# Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Composants utilisés](#)
[Informations générales](#)
[Problème](#)
[Solution](#)
[Configuration de pratique recommandée](#)
[Vérifiez](#)
[Dépannez](#)
[Informations connexes](#)

# Introduction

Ce document décrit comment configurer les services fédérés par Microsoft Active Directory (ADFS) comme fournisseur d'identité (IDP), qui envoie les petits groupes spécifiques de groupe au service de la sécurité Web de nuage de Cisco (CWS), plutôt qu'une liste complète d'adhésions à des associations.

# Conditions préalables

## Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration de sécurité Web de nuage utilisant le portail de ScanCenter
- Authentification du langage de balisage d'assertion de Sécurité (SAML)
- Gestion de serveur de Microsoft ADFS

## Composants utilisés

Les informations dans ce document sont basées sur la version 2.0 de Microsoft ADFS, s'exécutant sur les Windows Server 2008 R2.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

# Informations générales

Pendant la procédure d'authentification entre un navigateur de client, le serveur ADFS (le fournisseur ou l'IDP d'identité) et CWS (le fournisseur de services ou fournisseur de services),

toutes les informations est chiffré et ajouté à la chaîne d'URL dans le navigateur de client. Ceci signifie que la chaîne d'URL est plus longue quand plus d'informations sont envoyées à CWS.

En configurant l'authentification SAML (avec Microsoft ADFS) pour l'usage avec le service CWS, vous devriez configurer une confiance comptante d'interlocuteur pour fournir le nom d'utilisateur et l'information du groupe. Sécurité Web de nuage : Configurez l'utilisateur/groupe d'attributs avec PingFederate et ADFS tout en utilisant le SAML décrit cette étape plus en détail.

# Problème

Le nombre de groupes un utilisateur est ajouté à l'augmentation de volonté la taille URL. Si un utilisateur appartient à un grand nombre de groupes d'AD, l'URL deviendra une taille par lequel la limite URL imposée par navigateur soit atteinte, et la procédure d'authentification échouera.

Chaque navigateur peut définir leur propre longueur URL de maximum autorisé. RFC 2616 ne spécifie pas une longueur maximale, mais des limites pratiques sont imposées par des constructeurs de navigateur.

> Remarque: Il n'est pas possible de définir explicitement un nombre maximal de groupes parce qu'un groupe n'a pas un nombre fixe de caractères. Par exemple « GroupA » a moins de caractères que « Test_Group_A ». Définir un certain nombre de groupes qui reste au-dessous de la limite URL dépendra du décompte de caractères du nom de nom de domaine + de groupe.

# Solution

Vous pouvez configurer le serveur de Microsoft ADFS pour inclure les groupes spécifiques dans la procédure d'authentification. Typiquement vous sélectionneriez seulement les groupes utilisés dans les règles de filtrage de Web CWS. Exécuter un audit des stratégies existantes aidera à déterminer quels groupes sont déjà en service.

Nouveau et des déploiements existants devrait suivre la configuration de pratique recommandée tracée les grandes lignes ci-dessous. Ceci fournit les indemnités suivantes :

- Garde la taille URL à un minimum
- Accélère la procédure d'authentification entre l'IDP (ADFS) et le fournisseur de services (CWS)
- Enregistre la bande passante sur chaque demande d'authentification

## Configuration de pratique recommandée

Créez la « acceptation transforment des règles » en ouvrant des confiances de fournisseur de demandes et en créant deux transformez les règles :

> Le modèle de règle de demande d'utilisation « envoient des attributs de LDAP comme demandes »
>
> > **Mémoire d'attribut :** AD ;

**Attribut de LDAP :** Jeton-groupes - Noms sans réserve ;

**Type sortant de demande :** Groupe

Le modèle de règle de demande d'utilisation « envoient des attributs de LDAP comme demandes »

**Mémoire d'attribut :** AD ;

**Attribut de LDAP :** Sam-Compte-nom ;

**Type sortant de demande :** Nom

Créez la « émission transforment des règles » en ouvrant des confiances comptantes de partie et en créant deux transformez les règles :

L'utilisation modèle « transforment demande entrante »

**Type entrant de demande :** Nom

**Format :** non spécifié

**Type sortant de demande :** ID de nom

**Format :** Non spécifié

Choisi « traversez toutes les valeurs de demande »

Utilisez la « fonction émulation ou filtrez une demande entrante »

**Type entrant de demande :** Groupe

Choisi « traversez seulement les valeurs de demande qui commencent par une valeur spécifique :

Spécifiez vos noms de groupe d'AD

# Vérifiez

- Tandis qu'ouvert une session en tant qu'utilisateur final, parcourez à http://whoami.scansafe.net
- La sortie devrait répertorier seulement les groupes spécifiés dans la procédure ci-dessus, plutôt qu'une liste complète d'adhésions à des associations.

# Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

# Informations connexes

- Support et documentation techniques - Cisco Systems