Dépannage du connecteur Umbrella avec WMI et DCOM Log Collection

Table des matières

Introduction

Aperçu

Journaux des événements WMI et DCOM

- Journaux DCOM
- Journaux WMI
- Journaux de suivi WMI

Introduction

Ce document décrit comment collecter et examiner les journaux WMI et DCOM pour résoudre les problèmes d'autorisation du connecteur Umbrella avec Active Directory.

Aperçu

Le service Umbrella Connector se connecte à Active Directory à l'aide de WMI (Windows Management Instrumentation) et de DCOM (Distributed Component Object Model). Si ce processus échoue, c'est généralement parce que l'utilisateur OpenDNS_Connector n'a pas les autorisations correctes pour DCOM ou l'espace de noms WMI. Dans ce cas, cette erreur peut apparaître dans les journaux du connecteur OpenDNS :

```
EventMonitor Attach error: [AccessDenied] Access denied
```

Pour résoudre ce problème, utilisez les conditions préalables détaillées dans le Guide de configuration de l'intégration Active Directory. Si un débogage supplémentaire est requis ou si la confirmation d'un problème d'autorisations est nécessaire, consultez les journaux appropriés sur le contrôleur de domaine Windows.

Journaux des événements WMI et DCOM

Les journaux d'événements doivent être collectés à partir du contrôleur de domaine auquel le connecteur Umbrella est connecté (pas nécessairement à l'endroit où le connecteur est installé).

Journaux DCOM

Avant d'afficher les journaux DCOM, activez le débogage supplémentaire sur le contrôleur de domaine :

1. Ouvrez l'Éditeur du Registre Windows (regedit.exe).
2. Naviguez jusqu'à l'adresse :

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole
   ```

3. Créez un nouveau DWORD nommé ActivationFailureLoggingLevelet définissez la valeur sur 1.
4. Créez un nouveau DWORD nommé CallFailureLoggingLevel et définissez la valeur sur 1.
5. Reproduisez l'erreur « Accès refusé » en redémarrant le connecteur.
6. Ouvrez l'Observateur d'événements Windows (eventvwr.msc).
7. Accédez à Journaux Windows > Système.
8. Filtrer les événements avec la source **DistributedCOM**. Un problème d'autorisations DCOM pour OpenDNS_Connector apparaît comme un événement pertinent.

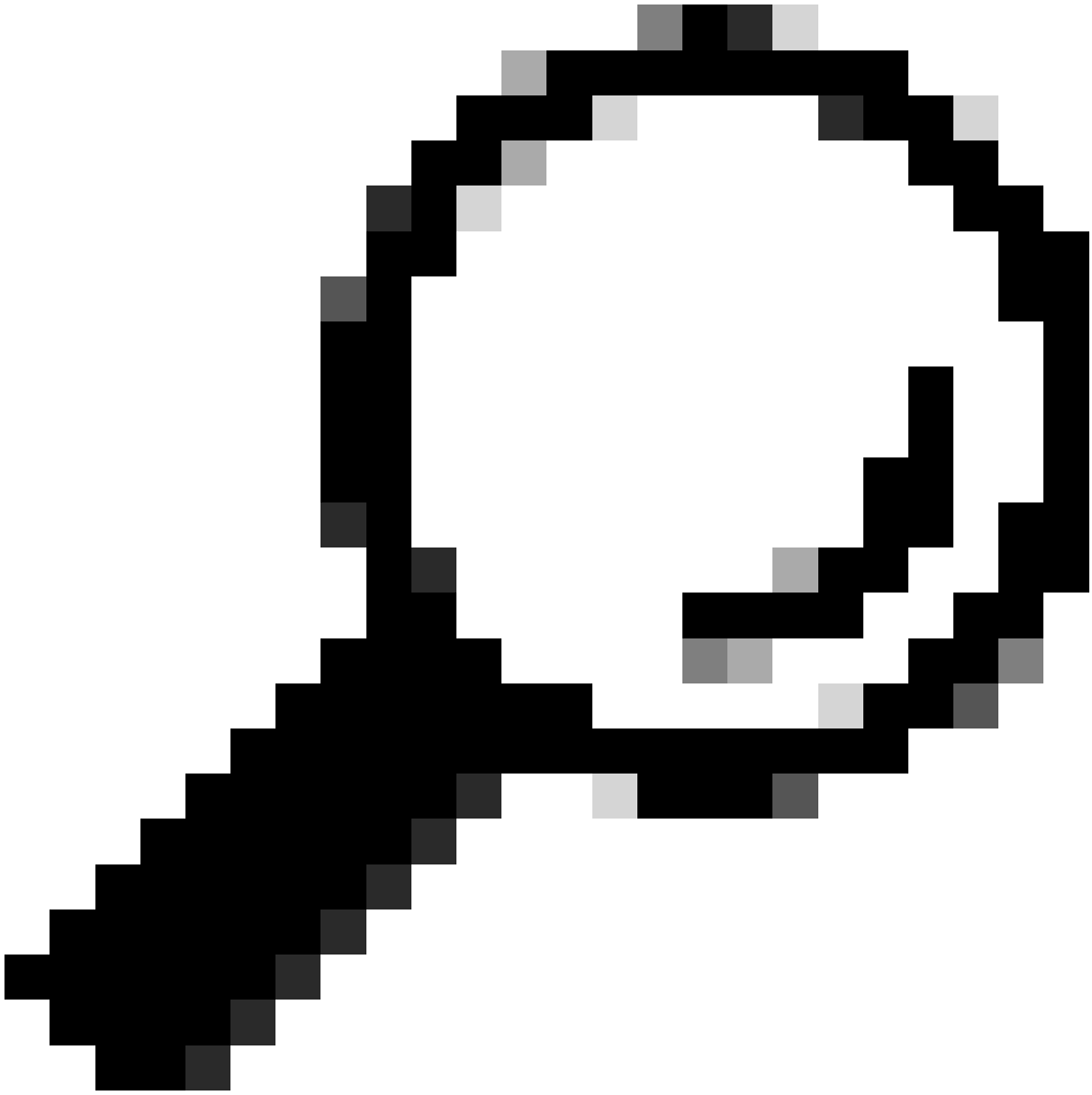
Journaux WMI

1. Ouvrez l'Observateur d'événements Windows (eventvwr.msc).
2. Dans le menu Affichage, cliquez sur Afficher les journaux d'analyse et de débogage.
3. Accédez à Applications and Service Logs > Microsoft > Windows > WMI Activity.
4. Trois fichiers journaux sont disponibles : Debug, Operational et Trace. Les problèmes d'autorisations sont généralement consignés dans le journal des opérations.
5. Un problème d'autorisations WMI pour OpenDNS_Connector est enregistré ici.

Journaux de suivi WMI

La journalisation de trace n'est pas activée par défaut, mais elle peut fournir des informations détaillées sur les requêtes WMI, y compris les tentatives réussies et les tentatives infructueuses.

1. Ouvrez l'Observateur d'événements Windows (eventvwr.msc).
2. Dans le menu Affichage, sélectionnez Afficher les journaux analytiques et de débogage.
3. Accédez à Applications and Service Logs > Microsoft > Windows > WMI Activity.
4. Cliquez avec le bouton droit sur le journal Trace et sélectionnez Propriétés.
5. Sélectionnez Enable Logging et cliquez sur OK. Une fois activé, les événements d'information sont consignés pour chaque requête WMI reçue.
6. Redémarrez le OpenDNS_Connectorservice pour générer de nouveaux événements, ce qui confirme si les requêtes sont en cours de traitement.



Conseil : Pour tester les autorisations en conjonction avec cette journalisation, utilisez l'outil WBEMtest.

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.