

Step 1:

contact Anass in private chat to be added in the test federation.

Step 2:

Check that your IdP is visible in the test federation:

```
https://vm-000069.vm.geant.org/rr3/signedmetadata/federation/Geant_Workshop/metadata.xml
```

Step 3:

Configure your IdP to trust the metadata from the test federation:

add the following just before the last line </MetadataProvider> :

```
# vim /opt/shibboleth-idp/conf/metadata-providers.xml

<MetadataProvider id="training-test-federation"
  xsi:type="FileBackedHTTPMetadataProvider"
  backingFile="%{idp.home}/metadata/training-test-federation.xml"
  metadataURL="https://vm-000069.vm.geant.org/rr3/signedmetadata/federation/Geant_Workshop/metadata.xml">

  <!-- Verify the signature on the root element of the metadata aggregate using a
  trusted metadata signing certificate. -->
  <MetadataFilter xsi:type="SignatureValidation" requireSignedRoot="true" certificateFi
  le="%{idp.home}/metadata/training-test-federation-cert.crt"/>

  <!-- Require a validUntil XML attribute on the root element and make sure its value
  is no more than 10 days into the future. -->
  <MetadataFilter xsi:type="RequiredValidUntil" maxValidityInterval="P10D"/>

  <!-- Consume only SP in the metadata aggregate -->
  <MetadataFilter xsi:type="EntityRoleWhitelist">
    <RetainedRole>md:SPSSODescriptor</RetainedRole>
  </MetadataFilter>
</MetadataProvider>
```

Step 4:

To allow the IdP to verify the signature of the xml metadata, and ensure that this metadata file is provided by the federation operator, you need to add manually the certificate used to sign the metadata:

```
# vim /opt/shibboleth-idp/metadata/training-test-federation-cert.crt
```

```
-----BEGIN CERTIFICATE-----
MIIFizCCA30gAwIBAgIJALey6jcy9MznMA0GCSqGSIb3DQEBCwUAMFwxZzA0MDcx
BAYTAK1ZMQ0wCwYDVQQHDARDAXR5M0Q0wCwYDVQQKDAROUkVOMRMwEQYDVQQQLDAPG
ZWRlcmF0aW9uMR0wGAYDVQQDBDF3d3cuZmVkdXJhdGlvbi5teTAeFw0yMTA0MDcx
NzAxMDRaFw0zMTA0MDUxNzAxMDRaMFwxZzA0MDcxZzA0MDcxZzA0MDcxZzA0MDcx
aXR5M0Q0wCwYDVQQKDAROUkVOMRMwEQYDVQQQLDAPGZWRlcmF0aW9uMR0wGAYDVQQD
DBF3d3cuZmVkdXJhdGlvbi5teTCCAIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoC
ggIBAMOXL87SdapCEX69gPIS8HZLHrSz2LEyfcTgFsu4W0w6FavXkBVcm57p/Jtm
trJ/OpBmtJFB7NI3uiVihV0kNqbFvVjL4n765rVAik61IaUaWJNDY8Q/ht4nDzsU
fNM0Yxz0duMwA0HaL1tvdPe1JnHnbqzKP7jsiMxLCu/VXWTFQ0b75yKlrgayzbRu
89NSluEnZf90fEbefa/hwCEFrLcXySm/30wo+9M7zz/CWUuynWqvoNxbHb0dplk
IwwKmezE++cM/0R20+/Aqod+wK41xKTKd1xYU/++vM2An7PzxpWLD77LYj0pBVci
JMy/mNPk0c5zxcNZpcGxt1Ahk8kx6Xdbu24J8kihcx0Y1FNxTafJ80q88iUXmrE
xn52WQ2miVBQvoMef50PKf01wBISpT0bS9EuXps00YcsXCfzS952iuWot5ZhXlWp
E25kDDkXq1u+N0Tylxc6yE8z7A45b8u/ZeZ9r3vJdTH1NzZ8cwQmQigXM2SujtuE
fP22Yj3t63sidPcg30vC1kUjDBjfRplwoK3EmPeOIiPPtyMXQL2L/Ayd3NADdWch
s3RH1g0+4gJ9CiiB6u/VXpPi51jIvFHU1yZKXhVBXePLhqaSnBqUFMNAWRsWOrgT
YXkUwfrCkoXmvEE/V5X/HBpS3QunE50QxJvQI0zFRAAvNy9tAgMBAAGjUDBOMB0G
A1UdDgQWBBRbo1eRZ3l0J6zyhAdSXj8nyt5s6DAfBgNVHSMEGDAWgBRbo1eRZ3l0
J6zyhAdSXj8nyt5s6DAMBGNVHRMEBTADAQH/MA0GCSqGSIb3DQEBCwUAA4ICAQB1
fCy5J7b9qRY4a4zjJHniw5rx79/f9fAUX25t7QP+Z5RjGcn/DT0+GVp16Z9pPK+8
9oc4e46zW6v7CF07y5BuJYRMA8hFgVxhGa0vS0WLYTJzpn1EyHob1d8jBFDUukB
FazSNgsdqATKw19AnTa4pIwf2jUNBhgLG8+qgXk6PZ5MD5q2LLUbwIhpDM3yNpaU
Iu8X7cqAZJ9gW/ozbDD0AnQwXfIm6MRdfT3CJ7EdupG6mSB+K3UoJqL+gS6nBuY
LhSgWj18VZ0cij7S8L+YmWNjfsTYQZLRjNMGhqtWley+F9SvrLUueuk9r2wD0
kFgjNESkz1tkyWA2MFYSTxJWesxcmJ29gTaZLbewe44vMahEcTo/wSxmjJ30A7bv
zb/gcSBLJhwM7w67hqlJki8g9rJiV00pggH0j f5qBIFnMrNBb2FDu0MyRvc2JFL7
eITTUzWpEzBp1LME6fFWTNHWEjqqV15eL0NFubp6Ydzjbo+Zz81CmX6X0bZ7UtHB
24S4x7++RLxj7K1DkzVb8rELws1SI6xtZeGbxZnpkH5VpUvWhYgS1VXX2/SI1/XT
Cv7ry5A/W0iAptKBR+E7lnNYd+m5WSYMiDkCOV5LuhFsbZi86HkQBZ0dlf1SAuQF
wWTLbUcrboFUPTsSdDgqhb2SYp2vKBKcabtYdk+a+w==
-----END CERTIFICATE-----
```

Step 5:

Now that your IdP is configured to trust the test federation, you need to choose which attributes your IdP is authorized to send to services registered in the test federation. Configure the IdP to release the `eduPersonPrincipalName` attribute for this test federation. It means the IdP will release the `eduPersonPrincipalName` to all SPs that are registered in the test federation .

add the following before the last line `</AttributeFilterPolicyGroup>` :

```
# vim /opt/shibboleth-idp/conf/attribute-filter.xml

<AttributeFilterPolicy id="releaseToAllSPsInTestFederation">
  <PolicyRequirementRule xsi:type="InEntityGroup" groupID="https://vm-000069.vm.geant.org/rr3" />
  <AttributeRule attributeID="eduPersonPrincipalName" permitAny="true" />
</AttributeFilterPolicy>
```

Step 6:

Restart Jetty

```
# systemctl restart jetty.service
```

Step 7:

check in the logs if everything is going well :

```
tail -f /opt/shibboleth-idp/logs/idp-process.log
```

Step 8:

Access the test service "myBlog". Login with shibboleth and choose your IdP:

`http://vm-000063.vm.geant.org/myBlog/`

You should see that you are logged in as your "`eduPersonPrincipalName`" value.

Example:

Logged in as `user1@vm.geant.org`

liste des billets

[liste des billets](#) | [écrire un billet](#) | [logout](#)

powered by myBlog