UCS Central용 LDAP 인증 컨피그레이션 예

목차

소개

이 문서에서는 Cisco UCS(Unified Computing System) Central에 대한 LDAP(Lightweight Directory Access Protocol) 인증의 샘플 컨피그레이션을 제공합니다. 이 절차에서는 bprocs.com의 예제 도메인인 UCS Central GUI(그래픽 사용자 인터페이스)와 testuser의 예제 사용자 이름을 사용합니다.

UCS Central 소프트웨어 버전 1.0에서는 LDAP만 지원되는 원격 인증 프로토콜입니다. 버전 1.0은 UCS Central 자체에 대한 원격 인증 및 LDAP 컨피그레이션을 매우 제한적으로 지원합니다. 그러나 UCS Central에서 관리하는 UCS Manager 도메인에 대한 모든 옵션을 구성하려면 UCS Central을 사용할 수 있습니다.

UCS Central 원격 인증의 제한 사항은 다음과 같습니다.

- RADIUS 및 TACACS는 지원되지 않습니다.
- 역할 할당에 대한 LDAP 그룹 구성원 매핑 및 여러 도메인 컨트롤러에 대한 LDAP 공급자 그룹은 지원되지 않습니다.
- LDAP는 역할을 전달하기 위해 CiscoAVPair 특성 또는 사용하지 않는 특성만 사용합니다. 전달

된 역할은 UCS Central 로컬 데이터베이스에서 미리 정의된 역할 중 하나입니다.
- 다중 인증 도메인/프로토콜은 지원되지 않습니다.

사전 요구 사항

요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- UCS Central이 구축되었습니다.
- Microsoft Active Directory가 구축되었습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- UCS Central 버전 1.0
- Microsoft Active Directory

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.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

정보 수집

이 섹션에서는 구성을 시작하기 전에 수집해야 하는 정보를 요약합니다.

참고: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 내용을 확인하십시오.

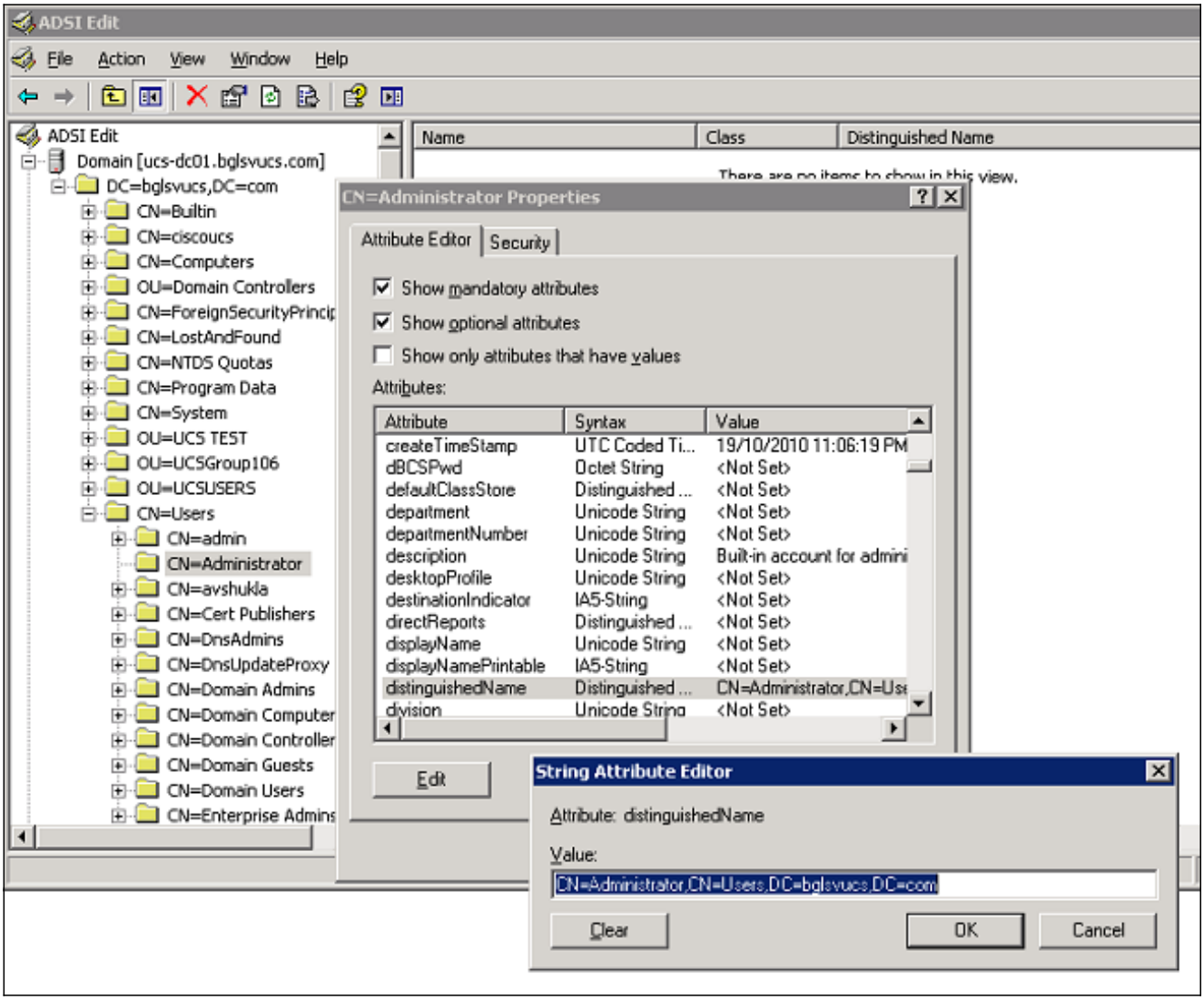
바인드 사용자 세부 정보

바인드 사용자는 도메인에 대한 읽기 액세스 권한이 있는 도메인의 모든 LDAP 사용자가 될 수 있습니다. LDAP 컨피그레이션에는 바인드 사용자가 필요합니다. UCS Central은 바인드 사용자의 사용자 이름과 비밀번호를 사용하여 사용자 인증을 위해 AD(Active Directory)에 연결하고 쿼리합니다. 이 예에서는 Administrator 계정을 바인드 사용자로 사용합니다.

이 절차에서는 LDAP 관리자가 DN을 찾기 위해 ADSI(Active Directory Service Interfaces) 편집기를 사용하는 방법에 대해 설명합니다.

1. ADSI 편집기를 엽니다.
2. 바인드 사용자를 찾습니다. 사용자가 AD와 동일한 경로에 있습니다.
3. 사용자를 마우스 오른쪽 단추로 누르고 등록 정보를 **선택합니다**.
4. 속성 대화 상자에서 distinguishedName을 두 번 **클릭합니다**.
5. Value 필드에서 DN을 복사합니다

.



6. 모든 창을 닫으려면 **취소**를 클릭합니다.

바인드 사용자의 비밀번호를 얻으려면 AD 관리자에게 문의하십시오.

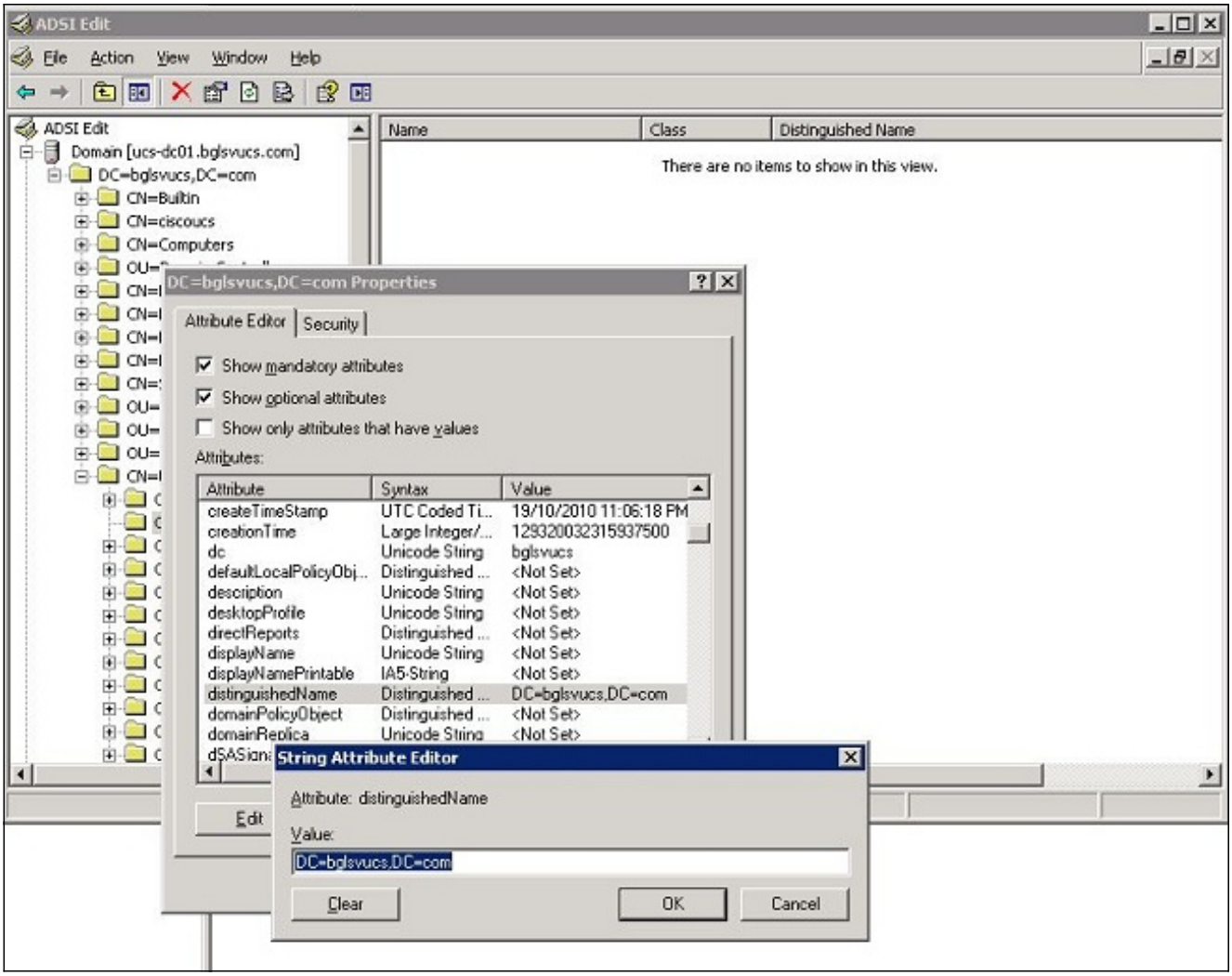
기본 DN 세부 정보

Base DN은 사용자 및 사용자 세부 정보 검색이 시작되는 OU(조직 구성 단위) 또는 컨테이너의 DN입니다. UCS 또는 UCS Central의 AD에서 생성한 OU의 DN을 사용할 수 있습니다. 그러나 도메인 루트 자체에 DN을 사용하는 것이 더 간단할 수 있습니다.

이 절차에서는 LDAP 관리자가 기본 DN을 찾기 위해 ADSI 편집기를 사용하는 방법에 대해 설명합니다.

1. ADSI 편집기를 엽니다.
2. 기본 DN으로 사용할 OU 또는 컨테이너를 찾습니다.
3. OU 또는 컨테이너를 마우스 오른쪽 버튼으로 클릭하고 **속성**을 선택합니다.
4. 속성 대화 상자에서 distinguishedName을 두 번 **클릭합니다**.
5. 값 필드에서 DN을 복사하고 필요한 기타 세부 사항을 확인합니다

.



6. 모든 창을 닫으려면 **취소**를 클릭합니다.

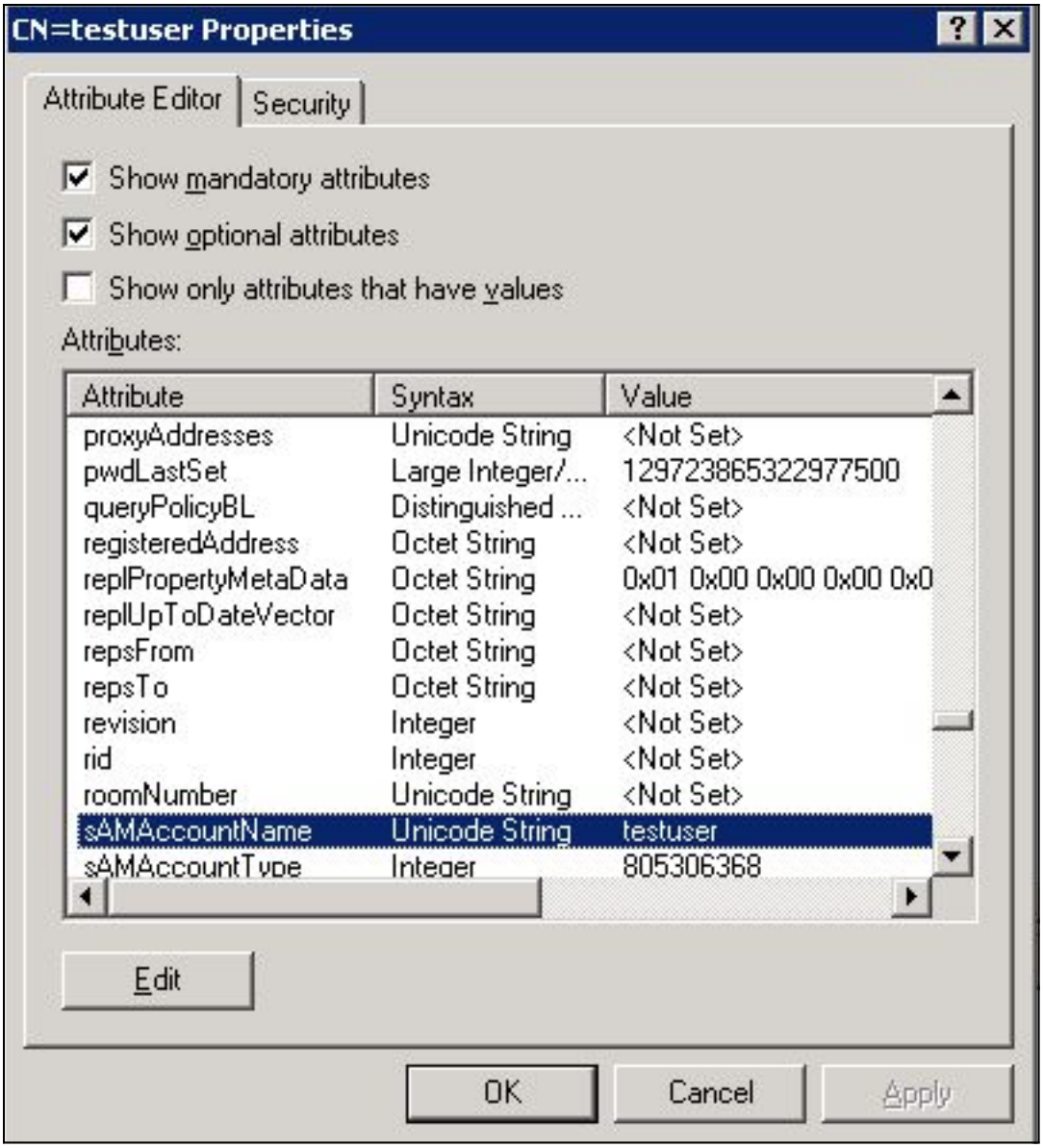
공급자 세부 정보

공급자는 UCS Central에서 LDAP 인증 및 권한 부여에서 주요 역할을 수행합니다. 공급자는 UCS Central에서 사용자를 검색 및 인증하고 역할 정보와 같은 사용자 세부 정보를 얻기 위해 쿼리하는 AD 서버 중 하나입니다. Provider AD 서버의 호스트 이름 또는 IP 주소를 수집해야 합니다.

필터 속성

필터 필드 또는 속성은 AD 데이터베이스를 검색하는 데 사용됩니다. 로그인 시 입력한 사용자 ID가 AD로 다시 전달되고 필터와 비교됩니다.

sAMAccountName=$userid를 필터 값으로 사용할 수 있습니다. sAMAccountName은 AD의 속성이며 AD 사용자 ID와 동일한 값을 가지며, UCS Central GUI에 로그인하는 데 사용됩니다.



특성 추가 및 구성

이 섹션에서는 LDAP 컨피그레이션을 시작하기 전에 CiscoAVPair 특성을 추가하고(필요한 경우) CiscoAVPair 특성 또는 기타 사전 정의된 특성을 업데이트하는 데 필요한 정보를 요약합니다.

특성 필드는 AD 특성(사용자 등록 정보 아래)을 지정하며, 이는 사용자에게 할당할 역할을 다시 전달합니다. UCS Central 소프트웨어의 릴리스 1.0a에서 이 역할을 전달하기 위해 AD의 사용자 지정 특성 CiscoAVPair 또는 기타 사용되지 않는 특성을 통합할 수 있습니다.

참고: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 내용을 확인하십시오.

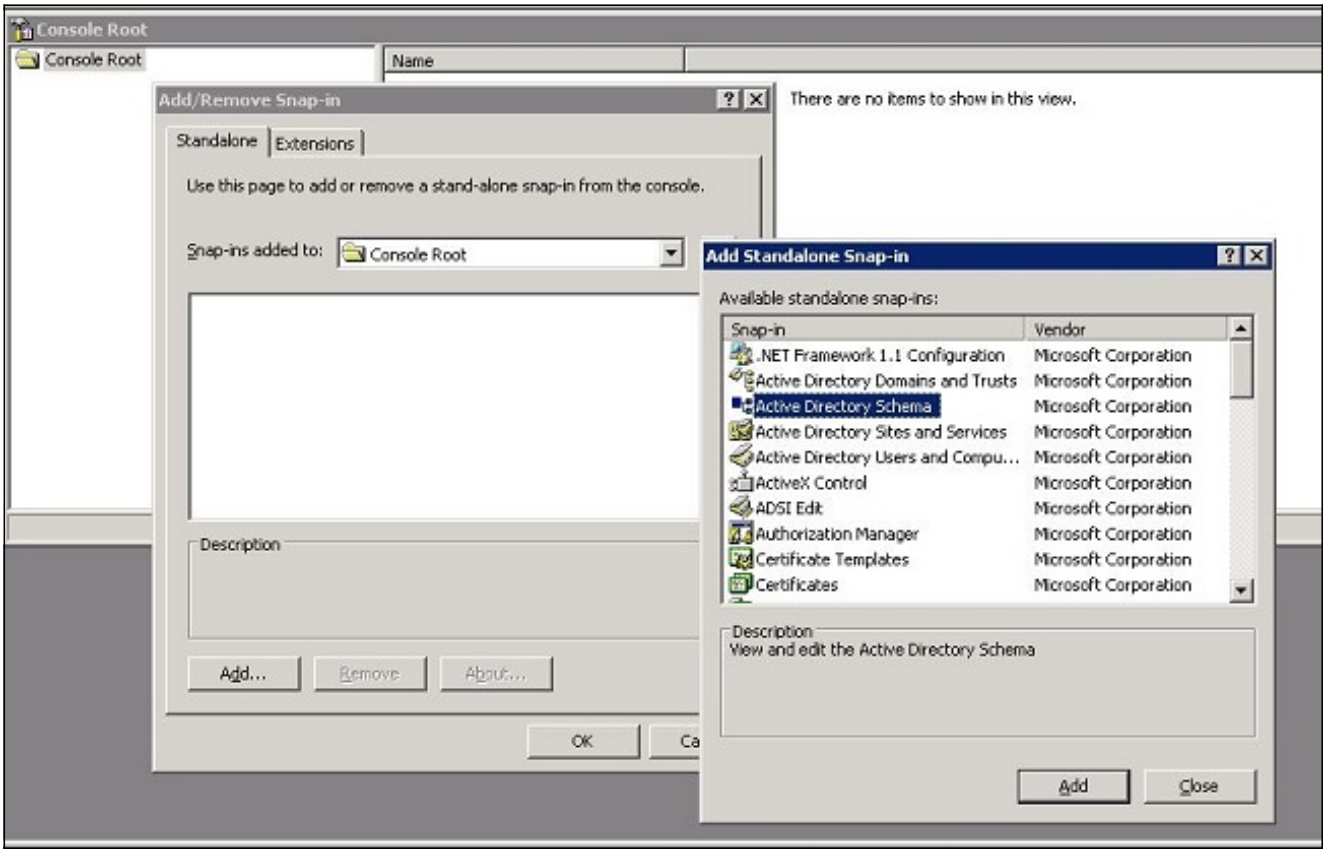
CiscoAVPair 특성 추가

도메인에 새 특성을 추가하려면 도메인의 스키마를 확장하고 클래스(이 예에서는 user)에 특성을 추가합니다.

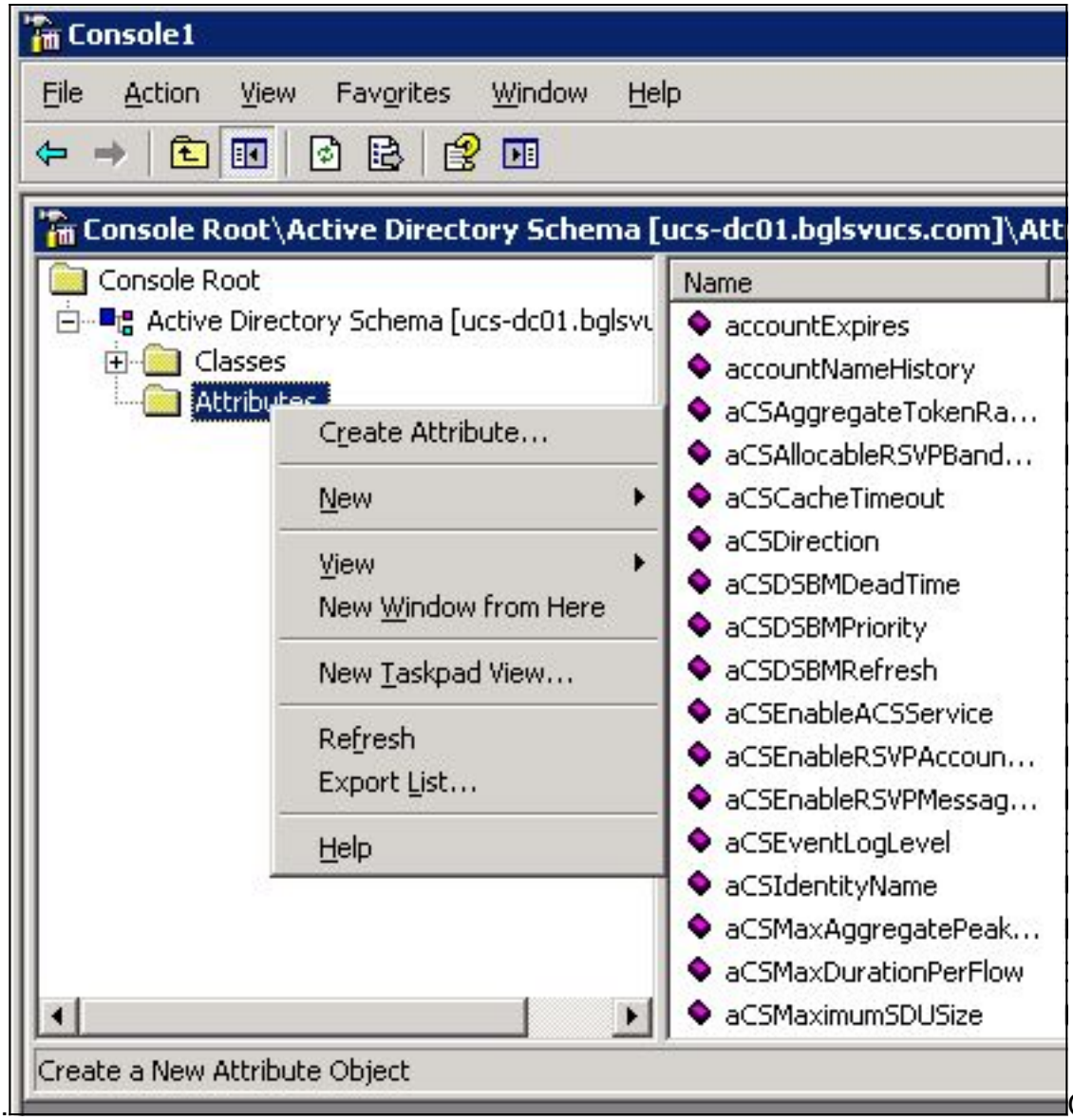
이 절차에서는 Windows AD 서버에서 스키마를 확장하고 CiscoAVPair 특성을 추가하는 방법에 대해 설명합니다.

1. AD 서버에 로그인합니다.
2. **시작 > 실행**을 클릭하고 mmc를 입력한 다음 **Enter를** 눌러 빈 MMC(Microsoft Management Console) 콘솔을 엽니다.
3. MMC에서 **파일 >** 스냅인 **추가/제거 > 추가**를 **클릭합니다**.
4. Add Standalone Snap-in(독립형 스냅인 추가) 대화 상자에서 **Active Directory 스키마**를 선택하고 **Add(추가)**를 클릭합니다

.

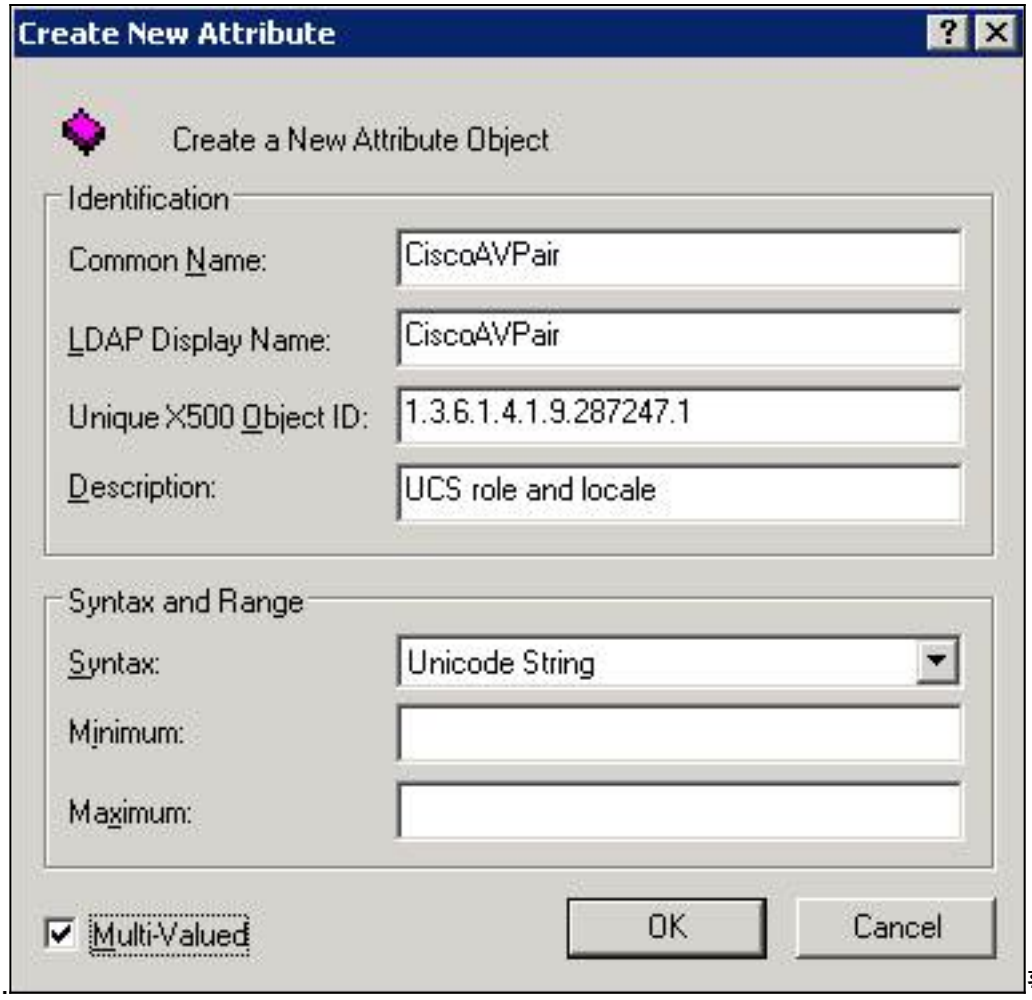


5. MMC에서 **Active Directory 스키마**를 확장하고 **속성**을 마우스 오른쪽 단추로 클릭한 다음 속성 **만들기를 선택합니다**



. Create New Attribute 대화 상자가 나타납니다

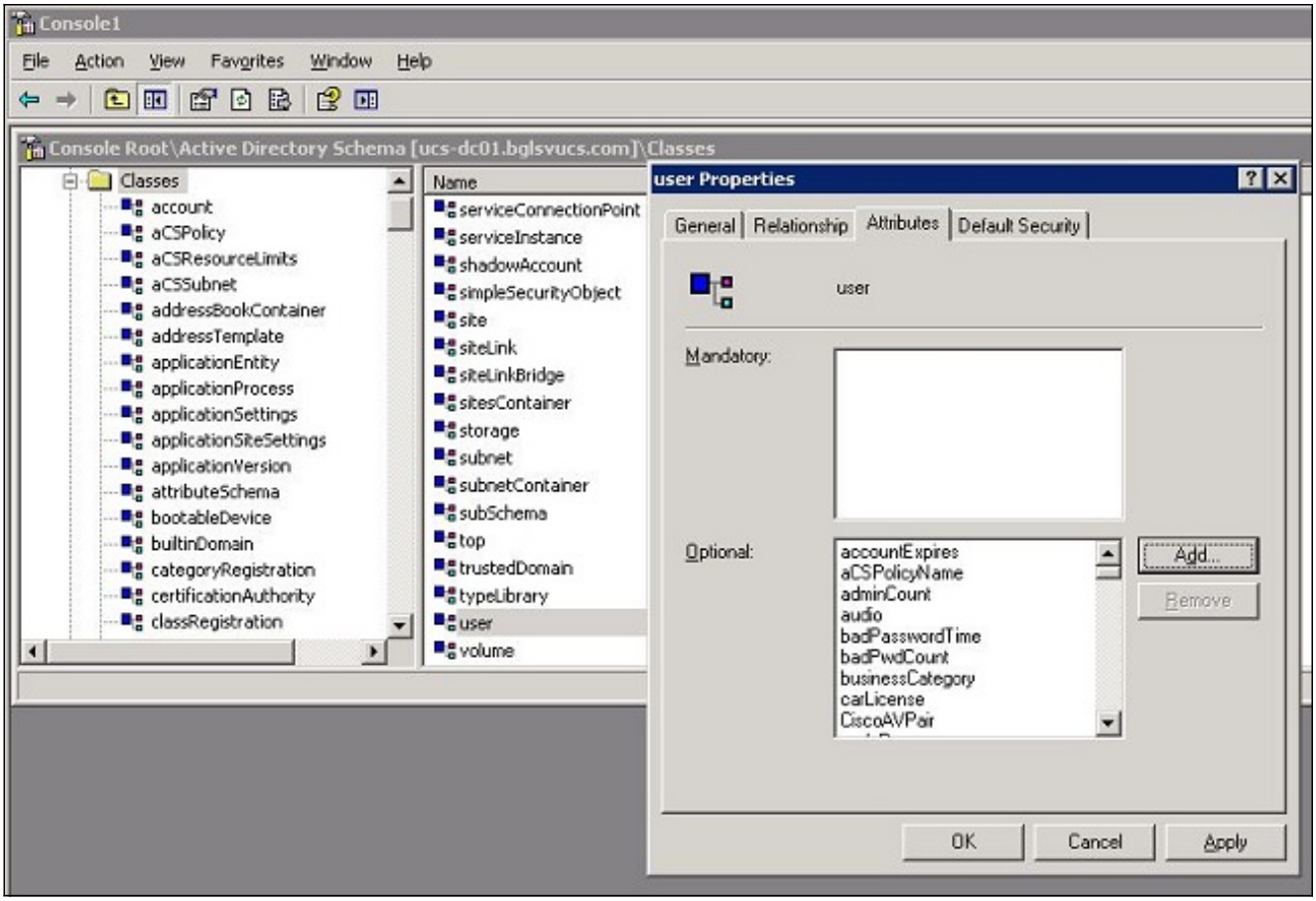
6. 원격 인증 서비스에서 CiscoAVPair라는 특성을 만듭니다.Common Name 및 LDAP Display Name 필드에 **CiscoAVPair를 입력합니다**.Unique 500 Object ID 필드에 **1.3.6.1.4.1.9.287247.1을 입력합니다**.Description(설명) 필드에 **UCS 역할 및 로캘을 입력합니다**.Syntax 필드의 드롭다운 목록에서 Unicode String을 선택합니다



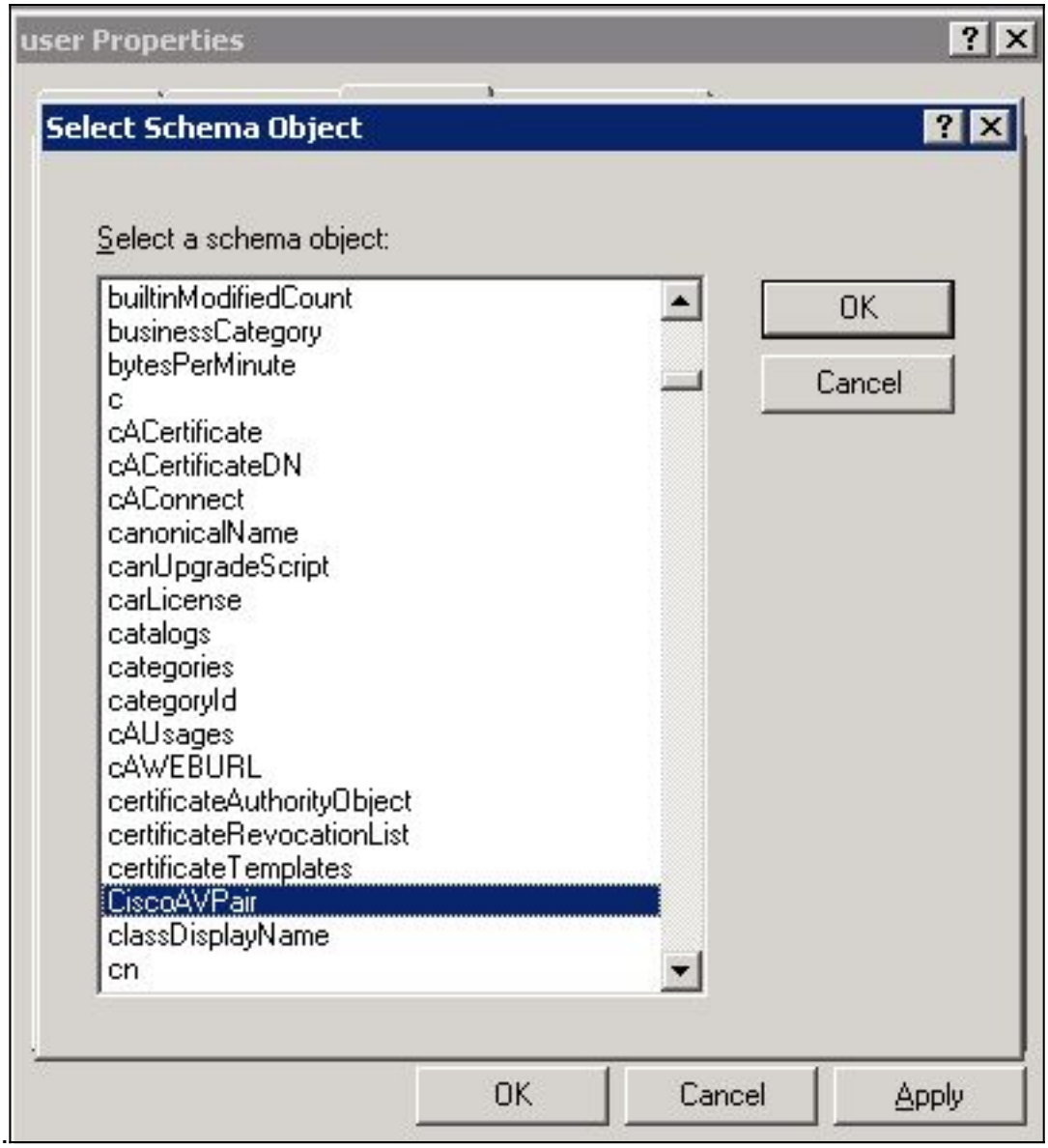
. **확인을** 클릭하여 특성을 저장하고 대화 상자를 닫습니다.스키마에 특성이 추가되면 해당 특성은 매핑되거나 사용자 클래스에 포함되어야 합니다. 이렇게 하면 사용자 속성을 편집하고 역할을 전달할 값을 지정할 수 있습니다.

7. AD 스키마 확장에 사용되는 동일한 MMC에서 **클래스**를 확장하고 **사용자**를 마우스 오른쪽 단추로 클릭한 다음 **속성을 선택합니다**.
8. 사용자 속성 대화 상자에서 속성 탭을 클릭하고 **추가**를 **클릭합니다**

.

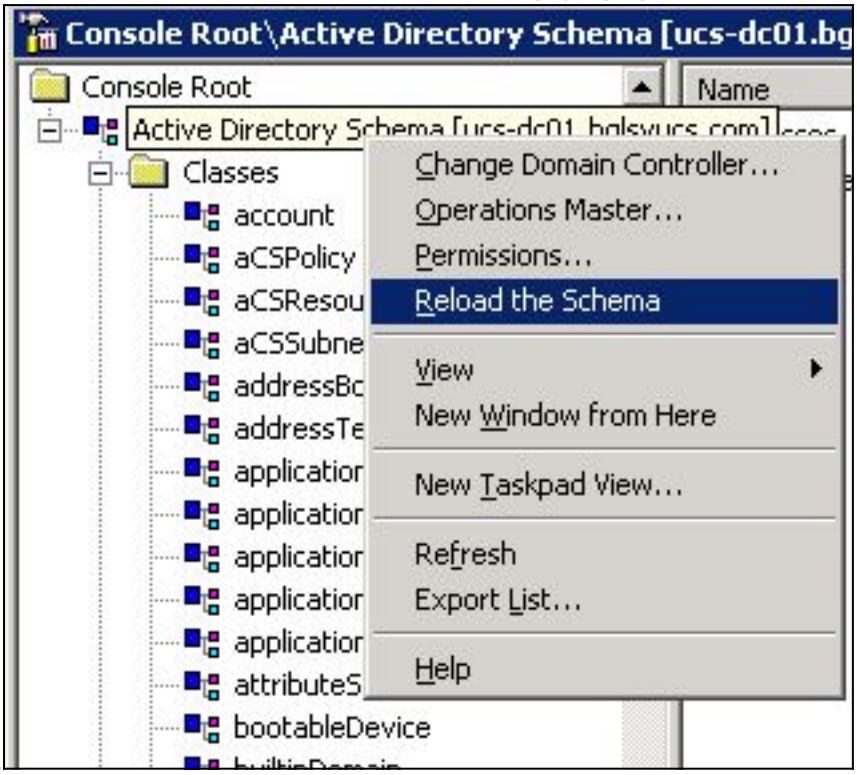


9. Select Schema Object(스키마 개체 선택) 대화 상자에서 **CiscoAVPair**를 클릭하고 **OK**(확인)를



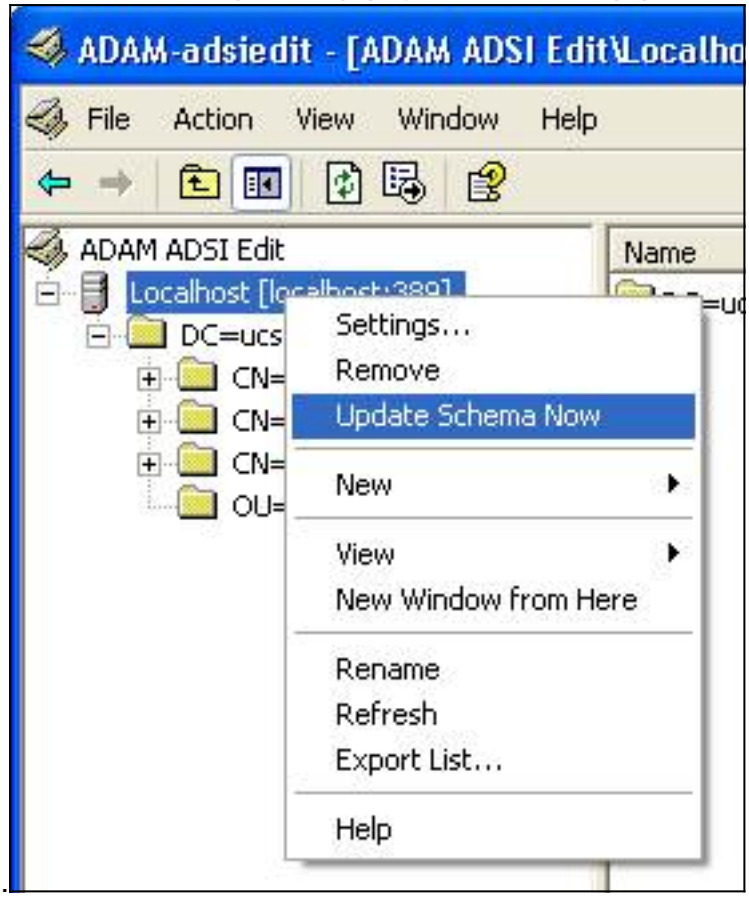
클릭합니다.

10. 사용자 속성 대화 상자에서 적용을 **클릭합니다**.
11. **Active Directory 스키마**를 마우스 오른쪽 단추로 클릭하고 **스키마 다시 로드를** 선택하여 새



변경 사항을 포함합니다.

12. 필요한 경우 ADSI 편집기를 사용하여 스키마를 업데이트합니다. Localhost를 마우스 오른쪽 **단추로** 누르고 **지금 스키마 갱신을 선택합니다**

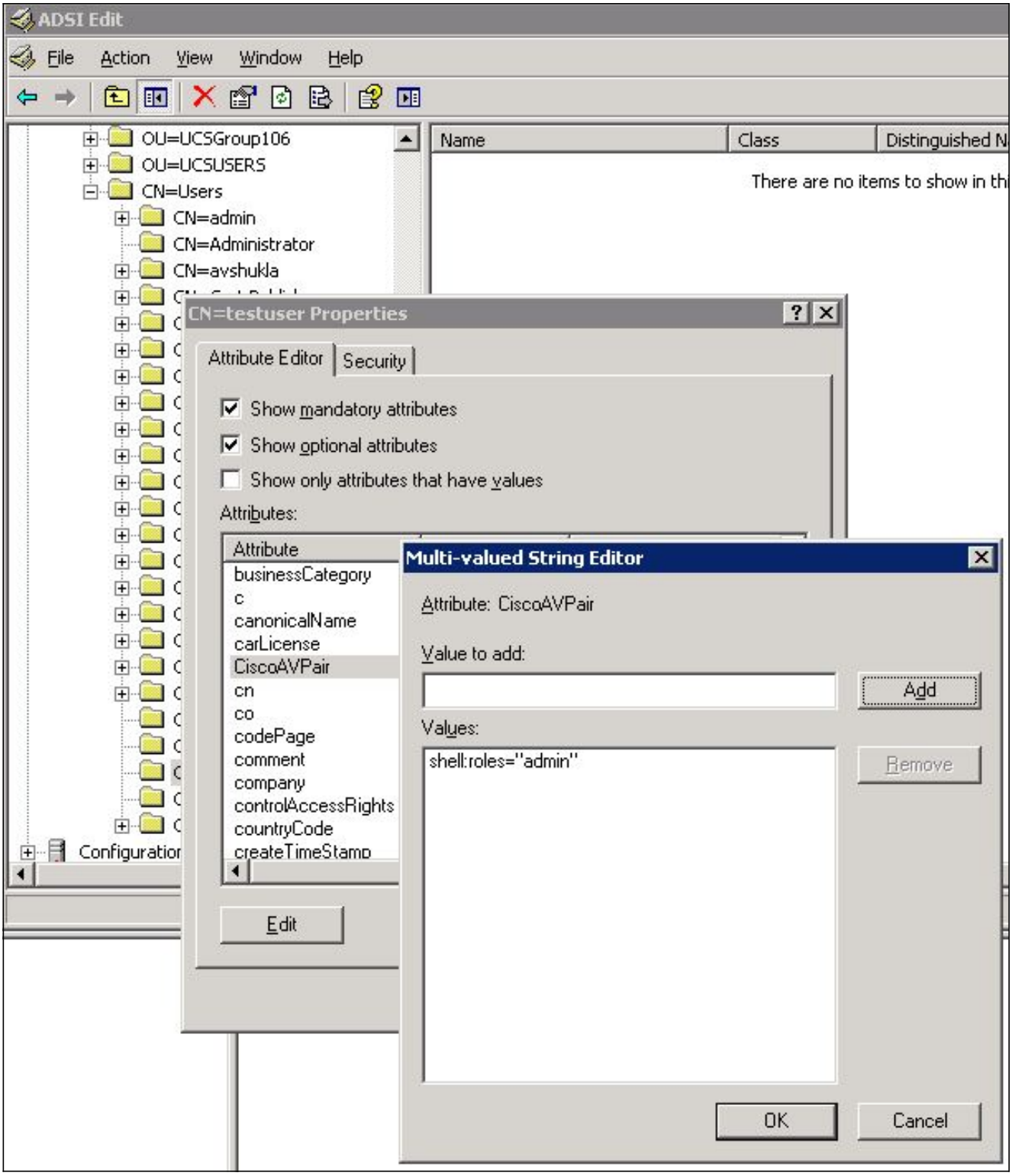


CiscoAVPair 특성 업데이트

이 절차에서는 CiscoAVPair 특성을 업데이트하는 방법에 대해 설명합니다. 구문은 `shell:roles="<role>"`.

1. ADSI Edit(ADSI 수정) 대화 상자에서 UCS Central에 액세스해야 하는 사용자를 찾습니다.
2. 사용자를 마우스 오른쪽 단추로 누르고 등록 정보를 **선택합니다**.
3. 속성 대화 상자에서 속성 **편집기** 탭을 클릭하고 **CiscoAVPair**를 클릭한 다음 **편집을 클릭합니다**.
4. 다중값 문자열 편집기 대화 상자의 값 필드에 **shell:roles="admin"** 값을 입력하고 **확인**을 클릭합니다

.



5. 확인을 클릭하여 변경 사항을 저장하고 속성 대화 상자를 닫습니다.

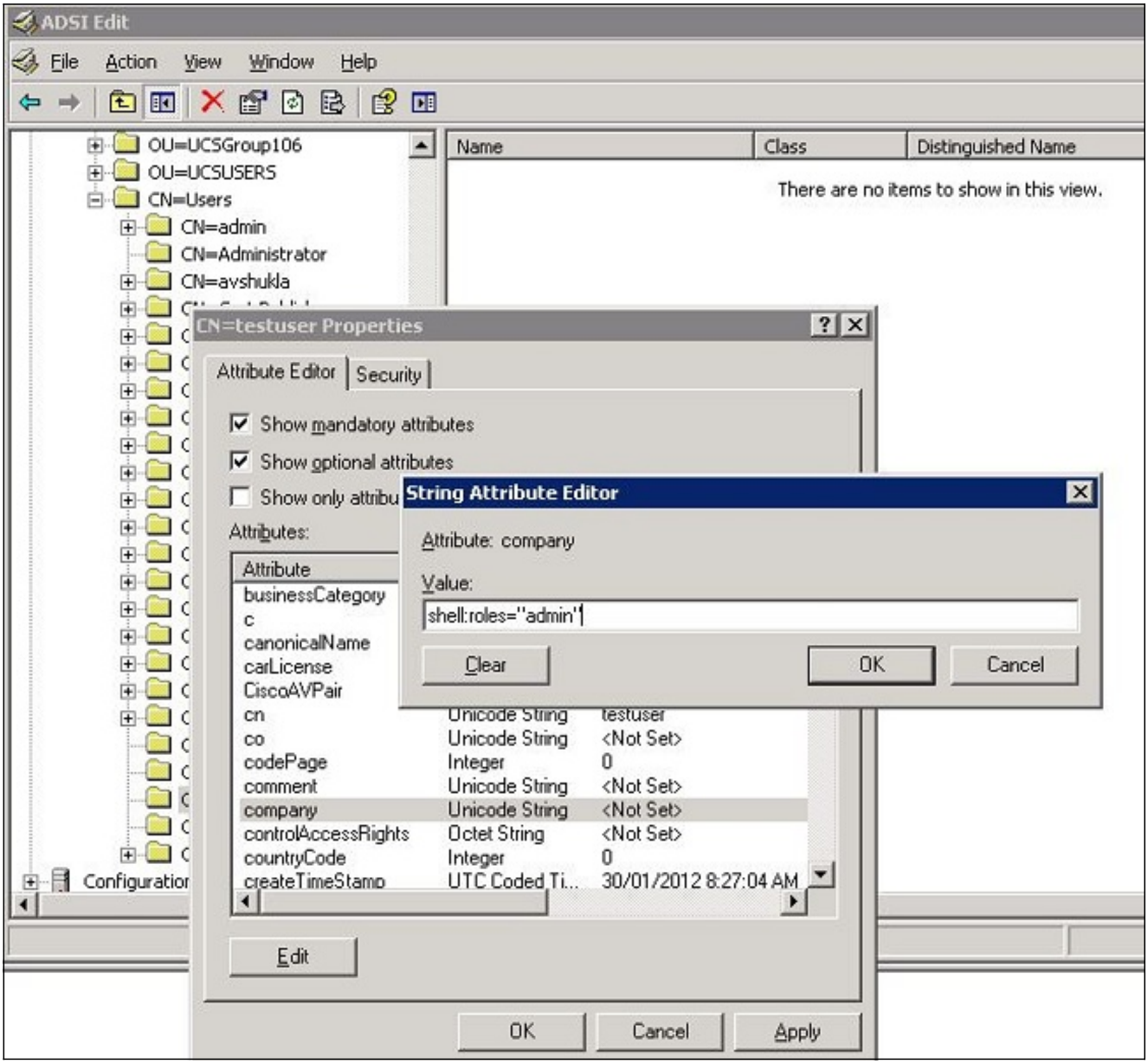
사전 정의 속성 업데이트

이 절차에서는 사전 정의된 특성을 업데이트하는 방법에 대해 설명합니다. 여기서 역할은 UCS Central에서 사전 정의된 사용자 역할 중 하나입니다. 이 예에서는 *회사*를 사용하여 역할을 전달합니다. 구문은 `shell:roles="<role>"`.

1. ADSI Edit(ADSI 수정) 대화 상자에서 UCS Central에 액세스해야 하는 사용자를 찾습니다.
2. 사용자를 마우스 오른쪽 단추로 누르고 등록 정보를 **선택합니다**.
3. 속성 대화 상자에서 속성 **편집기** 탭을 클릭하고 **회사**를 클릭한 다음 **편집을 클릭합니다**.
4. String Attribute Editor(문자열 속성 편집기) 대화 상자의 Value(값) 필드에 **shell:roles="admin"**

값을 입력하고 **OK(확인)**를 클릭합니다

.



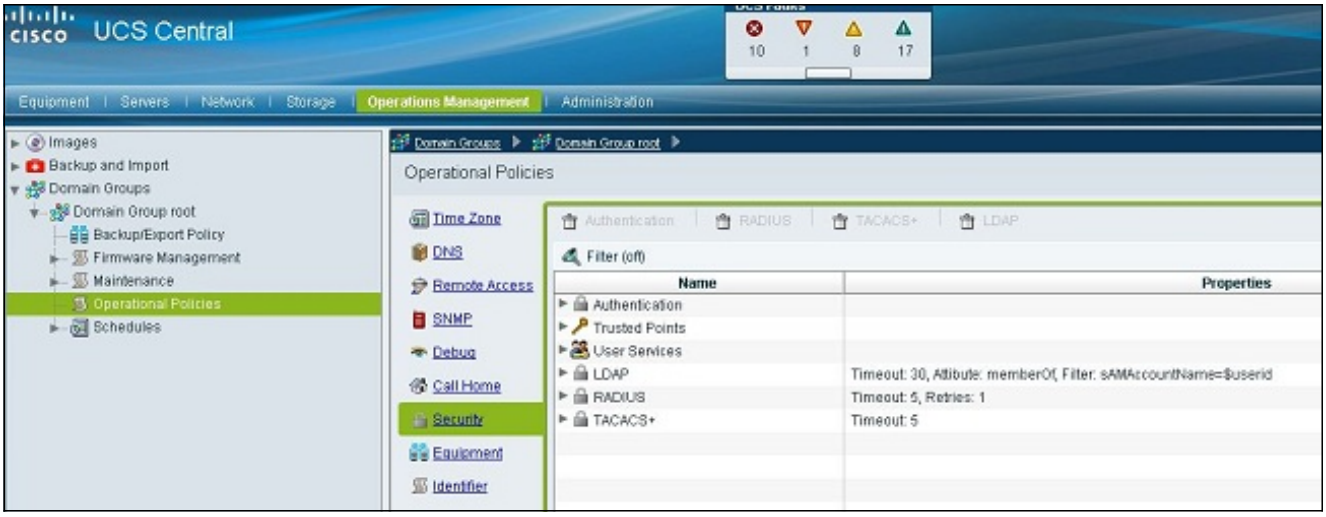
5. 확인을 클릭하여 변경 사항을 저장하고 속성 대화 상자를 닫습니다.

UCS Central에서 LDAP 인증 구성

UCS Central의 LDAP 컨피그레이션은 Operations Management(운영 관리)에서 완료됩니다.

1. 로컬 계정으로 UCS Central에 로그인합니다.
2. Operations **Management(운영 관리)**를 클릭하고 **Domain Groups(도메인 그룹)**를 확장한 다음 **Operational Policies(운영 정책) > Security(보안)**를 클릭합니다

.

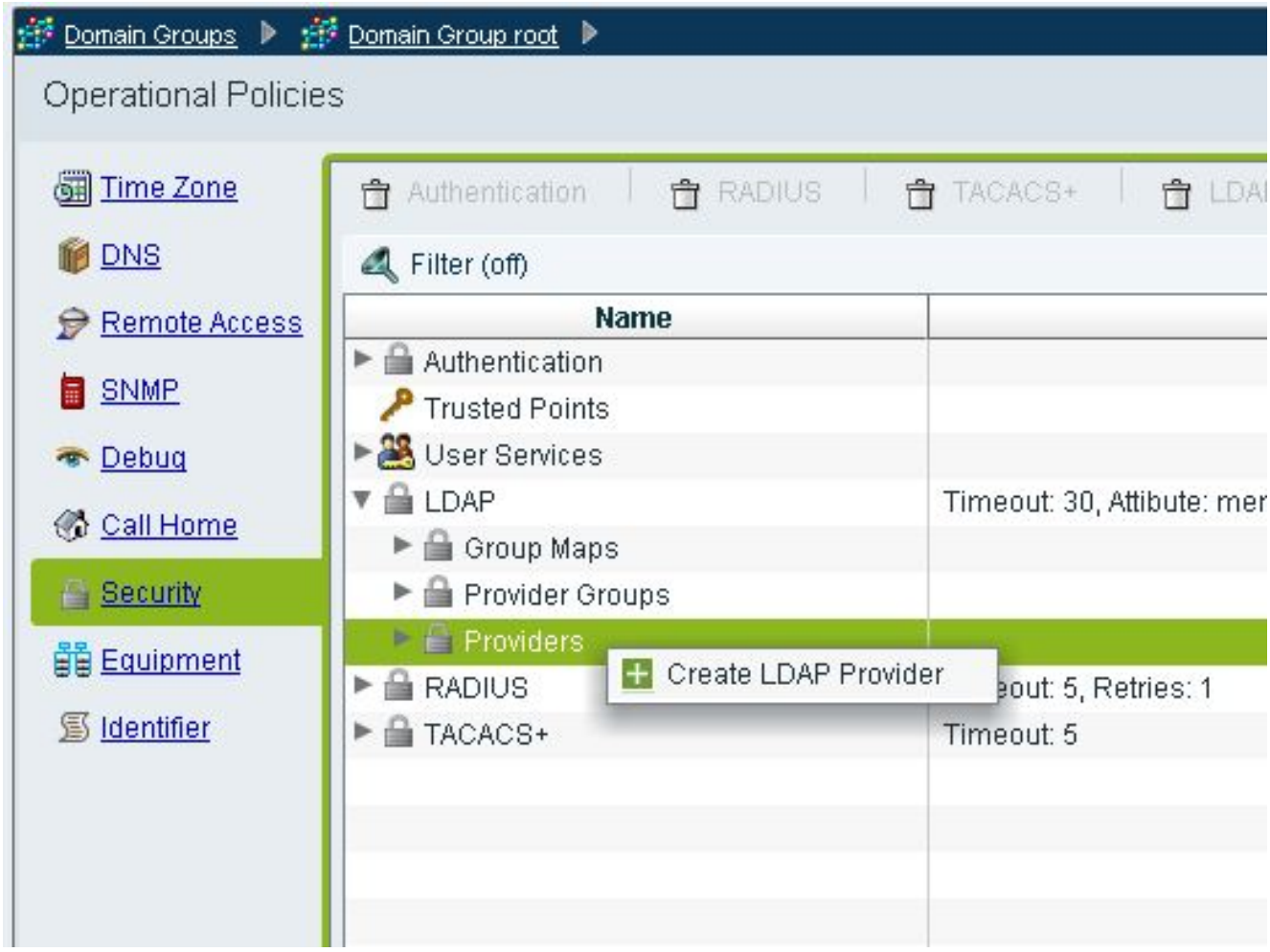


3. LDAP 인증을 구성하려면 다음 단계를 수행합니다.LDAP 제공자를 구성합니다.LDAP 제공자 그룹을 구성합니다(릴리스 1.0a에서는 제공되지 않음).기본 인증 규칙을 변경합니다.

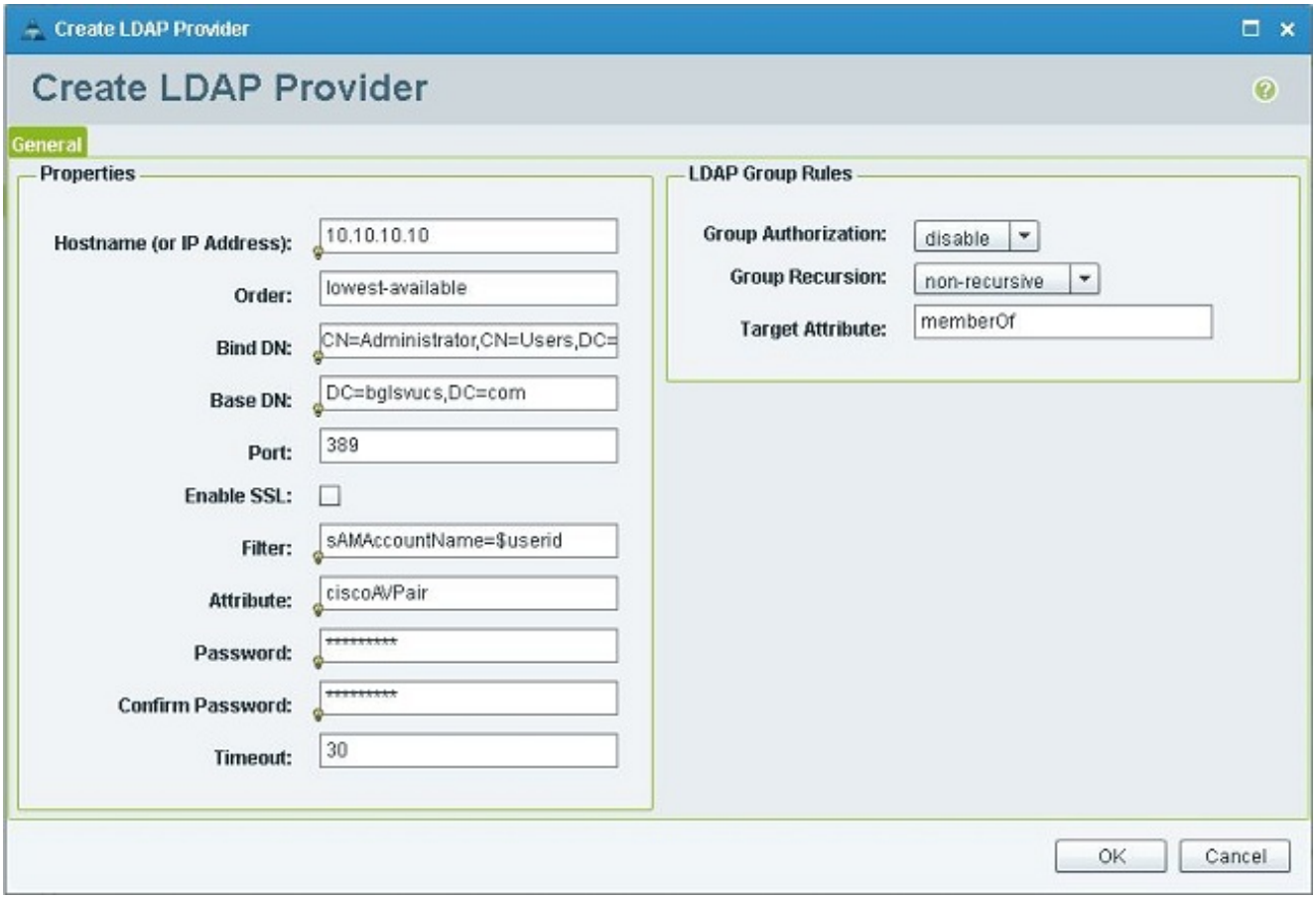
LDAP 제공자 구성

1. LDAP**를** 클릭하고 Providers(**제공자**)를 마우스 오른쪽 버튼으로 클릭한 다음 Create LDAP **Provider(LDAP 제공자 생성)를 선택합니다**

.



2. Create LDAP Provider(LDAP 제공자 생성) 대화 상자에서 이전에 수집한 세부 정보를 추가합니다.공급자의 호스트 이름 또는 IP바인드 DN기본 DN필터특성(CiscoAVPair 또는 회사와 같은 사전 정의된 특성비밀번호(바인드 DN에 사용된 사용자의 비밀번호
)



3. OK(**확인**)를 클릭하여 컨피그레이션을 저장하고 대화 상자를 닫습니다.

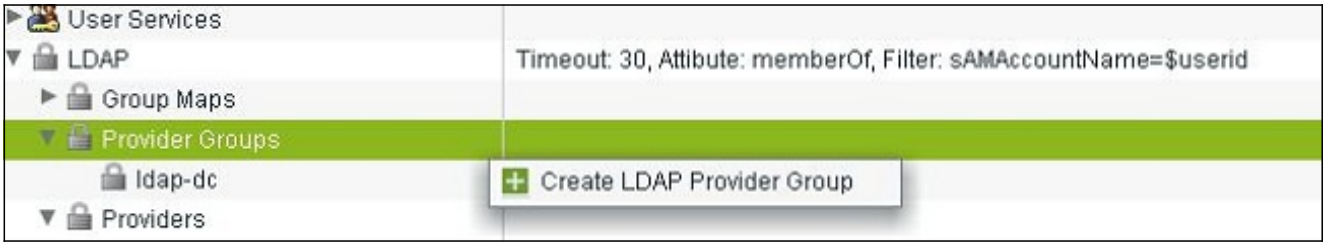
참고: 이 화면에서 다른 값을 수정할 필요가 없습니다. 이 릴리스의 UCS Central 인증에는 LDAP 그룹 규칙이 지원되지 않습니다.

LDAP 제공자 그룹 구성

참고: Release 1.0a에서는 공급자 그룹이 지원되지 않습니다. 이 절차에서는 나중에 컨피그레이션에서 사용할 더미 공급자 그룹을 구성하는 방법에 대해 설명합니다.

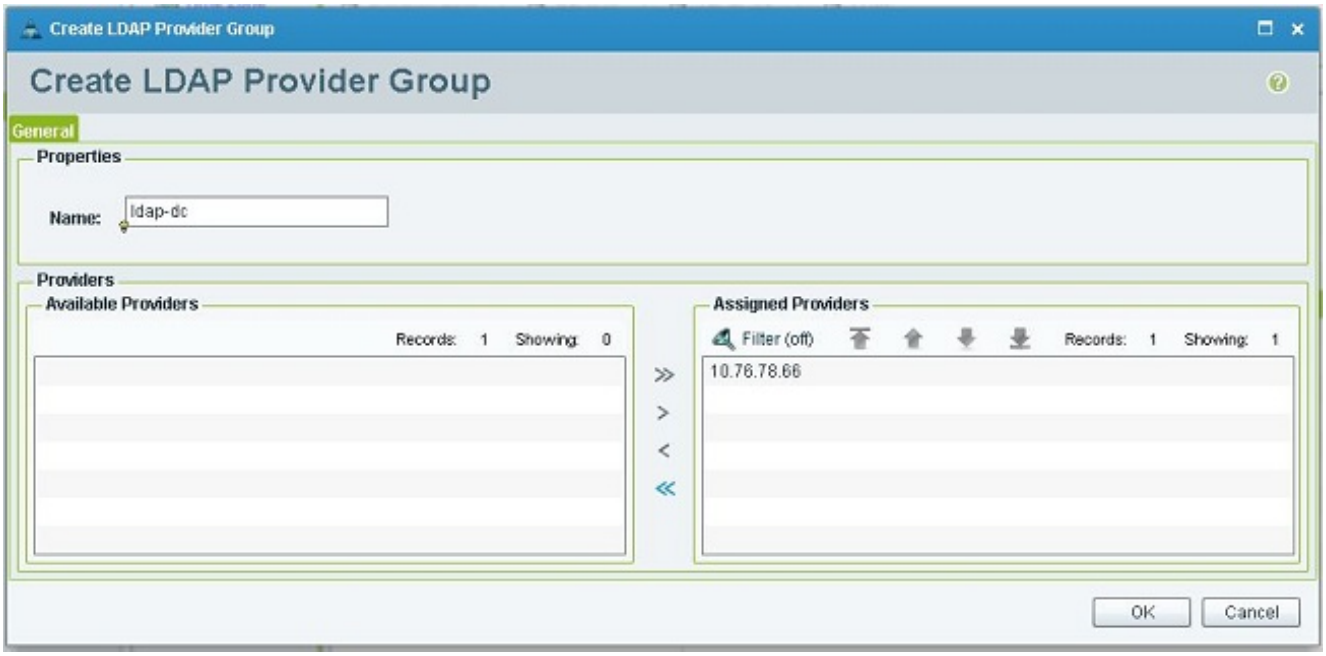
1. LDAP**를** 클릭하고 Provider **Group**(사업자 그룹)을 마우스 오른쪽 버튼으로 클릭한 다음 Create LDAP **Provider Group(LDAP 제공자 그룹 생성)을 선택합니다**

.



2. Create LDAP Provider Group(LDAP 제공자 그룹 생성) 대화 상자의 Name(이름) 필드에 그룹 이름을 입력합니다.
3. 왼쪽의 사용 가능한 공급자 목록에서 공급자를 선택하고 보다 큼 기호(**>**)를 클릭하여 해당 공급자를 오른쪽의 할당된 공급자로 이동합니다

.



4. 변경 사항을 저장하고 화면을 닫으려면 **확인**을 클릭합니다.

기본 인증 규칙 변경

릴리스 1.0a는 UCS Manager에서와 같이 여러 인증 도메인을 지원하지 않습니다. 이 문제를 해결하려면 기본 인증 규칙을 수정해야 합니다.

기본 인증에는 기본 로그인 또는 콘솔 로그인에 대한 인증을 수정할 수 있는 옵션이 있습니다. 여러 도메인이 지원되지 않으므로 로컬 계정 또는 LDAP 어카운트를 사용할 수 있지만 둘 다 사용할 수는 없습니다. 로컬 또는 LDAP를 인증 소스로 사용하려면 Realm 값을 변경합니다.

1. Authentication(**인증**)을 클릭하고 Native Authentication(**기본 인증)**을 마우스 오른쪽 버튼으로 클릭한 다음 Properties(속성)를 **선택합니다**.
2. 기본 인증, 콘솔 인증 또는 둘 다를 원하는지 결정합니다. GUI 및 CLI(Command-Line Interface)에 기본 인증을 사용합니다. VM(가상 머신) 커널 기반 KVM(가상 머신) 보기에 콘솔 인증을 사용합니다.
3. Realm 드롭다운 목록에서 ldap를 선택합니다. Realm 값은 로컬 또는 LDAP가 인증 소스인지 여부를 결정합니다

.

4. 페이지를 닫으려면 **확인**을 클릭합니다.
5. Policies(정책) 페이지에서 필요한 경우 **Save(저장)**를 클릭하여 변경 사항을 저장합니다.

참고: LDAP 인증이 올바르게 작동하는지 확인할 때까지 현재 세션에서 로그아웃하거나 콘솔 인증을 수정하지 마십시오. 콘솔 인증은 이전 컨피그레이션으로 되돌리는 방법을 제공합니다. 확인 섹션을 참조하십시오.

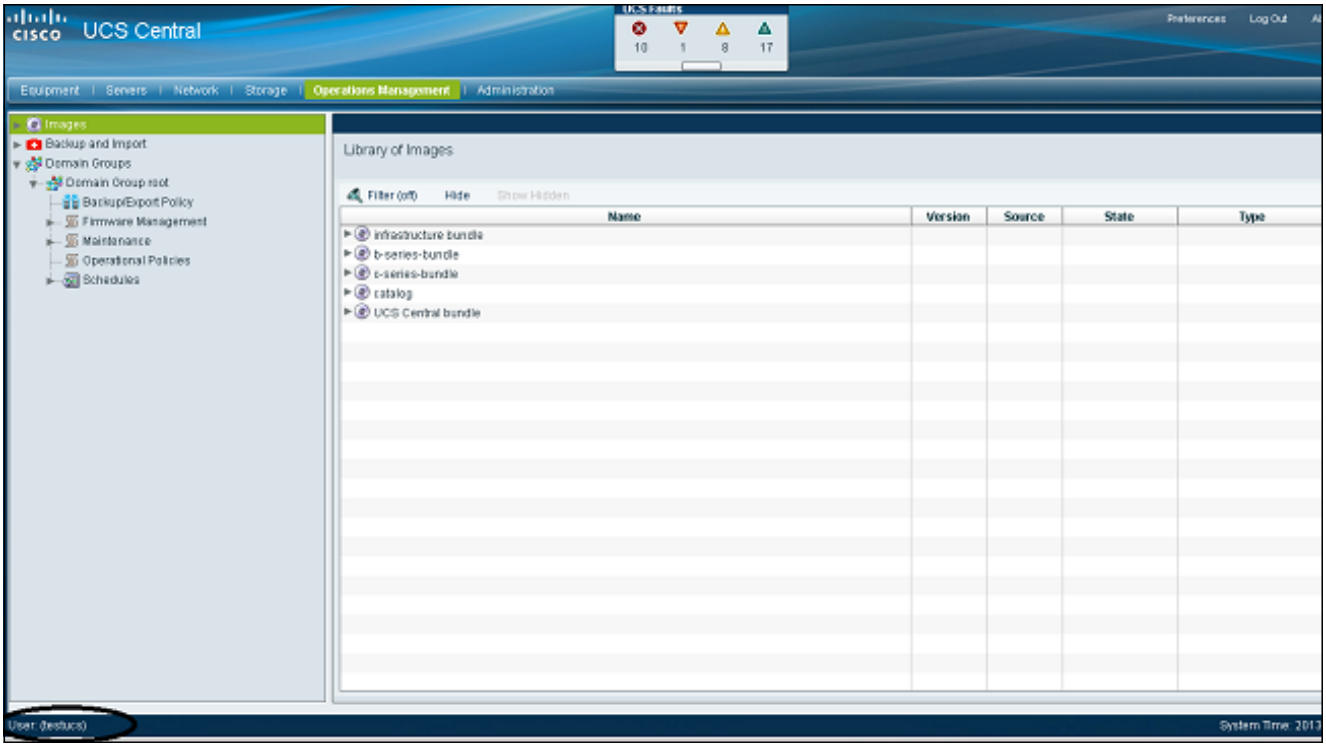
다음을 확인합니다.

이 절차에서는 LDAP 인증을 테스트하는 방법을 설명합니다.

1. UCS Central에서 새 세션을 열고 사용자 이름과 비밀번호를 입력합니다. 사용자 이름 앞에 도메인 또는 문자를 포함할 필요는 없습니다. 이 예에서는 testucs를 도메인의 사용자로 사용합니다.

2. UCS Central 대시보드가 표시되면 LDAP 인증이 성공합니다. 사용자가 페이지 하단에 표시됩니다

.



문제 해결

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

관련 정보

- 기술 지원 및 문서 – Cisco Systems