CEM용 Windows 도메인 컨트롤러에서 WMI 구성

목차

소개

이 문서에서는 CEM(Cisco Energywise Management)용 Windows 도메인 컨트롤러에서 WMI(Windows Management Instrumentation)를 구성하는 단계에 대해 설명합니다.WMI는 데이터를 수집하고 명령을 실행하기 위해 Windows 컴퓨터에 원격으로 액세스하는 데 사용됩니다.필요한 모든 단계를 동시에 수행하는 스크립트를 사용할 수 있지만 도메인 컨트롤러를 사용하여 도메인 장치에 정책을 적용하는 경우 장치가 로컬 변경 사항을 재정의하므로 도메인 정책의 설정을 변경하는 것이 좋습니다. 이 문서에서는 Windows 도메인 컨트롤러에서 그룹 정책을 구성하여 WMI 질문을 위한 도메인 장치를 준비하는 단계를 제공합니다.

> **참고:**WMI는 Windows 2000 SP2에서 사용할 수 있지만 CEM 응용 프로그램은 Windows 2000을 지원하지 않습니다.WMI를 사용하려면 CEM 응용 프로그램에 Microsoft Windows XP Professional SP2 이상이 필요합니다.

사전 요구 사항

요구 사항

Windows 도메인 컨트롤러, Cisco Energywise Management Suite 및 원격 머신(자산)에 액세스할 수 있는 것이 좋습니다.

사용되는 구성 요소

이 문서의 정보는 AD(Active Directory) 자산 커넥터를 사용하여 원격 디바이스에서 WMI 정보를 가져오는 CEMS 5.2 환경을 기반으로 합니다.

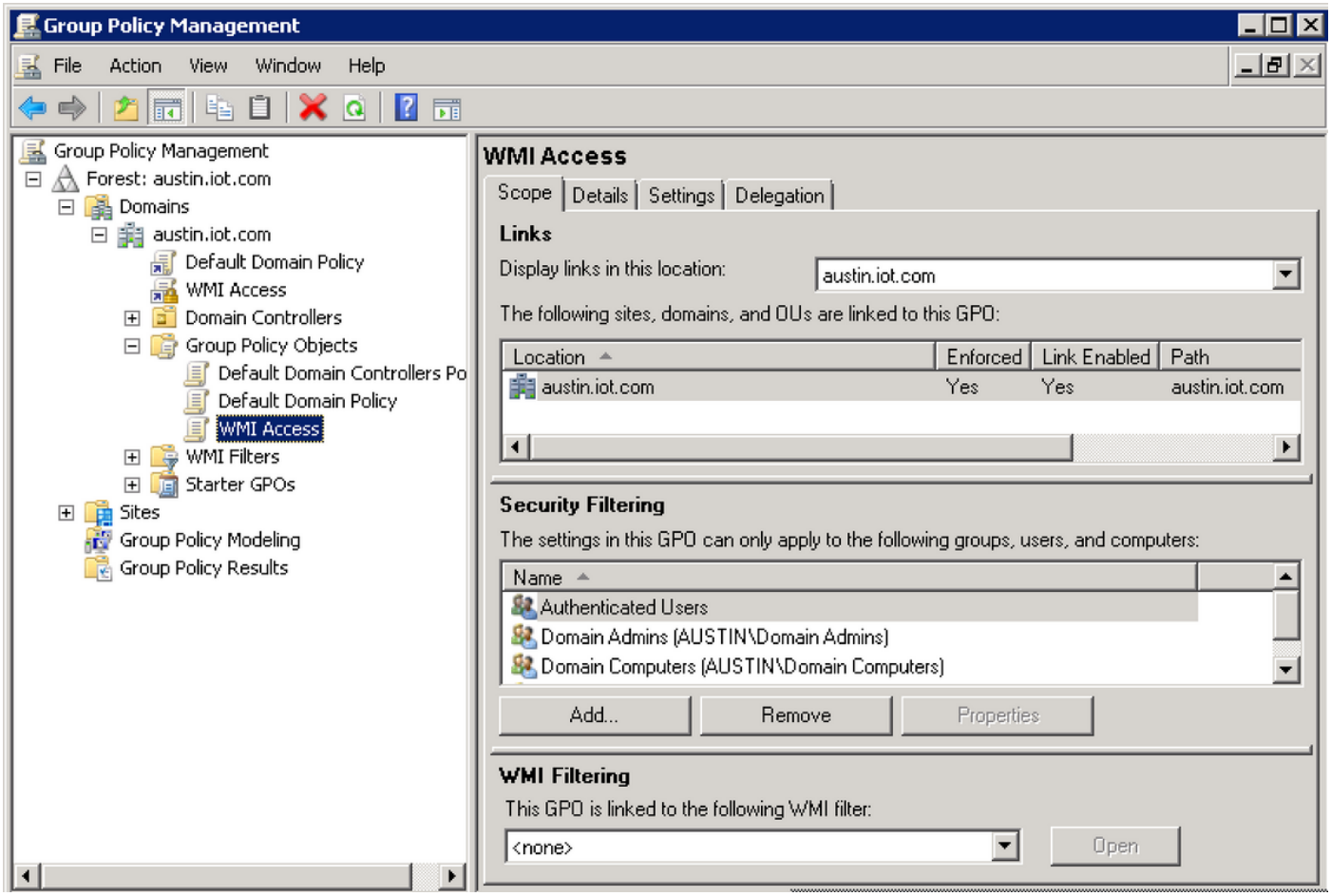
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든

명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

새 그룹 정책 개체 만들기

첫 번째 단계는 새 그룹 정책 개체를 만드는 것입니다.다음과 같이 Group Policy Management(그룹 정책 관리) 아래의 도메인 컨트롤러에서 그룹 정책 개체를 생성할 수 있습니다.



그룹 정책 개체

WMI:COM 보안 구성

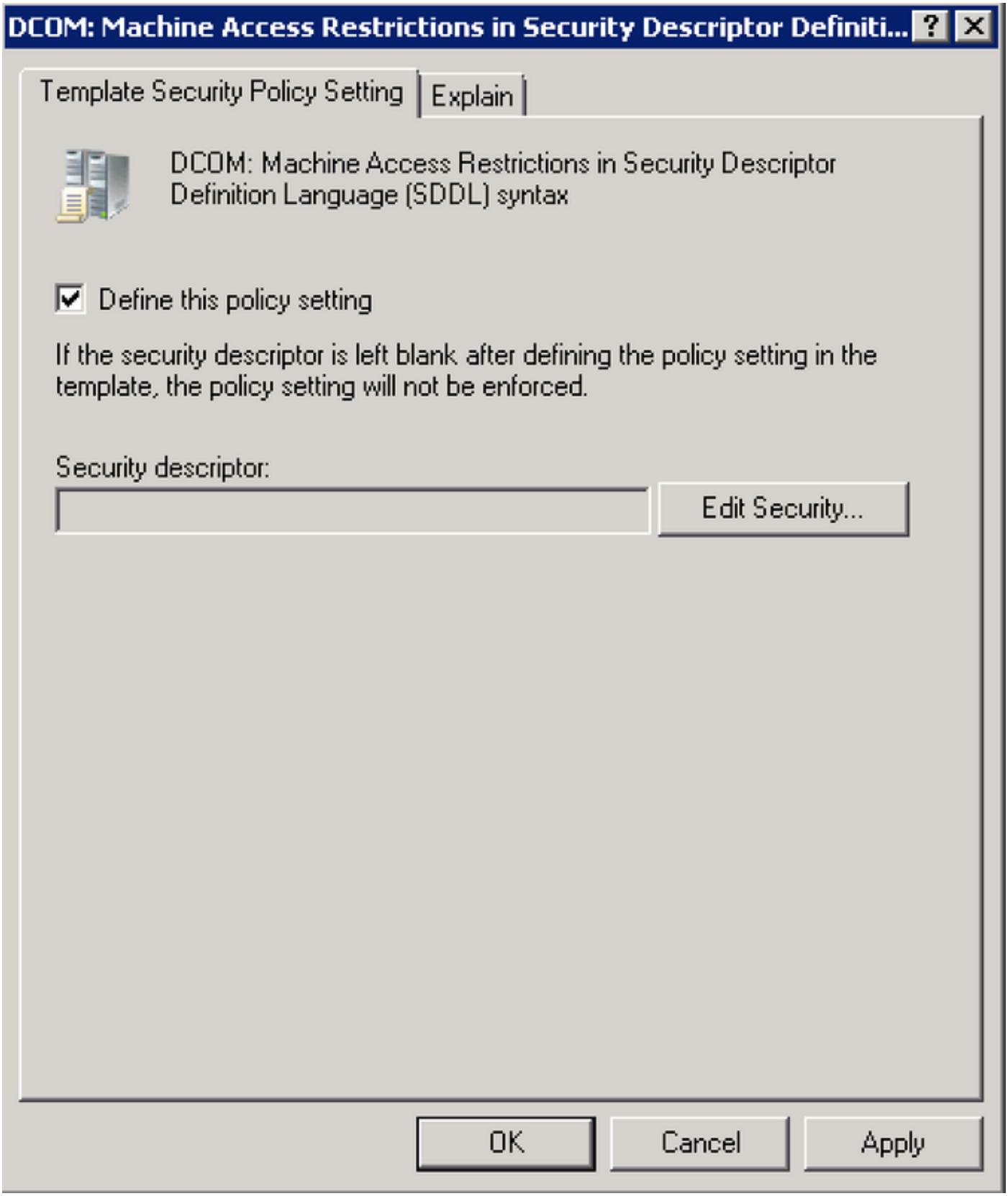
WMI 쿼리를 원격으로 실행하려면 특정 COM 권한이 필요합니다.이전 단계에서 생성된 그룹 정책 개체를 선택하고 마우스 오른쪽 단추를 클릭한 다음 **edit**를 선택한 다음 이 위치로 이동합니다.

GPMC(그룹 정책 관리 콘솔) > 컴퓨터 구성\Windows 설정\보안 설정\로컬 정책\보안 옵션

다음에 대한 COM 권한에 대해 Administrators 사용자의 원격 액세스 권한을 구성하는 스크린샷을 찾습니다.

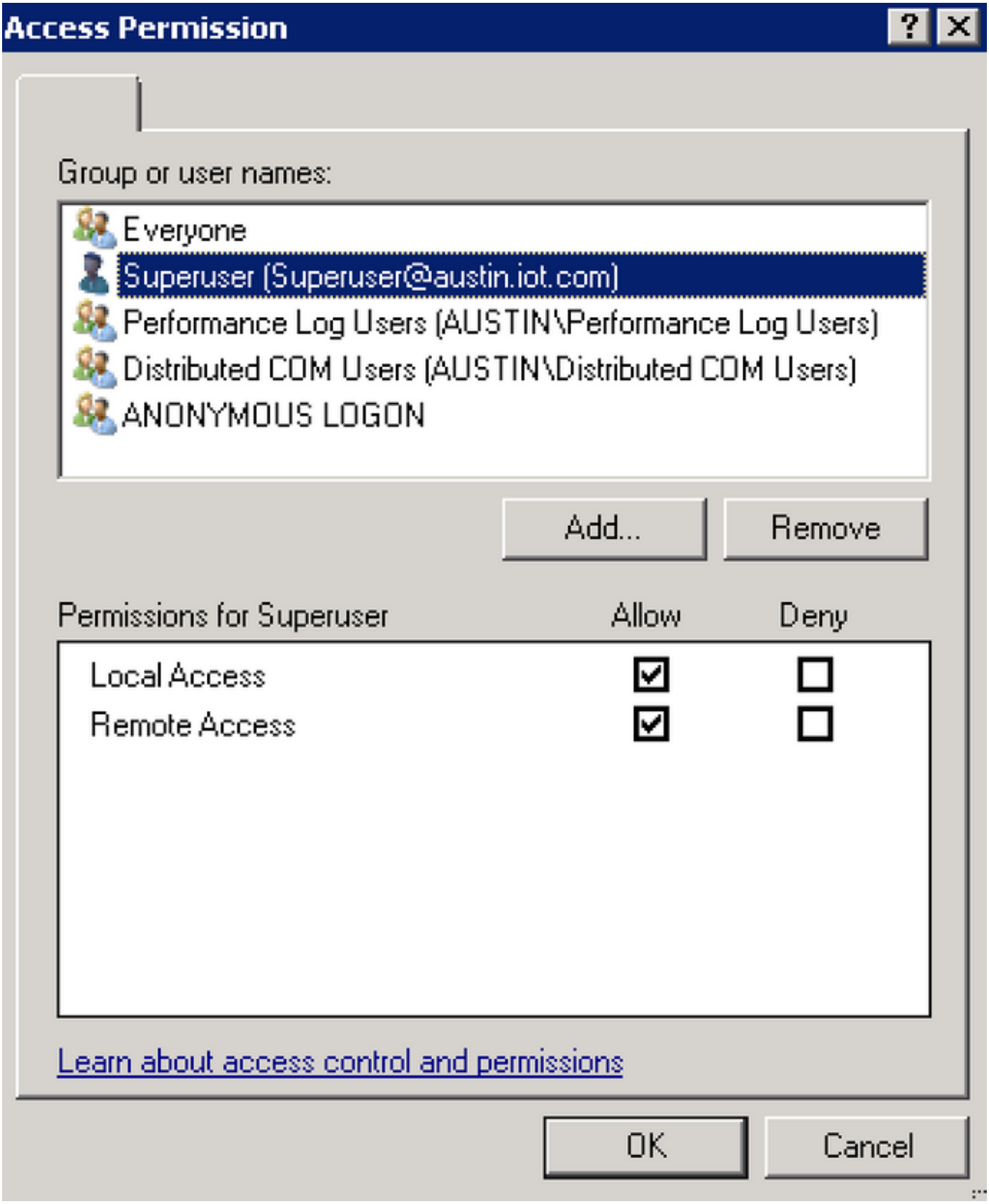
DCOM:SDDL(Security Descriptor Definition Language) 구문의 시스템 액세스 제한

DCOM:SDDL(Security Descriptor Definition Language)의 컴퓨터 실행 제한



DCOM 권한

Define **this policy setting(이 정책 설정 정의)**을 선택하고 Edit Security(**보안 수정)를 클릭합니다** .WMI에 사용할 계정에 로컬 및 원격 액세스 권한을 제공합니다.



DCOM 액세스 권한

사용자 권한 할당

CEM 응용 프로그램을 실행하려면 Backup files and directories(백업 파일 및 디렉토리) 및 Restore files and directories(복원 파일 및 디렉토리)가 모두 사용자 프로필을 로드해야 합니다.또한 POWER_OFF 작업이 작동하도록 하려면 원격 종료 권한에서 강제 종료가 필요합니다.

이러한 변경 사항은 이 그룹 정책 개체 내의 사용자 권한 할당 설정에서 이루어져야 합니다.WMI에 사용되는 계정에 이러한 권한을 제공해야 합니다.

SeRemoteShutdownPrivilege - 원격 시스템에서 강제 종료

SeBackupPrivilege - 파일 및 디렉토리 백업

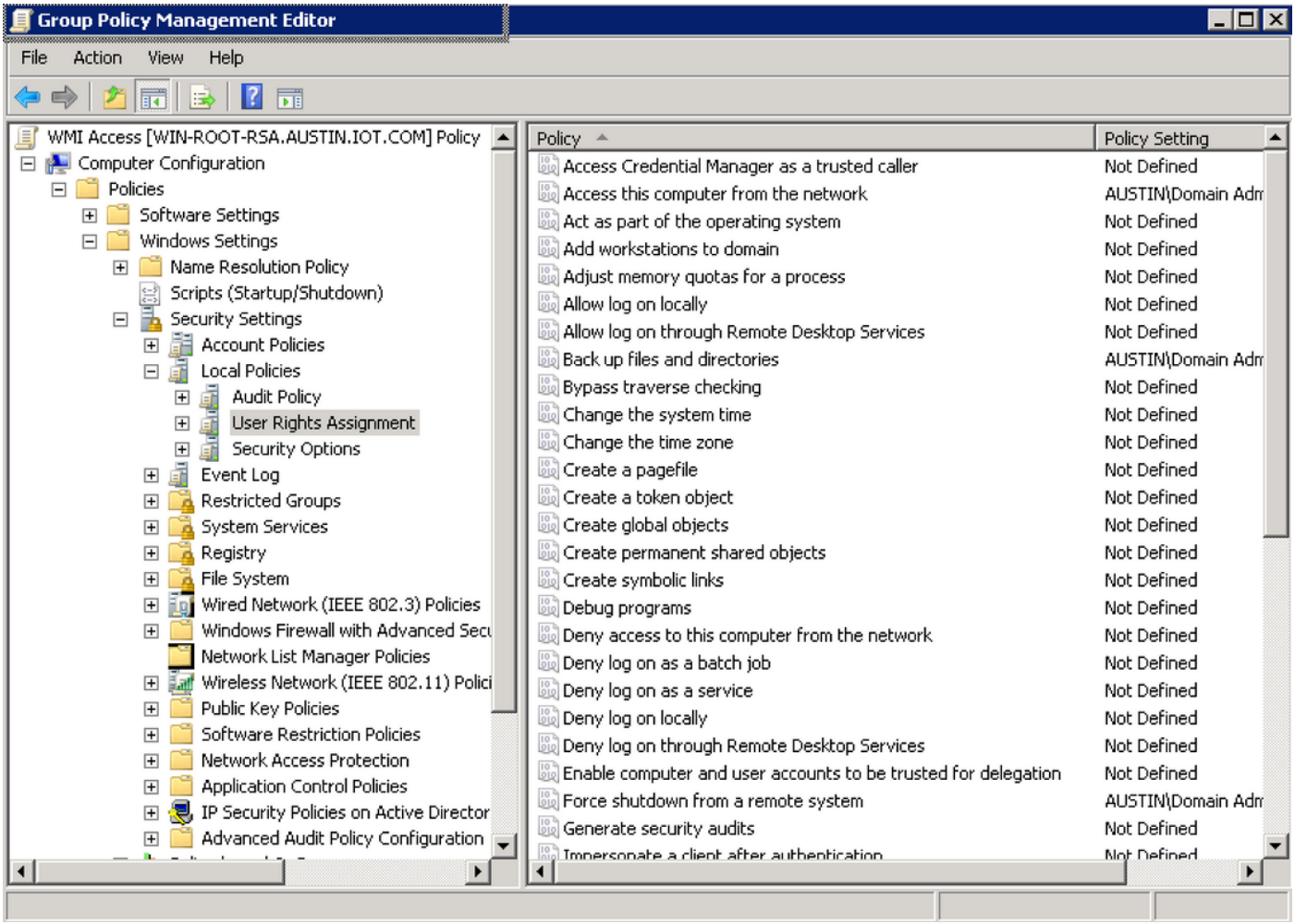
SeRestorePrivilege - 파일 및 디렉터리 복원

UseNetworkLogonRight - 네트워크에서 이 컴퓨터에 액세스

SeSecurityPrivilege - 감사 및 보안 로그 관리를 선택합니다.

다음 경로에서 이 설정을 구성할 수 있습니다.

그룹 정책관리 콘솔(GPMC) > 컴퓨터 구성\Windows 설정\보안 설정\로컬 정책\사용자 권한 할당



사용자 권한 할당

방화벽 구성

컴퓨터에 대한 WMI 호출을 수행하려면 외부에서 RPC 포트(TCP 135)에 액세스할 수 있어야 합니다.이 작업은 그룹 정책 관리 편집기를 사용하여 수행할 수 있습니다. 메뉴 트리에서 Computer Configuration(**컴퓨터 구성) > Policies(정책) > Administrative Templates(관리 템플릿)로 이동합니다.정책 정의 > 네트워크 > 네트워크 연결 > Windows 방화벽**

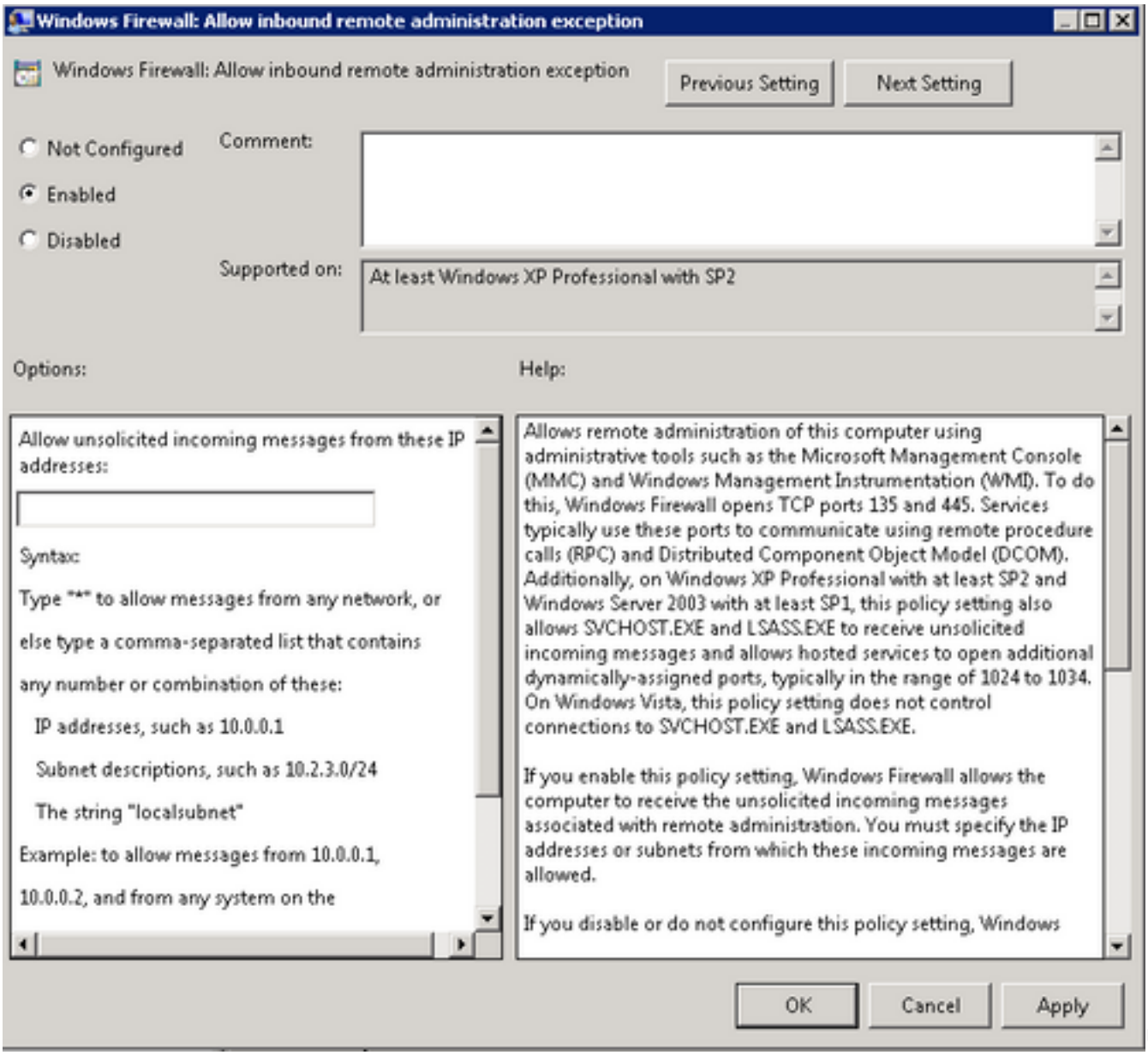
Domain **Profile(도메인 프로필)**을 선택하고 **Windows 방화벽**을 두 번 클릭합니다.**인바운드 원격 관**

리 예외를 허용합니다.Windows 방화벽:인바운드 원격 관리 예외 허용 창이 나타납니다.

Enabled를 **클릭합니다**.

Allow unsolicted incoming messages from these IP addresses(이러한 IP 주소로부터 원치 않는 수신 메시지 허용) 필드에 IP 주소를 지정해야 합니다.

임의의 네트워크에서 메시지를 허용하려면 *를 입력하거나, 특정 IP 주소 또는 서브넷을 포함하는 쉼표로 구분된 목록을 입력할 수 있습니다.



방화벽 구성

WMI 네임스페이스 보안

컴퓨터에 대한 WMI 액세스를 사용하려면 사용된 계정에 대해 특정 WMI 권한을 사용하도록 설정해야 합니다.이 구성은 Windows 도메인 컨트롤러의 그룹 정책을 통해 수행할 수 없습니다. WmiSetNsSecurity 도구를 사용하여 원격 컴퓨터에서 수행해야 합니다.

WMI 보안을 설정하고 Windows 명령줄 도구에서 명령(%account%을(를) 보안을 설정할 사용자 계

정으로 바꾸기)을 실행합니다.

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

WmiSetNsSecurity Root\CIMV2\power -r %account%

WmiSetNsSecurity Root\Default -r %account%

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

이 컨피그레이션은 남아 있는 모든 원격 시스템에 푸시해야 합니다.이 단계는 배치 스크립트를 생성하고 그룹 정책 아래의 관리자 로그온 스크립트 또는 시스템 시작 스크립트를 통해 푸시할 때도 수행할 수 있습니다.

파일 시스템 권한을 구성합니다.

CEM 애플리케이션에는 Windows 폴더(예: C:\Windows\Cisco)의 **Cisco** 하위 폴더에 액세스하여 스크립트를 저장하고 실행할 수 있는 전체 권한이 필요합니다.이 단계는 원격 자산에 대해 수행해야 하며 구성에 대한 자세한 내용은 원격 파일 시스템 권한 섹션의 이 문서에서 확인할 수 있습니다.

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

레지스트리 권한 구성

CEM 애플리케이션은 다양한 데이터를 저장하기 위해 디바이스 레지스트리에 액세스해야 합니다.이 문서의 레지스트리 권한 구성 섹션을 참조하십시오.

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

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

CEMS GUI에서 도메인 장치 중 하나에 대한 진단을 실행하여 WMI가 작동하는지 확인합니다.구성이 성공하면 WMI 관련 오류가 표시되지 않아야 합니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.