Shibboleth Identity Provider 3 on Windows

Nedan beskrivs installation av Shibboleth IdP på en Windows-miljö, direkt kopplad mot ett Active Directory. Standardbrandvägg med öppning för 443 och 8443.

Installera Shibboleth-IdP

Följ instruktionerna på Shibboleth-wikin: https://shibboleth.atlassian.net/wiki/spaces/IDP4/pages/1265631507/WindowsInstallation

Konfigurera Shibboleth IdP

Följ konfigurationsanvisningarna på SAML IdP Best Current Practice och anpassa filsökvägar där det behövs.

Logfiler

- Loggar för Shibboleth IdP:n hamnar i C:\Program Files (x86)\Shibboleth\IdP\logs
- Loggar för Jetty hamnar i C:\Program Files (x86)\Shibboleth\Jetty\logs

Vanliga fel

idp-process.log: Could not negotiate TLS connection, unable to find valid certification path to requested target

Detta betyder att SSL-uppkopplingen mot AD:t/LDAP:en misslyckades. En trolig orsak är att AD:ts/LDAP:ens certifikat inte är signerat av för JRE:n en betrodd part. För att lösa detta behöver AD:ts/LDAP:ens certifikat läggas in i en certifikatsfil.

Skapa filen "credentials/ldap-server.crt" och lägg in samtliga certifikat för servrarna i den. Se kommandon för att hämta certifikaten nedan.

Lägg till följande rad i filen conf/ldap.properties

```
idp.authn.LDAP.trustCertificates= %{idp.home}/credentials/ldap-server.crt
```

Flera AD-servrar med olika certifikat

Typiskt så har man flera AD-servrar i ett AD, exvis adserver1.hsk.se, adserver2.hsk.se, osv. Då har man ofta ett dns-entry, exvis ad.hsk.se, som pekar ut ad-servrarna med round-robin. Java kräver dock att certifikatet matchar servernamnet man anropar, så anropar man ad.hsk.se så måste certifikatet vara utställt på ad.hsk.se, inte adserver1.hsk.se. Enklaste lösningen är att välja en av AD-servrarna och bara peka ut den, nackdelen är att redundansen påverkas. AD-/LDAP-server konfigurerar man i dessa filer:

C:Program Files (x86)Internet2Shib2IdPconfattribute-resolver.xml

```
ldapURL="ldap://adserver1.hsk.se"
```

C:Program Files (x86)Internet2Shib2IdPconflogin.config

```
host="adserver1.hsk.se"
```

Okänt certifikat för LDAP:en

Om CN för certifikatet som AD/LDAP-servern presenterar inte matchar servernamnet du angett i attribute-resolver.xml och login.xml så kommer ett felmeddelande skrivas i idp-process.log. Lättast sättet att lista ut CN för certifikatet är att köra följande OpenSSL-kommande (installera först OpenSSL):

```
openssl s_client -connect <ldap-servernamn>:636
```

Man kan också köra dessa PowerShell-kommandon:

```
# Ange servernamn och port
$hostname = "ad.hsk.se"
$port = 636

# Anslut till servern och hämta certifikatet
$socket = New-Object Net.Sockets.TcpClient($hostname, $port)
$sslStream = New-Object System.Net.Security.SslStream $socket.getStream(),$false,{$true}
$sslStream.AuthenticateAsClient($null)
$cert = $sslStream.RemoteCertificate

# Skriv ut subject för certifikatet (CN)
$cert.Subject

# Konvertera certifikatet till DER-format
$certData = $cert.Export([System.Security.Cryptography.X509Certificates.X509ContentType]::Cert)

# Skriv ut certifikatet i fil
Set-Content -value $certData -Encoding byte -Path "cert.cer"

# Konvertera certifikatet till PKCS12-format
$certData = $cert.Export([System.Security.Cryptography.X509Certificates.X509ContentType]::Pkcs12)

# Skriv ut certifikatet i fil
Set-Content -value $certData -Encoding byte -Path "cert.p12"
```

Om certifikatet inte är signerad av en för JRE:n känd CA så behöver certifikatet läggas in i filen "credentials/ldap-server.crt", se ovan.

Inloggning misslyckas

Verifiera att baseDN i attribute-resolver.xml och login.config matchar strukturen i AD:t/LDAP:en. Default i AD är "CN=Users,DC=<domain>". Om man skapat ett OU som heter Person där man lägger alla användare så blir det istället "OU=Person,DC=<domain>". Det är också viktigt att man ser till att den användare som man använder för att autentisiera mot AD endast är en läsanvändare och inte en Domain Admin eller dylikt då lösenordet sparas i klartext på IdP-servern.

Starta om Shibboleth IdP

Shibboleth IdP läggs in som en tjänst i Windows, "Shibboleth 3 IdP Daemon". Den startas om i Kontrollpanelen - Administrative Tools - Services.

Publikt SSL-servercertifikat

Vid installationen automatgenereras ett självsignerat servercertifikat:

```
C:/Program Files (x86)/Shibboleth/IdP/credentials/idp-userfacing.p12
```

Detta anges i jetty-konfigurationen:

```
C:\Program Files (x86)\Shibboleth\IdP\jetty-base\start.d\idp.ini
```

JKS-filer hanteras av keytool som följer med Java JRE. För att importera ett befintligt certifikat med keytool behövs en p12-fil.

Skapa en PKCS12-fil (.p12, ibland döpt till .pfx)

Installera OpenSSL: http://www.openssl.org/related/binaries.html
Infiler:

cert.pem (ditt publika certifikat)

```
-----BEGIN CERTIFICATE-----
MIIC8TCCAdmgAwIBAgIJAOX3ZFUcjIISMA0GCSqGSIb3DQEBBQUAMA8xDTALBgNV
BAMMBHRlc3QwHhcNMTMwODA3MTIwNDA2WhcNMjMwODA1MTIwNDA2WjAPMQ0wCwYD
...
-----END CERTIFICATE-----
```

cert.key (din privata nyckel)

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAy0LvhsBvy922azM1wUTr17bNXoizoV2wS7k+sBjMZsKTBiLP
PNxHCSvnj7QatT7u3Na41e9pS8qL6QzCx8QbQrPpNOvTWGGqQ2fASGN5AcdV3iFx
...
-----END RSA PRIVATE KEY-----
```

ca.pem (alla certifikat i certifikatkedjan som signerat ditt certifikat)

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAdegAwIBAgIJALku0Pbyo44vMA0GCSqGSIb3DQEBBQUAMA4xDDAKBgNV
BAMMA2NhMTAeFw0xMzA4MDcxMjA0MDlaFw0yMzA4MDUxMjA0MDlaMA4xDDAKBgNV
...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIC7zCCAdegAwIBAgIJAM5c+U+BIBtvMA0GCSqGSIb3DQEBBQUAMA4xDDAKBgNV
dvdU1Z+4x8cbidSKZbpLa0VjdepZ2kQrnidAcnvC5wfWlYFWcwvIdTxqNCTnRtg9
...
-----END CERTIFICATE-----
```

```
openssl pkcs12 -export -in cert.pem -inkey cert.key -certfile ca.pem -passout pass:secretpassword1 -name mycert
-out cert.p12
```

Skapa en JKS-fil från en p12-fil

```
"%JAVA_HOME%\bin\keytool" -importkeystore -deststorepass secretpassword2 -destkeypass secretpassword2 -
destkeystore cert.jks -srckeystore cert.p12 -srcstoretype PKCS12 -srcstorepass secretpassword1 -alias mycert
```

Efter installationen

Ladda upp metadata till federationen

Metadata för IdP:n genereras automatiskt under installationen och hamnar i

```
C:\Program Files (x86)\Internet2\Shib2IdP\metadata\idp-metadata.xml
```

Denna ska skickas till federationsadministratören (operations@swamid.se)

Konfigurera metadata för att använda SWAMID

IdP:n behöver konfigureras för att hämta ner SWAMID:s metadata så den kan kommunicera med Service Providers i SWAMID.

- Konfigurera metadatahämtning i Shibboleth Identity Provider för SAML

Lägg till svenska som språk i Shibboleth

- Du gör Shibboleth enkelt tvåspråkig genom att installera svenska språkfiler.

Uppdatera attribute-resolver.xml enligt rekommendationer

- Example of a standard attribute resolver for Shibboleth IdP v4 and above

Lägg till release av statisk organisationsinformation

- Rekommenderad release av statisk organisationsinformation

Lägg in attributfilter för entitetskategorier

- Example of a standard attribute filter for Shibboleth IdP v4 and above

SAML f-ticks for Shibboleth

- SAML f-ticks for Shibboleth