Mise en place de l'authentification avec Shibboleth

L'authentification fédérée avec Shibboleth permet d'ouvrir la connexion à votre instance de Pod à toutes personnes possédant un compte dans une fédération Shibboleth. Comme par exemple la Fédération Education - Recherche de Renater.

De manière pratique, une fois avoir demandé l'authentification sur l'application l'utilisateur sera redirigé vers un service de type WayF (découverte d'établissement) dans lequel il pourra choisir l'établissement dont il provient. Il sera ensuite redirigé vers le système d'authentification de son établissement puis vers l'application Pod dans laquelle il sera connecté avec son compte.

Installation d'un SP (Service Provider) Shibboleth

Afin de pouvoir mettre en place l'authentification avec Shibboleth, il est nécessaire d'installer un Service Provider. Chaque application "Shibbolétisée" doit posséder son propre SP. A noter qu'il est également nécessaire d'avoir au préalable un IDP (Identity provider) dans votre établissement, si ce n'est pas déjà le cas, un tutoriel existe sur le site de Renater pour en installer un.

Pour installer un SP Shibboleth, vous pouvez suivre les différentes documentations :

- https://services.renater.fr/federation/documentation/guides-installation/sp3/chap01 (tutoriel de Renater pour installer un SP en version 3, en Français), jusqu'au chapitre 5 (voire 6 si on veut mettre en place son propre WayF (=service de découverte d'établissement)).
- https://wiki.shibboleth.net/confluence/display/SP3/Installation (Installation par le Wiki de Shibboleth en Anglais)

> **Information**
>
> Afin de pouvoir utiliser la Fédération Education - Recherche, il est nécessaire d'y inscrire son service. Toute cette procédure est détaillée dans le tutoriel de Renater. Il est conseillé dans un premier temps d'enregistrer son service dans la Fédération de Test, elle permet de tester son SP pour voir si tout fonctionne bien.

Configuration du Serveur Web

Shibboleth étant prévu pour fonctionner avec Apache2, il s'agit de la méthode recommandée pour le faire fonctionner. Néanmoins, étant donné que Podv2 utilise Nginx avec Uwsgi pour fonctionner, il est nécessaire d'apportes quelques changements dans la configuration.

Le but final est d'avoir un serveur Apache2 en frontal qui (grâce au mod_shib) communiquera avec Shibboleth et fournira des routes de connexion /déconnexion au service d'authentification. Ce dernier permettra également d'accéder à l'application par l'utilisation d'un ReverseProxy.

> **A noter**
>
> Il s'agit seulement d'une façon de faire, vous n'êtes pas obligé de mettre en place la communication entre Shibboleth et votre application de cette manière. Vous pouvez par exemple installer Shibboleth coté Nginx ou encore faire tourner votre instance de pod en utilisant le mod_wsgi de Apache et donc sans aucune utilisation de Nginx. Néanmoins, ces méthodes n'ont pas été testées et sont plus compliquées à mettre en place, libre à vous d'utiliser celle qui vous convient le mieux selon vos besoins.

Etape 1 : configuration de Nginx

Dans un premier temps, il est nécessaire de changer le port sur lequel Nginx fonctionne. (puisqu'on veut que Apache soit frontal)

Dans le bloc server du fichier pod_nginx.conf il faut donc changer le port d'écoute. Dans cet exemple, le port 8080 a été choisi, mais libre à vous d'en choisir un autre. Il est également nécessaire d'activer l'option proxy_pass_request_header pour permettre la bonne transmission des headers entre Apache et Nginx. Vous devrez également activer underscores_in_headers.

```
server{
    listen 8080;
    proxy_pass_request_headers on;
    underscores_in_headers on;
    ...
}
```

Etape 2 : configuration de Apache2

Coté apache (ou httpd), il faut configurer un VirtualHost (ou en modifiant le VirtualHost de base) ou configurer le httpd.conf si vous utilisez un serveur httpd.

Information

Selon que vous vous utilisez http ou la version complète d'apache, pensez à charger les modules mod_shib, mod_ssl (si besoin), mod_proxy et mod_proxy_http pour que l'ensemble des directives ci dessous fonctionnent

Dans l'exemple ci-dessous, l'application pod sera accessible à partir de la route/et toutes les routes relations à Shibboleth seront accessibles par /shib (encore une fois, c'est modifiable selon vos besoins)

- Pour l'accès à Pod :

```
<Location />
    ProxyPass https://127.0.0.1:8080/
    ProxyPassReverse http://127.0.0.1:8080/
    AuthType shibboleth
    Require shibboleth
    ShibUseHeaders On
</Location>
```

- Pour l'accès aux routes Shibboleth :

```
<Location /shib/secure> #Route de test qu'on peut supprimer par la suite

    ProxyPass !
    AuthType shibboleth
    ShibRequestSetting requireSession 1
    Require shib-session
</Location>

<Location /shib/Shibboleth.sso>
    ProxyPass !
    SetHandler shib
</Location>
```

Information

Si vous devez utiliser mod_ssl avec des échanges en HTTPS vous devrez peut être utilisées ces options (ou une partie du moins) en complément :

SSLProxyEngine On
SSLProxyVerify none
SSLProxyCheckPeerCN off
SSLProxyCheckPeerName off
SSLProxyCheckPeerExpire off
ProxyRequests Off
ProxyPreserveHost On

⚠️ Pensez également à tester votre installation de Shibboleth en vous rendant sur /shib/secure, il s'agit d'une route de test qui vous permettre de vérifier le bon fonctionnement de votre SP.

Etape 3 : configuration de Pod

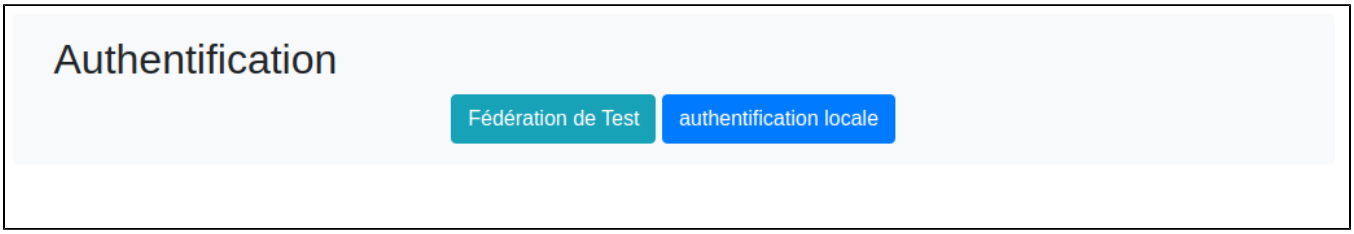
Pour prendre en charge l'authentification avec Shibboleth dans 3, il faut paramétrer 5 settings.

```
USE_SHIB=True #Active l'authentification Shibboleth dans la page de connexion

SHIB_NAME = "Fédération de Test" #Précise le nom de la fédération d'identité qui sera affichée sur le bouton de connexion

SHIBBOLETH_ATTRIBUTE_MAP = {
"HTTP_REMOTE_USER": (True, "username"),
"HTTP_DISPLAYNAME": (True, "first_name"),
"HTTP_DISPLAYNAME": (True, "last_name"),
"HTTP_MAIL": (False, "email"),
}  # Permet de préciser le mapping entre les attributs transmis par shibboleth et les attributs de la classe utilisateur

REMOTE_USER_HEADER = "REMOTE_USER" #Nom d'entête qui permet d'identifier l'utilisateur connecté par Shibboleth, vaut
HTTP_REMOTE_USER si on utilise un ReverseProxy avec Apache

SHIB_URL="https://univ-lr.fr/shib/Shibboleth.sso/Login" #Lien de connexion à Shibboleth

SHIB_LOGOUT_URL = "https://univ-lr.fr/shib/Shibboleth.sso/Logout" #Lien de dé-connexion à Shibboleth
```

Pensez également à ajouter l'authentification Shibboleth à l'attribut AUTH_TYPE :

```
AUTH_TYPE = (('local', ('local')), ('CAS', 'CAS'), ('Shibboleth','Shibboleth'))
```

Une fois la configuration dans pod effectué l'authentification Shibboleth s'affichera dans la page de connexion :



Il est totalement possible de faire cohabiter différents types d'authentification, vous pouvez très bien activer CAS, Shibboleth et l'authentification locale en même temps.

A partir de là, l'authentification Shibboleth devrait fonctionner correctement pour Pod. Si néanmoins des erreurs subsistent, pensez à regarder les logs de shibboleth-sp (/var/log/shibboleth) ou coté idp pour en connaitre la source.

Attention

Si vous constatez un message d'erreur 502 Bad Request, vérifiez la taille des entêtes renvoyés. Pensez à réduire le fichier **`attribute-map.xml`**