Utiliser wevtutil pour vérifier les autorisations du journal des événements

Table des matières

Introduction

Ce document décrit l'utilisation de wevtutil pour vérifier les autorisations d'événement de connexion du connecteur.

Vous pouvez tester si le connecteur peut lire les événements de connexion à partir d'un DC en utilisant wbemtest.

Si wbemtest ne parvient pas réellement à se connecter, cela est généralement dû à une erreur d'autorisation WMI/DCOM. Demandez de l'aide ailleurs.

Cependant, dans certaines circonstances, wbemtest se connecte mais n'affiche aucun événement.

Il y a deux raisons à cela :

- La stratégie d'audit est incorrecte. Par conséquent, les événements de connexion ne sont pas suivis sur le contrôleur de domaine. Demandez de l'aide sur la stratégie d'audit.
- Des événements sont en cours de journalisation sur le contrôleur de domaine, mais OpenDNS_Connector n'est pas autorisé à lire le journal des événements de sécurité. Continuer sur...

Notions de base - Lecteurs de journaux des événements

Dans la plupart des cas, il suffit d'ajouter l'utilisateur OpenDNS_Connector au groupe Lecteurs du journal des événements. Cela lui donne les autorisations nécessaires pour lire le journal des événements.

wevtutil - Vérifier les autorisations

Dans de rares cas, le groupe Lecteurs du journal des événements ne dispose pas des

autorisations par défaut. Nous pouvons utiliser wevtutil pour vérifier facilement les autorisations accordées au journal des événements de sécurité.

Exécutez simplement :

```
wevtutil gl security
```

1. Le résultat montre les autorisations à l'aide de la syntaxe SDDL comme suit :

   ```
   channelAccess: O:BAG:SYD:(A;;0x3;;;S-1-5-3)(A;;0x3;;;S-1-5-33)(A;;0x1;;;S-1-5-573)
   ```

2. Le SID des lecteurs de journaux des événements est S-1-5-32-573 ou peut être abrégé en ER.
3. La valeur hexadécimale correspond aux autorisations, telles que :
   - 0x1 = Lecture
   - 0x2 = écriture
   - 0x3 = Lecture/Écriture\

Correction 1 - Rétablir les paramètres par défaut

Les autorisations peuvent être réinitialisées par défaut en supprimant une valeur de Registre qui contient la chaîne SDDL personnalisée. Il s'agit d'une solution rapide, mais elle peut affecter d'autres logiciels qui lisent le journal des événements (le cas échéant).

Supprimez la valeur 'CustomSD' de HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Security

Correction 2 - Mettre à jour SDDL en utilisant wevtutil

Dans de rares cas, nous pouvons attribuer directement les autorisations à l'aide de wevtutil.

1. Obtenez les autorisations actuelles comme décrit précédemment, à l'aide de cette commande :

   ```
   wevtutil gl security
   ```

2. Notez la chaîne d'accès au canal. Par exemple :

   ```
   /ca:O:BAG:SYD:(A;;0x3;;;S-1-5-3)(A;;0x3;;;S-1-5-33)
   ```

3. Déterminez le SID de l'utilisateur OpenDNS_Connector :

```
wmic useraccount where name='OpenDNS_Connector' get sid
```

4. Vous pouvez donner un accès en lecture à OpenDNS_Connector en l'ajoutant à la chaîne d'accès au canal existante comme suit. Remplacez <SID> par le SID OpenDNS_Connector.

```
wevtutil sl security /ca:O:BAG:SYD:(A;;0x3;;;S-1-5-3)(A;;0x3;;;S-1-5-33)(A;;0x1;;;<SID>)
```

Pour référence, voici le SID du groupe Lecteurs du journal des événements.

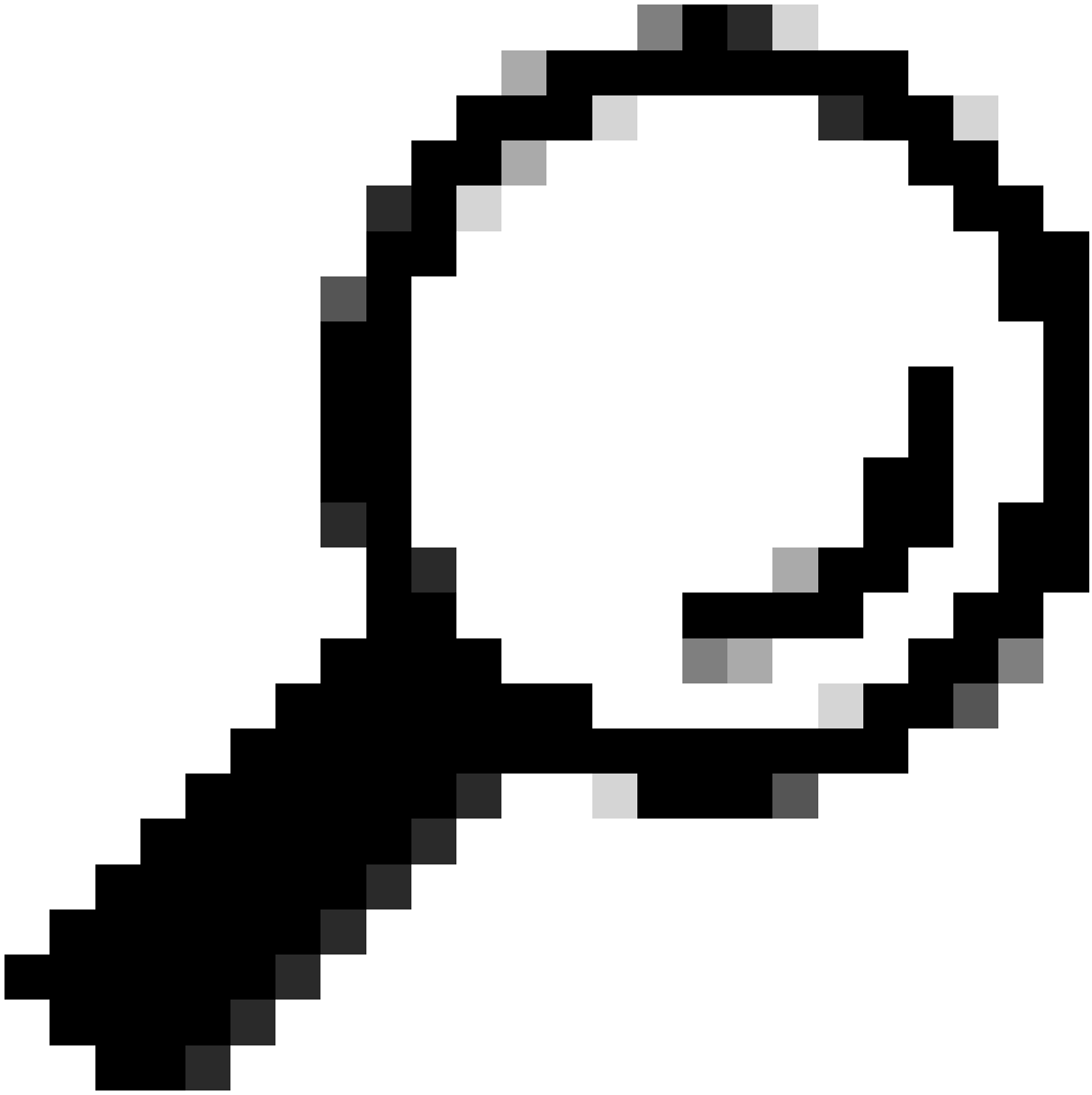
SID : S-1-5-32-573
Name : BUILTIN\Lecteurs du journal des événements
Description: Un groupe local intégré. Les membres de ce groupe peuvent lire les journaux des événements à partir de l'ordinateur local.

Correctif 3 - GPO

Ce paramètre de stratégie de groupe permet d'autoriser le compte Connecteur OpenDNS à lire (et à écrire !) dans le journal des événements de sécurité. Techniquement, ce paramètre donne plus d'autorisations que nécessaire, mais il s'agit d'un moyen facile d'effectuer la modification.

Configuration ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité\Stratégies locales\Attribution des droits utilisateur\Gérer l'audit et le journal de sécurité

Après avoir effectué la modification, veuillez exécuter « gpupdate /force » sur le ou les contrôleurs de domaine.



Remarque : Au niveau fonctionnel Windows 2003 / 2003, le groupe Lecteurs de journaux d'événements peut ne pas exister. Par conséquent, cet objet de stratégie de groupe est la méthode principale permettant au connecteur OpenDNS d'accéder à ces plates-formes.

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.