Configuración WMI en el regulador del Dominio de Windows para el CEM

Contenido

Introducción

Este documento describe los pasos para configurar Windows Management Instrumentation (WMI) en el regulador del Dominio de Windows para la Administración del EnergyWise de Cisco (CEM). WMI se utiliza para acceder remotamente las máquinas de las ventanas a las recolectares datos y para ejecutar los comandos. Aunque el script esté disponible que realiza todos los pasos necesarios inmediatamente, si el controlador de dominio se está utilizando para aplicar las directivas en los dispositivos del dominio, se recomienda para cambiar las configuraciones en la política de dominio, pues los dispositivos reemplazarían los cambios locales. Este documento presenta los pasos para configurar la directiva del grupo en el regulador del Dominio de Windows para preparar los dispositivos del dominio para la interrogación WMI.

> Nota: Aunque WMI esté disponible en el Windows 2000 con el SP2, la aplicación CEM no soporta el Windows 2000. Para utilizar WMI, la aplicación CEM requiere el Microsoft Windows XP SP2 profesional o más adelante.

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene acceso al regulador del Dominio de Windows, al conjunto de administración y a las máquinas remotas (activos) del EnergyWise de Cisco.

Componentes Utilizados

La información en este documento se basa en el entorno CEM 5.2 en el cual el conector del

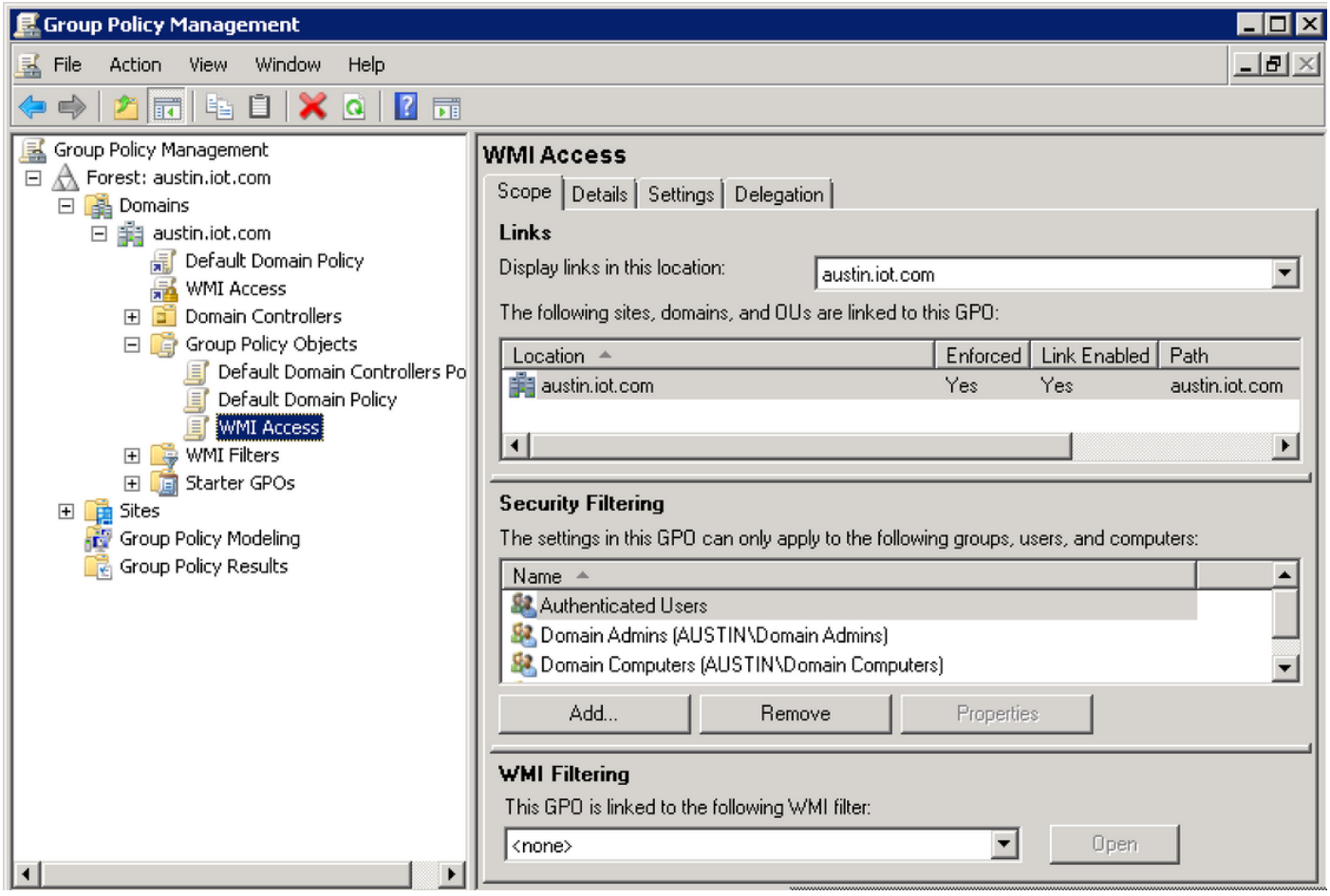
activo del Active Directory (AD) se utiliza para tirar de la información WMI de los dispositivos remotos.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configurar

Cree un nuevo objeto de la directiva del grupo

El primer paso es crear un nuevo objeto de la directiva del grupo. El objeto de la directiva del grupo se puede crear en el controlador de dominio bajo Administración de políticas del grupo como se muestra:



Objeto de la directiva del grupo

WMI: Seguridad de la configuración COM

Para ejecutar las interrogaciones WMI remotamente, se requieren los permisos específicos COM. Seleccione el objeto de la directiva del grupo creado en el paso anterior, haga clic con el botón derecho del ratón y selecto **edite** y después hojee a esta ubicación:

Agrupe la consola de Administración de políticas (GPMC) > configuración de Computadora \ las configuraciones \ los ajustes de seguridad \ las políticas locales \ las opciones de seguridad de Windows

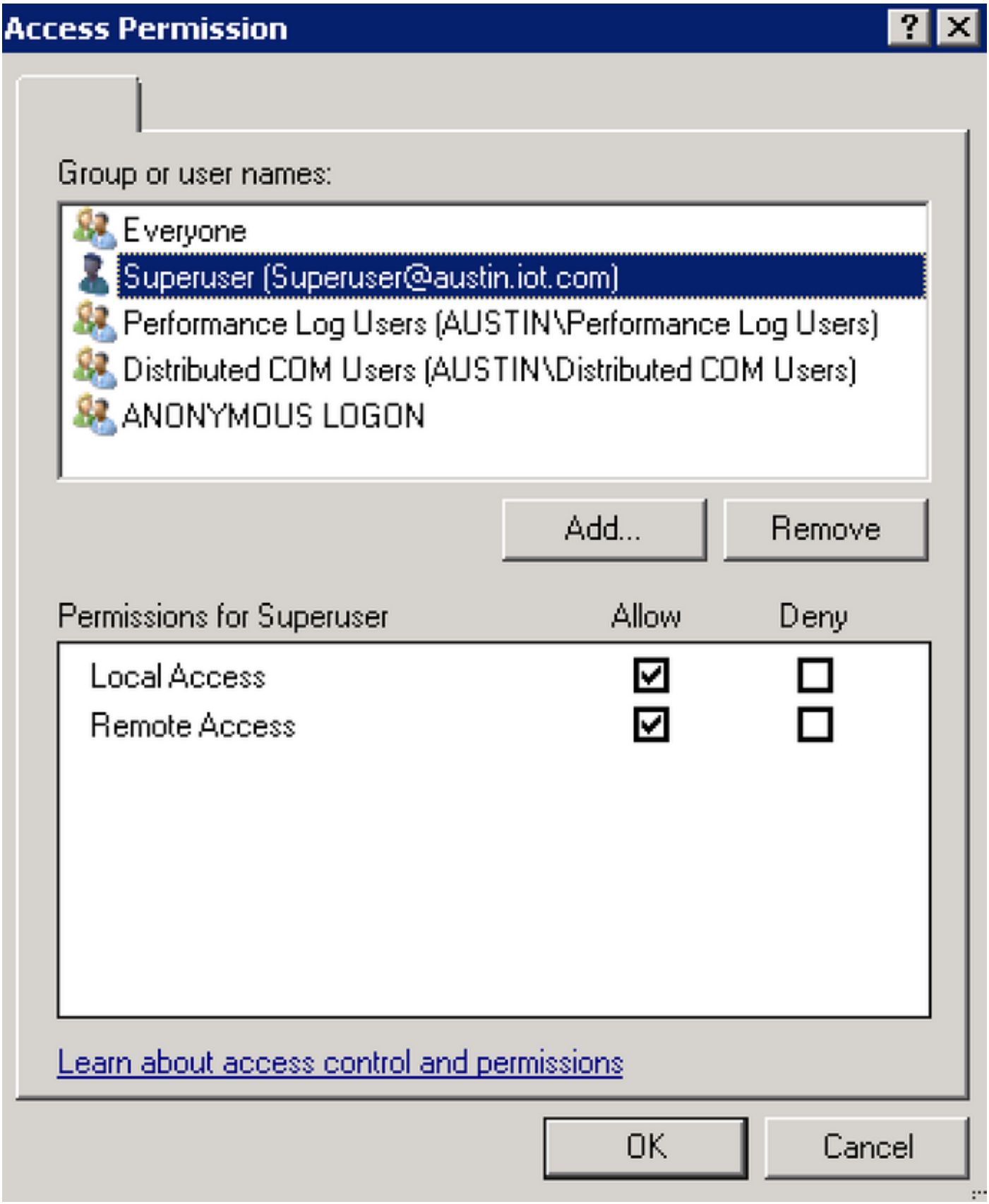
Encuentre el screenshots para configurar los Permisos de acceso remoto para el usuario de los administradores para los permisos COM para:

DCOM: Trabaje a máquina las restricciones de acceso en el sintaxis del Security Descriptor Definition Language (SDDL)

DCOM: Trabaje a máquina las restricciones del lanzamiento en el Security Descriptor Definition Language (SDDL)

Permisos DCOM

Selecto **defina esta configuración de la directiva** y haga clic en **editan la Seguridad**. Proporcione el local y los Permisos de acceso remoto a la cuenta que usted quiere utilizar para WMI.



Permisos de acceso DCOM

Asignación de derechos de usuario

La aplicación CEM requiere los archivos de backup y los directorios y los archivos y los directorios

del Restore cargar el perfil del usuario cuando intenta invocar un proceso. También requiere la fuerza apaga de un telecontrol apaga el privilegio de permitir que la acción POWER_OFF trabaje.

Estos cambios necesitan ser realizados en las configuraciones de la asignación de los derechos de usuario dentro de este objeto de la directiva del grupo. Las estas derechas necesitan ser proporcionadas a la cuenta usada para WMI.

SeRemoteShutdownPrivilege - La fuerza apaga de un sistema remoto

SeBackupPrivilege - Archivos de reserva y directorios

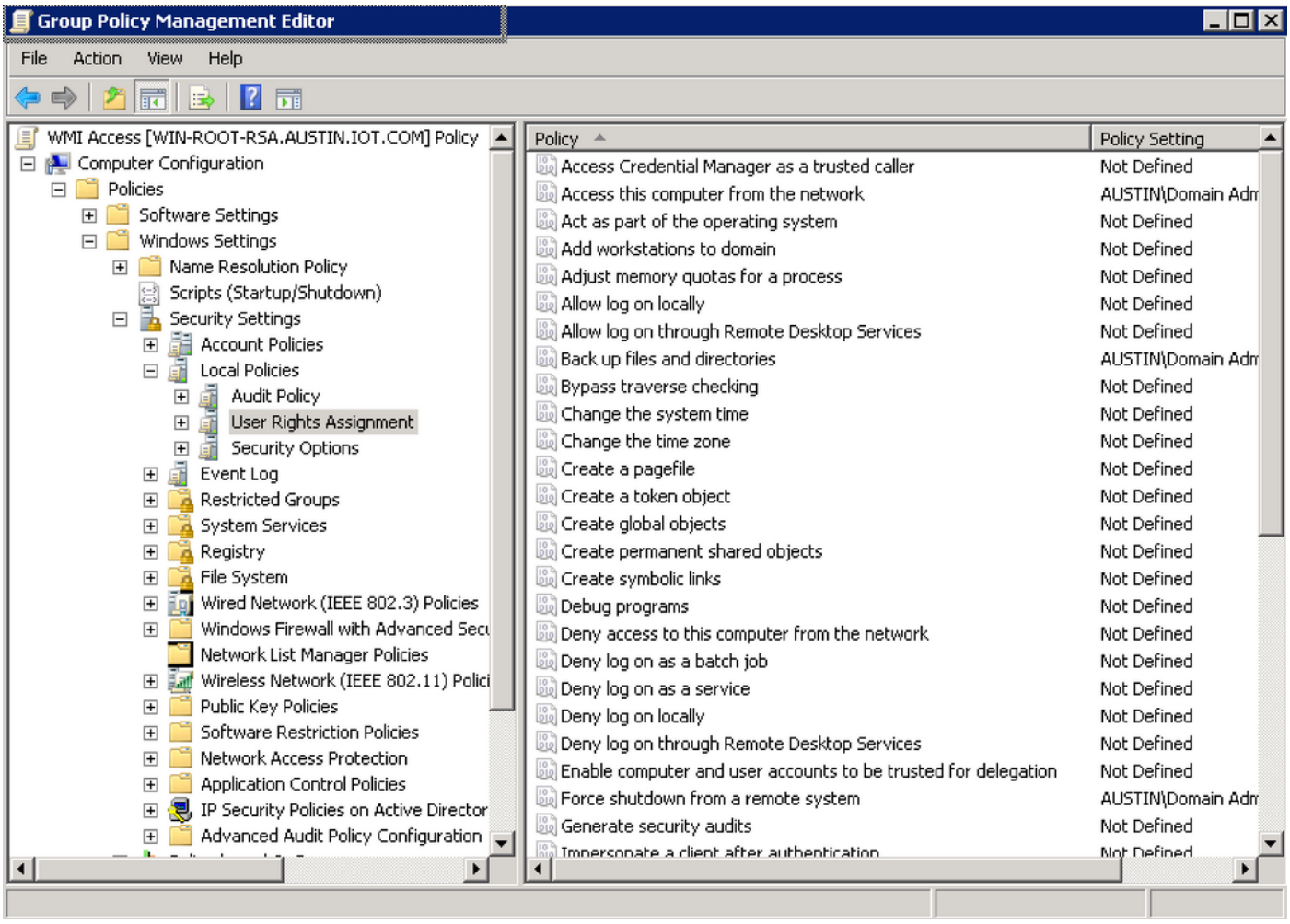
SeRestorePrivilege - Archivos y directorios del Restore

SeNetworkLogonRight - Acceda este ordenador de la red

SeSecurityPrivilege - Elija manejan el registro de seguridad y auditoría

Estas configuraciones se pueden configurar bajo esta trayectoria:

Agrupe la consola de PolicyManagement (GPMC) > configuración de Computadora \ las configuraciones \ los ajustes de seguridad \ las políticas locales \ asignación de derechos de usuario de Windows



Asignación de derechos de usuario

Configuración de escudo de protección

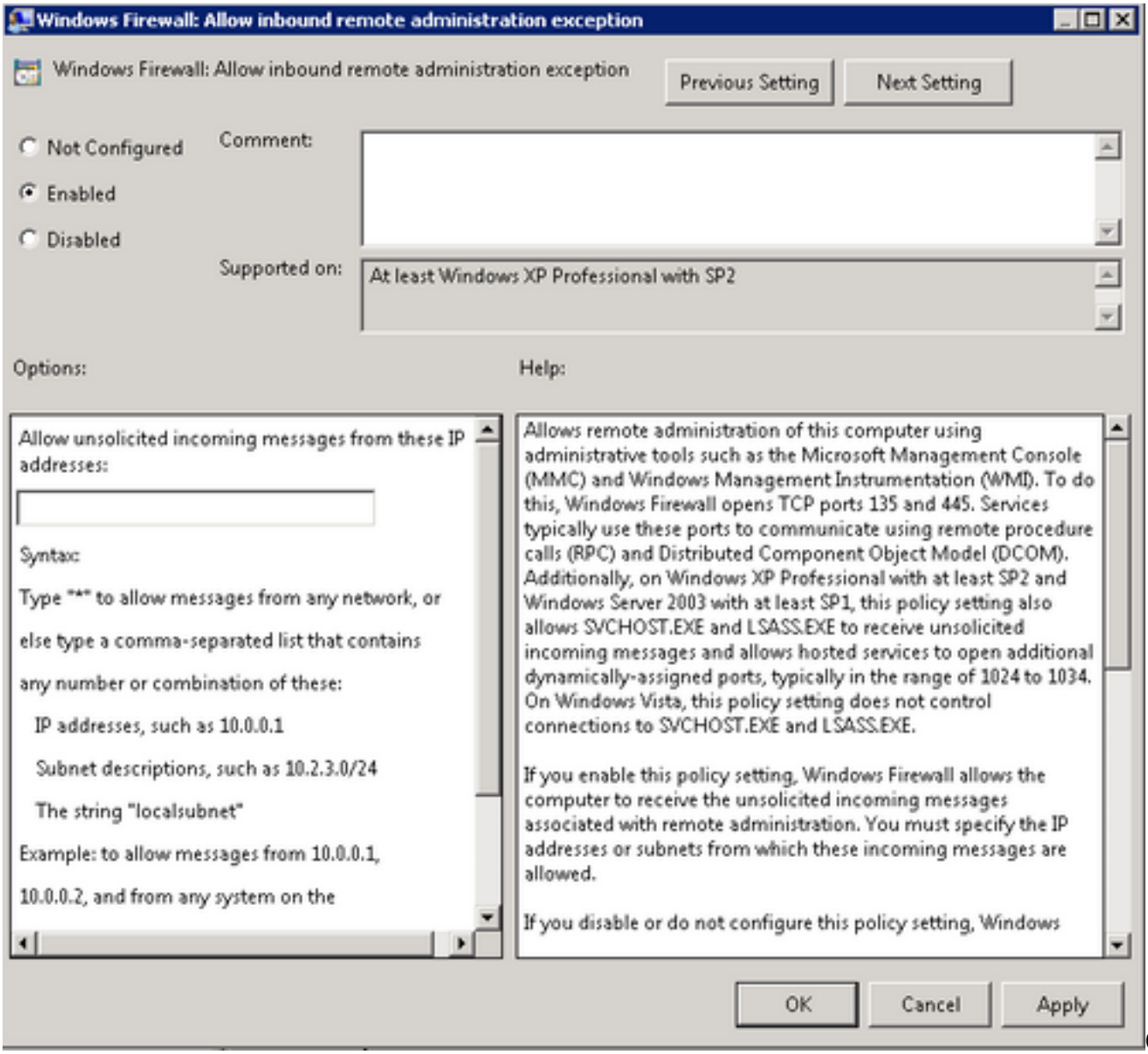
Para realizar las llamadas WMI a un ordenador, el puerto RPC (TCP 135) debe ser accesible externamente. Esto se puede hacer con el uso del editor de la Administración de políticas del grupo, del árbol de menú, navega a la **configuración de Computadora > a las directivas > a las plantillas administrativas: Definiciones de las políticas > red > conexiones de red > firewall de Windows**

Seleccione el **perfil de dominio**, y haga doble clic **firewall de Windows: Permita la excepción de administración remota entrante**. Firewall de Windows: Permita la ventana entrante de la excepción de administración remota aparece.

Tecleo **habilitado**.

Asegúrese de que usted especifique la dirección IP adentro no prohiba a mensajes entrantes no solicitados de estos el campo de los IP Addresses.

Usted puede ingresar * permitir los mensajes de cualquier red, o bien teclea una lista separada por coma que contenga los IP Addresses o las subredes específicos.



Con figuración de escudo de protección

Seguridad namespace WMI

Para habilitar el acceso WMI a una máquina, los permisos específicos WMI se deben habilitar para la cuenta usada. Esta configuración no se puede hacer vía la directiva del grupo en el regulador del Dominio de Windows, él necesita ser hecha en las máquinas remotas con la herramienta de WmiSetNsSecurity.

Fije la Seguridad WMI y funcione con el comando (substituya el %account% por la cuenta de usuario que usted quiere fijar la Seguridad para) en la herramienta de la línea de comando de Windows.

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

WmiSetNsSecurity Root\CIMV2\power -r %account%

WmiSetNsSecurity Root\Default -r %account%

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

Esta configuración necesita ser avanzada a todas las máquinas remotas que permanecen. Este paso puede también ser realizado cuando usted crea un script del lote y lo avanza vía una secuencia de comandos de inicio admin o una secuencia de mandos del inicio de máquina bajo directiva del grupo.

Permisos del sistema de archivos de la configuración.

La aplicación CEM requiere los permisos completos para acceder el subfolder de **Cisco** dentro de la carpeta Windows (e.g. C:\Windows\Cisco) para salvar y para ejecutar los scripts. Este paso necesita ser hecho en los activos remotos y los detalles de la configuración se pueden encontrar en este artículo bajo la sección del permiso del sistema de archivos remotos.

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

Permisos de registro de la configuración

La aplicación CEM necesita el acceso al registro del dispositivo salvar los diversos datos. Refiera a la sección que configura los permisos de registro en este artículo.

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

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Verifique el WMI que funciona ejecutando los diagnósticos en uno de los dispositivos del dominio de los CEM GUI. Una configuración exitosa no debe mostrar ninguna errores relacionados WMI.

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.