Geschäftsstelle | Secrétariat Edulog
Erlachstrasse 21
3012 Bern

+41 31 300 55 99
info@edulog.ch

edulog

TECHNIQUE

Préparation d'une infrastructure hybride (*AD* local et *Azure AD*) en tant qu'IdP pour Edulog.

22.3.2021 – Version 1.0

Föderation der Identitätsdienste im Bildungsraum Schweiz
Fédération des services d'identité de l'espace suisse de formation
Federazione dei servizi di identità nello spazio formativo svizzero
Federaziun dals servetschs d'identitad en il spazi da furmaziun svizzer

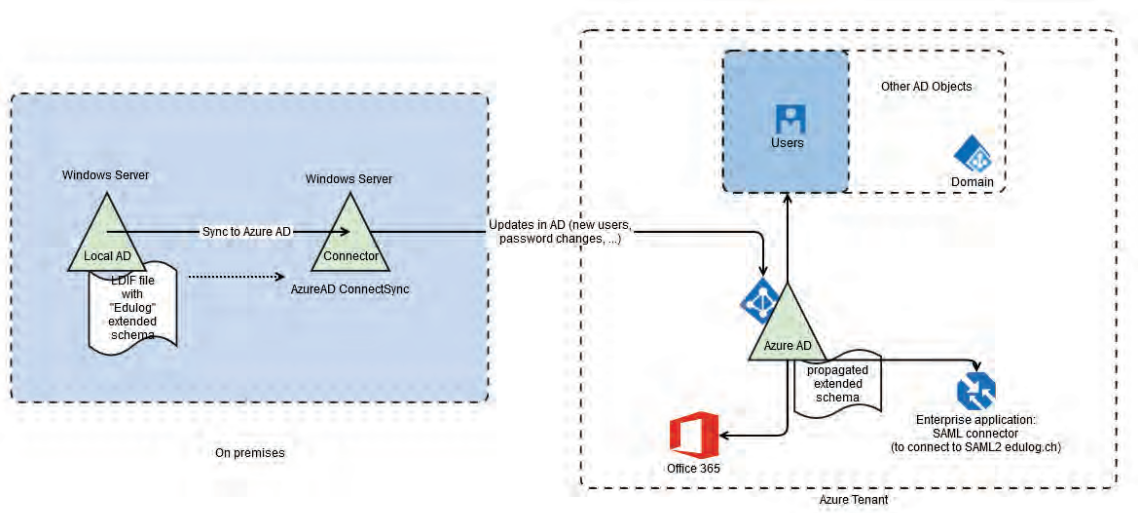
1. But du Document

Ce document explique aux fournisseurs d'identité (IdP) comment préparer une infrastructure hybride (*AD local* et *Azure AD*).

En effet, pour adhérer à Edulog, les IdP doivent :

- Vérifier que leurs identités disposent d'un certain nombre d'attributs[1]. Or certains de ces attributs n'existent pas originellement dans le schéma d'un *AD*, ni même dans le schéma de *Azure AD*. *La première partie de ce document explique comment installer l'extension du schéma de l'AD, propager les attributs et vérifier qu'ils sont atteignables*
- Posséder une infrastructure avec une interface SAML. *La seconde partie de ce document explique comment mettre en place une Entreprise Application sous Azure pour jouer ce rôle d'interface.*

Ce document s'adresse aux IdP qui ont un *AD* local et utilisent *Azure AD* comme interface *SAML* pour réaliser les connections avec Edulog.



[1] Ces attributs sont listés dans le « Guide des attributs – fournisseur d'identité », disponible ici : https://edulog.ch/fr/adhesion/documentation

2. Prérequis

Ce guide ne peut être utilisé que si les exigences techniques suivantes sont respectées :

- L'IdP utilise – dans sa propre infrastructure – un *AD* (que l'on appellera Local *AD*).
- L'IdP utilise un serveur avec *Azure AD ConnectSync* pour synchroniser les attributs (au moins ceux utilisés par Edulog), avec son compte *Azure AD*.
- L'IdP possède un tenant *Azure* avec *Azure AD*. Il utilise *Azure AD* comme interface *SAML* avec la Fédération Edulog.

3. Procédure complète

Nous rappelons ici les étapes techniques[2] nécessaires à un IdP (avec l'infrastructure précédemment citée) pour réaliser la configuration nécessaire à l'onboarding avec Edulog :

N°	Actions à réaliser	Moment
1	Installer l'extension du schéma de l'*AD* pour Edulog.	Chapitre 4
2	Propager les attributs avec *Azure AD ConnectSync* dans le tenant *Azure* et vérifier que les nouveaux attributs sont atteignables.	Chapitre 4
3	Créer une *Enterprise Application* (EA).	Chapitre 5
4	Configurer l'EA : utilisateurs autorisés, SSO avec les paramètres *SAML* nécessaires. Générer un fichier metadata.xml	Chapitre 6
5	Contacter ELCA, leur envoyer le fichier metadata.xml	Chapitre 6
6	Récupérer les données fournies par ELCA et modifier la partie SSO dans le tenant *Azure* avec les données nécessaires	Chapitre 6
7	Réaliser les tests de connexion avec ELCA.	Après
8	Réaliser la fédération des identités avec ELCA.	Après

Ce document traite les points 1 à 6.

[2] D'autres étapes non-techniques (contrats, etc) sont nécessaires pour l'intégration dans la Fédération. Elles ne sont pas traitées dans ce document.

4. Installer l'extension du schéma de l'*AD* pour Edulog

L'extension du schéma *AD* peut être problématique. Lorsqu'un nouvel attribut est créé, il n'y a aucun moyen de l'éliminer du schéma si une erreur a été commise. Il est préférable d'utiliser un fichier contenant les nouveaux attributs et leurs caractéristiques. Un fichier LDIF peut être utilisé à cet effet.

Important : toujours effectuer un test avant d'appliquer des modifications au schéma de l'*AD* !

Vue d'ensemble du processus :

1. Créer les nouveaux attributs dans le schéma *AD* local :
    a. permettre à l'*AD* de modifier le schéma ;
    b. permettre la visualisation du schéma ;
    c. charger un fichier LDIF avec les nouveaux attributs.[3]
2. Utiliser *Azure AD ConnectSync* pour propager les nouveaux attributs de l'*Azure AD*.
3. Vérifier la création des nouveaux attributs dans le schéma *Azure AD* (et certaines valeurs de test).

Fichier LDIF : la version actuelle du fichier LDIF utilisé dans ce document peut être demandée au secrétariat Edulog via info@edulog.ch.

4.1 Créer les nouveaux attributs dans le schéma *AD* local

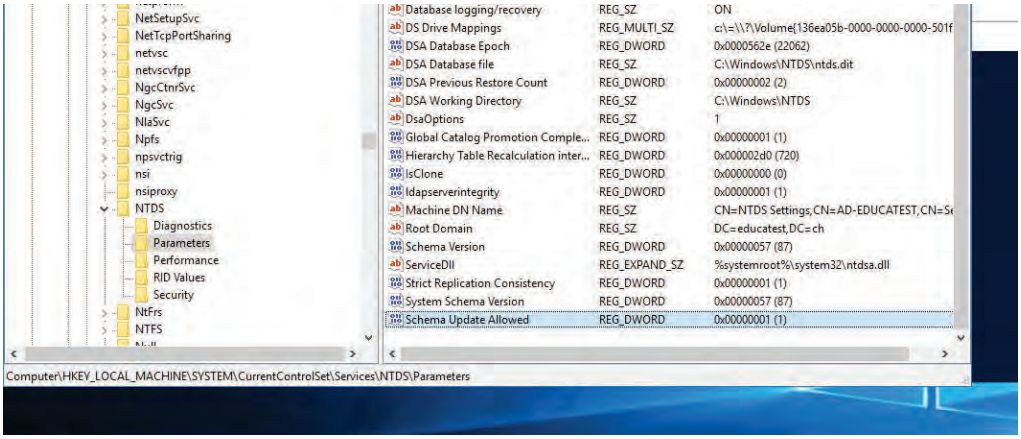
Avant de pouvoir créer les nouveaux attributs, il est nécessaire de réaliser certaines opérations sur l'*AD*. L'accès se fait avec des droits de « Schema Admin » (un compte administrateur du domaine, par défaut, devrait suffire). Si l'infrastructure comprend plus d'un serveur « Domain Controller », l'accès se fait sur celui qui a le rôle de « Schema Master ».

4.1.1 Permettre à l'*AD* de modifier le schéma

Une clef du registre doit être ajoutée sous HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters.

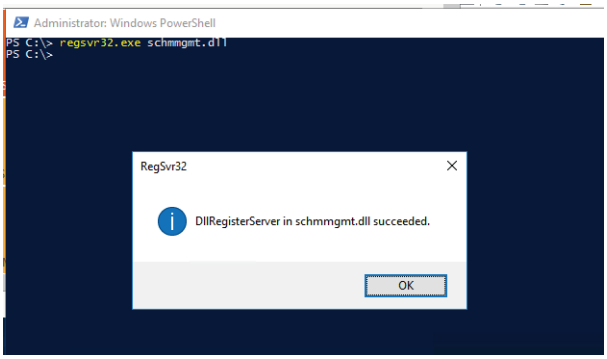
Le nom de la nouvelle clef doit être « Schema Update Allowed » de valeur 1 et format REG_DWORD.

[3] Pour ces sous-tâches, le document Microsoft suivant peut être utilisé : https://social.technet.microsoft.com/wiki/contents/articles/51121.active-directory-how-to-add-custom-attribute-to-schema.aspx

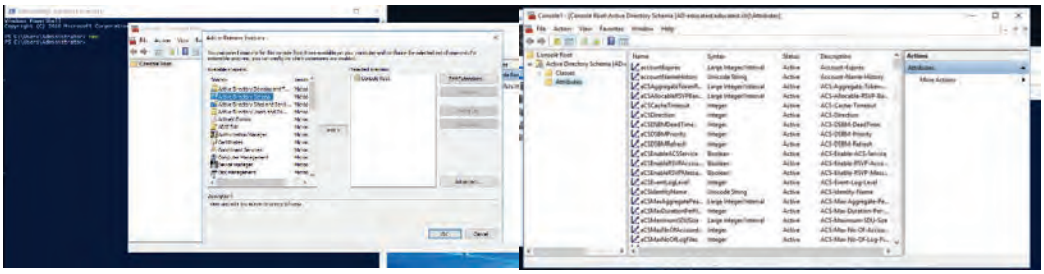


4.1.2 Permettre la visualisation du schéma

Pour pouvoir visualiser le « Schema Management » dans MMC, il faut d'abord enregistrer la DLL correspondante en écrivant la commande : *regsvr32.dll schmmgmt.dll*



On peut alors importer l'outil « Active Directory Schema » depuis MMC et finalement voir les attributs du schéma :



4.1.3 Importer le fichier LDIF dans *AD*

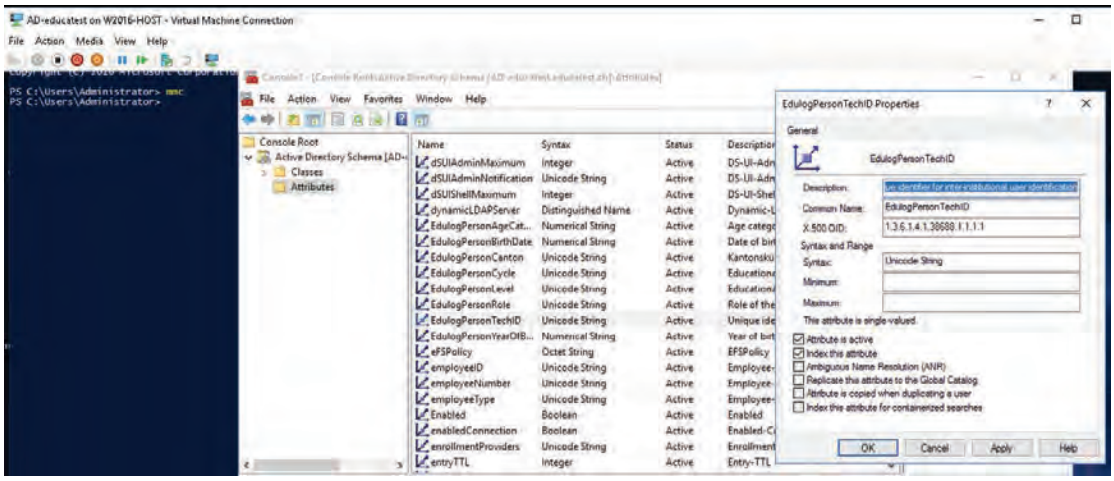
Pour importer le fichier LDIF avec les nouveaux attributs dans le schéma *AD*, (en tant qu'administrateur du schéma/domaine), utiliser la commande :

```
ldifde -i -f .\ldif_name_des_Datei.ldif -v -j .
```

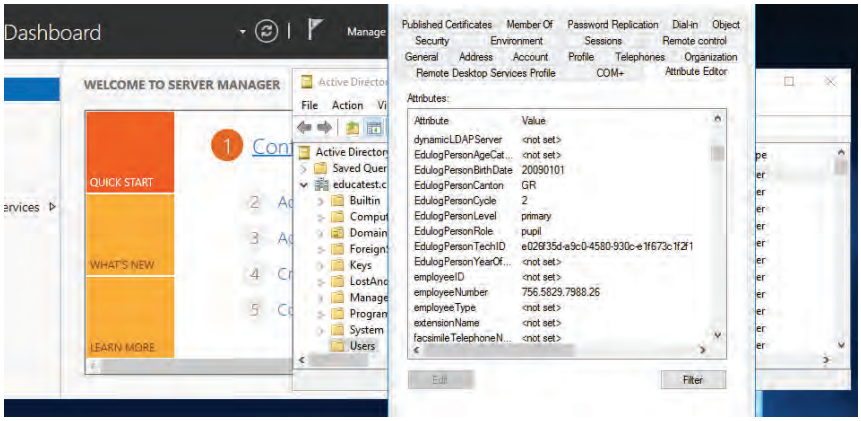
Important : le fichier LDIF doit être modifié pour prendre en compte le nom du domaine dans lequel il est utilisé (ex : DC=educatest,DC=ch si le domaine est educatest.ch)

4.2 Caractéristiques des nouveaux attributs dans l'*AD*

Une fois l'importation effectuée, vérifier la présence de ceux-ci dans l'index du catalogue global.



En utilisant l'outil d'administration « Active Directory Users and Computers », il est possible de modifier quelques-uns des nouveaux attributs avec l'éditeur d'attributs. De cette façon, une fois les opérations de synchronisation terminées, il est possible de vérifier la présence des attributs dans *Azure*.

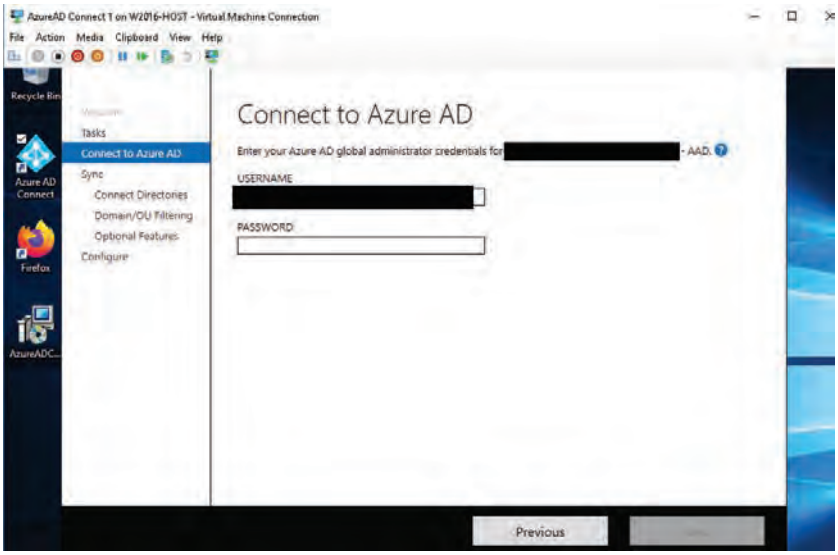


4.3 Configurer le service *Azure AD ConnectSync*

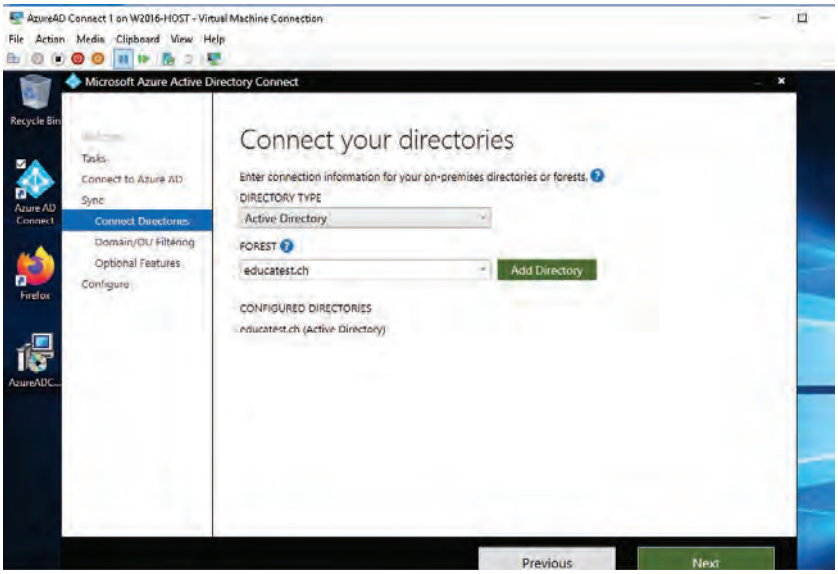
Pour exporter les nouveaux attributs du schéma vers *Azure AD*, utiliser *AAD ConnectSync*. Un serveur dédié pour cet outil est requis.

Voici, ci-dessous, les différentes étapes de la configuration du service pour synchroniser un domaine/forêt (ici : educatest.ch).

4.3.1 Connection au compte administration du tenant *Azure*

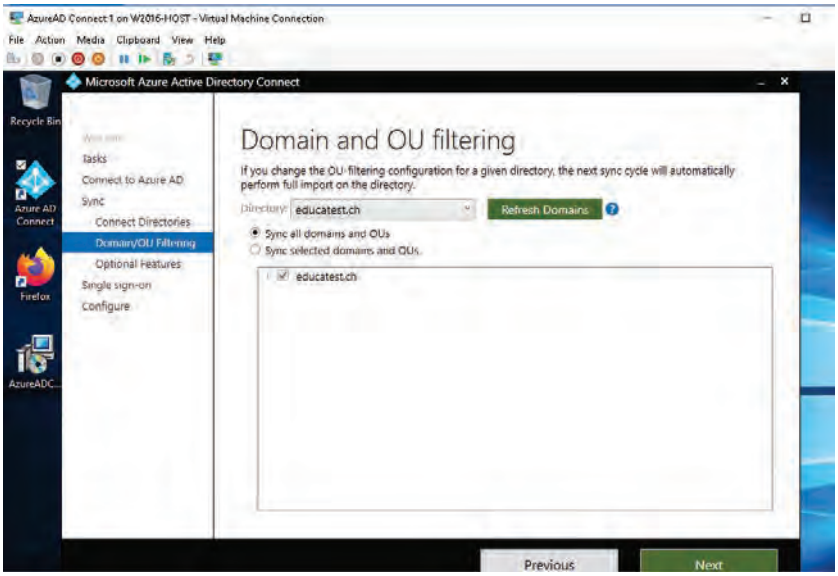


4.3.2 Sélectionner le type et la forêt *AD*

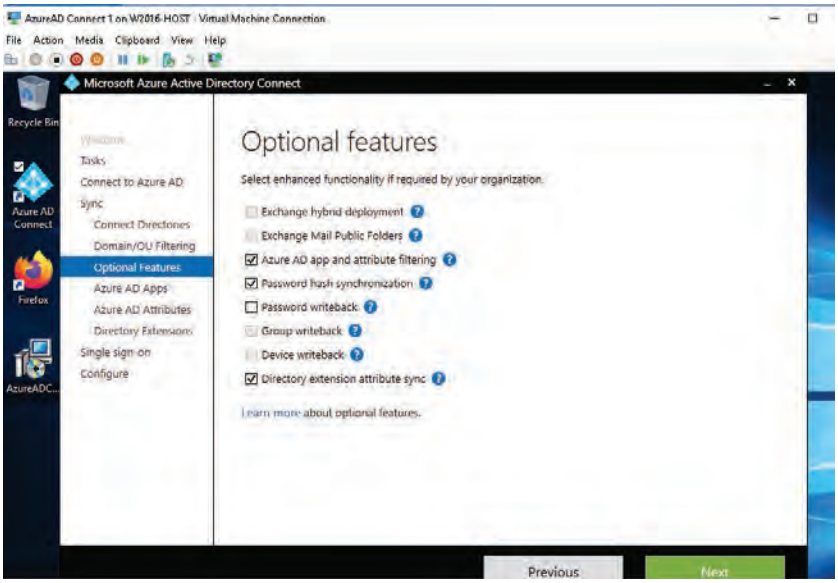


4.3.3 Sélectionner les domaines et unités organisationnelles (OU)

Dans l'exemple, on synchronisera l'ensemble des domaines et des OU de l'*AD*.



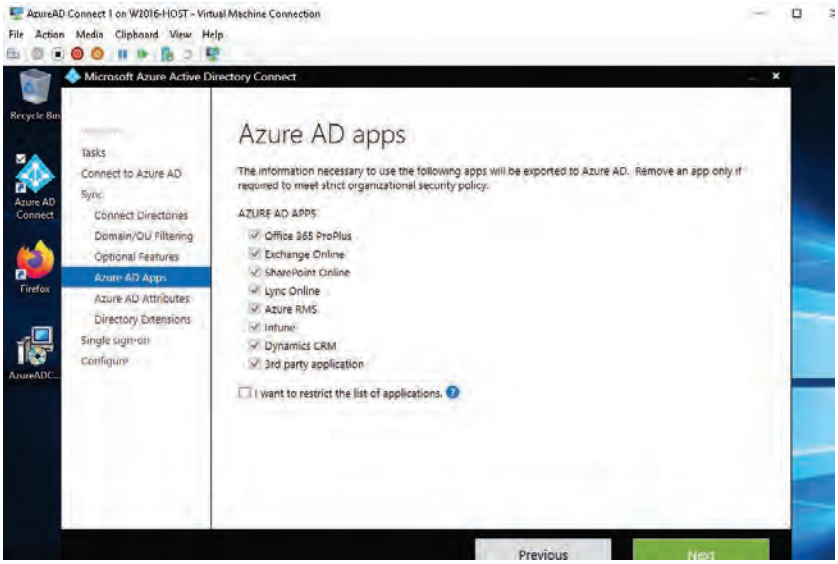
4.3.4 Configurer les options de synchronisation



Dans le cas des options de synchronisation, celles-ci doivent être adaptées à l'infrastructure.

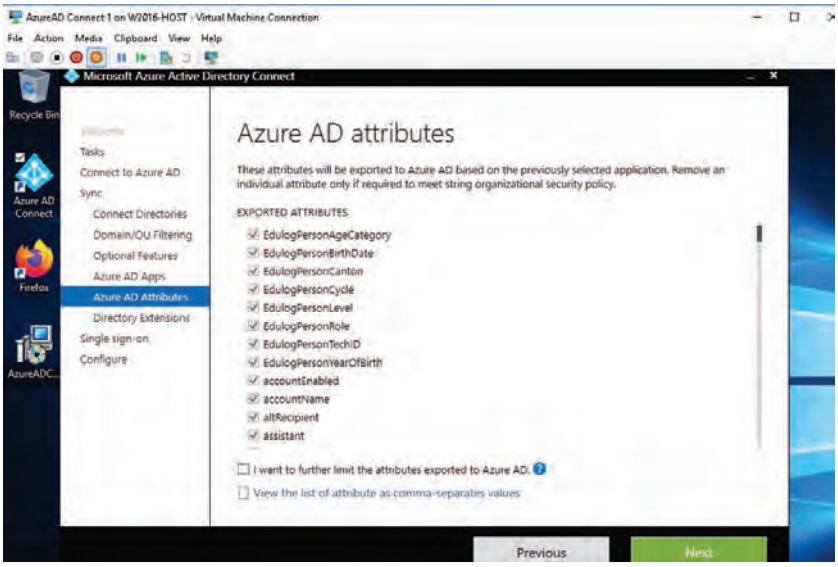
4.3.5 Sélectionner les applications externes

Le point suivant permet de sélectionner les applications externes avec lesquelles des informations seront partagées depuis l'*AD*.



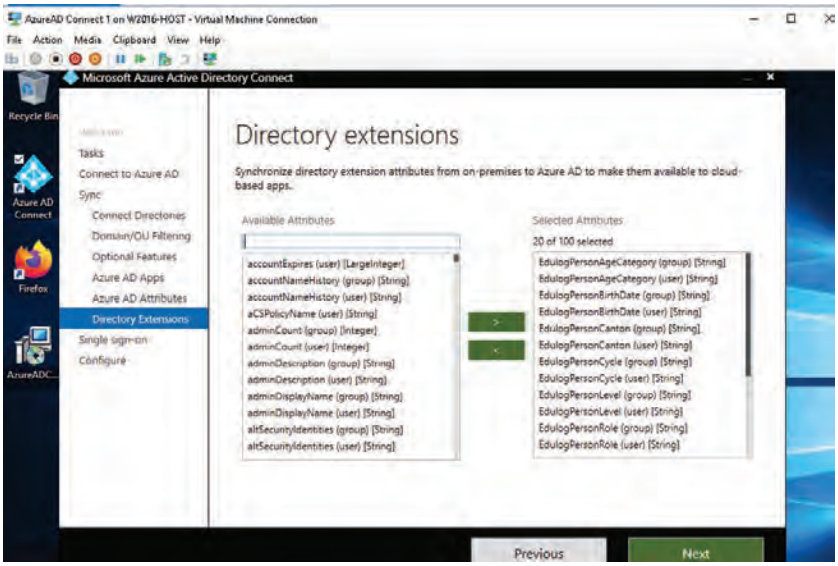
4.3.6 Attributs à exporter

Sélectionner les attributs à exporter sous *Azure*. Ne pas oublier les attributs d'Edulog !



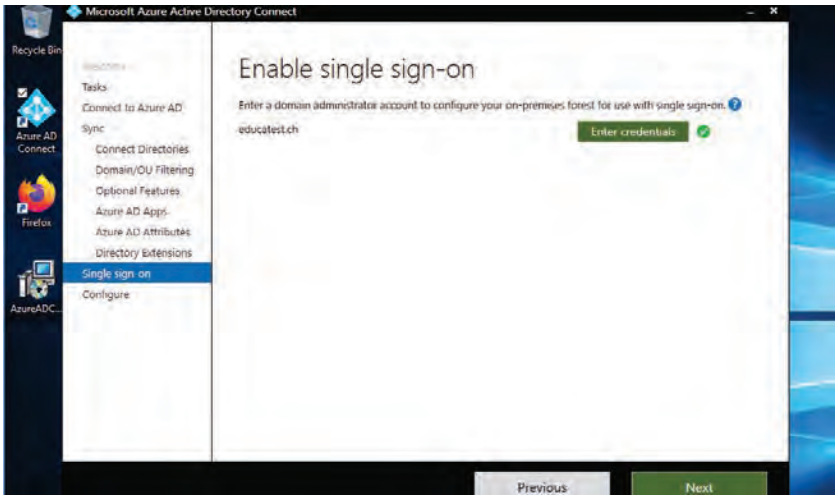
4.3.7 Directory extensions

Sélection d'autres attributs (si nécessaire).



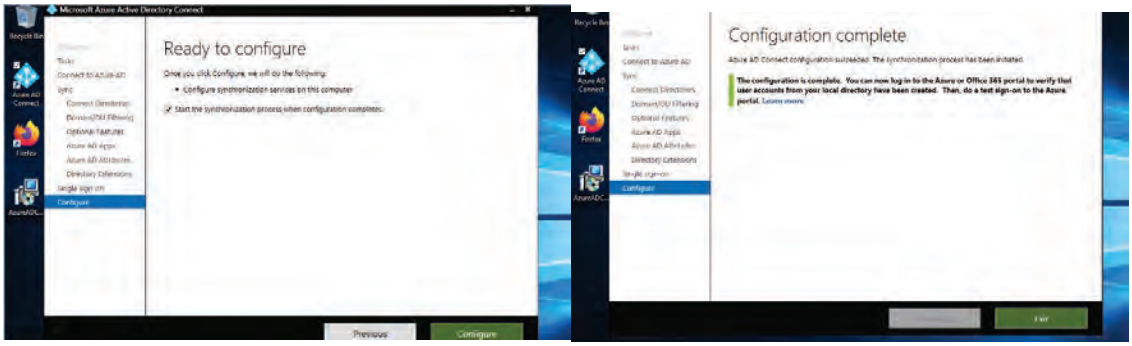
4.3.8 Configurer SSO

Pour configurer le SSO, se connecter avec un compte d'administrateur de domaine.



4.3.9 Valider la configuration

Une fois les options sélectionnées, appuyer sur le bouton « Configure ». Une série d'opérations est effectuée. Puis, un message indique que la configuration est terminée.



4.3.10 Remarque

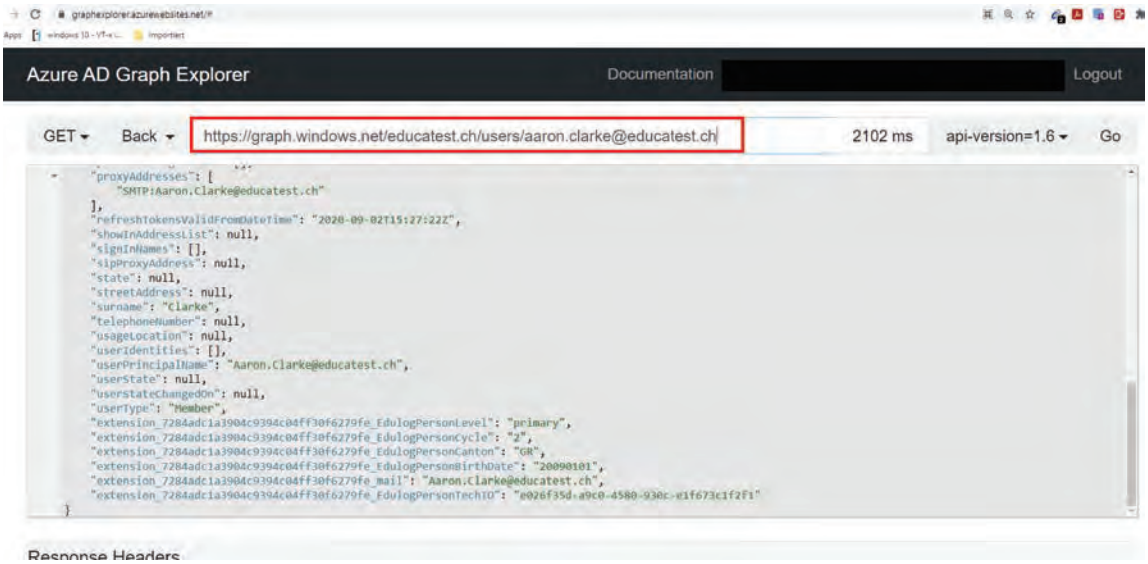
L'actualisation des attributs des utilisateurs de l'*AD* intervient de manière périodique. Pour forcer la synchronisation avec le tenant *Azure*, utiliser – depuis *Powershell* (comme administrateur, sur le serveur *Azure AD ConnectSync)* – la commande :

```
> Start-ADSyncSyncCycle
```

4.4 Vérifier la présence des attributs sous *Azure AD*

Après avoir attendu le temps nécessaire pour la propagation des modifications du schéma – ou avoir forcé la synchronisation – les nouveaux attributs et leurs valeurs sont visibles sous Azure en utilisant l'outil https://graphexplorer.azurewebsites.net/, la référence nécessaire à l'utilisateur et le domaine *AD* considéré (voir image).

Il faut être connecté à son tenant pour y accéder.



Il est alors possible de vérifier la présence des attributs Edulog du schéma de l'*AD* dans Azure (ils ne sont pas visibles à travers le portal.azure.com !). A noter que le format du nom des attributs Edulog est de la forme suivante :

extension_numero ID unique de votre application_nom de l'attribut Edulog

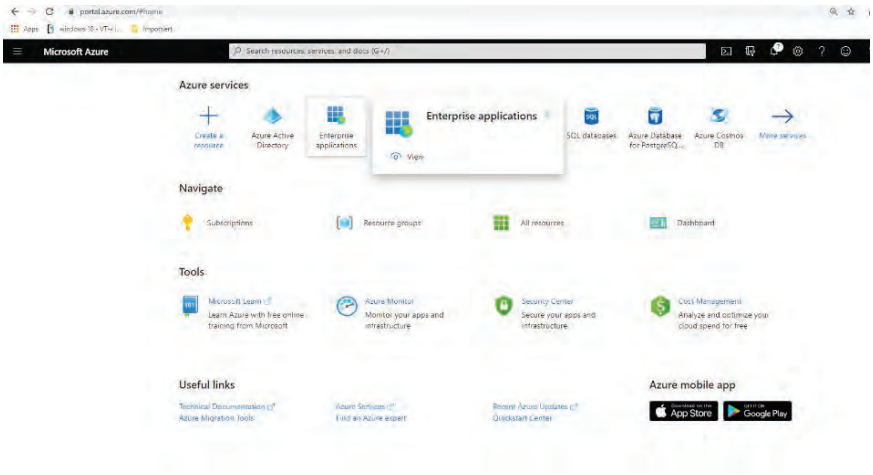
Exemple : **extension_111222233344556667788889999eeffff_EdulogPersonCanton**

5. Création d'une *Enterprise Application*

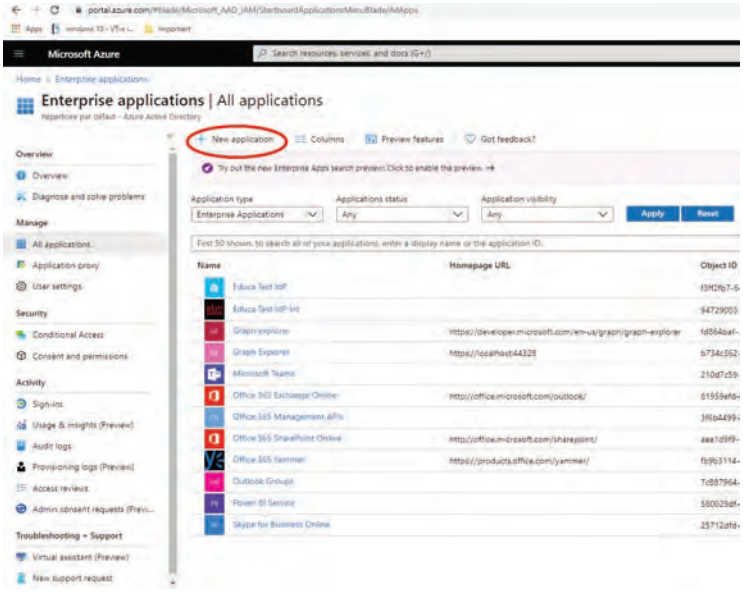
5.1 Sélection de l'Enterprise Application

Les *Enterprise Applications* d'*Azure* permettent non seulement d'avoir accès des applications spécifiques, mais aussi de définir des applications ad hoc qui permettront l'utilisation d'interfaces prédéfinies pour l'accès à nos identités incluses dans l'*Azure AD*.

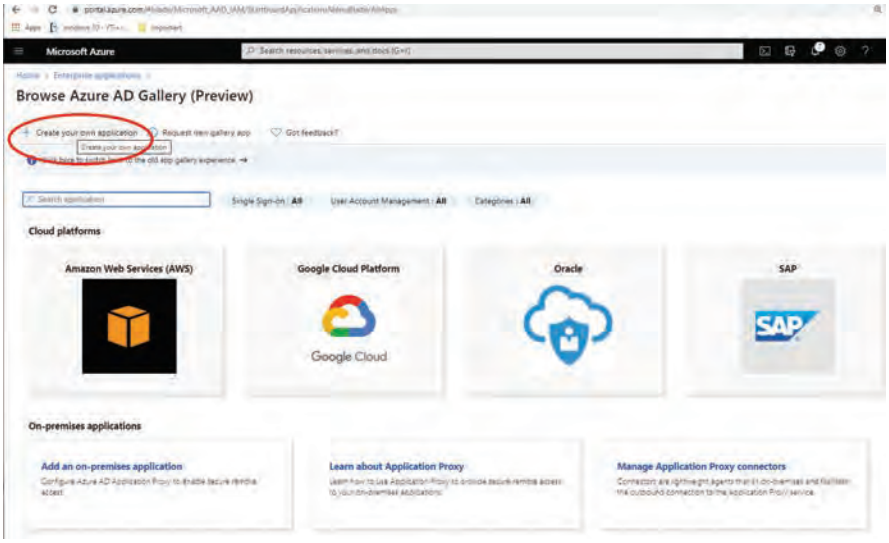
5.1.1 Cliquer sur « Enterprise applications »



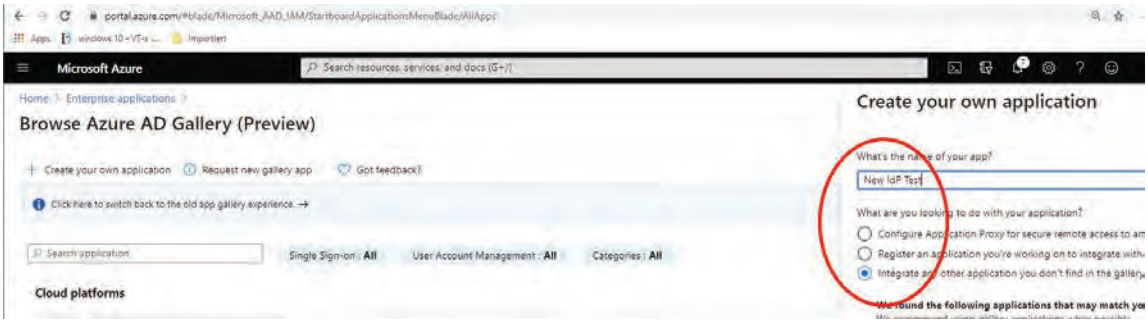
5.1.2 Cliquer sur « New application »



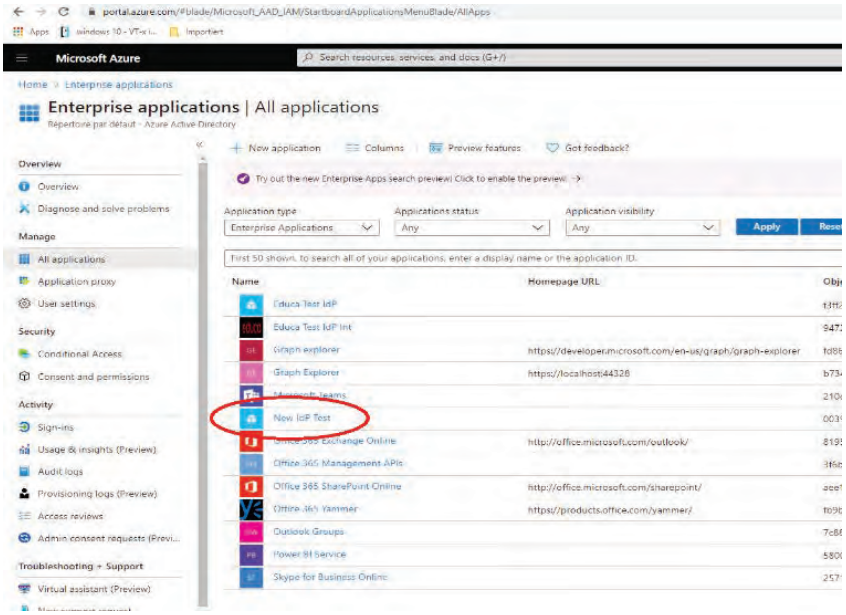
5.1.3 Sélectionner « Create your own application »



5.1.4 Donner un nom à l'application (ici « New IdP Test ») et sélectionner « Integrate any other application... »



5.1.5 Vérifier que l'application a été créée



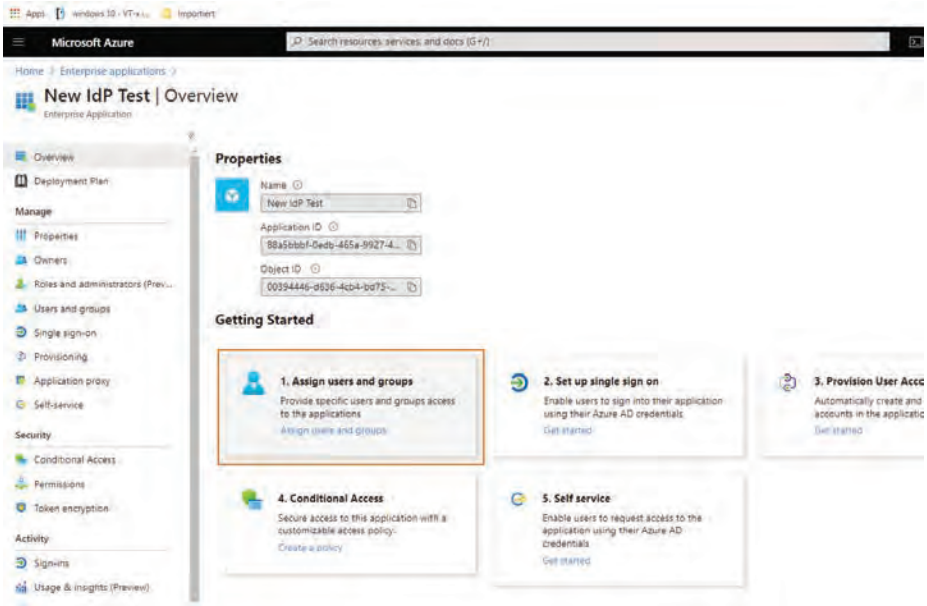
6. Configuration de l'*Enterprise Application*

Une fois l'application créée, il faut encore :

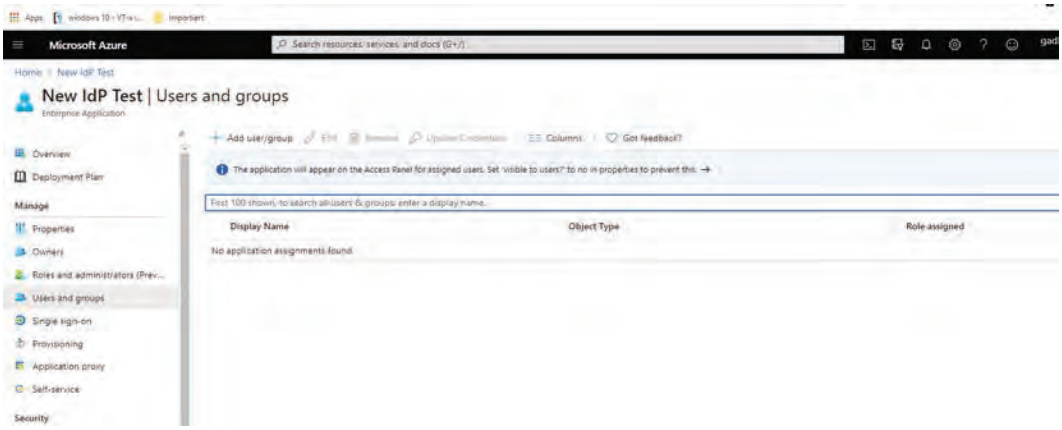
- autoriser des utilisateurs à l'utiliser ;
- configurer le SSO (et l'interface SAML) ;
- faire un test de connexion (interne – pas avec Edulog).

6.1 Autorisation d'utilisateurs

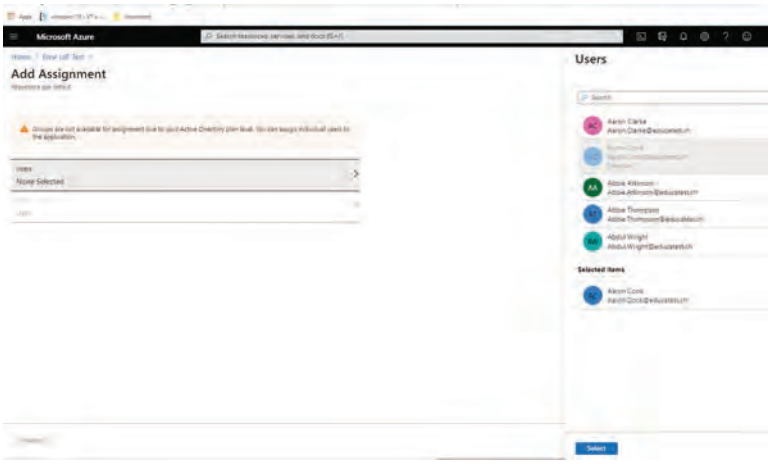
6.1.1 Aller sur l'application créée



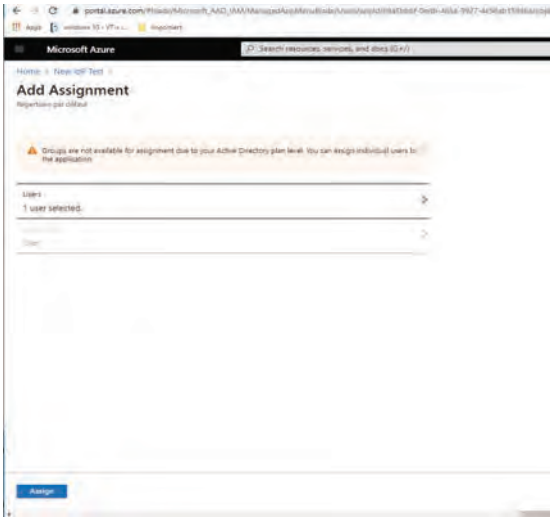
6.1.2 Cliquer sur « Users and Groups »



6.1.3 Sélectionner un utilisateur de l'*Azure AD* (cliquer sur « Select »)

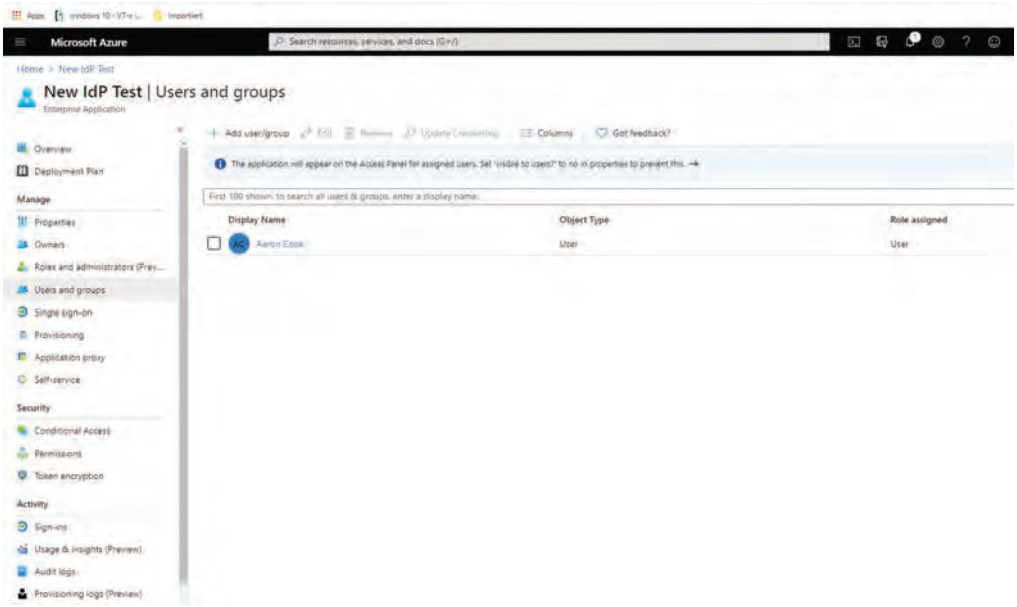


6.1.4 Cliquer sur « Assign » (par défaut, le rôle « user » est assigné)



Dans notre exemple, l'utilisateur sélectionné sera le seul à pouvoir s'authentifier à travers SAML2 en utilisant l'application. Il est possible de donner des autorisations sur la base de groupes ou effectuer des *bulk operations* pour éviter de devoir le faire un-par-un.

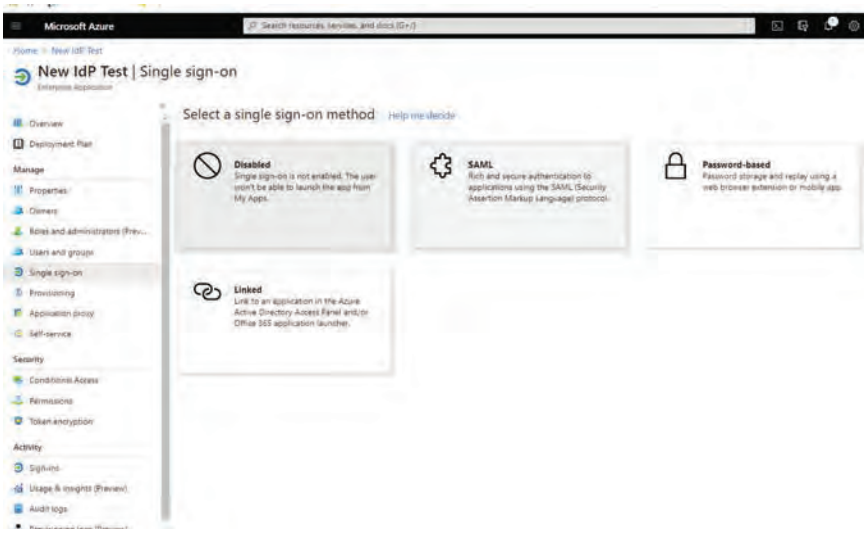
6.1.5 Sélection de l'utilisateur terminée



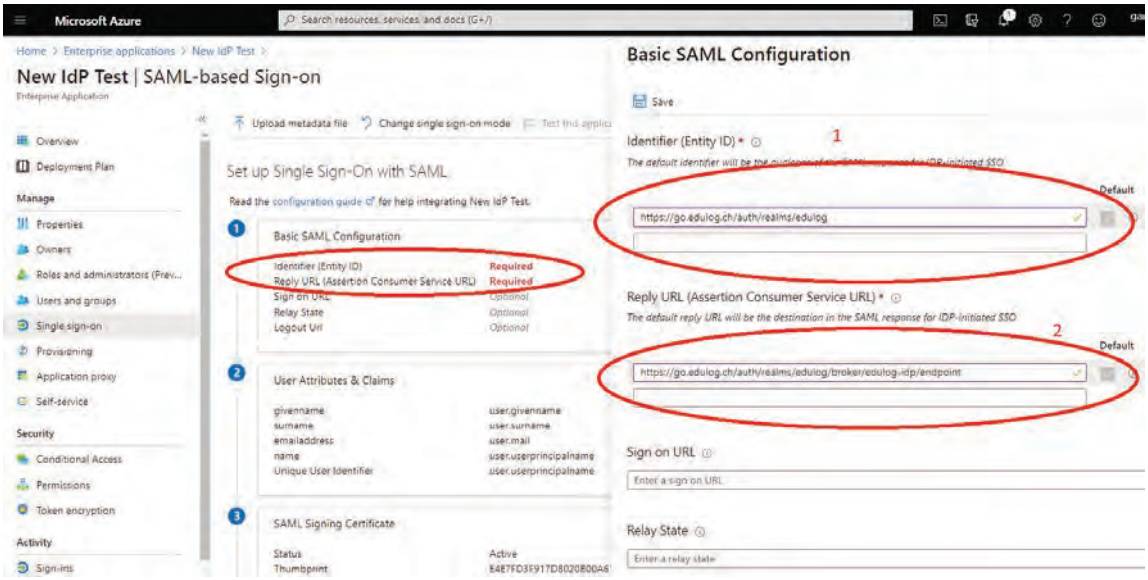
6.2 Configuration du SSO avec SAML

Les *Enterprise Applications* d'*Azure* peuvent utiliser le *Single Sign On* (SSO) pour l'authentification. Différentes méthodes sont proposées, mais Edulog ne supporte que SAML2. Nous allons maintenant configurer l'application créée antérieurement.

6.2.1 Cliquer sur « Single Sign On » et « SAML »



6.2.2 Modifier les paramètres « Basic SAML configuration »



Deux valeurs sont nécessaires :

- « Identifier (Entity ID) » : inscrire https://go.edulog.ch/auth/realms/edulog
- « Reply URL (Assertion Consummer Service URL) »
  - Attention ! Ici, la valeur finale doit être donnée par ELCA lors de l'*onboarding*. Il faudra la modifier après.
  - Il faut néanmoins remplir cette valeur pour finir la configuration. Par exemple : https://go.edulog.ch/auth/realms/edulog/broker/edulog-idp/endpoint

6.2.3 Modifier les « User Attributes & Claims »

Par défaut, Azure sélectionne quelques attributs des utilisateurs pour créer les assertions SAML. Ceux-ci doivent être modifiés avec les attributs qui seront envoyés à la Fédération Edulog. Voici un exemple avec tous les attributs publiés dans le Guide des attributs – fournisseur d'identité[4].
Après avoir modifié le schéma de l'*AD*, des attributs propres à Edulog ont été rajoutés à celui-ci. Avec la synchronisation à travers *Azure AD ConnectSync*, ils ont été transférés sur le tenant *Azure*.
Ils sont de la forme :

user. *nom de l'attribut Edulog (extension_numero ID unique de votre application_nom de l'attribut Edulog)*

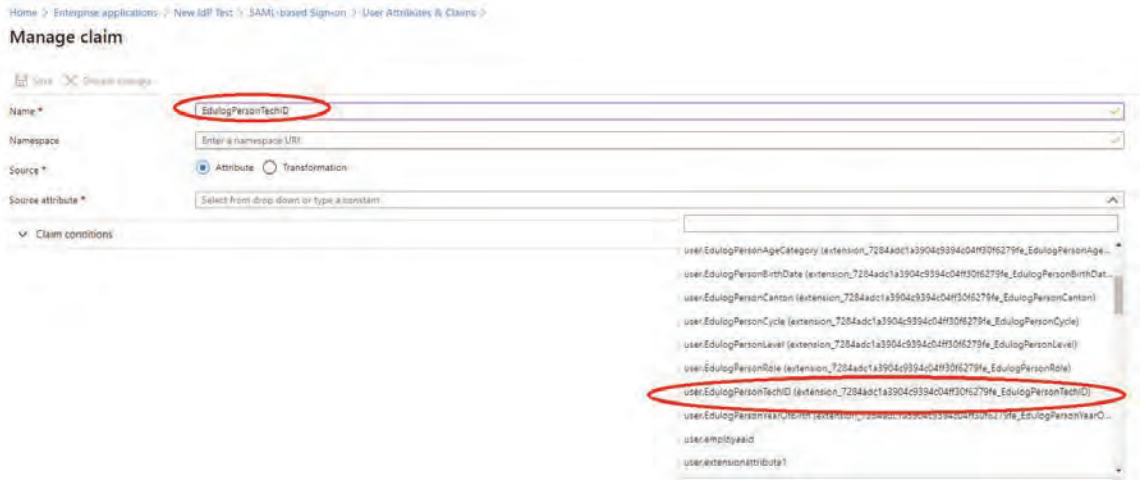
Exemple :
user.EdulogPersonCanton (extension_111222233344556667788889999eeffff_EdulogPersonCanton)

[4] Disponible sur : https://edulog.ch/fr/adhesion/documentation

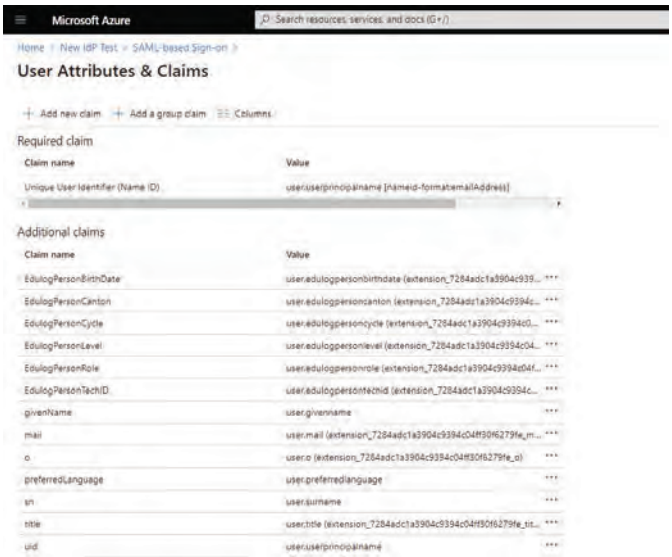
Il faut maintenant créer des « Claims » qui incorporent les attributs.

- Le « Name » du claim correspond au nom de l'attribut transmis à la Fédération : il doit être le même que celui du Guide des attributs d'Edulog.
- La « Source » doit être « Attribute ».
- Et le « Source attribute » doit correspondre à l'attribut sélectionné.

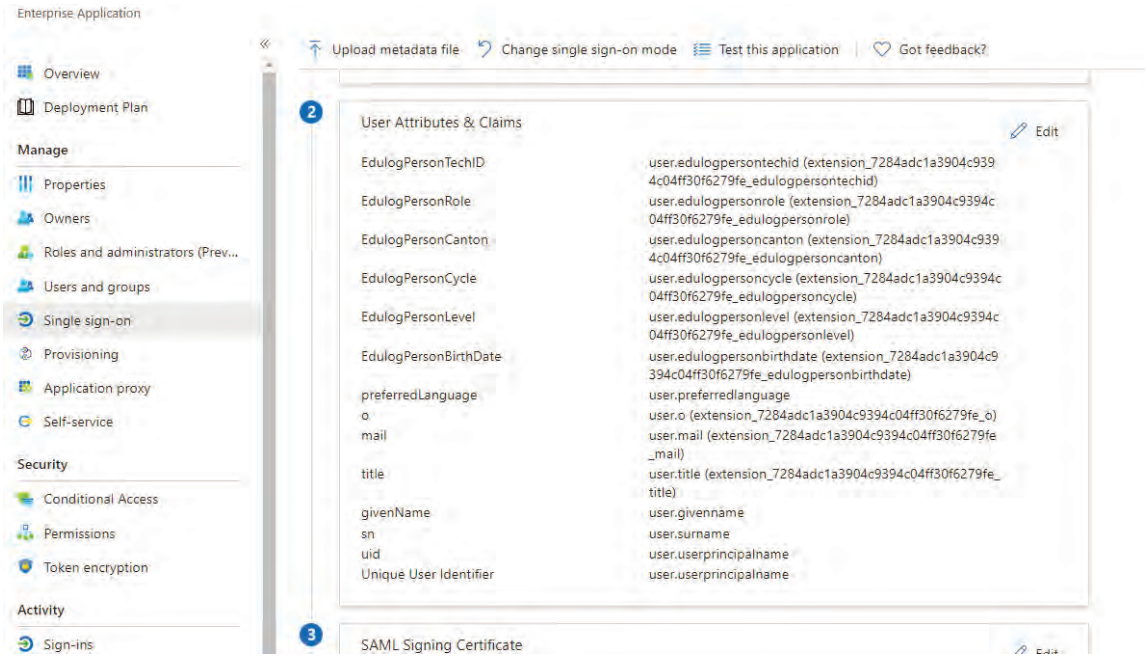
Voici un exemple avec l'attribut *EdulogPersonTechID* :



Répéter cette opération pour chacun des attributs. La liste finale des claims doit ressembler à ceci :



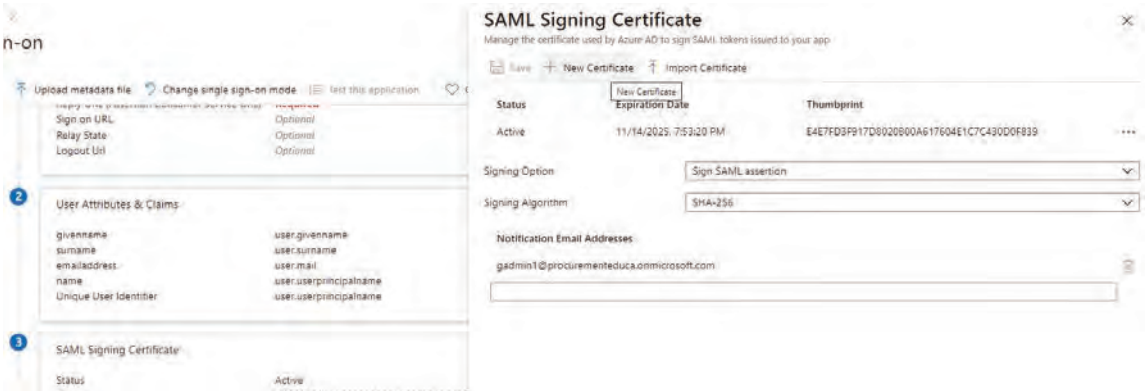
Une fois les claims validés, la partie « User attributes & Claims » de la page de configuration SAML de l'application ressemblera à ceci :



6.2.4 Générer un certificat pour la signature des assertions

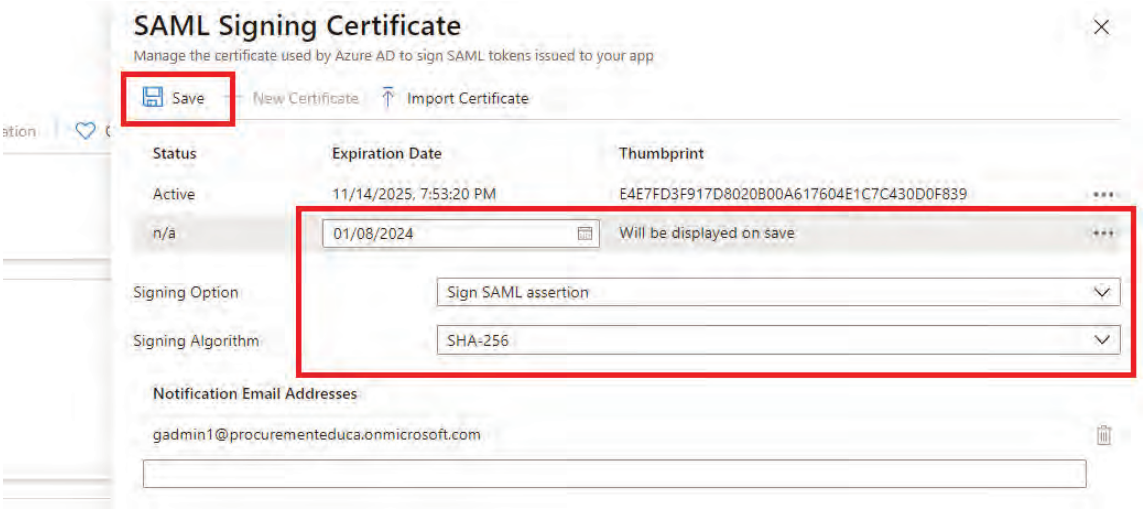
Il faut maintenant vérifier que le certificat remplit les conditions de sécurité exigées par Edulog[5]. Lors de la création de l'*Enterprise Application*, *Azure* génère automatiquement un certificat X509 v3. Ce certificat ne remplit pas les conditions de sécurité requises. Il faut donc créer un nouveau certificat avec les conditions de sécurité requises (c'est-à-dire 3 ans de validité, utilisation de l'algorithme de cryptage SHA-256 ; ne pas modifier ces valeurs) :

a. Pour créer le nouveau certificat : au point « SAML Signing Certificate » cliquer sur « Edit », puis dans la nouvelle fenêtre dans « New Certificate ». Il sera généré avec une validité de 3 ans uniquement.

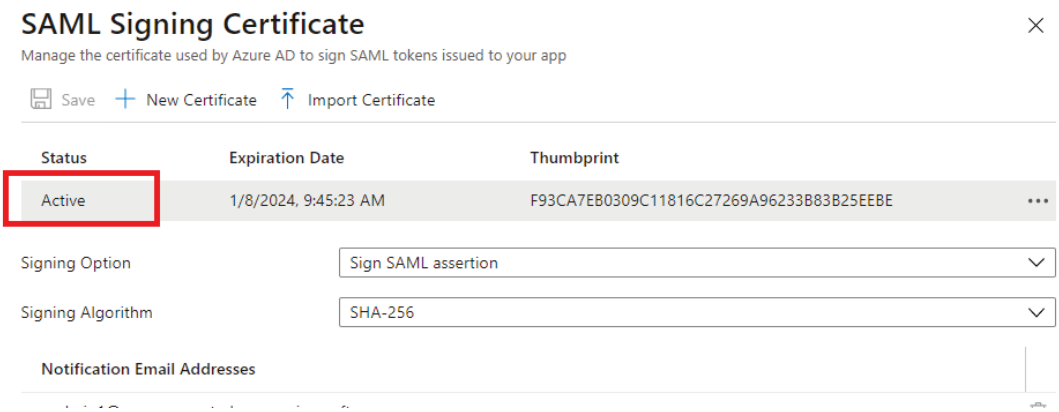


[5] Voir le document https://edulog.ch/fr/adhesion/documentation « Exigences de sécurité pour l'intégration ».

b. Une fois le certificat créé, il faut sauvegarder pour que celui-ci soit pris en compte.



c. Finalement le nouveau certificat doit être activé (cliquez sur les 3 points à droite), l'ancien sera alors éliminé. Le statut du certificat deviendra « Active ».



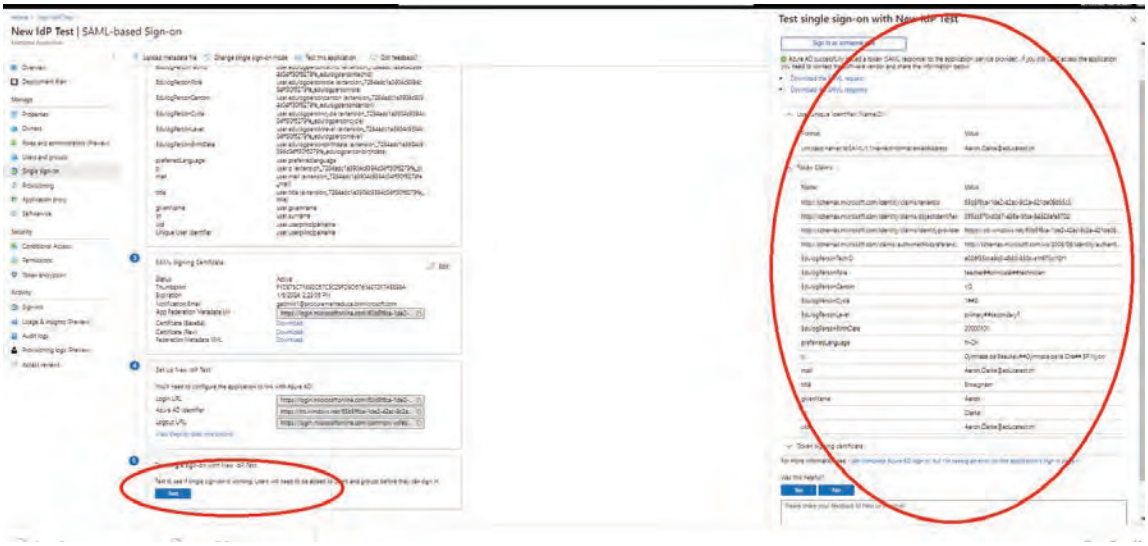
La clef doit avoir une validité de 3 ans. Toute autre valeur empêchera l'achèvement de l'onboarding à Edulog.

6.2.5 Faire un test de connexion sur le SAML-Endpoint

Le point « Test single sign-on with New IdP Test » de la configuration « SAML-based Sign On » permet de tester la configuration générée. Elle ne représente pas la connexion finale avec Edulog, mais permet de voir les attributs envoyés dans une assertion SAML via l'application Azure.

Le test doit se faire en utilisant l'utilisateur autorisé au chapitre 6.1 et son mot de passe. Sur le côté droit de l'écran, les valeurs transmises apparaissent au paragraphe « Token Claims ».

Par exemple :



Lorsque le test est valide, les valeurs ainsi que le message « Azure AD successfully issued a token (SAML Response)… » apparaissent.

6.2.6 Récupérer le lien et le fichier des métadonnées de votre application

- Dans « SAML-Based Sign-on » au point « SAML Signing Certificate », copier le lien « App Federation Metadata URL » qui est de la forme suivante : https://login.microsoftonline.com/XXXXXXXX-1de2-42ac-9c2a-421de09d55c3/federationmetadata/2007-06/federationmetadata.xml?appid=XXXXXXX-0edb-465a-9927-XXXXXXXXX
- Puis, toujours au point « SAML Signing Certificate », cliquer sur le bouton « Download » à côté du paragraphe « Federation Metadata XML ».

Envoyer ce fichier Metadata XML ainsi que le lien antérieur à ELCA pour réaliser l'*onboarding*.

6.2.7 Changer l'URL Reply (Assertion Consumer Service URL)

Dès qu'ELCA a validé votre configuration, vous recevez l'URL-Reply définitive vous sera transmise. Il faut l'insérer conformément au chapitre 6.2, point 2.

L'Enterprise Application sera alors configurée pour Edulog.

7. Annexe : Problèmes possibles

Si des utilisateurs sont créés et ne sont pas autorisés comme spécifié au chapitre 6.1, le test de connexion – vu au chapitre 6.2.5 « Faire un test de connexion sur le SAML-Endpoint » – ne marchera pas. Un message « Signing is unsuccessful » comme celui de l'exemple suivant sera alors affiché :