

Contenu

Question :

Pourquoi est-ce que je ne peux pas trouver des groupes d'AD pour les domaines de confiance tout en faisant une recherche dans le répertoire dans des stratégies d'accès ?

Environnement : L'appliance de sécurité Web de Cisco (WSA), authentification NTLM, a fait confiance à des domaines

Symptômes :

- L'utilisateur essaye à la consultation par « groupe de Répertoire actif » à l'utiliser comme *définition de membre de stratégie* dans une de ses stratégies d'Access et le groupe n'affiche pas dans la recherche dans le répertoire.
- Le groupe appartient à un domaine de confiance d'AD et pas le domaine que le WSA s'est joint à.

Ce comportement est par conception. Tout en configurant des groupes dans des stratégies d'accès, les groupes des domaines de confiance ne révéleront pas dans la *recherche dans le répertoire*.

Sur toutes les versions d'AsyncOS, WSA a la capacité d'authentifier des utilisateurs d'un domaine différent et d'apparier leurs groupes respectifs d'AD **si** l'autre domaine a une confiance bi-directionnelle avec le domaine joint par WSA.

Dans un tel scénario, nous pouvons ajouter les groupes du domaine de confiance dans des stratégies d'accès utilisant les étapes ci-dessous :

1. Parcourez au GUI --> gestionnaire de sécurité Web --> stratégies d'Access --> <Policy Name> --> groupes sélectionnés et utilisateurs --> groupes
2. Introduisez manuellement dedans le nom entier de groupe, avec le nom de domaine, dans le champ de « *recherche dans le répertoire* »
3. Cliquez sur « ajoutent » le bouton
4. Cliquez sur fait et puis soumettez et commettez les modifications

Notez que le WSA n'appariera pas les groupes manuellement configurés si l'autre domaine n'a pas des relations bidirectionnelles de confiance avec le domaine joint par WSA

Remarque: Sur des versions 7.7 et ultérieures d'AsyncOS, WSA prend en charge de plusieurs royaumes NTLM et pour des scénarios où il n'y a aucun rapport de confiance entre les 2 domaines, nous pouvons créer un nouveau royaume NTLM pour le deuxième domaine. Avec de plusieurs royaumes NTLM, WSA peut des groupes de consultation de différents domaines dans les stratégies d'accès.