Keycloak & umbrellaID integration

European Synchrotron Radiation Facility

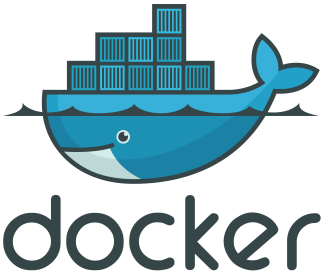
February 4th 2021

Docker

Keycloack

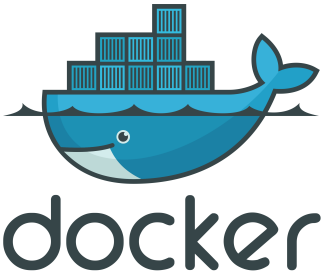
umbrellaID integration

Useful tools to debug SAML



- For the workshop
- Fast deployment
- Easy upgrade of Keycloak
- Not OS dependent
- True database ready-to-go
  - The Keycloak default one is an H2 embedded one
  - Not performant at all (SQLite like)

ESRF



- Can be installed without Docker to fits your needs
- Bare-metal : `https://www.keycloak.org/getting-started/getting-started-zip`
- Other : `https://www.keycloak.org/getting-started`

ESRF

Docker installation on Debian 10

```
[root@keycloak-demo]# apt-get update
[root@keycloak-demo]# apt-get install \
                        apt-transport-https \
                        ca-certificates curl \
                        gnupg-agent software-properties-common
[root@keycloak-demo]# curl -fsSL https://download.docker.com/linux/debian/gpg | apt-key add -
[root@keycloak-demo]# add-apt-repository \
                        "deb [arch=amd64] https://download.docker.com/linux/debian \
                        $(lsb_release -cs) \
                        stable"
[root@keycloak-demo]# apt-get update
[root@keycloak-demo]# apt-get install docker-ce docker-ce-cli containerd.io
```

Ubuntu : s/debian/ubuntu/g

Source : https://docs.docker.com/engine/install/debian/

Checking

```
[root@keycloak-demo]# docker version
Client: Docker Engine - Community
[...]

Server: Docker Engine - Community
 Engine:
  Version:          20.10.2
  API version:      1.41 (minimum version 1.12)
  Go version:       go1.13.15
  Git commit:       8891c58
  Built:            Mon Dec 28 16:15:28 2020
  OS/Arch:          linux/amd64
  Experimental:     false
[...]
```

Docker-compose installation

```
[root@keycloak-demo]# curl -L "https://github.com/docker/compose/releases/download/1.28.0/docker-compose-$(uname -s)-$(uname -m)" \
                      -o /usr/bin/docker-compose
[root@keycloak-demo]# chmod +x /usr/bin/docker-compose
[root@keycloak-demo]# docker-compose -v
docker-compose version 1.28.0, build d02a7b1a
```

Source : https://docs.docker.com/compose/install/

- You will need
  - A public domain name
  - Your machine exposed (or behind a reverse-proxy)
  - A valid SSL certificate for your domain

ESRF

- You will need
  - A public domain name
  - Your machine exposed (or behind a reverse-proxy)
  - A valid SSL certificate for your domain
- optionnaly
  - A LDAP directory
  - An AD one
- if any, you can create local users

ESRF

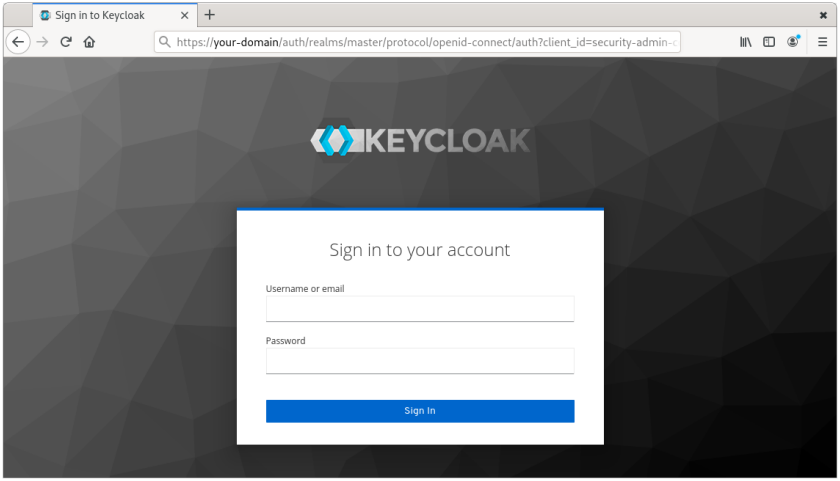
Starting Keycloak

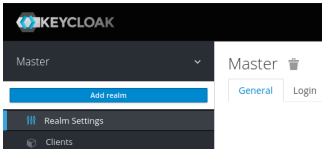
```
[root@keycloak-demo]# mkdir keycloak
[root@keycloak-demo]# cd keycloak
[root@keycloak-demo]# wget "https://gitlab.esrf.fr/anroux/panosc-keycloak-howto/-/raw/master/docker-compose.yml"
[you can customize the compose-file, by example ... the admin password!]
[put your certs in tls.crt and tls.key]
[root@keycloak-demo]# docker-compose up -d

[to see the logs in live, use]
[root@keycloak-demo]# docker-compose logs -f
```

That's all, wait until the service starts and you can browse `https://your-domain/auth/admin/`

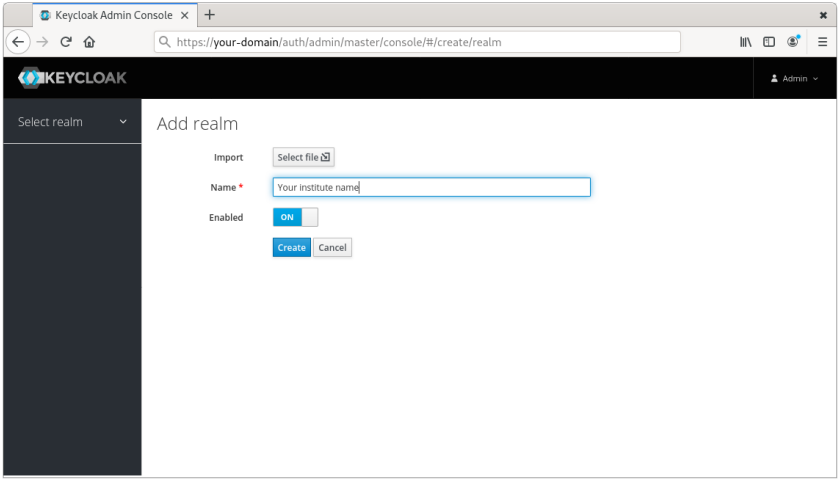
Login page


Sign in to Keycloak
https://your-domain/auth/realms/master/protocol/openid-connect/auth?client_id=security-admin-
KEYCLOAK
Sign in to your account
Username or email
Password
Sign In

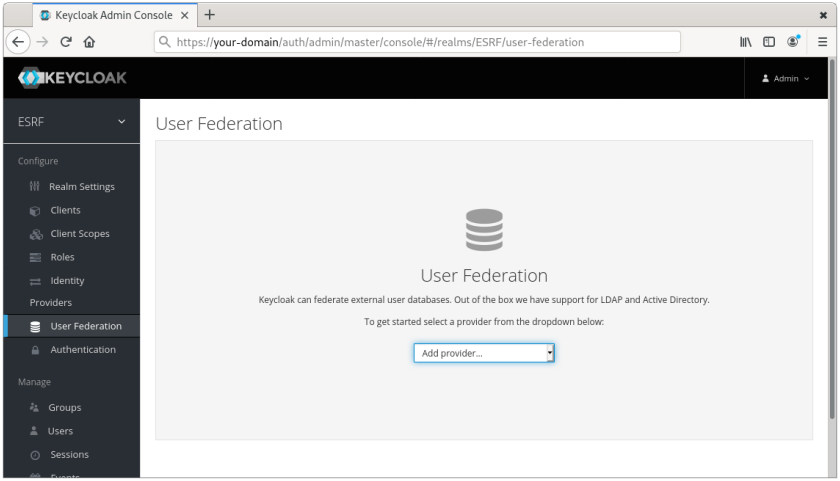


- Create a dedicated realm
  - The master realm is here for Keycloak's internals, do not use it !
  - Name it with the name of your institute

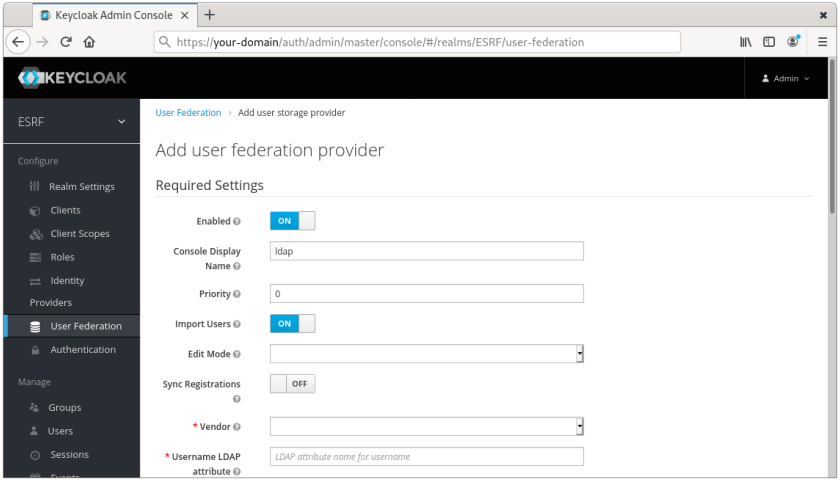
Realm creation



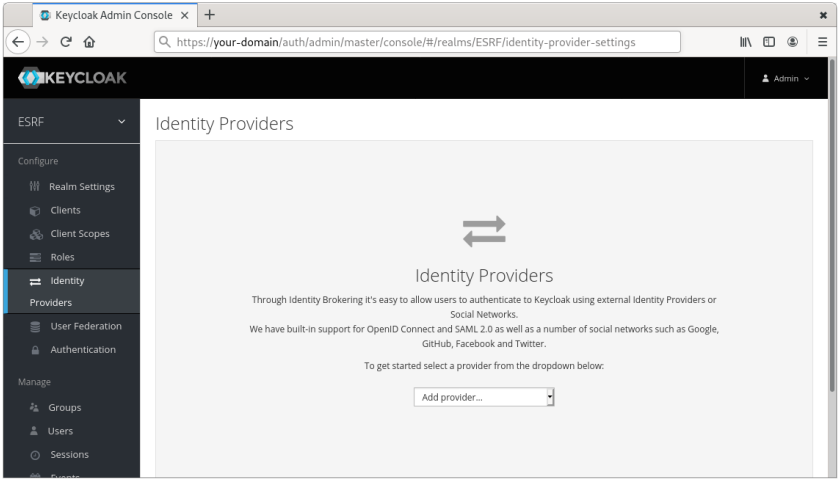
Add a user database (not mandatory)



Fill the form to fit your local infra



Add an Identity Provider



umbrellaID configuration (SAML)

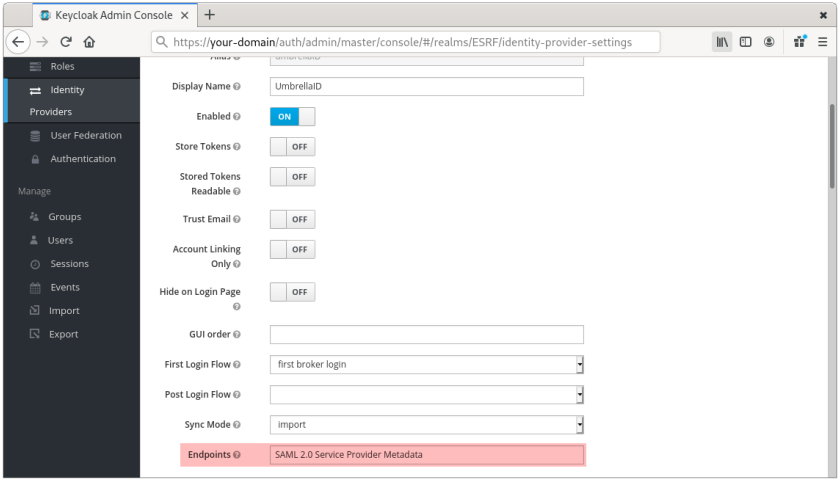
- SSO Service URL
  - `https://proxy.umbrellaid.org/saml2sp/sso/post`
- HTTP-POST Binding Response : `True`
- HTTP-POST Binding for AuthnRequest : `True`
- Want AuthnRequests Signed : `True`
- Validate Signature : `True`

umbrellaID certificate

```
-----BEGIN CERTIFICATE-----
MIIC5DCCAcwCCQCDHiNiZPpPhTANBgkqhkiG9w0BAQsFADAOMTIwMAYDVQQDDCl1
bWJyZWxsYWlkIHByb2QgcHJveHkgc2FtbF9wcm94eV9mcm9udGVuZDAeFw0xOTA5
MTcxNjQ0NDVaFw0yOTA5MTQxNjQ0NDVaMDQxMjAwBgNVBAMMKXVtYnJlbGxhaWQg
cHJvZCBwcm94eSBzYW1sX3Byb3h5X2Zyb250ZW5kMIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEAxCF5q0f4HB4oaE/naU3LPfyy9bXwYkONoBvA/AUMqNJt
XDsOgmkqSweIEhdVKTK1fHRK3mSq5ydFywwmF1GpKS1pAxwcvLdCVqHtX7kLoLZm
KzCbuEXaOgDU5asK+JY1KNIM/nDz3MxGqSSYnZgNv/NijT2HFr+f35awkbLxyGyk
2UVWIzH8p77/TrreVg9hjlfzllJOfiznBurTXtAOEjNsfPOJktiEX+doftXID2lv
zA+ebQj2kBc/jzTOl4bHBiofhIn+J5kQh9vtqLEWqYuZi8oeRbxc3cgwfeDmYfOT
n3zsr4LE5rY1eC3hewH8bQ3Qzu4q7A1hNxBWxAAHZQIDAQABMA0GCSqGSIb3DQEB
CwUAA4IBAQA7c+FG1oz/XCtxMxUbbx2juwfR8ryQrXMDEqRcCUVKfHHFiY6YyiW/
PNeKWyGnqFlDCyle9xwK/vCkNrKmkzmmMGYehu+fTNSywqgdG3LAnkHOyGoGGIdu
pXLXNgARNqsY6p7NcpZf+Jq8SyDpmghtyQfa+Z21OaTw3bZpagNCmsS21RprC7OD
pm1Tx85+4mV0yB6EfRBbftXreDA3BQfYcpS2uvAPi9wrqnNmlrUT3JgzNSKpAVle
SqZoKykKJSILi3D/MsMiKhBNTsxVJrEL7PZ2lAq8u7lc1x4PlVZRLNkB/34dVcFt
HTw0kqEgIxumBecJbZNwpz3kwgo/PRF/
-----END CERTIFICATE-----
```

Complete metadata at `https://proxy.umbrellaid.org/metadata/backend.xml`

Give to umbrellaID your SP-metadata



Login flow

- Default Keycloak authentication flow
  - Create a new local user for each umbrellaID one
- New authentication flow needed
  - Just allowing user to link to an existing account

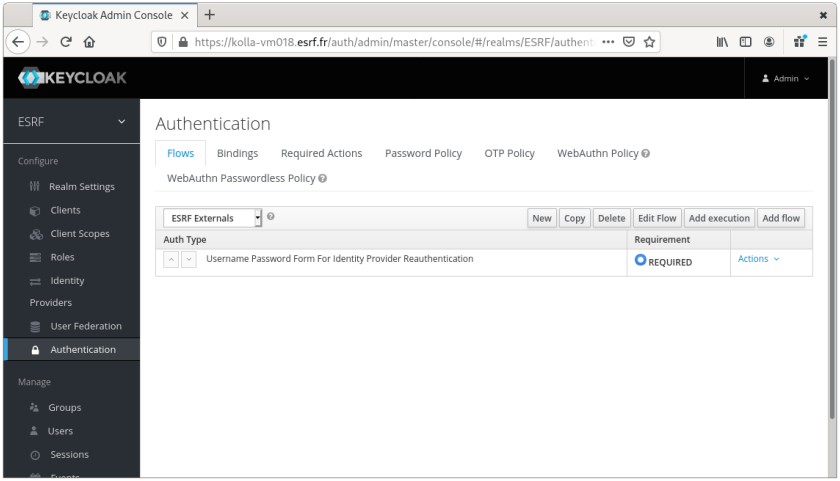
ESRF

Login flow

- Default Keycloak authentication flow
  - Create a new local user for each umbrellaID one
- New authentication flow needed
  - Just allowing user to link to an existing account

- Authentication → Flow
- New, then Add an execution
- "Username Password Form For Identity Provider Reauthentication"

Custom authentication flow

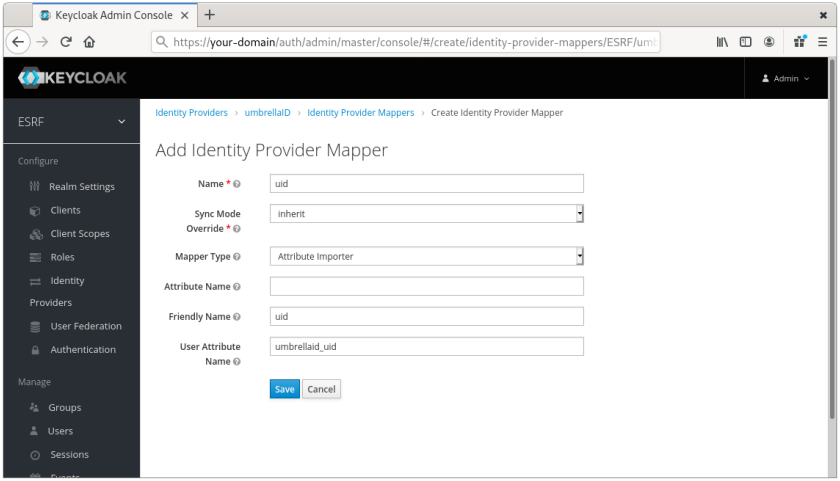


Sample SAML response from umbrellaID

```
<ns1:AttributeStatement>
    <ns1:Attribute FriendlyName="uid" Name="urn:oid:0.9.2342.19200300.100.1.1"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
        <ns1:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
            xsi:type="xs:string">anroux</ns1:AttributeValue>
    </ns1:Attribute>
    <ns1:Attribute FriendlyName="eduPersonPrincipalName" Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
        <ns1:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
            xsi:type="xs:string">xxxxxxxx-d4d9-4b0f-b207-xxxxxxxxxxxx@umbrellaid.org</ns1:AttributeValue>
    </ns1:Attribute>
    [...]
</ns1:AttributeStatement>
```

EAAHash, EAAKey, uid, displayName, mail, cn, eduPersonTargetedID, eduPersonUniqueId, eduPersonScopedAffiliation, eduPersonAffiliation, eduPersonPrincipalName and schacHomeOrganization are returned

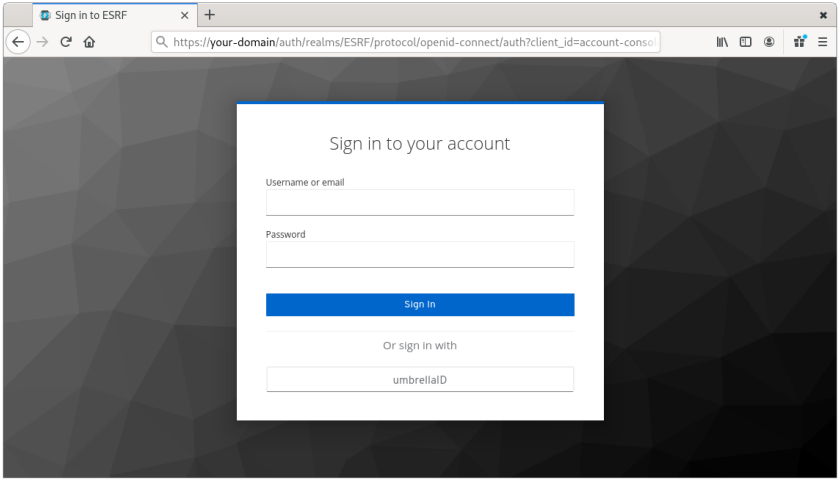
Attribute mapping



Try it at

`https://your-domain/auth/realms/YOUR-REALM/account`

The login screen with umbrellaID



Docker

Keycloack

umbrellaID integration

Useful tools to debug SAML

- https://chrome.google.com/webstore/detail/saml-chrome-panel/paijfdbeoenhembfhkhllainmocckace