Configurez WMI sur le contrôleur de domaine windows pour le CEM

Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Composants utilisés](#)
[Configurez](#)
[Créez un nouvel objet de stratégie de groupe](#)
[WMI : Configurez la Sécurité COM](#)
[Affectation de droits des utilisateurs](#)
[Configuration de Pare-feu](#)
[Sécurité de l'espace de noms WMI](#)
[Vérifiez](#)
[Dépannez](#)

Introduction

Ce document décrit les étapes pour configurer les Windows Management Instrumentation (WMI) sur le contrôleur de domaine windows pour la Gestion d'EnergyWise de Cisco (CEM). WMI est utilisé pour accéder à distance des ordinateurs de fenêtres pour recueillir des données et pour exécuter des commandes. Bien que le script soit disponible qu'exécute toutes les étapes nécessaires immédiatement, si le contrôleur de domaine est utilisé pour appliquer des stratégies sur les périphériques de domaine, il est recommandé de changer des configurations dans la stratégie de domaine, car les périphériques ignoreraient les modifications locales. Ce document présente les étapes pour configurer la stratégie de groupe sur le contrôleur de domaine windows pour préparer les périphériques de domaine pour l'interrogation WMI.

> Remarque: Bien que WMI soit disponible dans le Windows 2000 avec le SP2, l'application de CEM ne prend en charge pas le Windows 2000. Pour utiliser WMI, l'application de CEM exige le professionnel SP2 de Microsoft Windows XP ou plus tard.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez accès au contrôleur de domaine windows, à la suite logicielle de gestion d'EnergyWise de Cisco et aux ordinateurs distants (ressources).

Composants utilisés

Les informations dans ce document sont basées sur l'environnement des CEM 5.2 dans lequel le

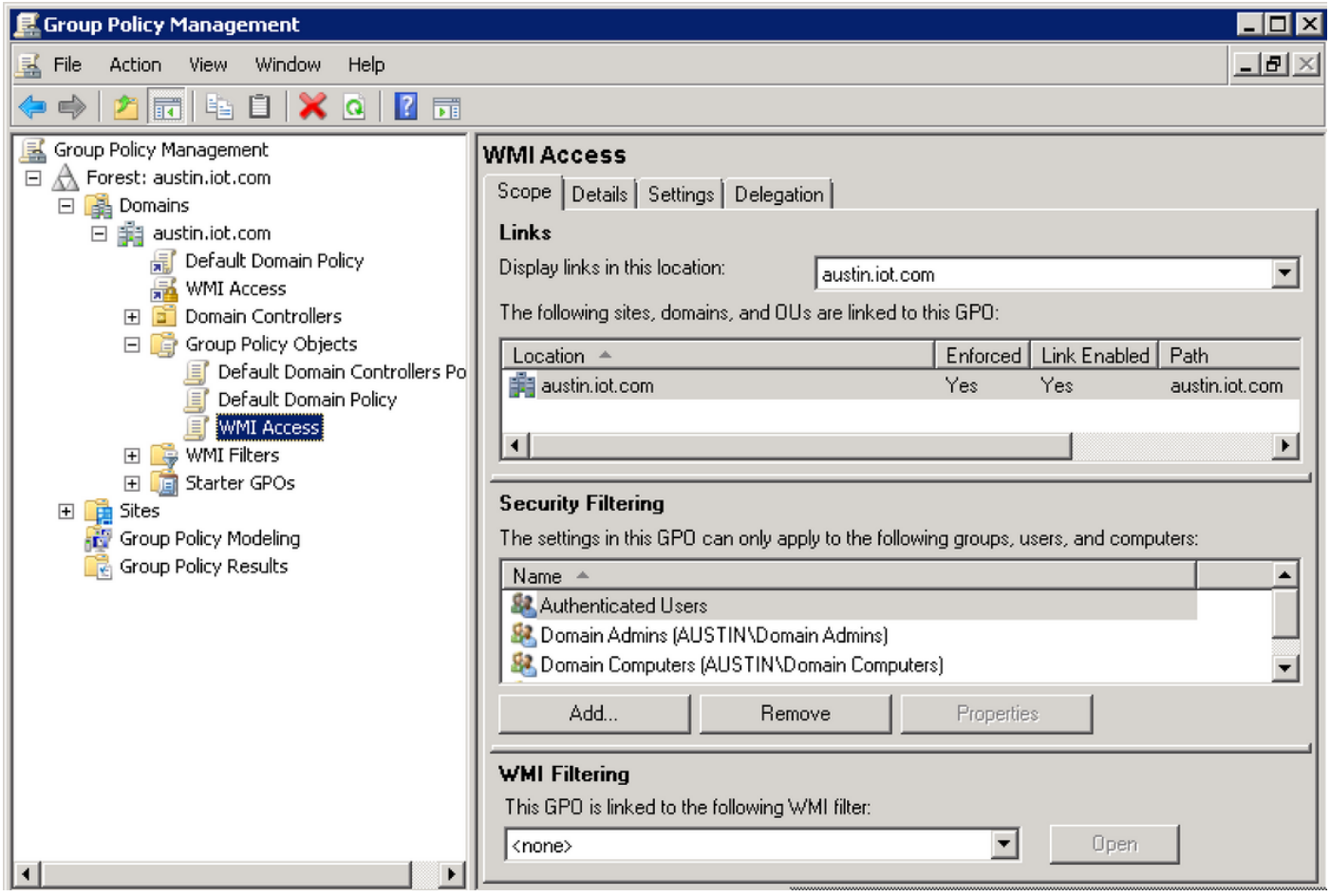
connecteur de ressource en Répertoire actif (AD) est utilisé pour tirer les informations WMI des périphériques distants.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Configurez

Créez un nouvel objet de stratégie de groupe

La première étape est de créer un nouvel objet de stratégie de groupe. L'objet de stratégie de groupe peut être créé sur le contrôleur de domaine sous la Gestion de stratégie de groupe comme affiché :



Objet de stratégie de groupe

WMI : Configurez la Sécurité COM

Pour exécuter des requêtes WMI à distance, des autorisations spécifiques COM sont exigées. Sélectionnez l'objet de stratégie de groupe créé dans l'étape précédente, cliquez avec le bouton droit et choisi **éditez** et puis parcourez à cet emplacement :

Console de gestion de stratégie de groupe (GPMC) > configuration de l'ordinateur \ paramètres de windows \ paramètres de sécurité \ stratégies locales \ options de Sécurité

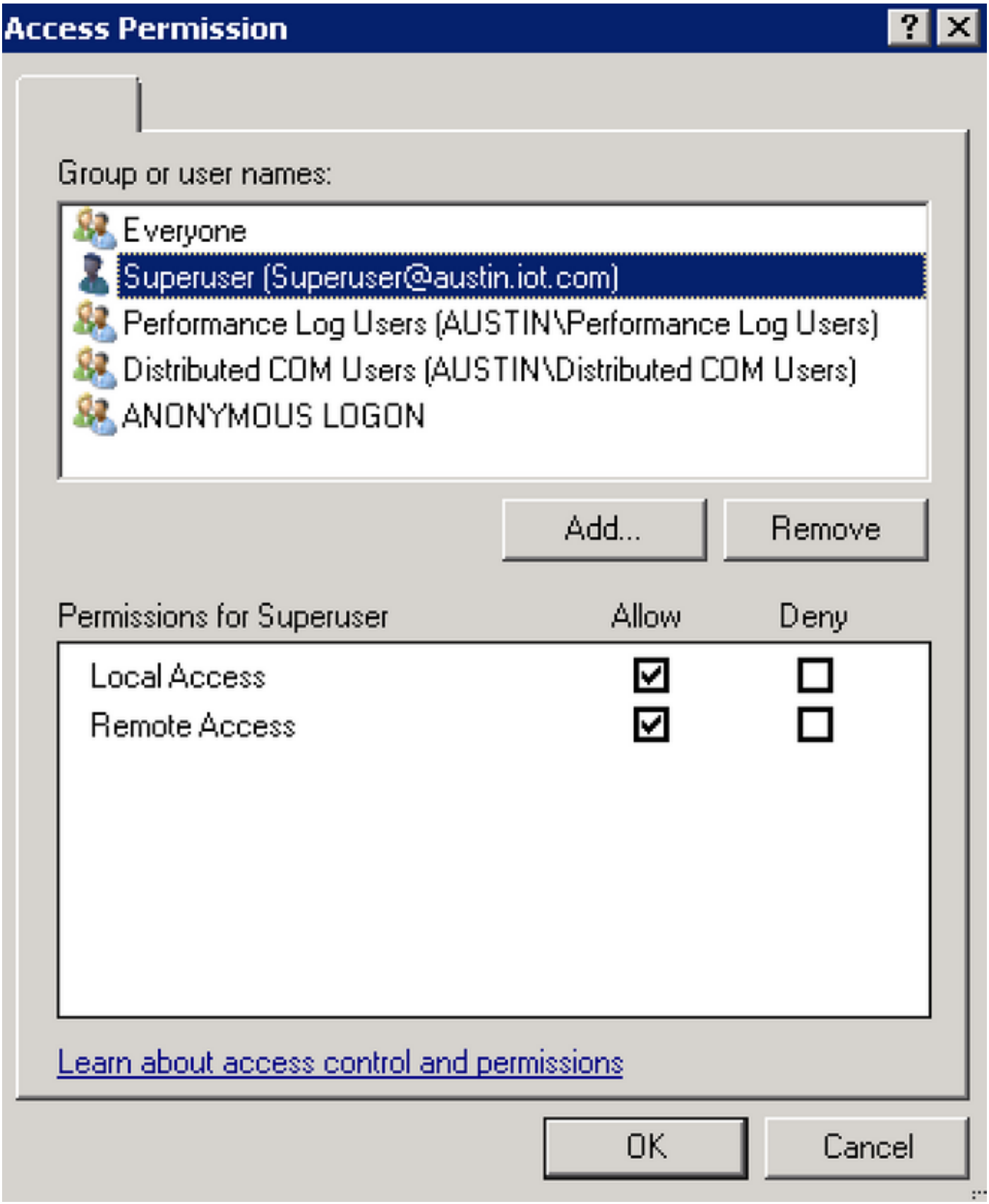
Trouvez les captures d'écran pour configurer des autorisations d'Accès à distance pour l'utilisateur d'administrateurs pour les autorisations COM pour :

DCOM : Usinez les restrictions d'Access en syntaxe du langage de définition de descripteur de Sécurité (SDDL)

DCOM : Restrictions de lancement d'ordinateur en langage de définition de descripteur de Sécurité (SDDL)

Autorisations DCOM

Choisi **définissez ce paramètre de la stratégie** et cliquez sur en fonction la **Sécurité Edit**. Fournissez les gens du pays et les autorisations d'Accès à distance au compte que vous voulez utiliser pour WMI.



Autorisation d'accès DCOM

Affectation de droits des utilisateurs

L'application de CEM exige des fichiers de sauvegarde et des répertoires et des fichiers et des répertoires de restauration de charger le profil utilisateur quand elle essaye d'appeler un processus. Il exige également l'arrêt de force d'un privilège distant d'arrêt de permettre l'action POWER_OFF de fonctionner.

Ces modifications doivent être apportées dans les configurations d'affectation de droits des utilisateurs dans cet objet de stratégie de groupe. Ces droites doivent être données au compte utilisé pour WMI.

SeRemoteShutdownPrivilege - Arrêt de force d'un système distant

SeBackupPrivilege - Sauvegardez les fichiers et les répertoires

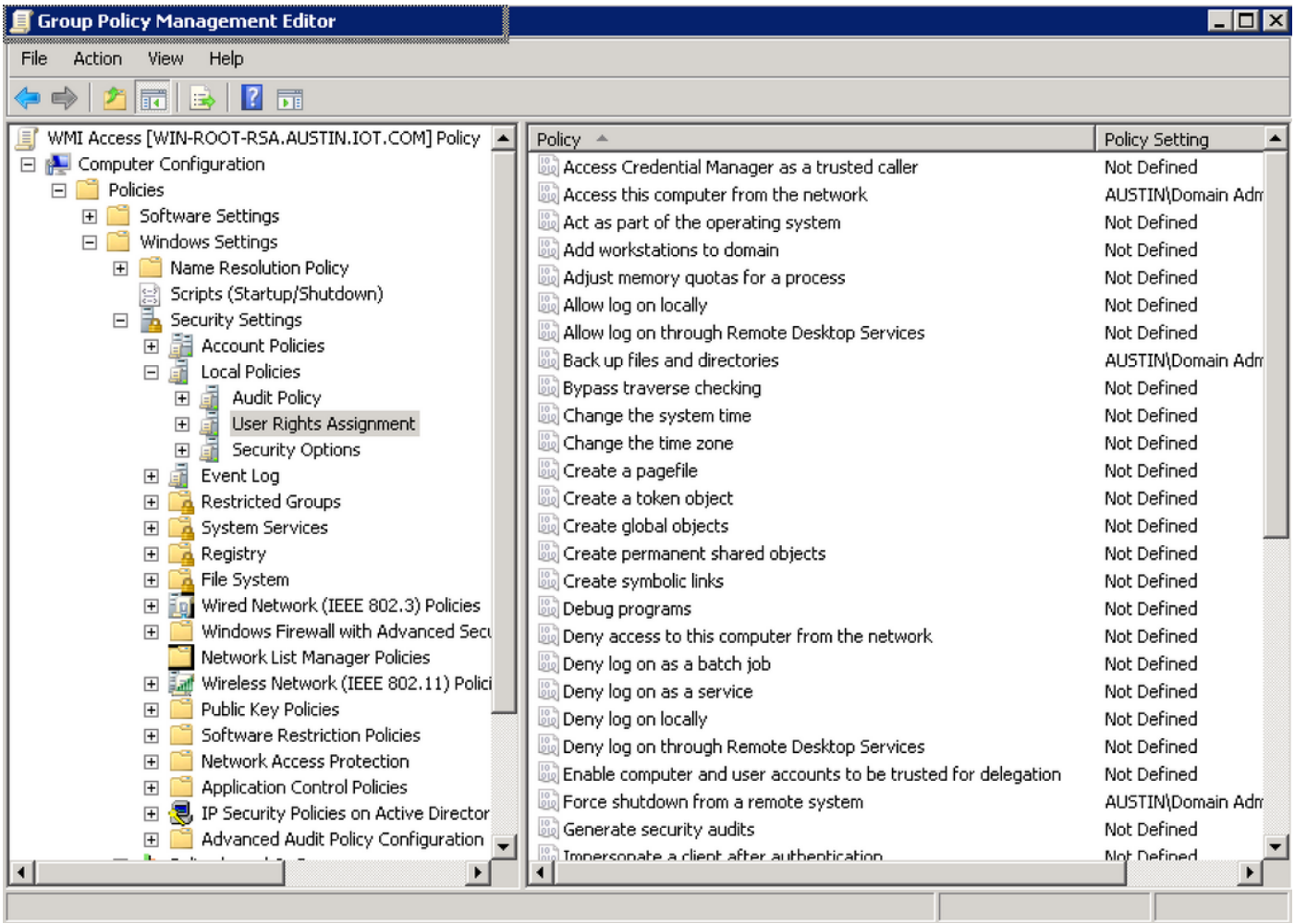
SeRestorePrivilege - Fichiers et répertoires de restauration

SeNetworkLogonRight - Accédez à cet ordinateur du réseau

SeSecurityPrivilege - Choisissez gèrent auditer et log de sécurité

Ces configurations peuvent être configurées sous ce chemin :

Groupez la console de PolicyManagement (GPMC) > configuration de l'ordinateur \ paramètres de windows \ paramètres de sécurité \ affectation locale de stratégies \ droits des utilisateurs



Affectation de droits des utilisateurs

Configuration de Pare-feu

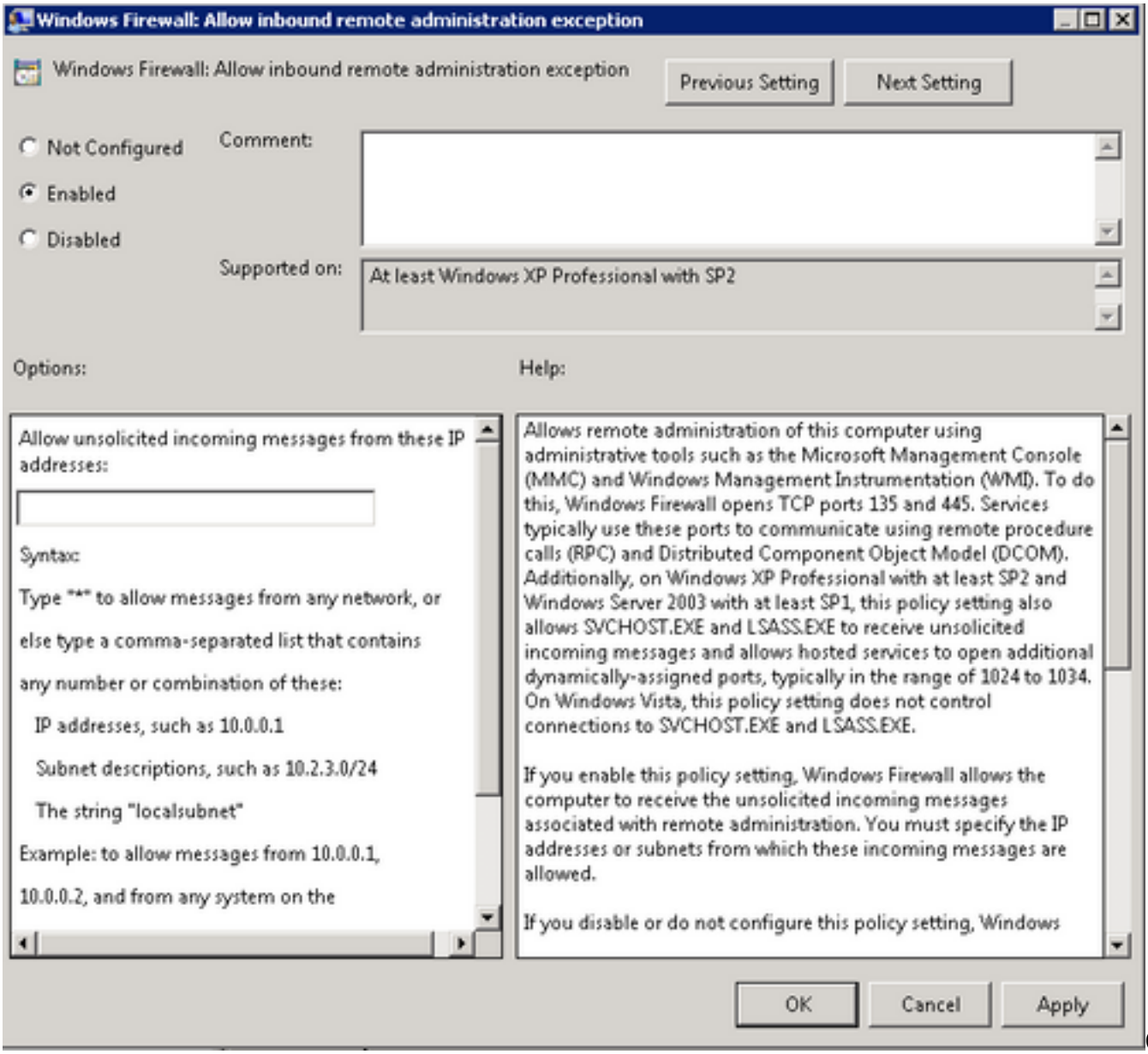
Pour exécuter des appels WMI à un ordinateur, le port RPC (TCP 135) doit être accessible extérieurement. Ceci peut être fait avec l'utilisation de l'éditeur de Gestion de stratégie de groupe, de l'arborescence de menu, naviguent vers la **configuration de l'ordinateur > les stratégies > les modèles administratifs : Définitions des politiques > réseau > connexions réseau > pare-feu Windows**

Profil choisi de **domaine**, et **pare-feu Windows de** double clic **: Permettez l'exception d'arrivée d'administration à distance**. Le pare-feu Windows : Permettez l'administration à distance d'arrivée que la fenêtre d'exception apparaît.

Clic **activé**.

Assurez-vous que vous spécifiez l'adresse IP permettez dedans les messages entrant non sollicités du champ de ces adresses IP.

Vous pouvez entrer * pour permettre des messages de n'importe quel réseau, ou bien tapez une liste virgule-séparée qui contient les adresses IP ou les sous-réseaux spécifiques.



Con
figuration de Pare-feu

Sécurité de l'espace de noms WMI

Pour activer l'accès WMI à un ordinateur, des autorisations spécifiques WMI doivent être activées pour le compte utilisé. Cette configuration ne peut pas être faite par l'intermédiaire de la stratégie de groupe sur le contrôleur de domaine windows, il doit être faite sur les ordinateurs distants avec l'outil de WmiSetNsSecurity.

Placez la Sécurité WMI et exécutez la commande (remplacez %account% par le compte utilisateur que vous voulez placer la Sécurité pour) sur l'outil de ligne de commande Windows.

```
WmiSetNsSecurity Root\CIMV2 -r %account%

WmiSetNsSecurity Root\CIMV2\power -r %account%

WmiSetNsSecurity Root\Default -r %account%

WmiSetNsSecurity Root\WMI -r %account%
```

Cette configuration doit être poussée à tous les ordinateurs distants qui restent. Cette étape peut également être exécutée quand vous créez un script en lots et le poussez par l'intermédiaire d'un script de connexion d'admin ou d'un script de démarrage d'ordinateur dans le cadre d'une stratégie de groupe.

Configurez les autorisations de système de fichiers.

L'application de CEM exige de pleines autorisations d'accéder au sous-dossier de **Cisco** à l'intérieur du dossier windows (par exemple C:\Windows\Cisco) pour enregistrer et exécuter des scripts. Cette étape doit être faite sur les ressources distantes et des détails de la configuration peuvent être trouvés en cet article sous la section d'autorisation de système de fichiers distant.

https://cem-update.cisco.com/download/files/5.0/docs/CEM_Online_Help/aa1808350.html

Configurez les autorisations de registre

L'application de CEM a besoin de l'accès au registre de périphérique pour enregistrer de diverses données. Référez-vous à la section configurant des autorisations de registre en cet article.

https://cem-update.cisco.com/download/files/5.0/docs/CEM_Online_Help/aa1808350.html

Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Vérifiez le WMI fonctionnant par des diagnostics d'exécution sur un des périphériques de domaine du GUI de CEM. Une configuration réussie ne devrait afficher aucune erreurs associées par WMI.

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.