# Sécurité Web sur le cloud : Configurez les attributs utilisateur/groupe avec PingFederate et ADFS lors de l'utilisation de SAML.

## Contenu



## Introduction

Ce document décrit comment configurer les serveurs PingFederate et ADFS (Active Directory Federated Services) IDP pour envoyer les détails des utilisateurs/groupes au service Cloud Web Security afin de filtrer les stratégies de manière granulaire.

## Conditions requises

Cisco recommande que vous ayez une compréhension de base des éléments suivants.

- Connexion/accès administratif au serveur PingFed/ADFS
- Connaissance de la navigation sur le serveur PingFed/ADFS
- Pour que la granularité fonctionne sur le trafic HTTPS, l'inspection HTTPS doit être appliquée pour tout le trafic

## Configuration

Suivez les étapes ci-dessous pour configurer les attributs utilisateur/groupe avec PingFederate et ADFS.

### PingFed

Sous **Sources d'attribut >** onglet **Recherche utilisateur** :

- Contrat d'attribut : **GROUPES_AUTHENTIFIÉS**
  Source : **LDAP**

  Valeur: **membreDe**

- Contrat d'attribut : **SUJET_SAML**
  Source : **LDAP**

  Valeur: **sAMAccountName**

### ADFS

Sous **Relations de confiance >** Onglet **Approbation de partie de confiance** :

- Contrat d'attribut LDAP : **Nom du compte SAM**
  Type de revendication sortante LDAP : **ID du nom**

- Contrat d'attribut LDAP : **Groupes de jetons**
  Type de revendication sortante LDAP : **Groupe**

## Vérification

## Dépannage

Il n'y a pas de section de dépannage pour ce document.