Authentification

- Keycloak
- Les roles

Keycloak

Les urls

- Url géneral: https://auth.ppsfleet.navy
- Pour gérer ses infos: https://auth.ppsfleet.navy/auth/realms/Ppsfleet/account/
- Pour l'interface admin de ppsfleet: https://auth.ppsfleet.navy/auth/admin/Ppsfleet/console/

Installation

Keycloak est lancé avec podman par l'utilisateur keycloak:

```
podman run -p 8080:8080 -e KEYCLOAK_USER=admin -e KEYCLOAK_PASSWORD=admin -e PROXY_ADDRESS_FORWARDING=true quay.io/keycloak/keycloak:11.0.3
```

Gérer le service

```
sudo -u keycloak podman start/stop a44b212348f0
```

Ne pas supprimer le container sans qu'une backup ait été effectué !

Todo: le relier à mysql

Relancer le service si y a plus rien qui marche

Ca utilisera la backup du 10/03/2022

```
podman run -p 8080:8080 --entrypoint /opt/jboss/tools/docker-entrypoint.sh -d -e PROXY_ADDRESS_FORWARDING=true localhost/keycloak-10-03-22-fixed:latest -Djboss.bind.address.private=127.0.0.1 -Djboss.bind.address=0.0.0.0
```

Backup

```
$ podman commit <id>
$ podman tag <id_image> keycloak-<date>
$ podman run -it -v /srv/keycloak/backup:/backup:rw --entrypoint=sh keycloak-<date>
$ HOSTNAME=alshain.ppsfleet.navy
$ /opt/jboss/keycloak/bin/standalone.sh -Dkeycloak.migration.action=export -Dkeycloak.migration.provider=singleFile -Dkeycloak.migration.realmName=Ppsfleet -Dkeycloak.migration.usersExportStrategy=REALM_FILE -Dkeycloak.migration.file="/backup/"$(date +%Y%m%d)".json"
```

Les services:

I - Bookstack

- https://github.com/elexis/elexis-environment/blob/master/docker/ee-util/assets/stage_ee_start_setup/keycloak/bookstack-saml.json
- https://github.com/BookStackApp/BookStack/issues/1157#issuecomment-585804153

```
AUTH_METHOD=saml2

# Set the display name to be shown on the login button.
# (Login with <name>)
SAML2_NAME=ppsfleet

# Name of the attribute which provides the user's email address

SAML2_EMAIL_ATTRIBUTE=email
SAML2_EXTERNAL_ID_ATTRIBUTE=username
SAML2_DISPLAY_NAME_ATTRIBUTES=firstName|lastName
```

```
# Enable SAML group sync.
SAML2_USER_TO_GROUPS=true

# Set the attribute from which BookStack will read groups names from.
SAML2_GROUP_ATTRIBUTE=Role

# Removed user from roles that don't match SAML groups upon login.
SAML2_REMOVE_FROM_GROUPS=true

# Name of the attribute(s) to use for the user's display name
# Can have mulitple attributes listed, separated with a '|' in which
# case those values will be joined with a space.
# Example: SAML2_DISPLAY_NAME_ATTRIBUTES=firstName|lastName
# Defaults to the ID value if not found.
#SAML2_DISPLAY_NAME_ATTRIBUTES=username

# Identity Provider entityID URL
SAML2_IDP_ENTITYID=https://auth.ppsfleet.navy/auth/realms/Ppsfleet/protocol/saml/descriptor
```

II - Nextcloud

https://auth.ppsfleet.navy/auth/realms/Ppsfleet

Si il y a une erreur du type: "account not provisioned" c'est durement un problème de certificat.

Le certificat se trouve dans keycloak: `Realm settings > keys > algorithm RS256 > Cetificate`

Il faut le mettre dans les paramètre de nextcloud: `SSO and SAML authentication > show optional Identity Provider settings > dernier champ`

Config:

Identifier: `https://auth.ppsfleet.navy/auth/realms/Ppsfleet`

Url target: `https://auth.ppsfleet.navy/auth/realms/Ppsfleet/protocol/saml`

Identity Provider Data

Configure your IdP settings here.

https://auth.ppsfleet.navy/auth/realms/Ppsfleet

https://auth.ppsfleet.navy/auth/realms/Ppsfleet/protocol/saml

Hide optional Identity Provider settings ...

https://auth.ppsfleet.navy/auth/realms/Ppsfleet/protocol/saml

URL Location of the IDP's SLO Response

-----BEGIN CERTIFICATE-----

Les roles

Groupes

Captains

Administrateur de la flotte. Ont tous les droits.

Roles :

- Nextcloud: admin, test, users
- Peertube: admin
- Wiki: Admin, Seaman

Gentlefolks

Groupe pour la famille, ou si on devient un chaton, pour nos invité·e·s premium, qui vont pas aider au bon fonctionnement du serveur mais vont utiliser le navire.

Sur nextcloud, capacité illimité. Sur le wiki, peuvent créer leur livre.

Roles :

- Nextcloud: users
- Peertube: user
- Wiki: Seaman

Travelers

Groupe pour les invité·e·s pas tant premium que ça. Capacité limité sur nextcloud. On peut les laisser editer les recettes ?

Roles :

- Nextcould: disabled
- Peertube: user
- Wiki: Seaman

Carpenters

S'occupent du travail manuel, ont accès au livre sur l'atelier. Pas de nextcloud, peuvent uploader des vidéos sur peertube, mais on les modère avant.

Roles:

- ...