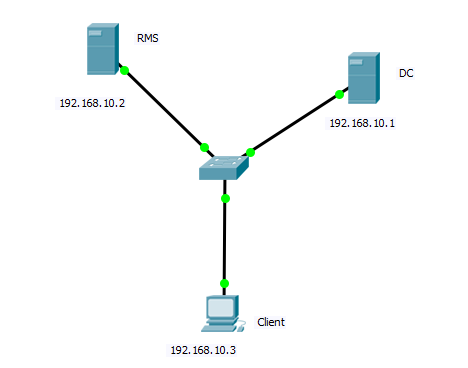
ACTIVE DIRECTORY RIGHT MANAGEMENT SERVİCES

Safa Onur Macit

**Proje Hakkında Bilgi**

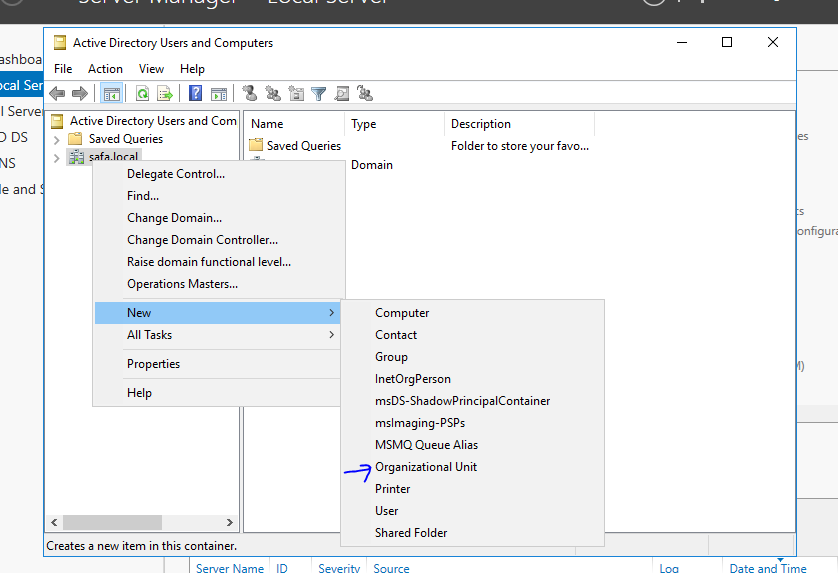
Active Directory Right Management Services (AD RMS), sunucu ve istemci bileşeninden oluşan bir sunucu işletim sistemi uygulamasıdır. AD RMS bileşeninin kullanılması ile, şirket içi yedeklere ve belgelere, yetkisiz kişilerin erişimi sınırlandırılmış olmaktadır. AD RMS’in sunucu tarafındaki bileşeni, Microsoft sunucu işletim sistemleri üzerinde çalışan web servislerinden, istemci bileşeni ise, sunucu ve client işletim sistemleri üzerinde çalışan şifrelenmiş dosyalara ve uygulamalara erişim gerçekleştirmeyi sağlamaktadır. AD RMS, Microsoft İnternet Information Services (IIS) üzerinde çalışan web hizmetleri kümesi tarafından yürütülmektedir.

**Topoloji**

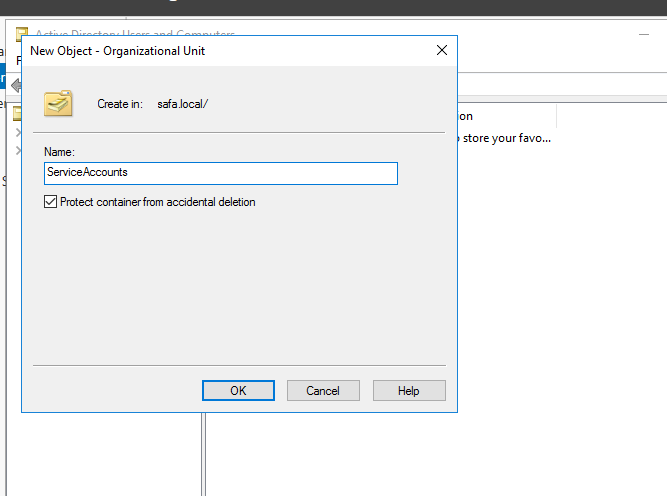


**Proje Adımları**

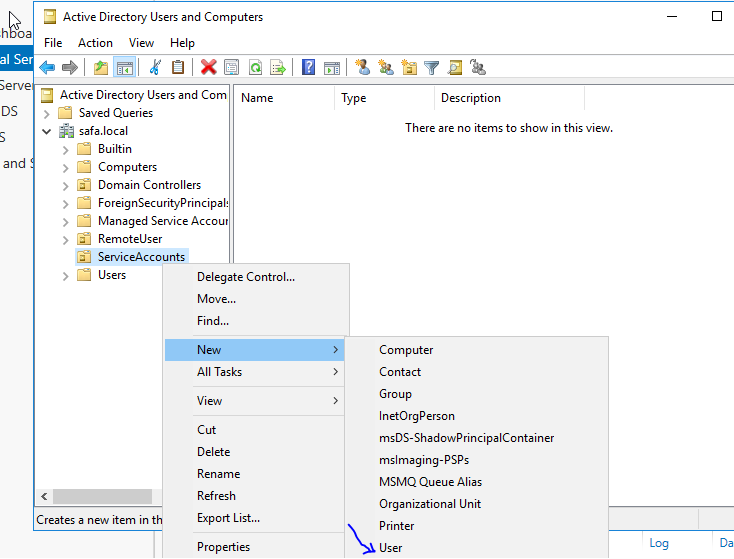
DC ile yeni bir OU oluşturulmak için Organizational Unit seçildi.



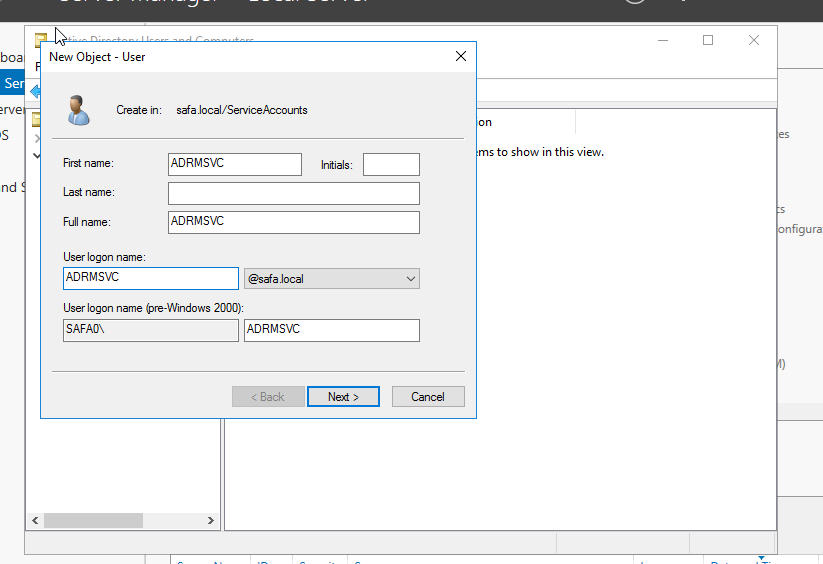
İsmine ServiceAccounts verildi ve OU oluşturuldu.



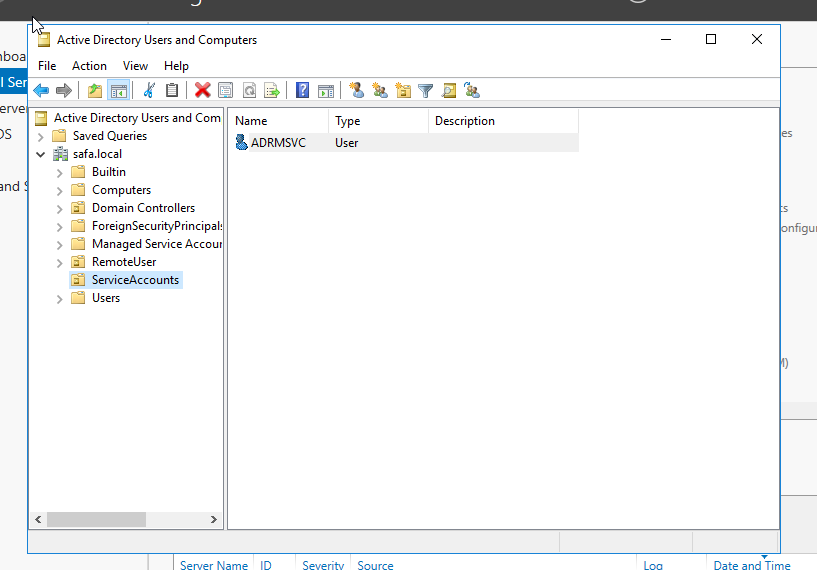
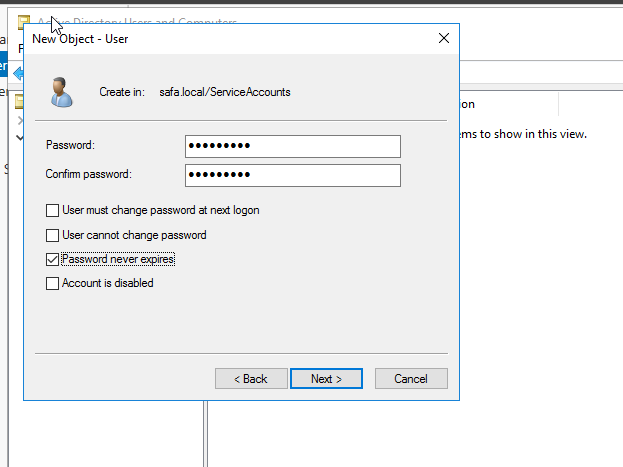
ServiceAccounts’un içine yeni bir user oluşturulmak için user seçildi.



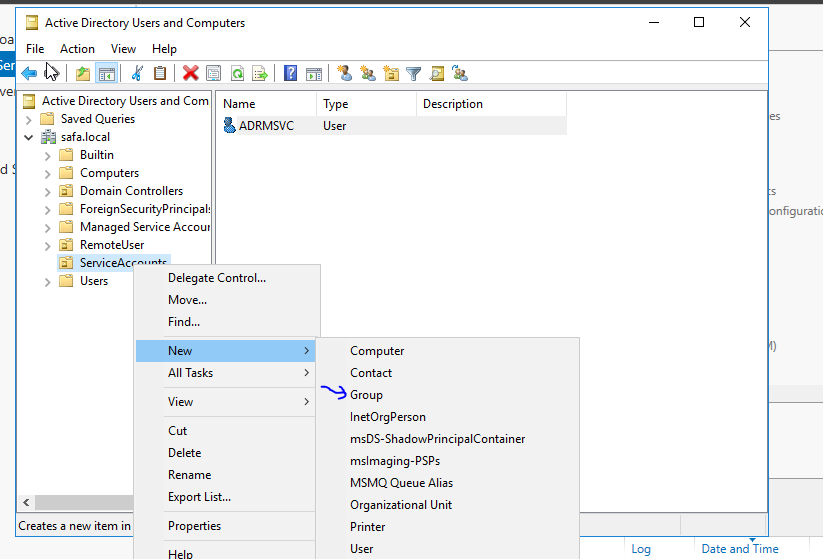
İsmine ve logon ismine ADRMSVC denildi.



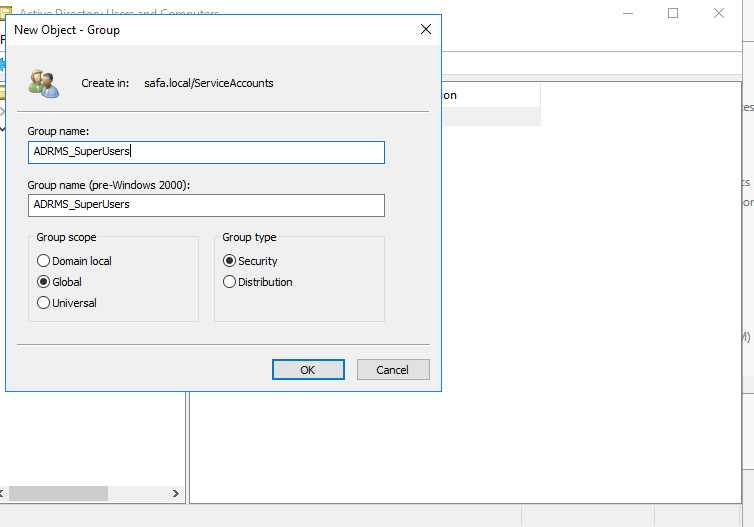
Şifre verildi değiştirilmemesi için 3.seçenek seçildi ve user oluşturuldu.



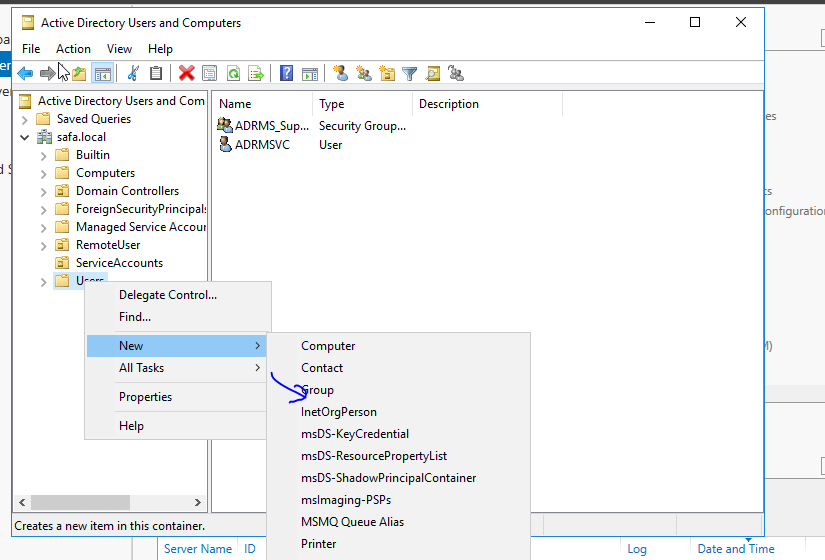
Aynı yerde yeni bir grup oluşturmak için Group seçildi.



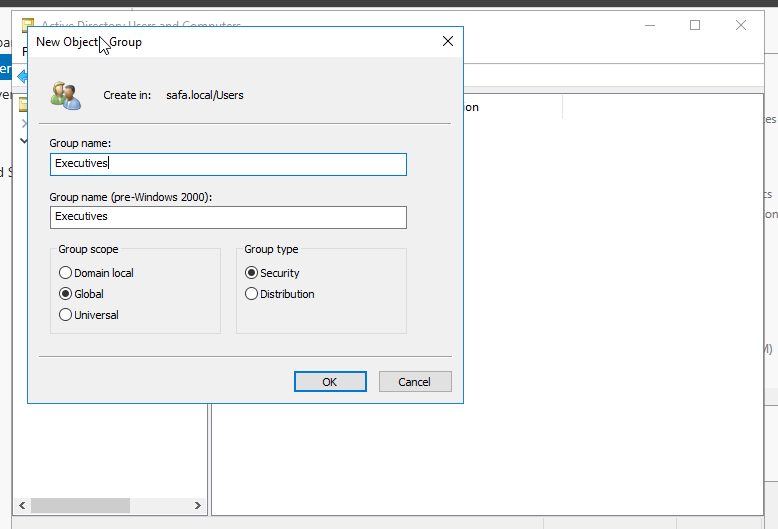
Grubun adı verildi.



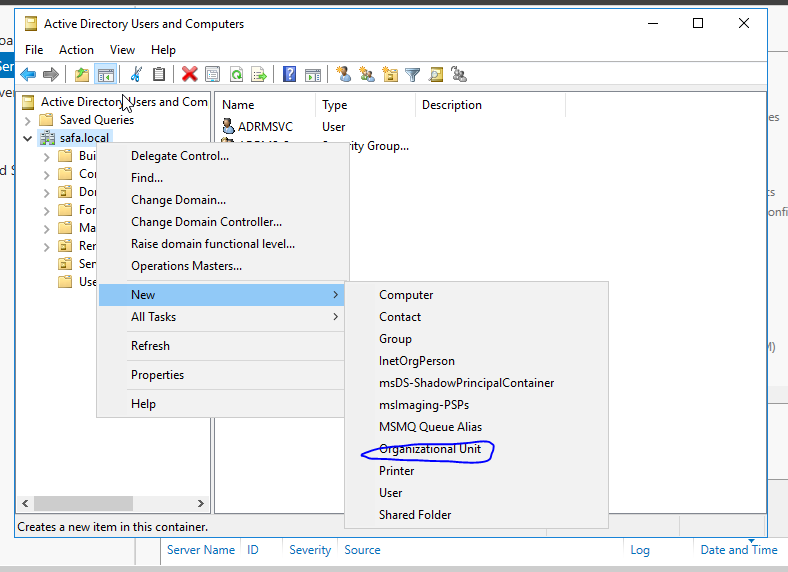
Users’ın içine yeni bir grup oluşturmak için Group denildi.



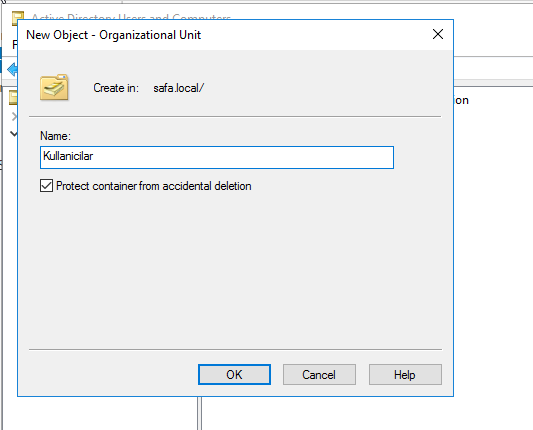
Grup ismi Executives olarak belirlendi.



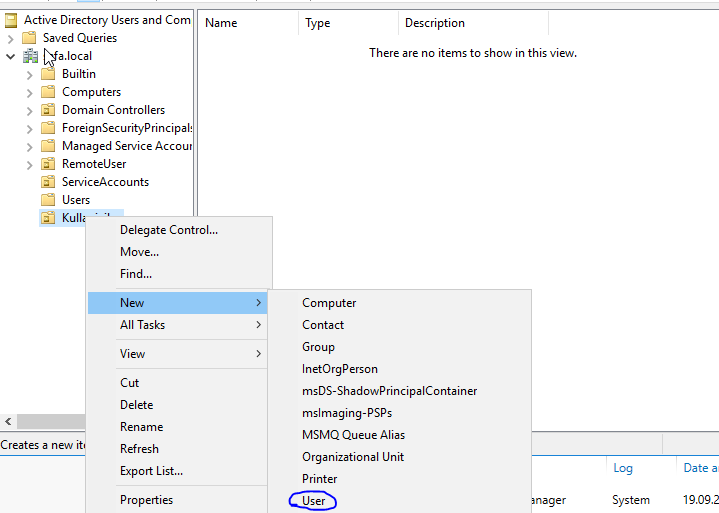
Oluşturulacak yeni kullanıcıları tutmak için yeni bir OU oluşturulacak. Bunun için OU seçildi.



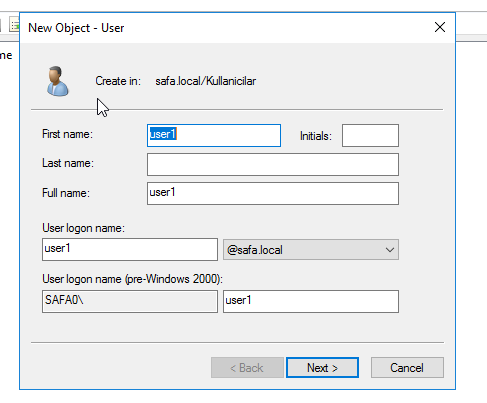
İsmi verildi.



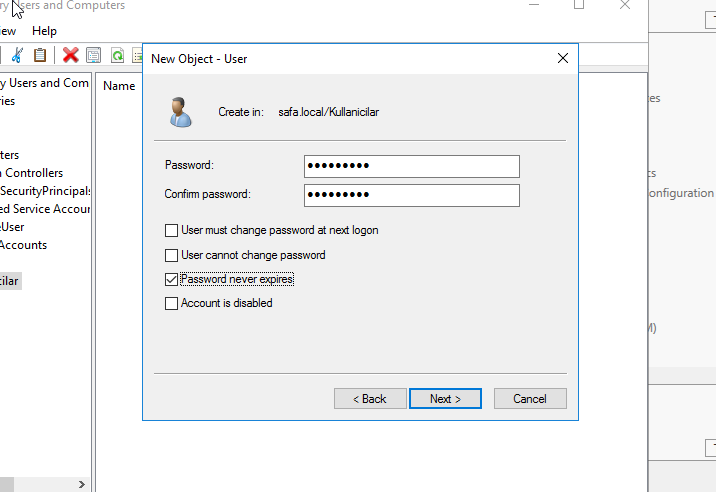
Kullanıcılar OU suna sonra kullanılacak 6 yeni user oluşturulacak. User denildi.



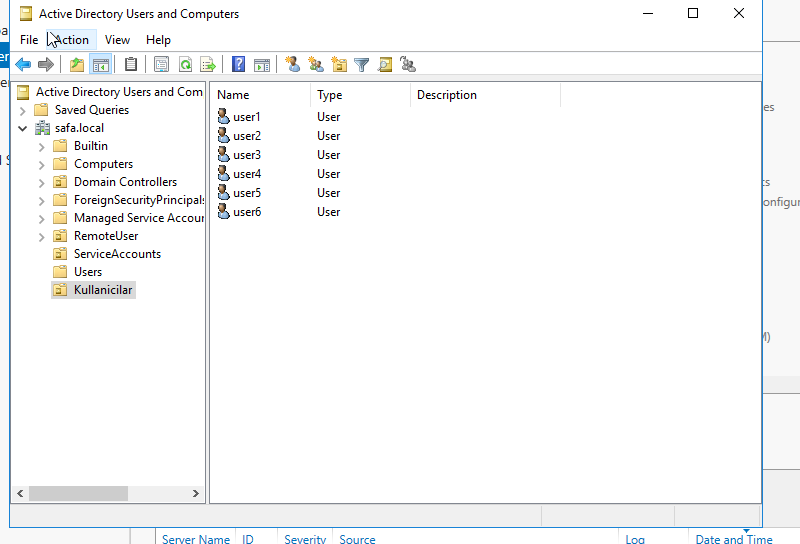
İsmi ve logon ismi verildi.



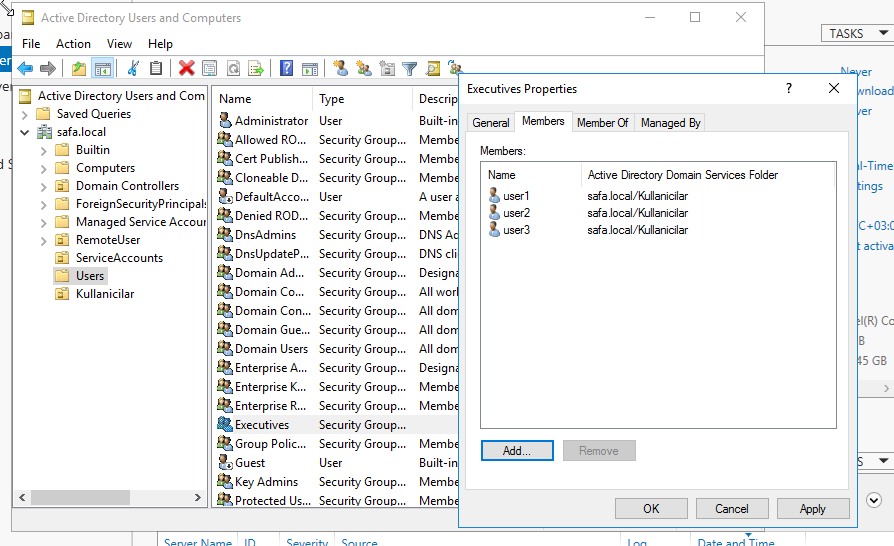
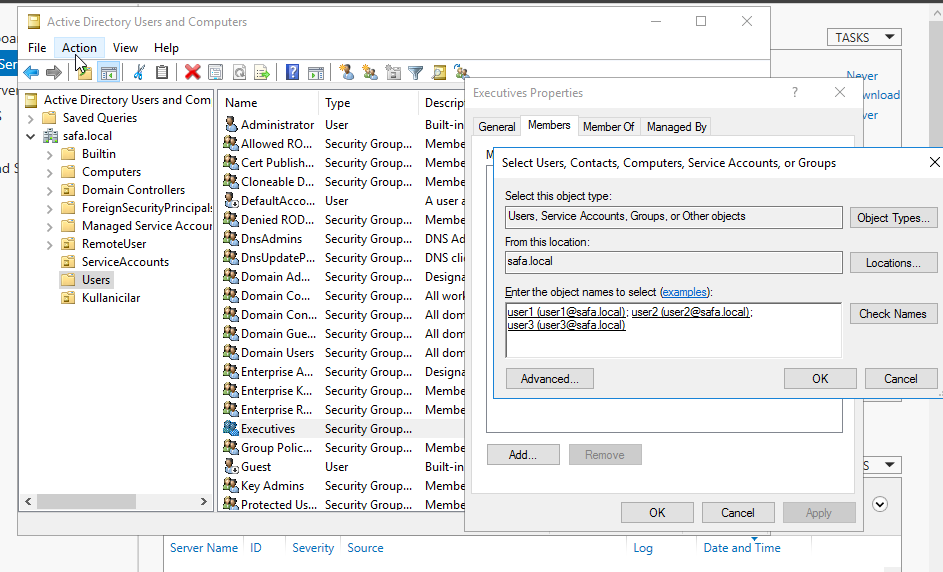
Şifresi verildi ve değiştirilmemesi için 3.seçenek seçildi ve user oluşturuldu.



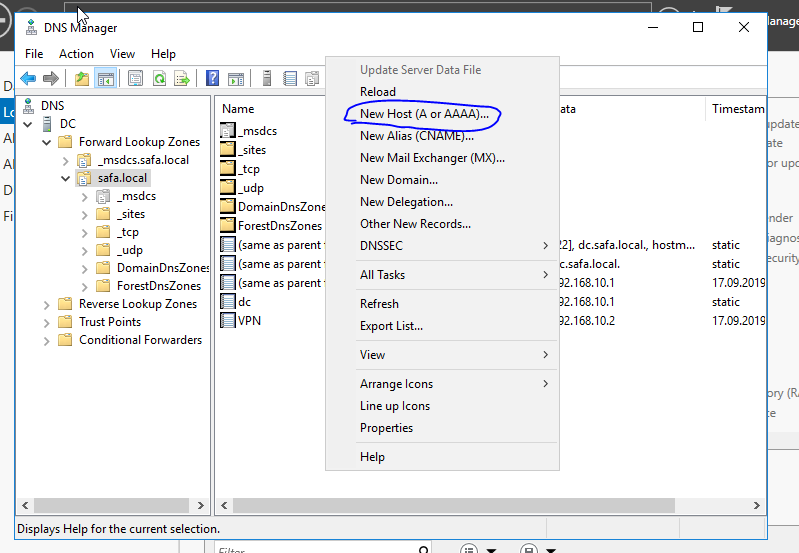
Böyle 6 tane user oluşturuldu.



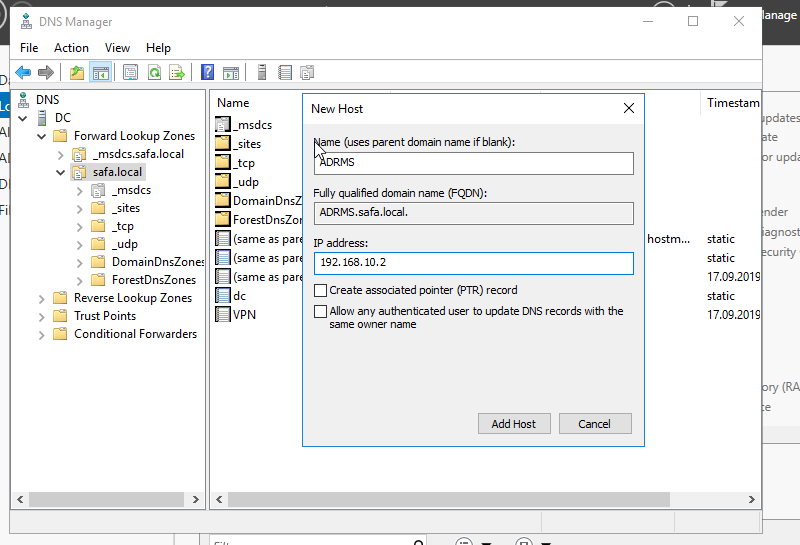
3 tanesi daha önce oluşturduğumuz Executives grubuna eklendi.



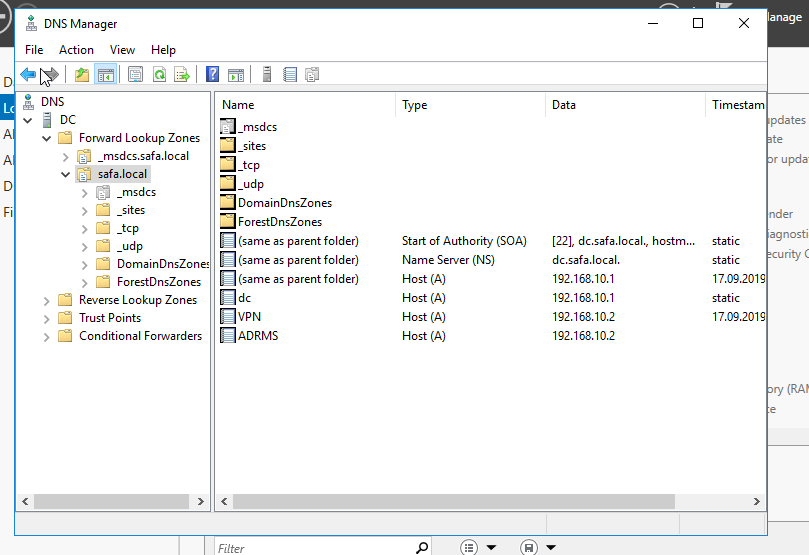
Daha sonra kullanmak için yeni bir host açıldı.



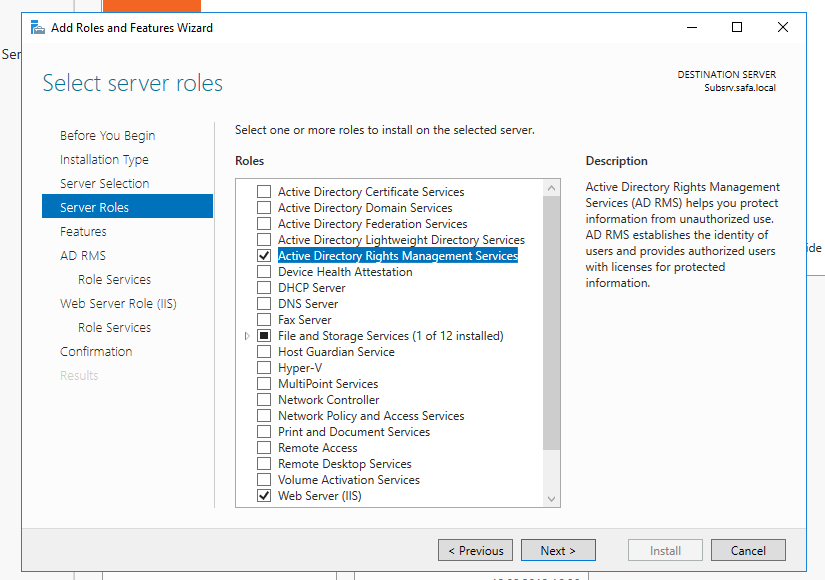
Host ismi olarak ADRMS seçildi ve IP adresi olarak RMS sunucusunun IP’si verildi.



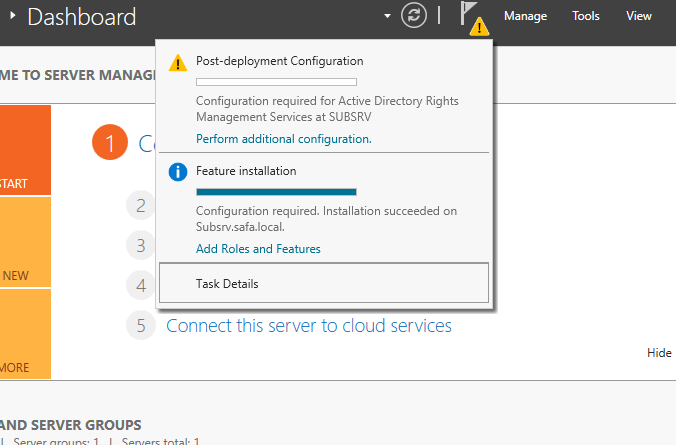
ADRMS oluşturuldu.



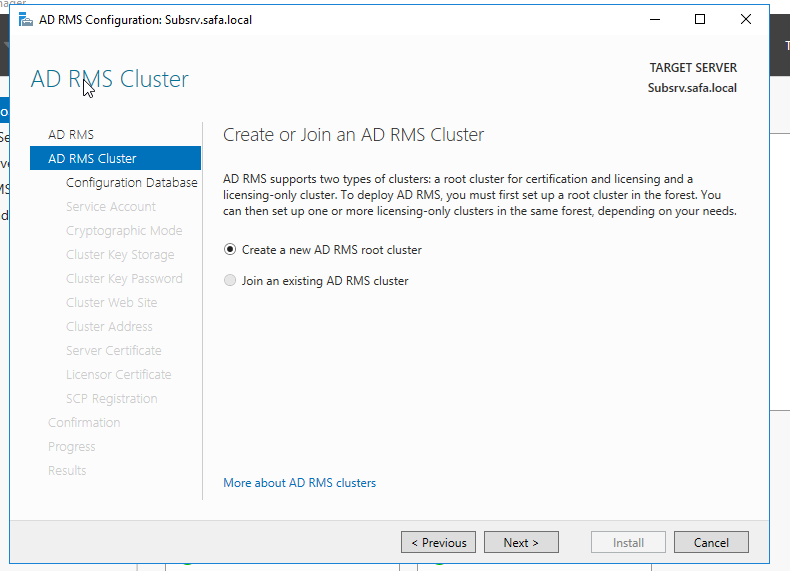
RMS Sunucusuna Active Directory Right Management Services rolü eklendi.



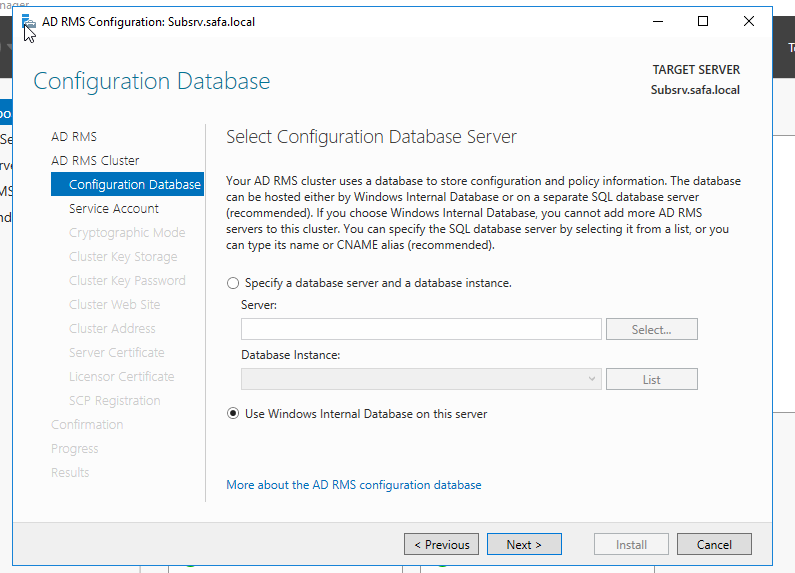
AD RMS konfigürasyonuna başlandı.



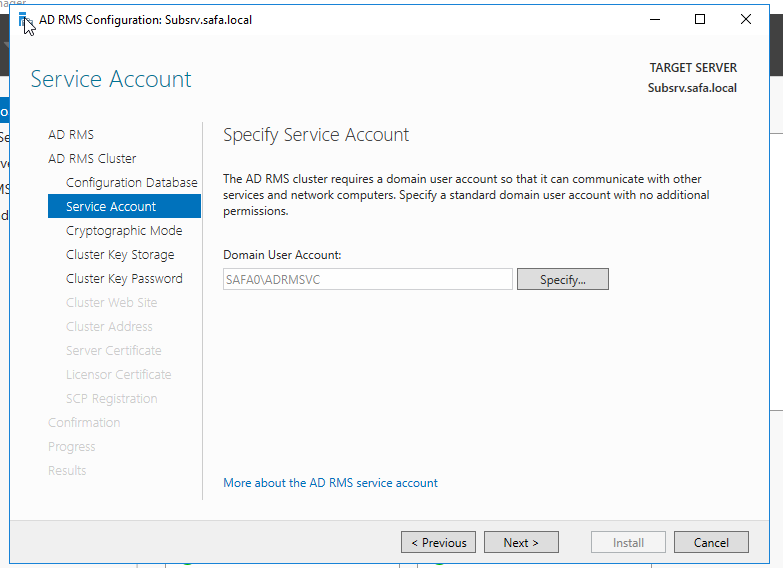
Yeni bir AD RMS oluşturulacağı için ilk seçenek seçildi.



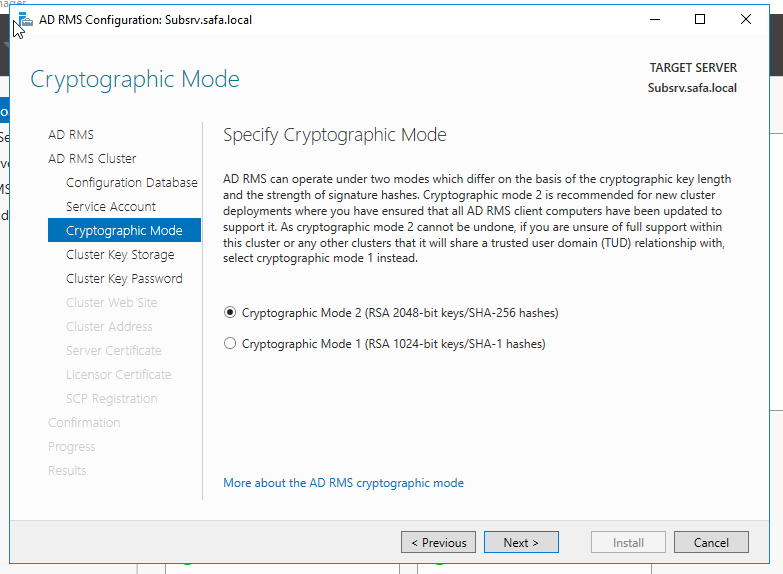
Yeni bir database server belirtmeyeceğimiz ve Windows’un database ’ini kullanacağımız için 2.seçildi.



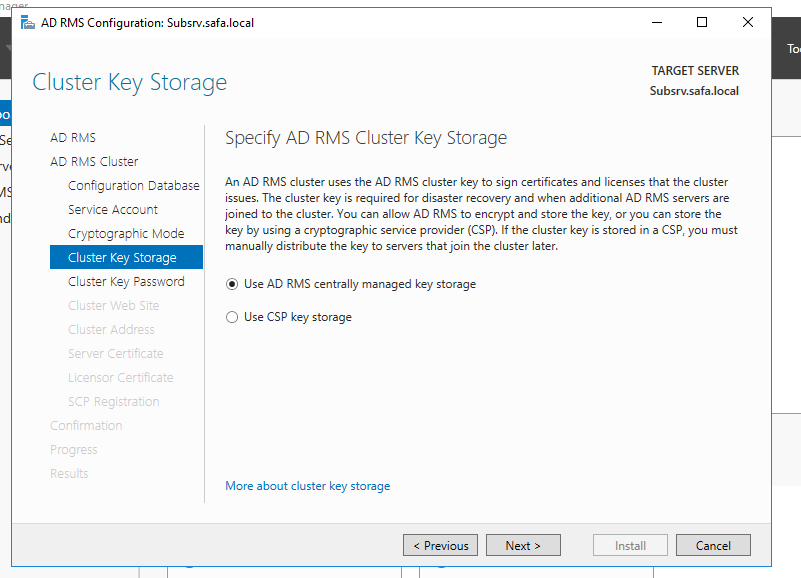
Domain User olarak daha önceden ServiceAccounts OU suna oluşturduğumuz ADRMSVC kullanıcısını belirttik.



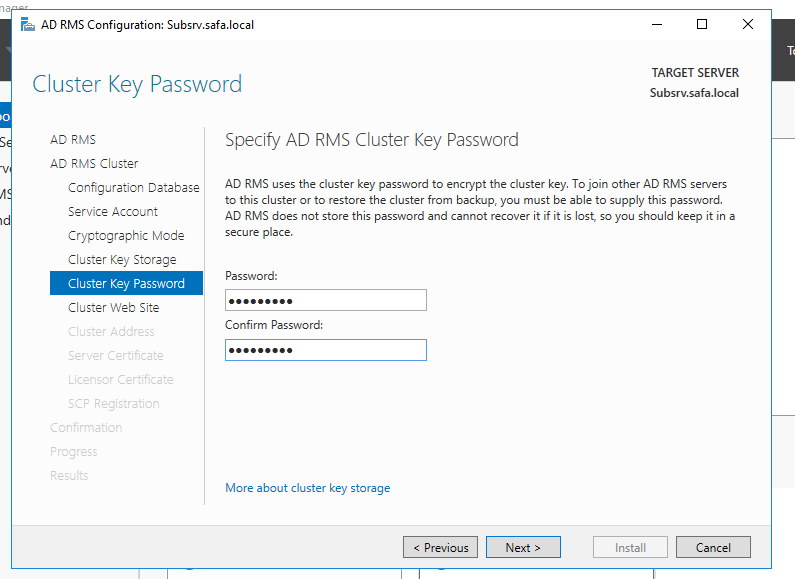
Cryptographic Mode 2 seçildi.



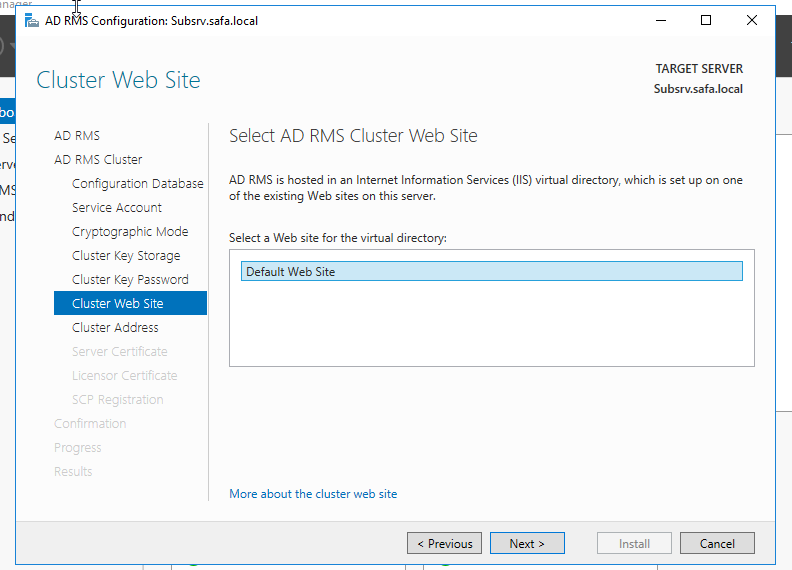
Cluster anahtarı için AD RMS’in anahtar deposu seçildi.



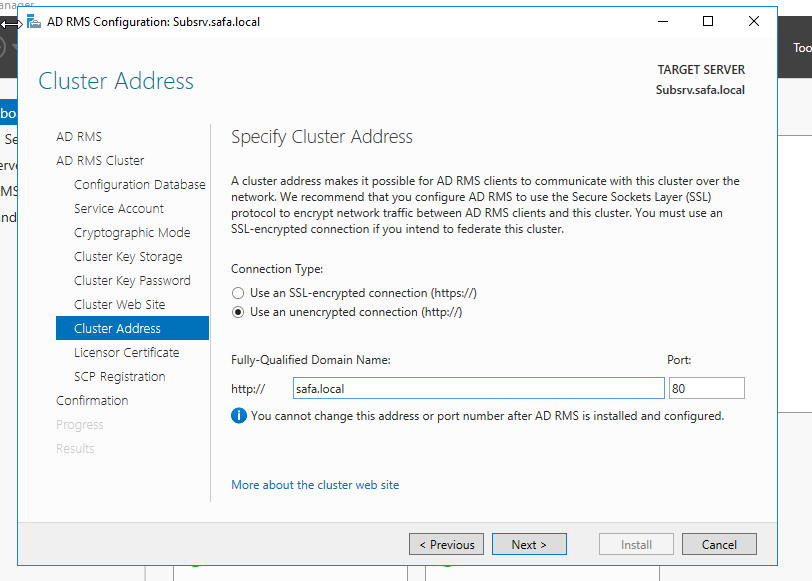
Anahtar için şifre verildi.



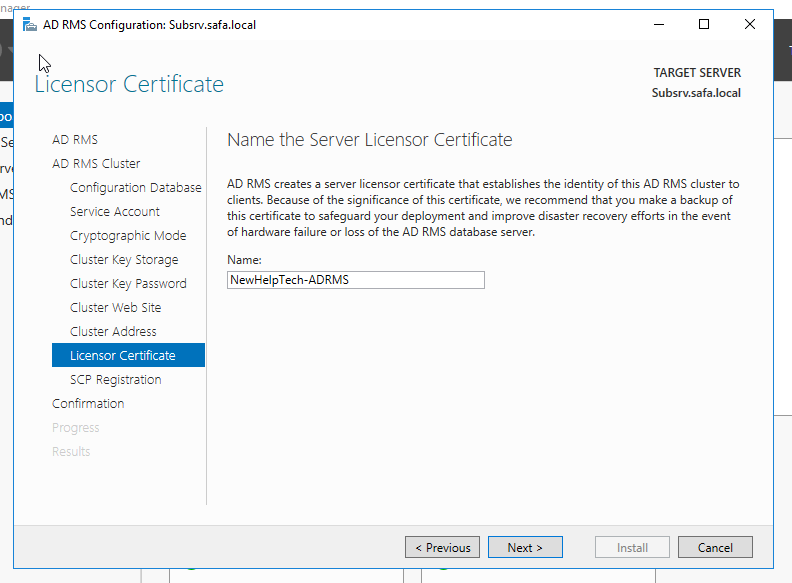
Kendiliğinden gelen Default Web Site seçildi.



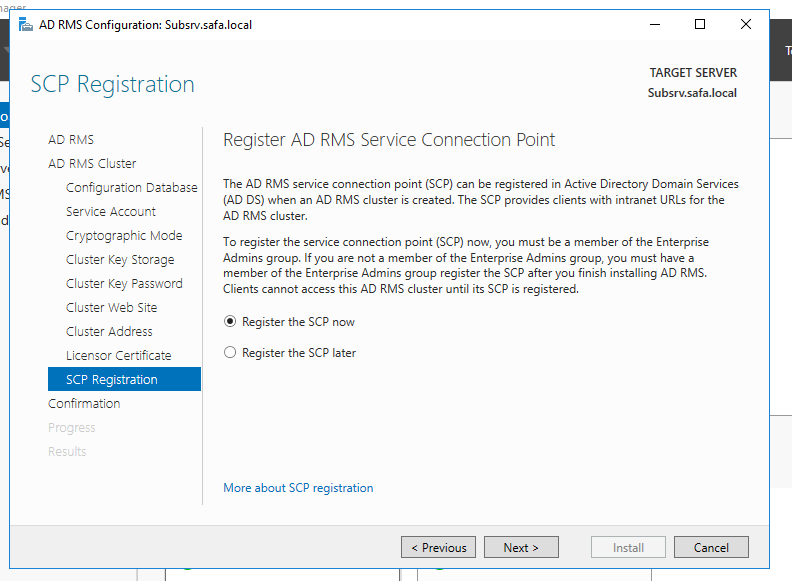
Şifresiz bağlantı seçildi. Uzantı olarak aşağıdaki gibi verildiğinde hata çıkacaktır. Doğru uzantı daha önce new host denilerek oluşturulan ADRMS.safa.local olmalıdır.



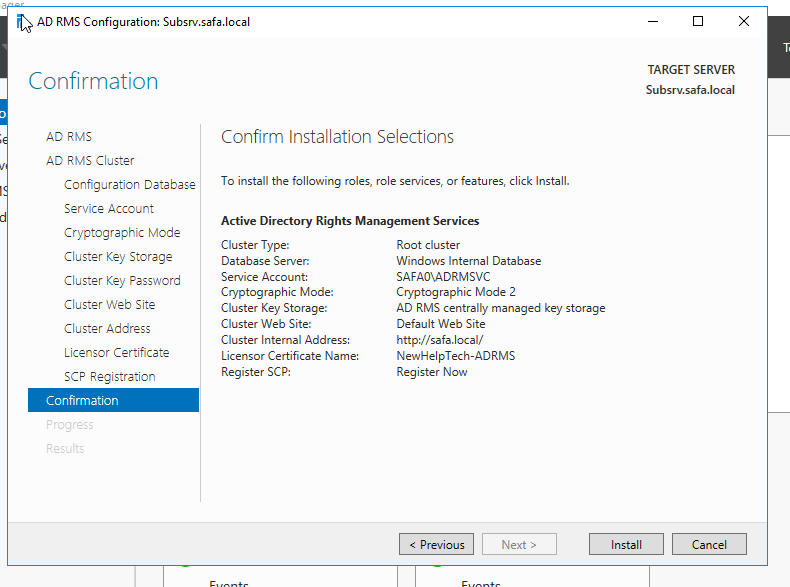
Bir isim girildi.



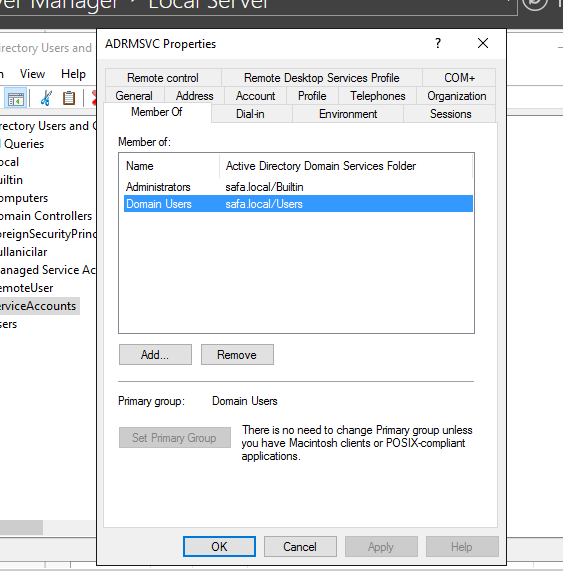
SCP’yi şimdi kaydetmek için ilki seçildi.



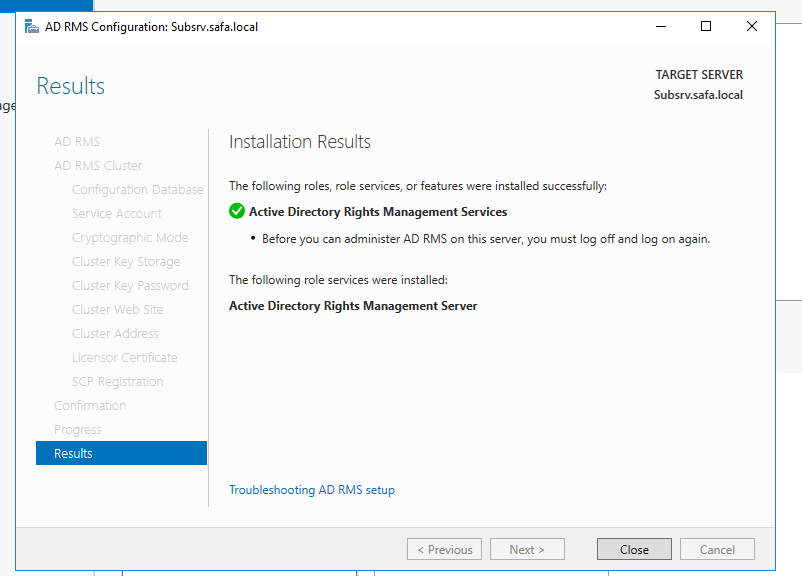
Yükleme hazır.



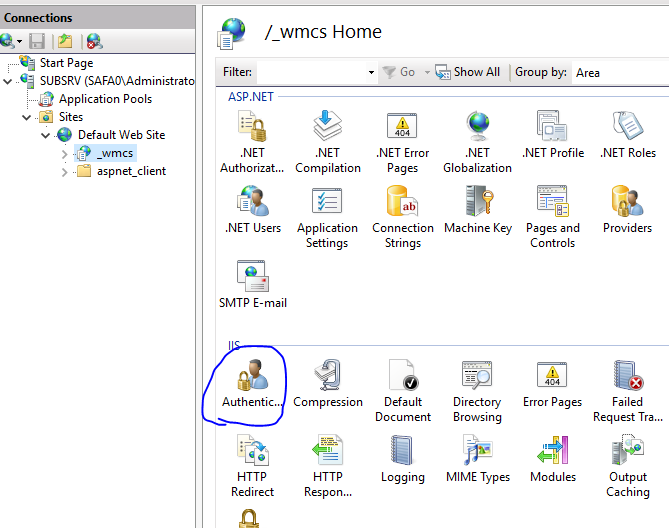
Fakat hata çıkacaktır. Bunu çözmek için DC’den ADRMSVC kullanıcının özelliklerine girip Administrators yetkisi verildi.



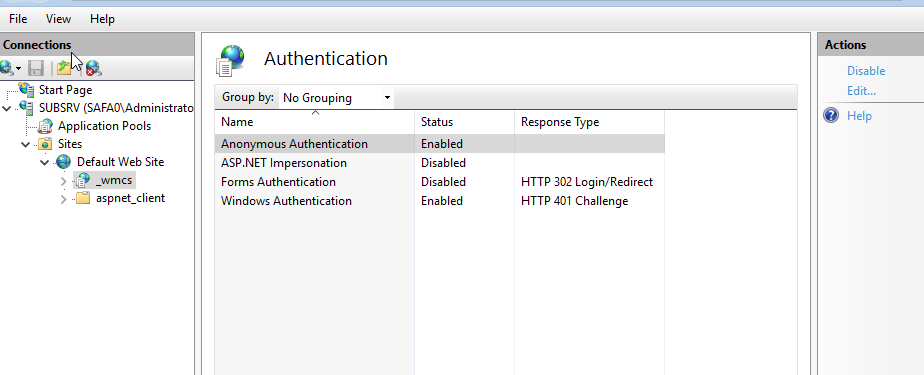
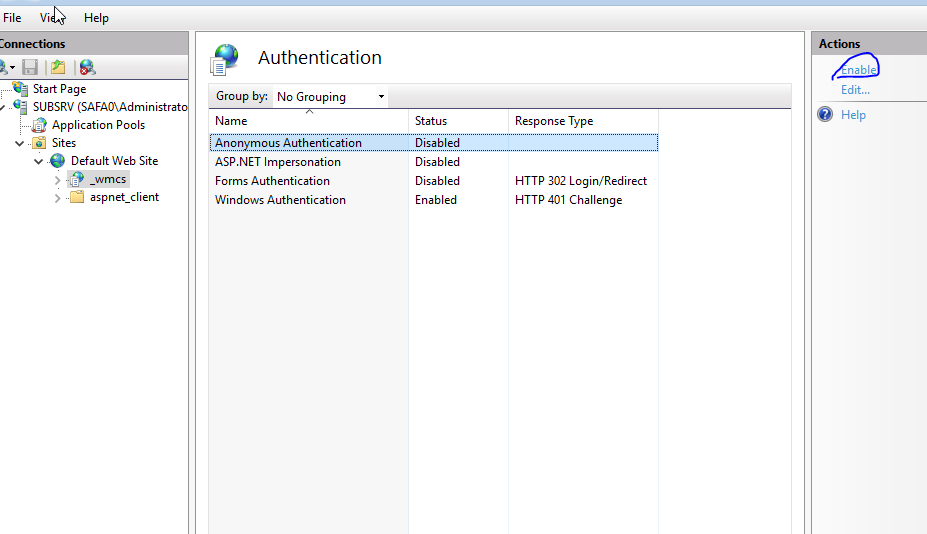
AD RMS kurulumu başarılı.



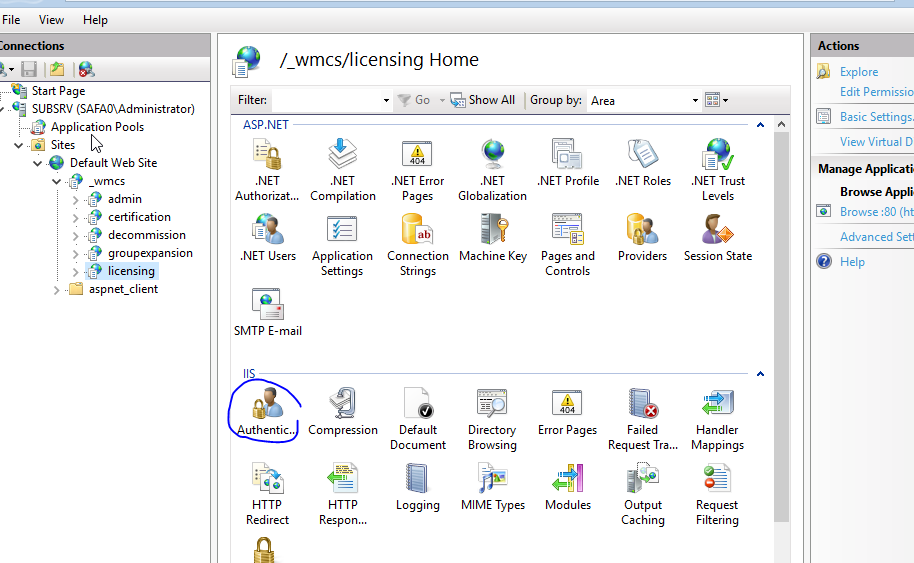
AD RMS nin kurulu olduğu RMS sunucusundan IIS e girildi ve Authentication seçildi.



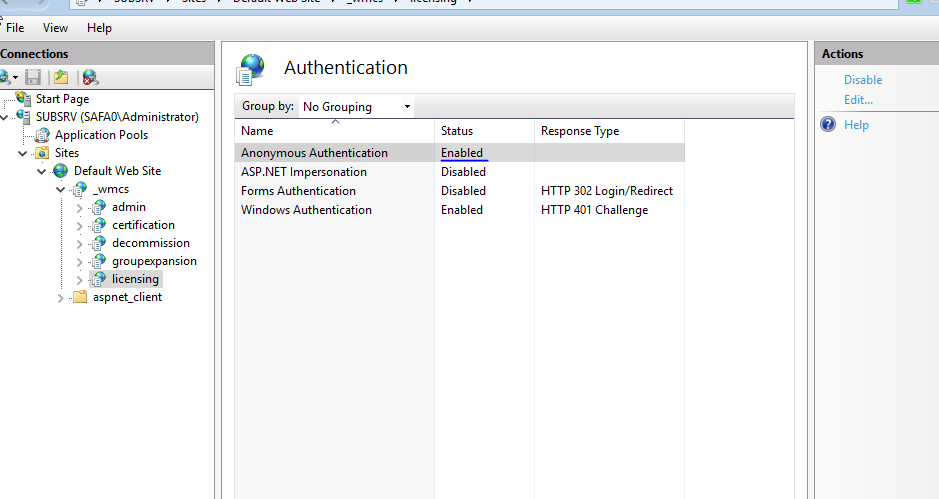
Anonymous Authentication bir web sitesinin genel alanlarını kullanıcı adı ve parola istemeden herkesin ziyaret etmesine izin verirken, yetkisiz kullanıcıların web sunucusunun önemli yönetici özelliklerine ve gizli bilgilere erişmesini engeller. İkinci özelliği kullanılacağı için Anonymous Authentication’u enable haline getirildi.



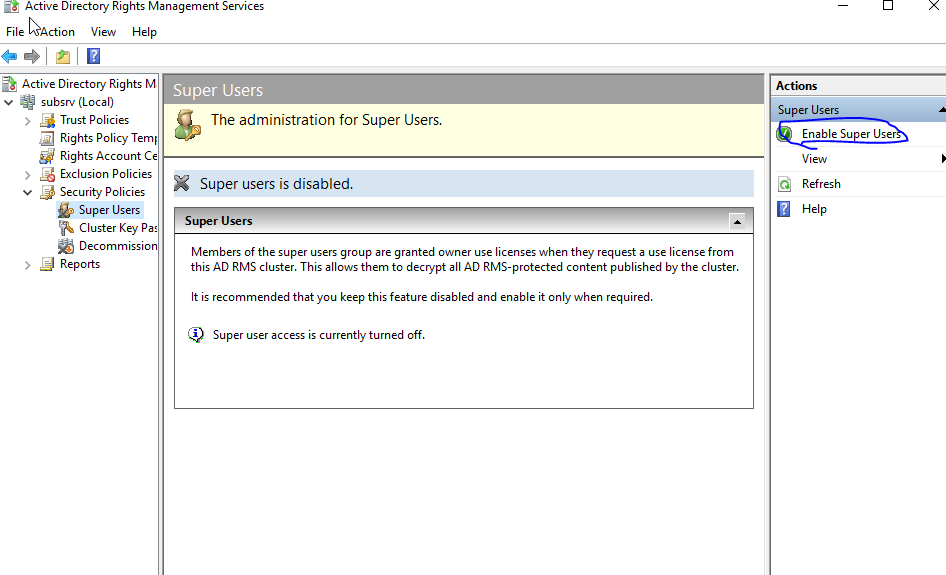
Aynı işlem licensing kısmından da yapıldı.



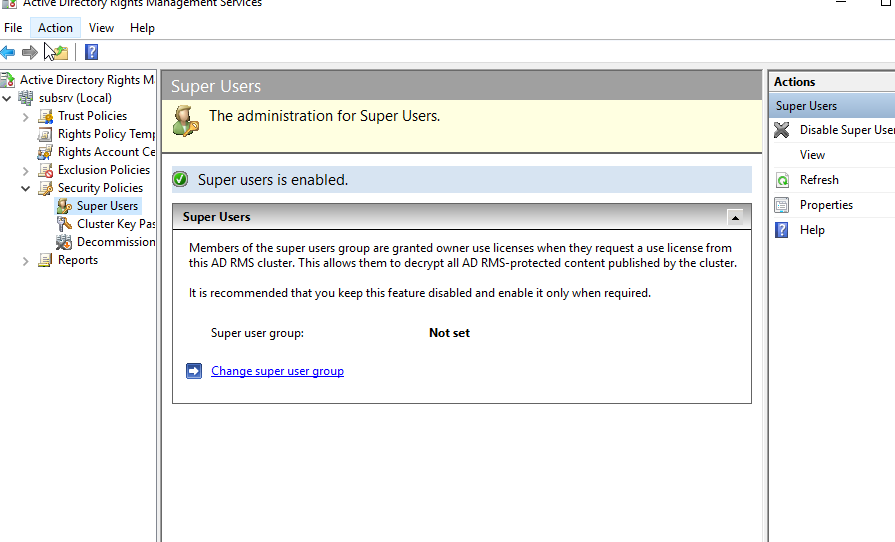
Bunu da enable yaptıktan sonra sign out yapıp tekrar oturum açmak gerekiyor.



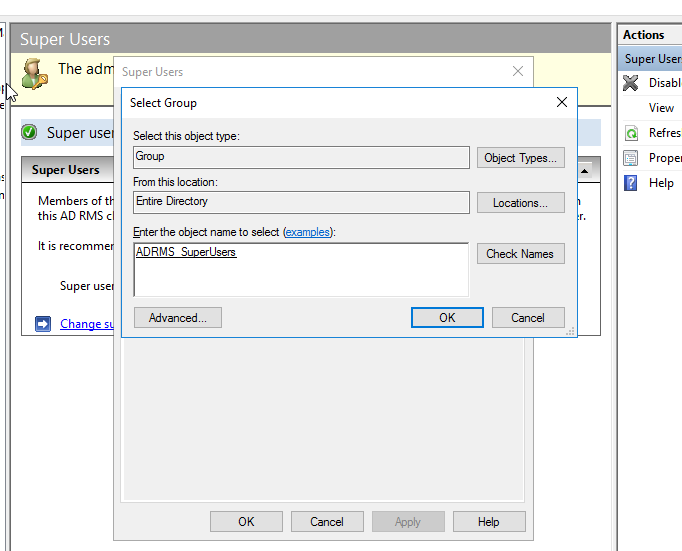
**SuperUsers,** sistemin tamamı üzerinde ve [ağ](https://wmaraci.com/nedir/ag) ya [da](https://wmaraci.com/nedir/da) [veritabanı](https://wmaraci.com/nedir/veritabani) gibi kritik bölgelerde kapsamlı değişiklikler yapma yetkisine sahip özel kullanıcı hesabıdır. Biz de bir tane Super User oluşturacağız. Bu sebeple Super Users aktif hale getirildi.



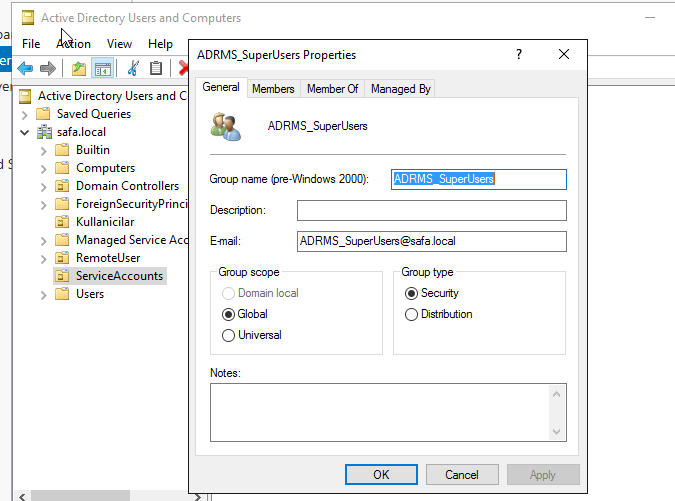
Super users grubu değiştirileceği için Change süper user group denildi.



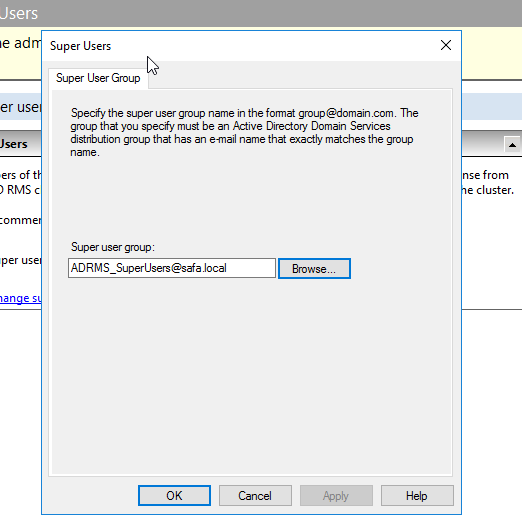
Daha önceden DC’de oluşturduğumuz grubu buraya ekliyoruz.



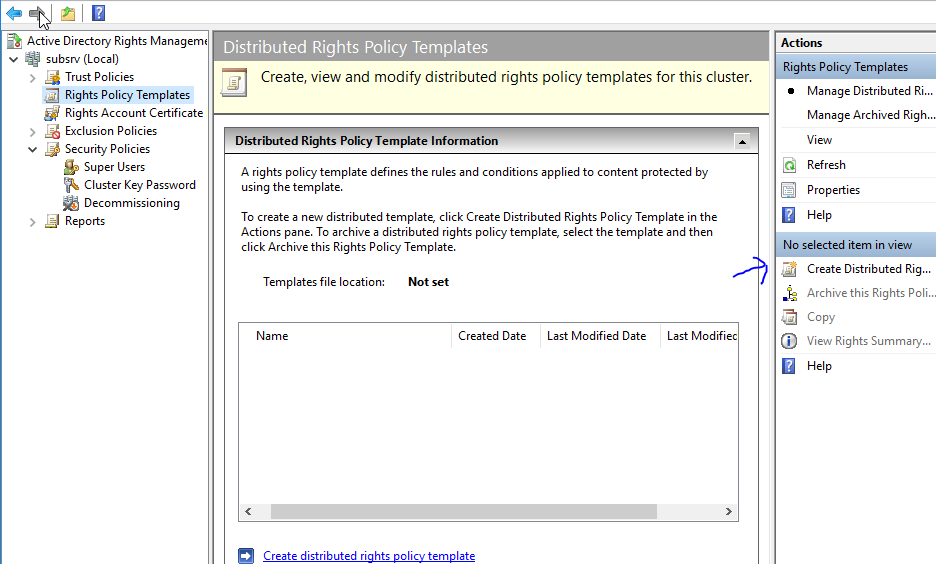
Hata verdiği için tekrar DC’ye gidip bu gruba bir E-mail adresi yazıldı.



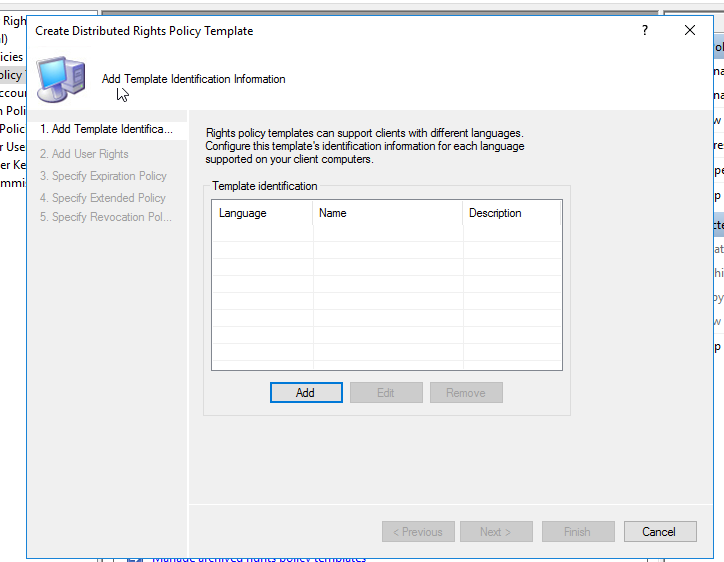
E-mail ekleyince hata vermeden geldi.



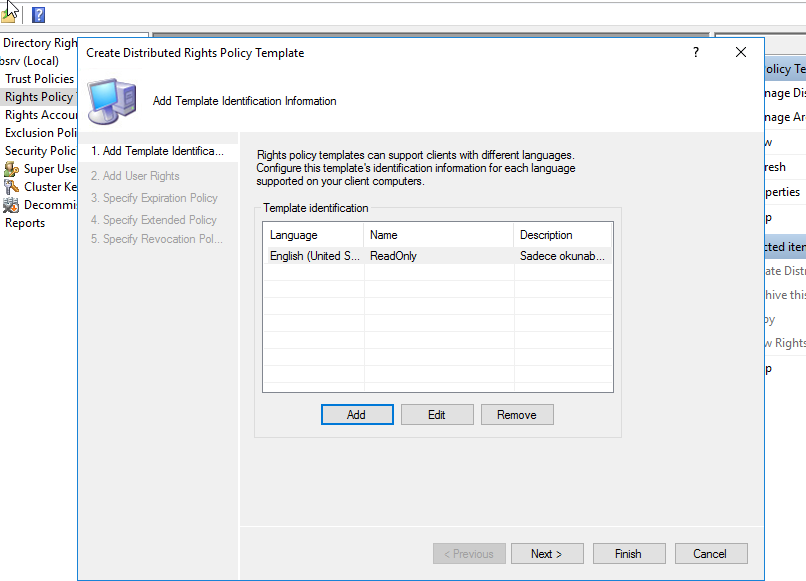
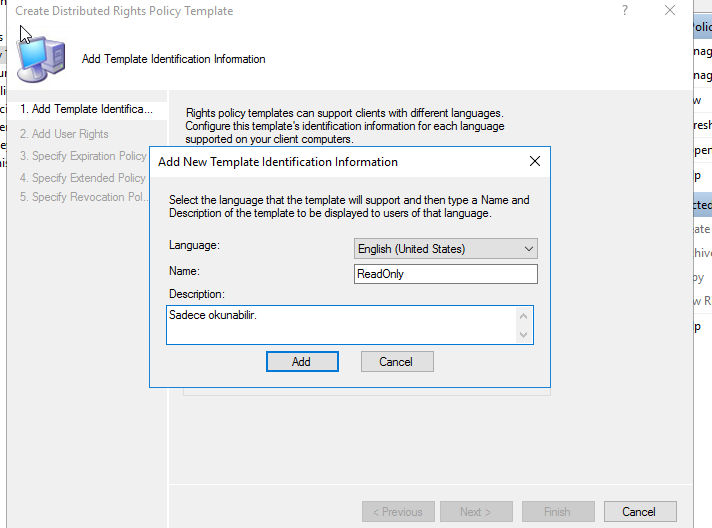
Distributed Rights Policy Template userların ya da grupların hakları korunan belli bir içerik ile ilgili yetkilerini kontrol eder. Biz de yeni bir Distributed Rights Policy Template oluşturacağız. Bu sebeple create denildi.



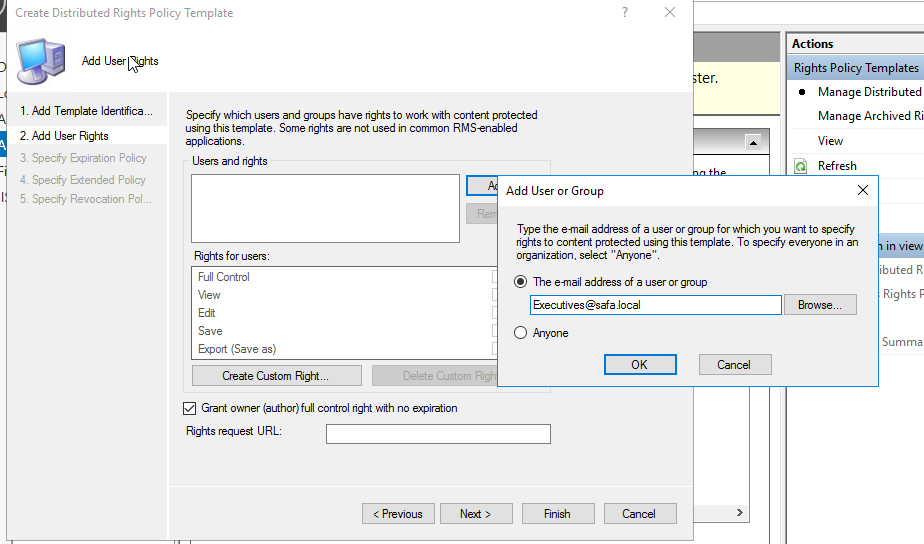
Add denildi.



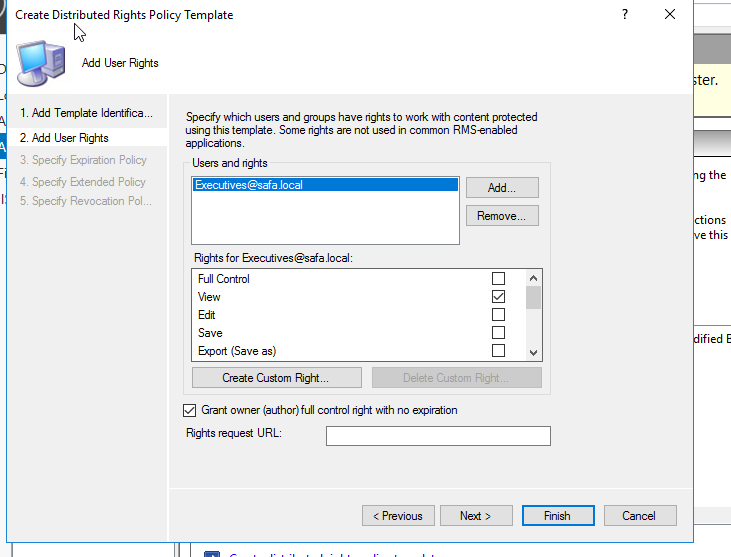
Dili seçildi ve bir isim girildi. İsmi ReadOnly yapıldı.



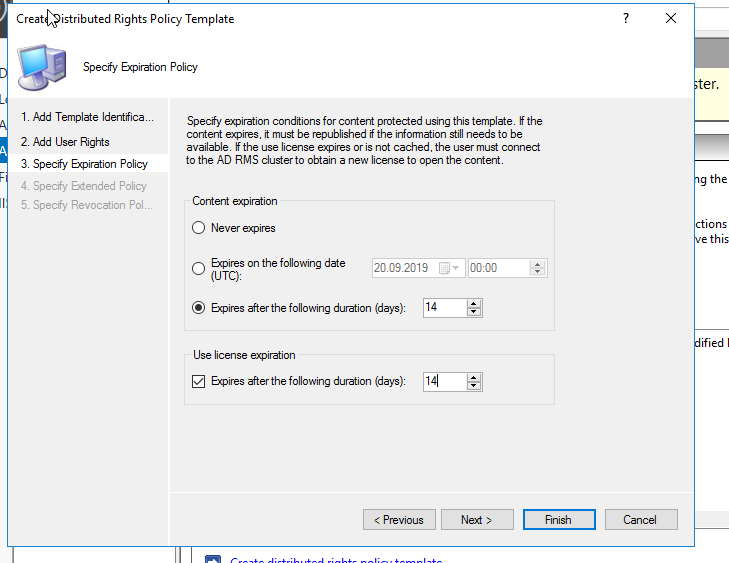
Next denilince karşımıza Right Policy’e grubumuzu ekleyeceğimiz kısım çıktı. Ekle denilip üç user’ımızın içinde olduğu grubu eklendi. Hata alınırsa daha önce yapıldığı gibi DC’den bu gruma E-mail adresi verilmesi gerekir.



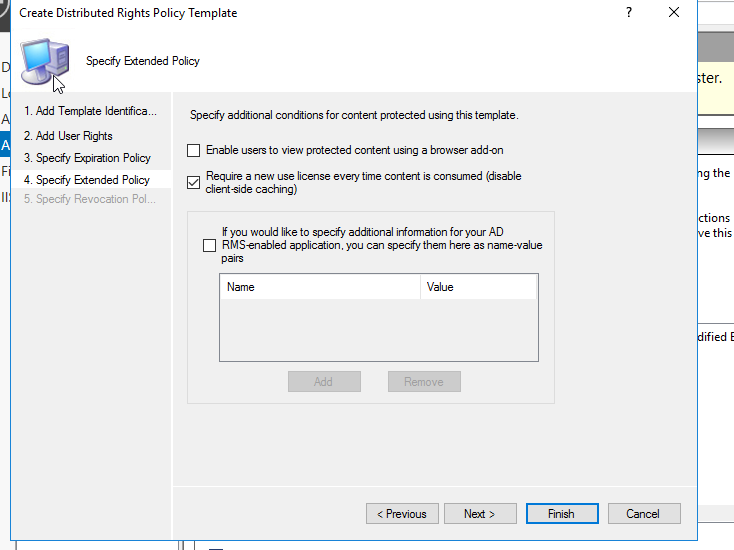
View özelliği verildi. Böylece bu gruba ait user’larda sadece okuma yetkisi olmuş oluyor.



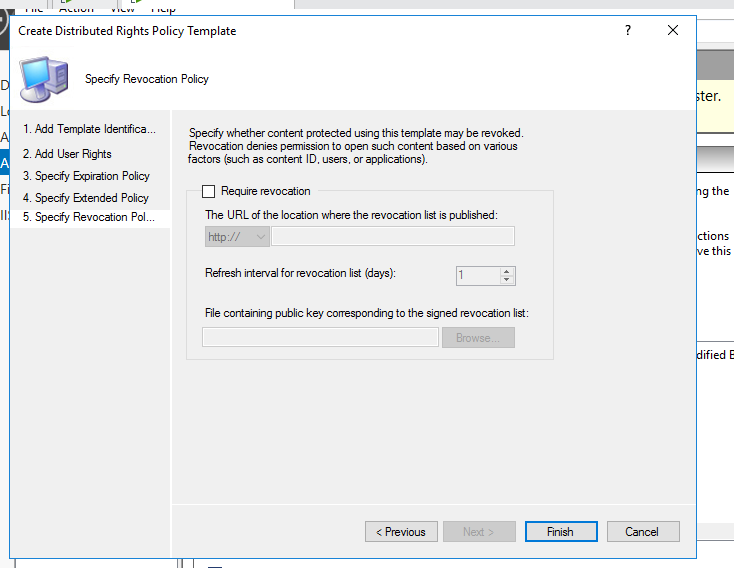
Bitiş süresi girildi.



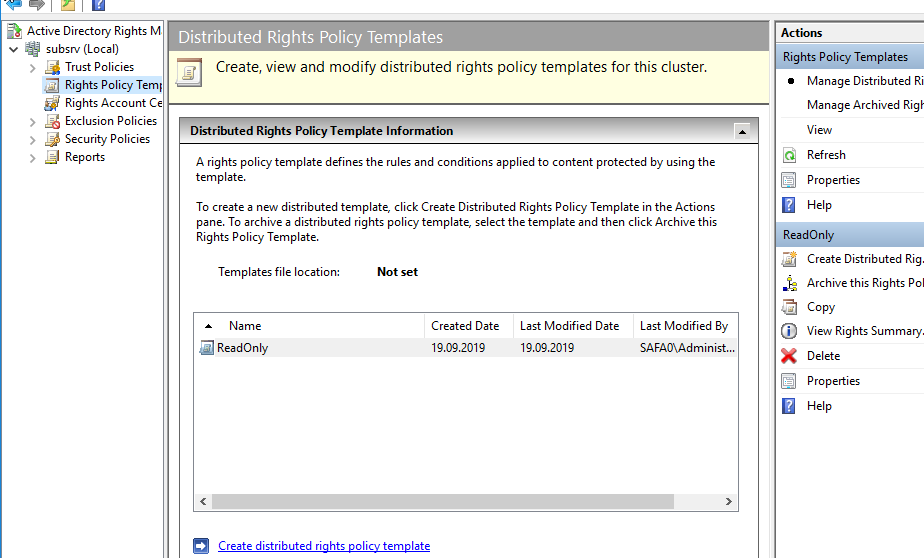
Her seferinde yeni lisans kullanılması gerektiği işaretlendi.



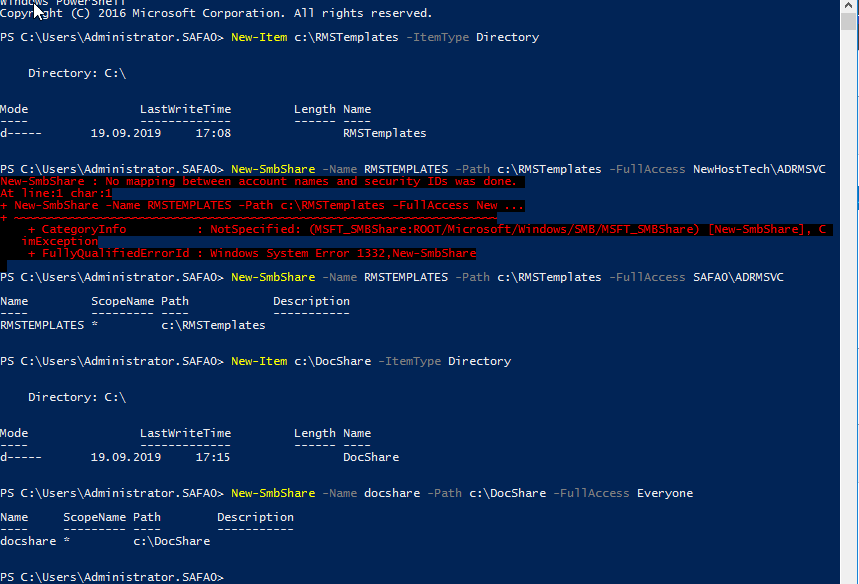
Ve bitirildi.



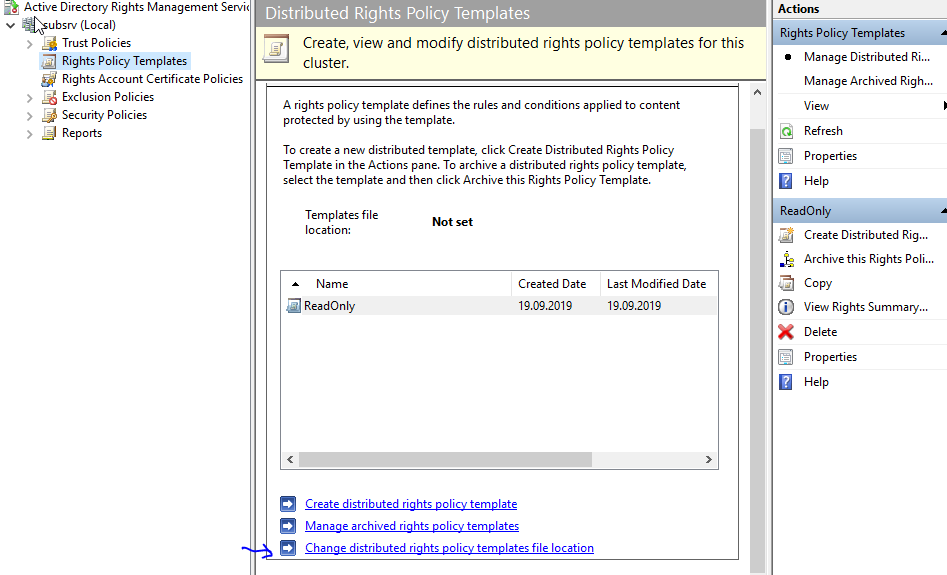
Template hazır.



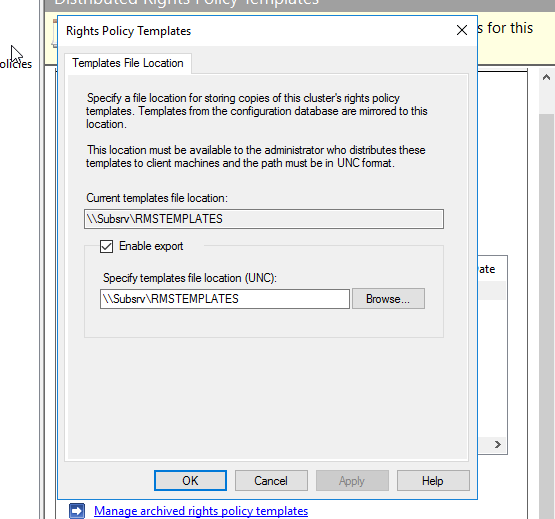
Gerekli powershell komutları yazıldı. RMSTEMPLATES ve DocShare diye 2 adet directory tipi klasör oluşturuldu. RMSTEMPLATES e sadece ADRMSVC kullanıcı için giriş izni, DocShare için herkese giriş izni verildi.



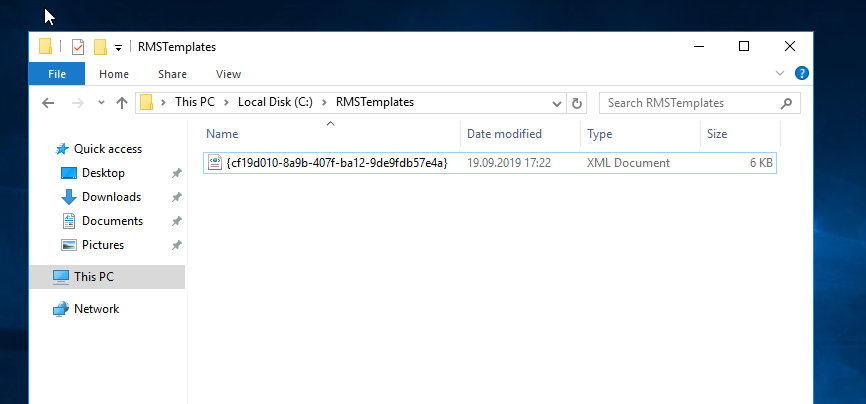
Daha önceden oluşturduğumuz Policy Template’in dosya konumunu değiştirmek için change denildi.



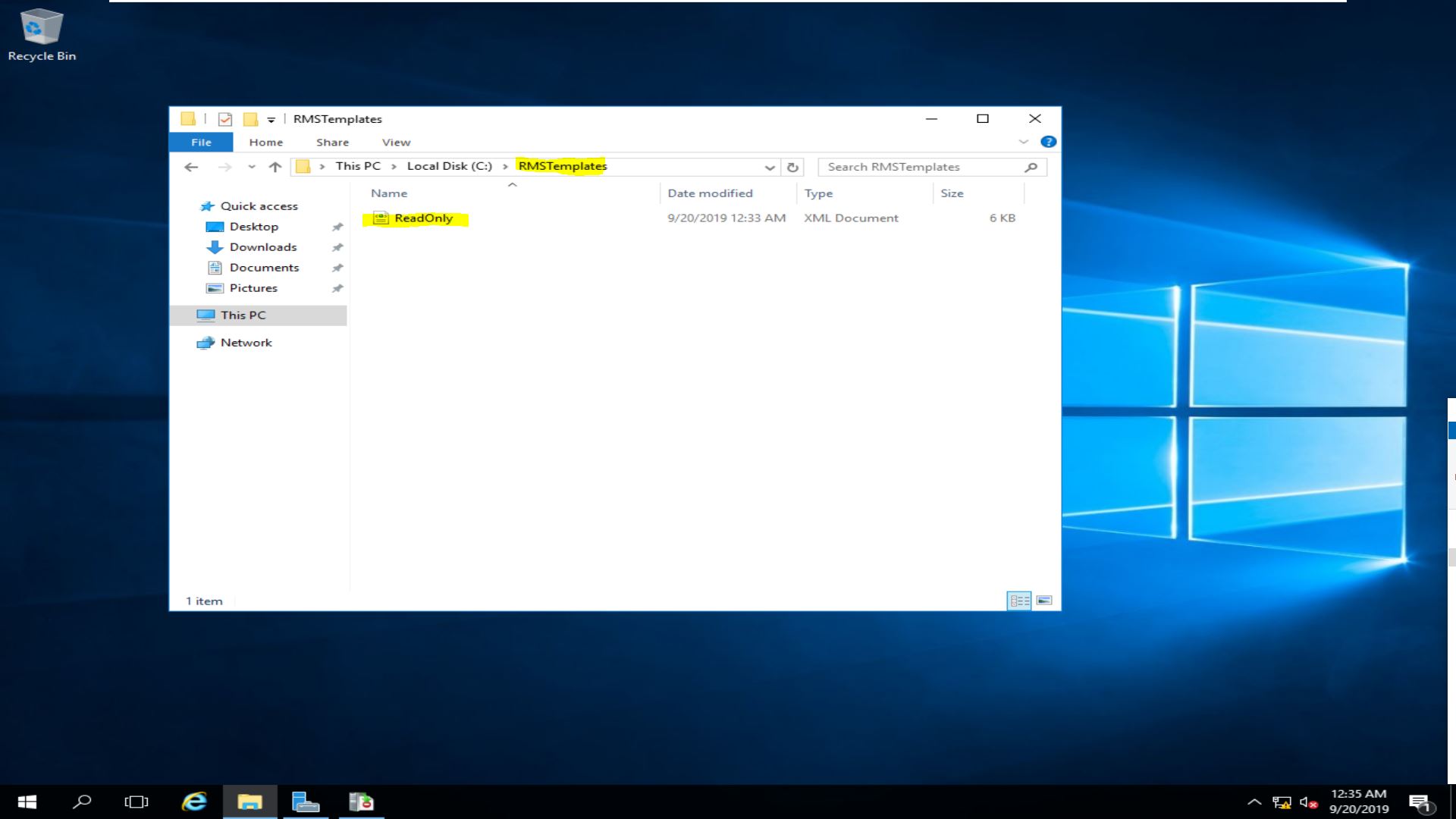
RMSTEMPLATES seçildi.



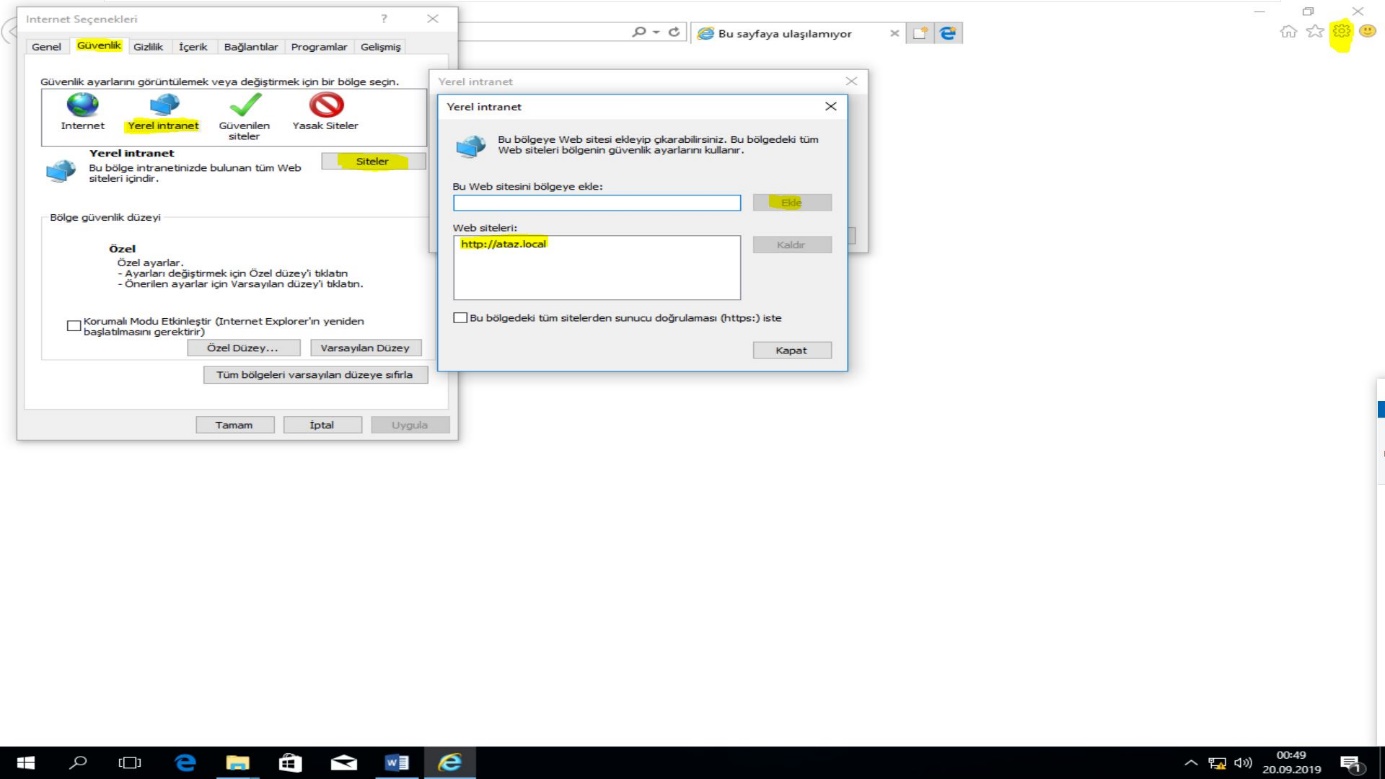
Policy template burada. Daha önce şöyle bir hata yapmıştık. AD RMS kurulurken safa.local yazılan yere ADRMS.safa.local yazılmalıydı. Yanlış yazıldığı için aşağıdaki gibi bir xml dökümanı geldi.



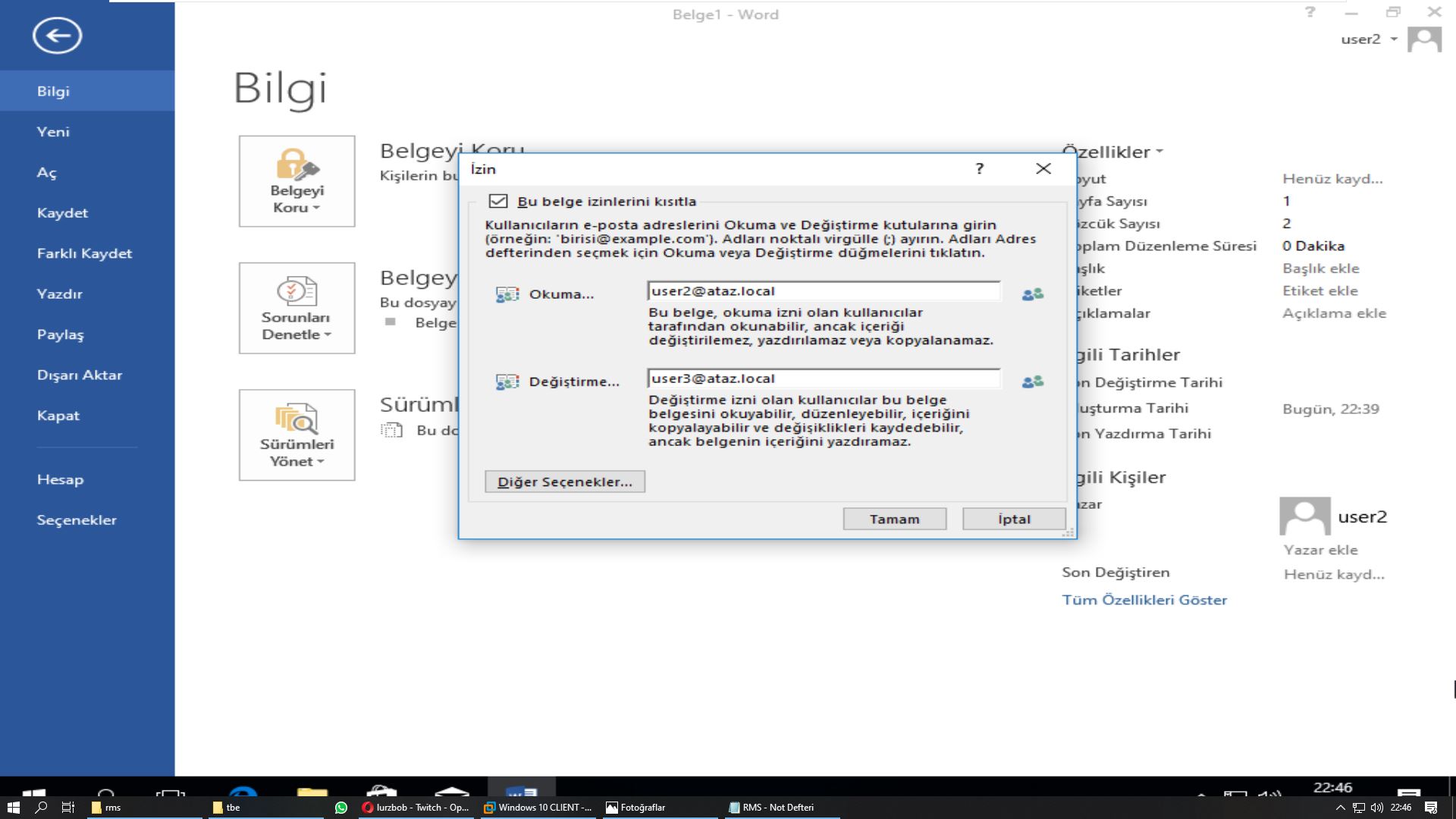
Doğru yani ADRMS.safa.local yazılsaydı ismini ReadOnly verdiğimiz için xml bu şekilde gelecekti.

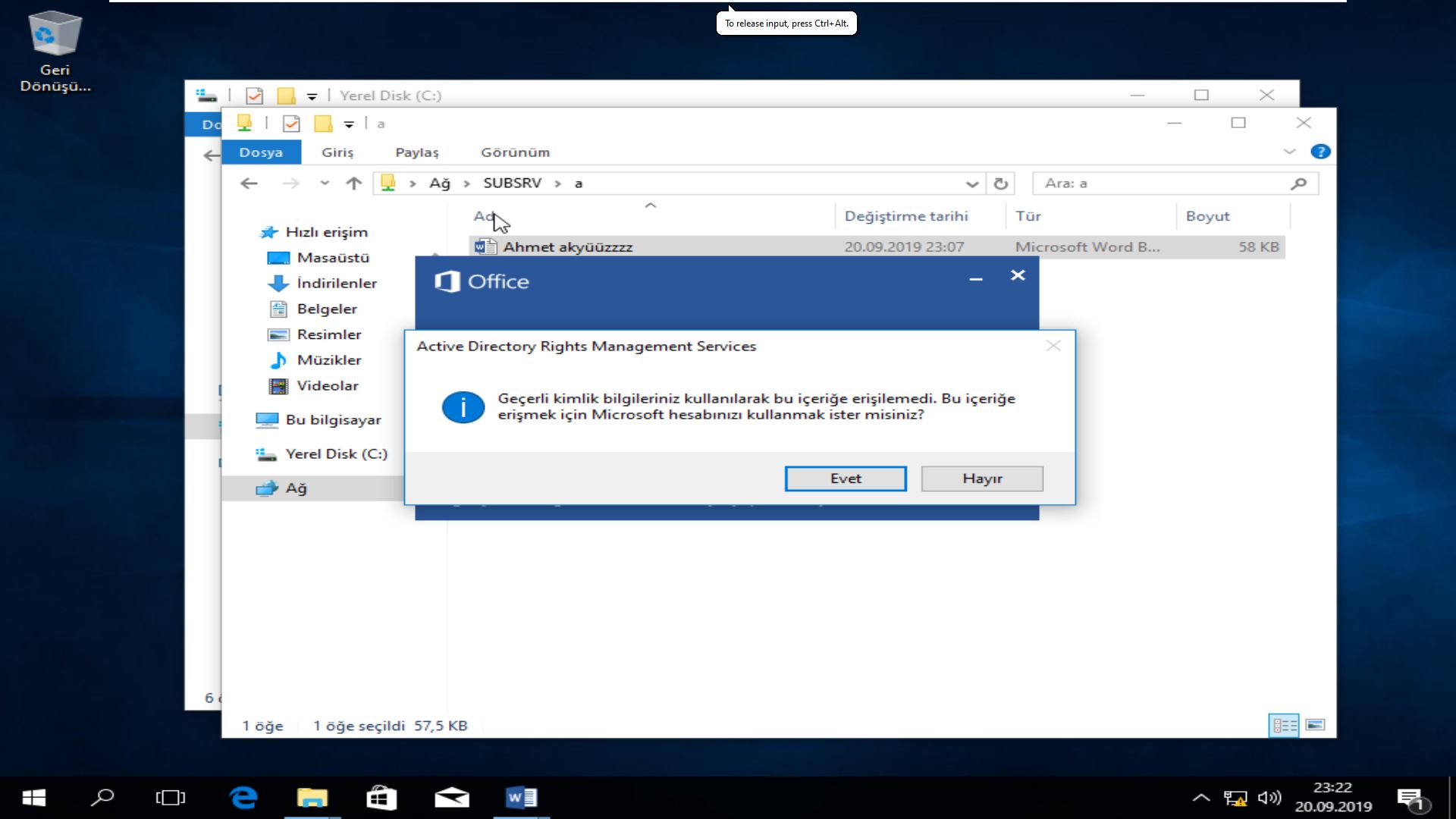


Daha sonra Internet Explorer’a girilerek internet seçeneklerinden yerel intranet seçildi ve sitelerden açılan pencereye gelişmişe tıklandı local’in ismi girildi. Bizde safa.local yazılacaktı.



Daha sonra user1 ile oluşturulan bir Word dosyasının içine yazı yazıldı. Belgeyi koru denildi. Erişimi kısıtla seçildi. User2 kullanıcısına izin verildi.





Ve user2 kendi oturumundan Word dosyasına sadece okuma yetkisiyle giriş yaptı.

