Configurer AzureAD comme fournisseur d'identité pour Authentic

Inspiré par le ticket #54831

Nomenclature

<tenant>	le nom de domaine de l'authentic, ex.: connexion-client.test.entrouvert.org

Configuration des clés RSAs

Deviendra obsolète quand cette génération sera entièrement faite dans le backoffice d'authentic.

- créer les clés, dans /var/lib/authentic2-multitenant/tenants/<tenant>/ faire :

```
sudo -u authentic-multitenant openssl req -x509 -sha256 -newkey rsa:2048 -nodes -keyout sp-saml.key -out sp-saml.crt -batch -subj '/CN=<tenant>' -days 3652
```

  le sudo est là pour que les clés aient les bons droits.
- configurer les clés, dans le même répertoire éditer settings.json et y ajouter :

```
{
  "MELLON_PUBLIC_KEYS": ["/var/lib/authentic2-multitenant/tenants/<tenant>/sp-saml.crt"],
  "MELLON_PRIVATE_KEY": "/var/lib/authentic2-multitenant/tenants/<tenant>/sp-saml.key",
}
```

Configuration AzureAD

Documentation Microsoft: https://learn.microsoft.com/fr-fr/azure/active-directory/develop/active-directory-saml-claims-customization

- configurer un nouveau fournisseur de service :
  - avec les métadonnées disponibles sur https://tenant/accounts/saml/metadata
  - avec ces revendications/claims "requis" :

Nom du claim	Format	Source	Valeur
(spécial) Unique User Identifier (Name ID)	persistent	Attribut	user.objectid
email	-	Attribut	user.mail
prenom	-	Attribut	user.givenname
nom	-	Attribut	user.surname
username	-	Attribut	user.userprincipalname

- avec des revendications/claims additionnels que vous jugeriez utiles (nous transmettre leur noms et leur significations)

Nous transmettre ensuite l'information "App Federation Metadata URL" qui devrait avoir la forme suivante:

```
https://login.microsoftonline.com/180627ee-80c9-4bec-95e6-81b5fecd81ff/federationmetadata/2007-06/federationmetadata.xml?appid=9b9854e3-633c-4124-8040-fe07dd445195
```

Configuration Authentic

- Aller sur https://<tenant>/manage/authenticators/

- Cliquer sur "Ajouter un nouveau moyen d'authentification"
- Choisir comme moyen d'authentification "SAML"
- Lui donner un nom
- Mettre la valeur de "App Federation Metadata URL" dans "URL des métadonnées"
- Configurer l'affectation des attributs (voir le tableau plus haut) et éventuellement la recherche d'utilisateur par attribut
- ATTENTION: AzureAD ne semble pas capable de fournir des noms de claim "simples" les claims définis plus haut arriveront tous préfixés avec l'espace de nom http://schemas.xmlsoap.org/ws/2005/05/identity/claims/, le mieux étant de les renommer avant de les utiliser selon cette correspondance :

Nom complet	Nom simplifié
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/email	email
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/prenom	prenom
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nom	nom
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/username	username

- ATTENTION 2: Le nom long doit aussi être utilisé pour la liaison par attribut, celle-ci ayant lieu pour l'instant avant le renommage (#69683), ainsi que pour le template de username