



Stockholms
universitet

Shibboleth IDP och ADFS + Sharepoint integration

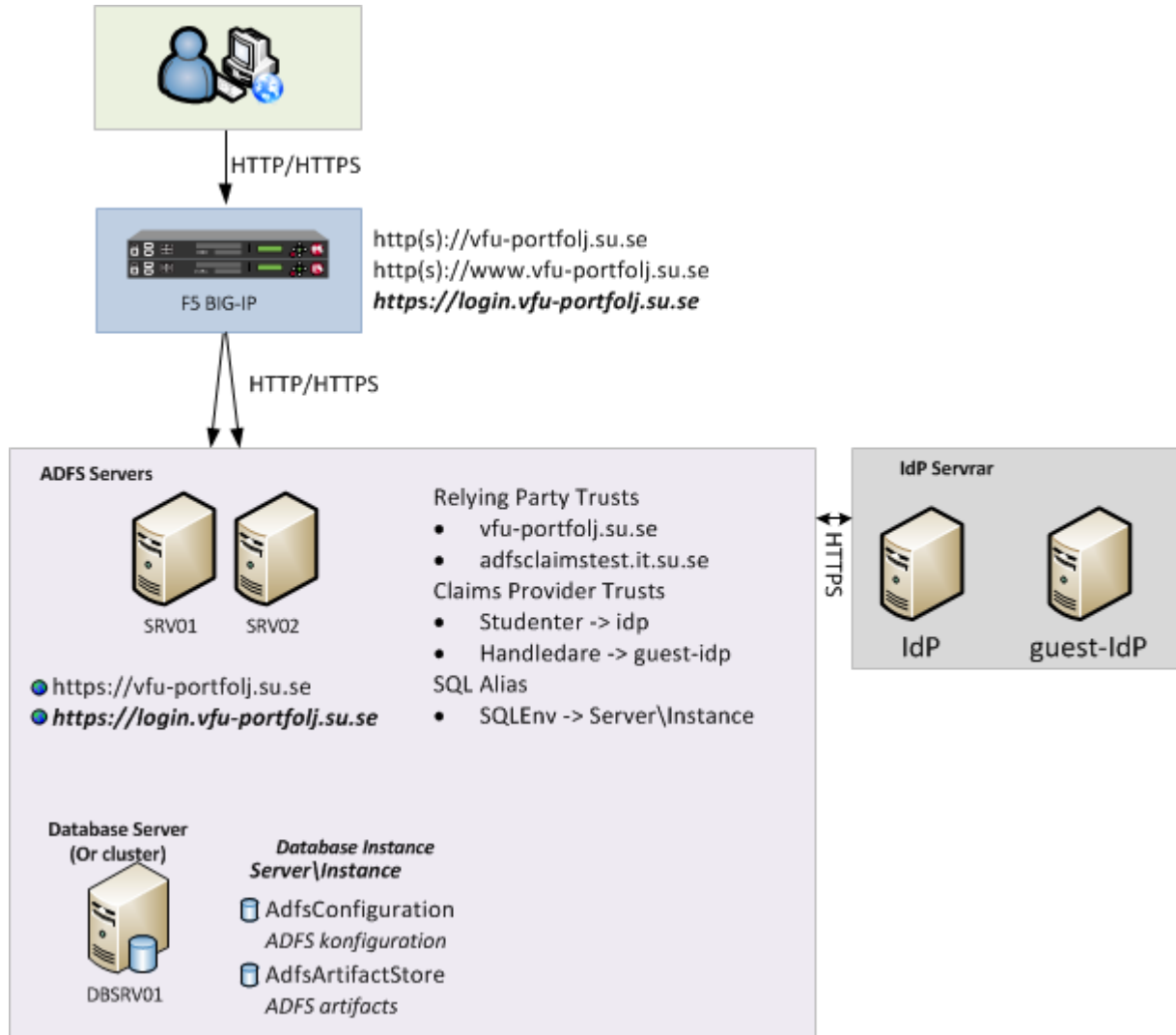
Terminologi

Shibboleth	ADFS
Identity Provider	Claims Provider
Attribut Release	Claims Provider Trust
Attribute map	Claim Rules
Service Provider	Relying Party
Sharepoint	Vad?
Trusted Identity Provider	ADFS RP som Sharepoint litar på

Arbetsgång

1. Lägga till vår(a) IDP(er) som Claims Provider(s)
2. Lägga till Claims Rules för Claims Provider Trust
3. Konfigurera Sharepoint som en Relying Party
4. Konfigurera Trusted Identity Provider i Sharepoint
5. Lägga till ADFS Relying Party i vårt Metadata
6. Släppa attribut från IDP till ADFS Relying Party

Översikt



Lägga till vår(a) IDP(er) som Claims Provider(s)

IDP'erna läggs in som Claims Providers via ADFS Powershell snap-in alternativt via ADFS GUI.

Vi har valt att köra allt med Powershell iom att vi även gör installation på detta vis då iom att vi valde en ADFS farm för redundans

Exempel via Powershell:

```
Add-PSSnapIn Microsoft.Adfs.PowerShell
```

```
Add-ADFSClaimsProviderTrust -Name 'Lärare och Studenter' -MetadataURL 'https://$FQDN/idp/profile/Metadata/SAML'  
-SigningCertificateRevocationCheck "None" -SignatureAlgorithm http://www.w3.org/2000/09/xmldsig#rsa-sha1
```

Lägga till Claims Rules för Claims Provider Trust

Vi har lagt in samtliga Claim Rules baserat på "Send Claims Using a Custom Rule" templatén.

Exempel för ePPN to UPN:

```
@RuleName = "ePPN to UPN"  
c:[Type == "urn:oid:1.3.6.1.4.1.5923.1.1.1.6"]  
=> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn", Issuer = c.Issuer,  
OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType);
```

Alt via GUI

```
Rule template: Send Claims Using a Custom Rule  
Custom rule:  
c:[Type == "urn:oid:1.3.6.1.4.1.5923.1.1.1.6"]  
=> issue(Type =  
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn", Issuer =  
c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType  
= c.ValueType);
```

Konfigurera Sharepoint som en Relying Party i ADFS

Konfiguration av ADFS för att släppa claims från ADFS till SharePoint
Applikationen konfigureras via GUI->Trust Relationships->Relying Party Trusts
Alternativt som vi har valt, att göra det via PowerShell
Applikationen läggs upp med identifierns:

Identifiers:

https://\$FQDN/

https://\$FQDN/_trust/

urn:sharepoint:\$FQDN (SharePoint är valfritt namn)

Resp Claim Rule läggs för den Relying partnern - lägg upp med "Pass through all claims values",
via GUI eller Powershell ex:

```
@RuleTemplate = "PassThroughClaims"
```

```
@RuleName = "ePPN to UPN"
```

```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"]
```

```
=> issue(claim = c);
```

Konfigurera SharePoint för att se ADFS som en Trusted Identity Provider.

1. Token Signing certifikatet från ADFS, exporteras till ett lämpligt share
 2. Lägg till certifikatet som en Trusted Root Authority i SharePoint
 3. Lägg in providern genom SharePoints Management Shell genom
SPClaimTypeMapping – Mapper inlagda claims
- Cert – Certifikatet för Token signing
Realm – urn:sharepoint:\$FQDN
Signinurl – Till ADFS (i vårt fall [https://\\$FQDN/adfs/ls](https://$FQDN/adfs/ls))
New-SPTtrustedIdentityTokenIssuer – för att lägga in samtliga värden ovan

Lägga till ADFS Relying Party i vårt Metadata

1. Hämta Metadatat från ADFS på URL `https://$FQDN/FederationMetadata/2007-06/FederationMetadata.xml`
2. Trimma/slimma metadatan (mha xsltproc och xmllint)
3. Lägga in den i vårt eget metadata (eller SWAMIDs)

Släppa attribut från IDP till ADFS Relying Party

På vanligt vis mha attribute-filter.xml

Länkar

AD FS 2.0 Step-by-Step and How To Guides

- Federated Collaboration with Shibboleth 2.0 and SharePoint 2010 Technologies
- AD FS 2.0 Step-by-Step Guide: Federation with Shibboleth 2 and the InCommon Federation

Demo

Logga in på vfu-portfoljen.su.se med SU-konto samt gästkonto.

Kontakt

Vid frågor/hjälp

SWAMID mailinglistan (så alla får ta del)
saml-admins@swamid.se

Direkt via mail/jabber
simlu@su.se stber@su.se