Sourcefire 사용자 에이전트에서 사용하는 Active Directory 사용자 계정에 최소 권한 부여

목차

소개

이 문서에서는 AD(Active Directory) 사용자에게 AD 도메인 컨트롤러를 쿼리하는 데 필요한 최소한의 권한을 제공하는 방법에 대해 설명합니다. Sourcefire 사용자 에이전트는 AD 도메인 컨트롤러를 쿼리하기 위해 AD 사용자를 사용합니다.쿼리를 수행하기 위해 AD 사용자는 추가 권한이 필요하지 않습니다.

사전 요구 사항

요구 사항

Cisco에서는 Microsoft Windows 시스템에 Sourcefire 사용자 에이전트를 설치하고 AD 도메인 컨트롤러에 대한 액세스를 제공해야 합니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

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

먼저 관리자는 사용자 에이전트 액세스를 위해 특별히 새 AD 사용자를 생성해야 합니다.이 새 사용

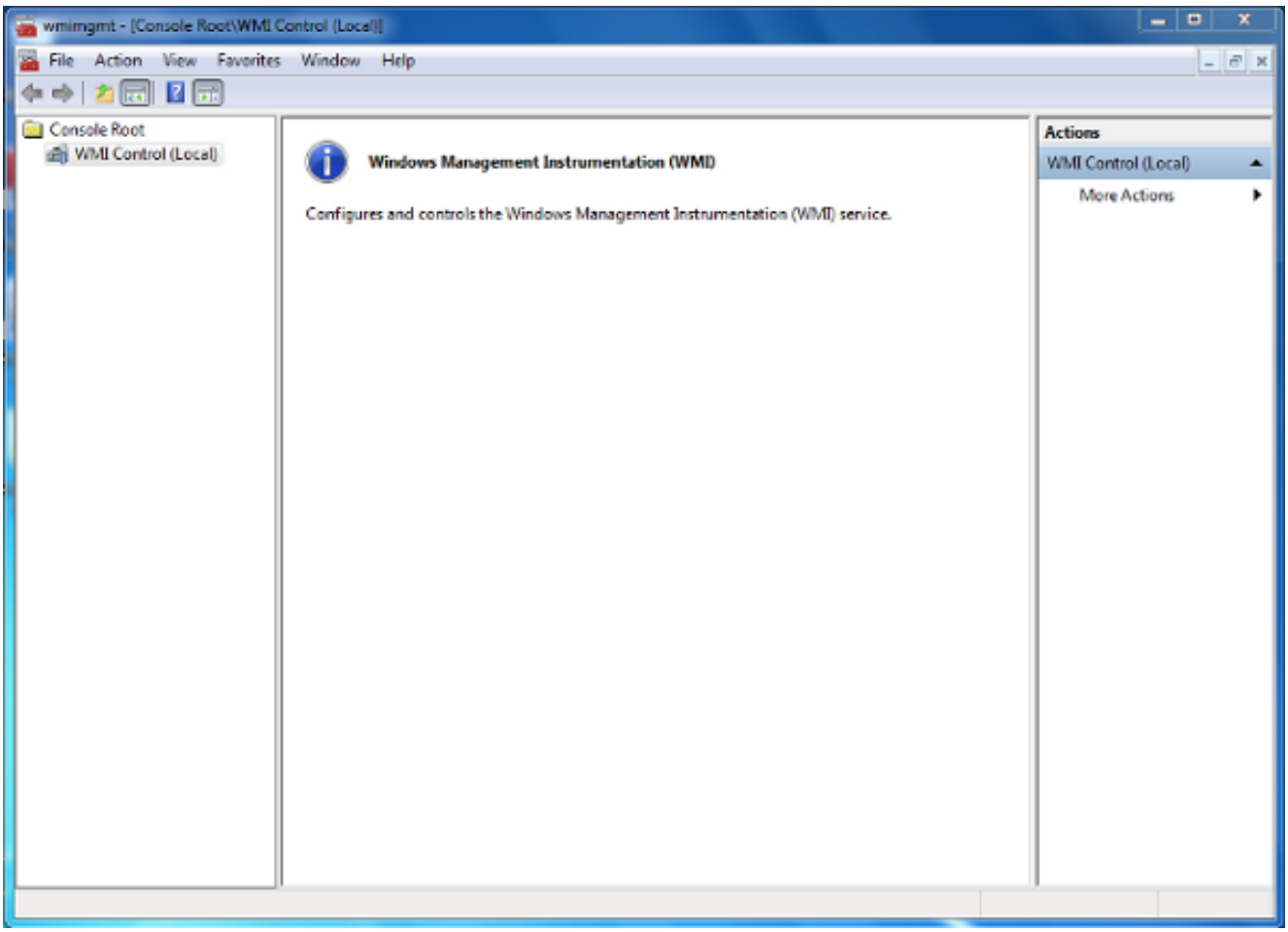
자가 도메인 관리자 그룹의 구성원이 아닌 경우(이 사용자는 이 그룹의 구성원이 아니어야 함) 사용자에게 WMI(Windows Management Instrumentation) 보안 로그에 액세스할 수 있는 권한을 명시적으로 부여해야 할 수 있습니다.권한을 부여하려면 다음 단계를 완료하십시오.

1. WMI 제어 콘솔을 엽니다.

   AD 서버에서 **시작** 메뉴를 선택합니다.

   Run(**실행**)을 클릭하고 wmimgmt.**msc를 입력합니다**.

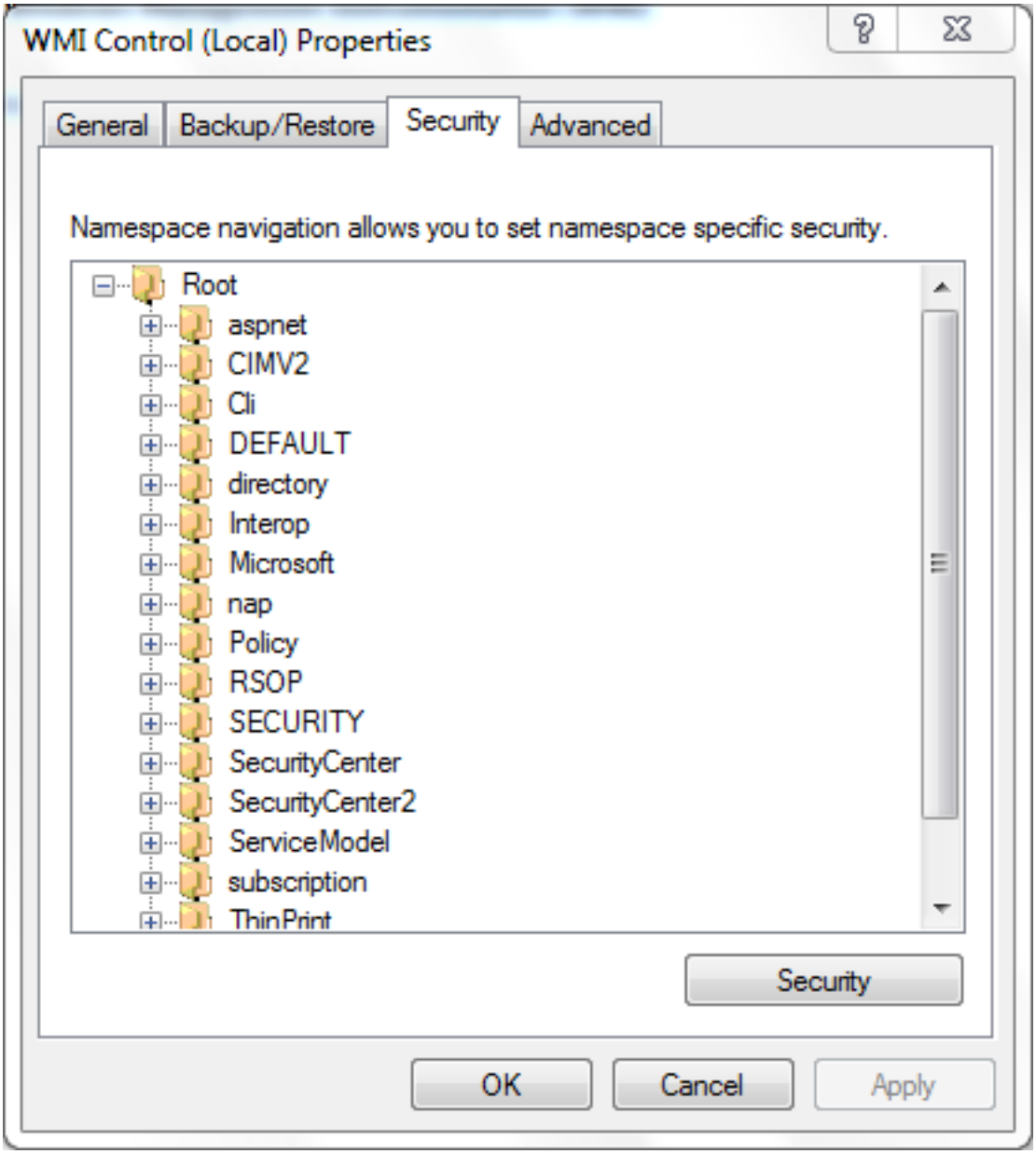
   확인을 **클릭합니다**.WMI 제어 콘솔이 나타납니다.



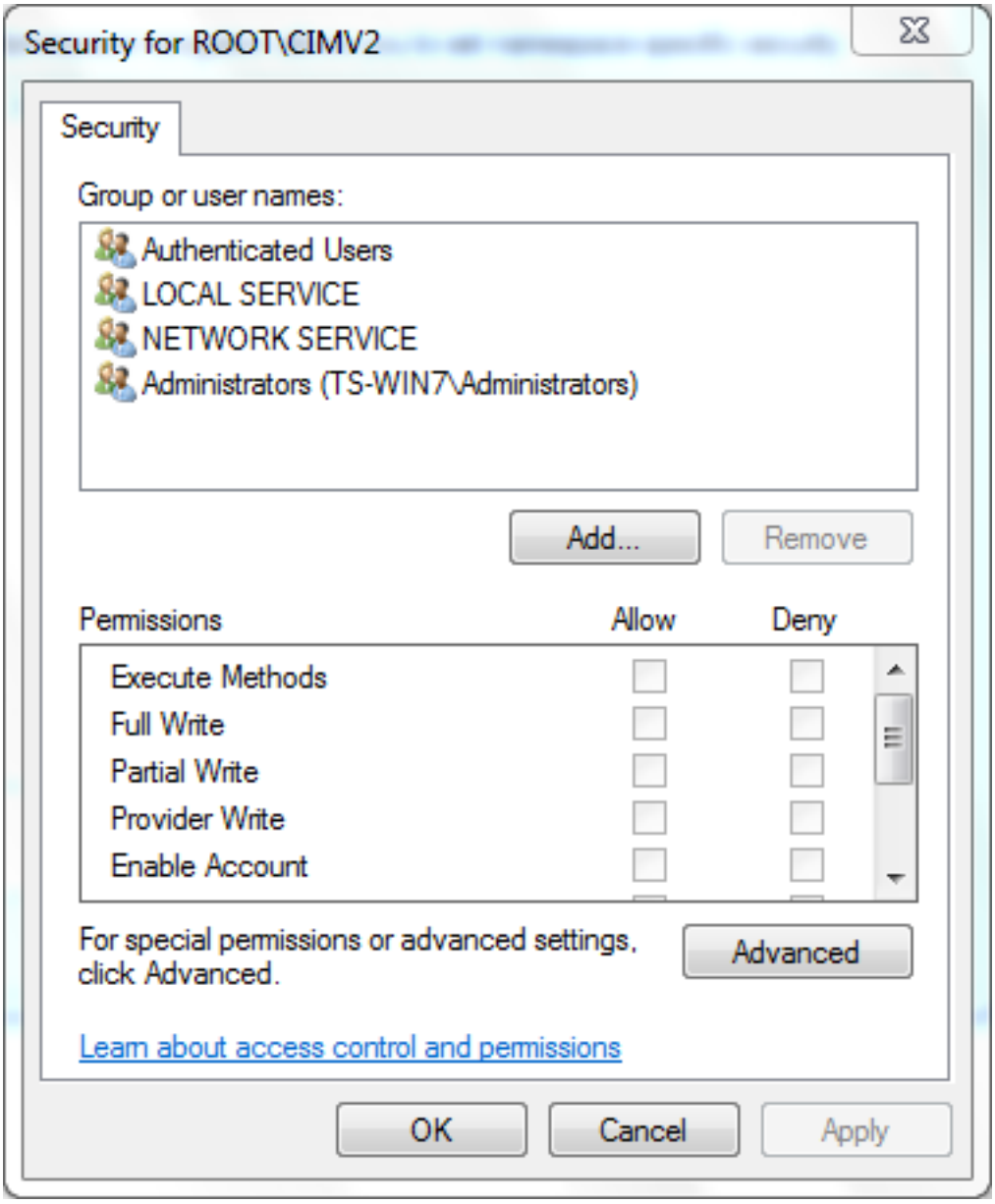
2. WMI 콘솔 트리에서 WMI **Control**을 마우스 오른쪽 단추로 클릭한 다음 **속성**을 클릭합니다.

3. **보안** 탭을 클릭합니다.

4. 사용자 또는 그룹 액세스(Root\CIMV2)를 부여할 네임스페이스를 선택한 다음 **보안을** 클릭합니다.



5. 보안 대화 상자에서 추가를 **클릭합니다**.



6. 사용자, 컴퓨터 또는 그룹 선택 대화 상자에서 추가할 개체(사용자 또는 그룹)의 이름을 입력합니다.이름 **확인**을 클릭하여 항목을 확인한 다음 **확인**을 클릭합니다.객체를 쿼리하려면 위치를 변경하거나 **고급**을 클릭해야 할 수 있습니다.자세한 내용은 문맥에 따른 도움말(**?**)을 참조하십시오.

7. 보안 대화 상자의 사용 권한 섹션에서 **허용** 또는 **거부**를 선택하여 새 사용자 또는 그룹에 사용 권한을 부여합니다(모든 사용 권한을 부여하는 것이 가장 쉬움). 사용자에게 최소한 **원격 사용** 권한을 부여해야 합니다.

8. 변경 사항**을** 저장하려면 Apply를 클릭합니다.창을 닫습니다.

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

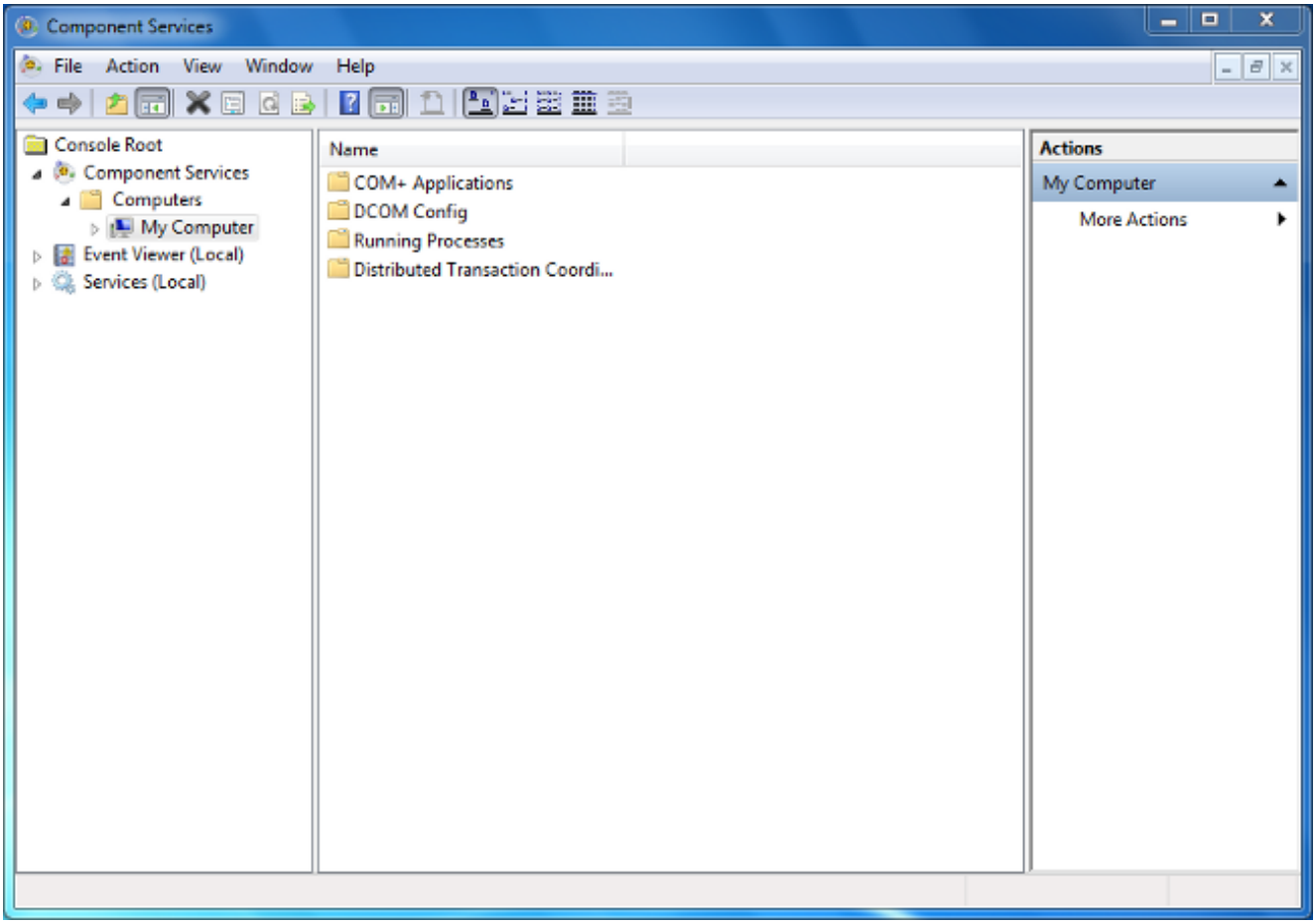
이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

구성 변경 후에도 문제가 계속되면 원격 액세스를 허용하려면 DCOM(Distributed Component Object Model) 설정을 업데이트하십시오.

1. **시작** 메뉴를 선택합니다.

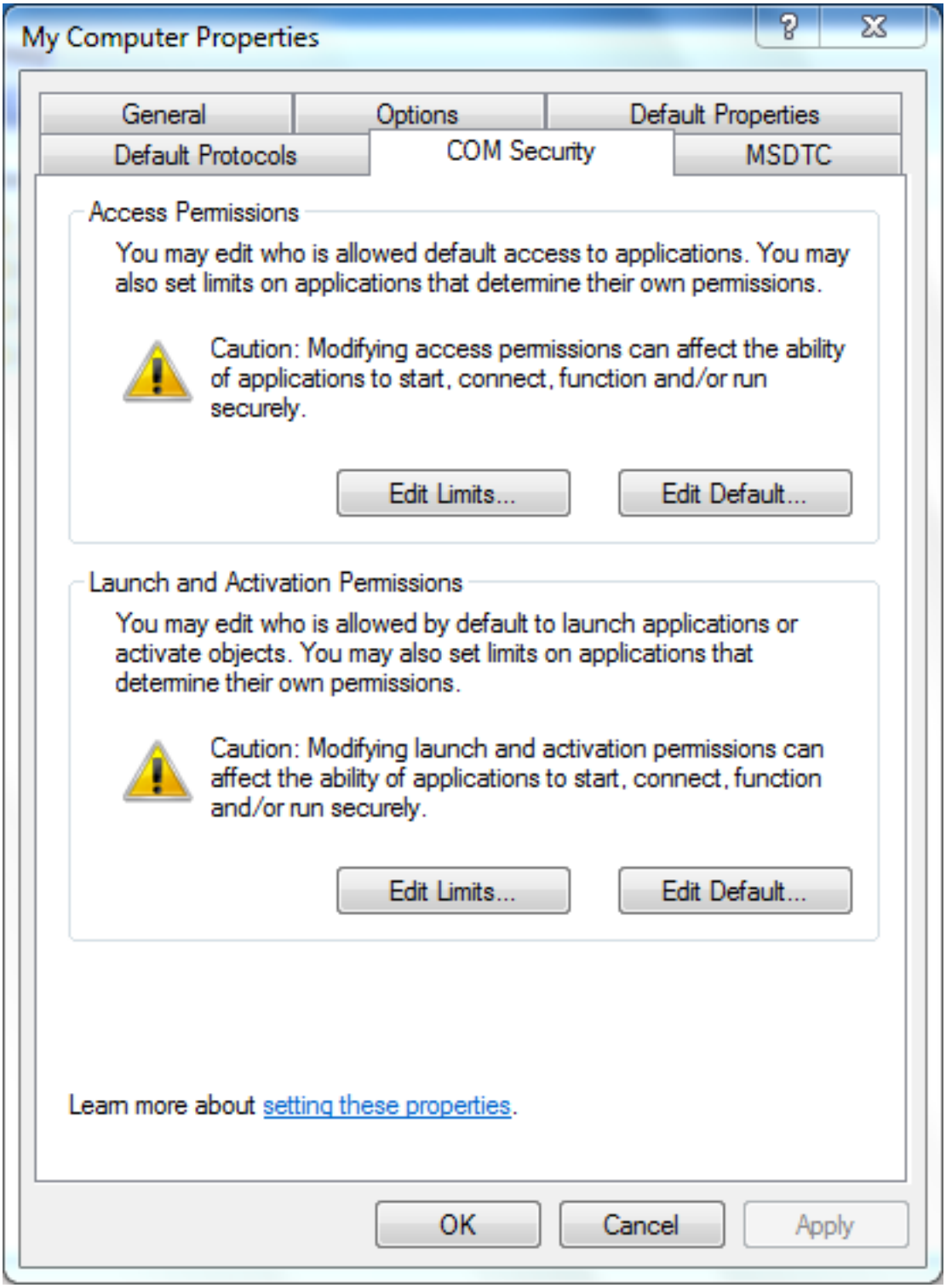
2. Run(**실행**)을 클릭하고 DCOMCNFG**를 입력합니다**.

3. **확인**을 **클릭합니다**.구성 요소 서비스 대화 상자가 나타납니다.



4. 구성 요소 서비스 대화 상자에서 **구성 요소 서비스**를 확장하고 **컴퓨터**를 **확장한** 다음 **내 컴퓨터**를 마우스 오른쪽 단추로 클릭하고 **속성**을 선택합니다.

5. 내 컴퓨터 속성 대화 상자에서 **COM 보안** 탭을 클릭합니다.



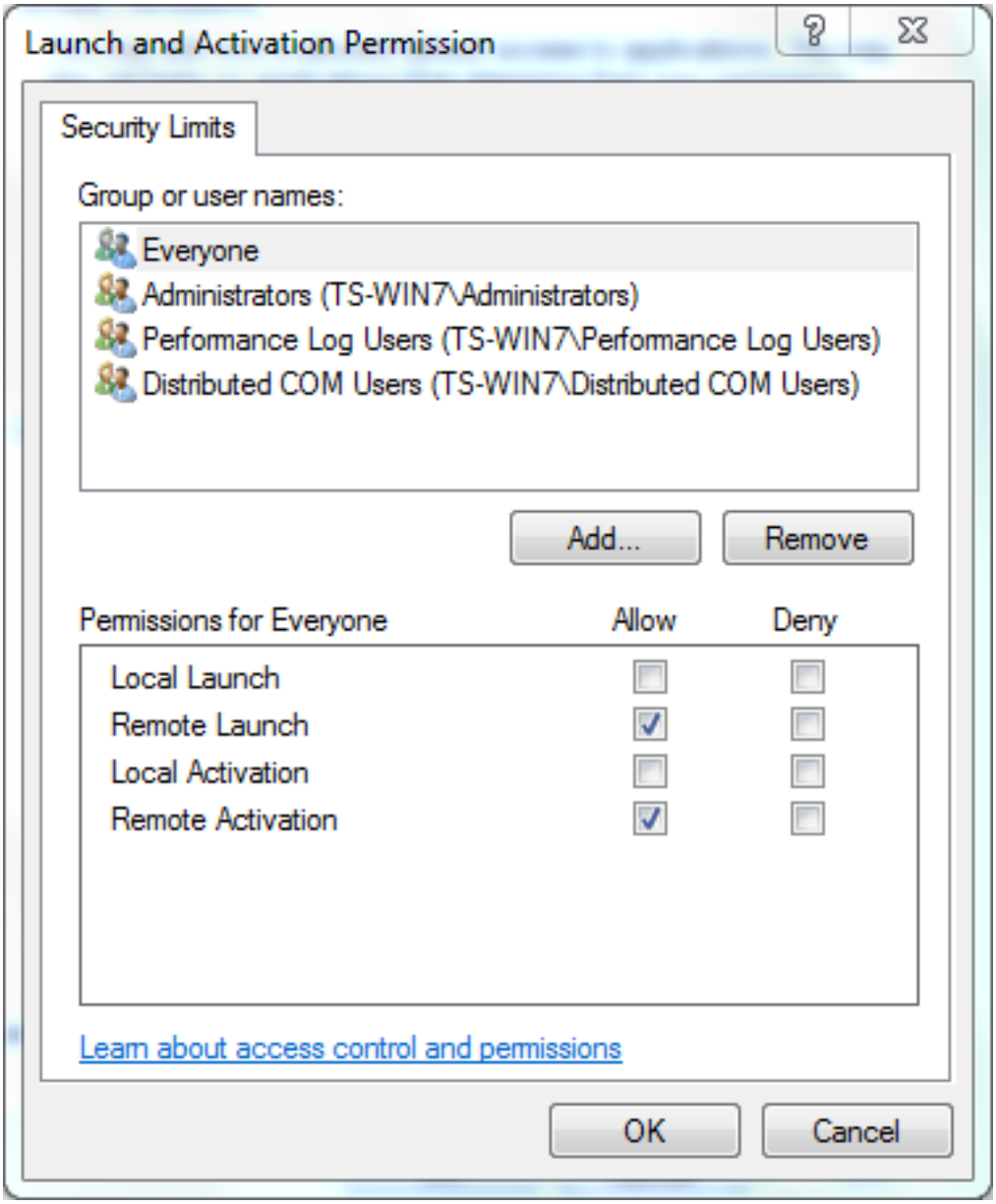
6. Launch and Activation Permissions(시작 및 활성화 권한)에서 Edit Limits(**제한 수정)를** 클릭합니다.

7. 그룹 또는 사용자 이름 목록에 이름이나 그룹이 나타나지 않으면 시작 및 활성화 권한 대화 상자에서 다음 단계를 완료합니다.

   Launch and Activation Permission(시작 및 활성화 권한) 대화 상자에서 Add(추가)를 **클릭합니다**.

   사용자, 컴퓨터 또는 그룹 선택 대화 상자에서 선택할 개체 이름 입력 필드에 사용자 이름과 그룹을 입력한 다음 **확인**을 클릭합니다.

8. Launch and Activation Permission(시작 및 활성화 권한) 대화 상자의 **Group or user names(그룹 또는 사용자 이름)** 섹션에서 사용자 및 그룹을 선택합니다.



9. Permissions for User(사용자에 대한 권한) 아래의 Allow(허용) 열에서 **Remote Launch** and **Remote Activation(원격 시작** 및 **원격 활성화**) 확인란을 선택한 다음 **OK(확인)를 클릭합니다**.**참고:**사용자 이름에는 AD 서버의 사용자 로그인 데이터를 쿼리할 권한이 있어야 합니다.프록시를 통해 사용자와 인증하려면 정규화된 사용자 이름을 입력합니다.기본적으로 에이전트를 설치한 컴퓨터에 로그인하는 데 사용한 계정의 도메인이 Domain(도메인) 필드에 자동으로 채워집니다.사용자가 다른 도메인의 구성원이면 제공된 사용자 자격 증명에 대한 도메인을 업데이트합니다.
10. 문제가 지속되면 도메인 컨트롤러에서 감사 및 보안 로그 관리 정책에 사용자를 추가하려고 시도합니다.사용자를 추가하려면 다음 단계를 완료하십시오.

    그룹 정책 관리 편집기를 **선택합니다**.

    Computer **Configuration(컴퓨터 구성)** > **Windows Settings(Windows 설정)** > **Security Settings(보안 설정)** > **Local Policies(로컬 정책)** > **User Rights Assignment(사용자 권한 할당**

)를 선택합니다.

감사 및 보안 로그 관리를 선택합니다.

사용자를 추가합니다.