Active Directory Tier Modeling Uygulanması

Bu makalede on prem domain ortamlarında mutlaka kullanılması gereken bir yapıyı anlatıyor olacağım. Microsoft best practice uygularılarında önerilen Tier modeling yapısını on prem damoin ortamına adepte edeceğiz.

Active directory Tier Modeling yapısında kendi kullanıcı hesabınız hariç 3 adet data hesap oluşturacağız.

Bunlar;

T0: Service Administratos (Domain Admins, Enteprise Admins) yetkileri olup, ortamımızda bulunan Domain Controller üzerinden işlem yapma ve erişim yetkisi olacaktır.

T1: Data Administrators (Server Admins) ortamımızda bulunan sunuculara erişim hakkı olacaktır.

T2: Workstation Administrator (Workstation Admins) ortamızda bulunan kullanıcı bilgisayarına erişim hakkı olacaktır. Kısacası clientlara.

Yapılandırılacak olan konfigürasyonumuzda toplamda 4 adet hesabımız olacaktır. Hesap isimlerini yapılandırırken ben kendime uygun algoritma kullanacağım. Siz kendi yapınıza göre konfigürasyon yapabilirsiniz.

Benim örneğimde

ural.tekin → sadece kendi bilgisayarımda sıradan domain user olarak ullanılacak hesabım.

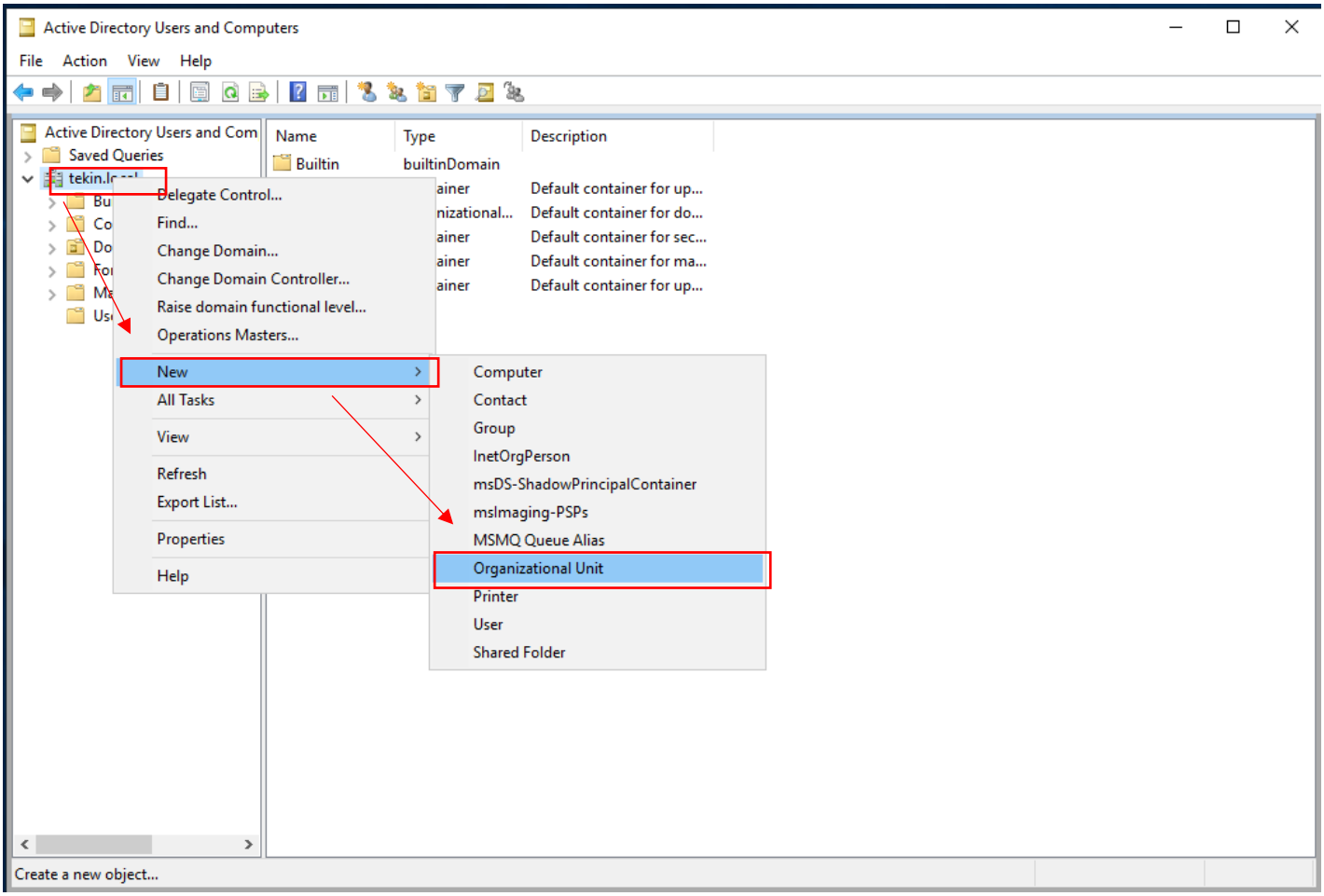
ural.tekindc → T0 kullanıcı seviyesi, on prem yapımdaki Domain controller üzerinde işlem yapabilmek için ve sadece dc makinemde admin yetkilerine sahip olacak hesabım. Bu kullanıcım için AD kullanıcı ayarlarında domain controller dan başka bir sunucuya bağlanmamsı için ayar yapacağım.

ural.tekinsrv → T1 kullanıcı seviyesi, ortamımda bulunan DC hariç diğer sunucular erişiminde ve yapılandırmasında kullanacağım hesabım Domain users yetkisi olacak olup, GPO kuralı ile ortamımdaki sunuculara local admin yapacağım.

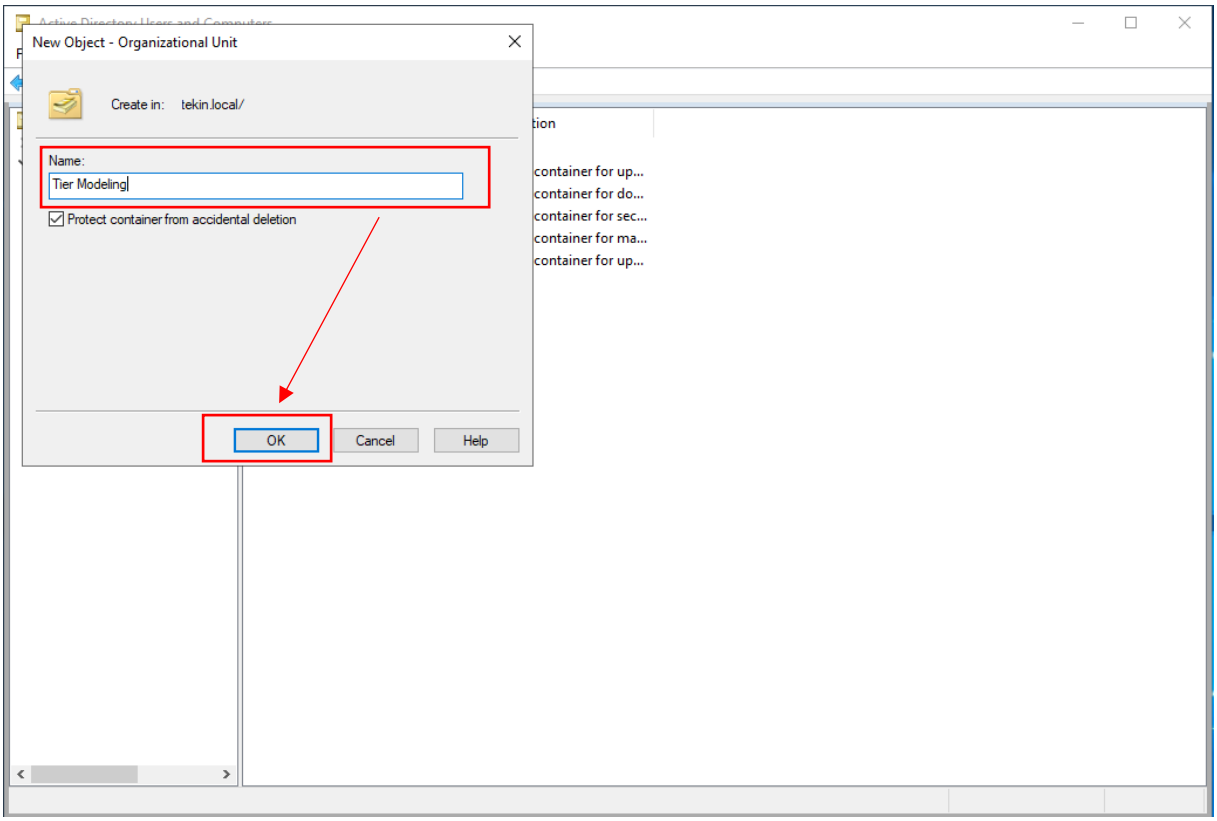
ural.tekinclt → T2 kullanıcı seviyesi, ortamımda bulunan kullanıcıların kullandıkları bilgisayarlara erişim ve ilgili kurulumları tamamlamak amacıyla

kullanacağım kullanıcım. Kullanıcı bilgisayarlarından tüm işlemleri program kurulumu yazıcı vb…. işlemler için sadece bu kullanıcı mı kullanacağım.

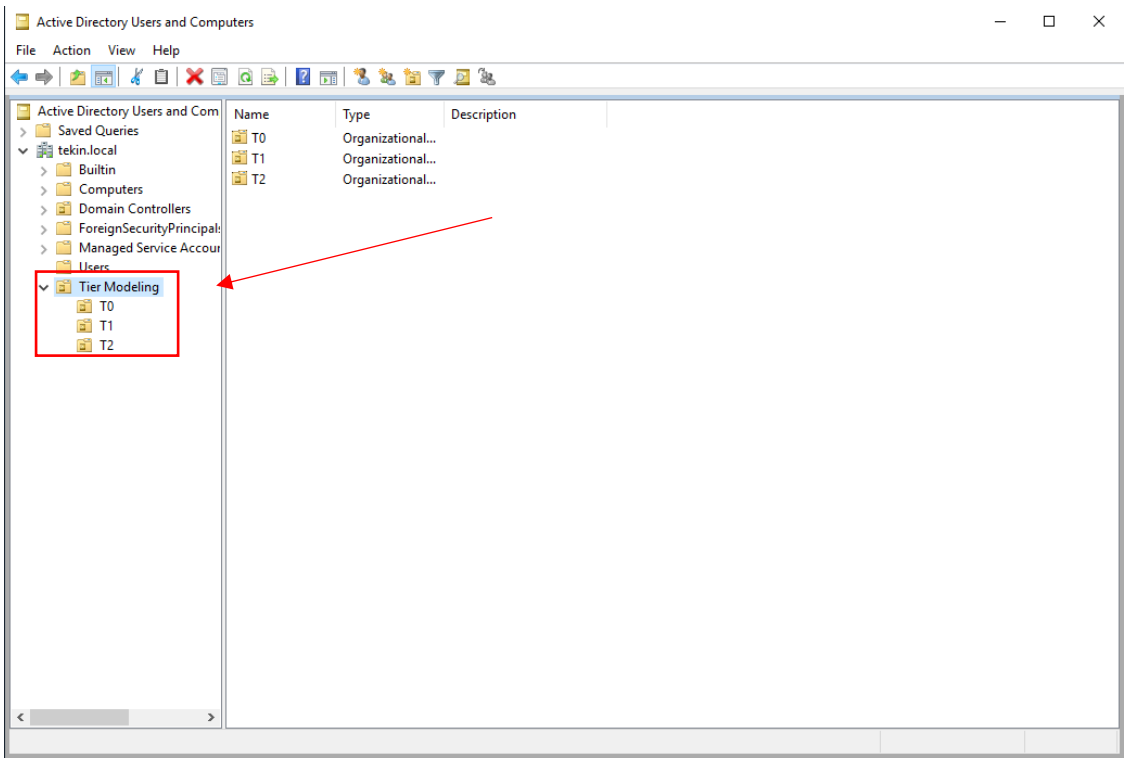
İlk olarak Domain controller sunucumdan Active Directory and Users konsolunu açıyorum. Karşıma gelen menüden **“Tier Modeling”** adında bir Organizational Unit oluşturacağım. Bunun için domaine geliyorum sağ tuş **“New”** ve **“Organizational Unit”** tıklıyorum.



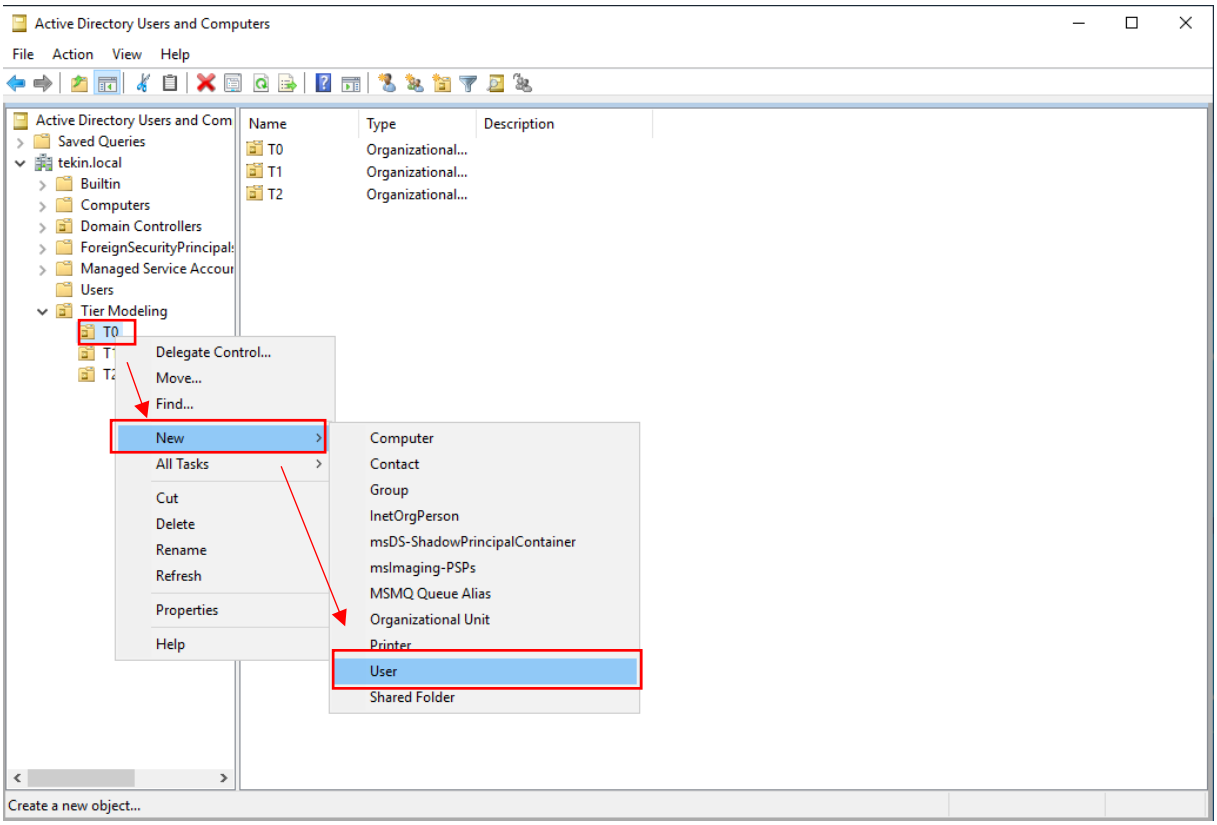
Sonraki adımda karşıma gelen ekrana “Tier Modeling” ismini veriyorum ve okey diyorum.



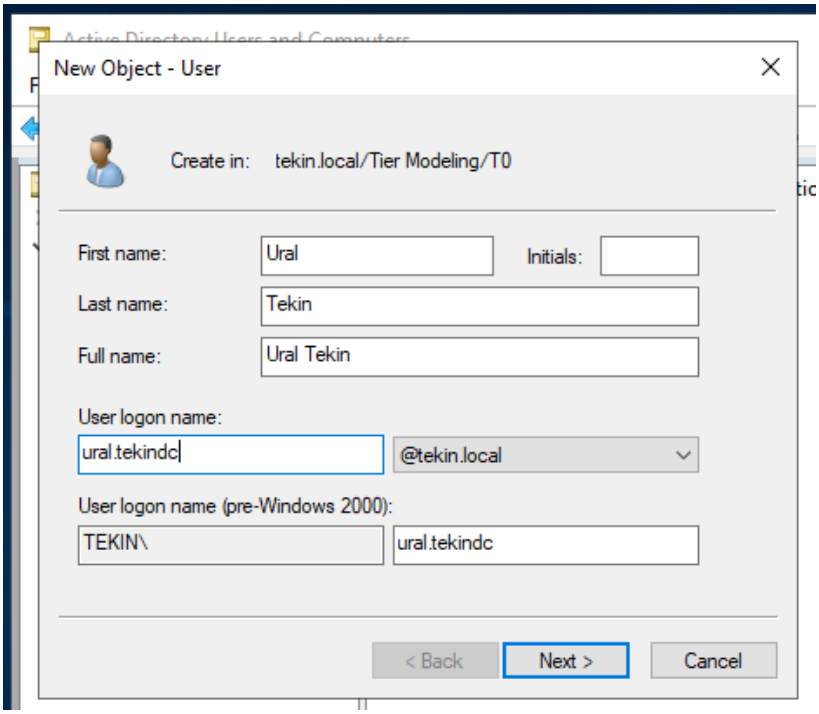
Ve yine aynı yöntemle bu sefer “Tier Modeling” OU sekmesine gelip altında T0, T1 ve T2 isimli organizational Unit leri oluşturuyorum.



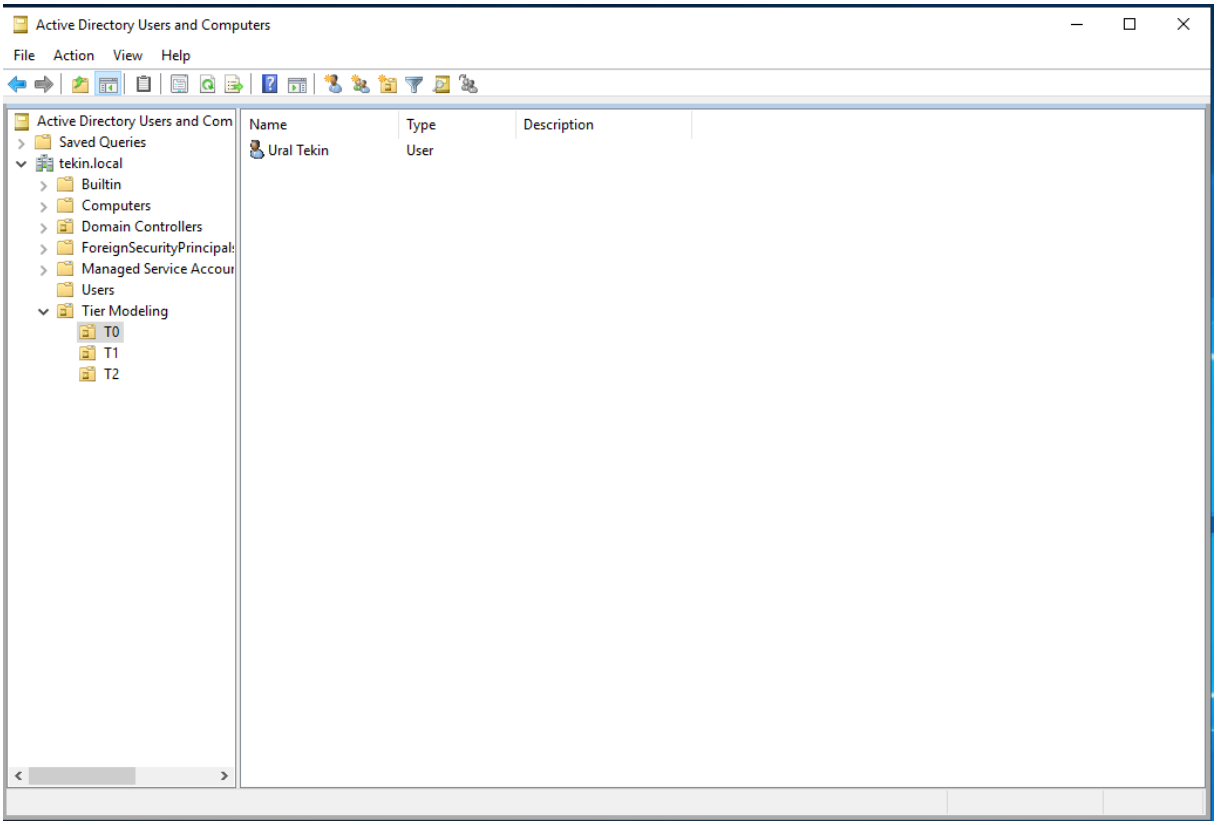
Gerekli olan OU ları oluşturduktan sonra **T0** ou üzerinde sadece Domain Contoller sunucum üzerine erişim yetkisi olacak yukarıda örneğini verdiğim kullanıcımı oluşturuyorum.



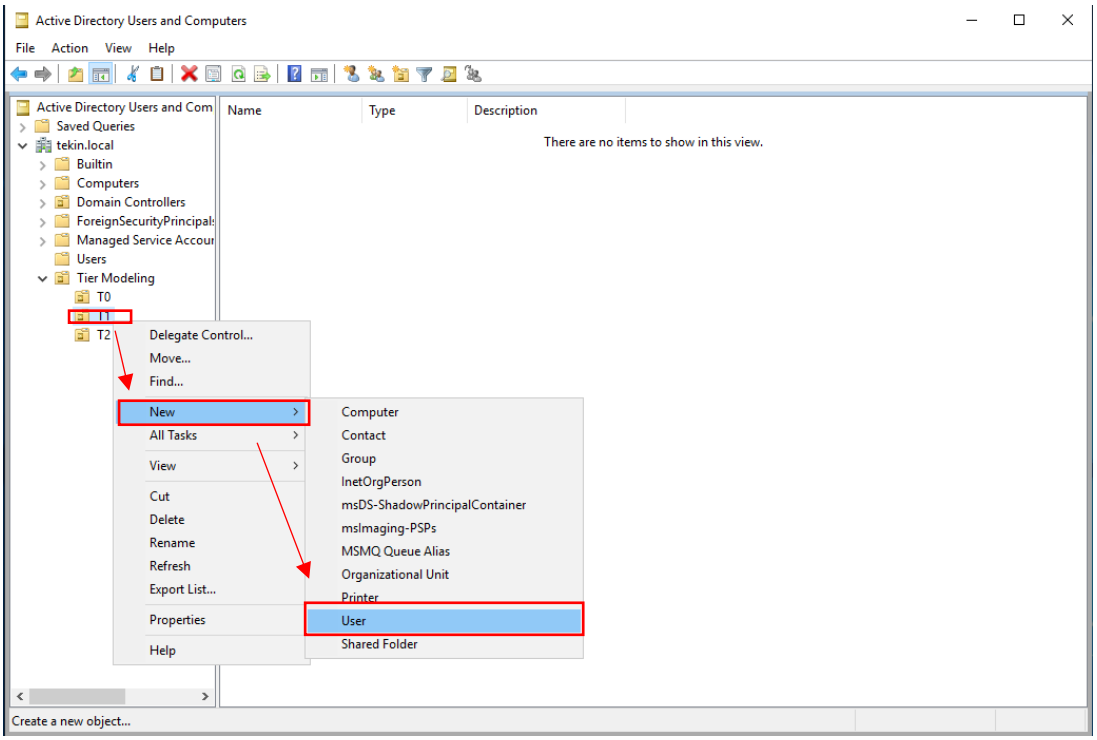
Karşıma çıkan menüden ilgili alanları doldurup **“Next”** diyerek kullanıcımı oluşturuyorum.



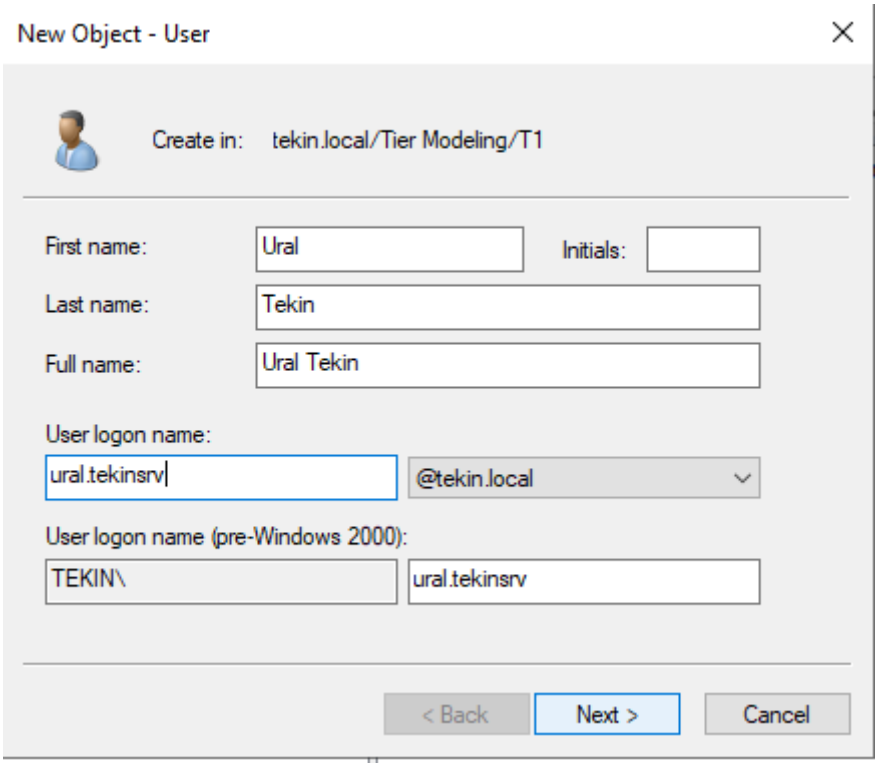
Görüldüğü üzere T0 Ou'sunda ilgili kullanıcı oluştur.



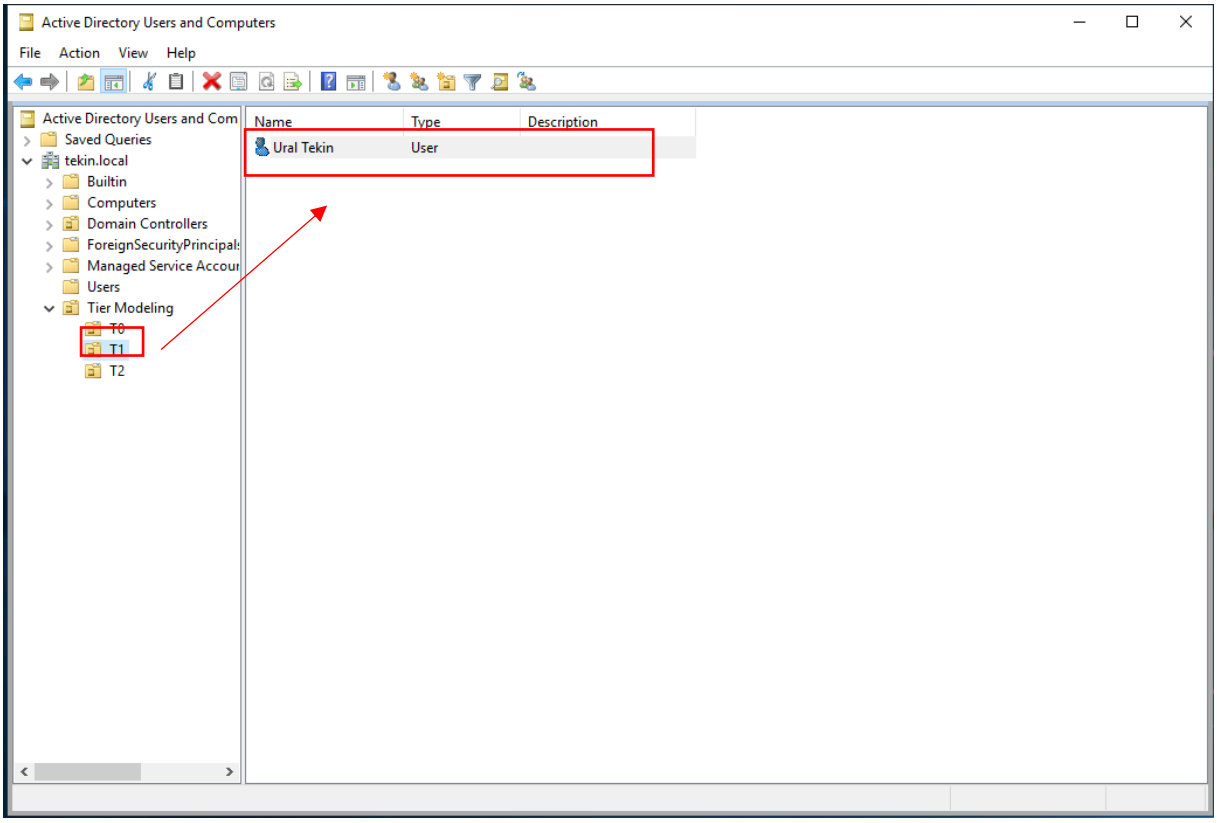
Bu kullanıcı oluşturma işlemine diğer OU'larda yukarıdaki topolojim ve örneğime bağlı kalarak T1 ve T2 Ou'sunda devam edeceğim. T1 OU' suna geliyorum ve ural.tekinsrv adlı kullanıcımı oluşturuyorum.



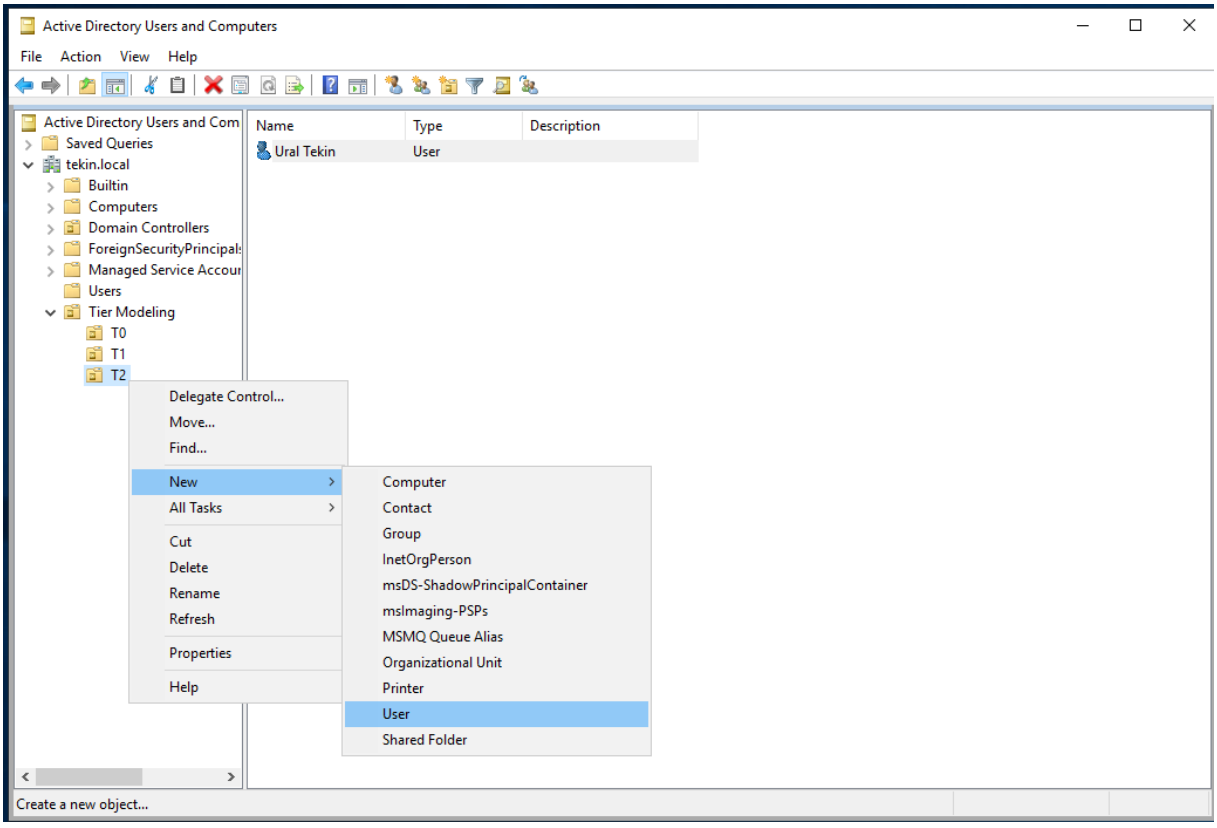
Karşıma gelen menüden ilgili bilgileri giriyorum ve next diyorum.



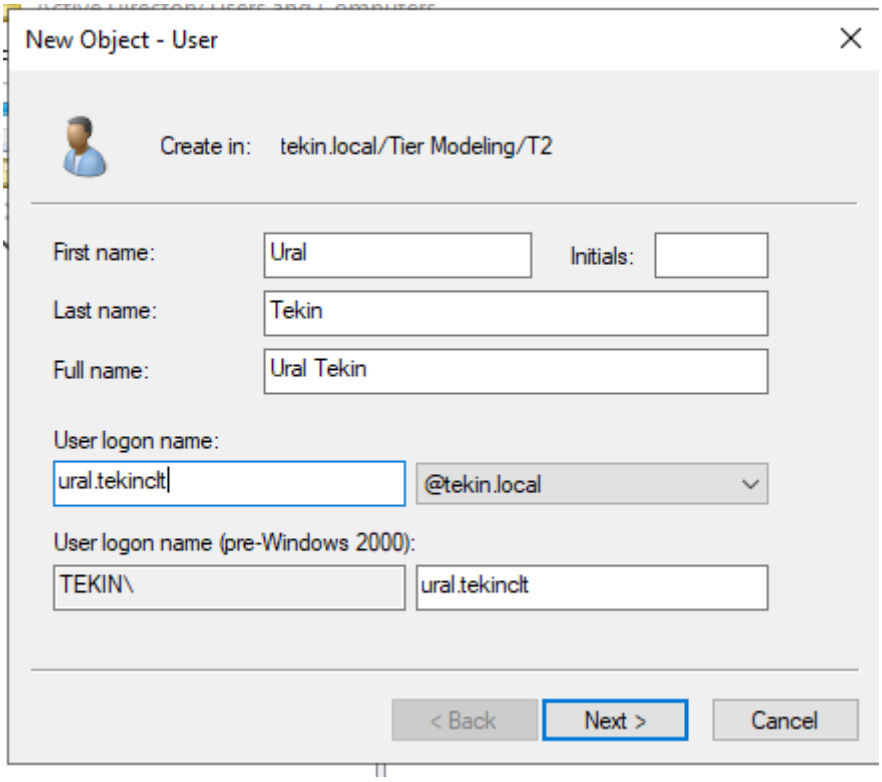
T1 OU'sundaki kullanıcım da oluşturuldu.



Şimdi **T2** OU'suna gidiyorum ve orada da kullanıcımı oluşturuyorum.

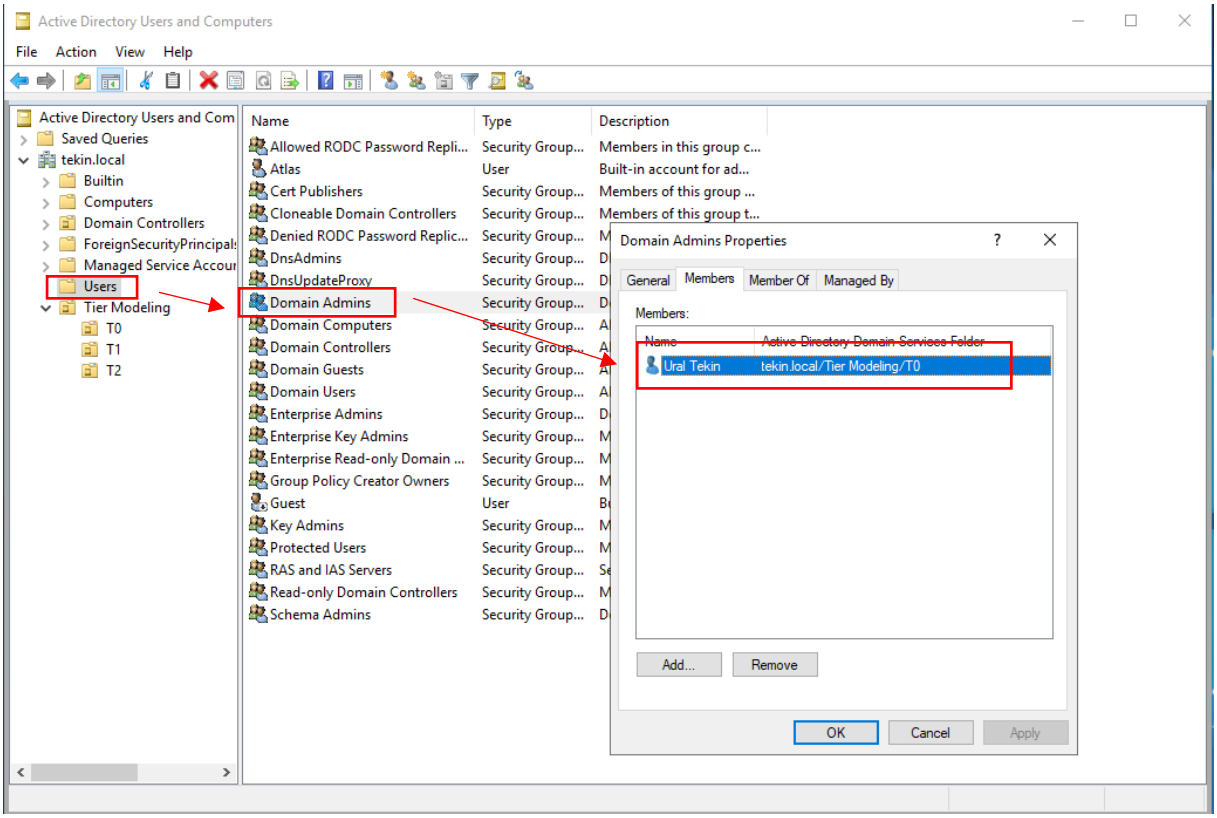


Karşıma gelen menüden ilgili alanları doldurup next diyerek kullanıcımı oluşturuyorum.



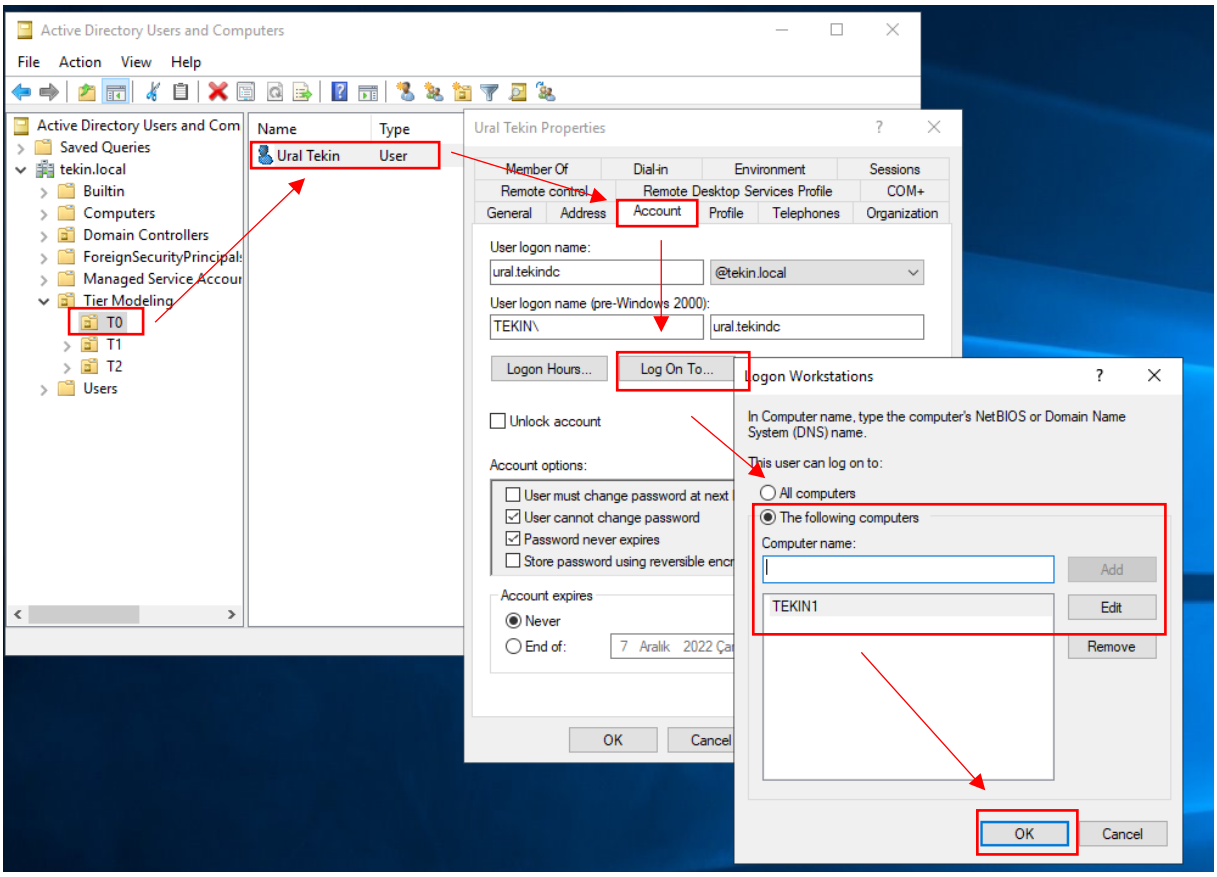
Kullanıcılarımız oluşturduktan sonra kalan konfigürasyonumuza devam ediyoruz.

İlk olarak Domain Admins grubundaki tüm kullanıcıları silip TO Ou'sunda oluşturduğum ural.tekindc kullanıcısını ekliyorum.

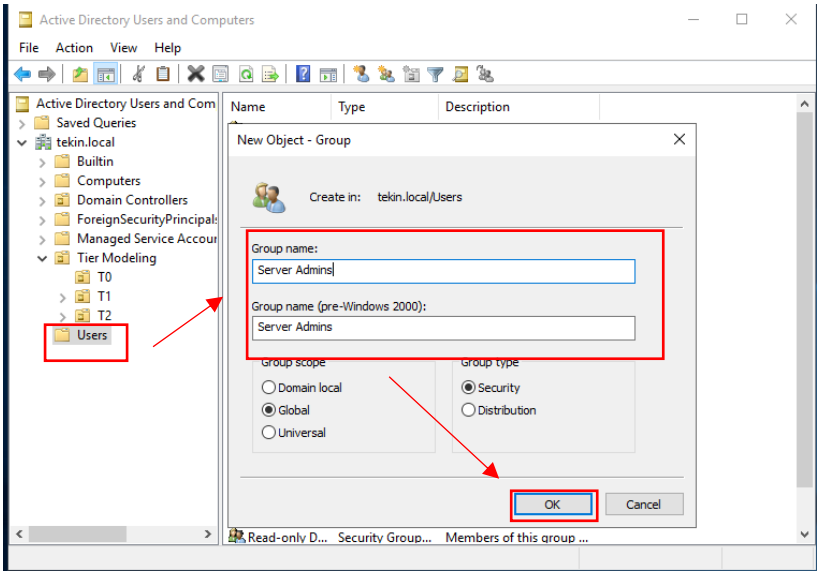


İlgili kullanıcımızı ekledikten sonra yapmamız gereken önemli bir değişiklik var. Standartta Domain Admins üyesi bir kullanıcı domainde tüm kaynaklara erişebilir ve admin yetkisi mevcuttur. Tier yapısında oluşturulan bu kullanıcının ortamızmızdaki sadece DC makinemize erişmesini istiyorum. Bu nedenle T0 Ou'sunda bulunan ural.tekindc kullanıcıma gelerek ilgili ayarlarımı gerçekleştireceğim.

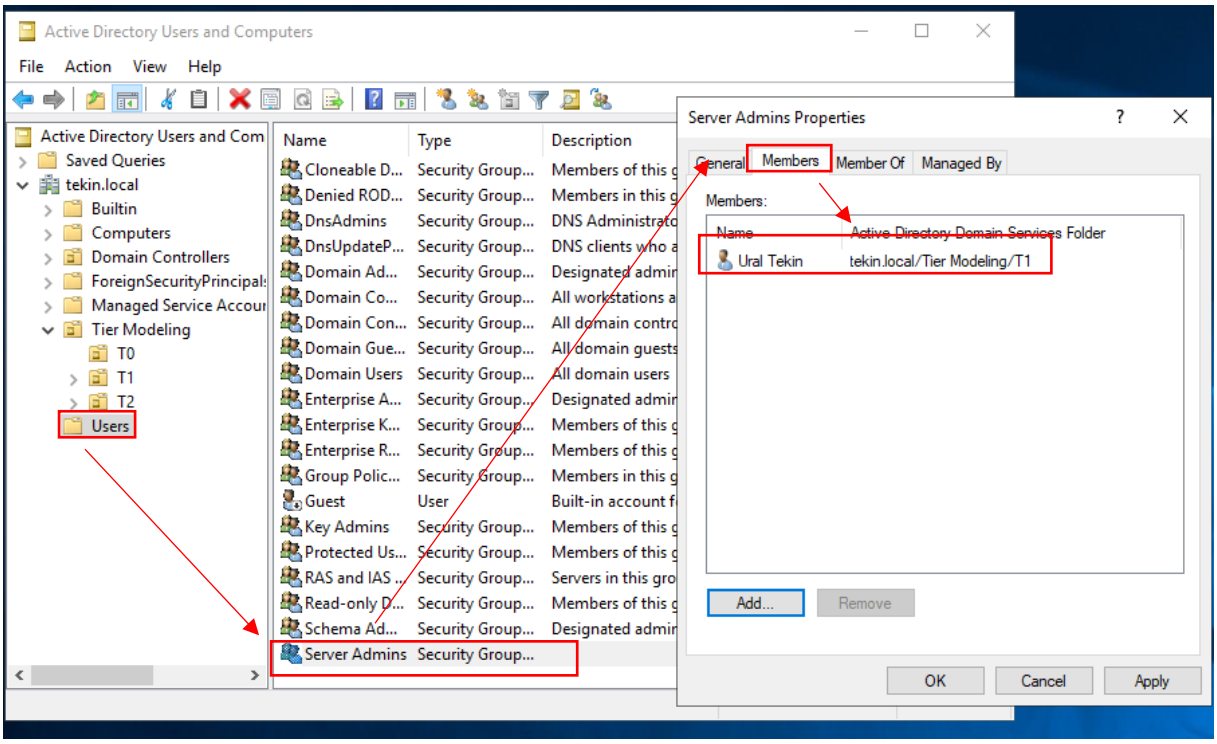
İlgili kullanıcıma çift tıklayıp **Account** menüsünden **Log On To..** tıklıyorum. Karşıma gelen ekrandan **“The Following computers”** seçeneğini seçip Domain Controller ismini yazıp **Add** diyerek ok liyorum.



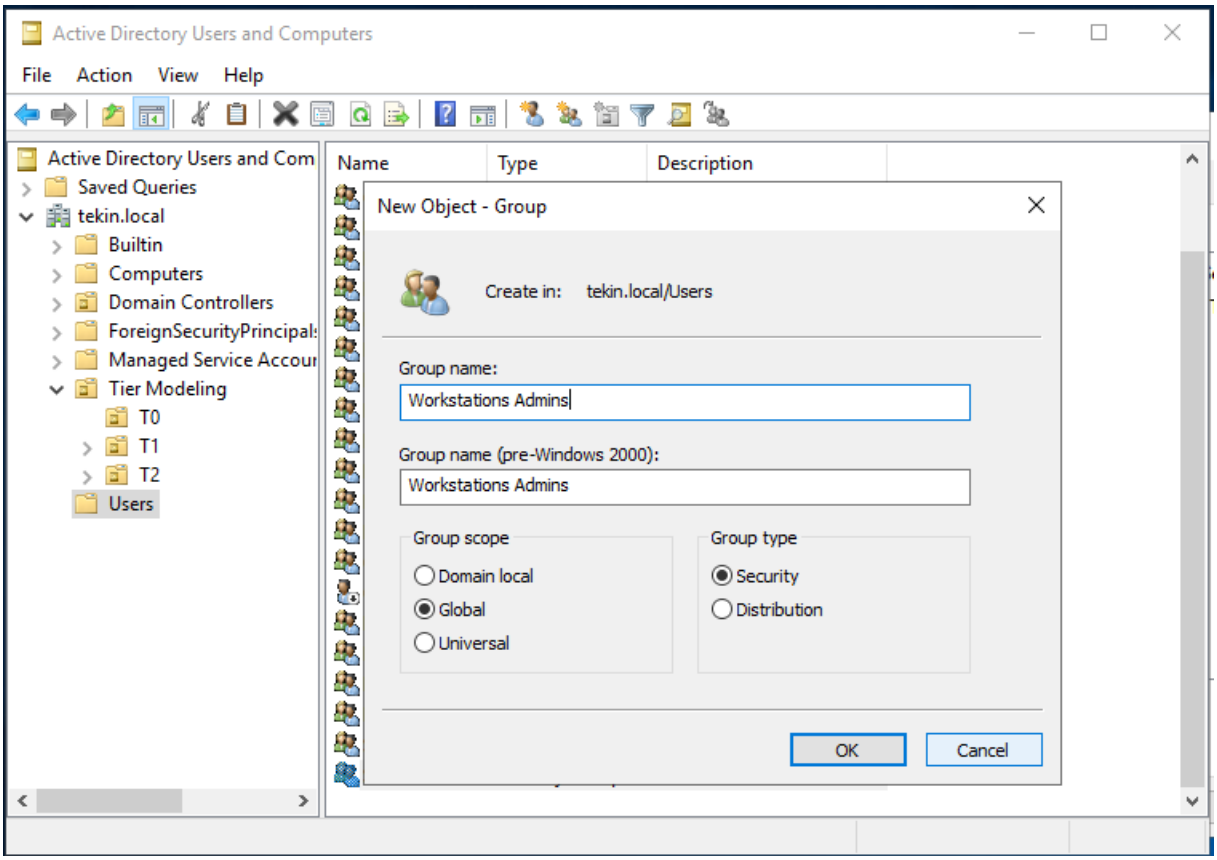
İlgili yapılandırmamdan sonra T1 OU’sundaki ural.tekinsrv kullanıcım için gerekli ayarları yapacağım. Bu nedenle ilk olarak “Server Admins” adında bir securty Group oluşturuyrum.



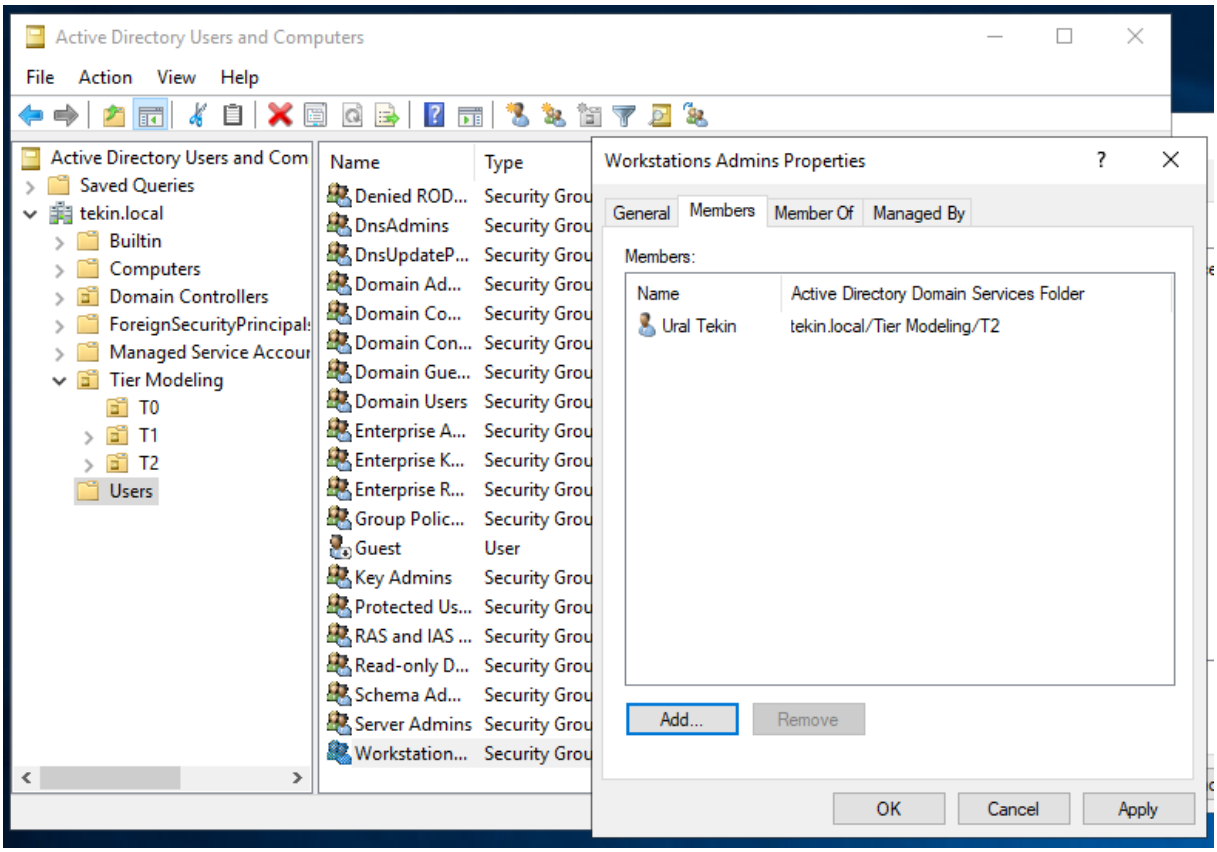
Oluşturmuş olduğum bu gruba **T1** OU'sunda bulunan **ural.tekinsrv** kullanıcımı üye yapıyorum.



Aynı işlemleri **T2** OU'sunda bulunan ural.tekinclt kullanıcım içinde yapacağım. Bunun için **"Workstations Admins"** isminde bir securty group oluşturuyorum.



İlgili grubumu oluşturduktan sonra T2 OU da bulunan ural.tekinclt isimli kullanıcımı bu grup a üye yapıyorum.



Böylelikle buraya kadar T0, T1 ve T2 adında OU lar oluşturdu. Bu OU lar altında ilgili kullanıcıları oluşturup aynı zamanda grup yetkilendirmelerini tamamladım.

Bu adımlarla birlikte 4 adet kullanıcım oluştu.

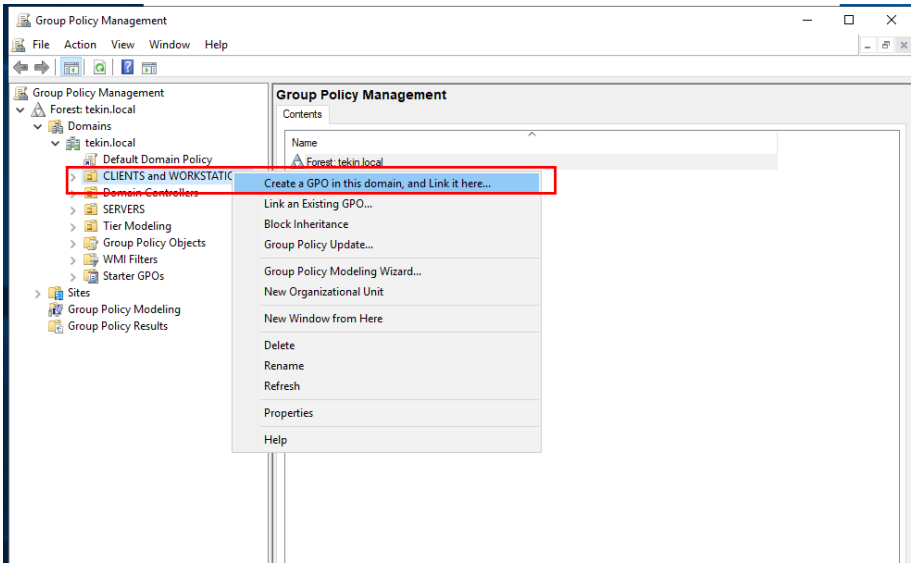
Sırada oluşturmuş olduğumuz server admins ve Workstations admins kullanıcılarını GPO ile domain ortamımızda bulunan envarterlere eklemek. Bunu yapmamdaki amaç büyük yapılarda tek tek bilgisayarları dolaşmak çok zamanımı alacaktır. Ayrıca büyük iş gücü. Ana amaç bunu önlemek.

Bu nedenle GPO konsolumu açarak ilgili ayarları yapılandıracağım.

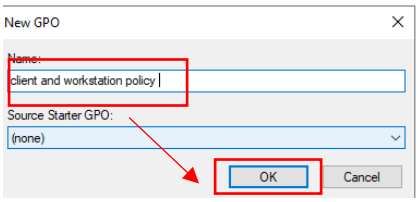
Ben domain ortamımda son kullanıcı ve workstationlar bir OU da Sunucuları ise başka bir OU da tutuyorum.

Group Policy Management konsolumu açıyorum. İlk olarak client ve Workstation cihazlarıma T2 Ou' sunda bulunan ural.tekinclt kullanıcımı local admin olarak tanımlayacağım.

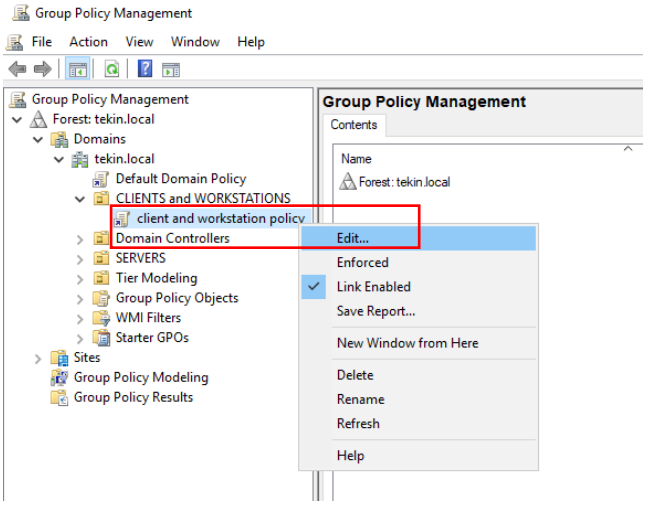
Bu nedenle ilgli OU ya gelip bir kural oluşturmak için sağ tuş "Create a GPO in this domains" seçeneğine tıklıyorum.



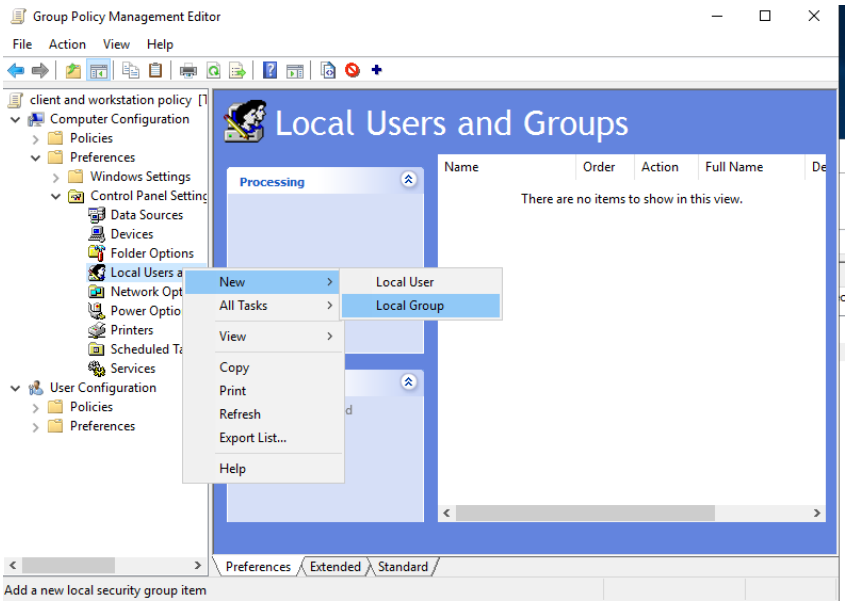
karşıma gelen pencereden kuralıma isim verip ok diyorum.



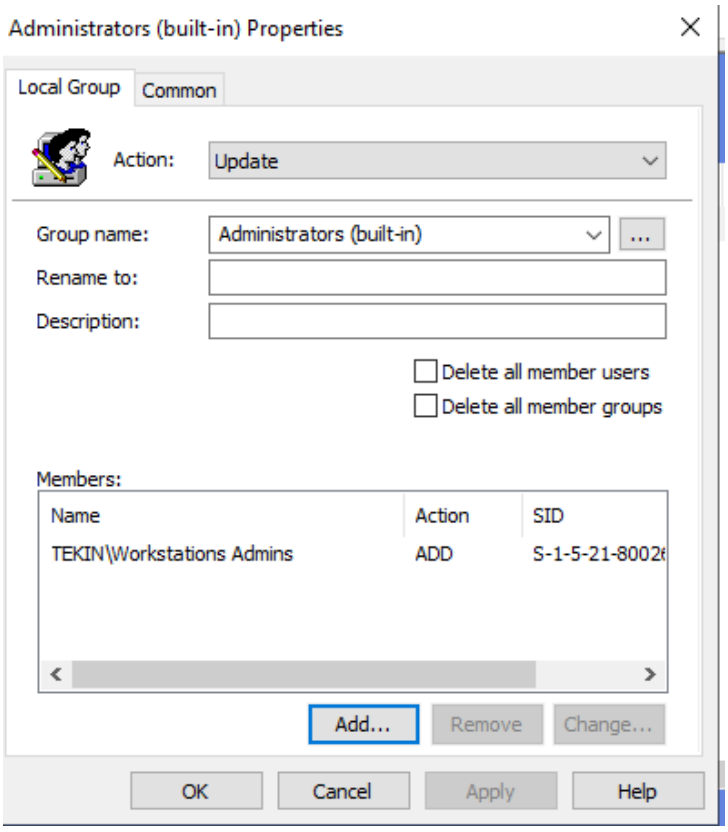
Sonrasında ilgili kuralımın üzerine gelip sağ tuş edit diyorum ve düzenlemeye başlıyorum.



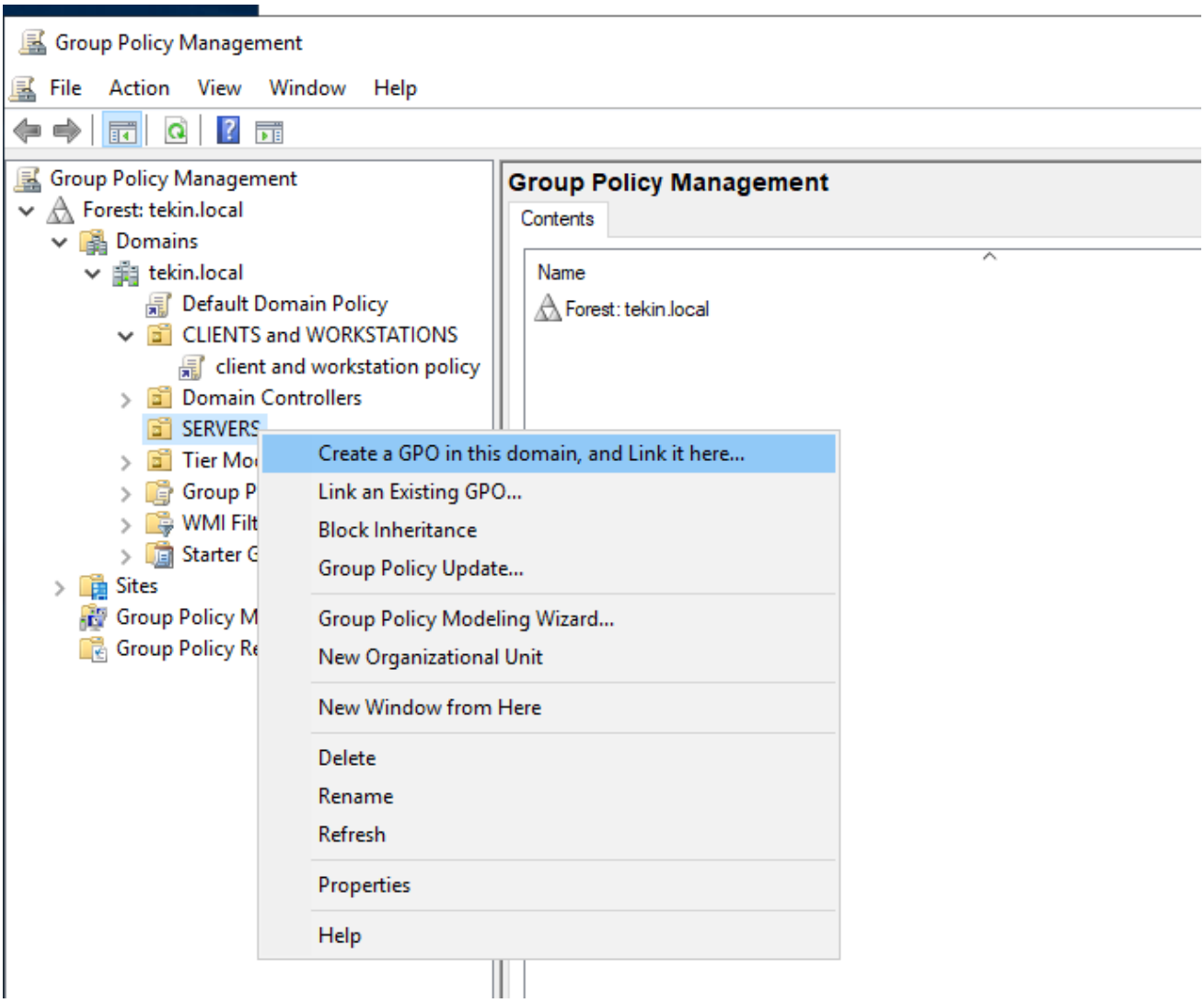
Karşımıza gelen pencereden Computer Configiration/Preferences/Control Panel Settings/Local Users and Groups alanına geliyoruz. Buradan New/Local Group diyorum.



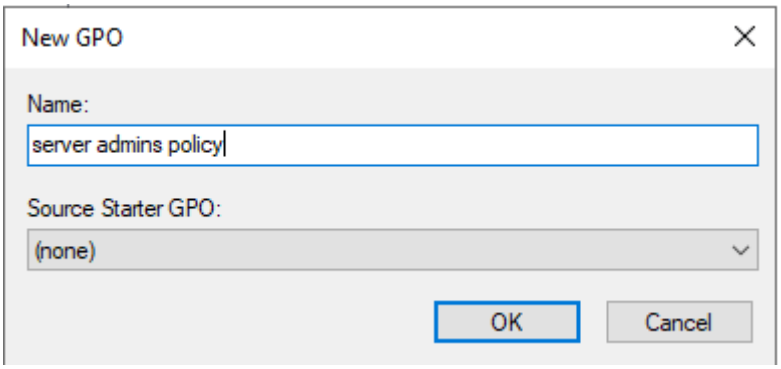
Karşıma gelen ekrandan Action kısmını update olarak bırakıyourum. Groupname kısmından Administrators seçiyorum. Aşağıda Add diyerek T2 ou sunda bulunan ural.tekinclt isimli workstations admins kullanıcımı seçiyorum ok diyerek işlemimi tamamlıyorum.



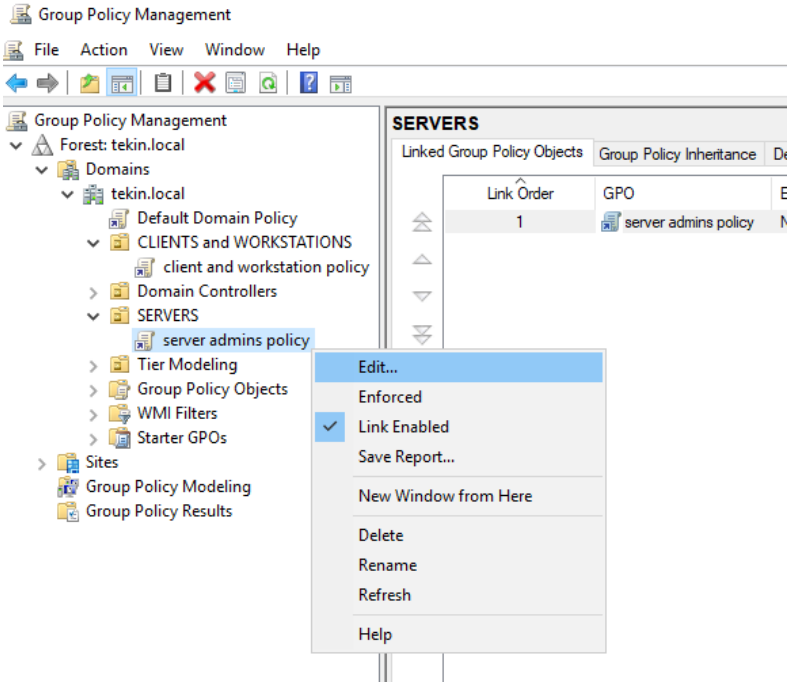
Sonraki adımda ortamımda bulunan serverlar için kural oluşturacağım. SERVERS OU suna geliyorum sağ tuş Create a GPO in this domain diyorum.



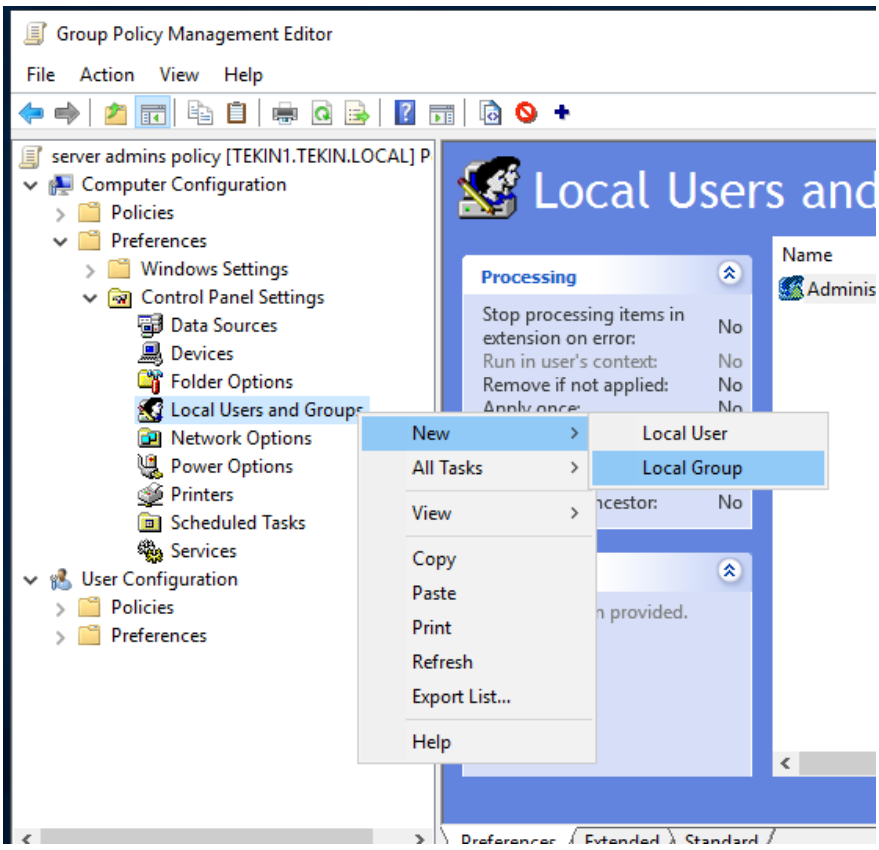
Karşıma gelen ekrandan kuralıma isim veriyorum ve ok diyorum.



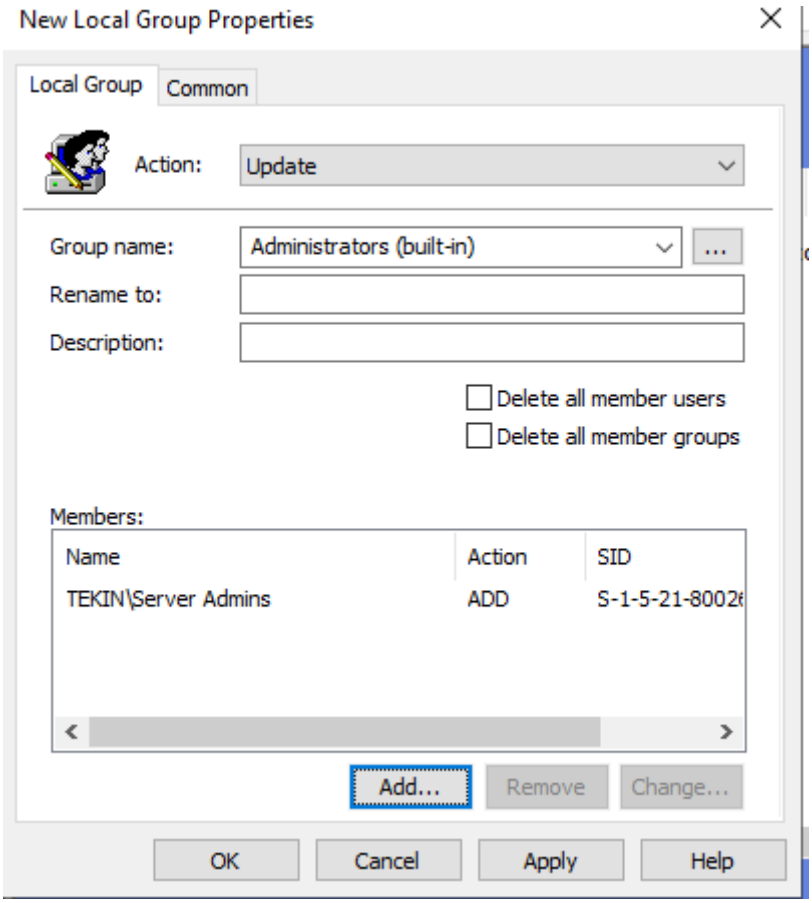
İlgili kuralımın üzerinde gelip edit diyorum.



Karşımıza gelen pencereden Computer Configiration/Preferences/Control Panel Settings/Local Users and Groups alanına geliyoruz. Buradan New/Local Group diyorum.



Karşıma gelen ekrandan yine action kısmını update olarak bırakıyorum. Group name kısmından Administrator seçeneğini seçip Add diyerek “server admins” grubunu seçip ok diyorum.



Son olarak Domain Contraller run konsolu açaraka GPO kurallarımın anında aktif olması için gpupdate /force komutunu giriyorum.

Client’lar bir somraki açılışta kuralları direk alacaklardır.