Geschäftsstelle | Secrétariat Edulog
Erlachstrasse 21
3012 Bern

+41 31 300 55 99
info@edulog.ch

TECHNIQUE

Préparation d'une infrastructure locale (*AD* local et *AD FS*) en tant qu'IdP

22.02.2022 – 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

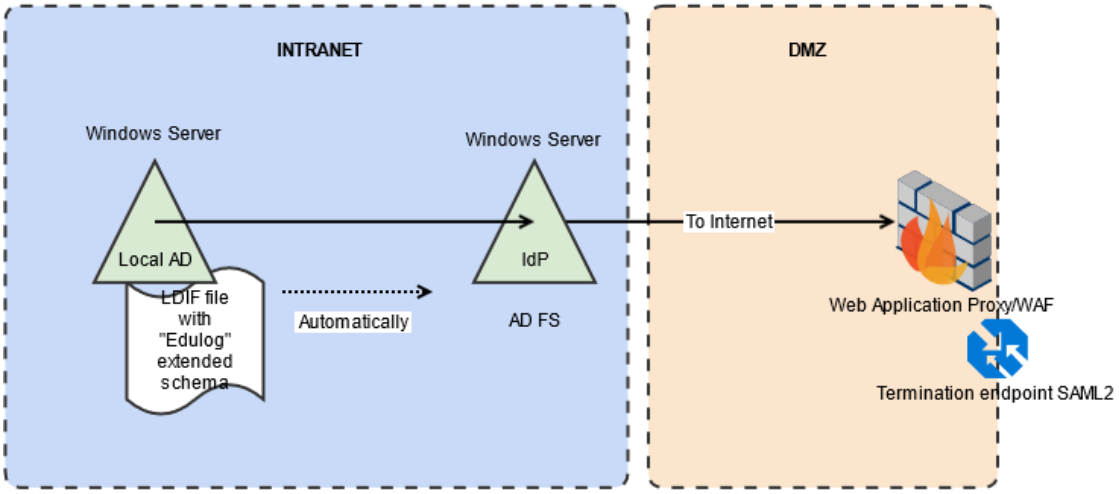
1. But du document

Ce document montre comment un fournisseur d'identités (IdP) peut préparer une infrastructure locale (*AD local* et *AD FS*).

Pour adhérer à Edulog, un IdP doit :

- **Vérifier que ses identités disposent d'un certain nombre d'attributs**[1]. Or certains de ces attributs n'existent pas originellement dans le schéma d'un *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 configurer *AD FS* pour jouer ce rôle d'interface.

Ce document s'adresse aux IdP qui ont un *AD* local et utilisent *AD FS* 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 le rôle *Active Directory Federation Services* (*AD FS*) pour connecter avec Edulog en utilisant le protocole SAML2.

3. Procédure complète

Ci-dessous un aperçu des 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	Installation d'un serveur *AD* FS	Chapitre 5
3	Configuration du serveur *AD* FS avec Edulog	Chapitre 6
4	Réaliser les tests de connexion avec ELCA.	Après
5	Réaliser la fédération des identités avec ELCA.	Après

Ce document traite les points 1 et 3.

[2] D'autres étapes non-techniques sont nécessaires pour l'intégration dans la Fédération. Elles ne sont pas traitées dans ce document. Un aperçu sur le processus complet se trouve sous https://edulog.ch/fr/adhesion.

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 réaliser 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. Les nouveaux attributs sont automatiquement disponibles pour les serveurs appartenant à la forêt.

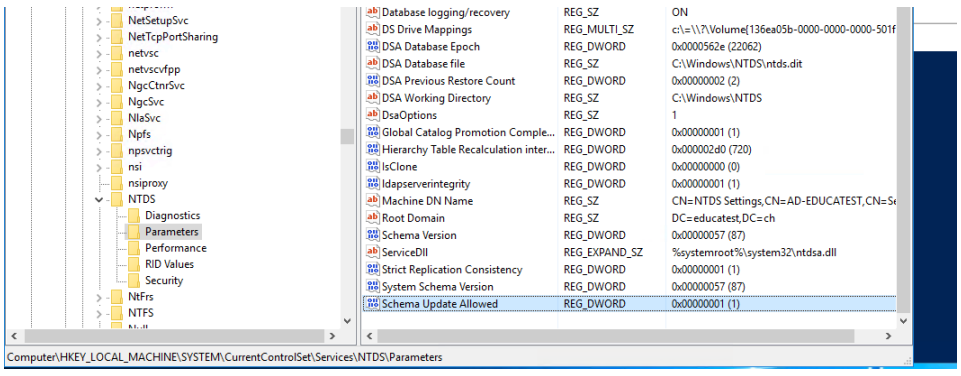
Fichier LDIF : la version actuelle du fichier LDIF utilisé dans ce document peut être demandée au secrétariat Edulog via info@edulog.ch.

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

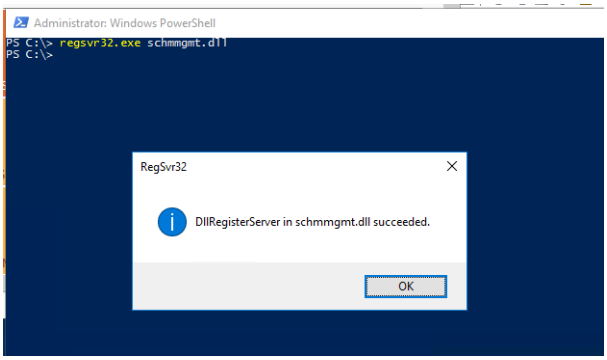
Une clef du registre doit être ajoutée sous HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters. Le nom de la nouvelle clef doit être « Schema Update Allowed » de valeur 1 et format REG_DWORD.



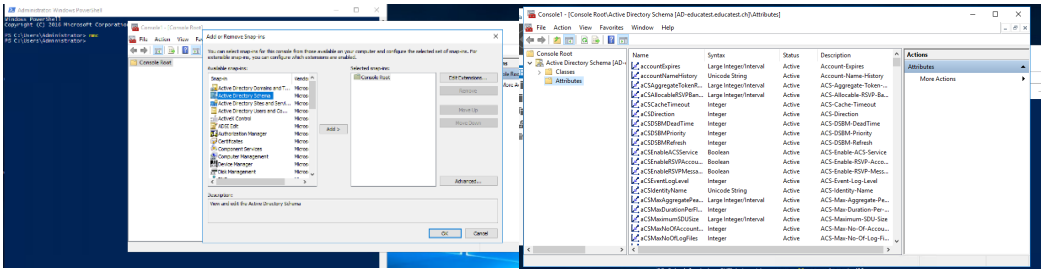
[3] Pour ces sous-tâches, le document Microsoft suivant peut être utilisé : https://social.technet.microsoft.com/wiki/contents/articles/51121.active-directory-how-to-add-custom-attribute-to-schema.aspx

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*

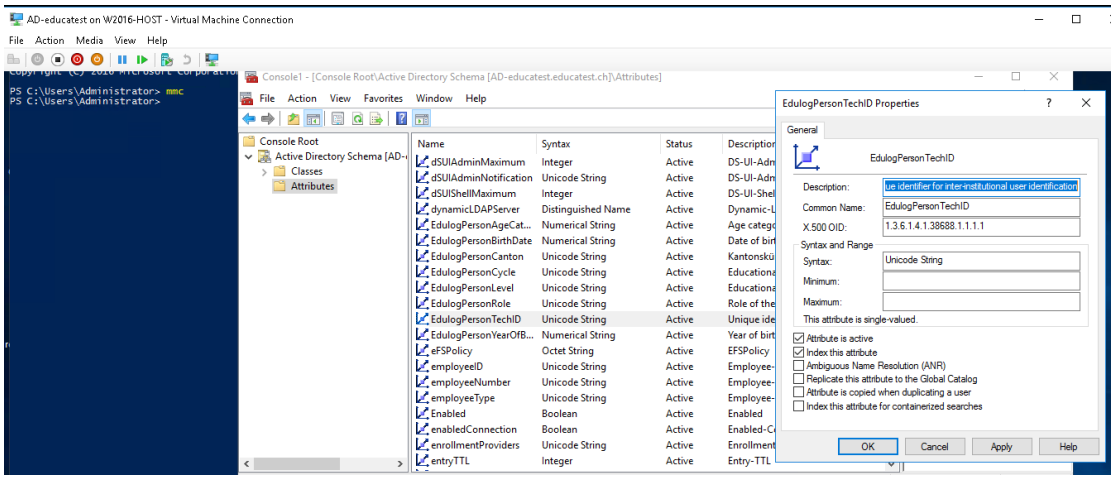
Pour importer le fichier LDIF avec les nouveaux attributs dans le schéma *AD*, (en tant qu'administrateur du schéma/domaine), utiliser la commande :

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

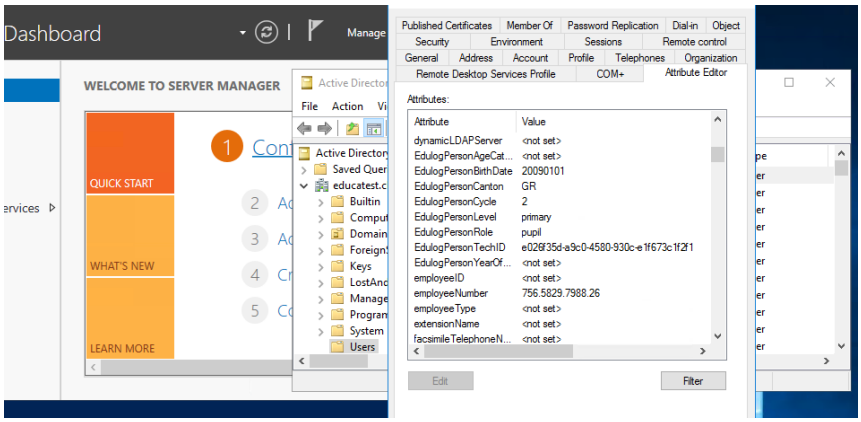
Important : le fichier LDIF doit être modifié pour prendre en compte le nom du domaine dans lequel il est utilisé (ex : DC=educatest,DC=ch si le domaine est educatest.ch)

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 le domaine.



5. Installation d'un serveur avec le rôle *AD FS*

Active Directory - Federation Services (*AD FS*) est l'implémentation de Windows fournissant des services de fédération à une architecture *AD*. Entre autres, elle permet la mise en œuvre d'une interface SAML.

Pour cela, il faut préparer un serveur Windows (préférablement Windows server 2016 ou plus) et réaliser l'installation du rôle d' *AD FS*[4].

De plus, il faut tenir compte d'une série de « bonnes pratiques » que définit Microsoft[5] Entre autres, l'installation d'un ou plusieurs Web Application Proxy/ies, qui n'est pas obligatoire, mais fortement recommandé pour un ensemble en production.

6. Configuration du serveur *AD* FS

La configuration du lien SAML avec Edulog se fait en trois parties :

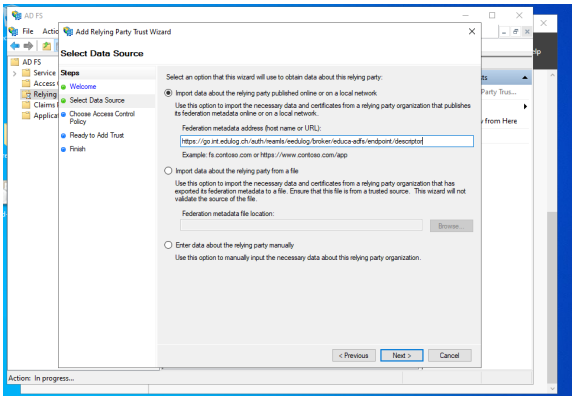
1. Création d'un Relying Party Trust
2. Valider le certificat d'Edulog
3. Création d'une Claim Issuance Policy

A noter qu'un « Relying Party » est un *Service Provider* sous SAML (par simplification).

6.2 Création d'un *Relying Party Trust* pour Edulog

Dans le serveur *ADFS*, depuis le « Server Manager », lancer l'application *AD FS* (sous l'onglet « Tools »). Cliquer sur *AD FS* et « Relying Party », sélectionner « Add Relying Party Trust ».

6.2.1 Importer le fichier metadata d'Edulog

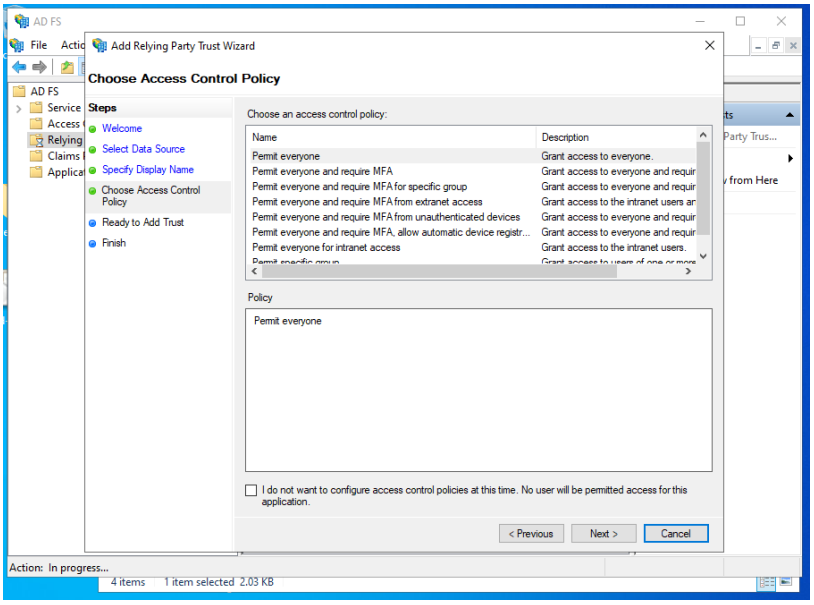


Trois options sont possibles pour réaliser la configuration.

Les deux premières sont préférables : écrire le lien http où trouver le fichier metadata d'Edulog, ou bien importer ce même fichier. Dans les deux cas, il est nécessaire de contacter au préalable ELCA qui fournira l'information correspondante.

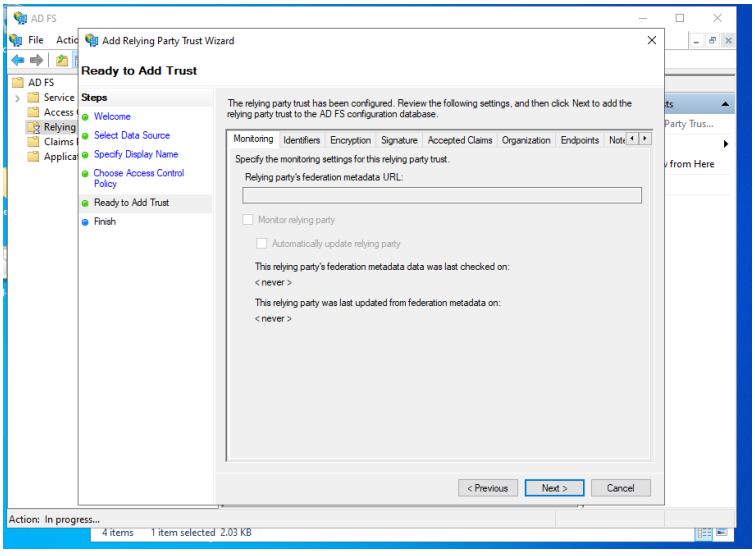
[4] Ce guide ne documente pas comment le faire. Voir par exemple : https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/checklist--setting-up-a-federation-server.
[5] Voir https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/best-practices-securing-ad-fs

6.2.2 Sélectionner la « Access Control Policy »

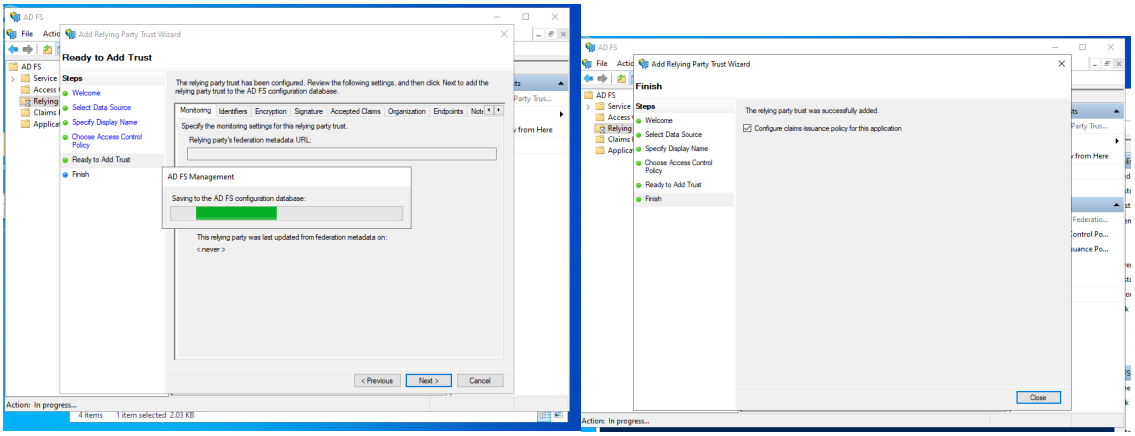


Sélectionner « Permit everyone ».

6.2.3 Cliquer sur « Next »

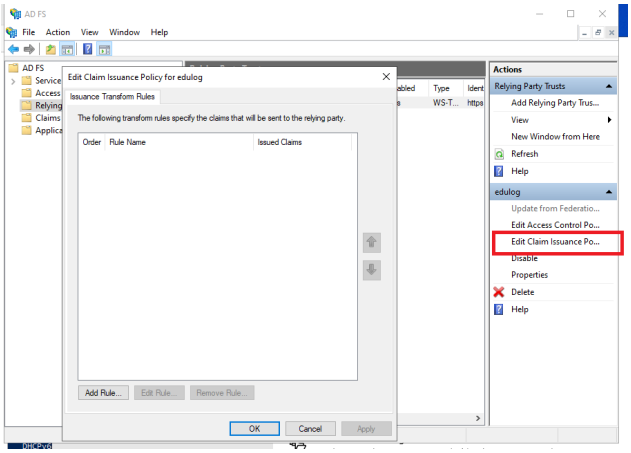


6.2.4 Attendre la création du « Trust » et conclure

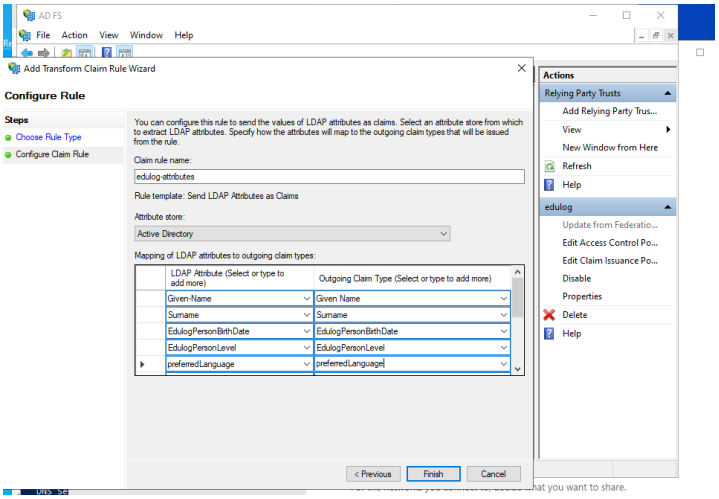


6.3 Création d'une *Claim Issuance Policy*

6.3.1 Cliquer sur « Edit Claim Issuance Policy »



6.3.2 Ajouter une règle pour les attributs d'Edulog

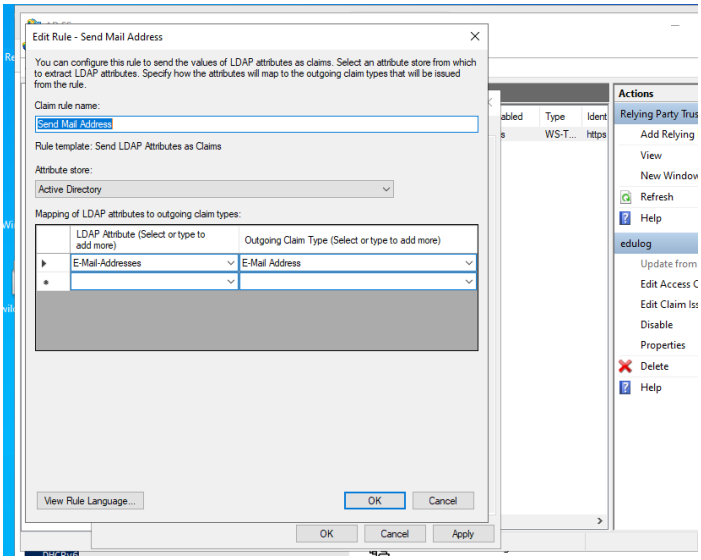


Choisir un « Attribute store » de type Active Directory. Puis écrire chacun des attributs d'Edulog dans la colonne « LDAP attribute » (**les attributs ne sont pas visibles dans le menu « drop-down », il faut écrire le nom exact des attributs sur chacune des lignes**).

Pour chacun des attributs, dans la colonne « Outgoing Claim Type », remettre le même attribut (qui maintenant est visible dans le menu « drop-down »).

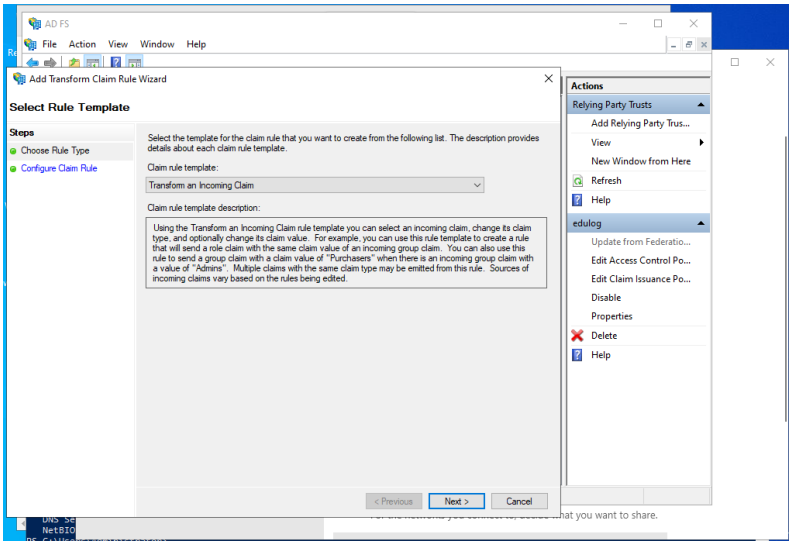
Cliquer sur « Finish ».

6.3.3 Créer une règle pour l'attribut « E-Mail Address »



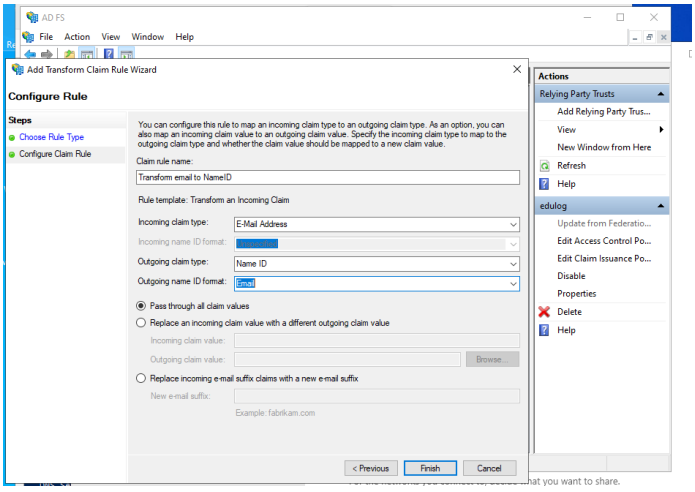
Refaire les mêmes opérations (cf. 6.3.2) avec l'attribut « E-Mail-Address » (dans le menu « drop-down »).

6.3.4 Créer une règle de type « Transform an Incoming Claim »



Cliquer sur « Next ».

6.3.5 Créer l'attribut « Name ID »



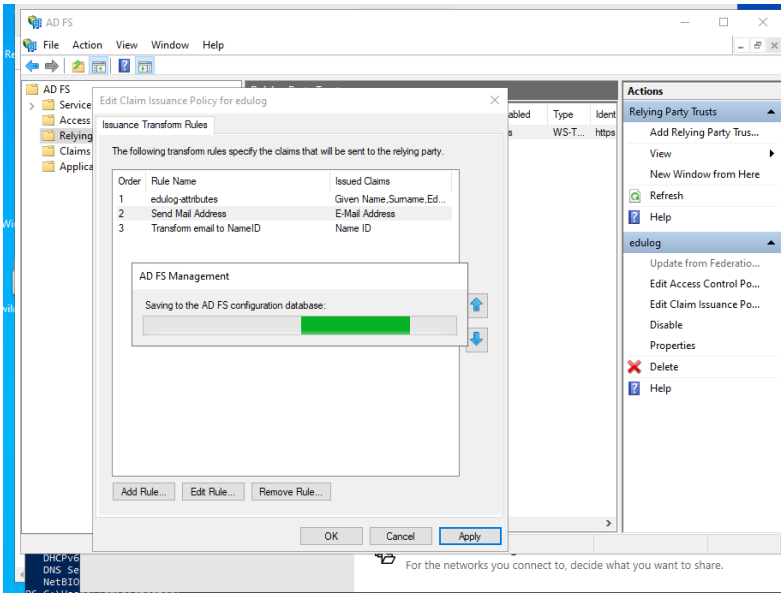
Pour cela sélectionner dans « Incoming claim type » le type « E-Mail Address ».

Choisir le format du Name ID de type « Email ».

Choisir l'option « Pass through all claim values ».

Cliquer sur « Finish ».

6.3.6 Valider la configuration



Cliquer sur « Apply » et attendre la création du lien.