Dépannage de " ; Accès refusé" ; Alerte dans le connecteur AD Umbrella

Table des matières

Introduction

Ce document décrit le dépannage de « Accès refusé » lorsque le connecteur Cisco Umbrella Active Directory (AD) est à l'état Alerte ou Erreur.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur Cisco Umbrella.

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.

Problème

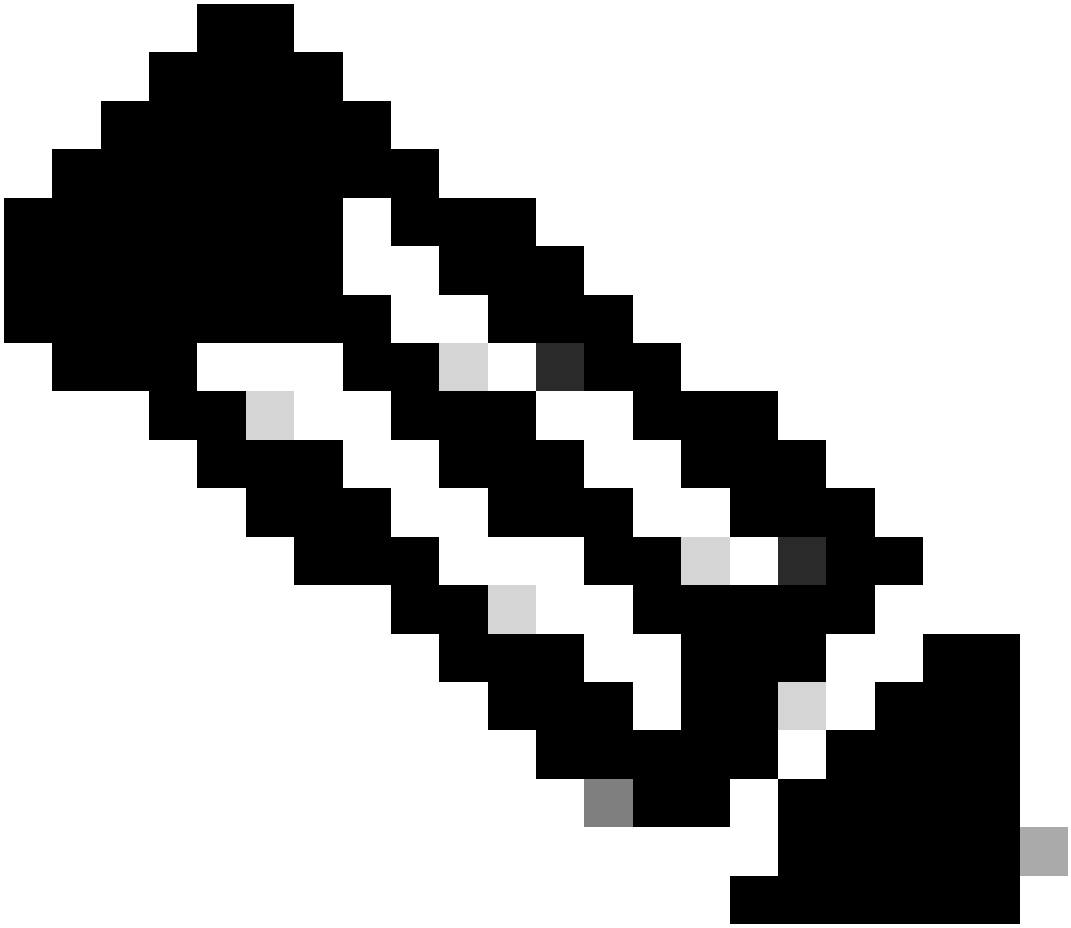
Vous remarquez qu'un connecteur AD affiche un état d'alerte ou d'erreur, et le message répertorié lorsque vous passez le curseur sur l'alerte inclut « Accès refusé » à l'un des serveurs AD inscrits.

Solution

Assurez-vous que l'utilisateur OpenDNS_Connector est membre des groupes AD suivants :

- Lecteurs de journaux des événements
- Utilisateurs COM distribués
- Contrôleurs de domaine d'entreprise en lecture seule

La solution est de s'assurer que DCOM, WMI et Manage Audit and Security Log sont configurés correctement sur le serveur AD en question.



> Remarque : Par défaut, plusieurs domaines ou forêts ne sont pas pris en charge. Reportez-vous à l'annonce relative à la prise en charge des domaines Multi-AD dans Umbrella. Vous pouvez également contacter Umbrella Support à propos de votre configuration pour obtenir de l'aide si vous rencontrez ces problèmes.

Pour vérifier les autorisations WMI :

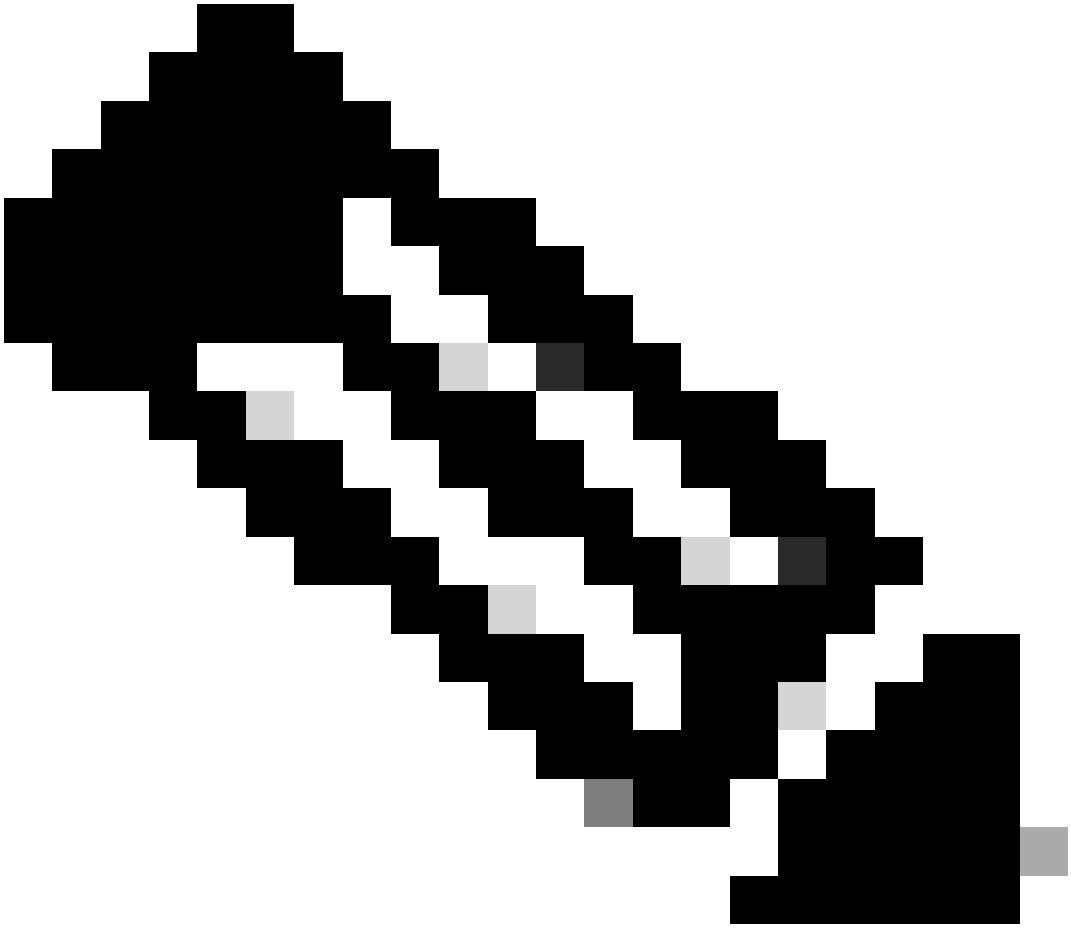
1. Sélectionnez Démarrer > Exécuter > wmimgmt.msc pour accéder à la console Contrôle de l'infrastructure de gestion Windows.
2. Cliquez avec le bouton droit sur Contrôle WMI > Propriétés > onglet Sécurité.

3. Sélectionnez Root > espace de noms CIMV2 et cliquez sur le bouton Security.
4. Ajoutez l'utilisateur OpenDNS_Connector et autorisez ces autorisations :

- Activer le compte
- Activation à distance
- Sécurité de lecture

Pour vérifier les autorisations DCOM :

1. À partir d'une ligne de commande, exécutez dcomcnfg.
2. Accédez à Racine de la console > Services de composants > Ordinateurs.
3. Cliquez avec le bouton droit sur Poste de travail et sélectionnez Propriétés.
4. Dans Propriétés du Poste de travail, sélectionnez l'onglet Sécurité COM.
5. Dans la section Autorisations de lancement et d'activation, sélectionnez Modifier les limites.
6. Ajoutez l'utilisateur OpenDNS_Connector et autorisez les autorisations Lancement à distance et Activation à distance.
7. Cliquez sur OK pour confirmer et fermer les Propriétés du Poste de travail.



Remarque : Dans la plupart des cas, si des modifications DCOM sont apportées, un redémarrage de ce contrôleur de domaine est nécessaire pour que les modifications prennent effet.

Pour vérifier « Gérer les journaux d'audit et de sécurité » sur les serveurs Windows 2003 :

1. Sur un contrôleur de domaine, ouvrez une invite de commandes et tapez cette commande (si vous exécutez Windows 2003, remplacez /r par /v) :

```
gpresult /scope computer /r
```

2. Recherchez la ligne Objets de stratégie de groupe appliqués. Elle contient une liste des stratégies appliquées à ce contrôleur de domaine. Prenez note d'un qui peut être appliqué à tous les contrôleurs de domaine.
(comme « Stratégie des contrôleurs de domaine par défaut »). Si aucun n'existe, vous devez en créer un et l'appliquer.

Pour modifier la stratégie appropriée :

3. Ouvrez le volet Gestion des stratégies de groupe (via Démarrer/Outils d'administration). Sélectionnez la stratégie souhaitée. Quelque chose dans le dossier « Contrôleurs de domaine » est un candidat probable.

4. Cliquez avec le bouton droit sur cette stratégie et sélectionnez Modifier pour afficher l'Éditeur de gestion des stratégies de groupe.

5. Accédez au dossier Configuration ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité\Stratégies locales\Attribution des droits utilisateur et sélectionnez Gérer le journal d'audit et de sécurité pour afficher ses propriétés.

6. Sélectionnez Définir ces paramètres de stratégie > Ajouter un utilisateur ou un groupe. Recherchez et sélectionnez l'utilisateur OpenDNS_Connector.

7. Exécutez la commande « gpupdate /force » sur le contrôleur de domaine pour vous assurer que la stratégie est appliquée.

Motif

Cette erreur indique généralement que l'utilisateur OpenDNS_Connector ne dispose pas des autorisations suffisantes pour fonctionner.

Le script Connecteur Windows définit normalement les autorisations requises pour l'utilisateur OpenDNS_Connector. Cependant, dans les environnements Active Directory stricts, certains administrateurs ne sont pas autorisés à exécuter des scripts VB sur leurs contrôleurs de domaine

et doivent donc répliquer manuellement les actions du script de configuration Windows.

Additional Information

Pour plus d'informations sur la résolution de ce problème, consultez la rubrique « Accès refusé ».

Si, après avoir confirmé/modifié les paramètres susmentionnés, vous voyez toujours des messages « Accès refusé » dans le tableau de bord, veuillez envoyer un message d'assistance aux journaux du connecteur comme indiqué dans cet article : Fournir une assistance avec les journaux du connecteur Active Directory.

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.