

Active Directory

Right Management Services

LABORATUVAR RAPORU

MİDYA ŞOLA

AHMET AKYÜZ

1.Active Directory Right Management Services Hakkında Bilgi

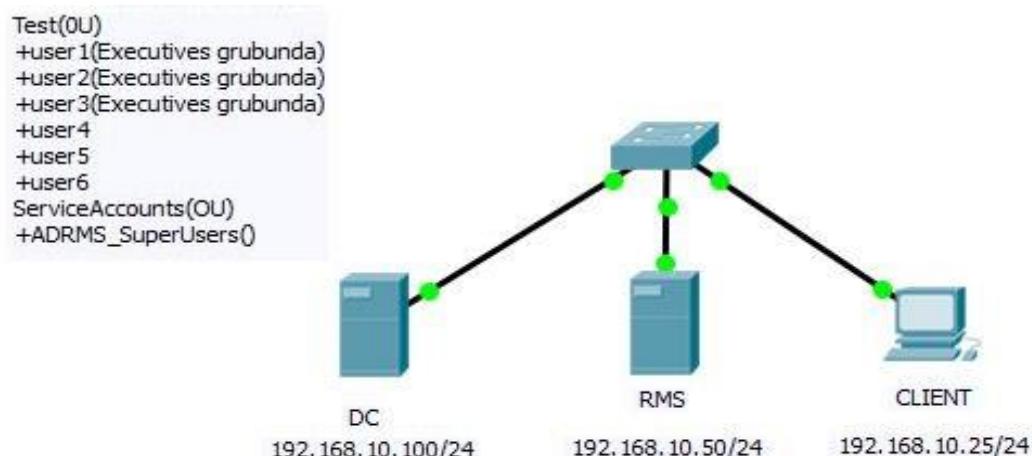
Active Directory Rights Management Services (AD RMS), önemli bilgilerin korunması. Kelime işlemciler, e-posta istemcileri ve sektörel uygulamalar önemli bilgilerin korunmasında yardımcı olmak üzere AD RMS'yi kullanabilir. Kullanıcılar bilgiyi kimlerin açabileceğini, değiştirebileceğini, yazdırabileceğini, iletebileceğini veya diğer işlemleri yapabileceğini tanımlayabilirler. Kuruluşlar “gizli – salt okuma amaçlı” gibi doğrudan bilgiye uygulanabilecek, özel kullanım ilkesi şablonları oluşturabilir.

Kalıcı koruma. AD RMS kullanım haklarını belgenin içine kilitleyerek ve bilginin uygun alıcılar tarafından açıldıktan sonra bile nasıl kullanılacağını denetleyerek, var olan güvenlik duvarları ve erişim denetim listeleri (ACL) gibi çevresel güvenlik çözümlerini güçlendirir.

Esnek ve özelleştirilebilir teknoloji. Bağımsız yazılım satıcıları (ISV) ve uygulama geliştiricileri her tür uygulamayı AD RMS kullanır hale getirebilir veya Windows'da ya da diğer işletim sistemlerinde çalışan içerik yönetim sistemleri veya portal sunucuları gibi diğer sunucuların, önemli bilgilerin korunmasına yardımcı olmak için AD RMS ile birlikte çalışmalarını sağlayabilirler. ISV'ler bilginin korunması işlevini belge ve kayıt yönetimi, e-posta ağ geçitleri ve arşiv sistemleri, otomatik iş akışları ve içerik incelemeleri gibi sunucu tabanlı çözümlerle tümlüşük hale getirebilirler.

AD RMS, kuruluşların güvenilir bilgi koruma çözümleri oluşturmalarına yardımcı olmak üzere geliştirici araçları ve endüstride kullanılan şifreleme, sertifika ve kimlik doğrulama gibi güvenlik teknolojileri sağlar. Özel AD RMS çözümleri oluşturmak için bir AD RMS yazılım geliştirme seti (SDK) vardır.

2. TOPOLOJİ

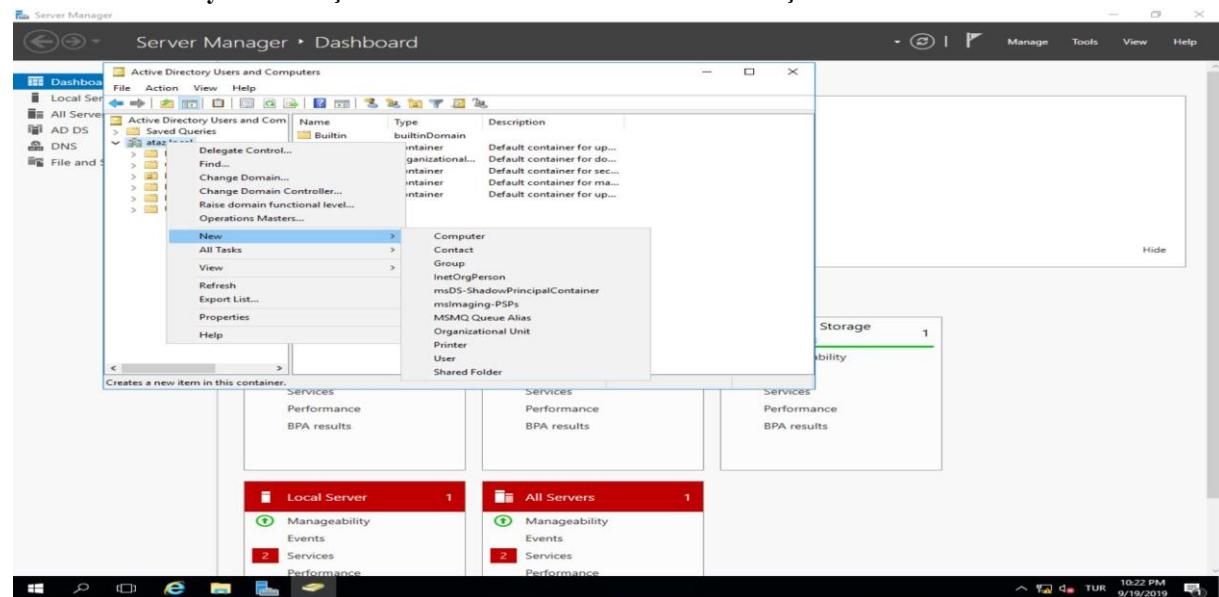


3. İŞLEM BASAMAKLARI

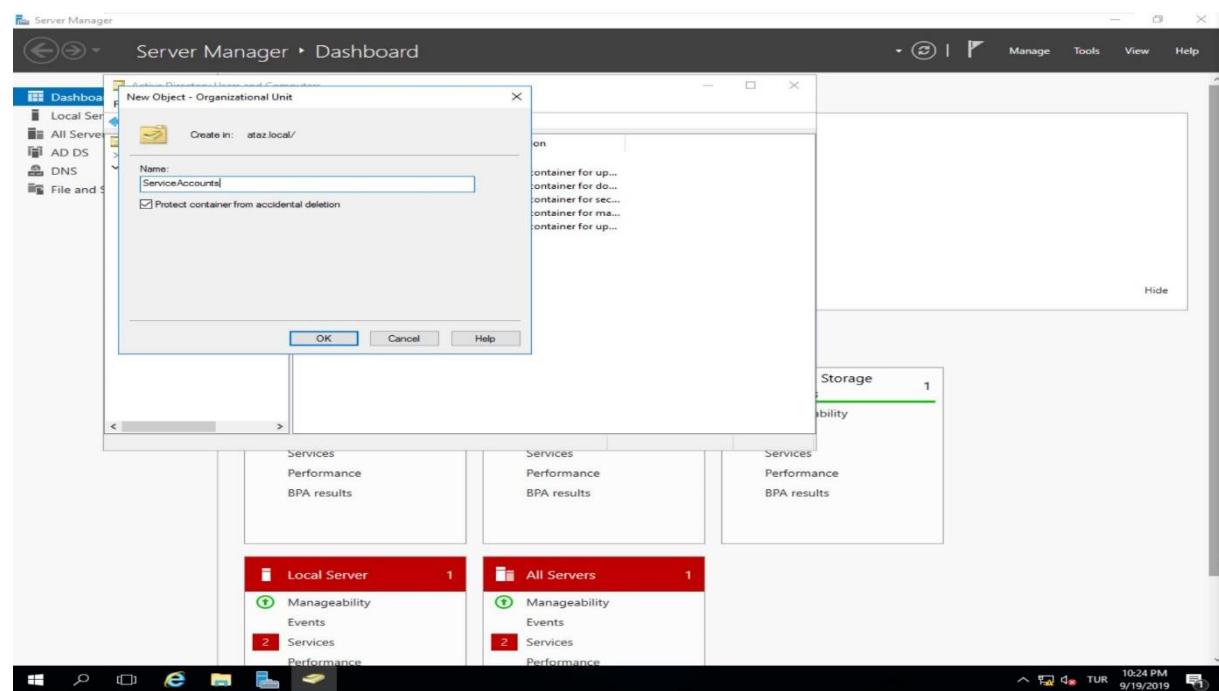
- 1.DC,RMS ve Client'e statik olarak ip ataması yapılır.
- 2.DC'ye Active Directory Domain Services kurulur ve Client ve RMS oluşturulan domainlere katılır.
- 3.DC üzerinde ServiceAccounts isimli bir OU oluşturulur. OU'nun içinde ADRMSVC isimli bir kullanıcı hesabı oluşturulur.Test etmek için Yeni bir OU oluşturulup içine kullanıcılar eklendi.
- 4.RMS Server'a Active Directory Right Management Service rolünü yükledim ve konfigürasyonu yapıldı.
5. Internet Information Services (IIS)'dan Sites-vmcs işlemleri yapıldı.
6. Active Directory Rights Management Services'dan eklediğim grupper aktif haline getirildi.
- 7.PowerShell'den Rights Policy Template Distribution konfigurasyonunu yapıldı.
- 8.Test yapmak için İnternet ayarları ve dosya işlemleri yapıldı.

4.PROJE ADIMLARI

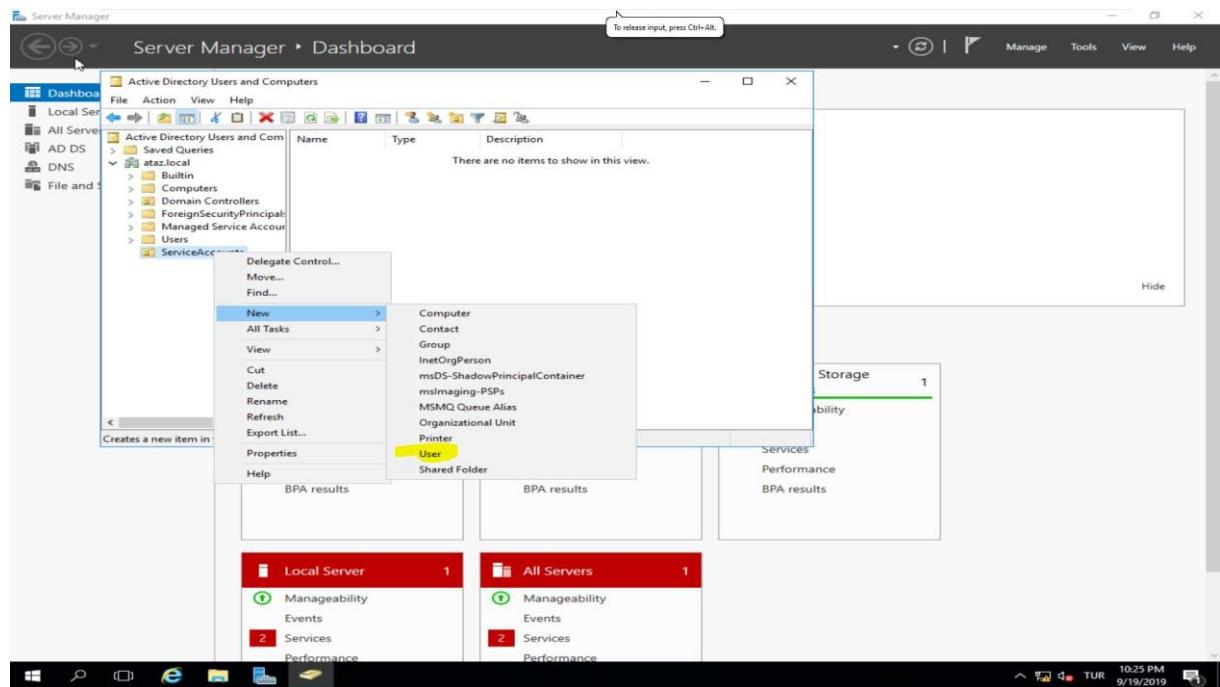
1. RMS servisini yönetmek için “ServiceAccounts” isimli bir OU oluşturdu.



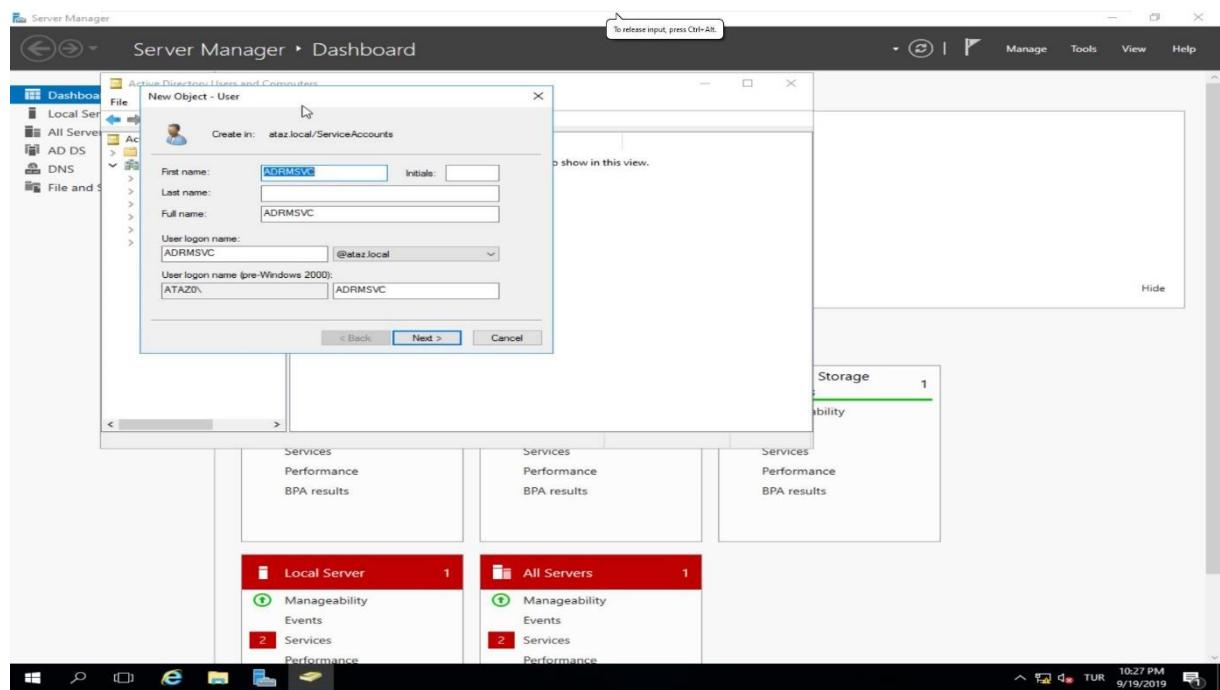
2.



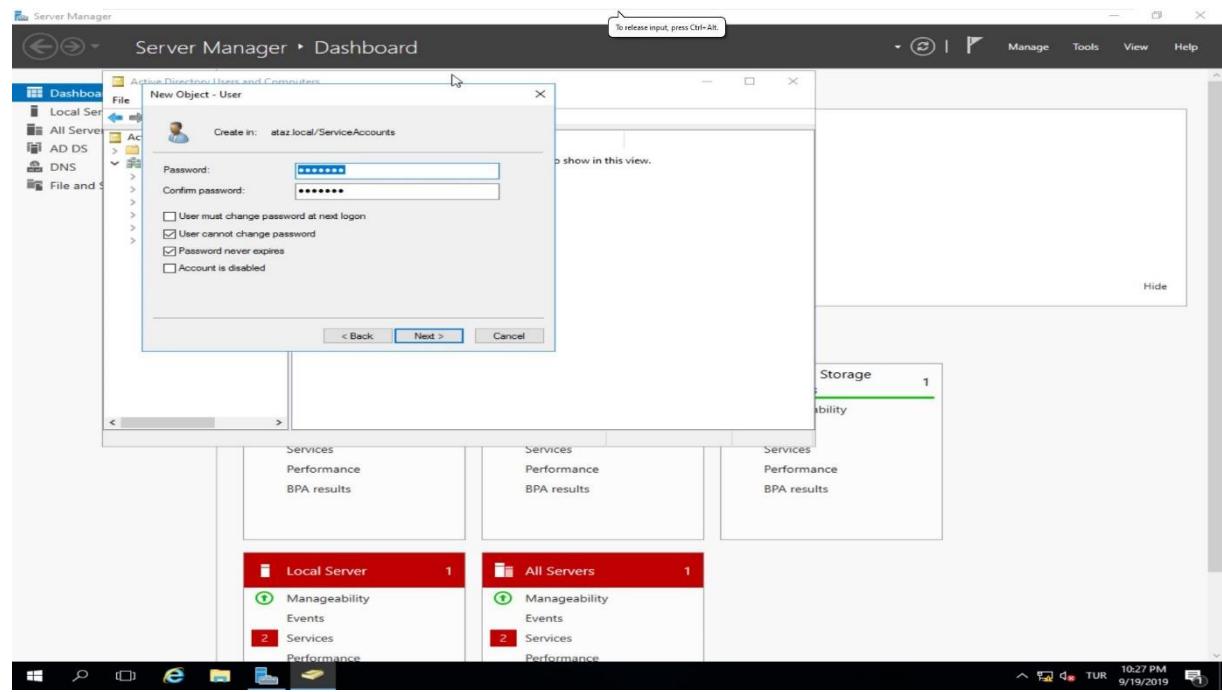
3. Bu OU nun içinde “AD RMSVC” isimli bir kullanıcı hesabı oluşturdu.



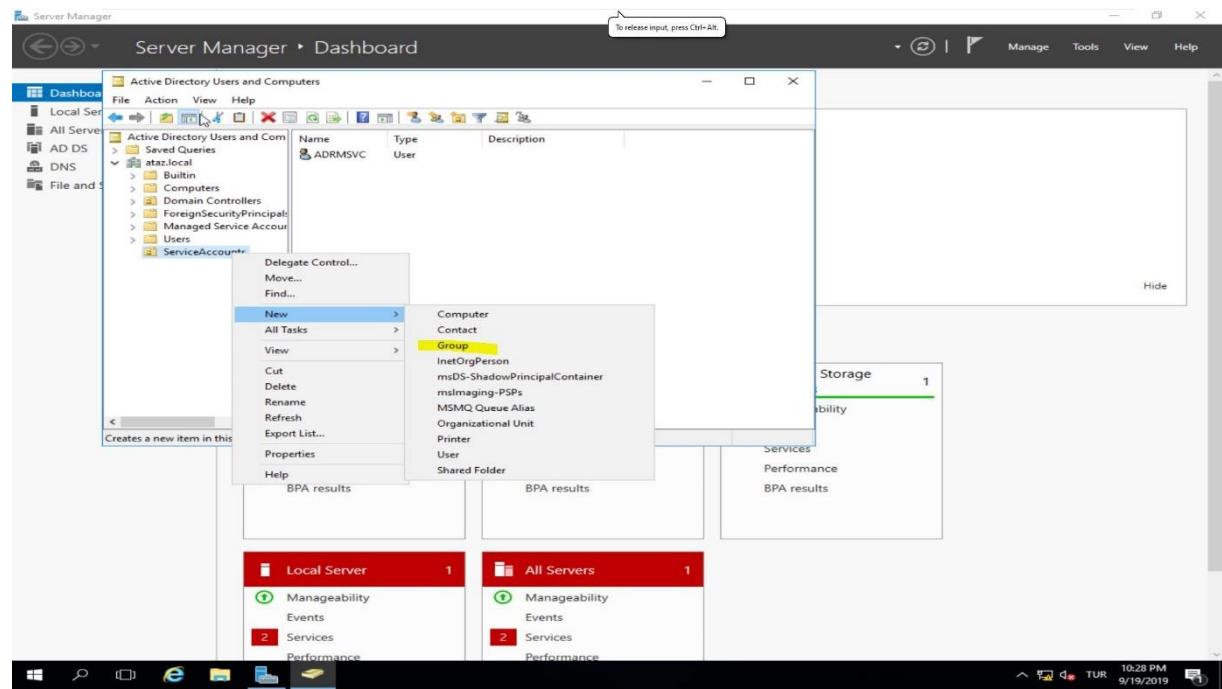
4.



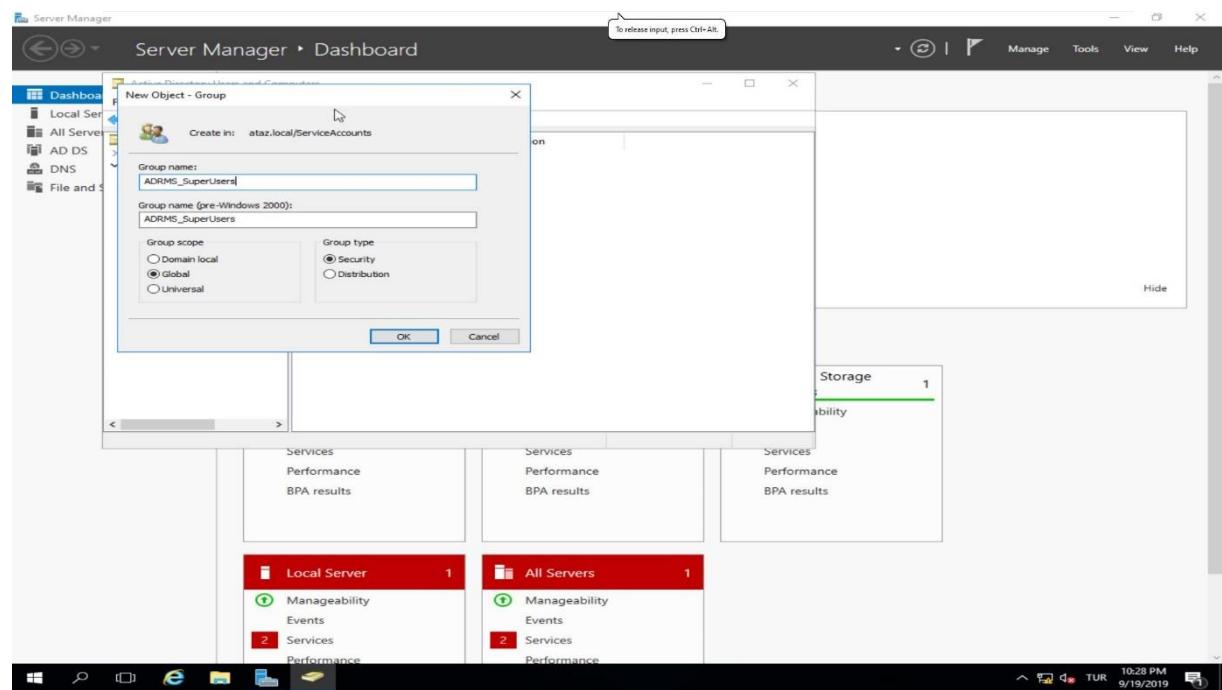
5.



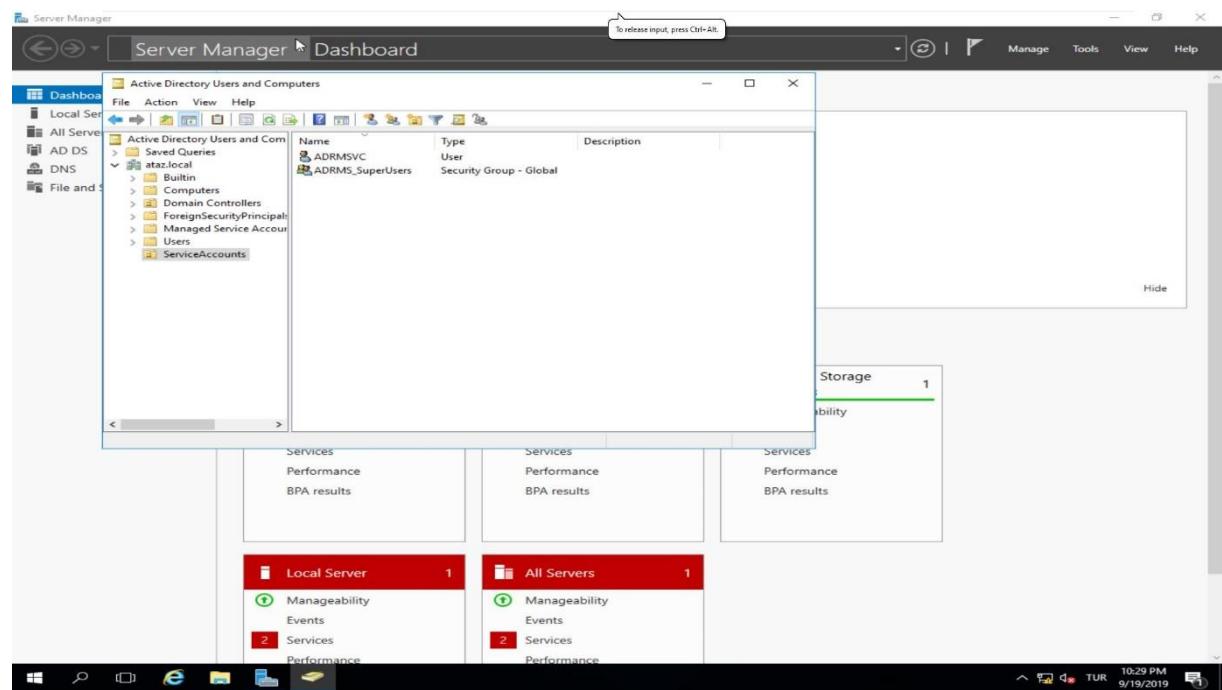
6. "ServiceAccounts" OU içinde "ADRMS_SuperUsers" grubu oluşturdu.



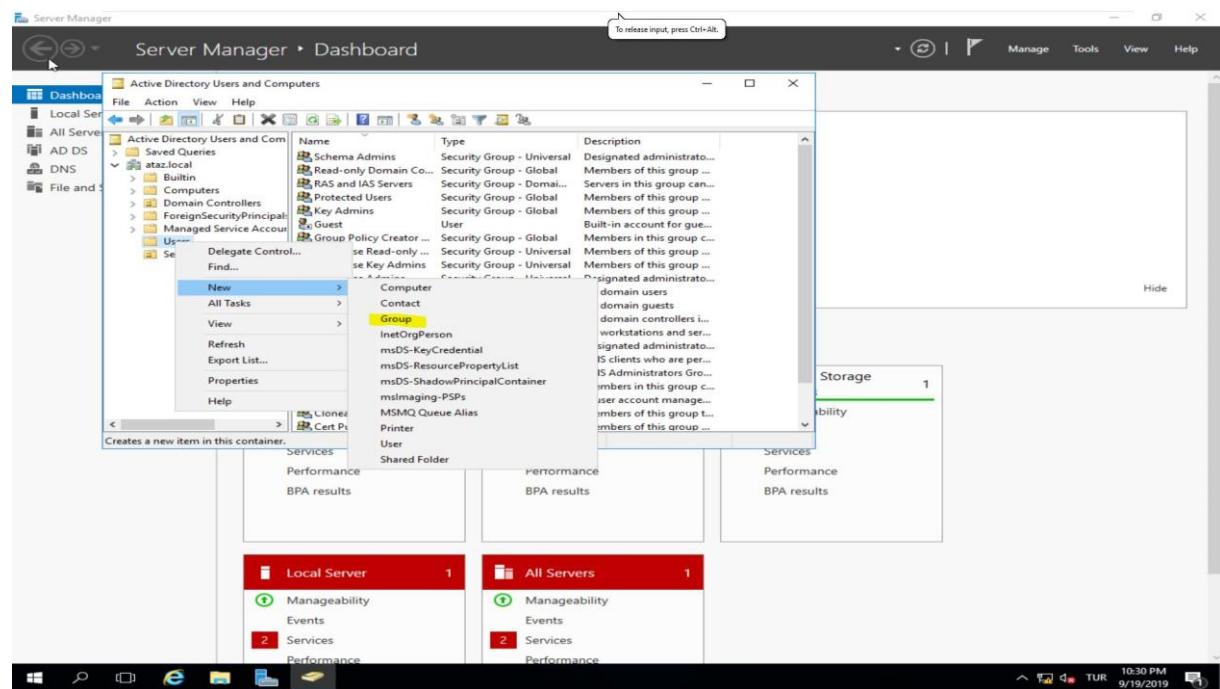
7.



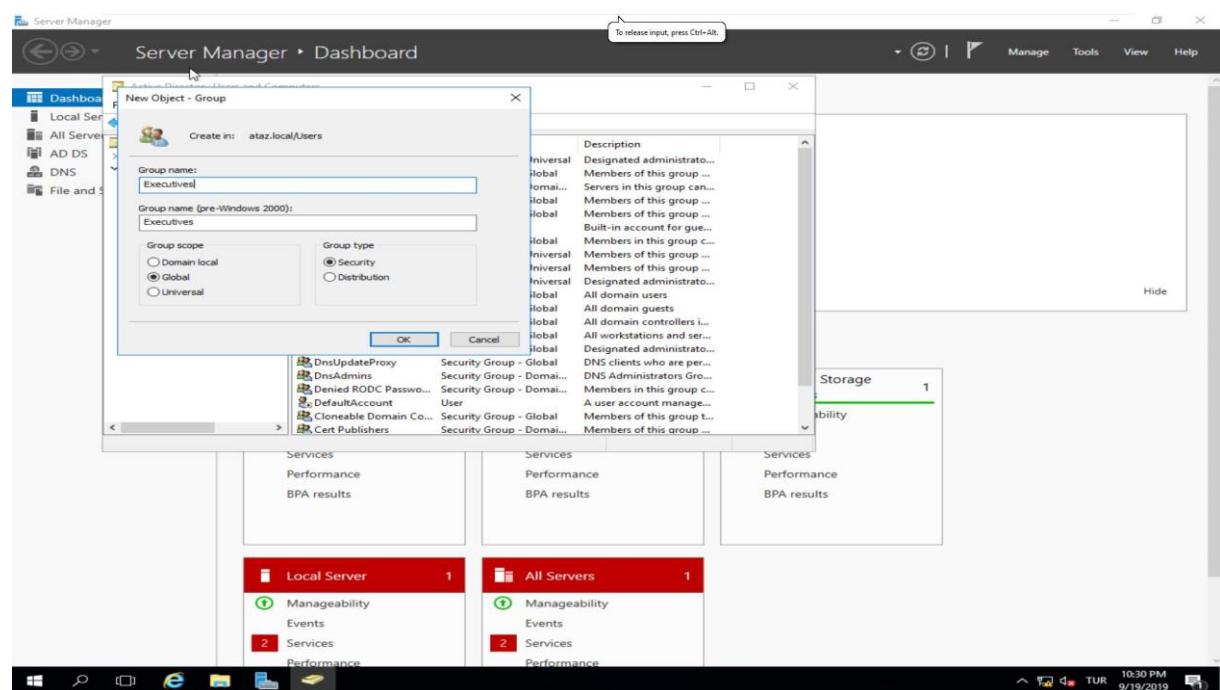
8.



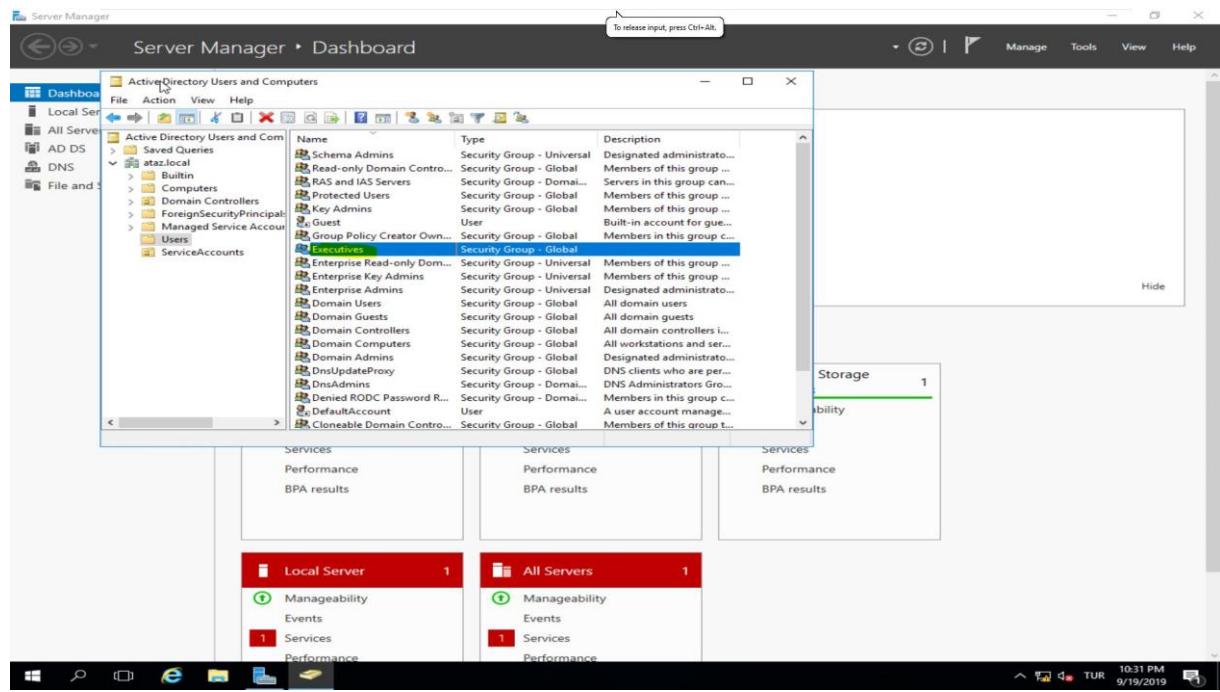
9. "Users" container içinde "Executives" isimli bir grup oluşturuldu.



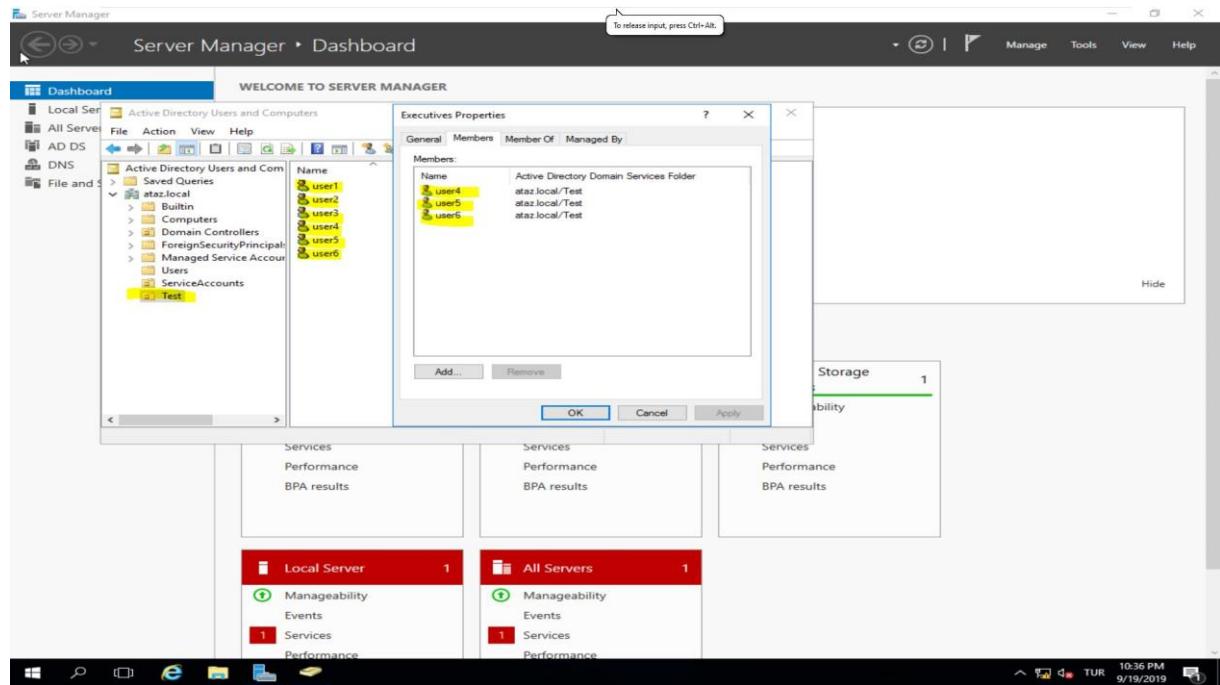
10.



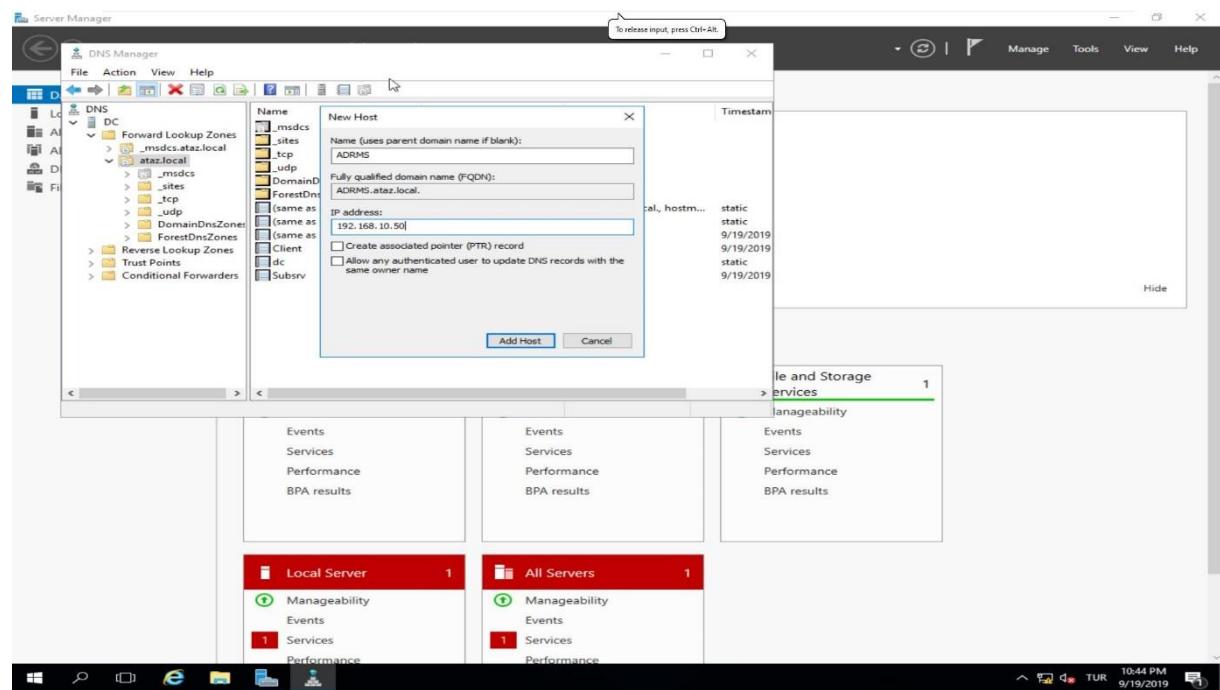
11.



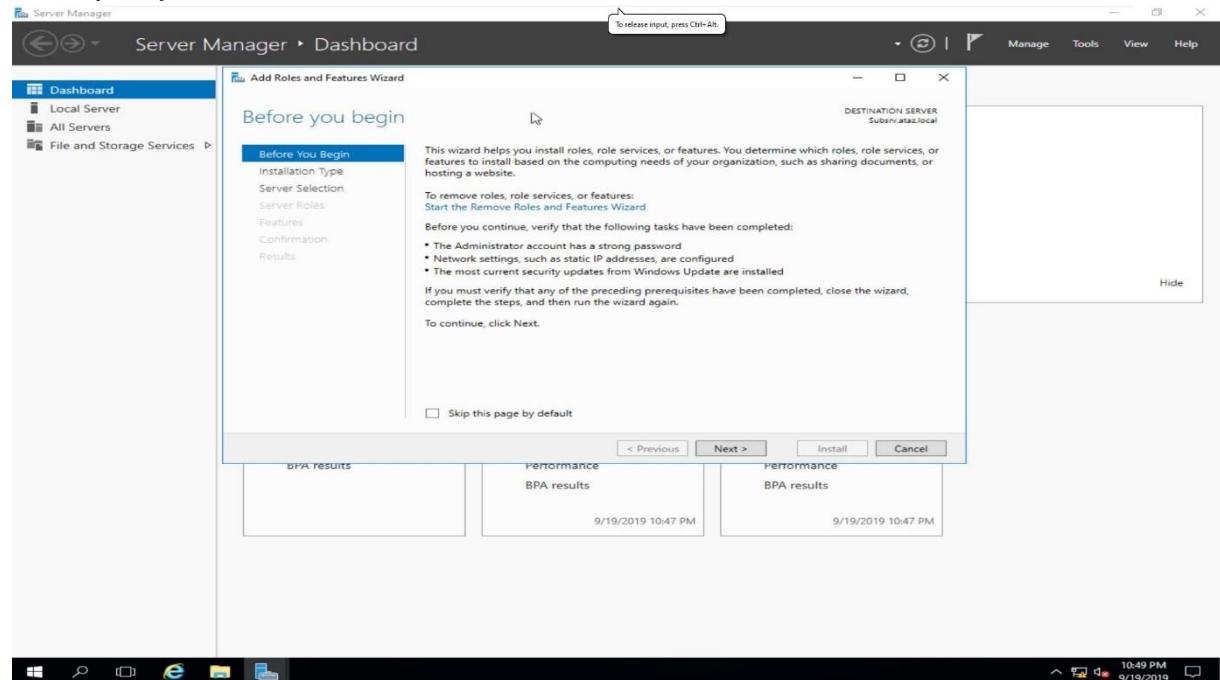
12. Test için “Test” adında OU oluşturulup ve içinede 6 kullanıcı oluşturulup “Executives” gruba 3 tanesini ekleydik.



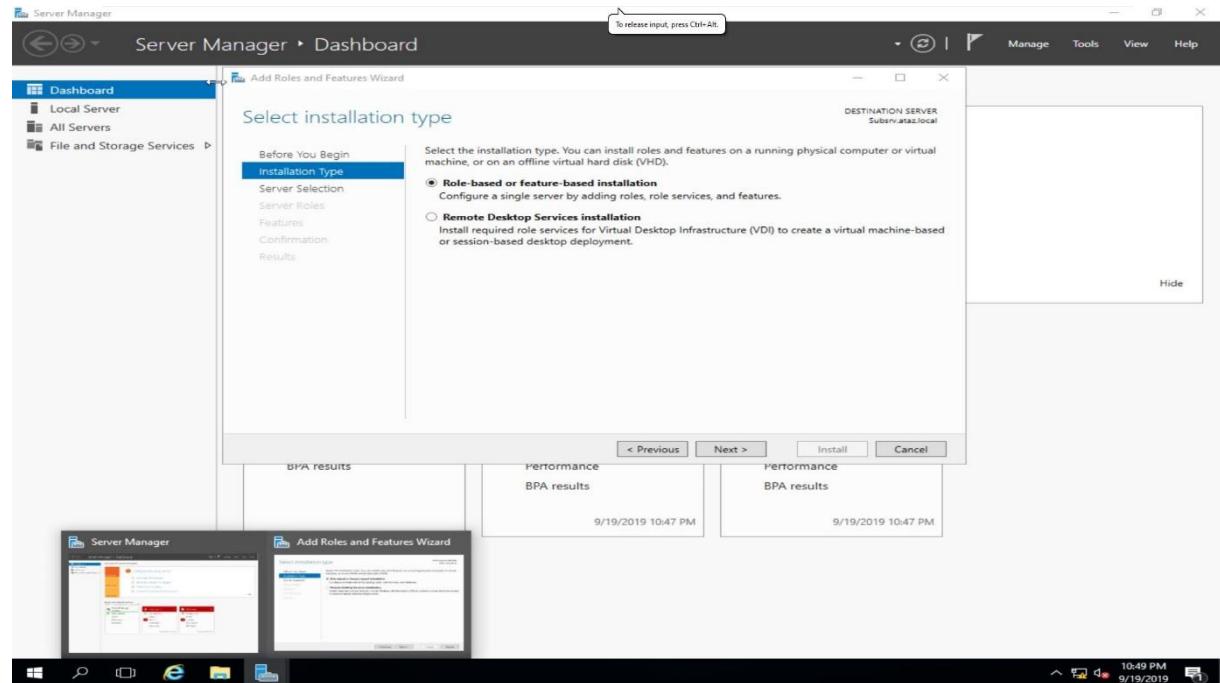
13. DC üzerinde Subsrv(RMS bilgisayar adı ip(192.168.10.50) si ile ADRMS adında bir A kaydı oluşturdu.



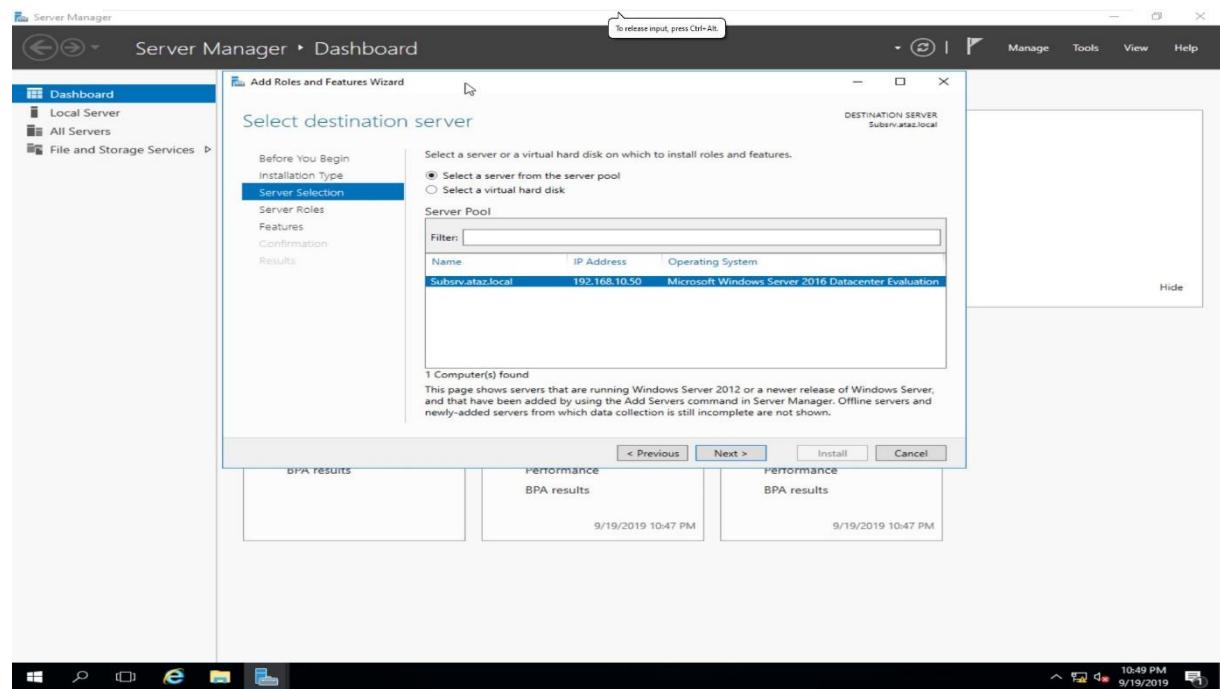
14. Subsrv üzerinde domain controller olarak oturum açıp "Active Directory Right Management Service" rolünü yükleyelim.



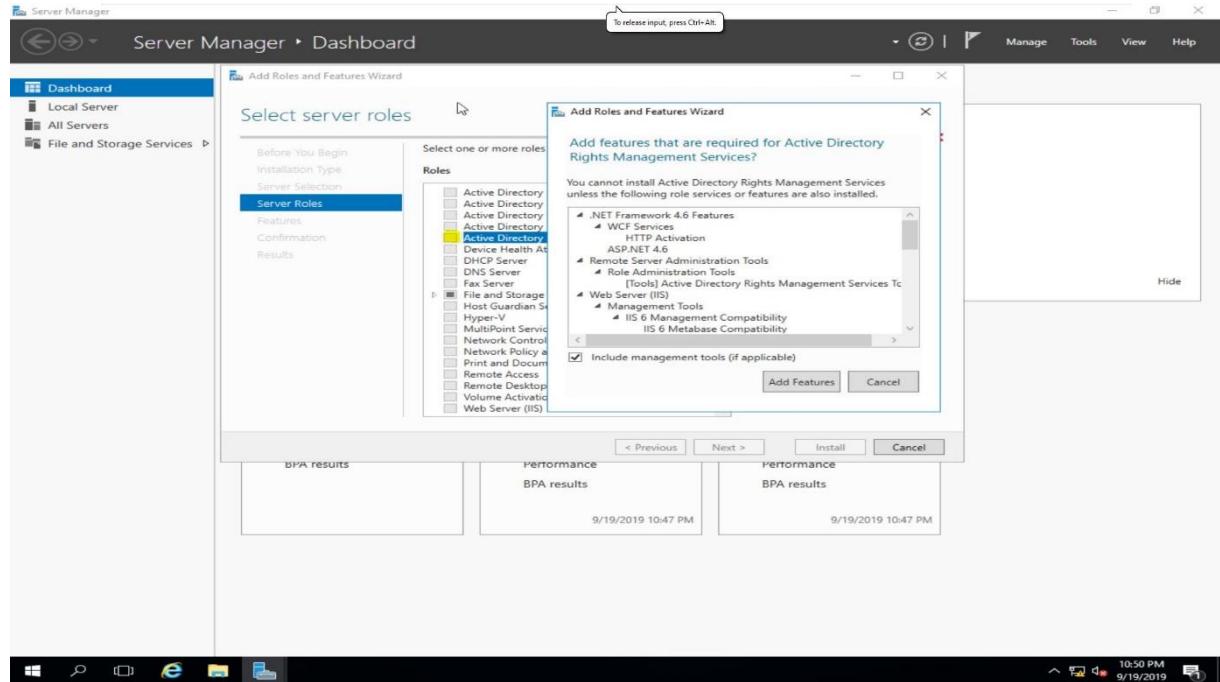
15.Yükleme tipini seçiyoruz.



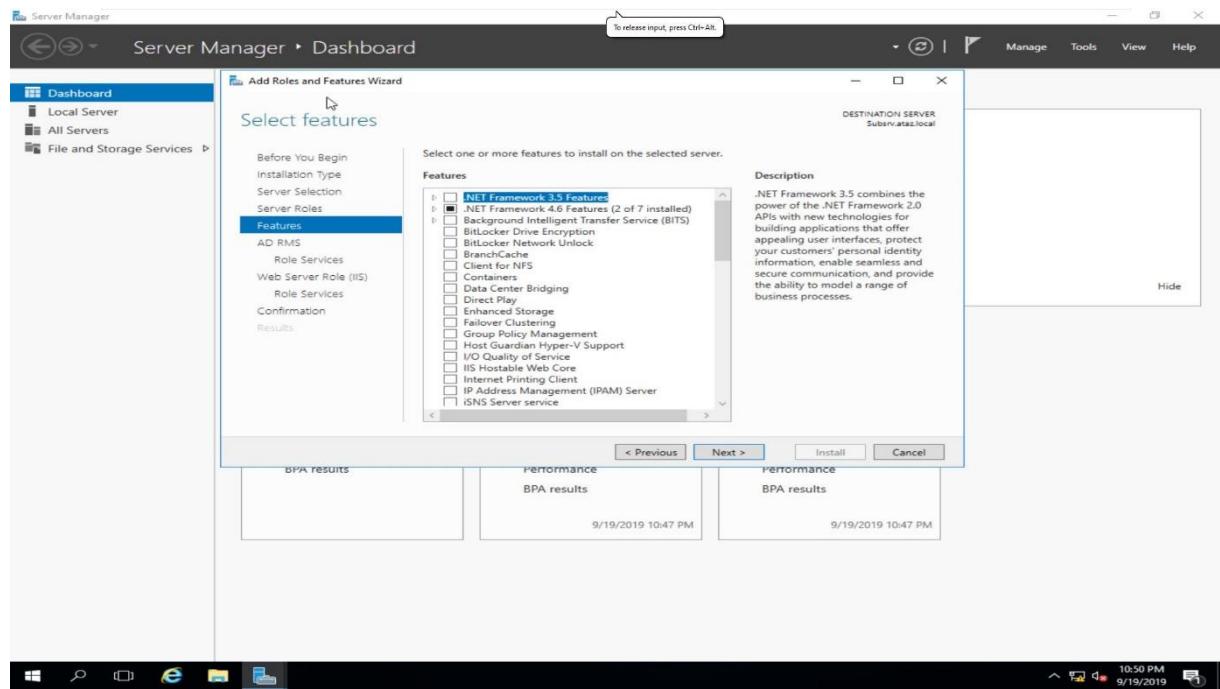
16.



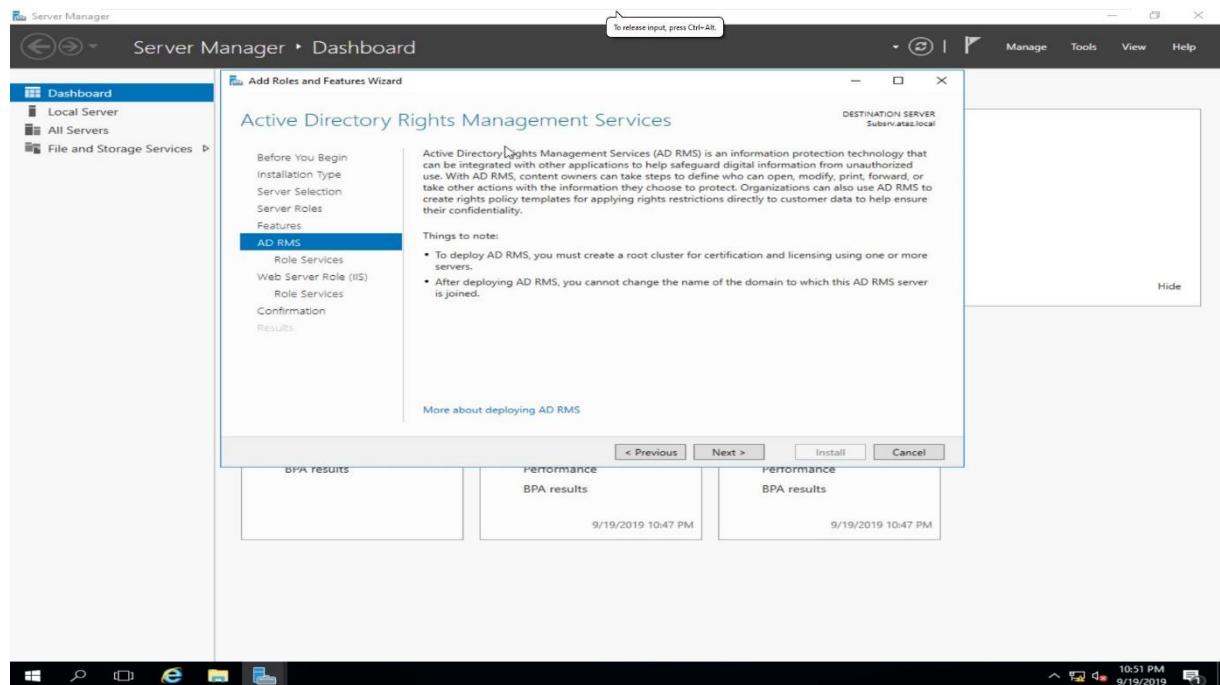
17. Listededen "Active Directory Right Management Service" rolünü seçiyoruz.



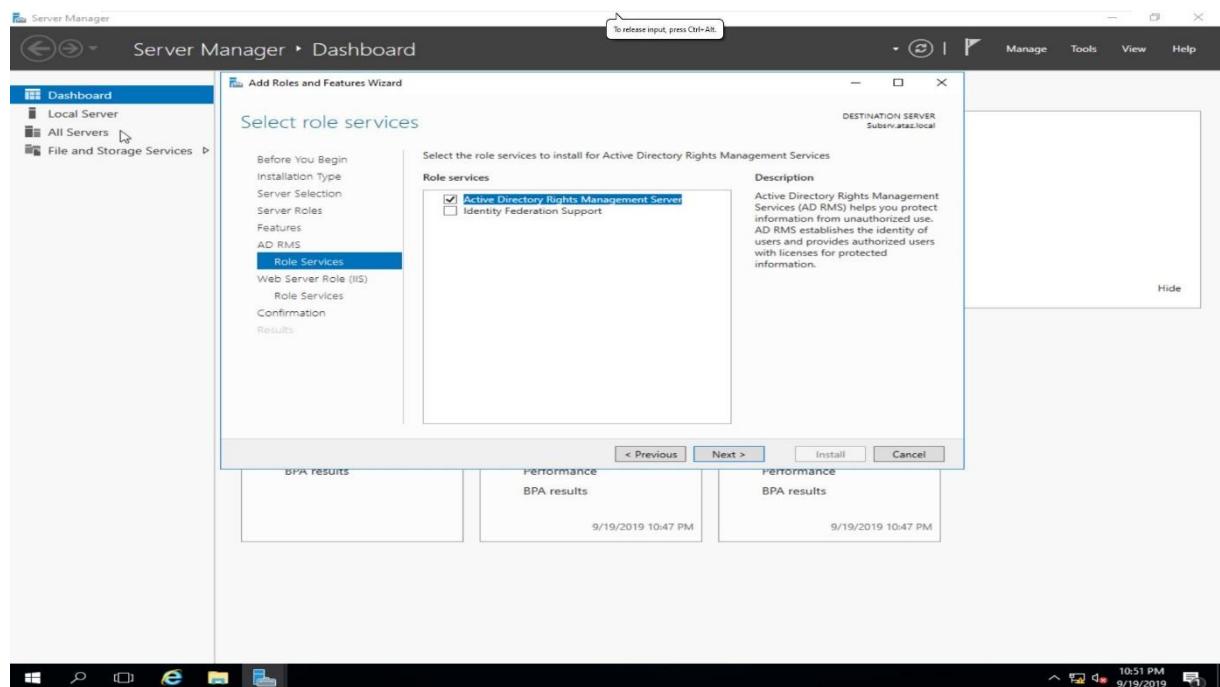
18. Ekstra bir özellik seçmiyoruz.



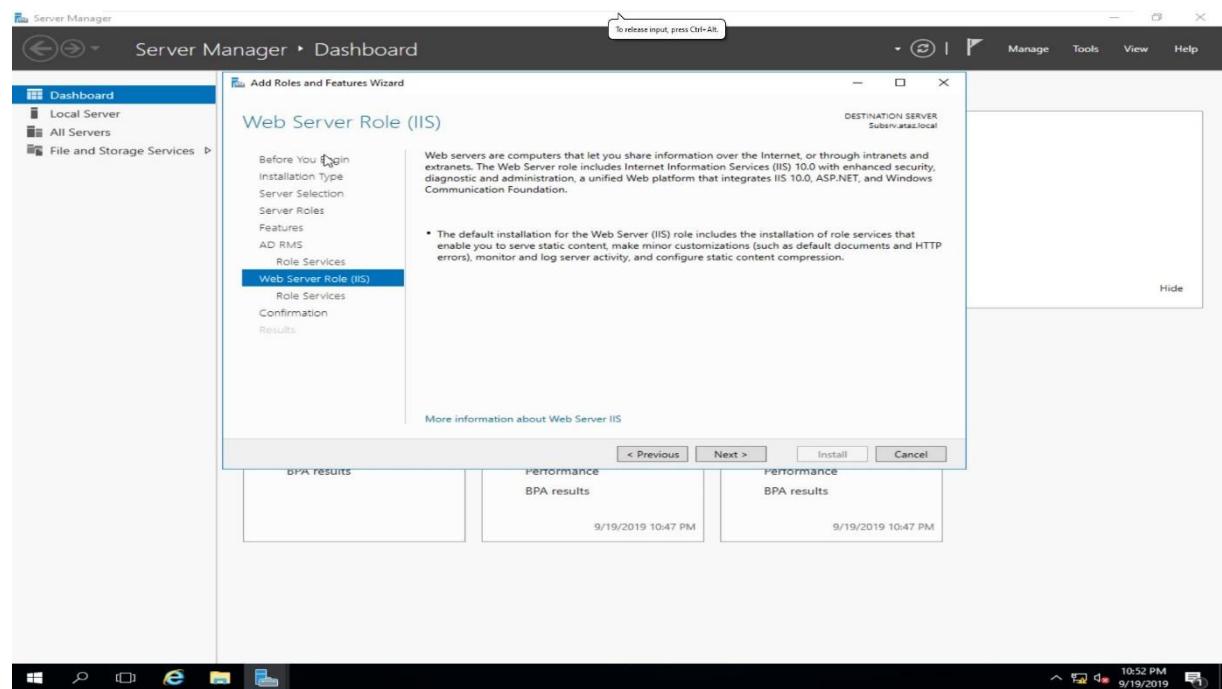
19.



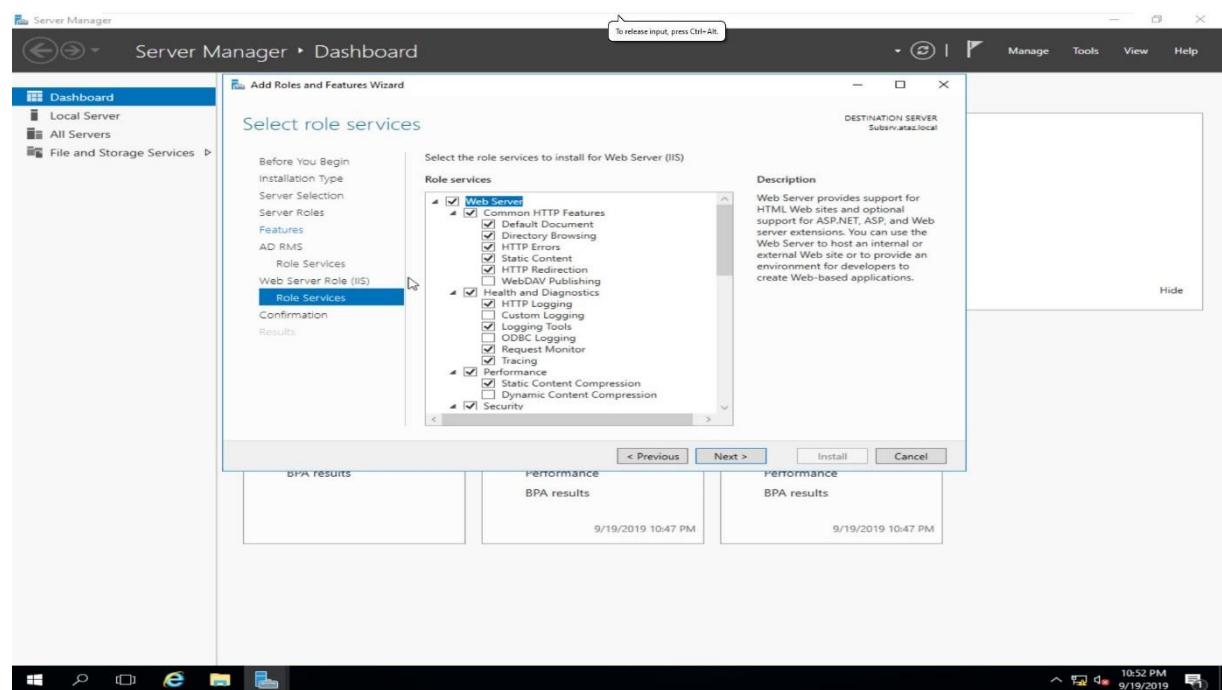
20.Rolün servislerini seçiyoruz.



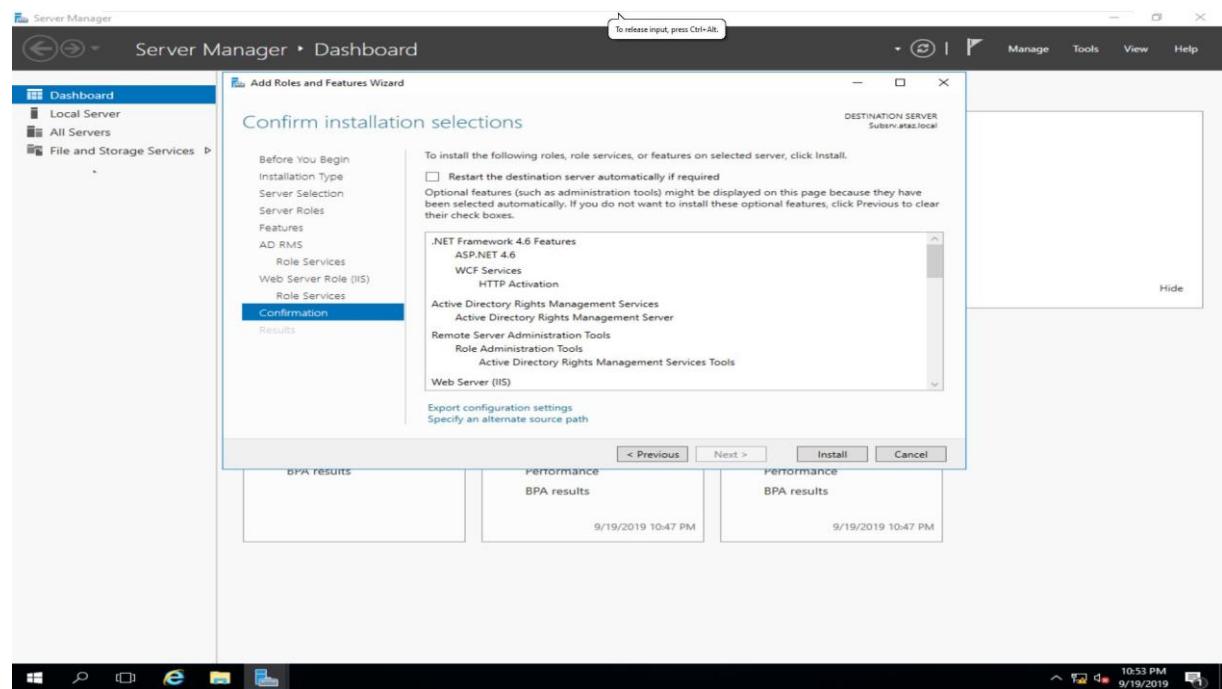
21. Rolün yanında ektradan “web server” ayarları yapıyoruz.



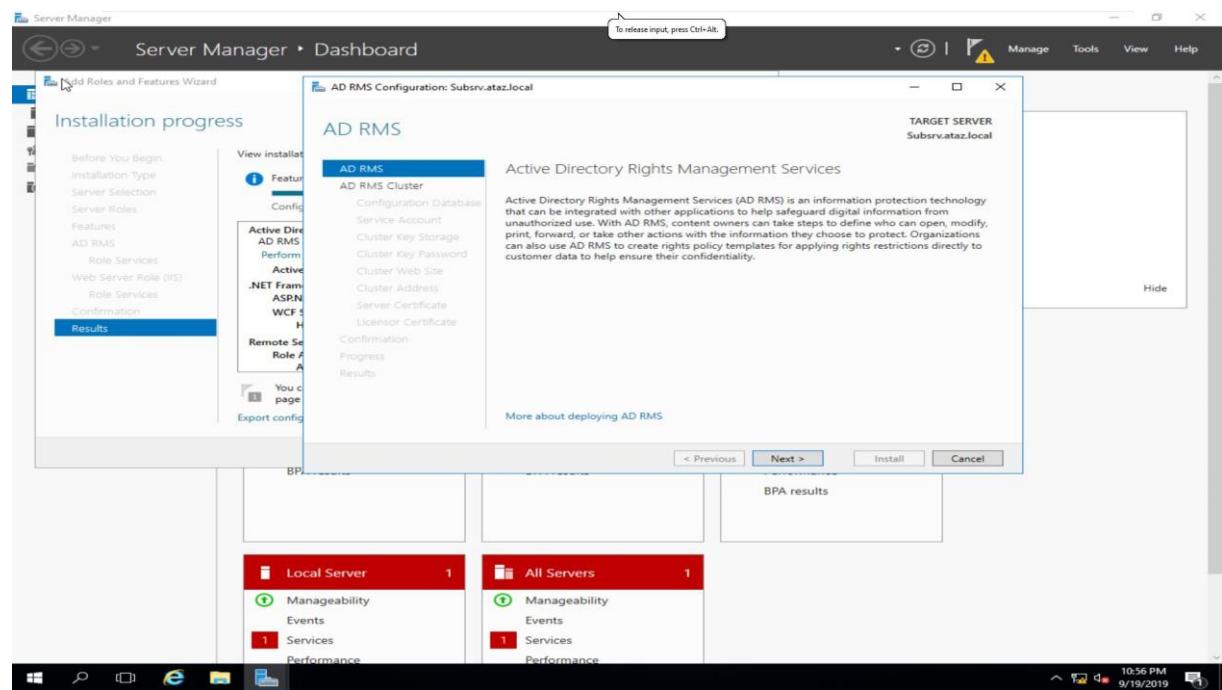
22.



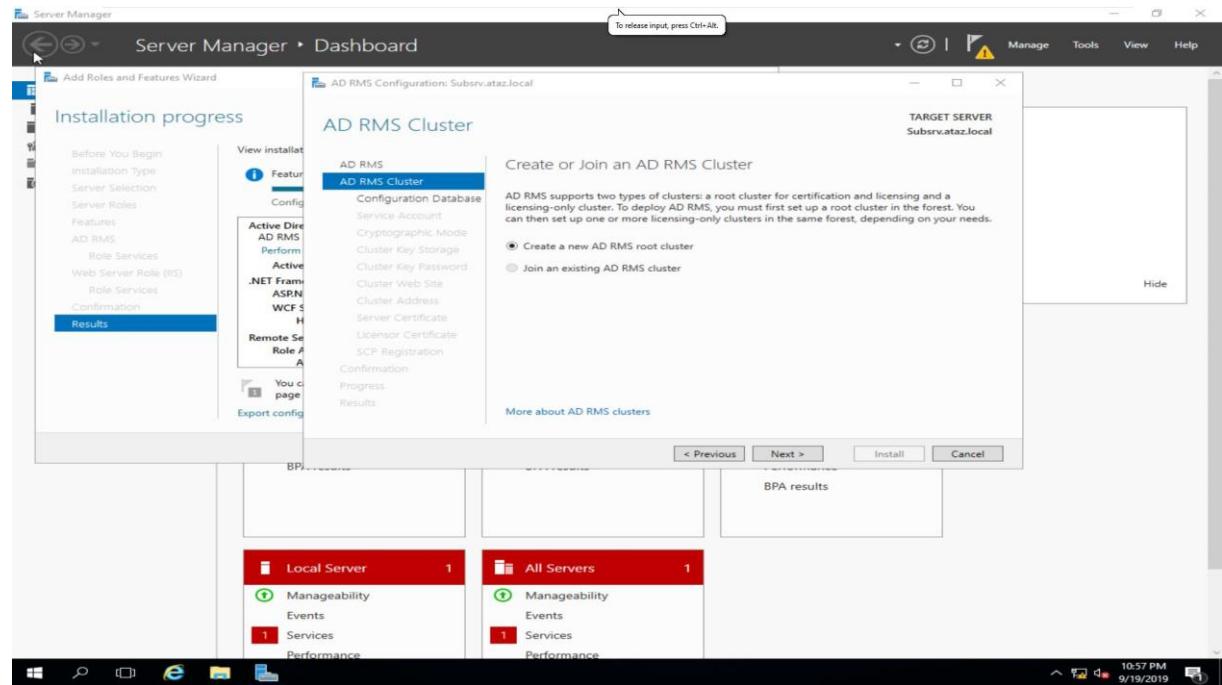
23."Insall" seçip rolü yükleme işlemi bitiyoruz.



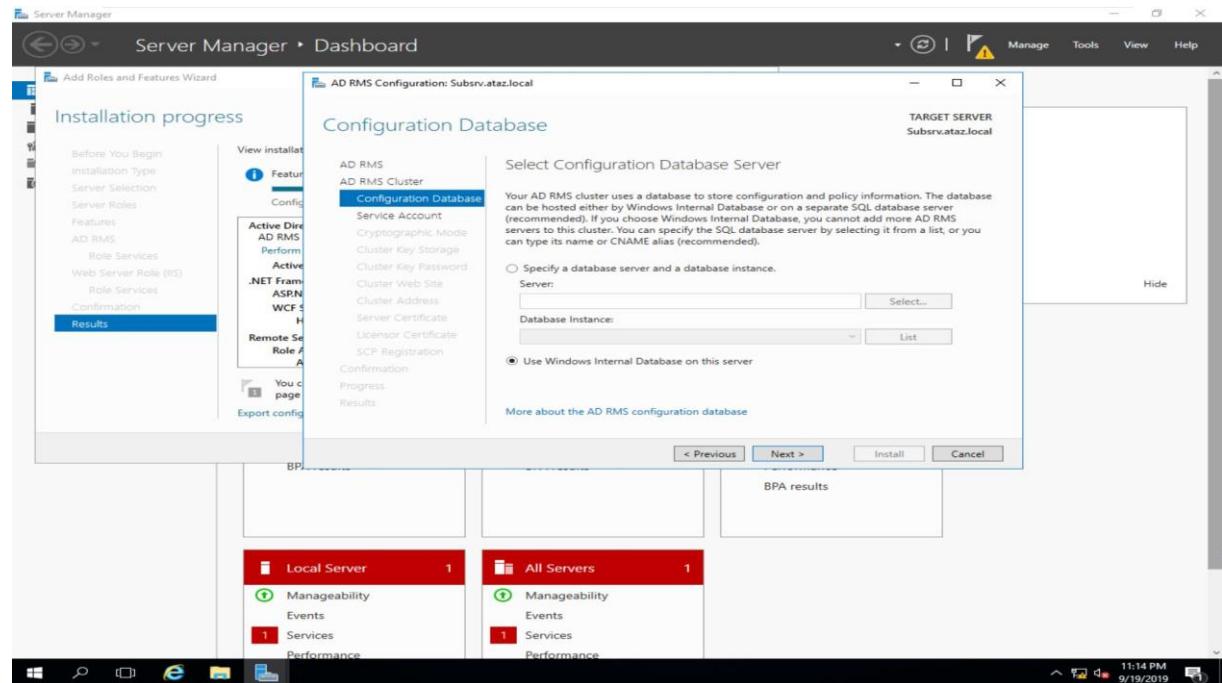
24.Rolü yüklemeyi bittikten sonra "Perform Additional Configuration" tıklayalım.



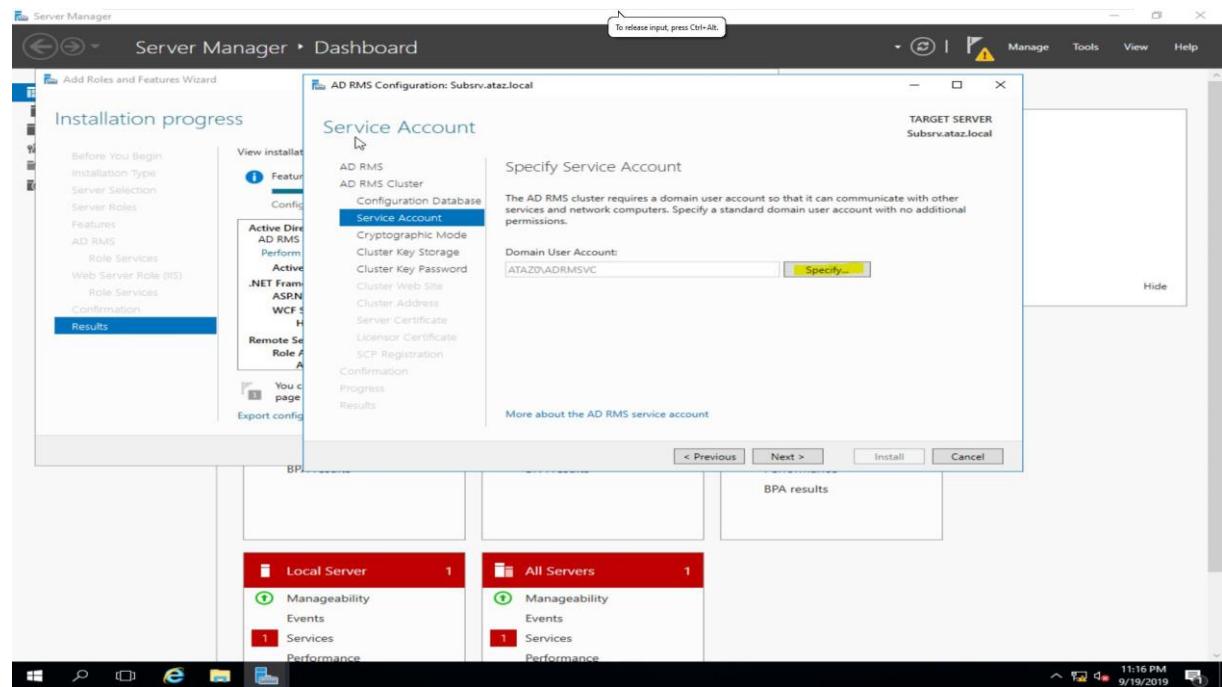
25. Konfigurasyon aşamalarında ilk olarak "Create a New AD RMS root cluster" yeni cluster oluşturalım.



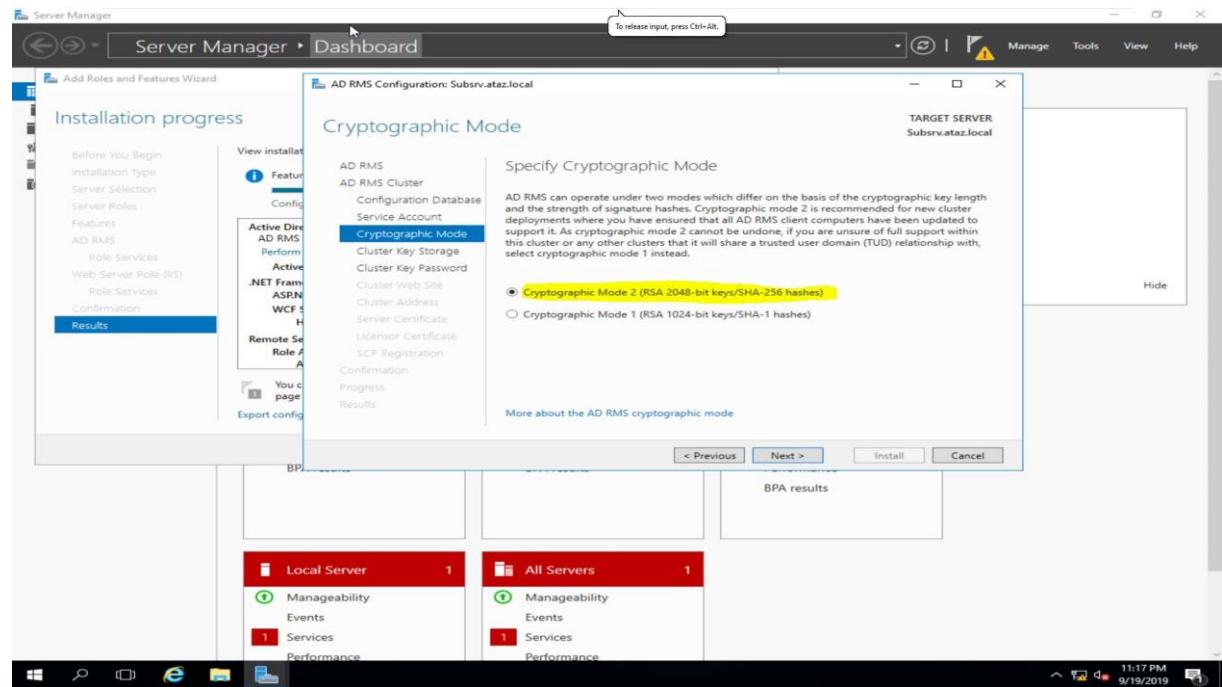
26. Database olarak "Use Windows Internal Database on this server" seçeneğini kullanalım.



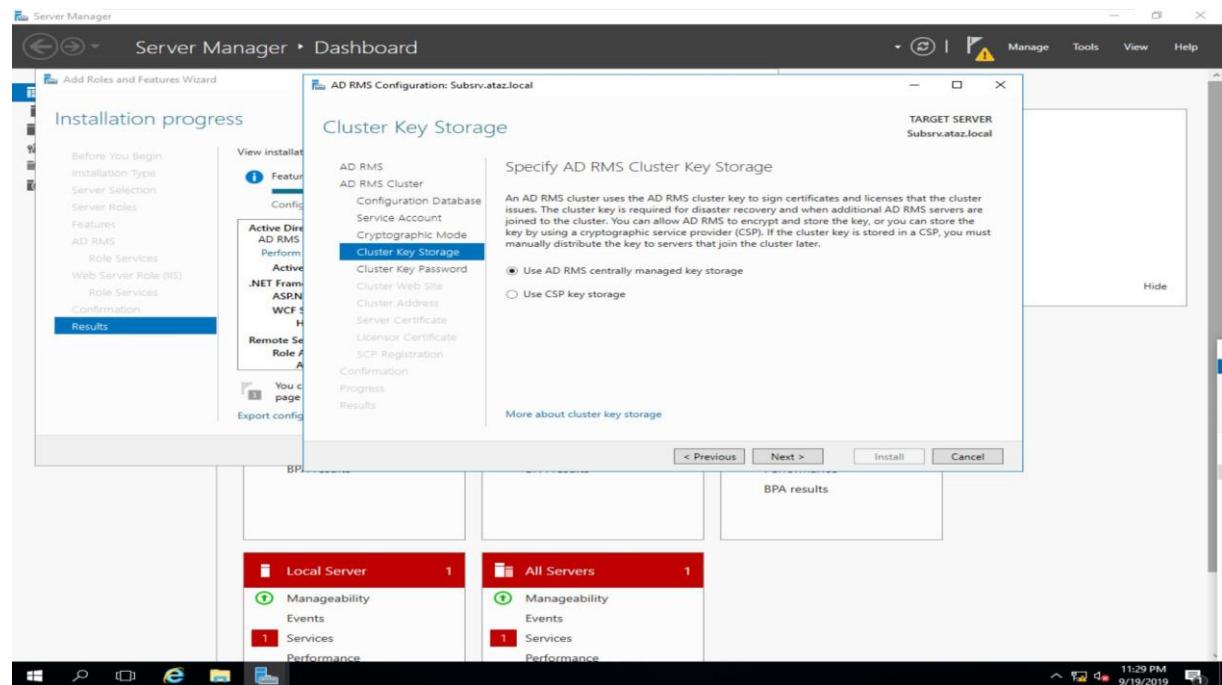
27. Hesap olarak oluşturduğumuz “ATAZ0\AD RMS SVC” hesabını kullanalım.



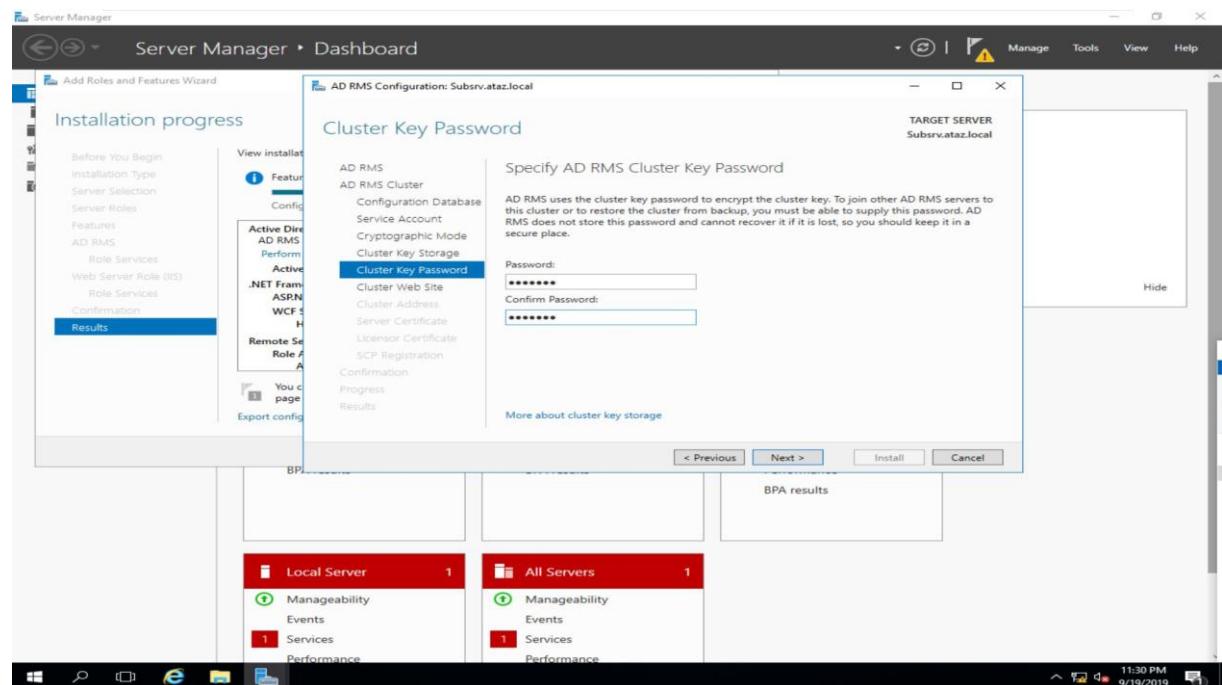
28. "Cryptographic Mode 2" kullanım.



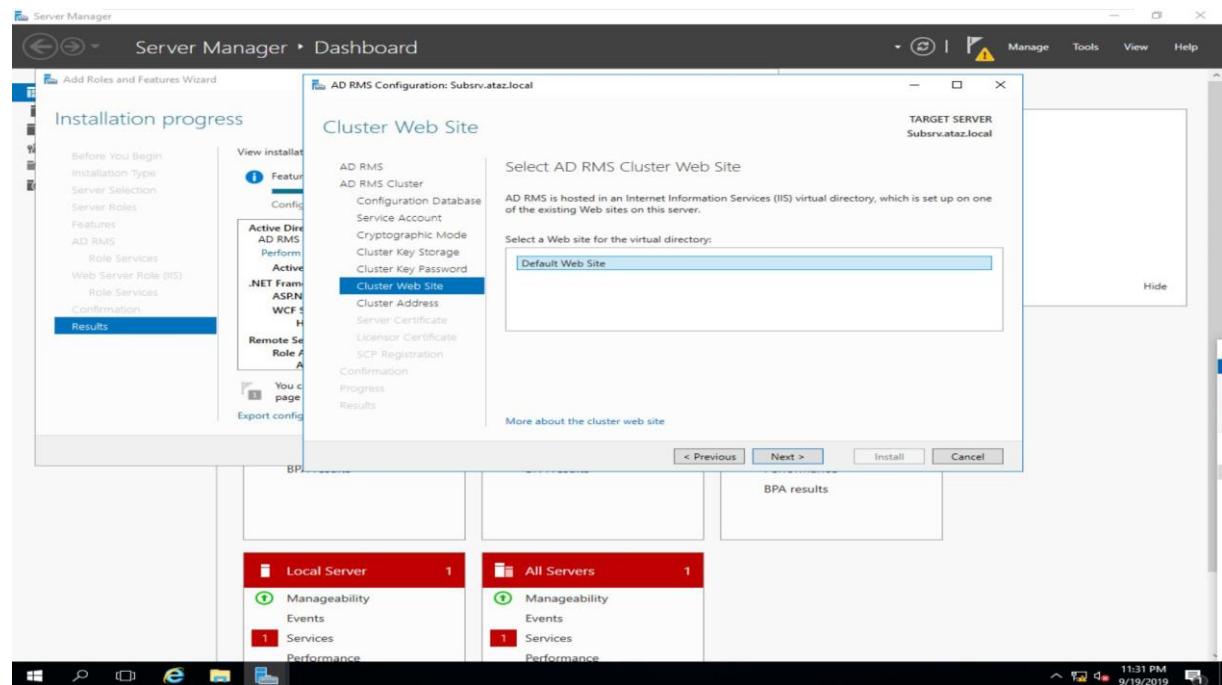
29. Cluster key olarak "Use AD RMS centrally managed key storage" seçelim.



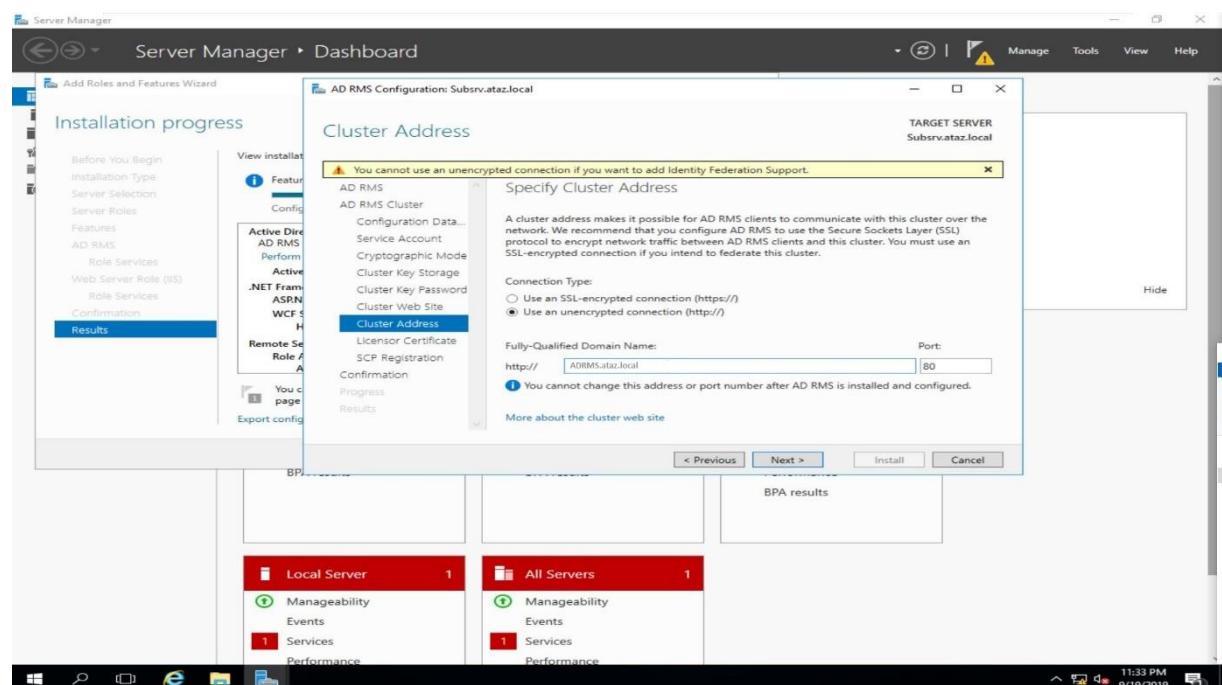
30. "Cluster Key Password" oluşturulur.



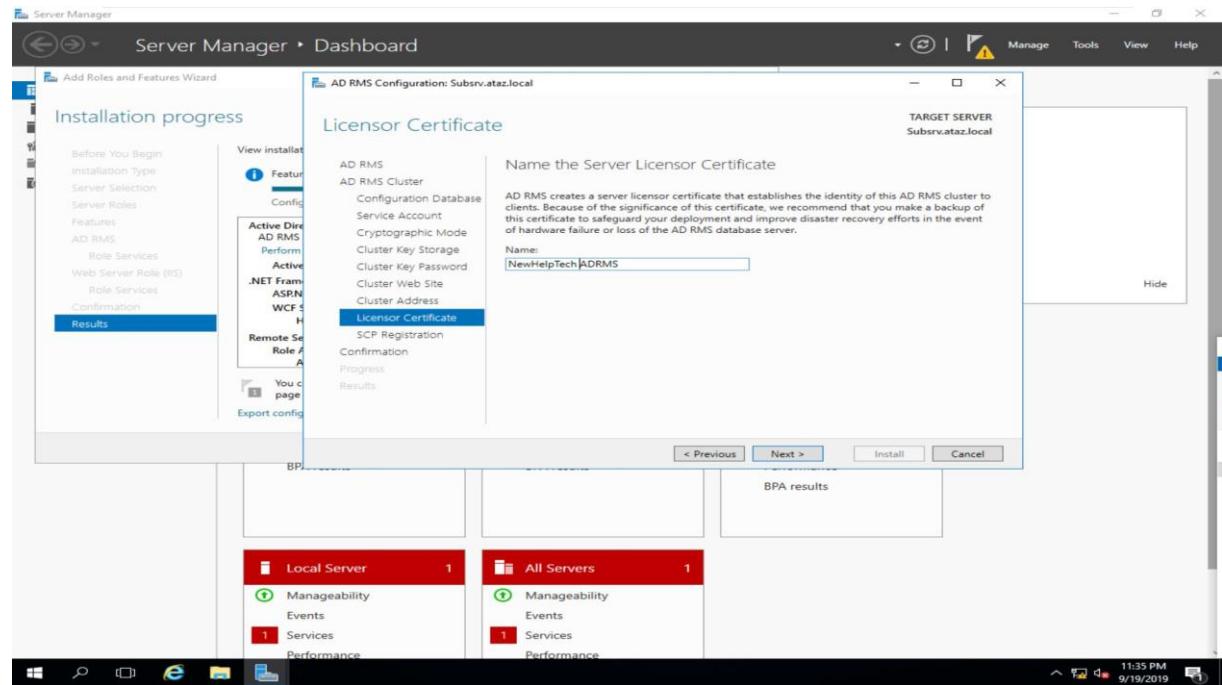
31.Cluster web sitesini “Default Web Site” seçili olduğunu doğrulayalım ve “Next” diyelim.



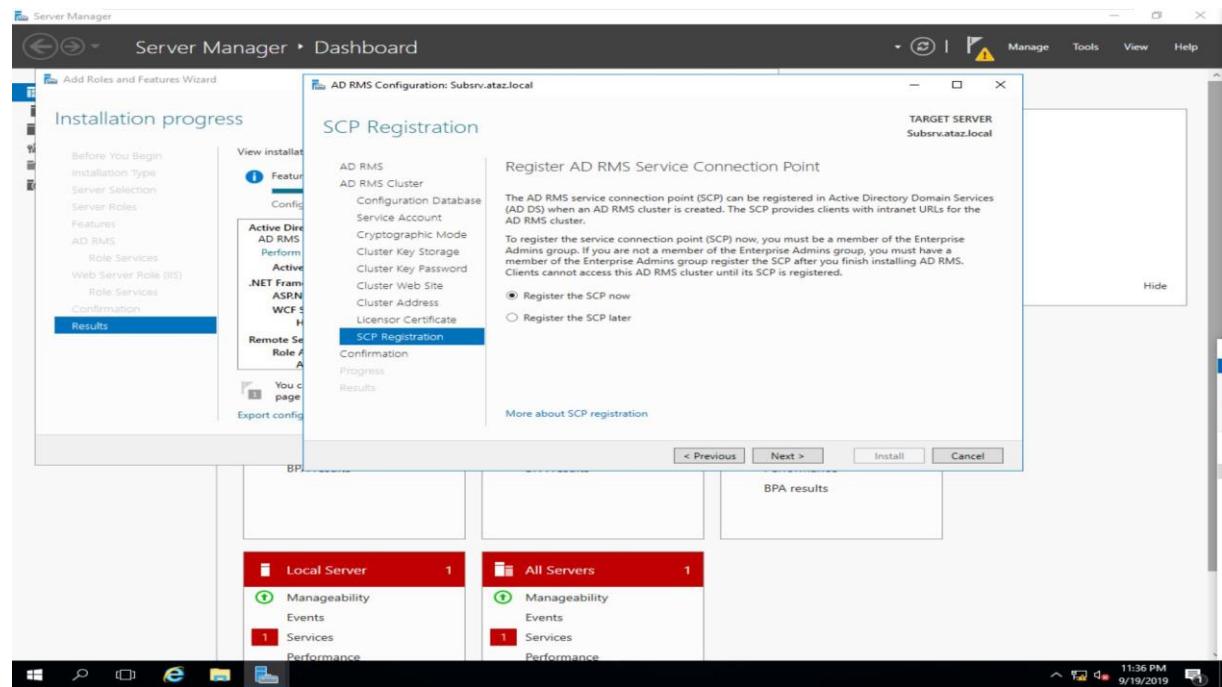
32.Bu aşamada "Use an unencrypted connection (http://)" seçim ve domain name olarak "ADRMS.ataz.local" yazalım.



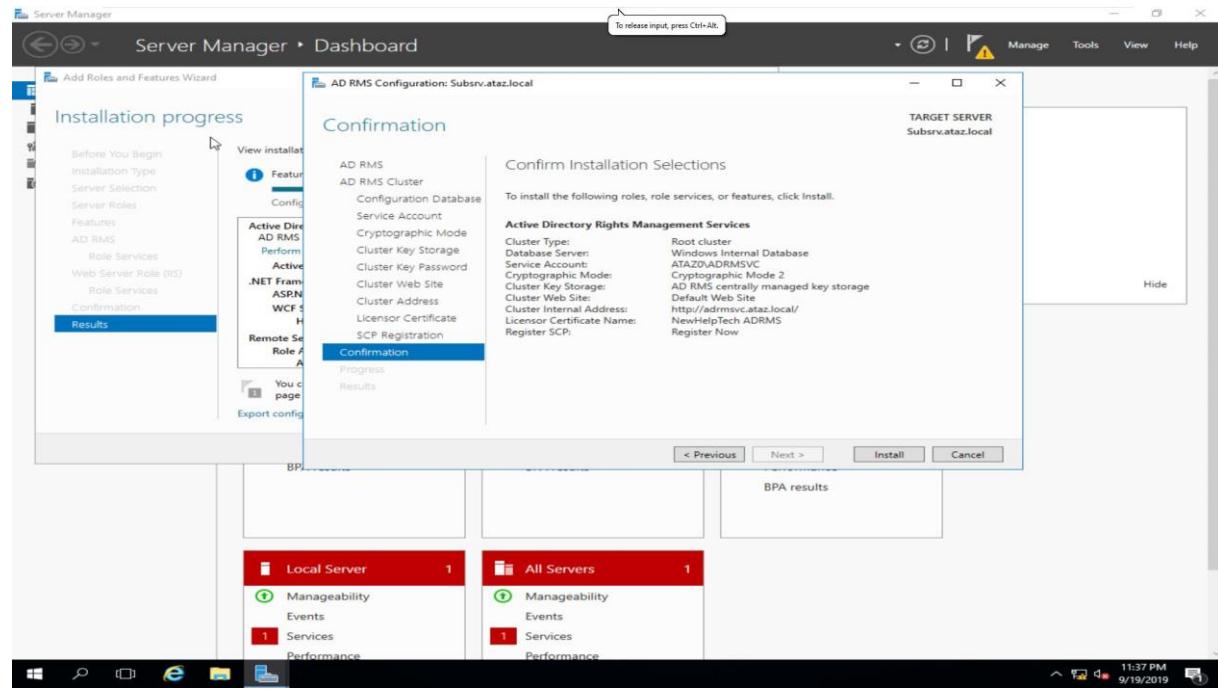
33. "Licensor Certificate" için isim belirleyelim name "NewHelpTech ADRMS" olarak girelim ve "Next" diyelim.



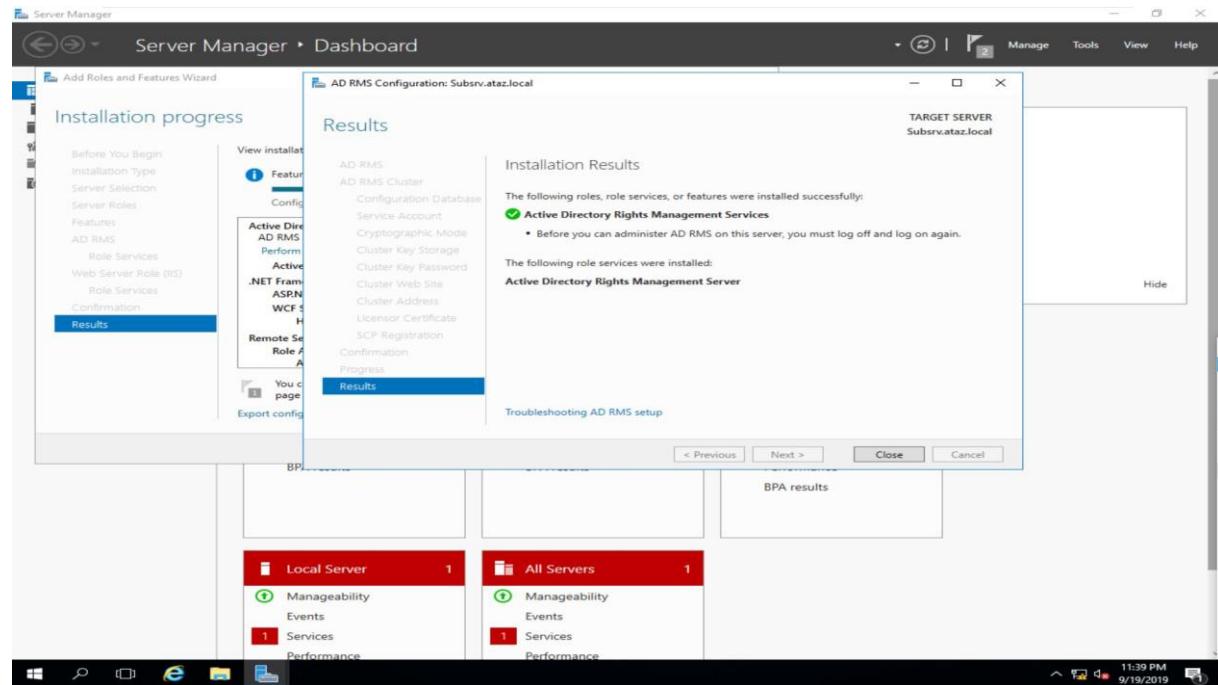
34. "Register the SCP now" seçelim.



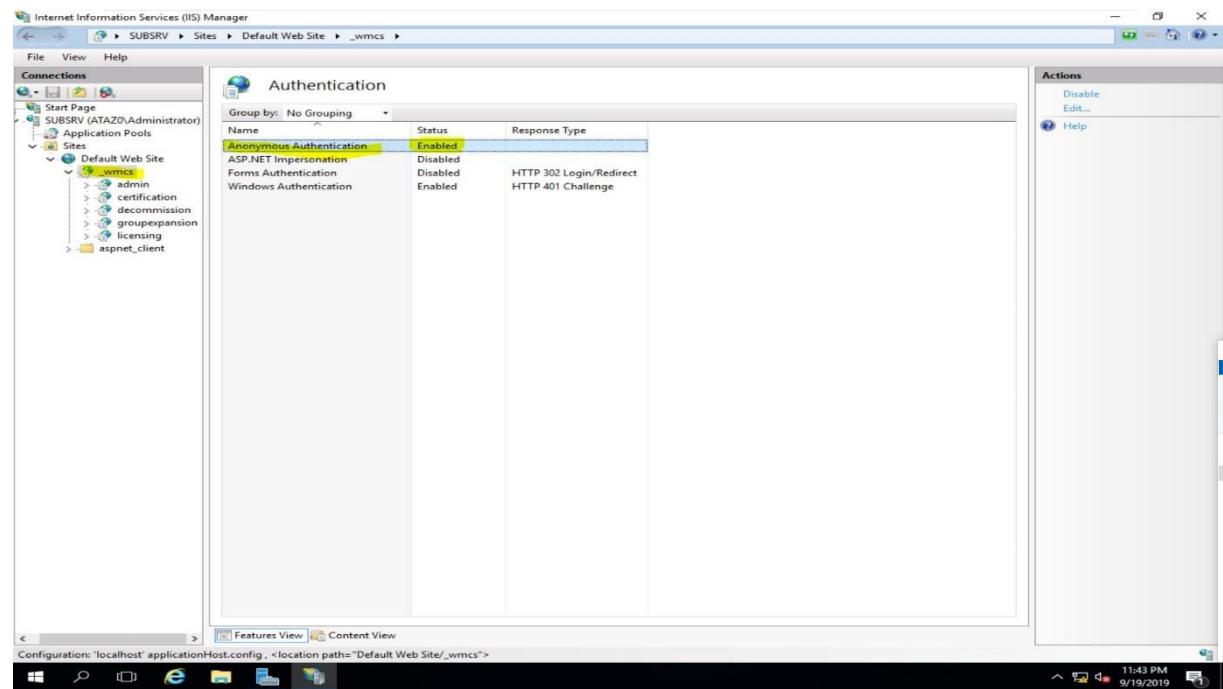
35."Insall" diyelim ve işlemleri yükleme başlatalım.



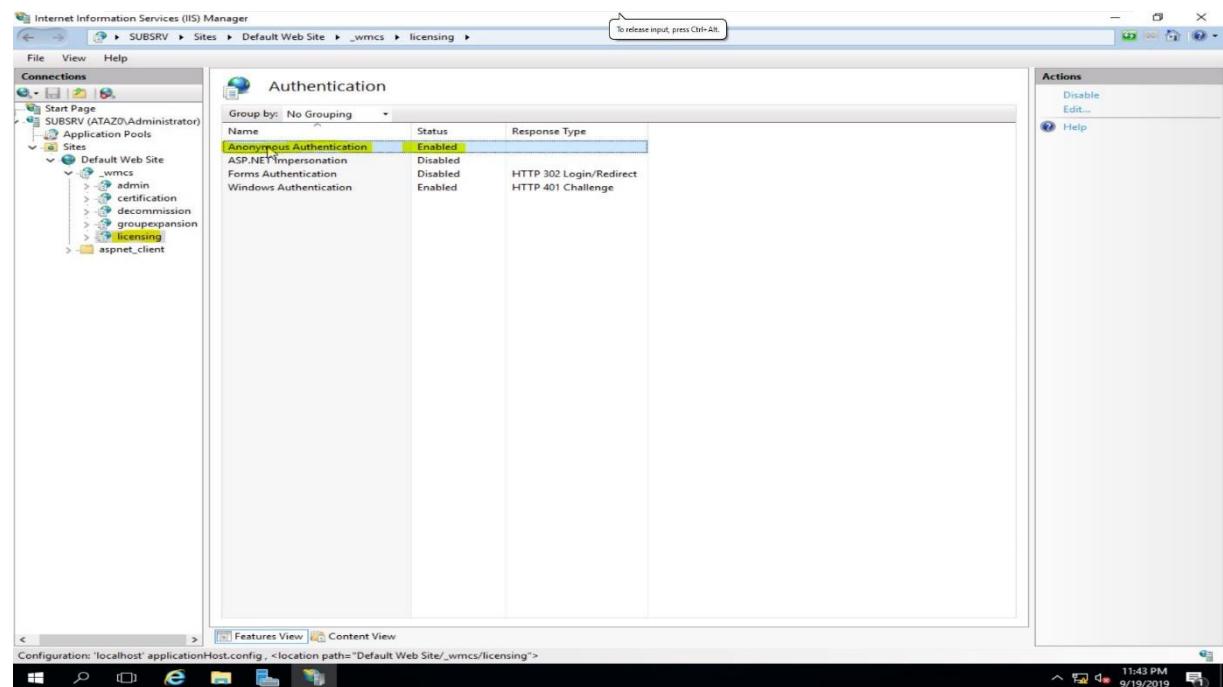
36.Yükleme işlemleri bitince “Close” diyip tamamlayalım.



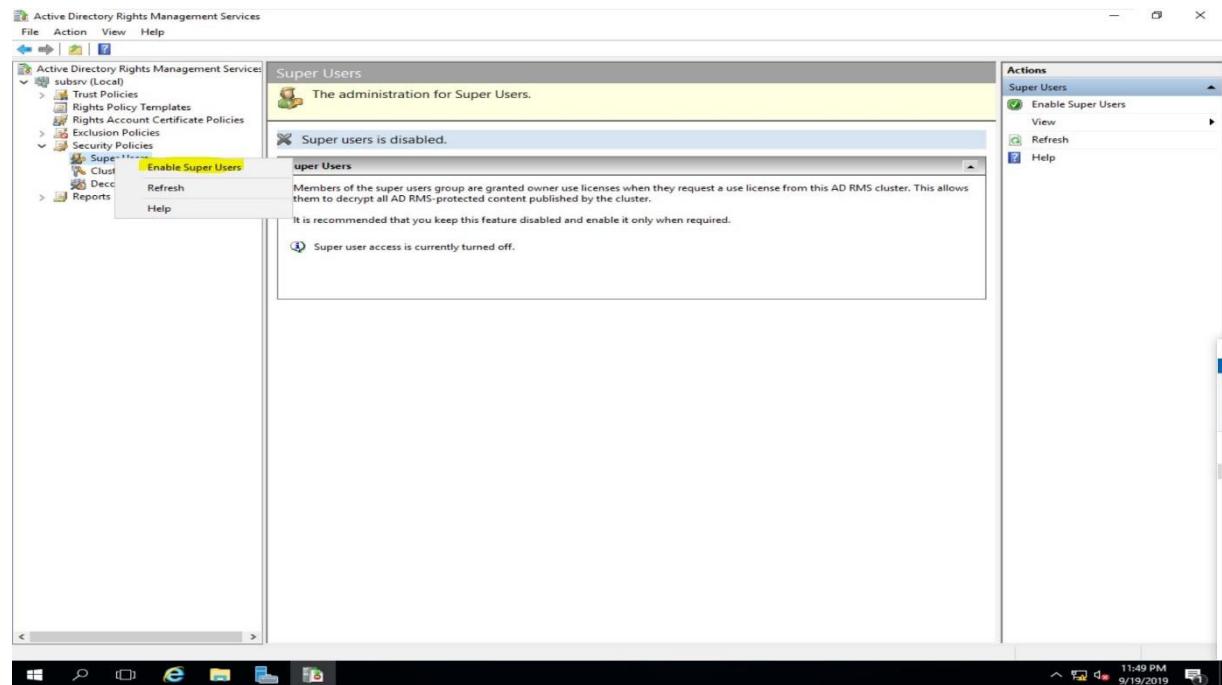
37.Yükleme işlemleri bittikten sonra “Internet Information Services (IIS) Manager” açalım ve “Sites\Default Web Site” genişletelim “vmcs” seçili iken sağ tarafta “Authentication” dan "Anonymous Authentication" i “Enable” hale getirelim.



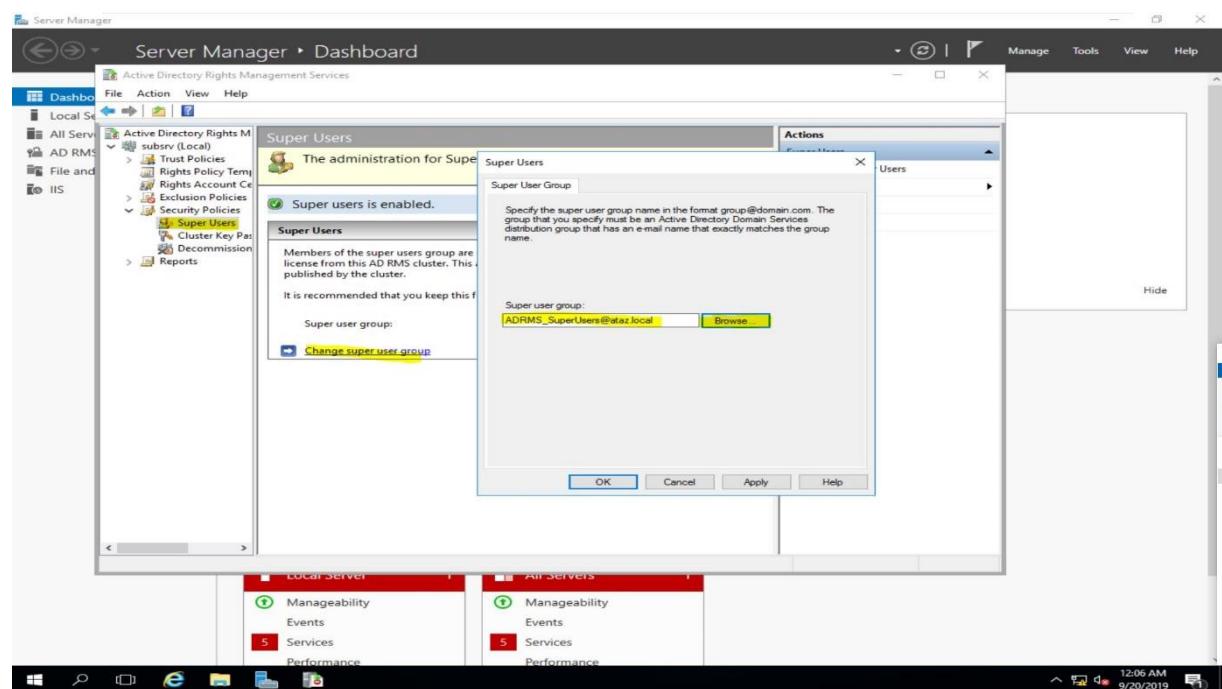
38.Yine aynı sekilde” vmcs” i genişletelim ve” licensin” seçiliyken “Authentication” içersinden "Anonymous Authentication" i “Enable” hale getirelim. Bu adımı yaptıktan sonra Rms yönetmek için hesabı "sign out" olmamız lazım ve sonra tekrardan oturum açalım.



39.Tekrar oturum açtıktan sonra Tools'dan “Active Directory Rights Management Services” konsolunu açıp “Subsrv(local)” altında Security Policies \ Super Users “Enable” yapalım.

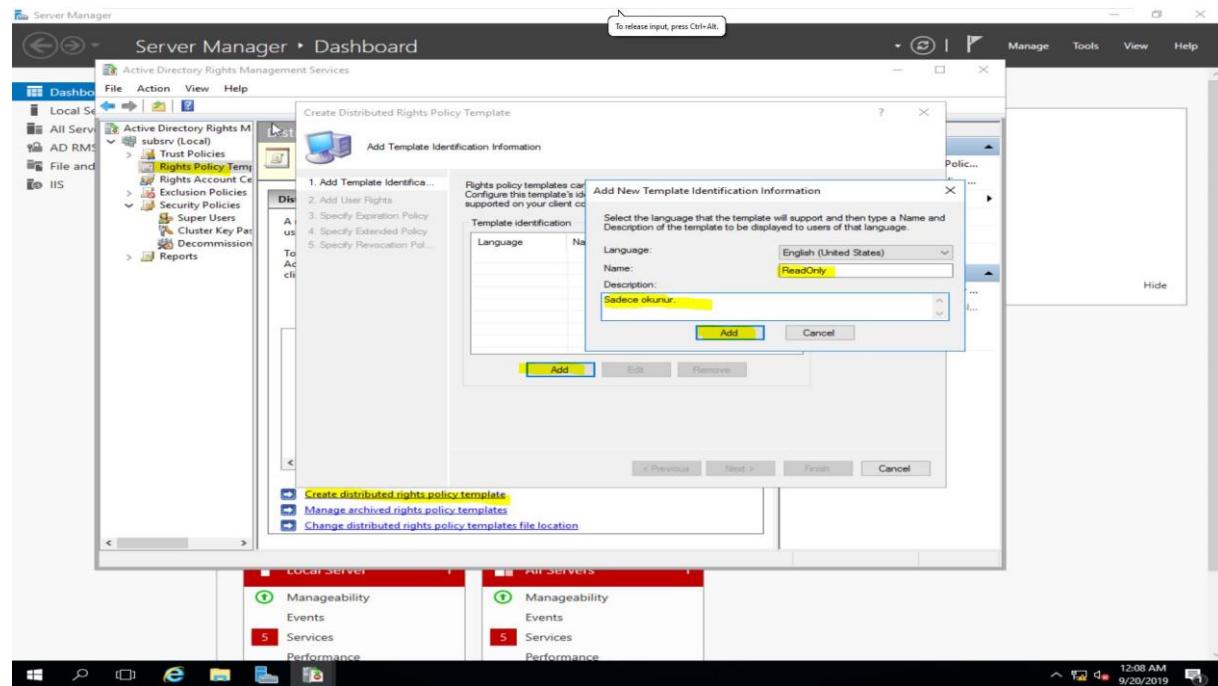


40.Super User Grup olarak bizim oluşturduğumuz “ADRMS_Superusers” seçelim. Bu adımda oluşturduğumuz grubun mail adresinin (ADRMS_Superusers@ataz.local) olduğunu yoksa eklememiz gerekmektedir aksi takdirde hata ile karşılaşırız.

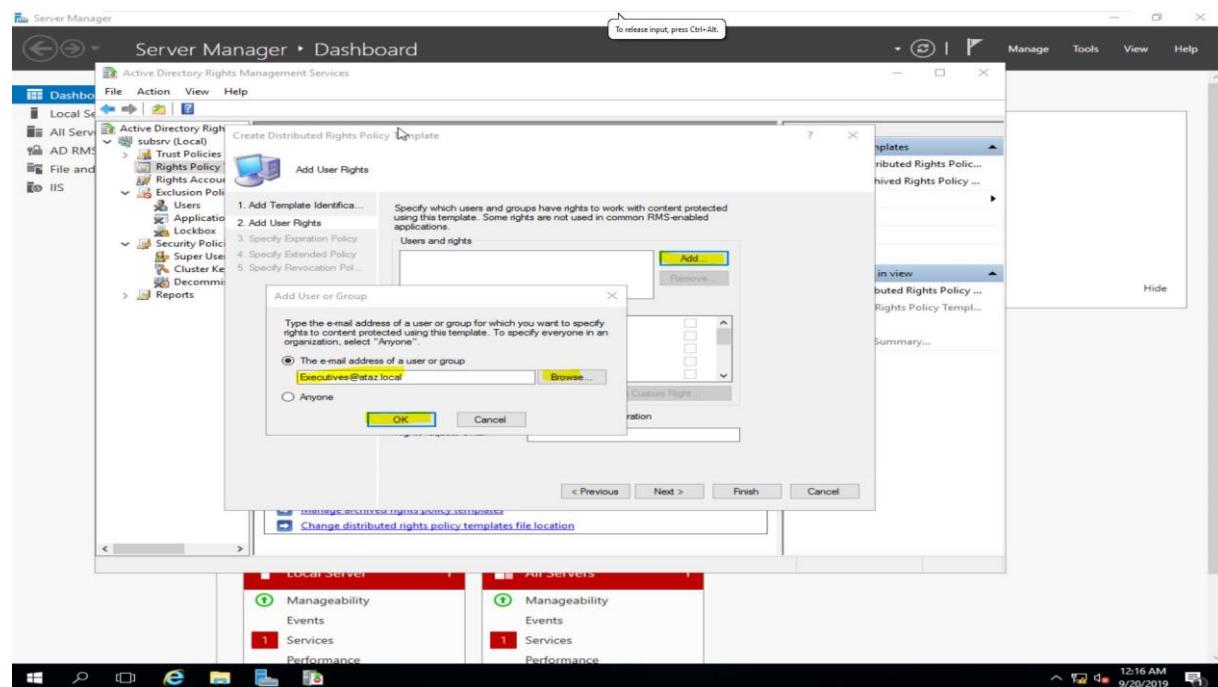


41.Daha sonra “Subsrv(local)” altında "Rights Policy Templates" seçip Action panelden "Create Distributed Rights Policy Template." Tıklayalım ve "Add Template Identification information box" açılacak, “Add” e tıklayalım.

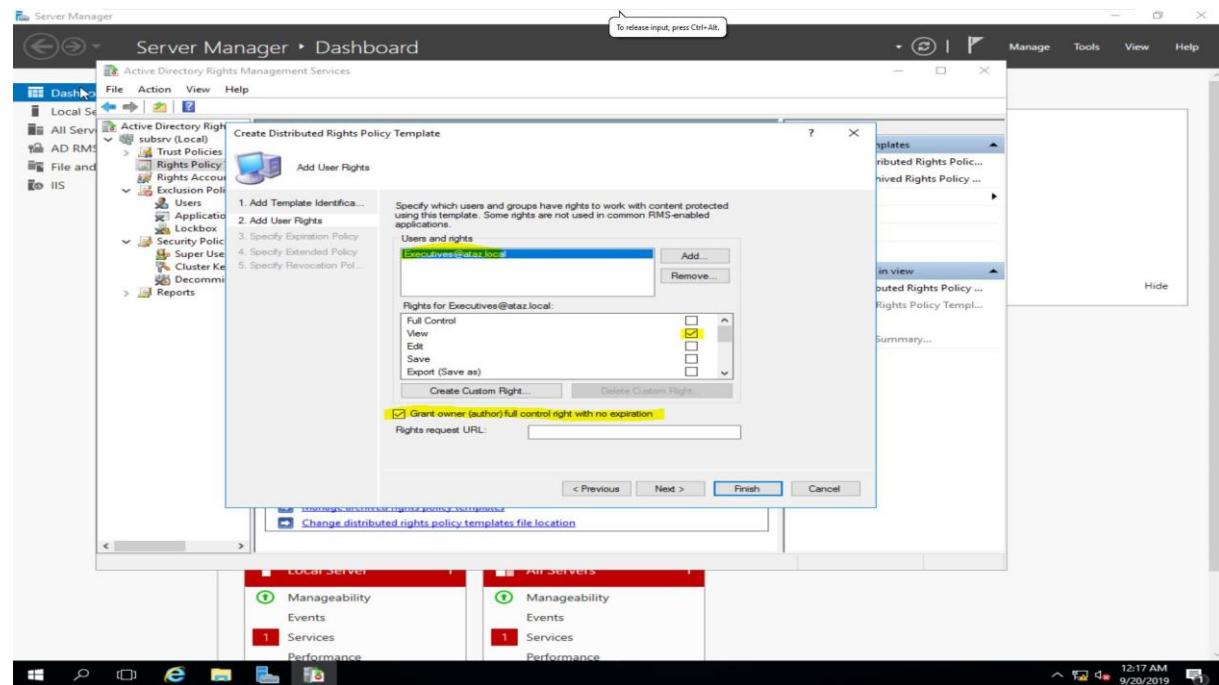
- Language: English (United States)
- Name: ReadOnly
- Description : Sadece okunabilir yada size bir açıklama ekleyelim.



42. "Add User or Group " penceresinde grup olarak "User"da oluşturduğumuz "Executives" seçelim. Aynı şekilde mail adresi olduğuna dikkat edelim.

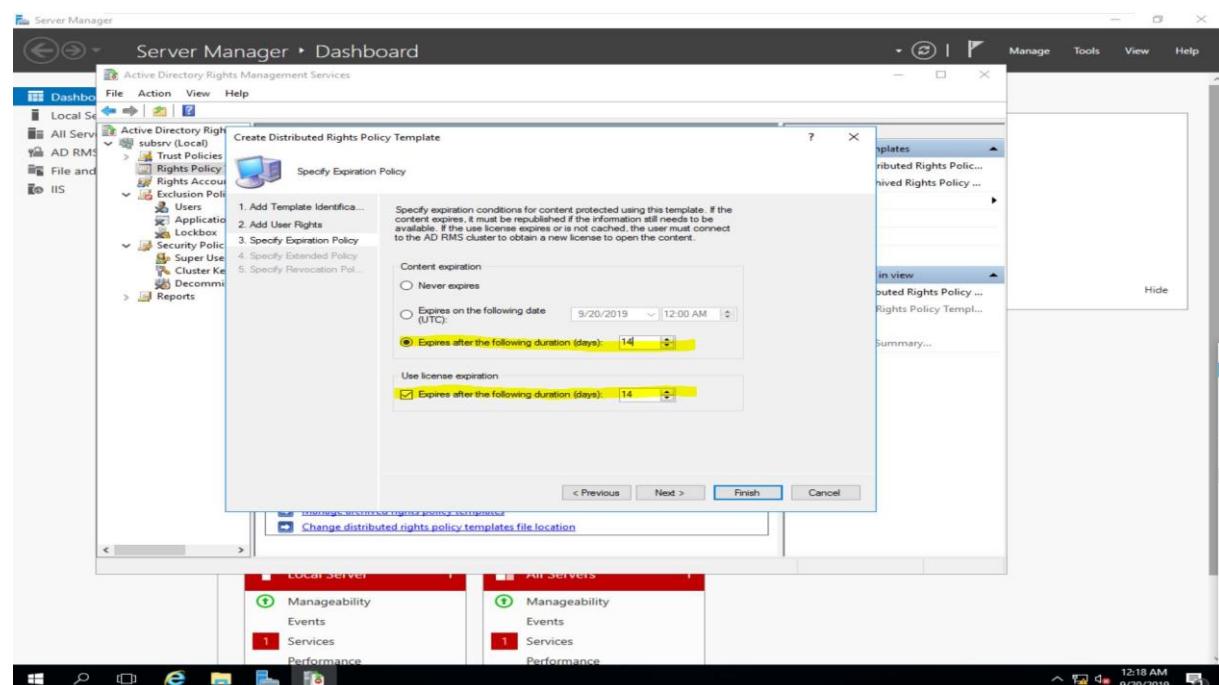


43. "Executives" seçtiğten sonra gruba "view" hakkı verelim ve "Grant owner (author) full control right with no expiration" seçenekinin işaretli olduğundan emin olalım.

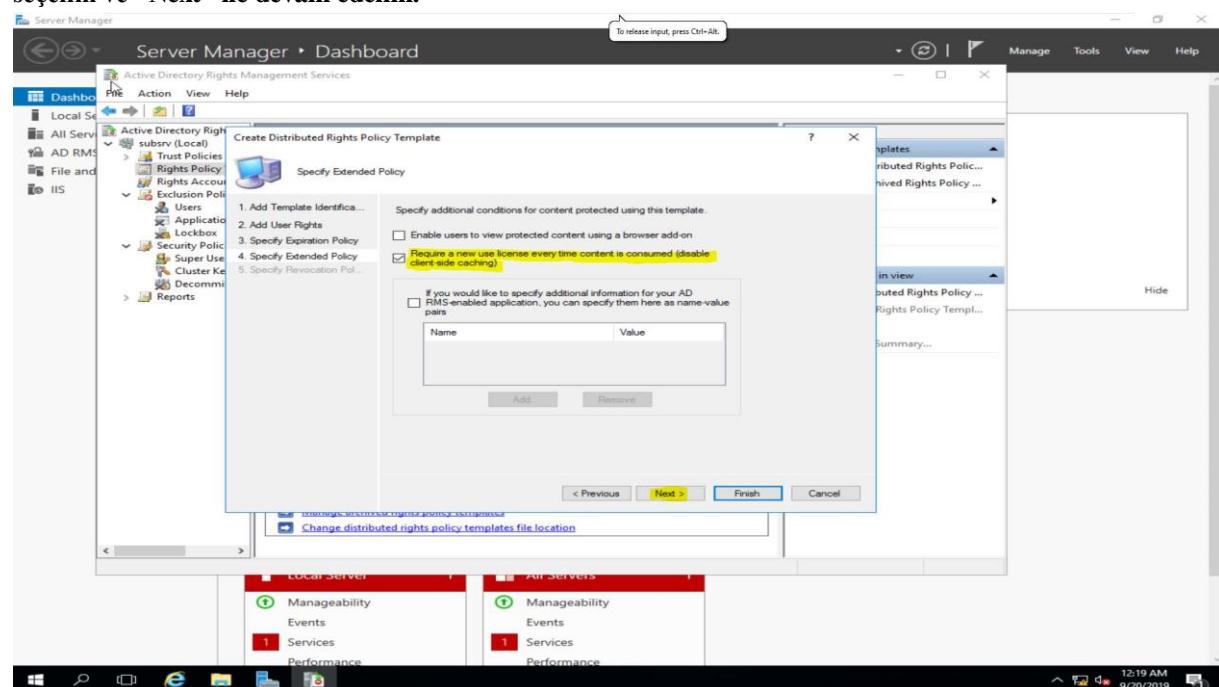


44. "Content Expiration: Expires after the following duration (days): 14"

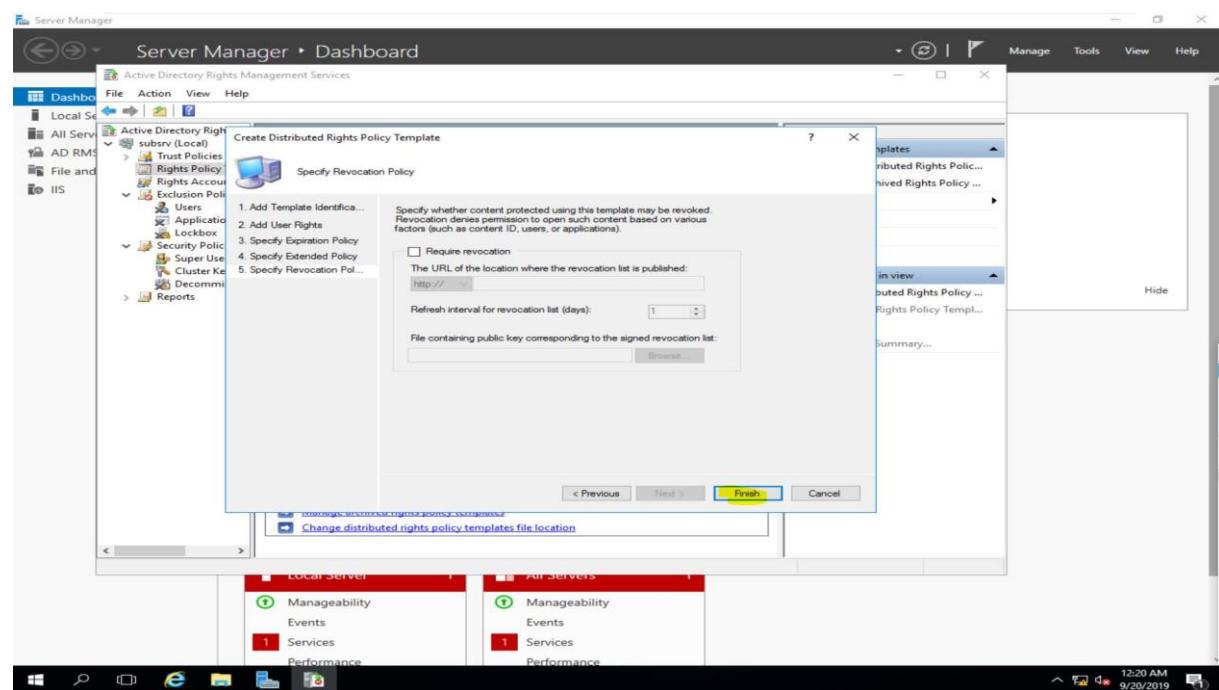
"Use license expiration: Expires after the following duration (days): 14" olarak belirylelim.



45. "Require a new use license every time content is consumed (disable client-side caching)" seçeneğini seçelim ve "Next" ile devam edelim.

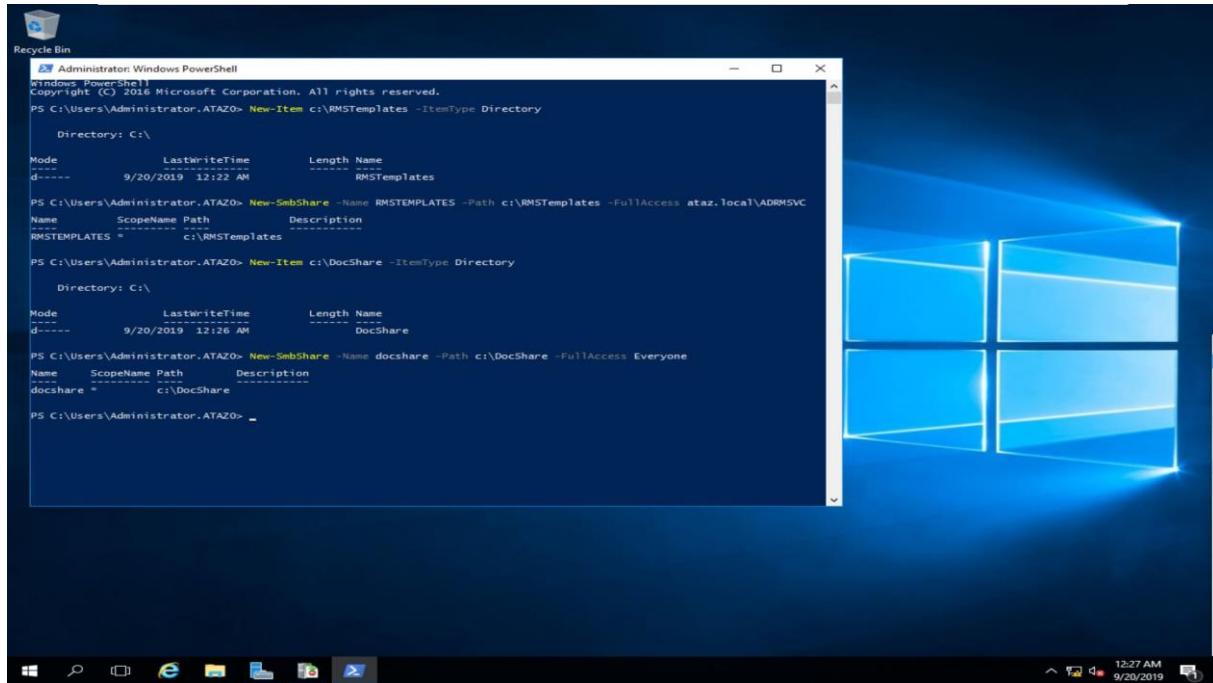


46. "Finish" ile bitirelim

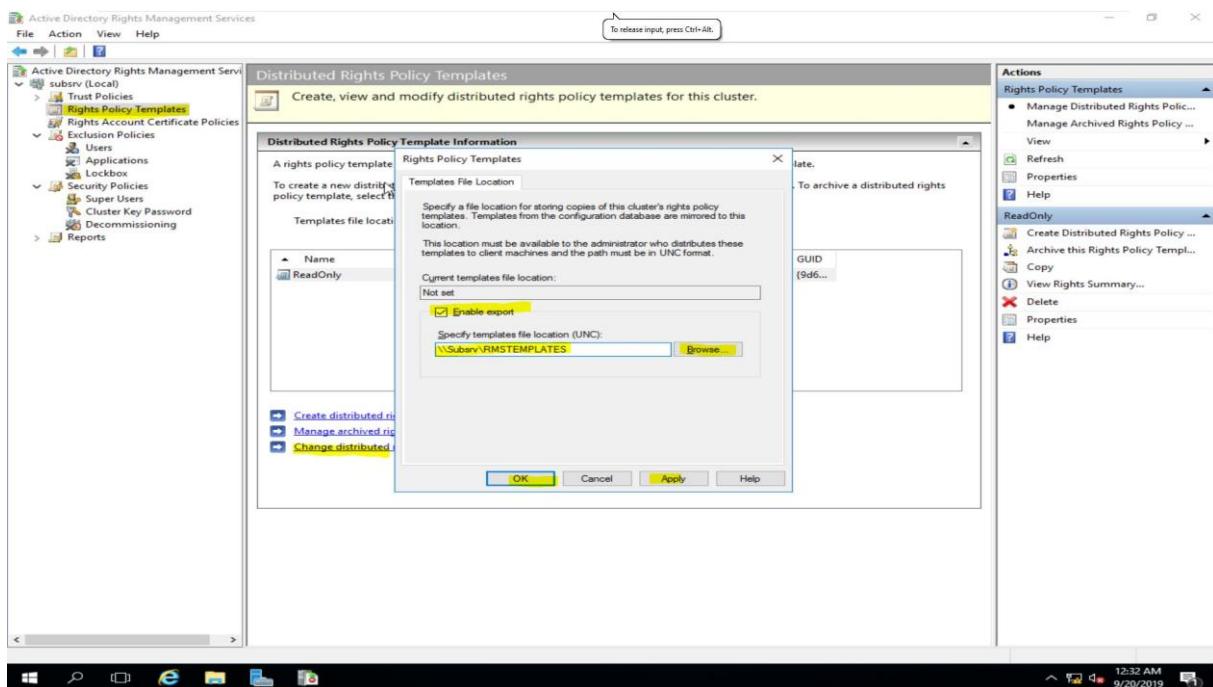


47. Şimdi ise "Rights Policy template Distribution" konfigurasyonunu işlemlerini yapacağımız.Bunu için PowerShell açıp aşağıdaki komutları yazalım (ataz.local yerine sizin domain adınız olacak)

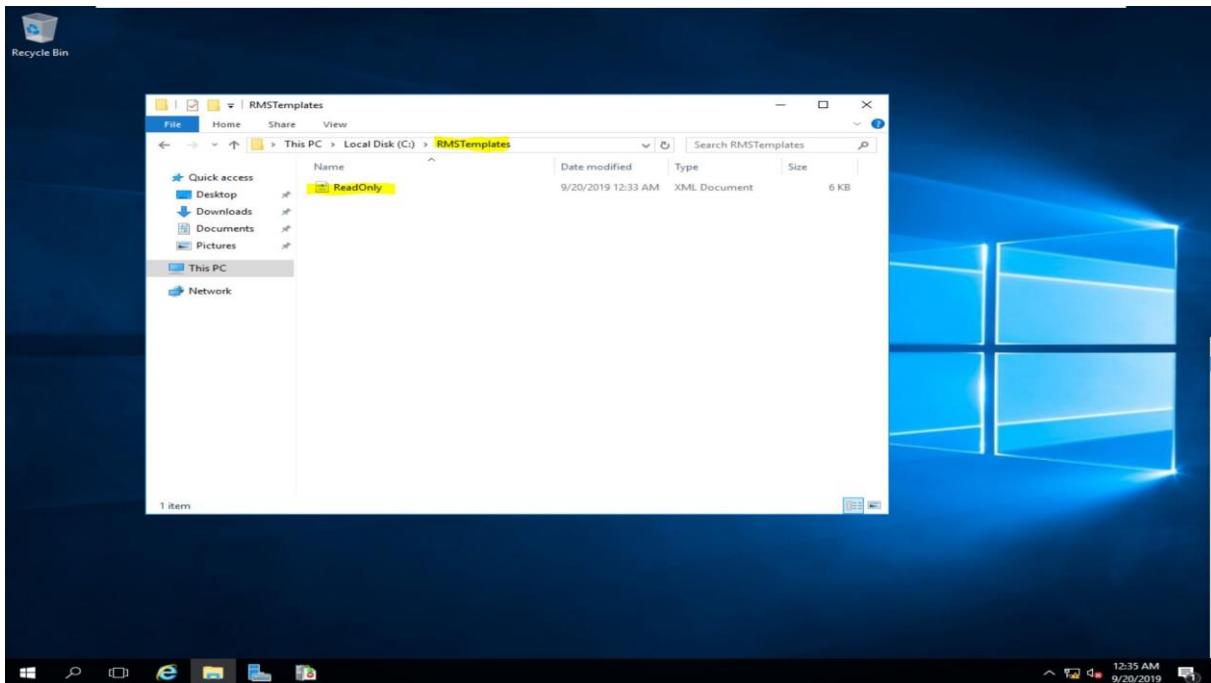
- New-Item c:\RMSTemplates -ItemType Directory
- New-SmbShare -Name RMSTEMPLATES -Path c:\RMSTemplates -FullAccess ataz.local\ADRMSVC
- New-Item c:\DocShare -ItemType Directory
- New-SmbShare -Name docshare -Path c:\DocShare -FullAccess Everyone



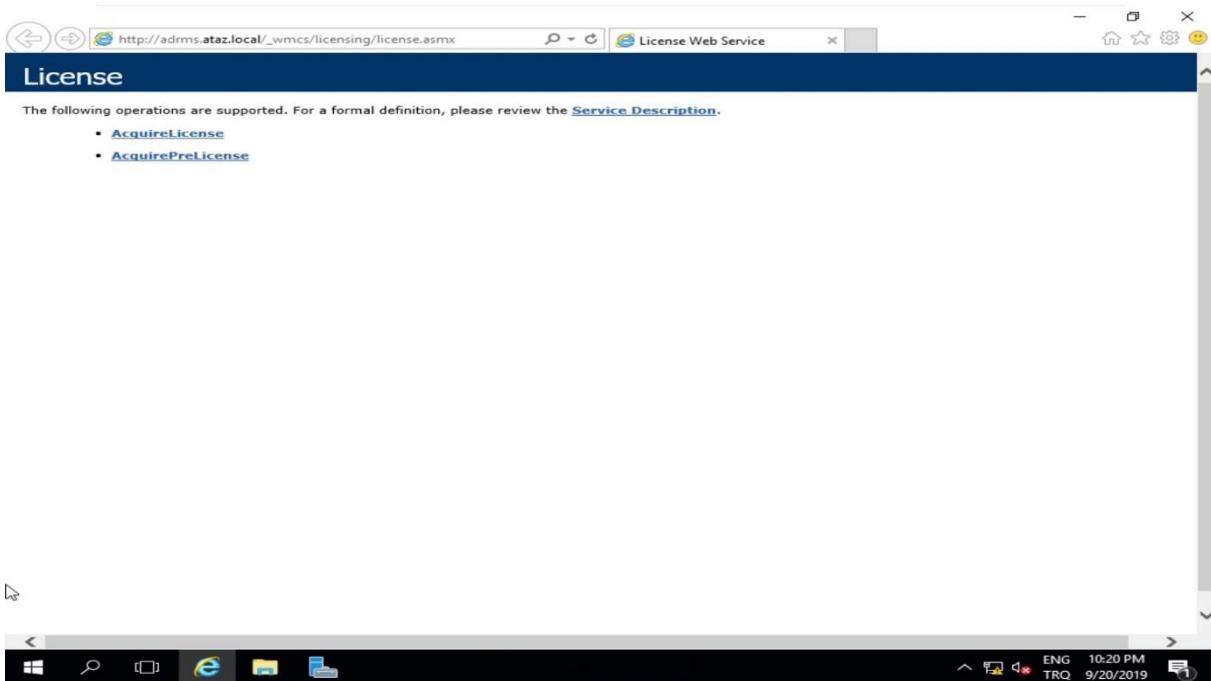
48. "AD RMS Console"'dan Rights "Policy Templates node" a tıklayalım. "Distributed Rights Policy Templates" alanında "Change distributed rights policy templates file location" tıklayalım. Açılan ekranda "enable export" u işaretliyelim.Sonra "Specify Templates File Location (UNC)" içine "\\\Subsrv\RMSTEMPLATES" teplateeler için oluşturduğumuz paylaşımın yolunu yazalım.



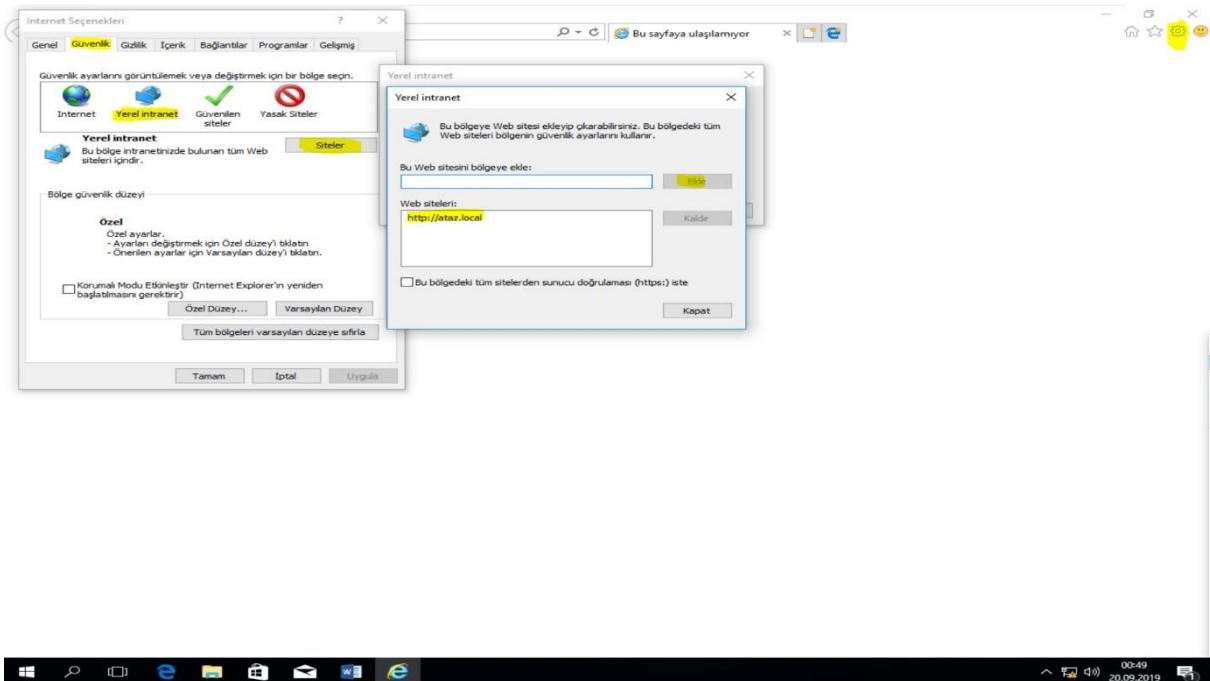
49. C:\rmstemplates klasörünün içinde "ReadOnly.xml" dosyası bulunduğuunu doğrulayalım. Eğer burada random isimli bir .xml dosyası varsa 32.adımdaki name adını yanlış yapmışsınızdır.



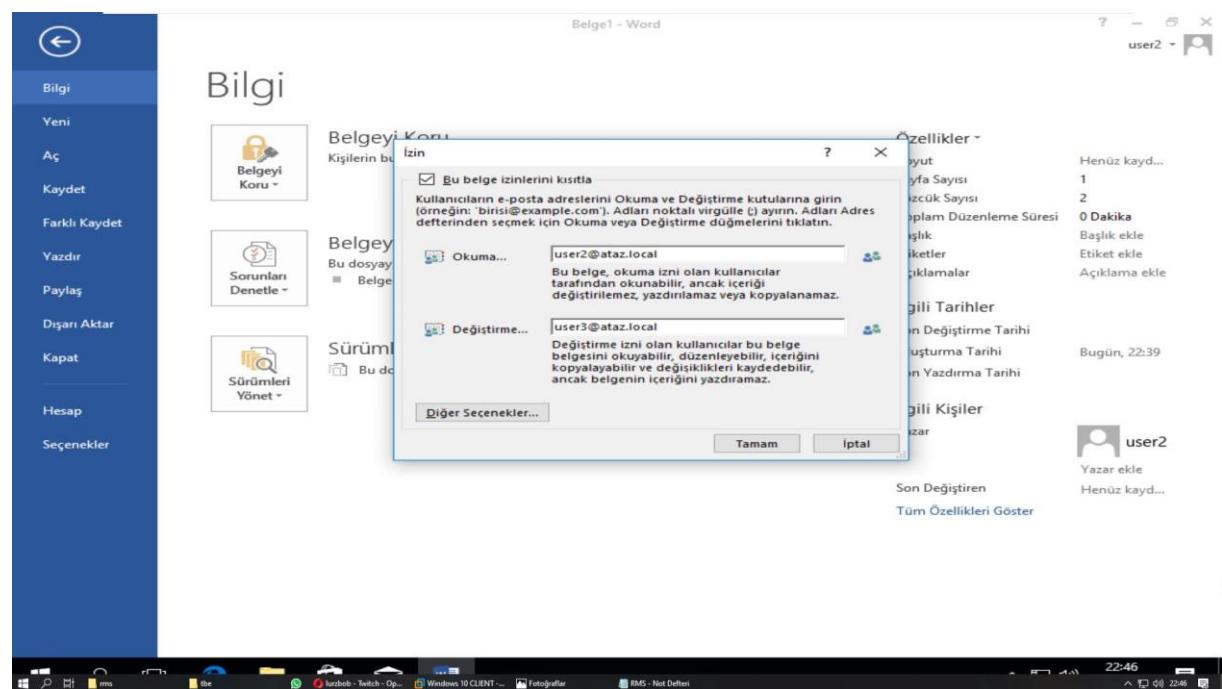
50.Yaptığımız işlemlerle adrese ulaşabiliyoruz.



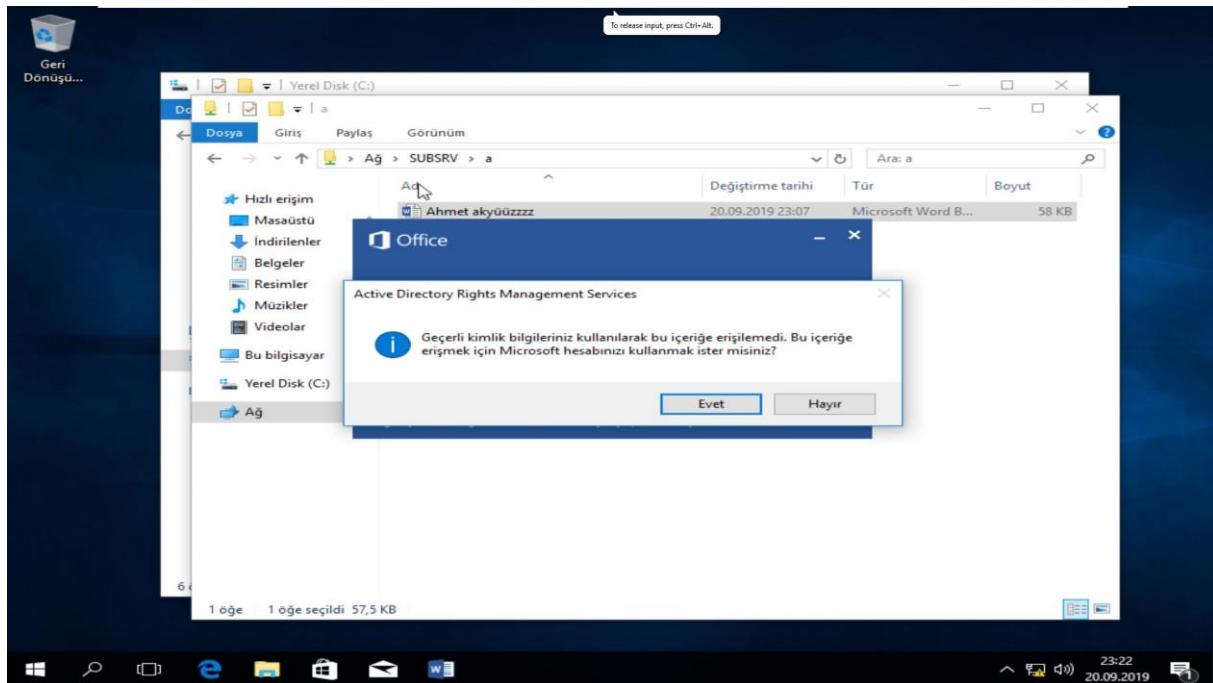
51.Bu aşamadan sonra artık yaptığımız işlemleri test etme olayı geçiyoruz. Bunun için Client ile “Executive” grubundan biri ile girip oturum açıyoruz. Daha sonra Internet Explorer açıp “Internet options\Security\Local Intranet\Sites\Advance” tıkla Add seçip “<http://ataz.local> veya kendizinki neyse ekleyelim.



52. Şimdi ise bir Word dosyası oluşturup içine bir şeyler yazıp “Dosya\Bilgi\Belgeyi Koru\Erişimi Kısıtlı” deyip “Sınırlı Erişim” seçelim. Erişim Kısıtlı’da bizim yaptığımız ReadOnly’de göreceksiniz. Sınırlı erişimde Okuma ve Değiştirme olarak kullanıcıları yada grupları seçiyoruz.



53.Yaptımızı dosyayı RMS'de ortak bir klasöre ekleyip paylaşımı açalım ve izin vermediğimiz kullanıcı ile girince dosya açamadık.



54.Aynı sekil de izin verdiğiimiz kullanıcı ile giriş yapınca Word dosyasına eriştiğimizi göreceksiniz.

