Configurar WMI no controlador do domínio do Windows para o CEM

Índice

[Introdução](#)
[Pré-requisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Configurar](#)
[Crie um objeto novo da política do grupo](#)
[WMI: Configurar a Segurança COM](#)
[Atribuição dos direitos do usuário](#)
[Configuração de firewall](#)
[Segurança namespace WMI](#)
[Verificar](#)
[Troubleshooting](#)

Introdução

Este documento descreve as etapas para configurar Windows Management Instrumentation (WMI) no controlador do domínio do Windows para o Gerenciamento da EnergyWise de Cisco (CEM). WMI é usado para alcançar remotamente máquinas dos indicadores aos acúmulos de dados e para executar comandos. Embora o script esteja disponível que executa todas as etapas necessárias imediatamente, se o controlador de domínio está sendo usado para aplicar políticas nos dispositivos do domínio, recomenda-se mudar ajustes na política de domínio, porque os dispositivos cancelariam as mudanças locais. Este documento apresenta as etapas para configurar a política do grupo no controlador do domínio do Windows para preparar os dispositivos do domínio para a interrogação WMI.

> Nota: Embora WMI esteja disponível no Windows 2000 com SP2, o aplicativo CEM não apoia o Windows 2000. Para usar WMI, o aplicativo CEM exige o Microsoft Windows XP SP2 profissional ou mais tarde.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o acesso ao controlador do domínio do Windows, à suite de gerenciamento da EnergyWise de Cisco e às máquinas remotas (ativos).

Componentes Utilizados

A informação neste documento é baseada no ambiente CEM 5.2 em que o conector do ativo do

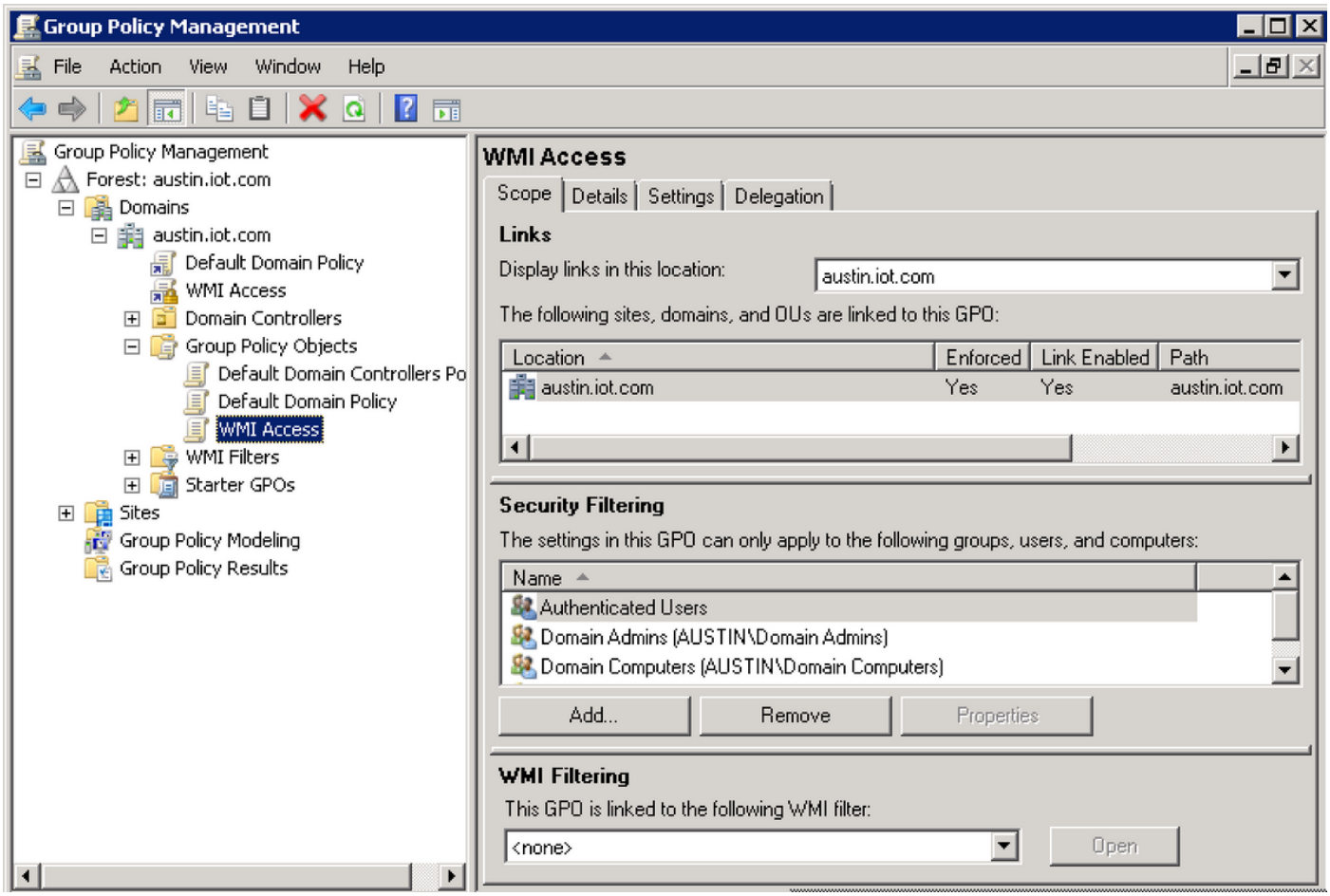
diretório ativo (AD) é usado para puxar a informação WMI dos dispositivos remotos.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Configurar

Crie um objeto novo da política do grupo

A primeira etapa é criar um objeto novo da política do grupo. O objeto da política do grupo pode ser criado no controlador de domínio sob o Gerenciamento de políticas do grupo como mostrado:



Objeto da política do grupo

WMI: Configurar a Segurança COM

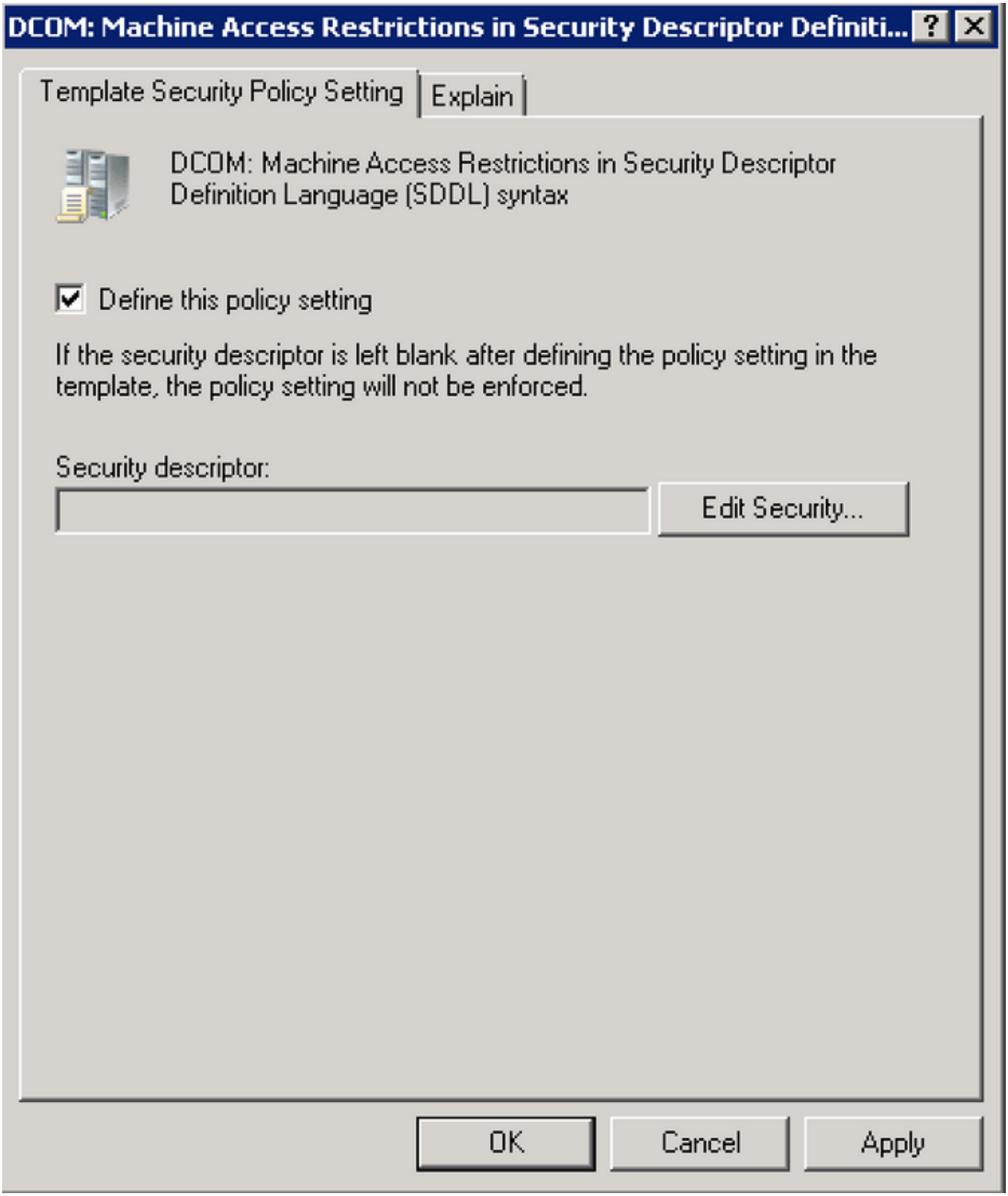
Para executar remotamente perguntas WMI, as permissões específicas COM são exigidas. Selecione o objeto da política do grupo criado na etapa precedente, clicar com o botão direito e seleto **edite** e consulte então a este lugar:

Agrupe o console de Gerenciamento de políticas (GPMC) > configuração de computador \ ajustes \ configurações de segurança \ políticas local \ opções de segurança de Windows

Encontre os screenshots para configurar permissões de acesso remoto para o usuário dos administradores para as permissões COM para:

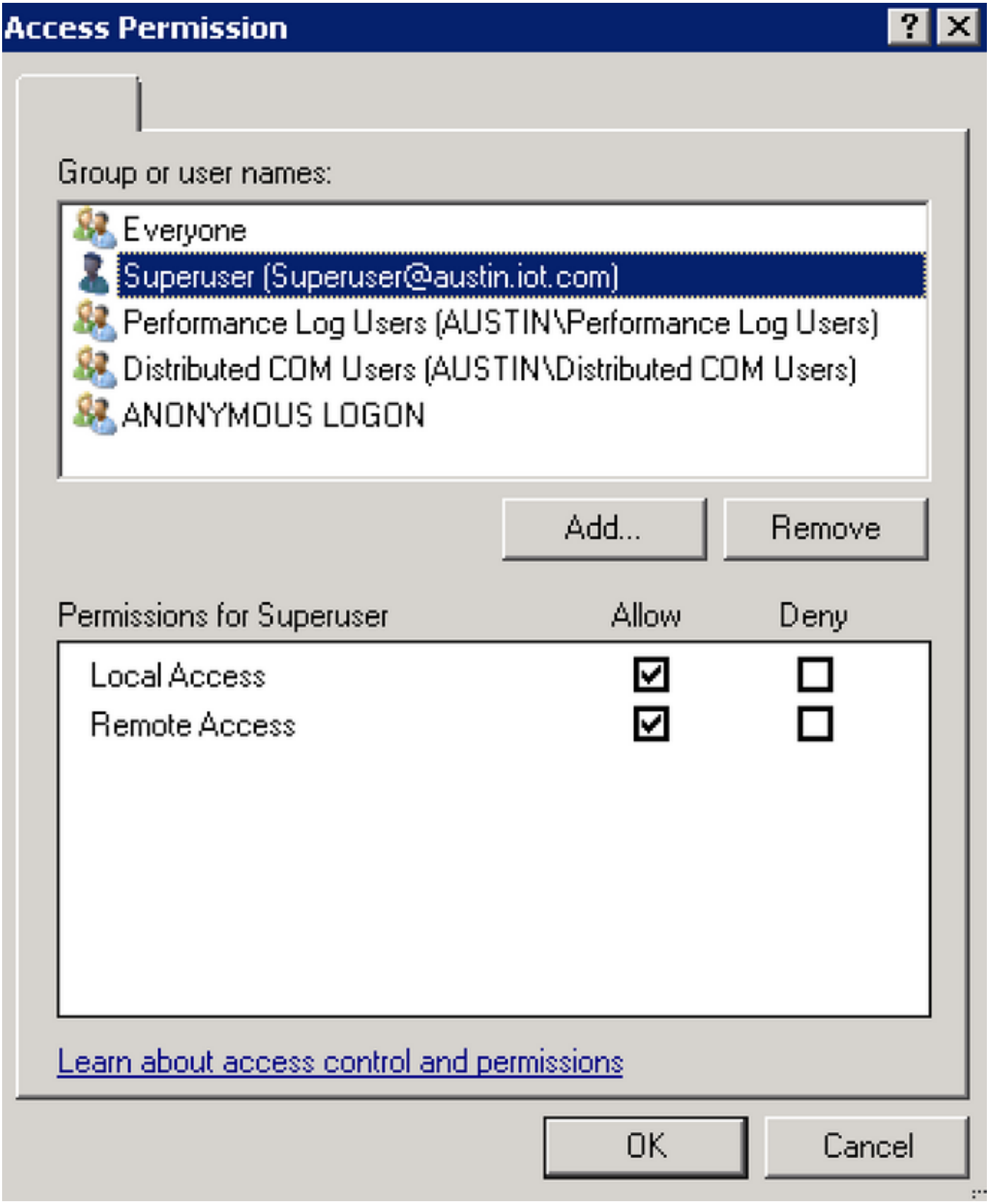
DCOM: Faça à máquina restrições de acesso na sintaxe da língua da definição do descritor de segurança (SDDL)

DCOM: Faça à máquina limitações do lançamento na língua da definição do descritor de segurança (SDDL)



Permissões DCOM

Seleto **defina este ajuste da política** e clique sobre a **Segurança Edit**. Forneça o local e as permissões de acesso remoto à conta que você quer se usar para WMI.



Permissões de acesso DCOM

Atribuição dos direitos do usuário

O aplicativo CEM exige os arquivos de backup e diretórios e arquivos e diretórios da restauração carregar o perfil de usuário quando tenta invocar um processo. Igualmente exige a parada programada da força de um privilégio remoto da parada programada permitir que a ação POWER_OFF trabalhe.

Estas mudanças precisam de ser feitas nos ajustes da atribuição dos direitos do usuário dentro deste objeto da política do grupo. Estes direitos precisam de ser fornecidos à conta usada para WMI.

SeRemoteShutdownPrivilege - Parada programada da força de um sistema remoto

SeBackupPrivilege - Arquivos alternativos e diretórios

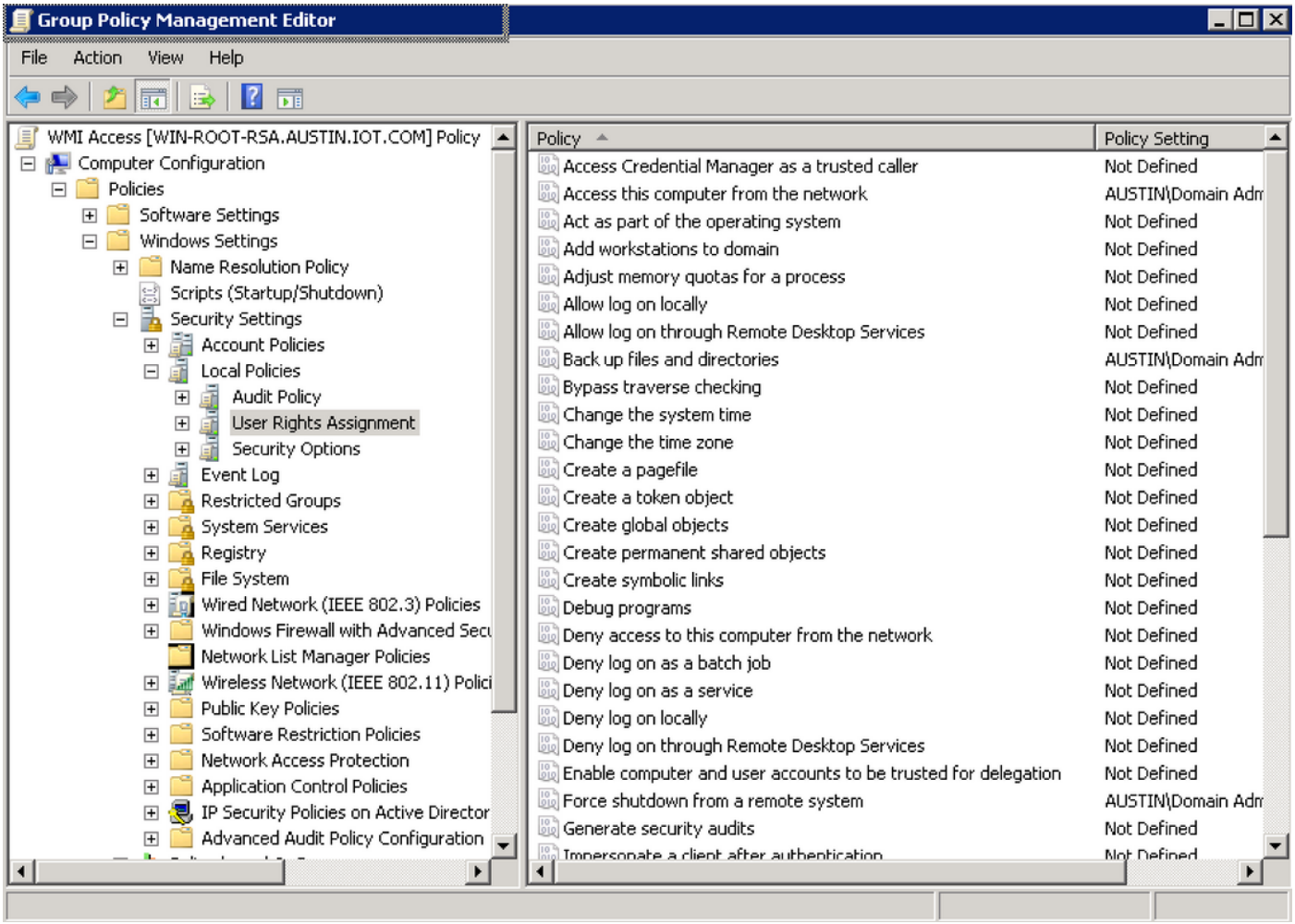
SeRestorePrivilege - Arquivos e diretórios da restauração

SeNetworkLogonRight - Alcance este computador da rede

SeSecurityPrivilege - Escolha o exame e o registro de segurança Manage

Estes ajustes podem ser configurados sob este trajeto:

Agrupe o console de PolicyManagement (GPMC) > configuração de computador \ ajustes de Windows \ configurações de segurança \ políticas local \ atribuição dos direitos do usuário



Atribuição dos direitos do usuário

Configuração de firewall

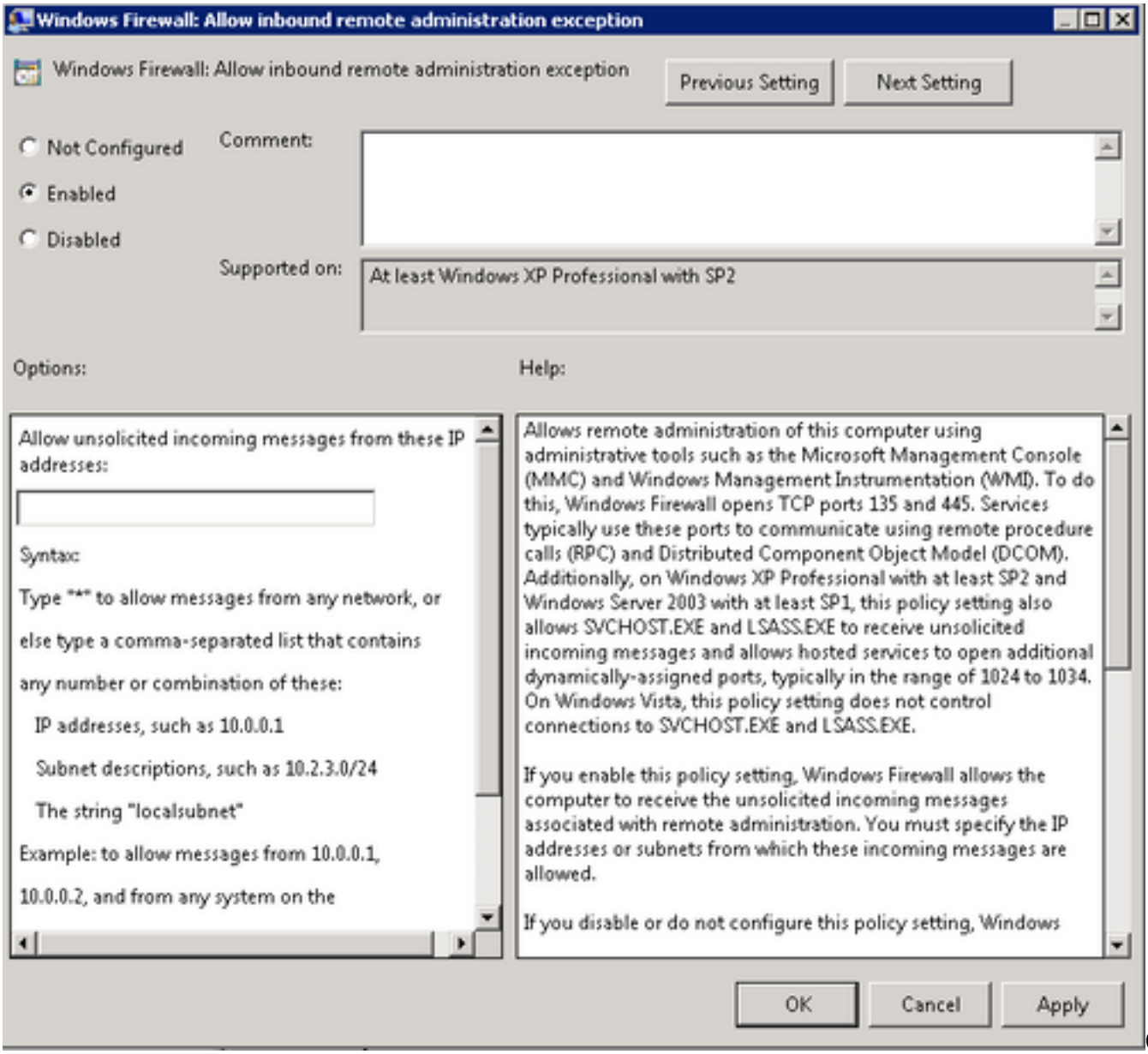
Para executar atendimentos WMI a um computador, a porta RPC (TCP 135) deve ser acessível externamente. Isto pode ser feito com o uso do editor do Gerenciamento de políticas do grupo, da árvore de menu, navega à **configuração de computador > às políticas > moldes administrativos: Definições de política > rede > conexões de rede > Windows Firewall**

Selecione o **perfil do domínio**, e fazer duplo clique o **Windows Firewall: Permita a exceção de entrada da administração remota**. O Windows Firewall: Permita a administração remota de entrada o indicador da exceção que aparece.

Clique **permitido**.

Assegure-se de que você especifique o endereço IP de Um ou Mais Servidores Cisco ICM NT permita dentro mensagens recebida espontâneos do campo destes endereços IP de Um ou Mais Servidores Cisco ICM NT.

Você pode entrar * para permitir mensagens de toda a rede, ou então datilografa uma lista vírgula-separada que contenha endereços IP de Um ou Mais Servidores Cisco ICM NT ou sub-redes específicas.



Con figuração de firewall

Segurança namespace WMI

Para permitir o acesso WMI a uma máquina, as permissões específicas WMI devem ser

permitidas para a conta usada. Esta configuração não pode ser feita através da política do grupo no controlador do domínio do Windows, ele precisa de ser feita nas máquinas remotas com a ferramenta de WmiSetNsSecurity.

Ajuste a Segurança WMI e execute o comando (substitua %account% com a conta de usuário que você quer ajustar a Segurança para) na ferramenta da linha 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 configuração precisa de ser empurrada para todas as máquinas remotas que permanecem. Esta etapa pode igualmente ser executada quando você cria um script do grupo e o empurra através de um script de logon admin ou de um script de inicialização de máquina sob uma política do grupo.

Configurar permissões do sistema de arquivos.

O aplicativo CEM exige permissões completas alcançar a subpasta de **Cisco** dentro do dobrador de Windows (por exemplo C:\Windows\Cisco) para armazenar e executar scripts. Esta etapa precisa de ser executada em ativos remotos e os detalhes de configuração podem ser encontrados neste artigo sob a seção da permissão do sistema de arquivo remoto.

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

Configurar permissões do registro

O aplicativo CEM precisa o acesso ao registro do dispositivo de armazenar vários dados. Refira a seção que configura permissões do registro neste artigo.

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

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Verifique o WMI que funciona executando diagnósticos em um dos dispositivos do domínio dos CEM GUI. Uma configuração bem-sucedida não deve mostrar nenhuns erros relacionados WMI.

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.