Comprendre le script de configuration de Windows DC

Table des matières

Introduction

Présentation du script de configuration DC

Étape 1 - Tests

Étape 1b - Résultats des tests

Étape 2 - Modifications de la configuration automatique

Étape 2b - Avertissements de configuration automatique

Étape 3 - Inscription

Introduction

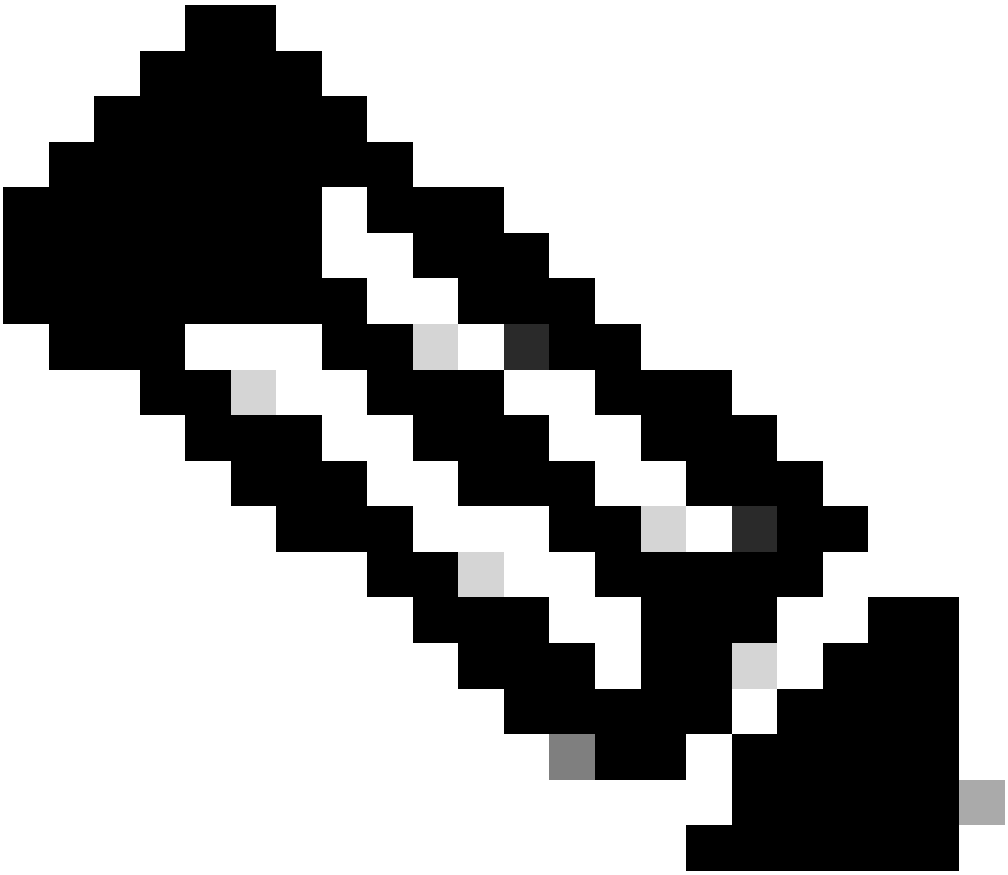
Ce document décrit les modifications apportées à votre environnement Windows par notre script de configuration du contrôleur de domaine.

- Pour les prérequis de base, consultez la documentation Insights : https://docs.umbrella.com/deployment-umbrella/docs/2-prerequisites
- Pour obtenir des informations détaillées sur la définition manuelle de ces autorisations, consultez cet article : Autorisations requises pour l'utilisateur OpenDNS_Connector.

Présentation du script de configuration DC

Chaque contrôleur de domaine nécessite un enregistrement unique avec l'API/le tableau de bord Umbrella. Notre script de configuration du contrôleur de domaine lance ceci avec les fonctions suivantes :

1. Vérifier que les autorisations nécessaires et les règles de pare-feu sont configurées
2. (Facultatif) Configurez automatiquement ces autorisations
3. (Facultatif) Enregistrez le contrôleur de domaine avec l'API/le tableau de bord Umbrella, uniquement si ces vérifications ont réussi.



Remarque : Une liste de contrôleurs de domaine peut également être enregistrée manuellement par le support Umbrella. Ceci est généralement utile dans les scénarios où l'accès à l'API / Internet n'est pas possible pour le contrôleur de domaine. Cependant, les modifications d'autorisation décrites DOIVENT toujours être configurées, nous vous recommandons donc fortement d'exécuter le script de configuration.

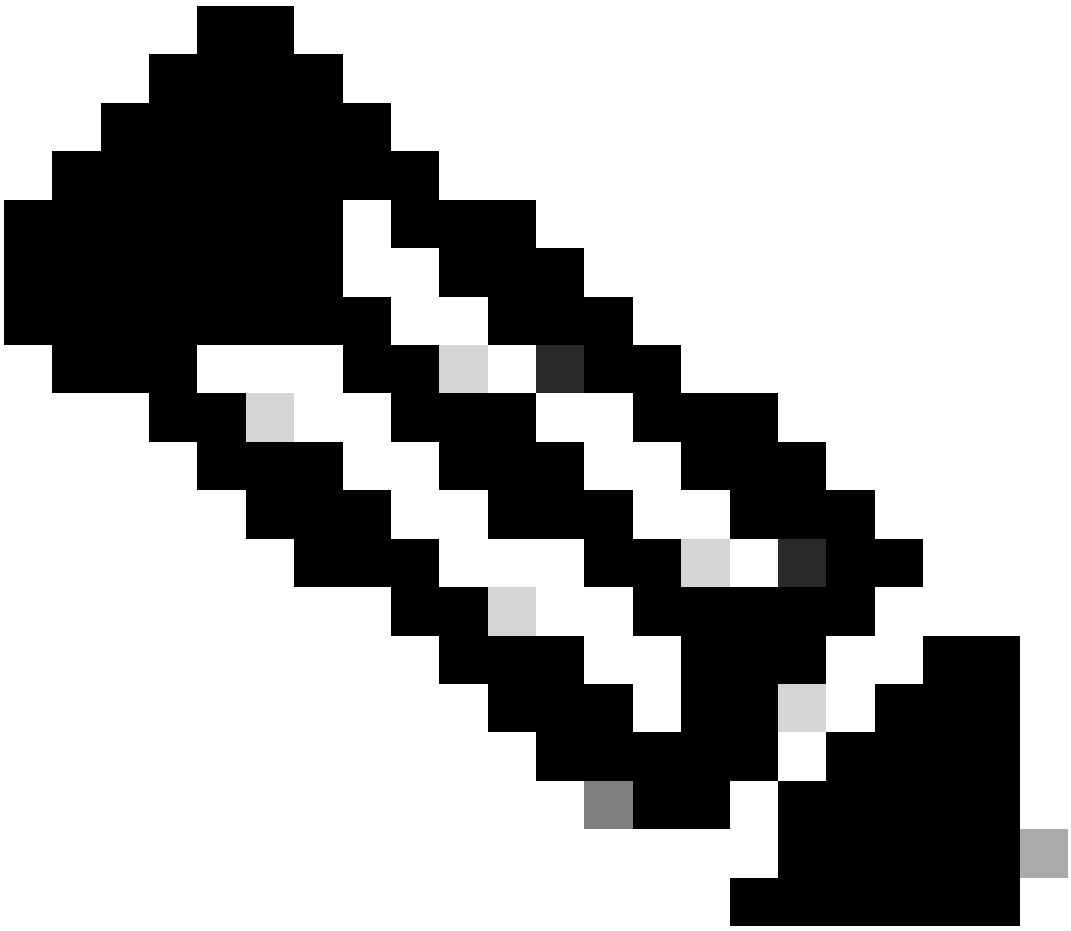
Lors de l'exécution initiale du script, aucune modification n'est apportée à l'environnement. Le script vérifie si toutes les autorisations nécessaires sont en place. En cas de problème, vous êtes invité `(O/N)` mais vous devez apporter des modifications.

Une fois le script d'enregistrement terminé, aucun logiciel n'est nécessaire pour s'exécuter sur le contrôleur de domaine lui-même. Cependant, le service Connecteur OpenDNS doit être installé sur au moins un ordinateur (par ex. Contrôleur de domaine ou serveur membre).

Étape 1 - Tests

Le script collecte initialement ces informations :

- Vérifie la version du système d'exploitation et le niveau fonctionnel de forêt
- Vérifie si le script est exécuté en tant qu'administrateur.
- Obtient les informations d'adresse IP, de nom d'hôte et de nom de domaine des serveurs
- Vérifiez si le Pare-feu Windows est activé et si la règle intégrée 'Administration à distance' est autorisée
- Recherche le compte d'utilisateur de domaine requis 'OpenDNS_Connector'



Remarque : Si l'utilisateur OpenDNS_Connector n'existe pas, le script imprime les résultats et abandonne. Cet utilisateur de domaine doit être créé manuellement avant d'exécuter le script. Si le compte OpenDNS_Connector existe, le script procède à ces vérifications.

- Vérifie si l'utilisateur OpenDNS_Connector dispose d'autorisations pour « Remote Enable » et « Read Security » dans l'espace de noms WMI root\cimv2.
- Vérifie si le compte OpenDNS_Connector dispose de l'autorisation 'Réplication des

modifications d'annuaire' Active Directory, qui est normalement accordée par l'appartenance au groupe Contrôleurs de domaine en lecture seule d'entreprise.
- Vérifie si le compte OpenDNS_Connector est membre du groupe 'Lecteurs du journal des événements'
- Vérifie si le compte OpenDNS_Connector est membre du groupe 'Utilisateurs COM distribués'
- Vérifie le jeu de stratégies résultant (RSOP) pour voir si l'option Auditer les événements de connexion est activée via la stratégie de groupe
- Vérifie le jeu de stratégie résultant (RSOP) pour voir si le compte OpenDNS_Connector a le droit 'Gérer le journal d'audit et de sécurité' attribué

Étape 1b - Résultats des tests

Les résultats imprimés par le script de configuration varient en fonction de la version du système d'exploitation.

Sur le serveur 2003 et les versions ultérieures, les résultats suivants s'affichent :

```
AD User Exists:                true/false
WMI Permissions Set:           true/false
DCOM Permissions Set:          true/false
RDC Permissions Set:           true/false
Audit Policy Set:              true/false
Manage Event Log Policy Set:   true/false
Distributed COM MemberOf:      true/false
```

Sur Server 2008 et les versions ultérieures (uniquement lorsque le niveau fonctionnel de la forêt est 2008+), ces informations sont également affichées. (Ce groupe n'existe pas dans les versions antérieures) :

```
Event Log Readers MemberOf:     true/false
```

Étape 2 - Modifications de la configuration automatique

Si ces vérifications échouent, vous êtes invité `"Voulez-vous que nous configurions automatiquement ce contrôleur de domaine (y ou n) ?"` avant d'apporter des modifications.

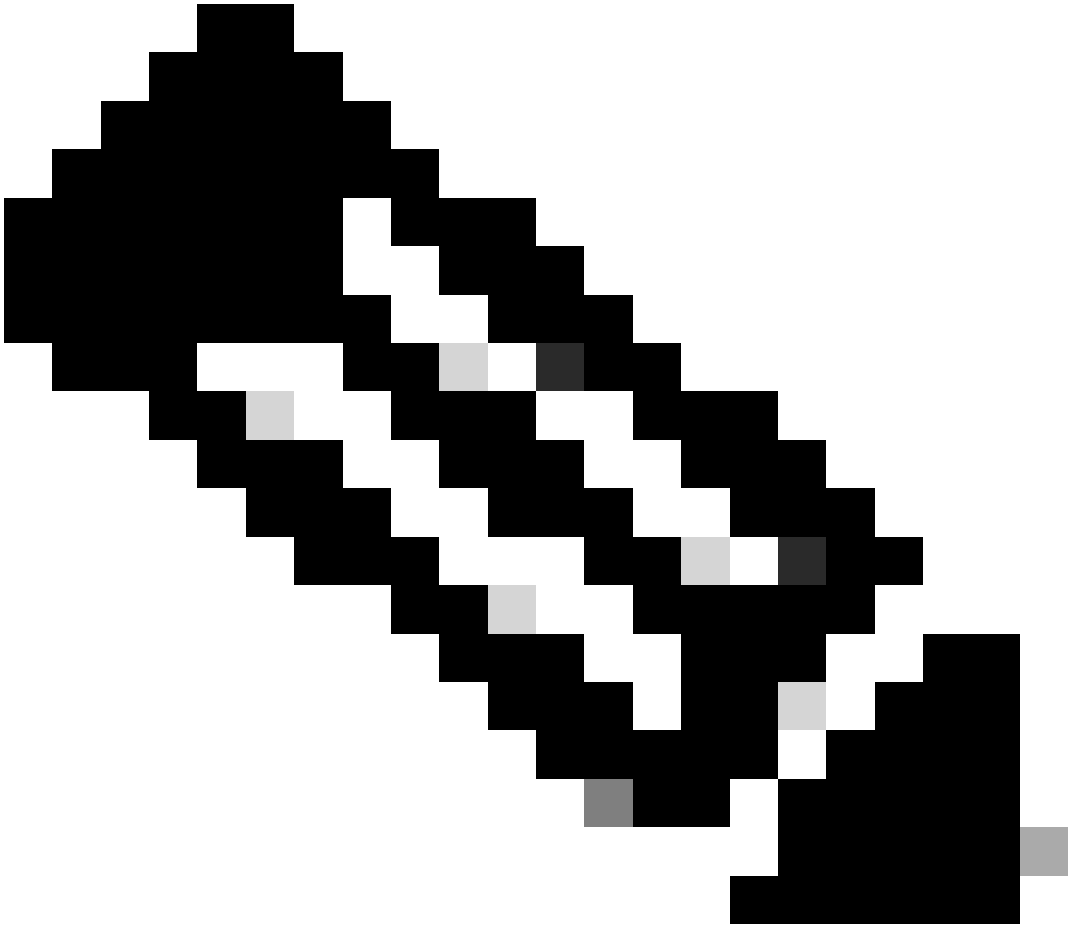
Ces modifications sont effectuées :

- Active la règle intégrée 'Administration à distance' du Pare-feu Windows, si nécessaire
- Accorde explicitement les autorisations « Remote Enable » et « Read Security » du compte « OpenDNS_Connector » dans l'espace de noms WMI root\cimv2.
- Accorde explicitement les autorisations du compte 'OpenDNS_Connector' 'Replicating

Directory Changes'
- Ajoute le compte « OpenDNS_Connector » au groupe « Utilisateurs COM distribués »

Sur 2008+ ce changement est également effectué :

- Ajoute le compte 'OpenDNS_Connector' au groupe 'Event Log Readers'



Remarque : Si la configuration automatique est refusée ou si ces modifications échouent, le script ne procède pas à l'enregistrement.

Étape 2b - Avertissements de configuration automatique

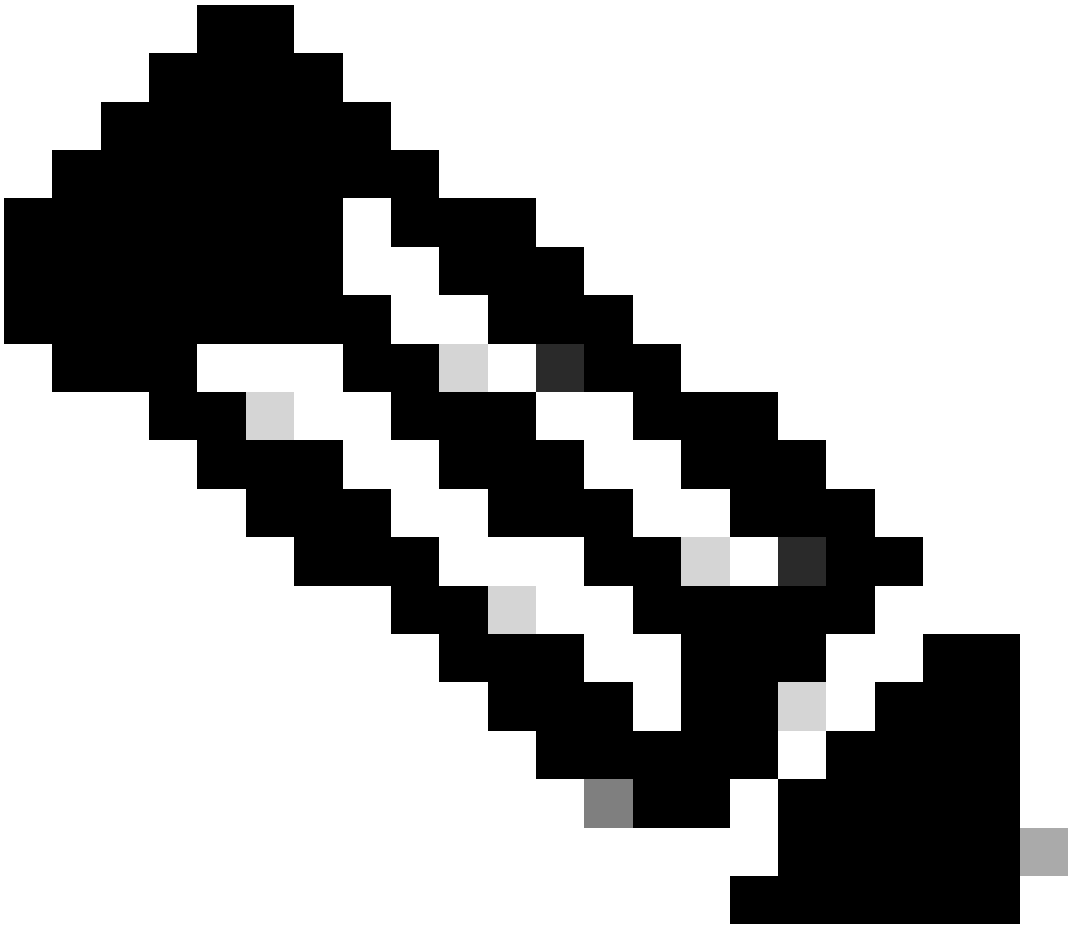
Le script génère des avertissements si les paramètres de stratégie de groupe ne sont pas correctement configurés. Le script ne parvient pas à corriger ces problèmes.

Tous les systèmes opérationnels :

- Le script AVERTIT si le paramètre 'Auditer les événements de connexion' n'est pas correctement configuré dans la stratégie de groupe, mais ne modifie pas la stratégie de groupe.

En 2003 (Et 2003 Au Niveau Fonctionnel) :

- Le script AVERTIT si le droit 'Gérer le journal d'audit et de sécurité' n'est pas correctement configuré dans la stratégie de groupe, mais ne modifie pas la stratégie de groupe.



> Remarque : Corrigez manuellement ces problèmes et réexécutez le script de configuration. Le script ne poursuit pas l'enregistrement tant que ces erreurs n'ont pas été corrigées.

Étape 3 - Inscription

Le script vous invite avant d'enregistrer le contrôleur de domaine avec Umbrella "`Voulez-vous enregistrer ce contrôleur de domaine (y ou n) ?"`.Ces informations sont envoyées à Umbrella :

- Nom d'hôte/étiquette du contrôleur de domaine
- le nom de domaine
- Adresse IP
- Votre ID et votre jeton d'organisation uniques (contenus dans votre script) pour identifier de manière unique le contrôleur de domaine auprès de votre organisation-cadre.

L'enregistrement s'effectue en toute sécurité via https://api.opendns.com

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.