Configurer des utilisateurs, des groupes et des ordinateurs à partir d'Active Directory pour la synchronisation avec le service de connecteur OpenDNS

Table des matières

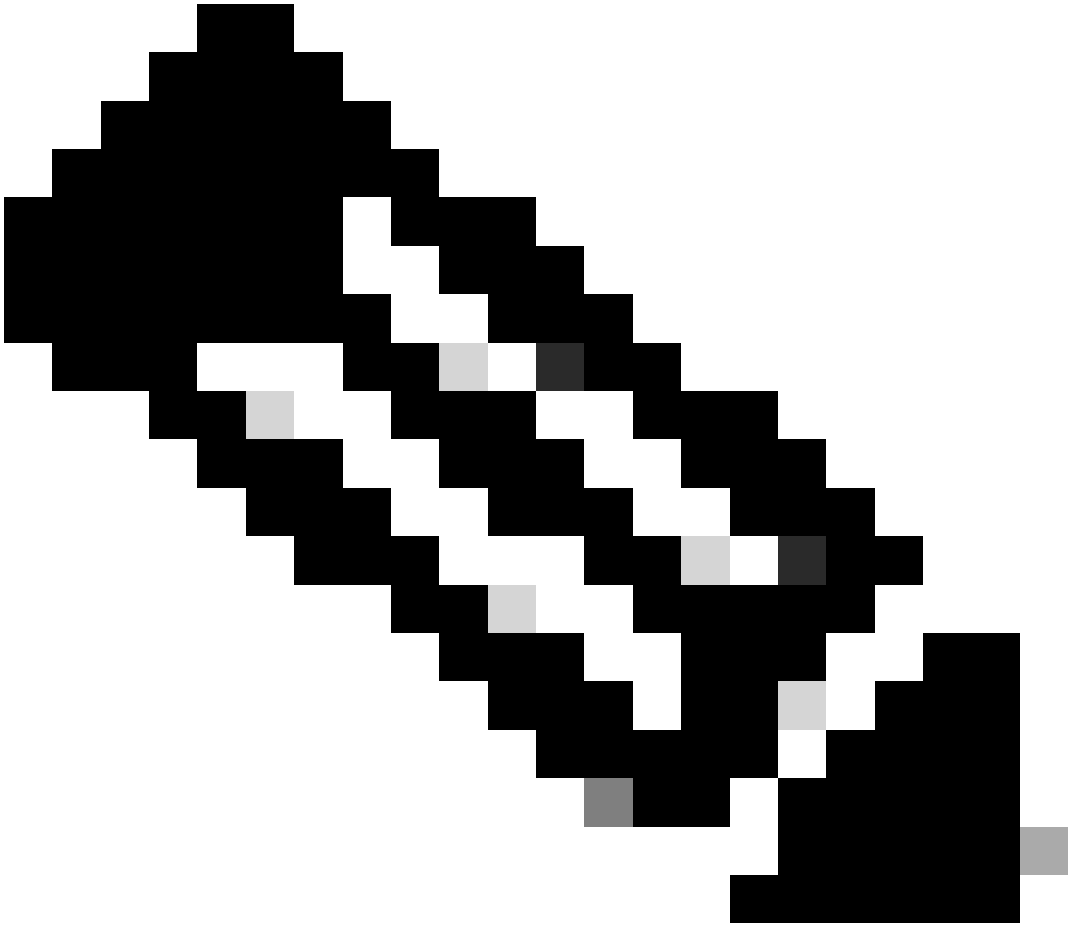
Introduction

Ce document décrit comment synchroniser des utilisateurs, des groupes et des ordinateurs à partir d'Active Directory avec le service OpenDNS Connector.

Aperçu

Dans le cadre de son fonctionnement, le service OpenDNS Connector synchronise une liste d'utilisateurs, de groupes et d'ordinateurs à partir d'Active Directory à l'aide du protocole LDAP. Cet article décrit comment vérifier que le compte OpenDNS_Connector a les autorisations correctes pour lire ces objets.

Chaque objet (utilisateurs/groupes/ordinateurs) dans Active Directory est associé à des autorisations de sécurité ACL, et chaque objet doit autoriser le compte utilisateur OpenDNS_Connector à lire ses attributs.



Remarque : Cet article suppose que les pré-requis normaux pour le compte 'OpenDNS_Connector' ont déjà été vérifiés. Si des utilisateurs/groupes AD sont absents du tableau de bord, consultez d'abord cet article : Utilisateurs/groupes AD manquants dans le tableau de bord Umbrella.

Autorisations par défaut

Par défaut, tous les utilisateurs authentifiés peuvent lire les propriétés des utilisateurs/groupes/ordinateurs, de sorte que l'utilisateur OpenDNS_Connector n'a pas besoin d'autorisations supplémentaires pour effectuer la synchronisation LDAP.

Les autorisations par défaut sont normalement définies comme suit :

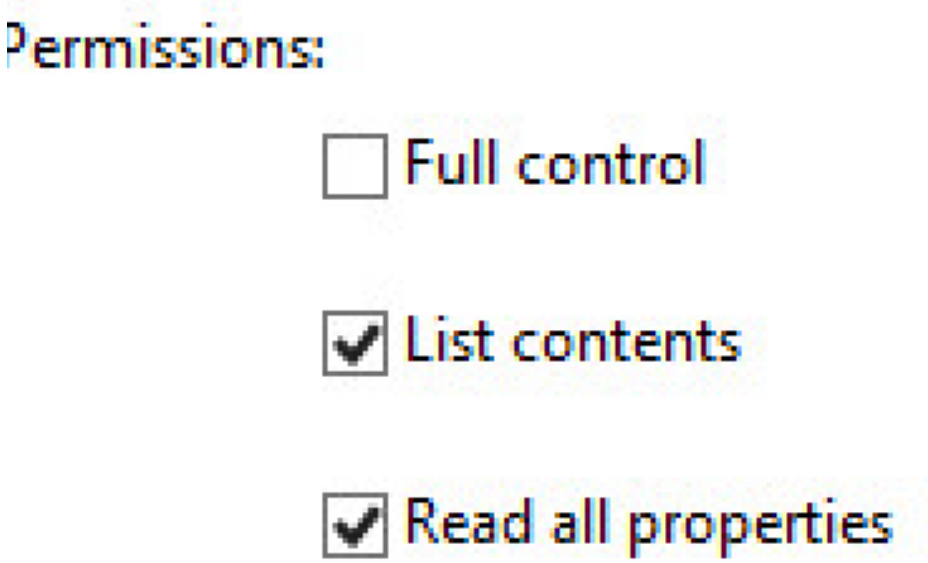
1) Le groupe « Accès compatible avec les versions antérieures à Windows 2000 » se voit attribuer des autorisations de lecture (lecture de toutes les propriétés) sur le domaine pour « Objets utilisateur descendants », « Objets groupe descendants » et « Objets ordinateur descendants ».

Vous pouvez revérifier ceci comme suit :

- Ouvrir les utilisateurs et ordinateurs Active Directory
- Cliquez sur 'Affichage' et cochez l'option 'Fonctionnalités avancées'.
- Cliquez avec le bouton droit sur l'objet Domaine et sélectionnez 'Propriétés' puis 'Sécurité > Avancé'
- Sélectionnez l'entrée « Accès compatible avec les versions antérieures à Windows 2000 » avec les autorisations « Spéciales » :

115011616667

- Cliquez sur 'Modifier' pour afficher ces autorisations en détail.
- Sélectionnez 'Objets utilisateur descendants' dans la section S'applique à
- Recherchez ces autorisations :

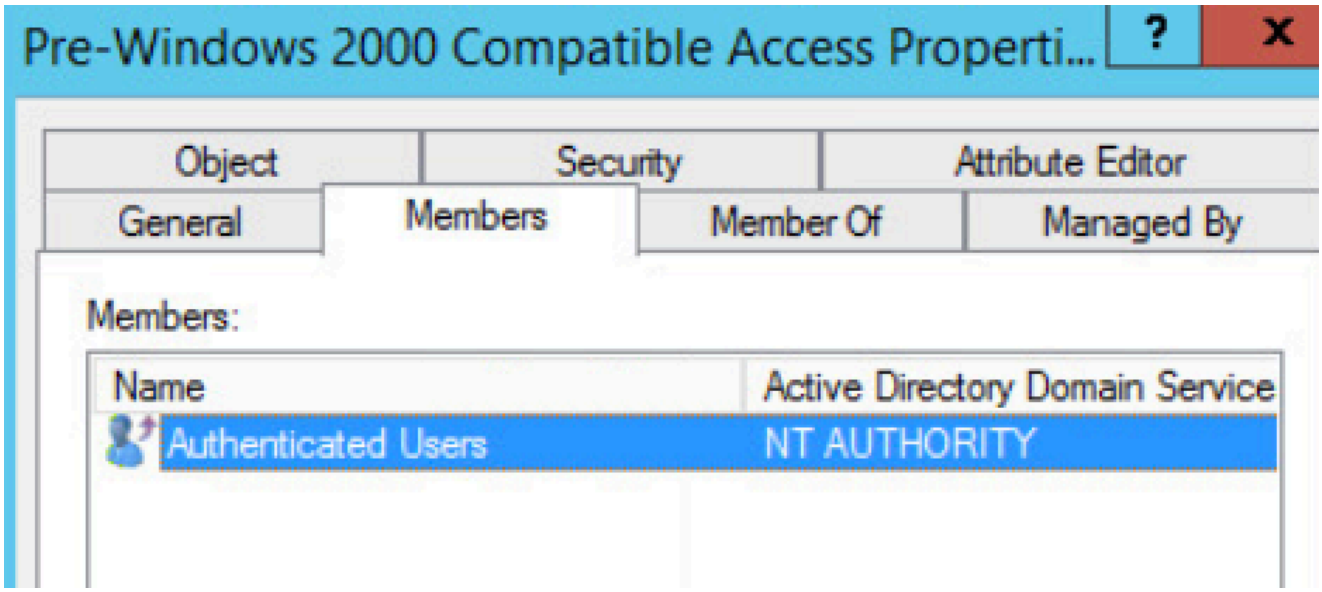


115011616687

- Répétez ces étapes pour 'Objets Groupe descendant' et 'Objets Ordinateur descendant'

2) Le groupe Tous les utilisateurs authentifiés est membre du groupe Accès compatible pré-Windows 2000 qui fournit ces paramètres à tous les utilisateurs.

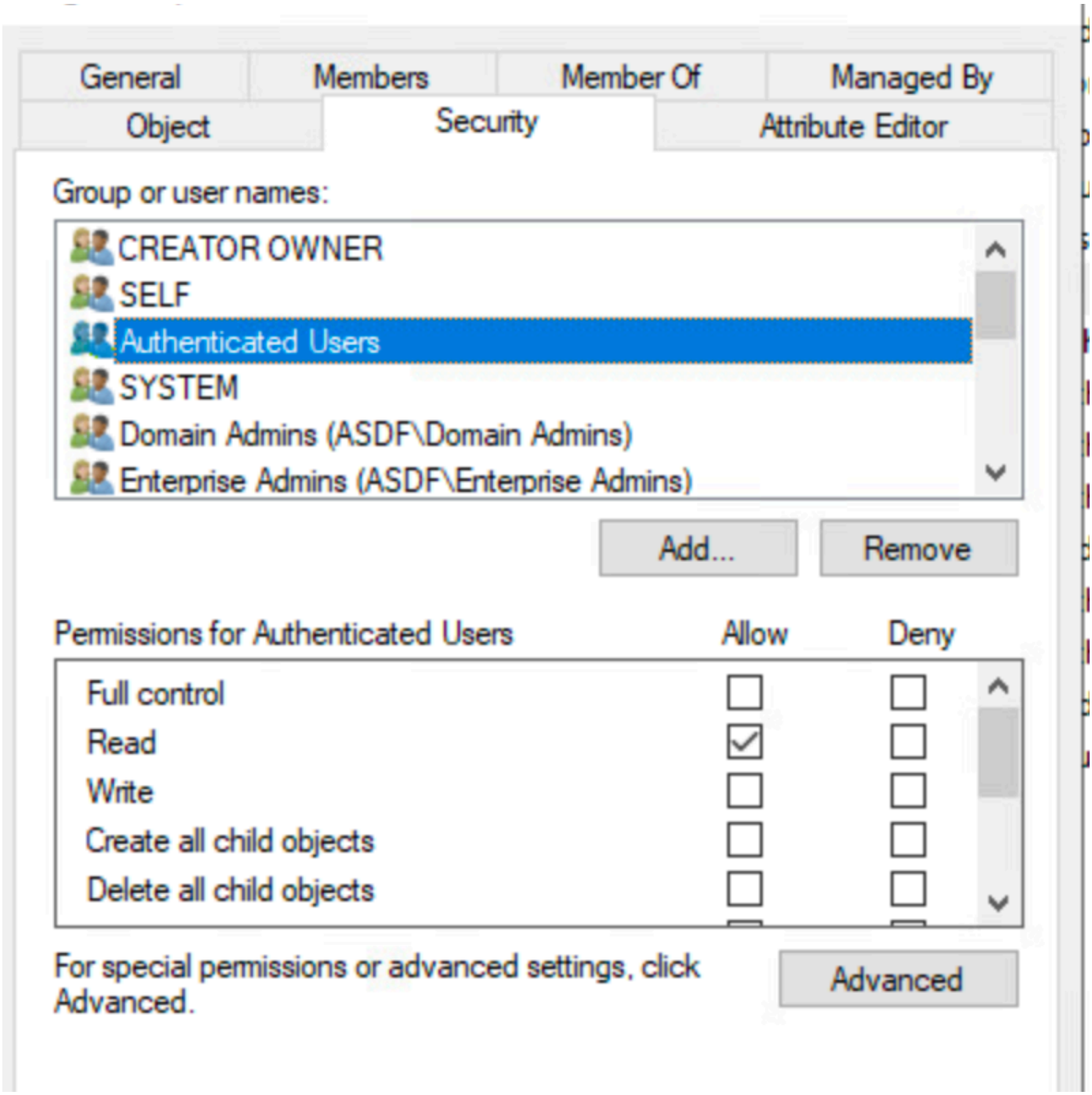
- Cliquez avec le bouton droit sur le groupe Accès compatible avec les versions antérieures à Windows 2000, qui se trouve normalement dans le conteneur Active Directory intégré.
- Sélectionnez 'Propriétés' et accédez à l'onglet 'Membres'.
- Vérifiez si 'Utilisateurs authentifiés' est répertorié.



115011616707

Cependant, dans certains environnements Active Directory, ce modèle d'autorisations a pu être modifié et les utilisateurs authentifiés ont été supprimés. Cela peut se manifester par le fait que certains utilisateurs sont absents du tableau de bord Umbrella ou que les appartenances à des groupes sont incorrectes. Si c'est le cas, ajoutez l'utilisateur OpenDNS_Connector à ce groupe, redémarrez le service de connecteur et les éléments manquants s'affichent dans Umbrella.

Dans certains cas rares, cela ne résout toujours pas le problème. Si vous trouvez que c'est le cas, vérifiez l'onglet de sécurité des groupes dans Active Directory, assurez-vous que vous voyez les utilisateurs authentifiés répertoriés ici avec un accès en lecture d'archivage. Si cette case n'est pas cochée, cochez-la et redémarrez le service de connexion pour voir si les membres du groupe s'affichent. En outre, s'ils trouvent ce paramètre de sécurité absent de tous les groupes, ils doivent appliquer les modifications à tous les groupes globalement en bloc.



28728163336852

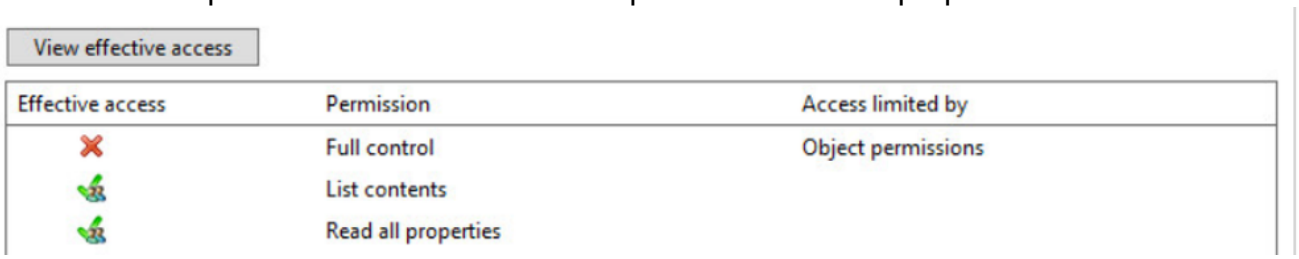
Afficher l'accès effectif

Vous pouvez utiliser l'outil 'Accès effectif' de Windows pour voir si l'utilisateur OpenDNS_Connector est capable de lire un objet particulier manquant (ou ayant une appartenance incorrecte au groupe).

- Ouvrir les utilisateurs et ordinateurs Active Directory
- Cliquez sur 'Affichage' et cochez l'option 'Fonctionnalités avancées'.
- Recherchez l'objet utilisateur et cliquez avec le bouton droit de la souris pour sélectionner «

Propriétés »

- Accédez à 'Sécurité > Avancé > Accès effectif' (cela peut dire 'Autorisations effectives')
- Cliquez sur 'Sélectionner un utilisateur' puis sélectionnez le compte d'utilisateur 'OpenDNS_Connector'.
- Cliquez sur OK, puis sur Afficher l'accès effectif
- Assurez-vous que l'utilisateur du connecteur peut lire toutes les propriétés :

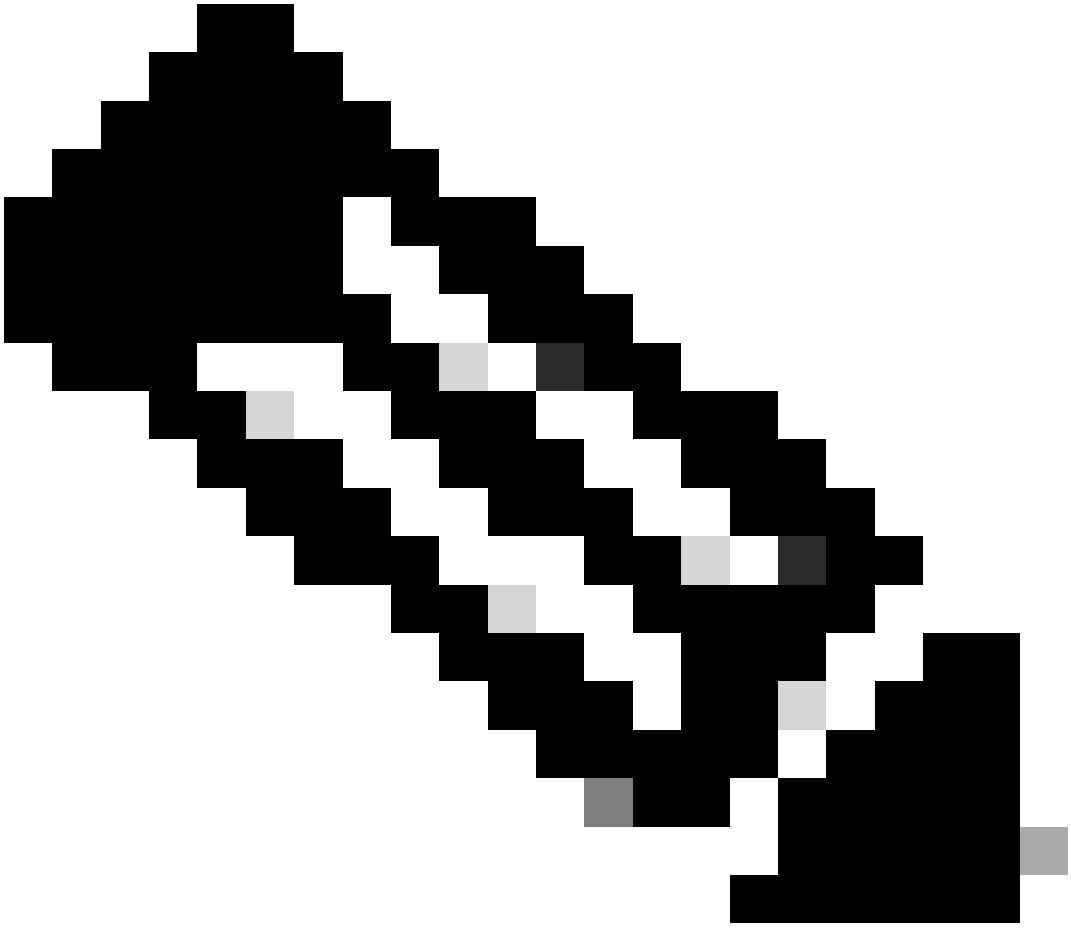


115011616727

Définition des autorisations LDAP OpenDNS_Connector

L'assistant « Delegate Control » dans Active Directory permet d'attribuer rapidement les autorisations nécessaires à l'utilisateur « OpenDNS_Connector » :

1) Accédez à Outils d'administration et ouvrez le composant logiciel enfichable Utilisateurs et ordinateurs Active Directory.
2) Cliquez avec le bouton droit sur le domaine qui inclut OpenDNS_Connector et sélectionnez "Delegate Control...", puis cliquez sur Next.
3) Ajoutez l'utilisateur OpenDNS_Connector, puis cliquez sur Suivant.
4) Sélectionnez "Lire toutes les informations utilisateur" et cliquez sur Suivant. [Voir l'image 3.]
7) Cliquez sur Terminer. [Voir l'image 6.]



Remarque : Ces étapes peuvent échouer si l'héritage est désactivé sur certains objets. Pour ces objets, vous devez définir les autorisations manuellement.

script userPerms

Le script powershell joint est une autre méthode pour obtenir les autorisations d'un objet spécifique (par ex. utilisateur) dans Active Directory. Veuillez inclure le résultat de ce script lorsque vous contactez le support technique Umbrella.

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.