Ajouter manuellement l'UID d'attribut requis dans le serveur ADFS

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Configurer

- Scénario 1
- Scénario 2
- Configurations

Ajouter une règle de revendication personnalisée dans le serveur ADFS sous Webex Relying Party Trust

- Étapes de création de cette règle

Introduction

Ce document décrit comment ajouter manuellement un UID d'attribut dans l'approbation de partie de confiance ADFS à l'aide d'un syntex.

Conditions préalables

Exigences

- serveur ADFS
- Concentrateur De Commande

Composants utilisés

- serveur ADFS
- Concentrateur de contrôle Cisco Webex
- AD sur site

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Configurer

Ceci est utile en cas de problème d'ajout d'une revendication d'attribut dans ADFS en raison d'un

attribut existant.

Scénario 1

Vous avez une approbation de partie de confiance existante qui a une règle de revendication créée avec un attribut nommé UID ou UID.

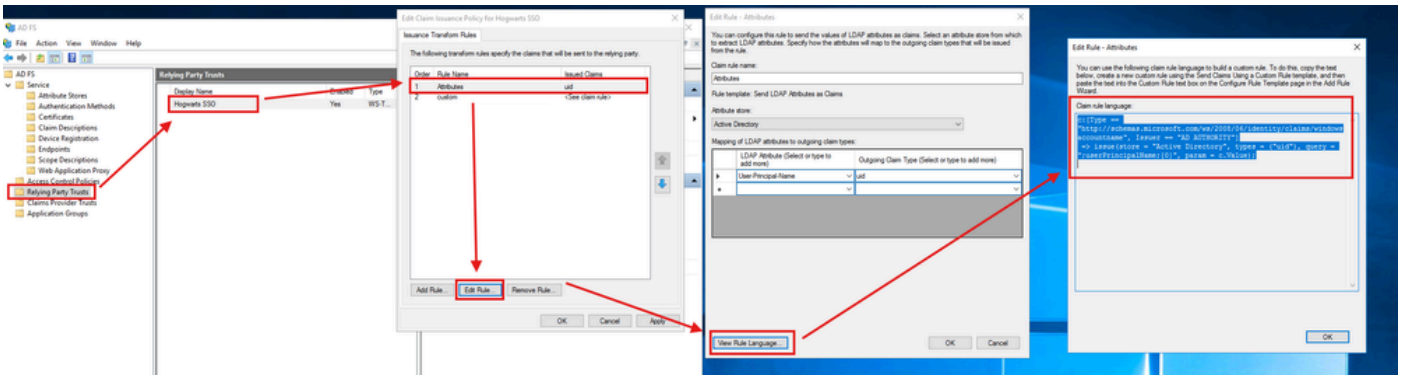
Ceci échoue l'authentification puisque Webex (SP) est sensible à la casse au sujet de l'attribut requis et il doit être uid et doit passer l'adresse e-mail de l'utilisateur dans la réponse SAML.

Scénario 2

Vous avez une approbation de partie qui a une règle de revendication passant un attribut nommé uid mais associé à un attribut différent dans AD que ce qui est nécessaire (emailAddress/UserPrincipleName). Cela crée des problèmes.

Configurations

Dans une configuration idéale, telle que décrite dans le guide Cisco Webex, la configuration ADFS doit se présenter comme suit :



Les administrateurs ADFS peuvent le consulter à partir de leurs approbations de partie de confiance-> Approbation qu'ils ont créée pour Webex -> Modifier la stratégie d'émission de demande -> Modifier la règle -> Attributs -> Afficher la langue de la règle.

Le langage de la règle en texte clair est le suivant :

c : [Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Émetteur == "AUTORITÉ AD"]
=> issue(store = "Active Directory", types = ("uid"), query = ";userPrincipalName ; {0}", param = c.Value);

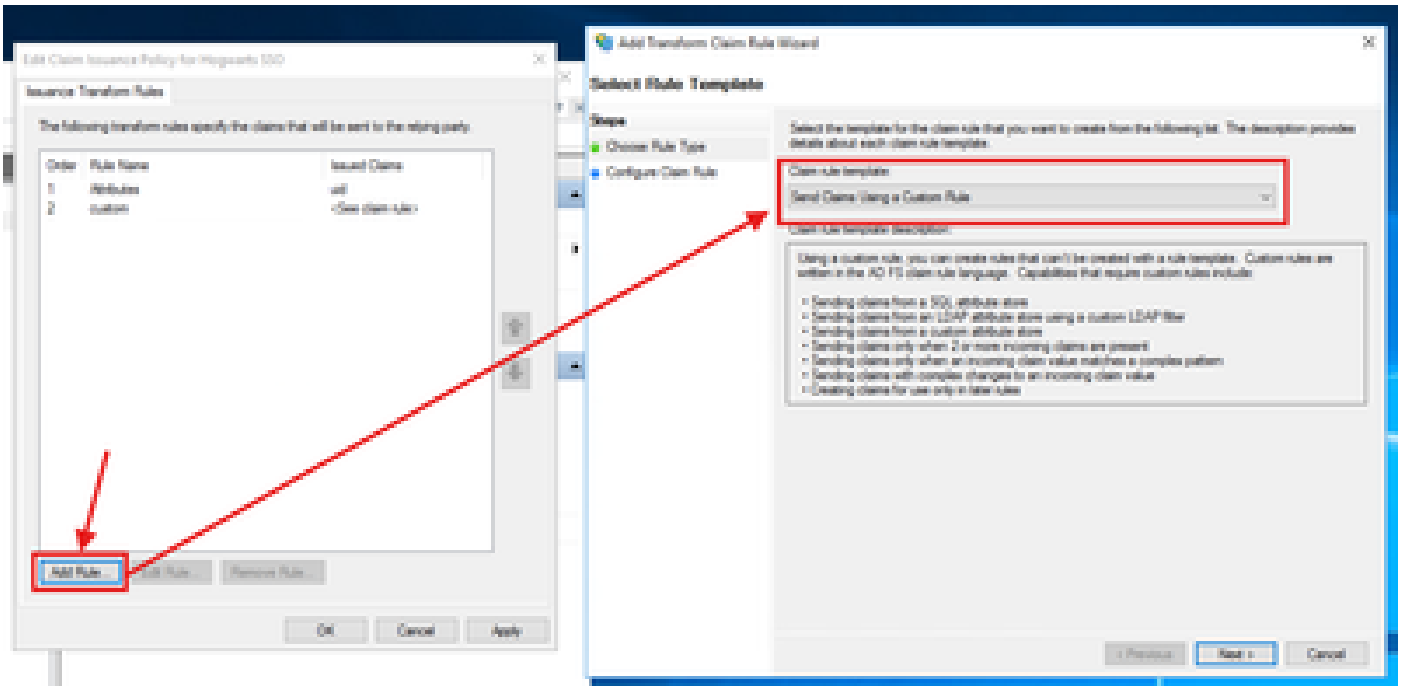
Comme la configuration ne s'affiche pas correctement, créez manuellement cette règle à l'aide du texte brut du langage de la règle.

Ajouter une règle de revendication personnalisée dans le serveur ADFS sous Webex Relying Party Trust

Étapes de création de cette règle

1. Dans le volet ADFS principal, sélectionnez la relation d'approbation que vous avez créée, puis sélectionnez Modifier les règles de revendication. Sous l'onglet Règles de transformation d'émission, sélectionnez Ajouter une règle.
2. Sélectionnez Envoyer les revendications à l'aide d'une règle personnalisée, puis sélectionnez Suivant.
3. Copiez la règle à partir de votre éditeur de texte (en commençant par c:) et collez-la dans la zone de règles personnalisée sur votre serveur ADFS.

Cela doit ressembler à ceci :



Une fois que cela est fait, vous pouvez tester SSO à partir du Control Hub et cela doit fonctionner comme prévu.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.