP-variabler av Apache. Om hela eller en viss del av siten är skyddad och applikationen endast kräver en lyckad inloggning, behöver inget speciellt göras. Inloggningen hanteras då av Shibboleth och mod_shib i Apachen, innan applikationen görs tillgänglig.
- Om applikationen däremot behöver veta användarnamn eller andra attribut-värden, måste alla sidor som kräver inloggning, kunna läsa de aktuella HTTP-variablerna.
- http environment eller http headers
- Olika tjänster vill få översända attribut levererade på olika sätt, ex.vis kommer java-applikationer att ta emot http omgivningsvariabler, medan exempelvis php-applikationer behöver få variablerna levererade som http headers. I den av shibbolethinstallationen skapade shib.conf kan man lägga till:

  ShibUseHeaders On

  för att få attributen levererade som http headers.

# Windows Server med IIS7

- Det finns installationsanvisningar för andra versioner av IIS under: https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPWindowsInstall
- Där finns också anvisningar om man vill köra apache httpd som webserverver
- Jag har valt att redovisa hur man kan installera shibboleth om man redan har IIS 7 installerad på en 64-bitars windows server
- Nuvarande versioner av shibboleth installationsprogram kräver att man har satt kompatibilitet med IIS 6
- Installationen måste tyvärr avslutas med att man bootar om servern, varför det är bra att planera insatsen om det är så att servern tjänar flera andra tjänster/applikationer.

# Installera..

- Först måste man göra IIS beredd att kunna hanteras av installationsprogrammet. Om man inte gör det måste man göra IIS-inställningarna manuellt:
- I IIS Management Console:
  disable IIS "Shared Configuration” option
  installera alla "IIS 6 Management Compatibility”
- Hämta shibboleth-sp-2.5.3-win64.msi från http://shibboleth.net/downloads/service-provider/latest/win64/ och kör installation. Svara ja på frågan om ISAPI skall konfigueras. Avsluta med omstart.
- KLART! Nu återstår bara att konfigurera shibboleth!

# Konfiguration av shibboleth SP

- Om man har installerat enligt ovan, så finns shibboleth på /etc/shibboleth för linux och på c:\opt\shibboleth\etc\shibboleth för windows. Dessa defaults kan ändras under installation.
- De filer man behöver konfigurera är attribute-map.xml och shibboleth2.xml
- Om man hämtar IdP-metadata från SWAMID måste man också hämta ned SWAMIDs ”signer-cert”

# attribute-map.xml

SWAMID rekommenderar att alla bortkommenderade attribut i attribute-map.xml görs tillgängliga, samt att man lägger till norEdu-attributen.

Ta bort kommentaren kring de två sista attribut-blocken under texterna:

”Some more eduPerson attributes...” samt ” Examples of LDAP-based attributes...”.

norEdu-attributen kan hämtas här:

- https://wiki.swamid.se/pages/viewpage.action?pageId=31201547

# norEdu-attributen

```
<Attribute name="urn:mace:dir:attribute-def:norEduPersonLegalName" id="norEduPersonLegalName"/>
<Attribute name="urn:mace:dir:attribute-def:norEduPersonNIN" id="norEduPersonNIN"/>
<Attribute name="urn:mace:dir:attribute-def:norEduPersonLIN" id="norEduPersonLIN"/>
<Attribute name="urn:mace:dir:attribute-def:norEduOrgAcronym" id="norEduOrgAcronym"/>
<Attribute name="urn:mace:dir:attribute-def:norEduPersonBirthDate" id="norEduPersonBirthDate"/>
<Attribute name="urn:mace:dir:attribute-def:norEduOrgUniqueIdentifier" id="norEduOrgUniqueIdentifier"/>
<Attribute name="urn:mace:dir:attribute-def:norEduOrgUnitUniqueIdentifier" id="norEduOrgUnitUniqueIdentifier"/>
<Attribute name="urn:mace:dir:attribute-def:norEduOrgNIN" id="norEduOrgNIN"/>
<Attribute name="urn:mace:dir:attribute-def:norEduOrgUniqueNumber" id="norEduOrgUniqueNumber"/>
<Attribute name="urn:mace:dir:attribute-def:norEduOrgUnitUniqueNumber" id="norEduOrgUnitUniqueNumber"/>

<Attribute name="urn:oid:1.3.6.1.4.1.2428.90.1.10" id="norEduPersonLegalName"/>
<Attribute name="urn:oid:1.3.6.1.4.1.2428.90.1.5" id="norEduPersonNIN"/>
<Attribute name="urn:oid:1.3.6.1.4.1.2428.90.1.4" id="norEduPersonLIN"/>
<Attribute name="urn:oid:1.3.6.1.4.1.2428.90.1.6" id="norEduOrgAcronym"/>
<Attribute name="urn:oid:1.3.6.1.4.1.2428.90.1.3" id="norEduPersonBirthDate"/>
<Attribute name="urn:oid:1.3.6.1.4.1.2428.90.1.7" id="norEduOrgUniqueIdentifier"/>
<Attribute name="urn:oid:1.3.6.1.4.1.2428.90.1.8" id="norEduOrgUnitUniqueIdentifier"/>
<Attribute name="urn:oid:1.3.6.1.4.1.2428.90.1.12" id="norEduOrgNIN"/>
<Attribute name="urn:oid:1.3.6.1.4.1.2428.90.1.1" id="norEduOrgUniqueNumber"/>
<Attribute name="urn:oid:1.3.6.1.4.1.2428.90.1.2" id="norEduOrgUnitUniqueNumber"/>
<Attribute  name="urn:oid:1.3.6.1.4.1.25178.1.2.9" id="schacHomeOrganization" />
```

# shibboleth2.xml

- Detta är den centrala konfigurationsfilen för din shibboleth-installation
- För att konfigurera shibboleth2.xml behöver du veta följande:
- Vilken IdP eller DS som SP:n skall återpeka användaren till för autentisiering (och attributöverföring)
- Var metadata för IdP(erna) skall hämtas
- Hur dessa metadata är signerade

# Shibboleth2.xml forts.. 1

- Sök upp:
  <ApplicationDefaults entityID=https://sp.example.org/shibboleth
  REMOTE_USER="eppn persistent-id targeted-id">
- Ändra till SP:ns maskinnamn
- I windows tillkommer taggarna:
  <Site id="1" name="sp.example.org"/>
  och
  <Host name="sp.example.org"
  <Path name="secure" authType="shibboleth" requireSession="true"/>
- Ändra dem så shibboleth skickar till rätt applikation!

# Shibboleth2.xml forts.. 2

- Om du registrerar din SP hos SWAMID och vill använda SWAMIDs DS (Discovery Service) för val av IdP skall du kommentera bort elementet som börjar med:
  <SSO entityID…
- Och i stället lägga till en SessionInitator (exemplet förutsätter att du registrerat dina metadata i SWAMIDs testmetadataström):

```
<SessionInitiator type="Chaining" Location="/DS/ds-test.swamid.se" id="ds-test.swamid.se-DS" relayState="cookie">
<SessionInitiator type="SAML2" defaultACSIndex="1" acsByIndex="false" template="bindingTemplate.html"/>
<SessionInitiator type="Shib1" defaultACSIndex="5"/>
<SessionInitiator type="SAMLDS" URL="http://ds-test.swamid.se/role/idp.ds"/>
</SessionInitiator>
```

I annat fall lägger du in din IdP:s URL i <SSO entityID… i stället för idp.example.org/…

# Shibboleth2.xml forts.. 3

- I Sessions-taggen, sätt handlerSSL=”true” och cookieProps=”https”
- Lägg till SWAMID som metadata provider:

```
<!-- SWAMID Metadata -->
        <MetadataProvider
                type="XML"
                uri="http://md.swamid.se/md/swamid-idp-transitive.xml "
                backingFilePath=”swamid-metadata.xml" reloadInterval="300">
            <SignatureMetadataFilter certificate="swamid-signer.crt"/>
    </MetadataProvider>
```

# Konfiguration av shibboleth SP – sista detaljen

- Nu återstår bara en sak – att hämta SWAMIDs ”signer-cert” och lägga det där du angav i shibboleth2.xml (i exemplet ”swamid-signer.crt”)
- Linux:
  # wget -O /etc/shibboleth/swamid-signer.crt https://md.swamid.se/md/md-signer.crt
- Windows:
  Öppna en browser och hämta certifikatet på md.swamid.se/md/md-signer.crt. Lägg det som md-signer.crt på c:\opt\shibboleth\etc\shibboleth

# Till sist..

- Starta om allt och se att det fungerar… ☺
- Nu skall du kunna hämta metadata genom: https://tjänst.xx.se/Shibboleth.sso/Metadata
- Titta på metadata – ser det konstigt ut, måste du kanske starta om webservern och försöka igen
- Skicka in metadata till operations@swamid.se tillsammans med uppgift om önskad entitetskategori och MDUI-information (Se wiki.swamid.se)

# Slut för idag

- Frågor?
  - Fråga oss nu
  - Skicka frågor till operations@swamid.se
  - Skicka frågor eller ring någon i SWAMID operations
- Glöm inte att komma på SWAMIDs första workshop för året i Uppsala den 17-18/3!!!!
- Har du någon intressant fråga att diskutera i openspace den 18/3??