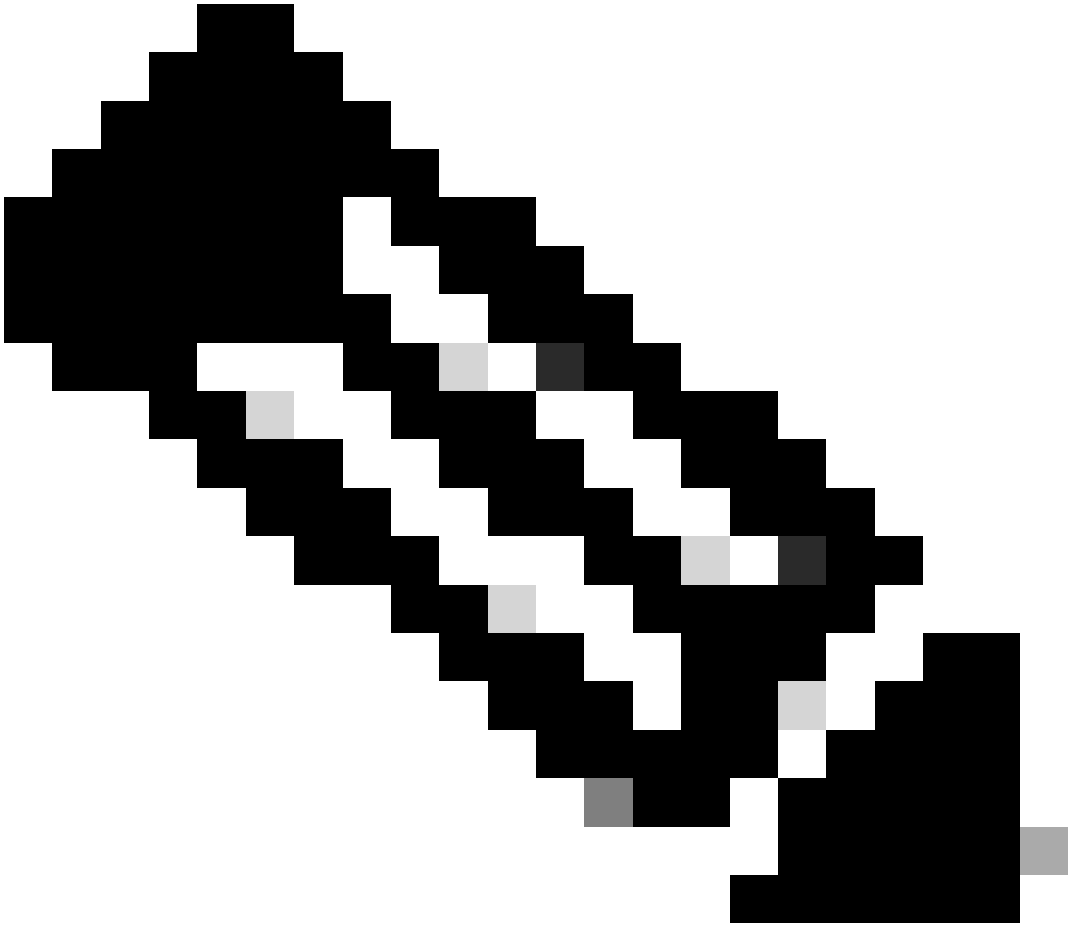
Comprendre les autorisations requises pour l'utilisateur OpenDNS_Connector

Table des matières

Introduction

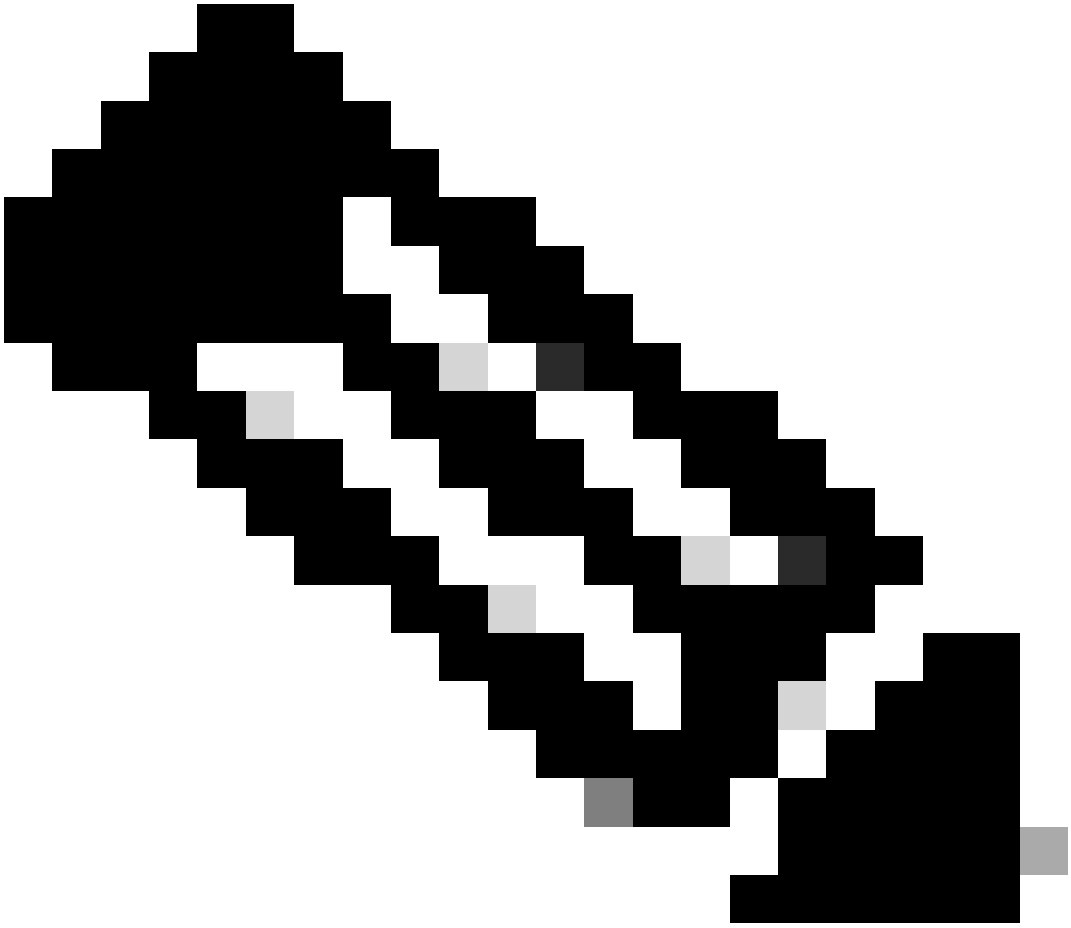
Ce document décrit les autorisations requises pour les utilisateurs d'OpenDNS_Connector.



Remarque : Dans le cadre des efforts de rebranding, le nom d'utilisateur Active Directory « OpenDNS_Connector » a récemment été mis à jour pour devenir « Cisco_Connector ».

Aperçu

Le script Connecteur Windows définit normalement les autorisations requises pour l'utilisateur Cisco_Connector. Cependant, dans les environnements Active Directory stricts, certains administrateurs peuvent ne pas être autorisés à exécuter des scripts VB sur leurs contrôleurs de domaine et doivent donc répliquer manuellement les actions du script de configuration Windows. Cet article détaille les autorisations requises pour être définies sur le contrôleur de domaine.



Remarque : Aux fins de cet article, Cisco_Connector est supposé être le sAMAccountName de votre compte Connector dans Active Directory. Si vous utilisez plutôt un nom personnalisé, suivez les mêmes instructions que le sAMAccountName de votre compte de connecteur au lieu de Cisco_Connector.

Si l'utilisateur Cisco_Connector n'a pas les autorisations suffisantes pour fonctionner, un connecteur AD affiche un état d'alerte ou d'erreur dans le tableau de bord, et le message répertorié lorsque vous passez le curseur sur l'alerte est Accès refusé à l'un des contrôleurs de domaine inscrits.

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

- Contrôleurs de domaine d'entreprise en lecture seule
- Lecteurs de journaux d'événements (uniquement si le déploiement inclut des appareils virtuels)

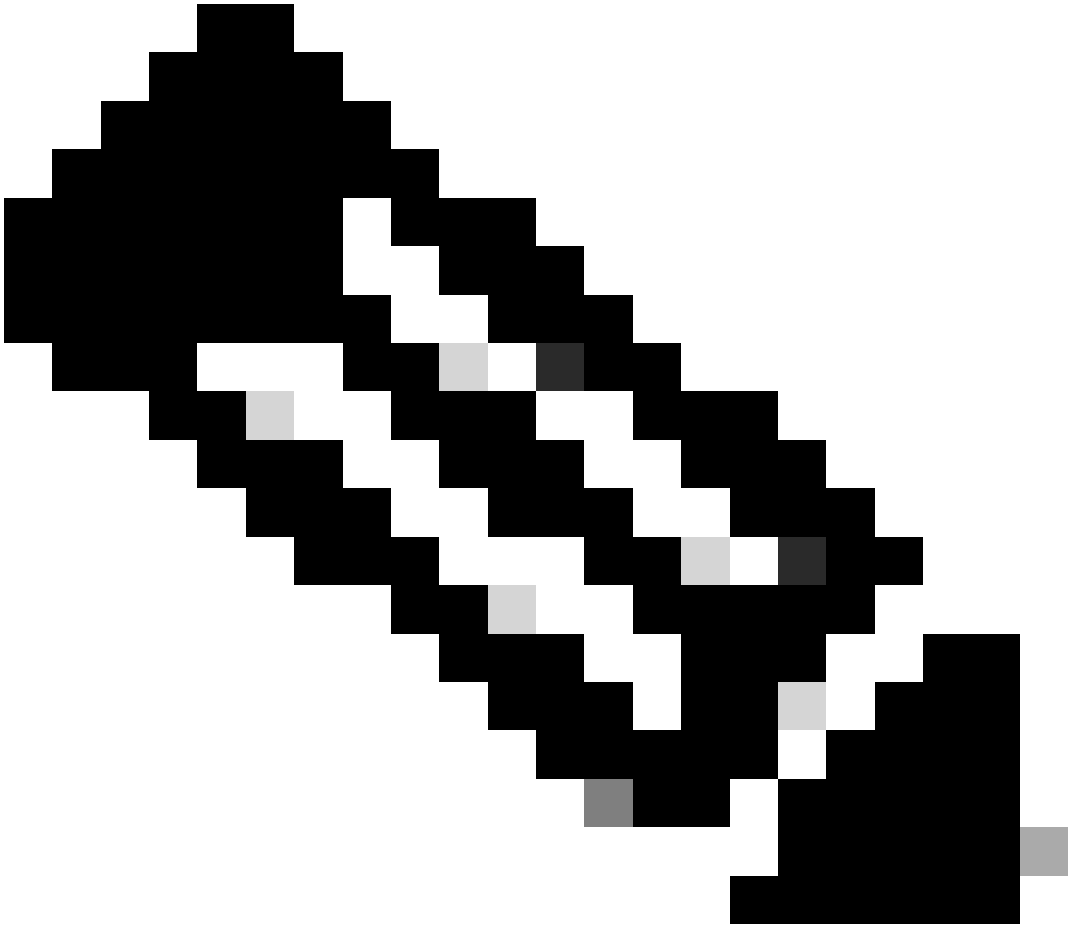
En outre, l'utilisateur Cisco_Connector doit appartenir aux groupes « Utilisateurs du domaine » et

« Utilisateurs ». Vous pouvez vérifier l'appartenance au groupe de l'utilisateur Cisco_Connector à l'aide de la commande :

dsquery user -samid Cisco_Connector | dsget user -memberof -expand

Le connecteur AD Umbrella effectue deux tâches principales pour lesquelles ces autorisations sont nécessaires. Tout d'abord, il extrait les informations LDAP d'Active Directory afin de vous permettre de créer des stratégies basées sur un groupe AD et de pouvoir afficher les noms d'utilisateur et de groupe AD dans le tableau de bord Umbrella. L'autorisation `Répliquer les modifications de répertoire` autorise cela.

Ensuite, il collecte les événements de connexion des contrôleurs de domaine et les transmet aux appliances virtuelles. Cela permet aux appliances virtuelles de créer leurs mappages IP-utilisateur et ainsi d'identifier les utilisateurs. Toutes les autorisations s'appliquent à cette application, à l'exception de l'autorisation `Répliquer les modifications de répertoire`. Ces autorisations sont requises uniquement si le déploiement inclut des appliances virtuelles dans le même site Umbrella que les contrôleurs de domaine.



Remarque : Outre la définition des autorisations requises pour l'utilisateur Cisco_Connector, le script de configuration du contrôleur de domaine enregistre également un contrôleur de domaine en émettant des appels d'API à Umbrella. Si vous modifiez manuellement les autorisations au lieu d'utiliser le script de configuration, cette inscription doit également être effectuée manuellement. Reportez-vous à la documentation Umbrella pour savoir comment ajouter manuellement des contrôleurs de domaine sur le tableau de bord Umbrella.

Autorisations requises

- Répliquer les modifications de répertoire
- Lecteurs de journaux des événements
- Administrateur distant
- Stratégie d'audit

Répliquer les modifications de répertoire

Cette autorisation permet à l'utilisateur Cisco_Connector d'interroger LDAP. Il s'agit de l'autorisation requise généralement accordée au groupe « Contrôleurs de domaine en lecture seule d'entreprise ». Le tableau de bord Umbrella fournit ainsi les informations nécessaires pour afficher les noms des objets AD et déterminer les appartenances aux groupes. Le connecteur demande les attributs suivants :

`cn` : nom commun.

`dn` : nom distinctif.

`dNSHostName` : nom du périphérique tel qu'il est enregistré dans DNS.

`mail` : adresses e-mail associées à l'utilisateur.

`memberOf` : groupes qui incluent l'utilisateur.

`objectGUID` : ID de groupe de l'objet. Cette propriété est envoyée à Secure Access sous forme de hachage.

`primaryGroupId` : ID de groupe principal disponible pour les utilisateurs et les groupes.

`primaryGroupToken` : jeton de groupe principal disponible uniquement pour les groupes. Les mots de passe ou les hachages de mot de passe ne sont pas récupérés. L'accès sécurisé utilise la

`primaryGroupToken` dans la stratégie d'accès, la configuration et les rapports. Ces données sont également requises pour chaque filtrage utilisateur ou par ordinateur.

`sAMAccountName` : nom d'utilisateur que vous utilisez pour vous connecter au connecteur Cisco AD.

`userPrincipalName`

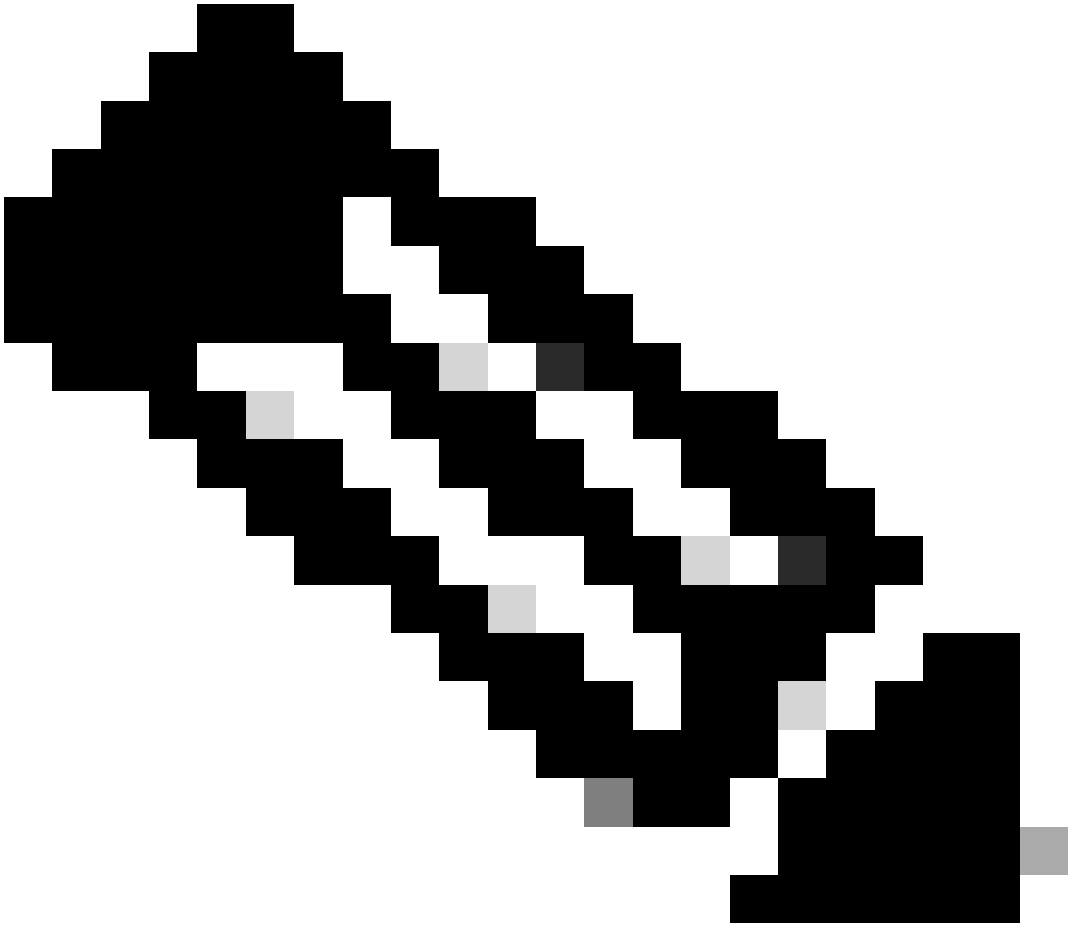
: nom principal de l'utilisateur.

À partir de ces objectClasses :

```
(&(objectCategory=person)(objectClass=user))
(objectClass=organizationalunit)
(objectClass=computer)
(objectClass=group)
```

Le groupe intégré « Contrôleurs de domaine d'entreprise en lecture seule » doit fournir cette autorisation, et par conséquent l'utilisateur Cisco_Connector doit être membre de ce groupe. Vous pouvez vérifier les autorisations du groupe ou spécifier les autorisations spécifiquement pour l'utilisateur Cisco_Connector (si le groupe ne fournit pas ces autorisations) :

- Ouvrez le composant logiciel enfichable Utilisateurs et ordinateurs Active Directory
- Dans le menu Affichage, cliquez sur Fonctionnalités avancées.
- Cliquez avec le bouton droit sur l'objet de domaine, tel que « société.com », puis cliquez sur Propriétés.
- Dans l'onglet Security, sélectionnez l'utilisateur « Enterprise Read-only Domain Controllers » ou « Cisco_Connector ».
    - Si nécessaire, vous pouvez ajouter l'utilisateur « Cisco_Connector » en cliquant sur « Ajouter ».
    - Dans la boîte de dialogue Sélectionner des utilisateurs, des ordinateurs ou des groupes, sélectionnez le compte d'utilisateur souhaité, puis cliquez sur Ajouter.
    - Cliquez sur OK pour revenir à la boîte de dialogue Propriétés.
- Cochez les cases Réplication des modifications de répertoire et Lecture dans la liste.
- Cliquez sur Appliquer, puis sur OK.
- Fermez le composant logiciel enfichable.

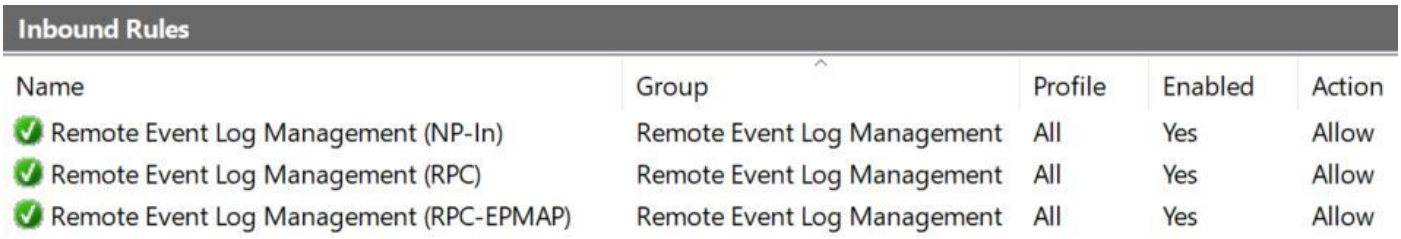


Remarque : Dans un scénario de domaine parent/enfant, le « contrôleur de domaine en lecture seule d'entreprise » n'existe que dans le domaine parent. Dans ce cas, les autorisations doivent être ajoutées manuellement pour Cisco_Connector, comme indiqué.

Lecteurs de journaux des événements

Cette modification n'est nécessaire que si le déploiement inclut des appliances virtuelles dans le même site Umbrella que le contrôleur de domaine. L'appartenance à ce groupe permet à l'utilisateur Cisco_Connector de lire les événements de connexion à partir des journaux des événements.

Sur l'ordinateur contrôleur de domaine, dans les paramètres avancés du pare-feu Windows, assurez-vous que les règles entrantes pour la gestion à distance du journal des événements (NP-In, RPC et RPC-EPMAP) sont autorisées. Le connecteur AD Umbrella peut consigner une erreur indiquant « Le serveur RPC n'est pas disponible » et peut ne pas être en mesure de lire les événements de connexion si ces règles ne sont pas autorisées.



360090909832

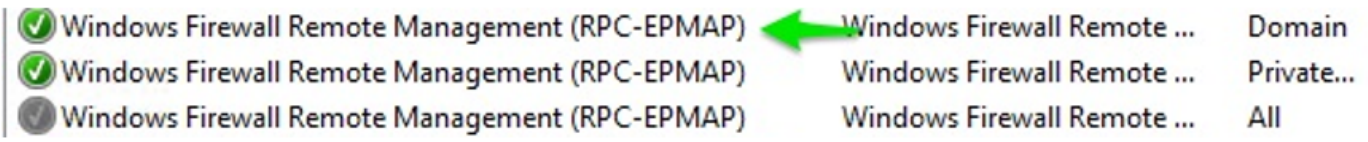
Vous pouvez également activer ces règles via cette commande : netsh advfirewall firewall set rule group="Gestion du journal des événements à distance" new enable=yes

Administrateur distant

L'administration à distance est nécessaire pour permettre au connecteur de lire les événements de connexion sur le contrôleur de domaine. Cette autorisation n'est requise que si le déploiement inclut des appliances virtuelles dans le même site Umbrella que le contrôleur de domaine.

À partir d'une invite de commandes, exécutez les commandes suivantes :

```
netsh advfirewall firewall set rule group="remote administration" new enable=yes
netsh advfirewall set currentprofile settings remotemanagement enable
```



4413613529492

Stratégie d'audit

Cette modification n'est nécessaire que si le déploiement inclut des appliances virtuelles dans le même site Umbrella que le contrôleur de domaine. La stratégie d'audit définit les événements qui sont consignés dans le journal des événements du contrôleur de domaine. Le connecteur exige que les événements de connexion réussis soient enregistrés afin que les utilisateurs puissent être mappés à leurs adresses IP.

Dans les environnements Windows Server 2008+ normaux, le paramètre hérité « Auditer les événements de connexion » doit être configuré. Plus précisément, la stratégie « Auditer les événements de connexion » doit être définie sur « Réussite ». Vous pouvez vérifier cela en exécutant cette commande à partir d'une invite de commandes :

```
GPRESULT /z
```

Cette stratégie est définie comme un objet de stratégie de groupe. Pour le modifier, modifiez la stratégie de groupe appropriée pour votre contrôleur de domaine (généralement la « stratégie de contrôleur de domaine par défaut ») et définissez cette stratégie pour inclure les événements « Success » :

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit Policy\Audit lo
```

Assurez-vous de mettre à jour la stratégie de groupe sur le contrôleur de domaine après avoir effectué cette modification.

Cependant, Windows Server 2008 a également introduit la configuration avancée de la stratégie d'audit. Bien que les stratégies d'audit Windows héritées puissent toujours être utilisées, elles sont ignorées si l'une des stratégies d'audit avancées est définie. Reportez-vous à la documentation Microsoft pour comprendre comment les deux stratégies d'audit interagissent.

Pour les besoins du connecteur, si des stratégies d'audit avancées sont définies (y compris celles qui ne sont pas spécifiquement liées à l'ouverture de session), alors les stratégies d'audit avancées DOIVENT être utilisées.

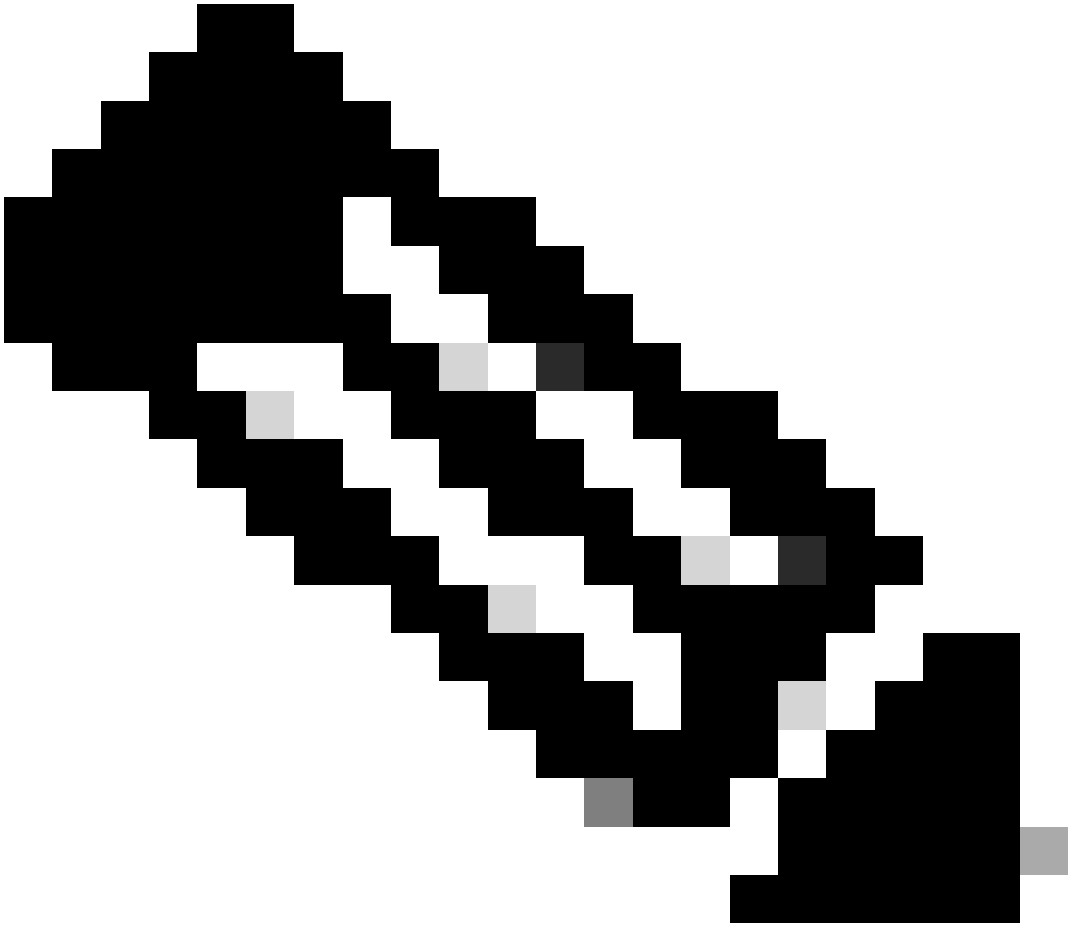
La stratégie d'audit avancée doit être définie pour tous les contrôleurs de domaine utilisant la stratégie de groupe. Modifiez la stratégie de groupe appropriée pour votre contrôleur de domaine (généralement la « stratégie de contrôleur de domaine par défaut ») et passez à cette section :

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\
```

Dans cette section, définissez ces stratégies pour inclure les événements « Success » et « Failure » :

```
Audit Logon
Audit Logoff
Audit Other Logon/Logoff Events
```

Veillez à mettre à jour la stratégie de groupe sur le contrôleur de domaine après avoir effectué cette modification.



Remarque : Si vous déployez le connecteur AD avec des appareils virtuels, les modifications de la règle de pare-feu et les paramètres de stratégie d'audit doivent être effectués sur tous les contrôleurs de domaine du domaine avec lequel le connecteur communique.

Si après avoir confirmé/modifié les paramètres susmentionnés, vous voyez toujours des messages « Accès refusé » dans le tableau de bord, veuillez envoyer les journaux de prise en charge du connecteur Umbrella, comme indiqué dans cet article : Fournir une assistance avec les journaux des connecteurs AD

Lorsque vous fournissez ces informations au support, incluez le résultat de ces deux commandes :

```
auditpol.exe /get /category:* > DCNAME_auditpol.txt
GPRESULT /H DC_NAME.htm
```

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.