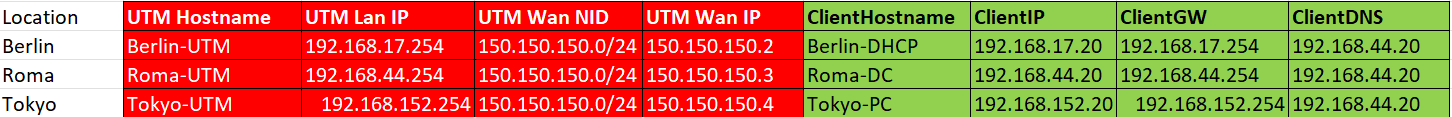
|  |  |
| --- | --- |
| PROJE | |
| ADI | SPQR ÜÇ LOKASYONLU NETWORK PROJESİ |
| TARİHİ | 14.06.2023 - 15.06.2023 |
| ŞİRKET | GÖKALEMİN A.Ş. |
| MÜŞTERİ ÜNVANI | SPQR LTD. ŞTI. |
| SORUMLULAR | Alptuğ ASLAN, Nesrin GÖKALEMİN, Yunus MAMAN |
| DENETLEYİCİ | Turgay KAYA |



**PROJE AMACI**

**3 tane farklı bölgedeki Lan(clientları ve serverları) Wan (Sophos)tek bir domain çatısı altında toplayıp birbirleriyle iletişimlerini sağlanıp active directory ve UTM kontrolünde internet çıkışı sağlamak.**

**PROJE BİLEŞENLERİ**

**PROJE ANA HATLARI**

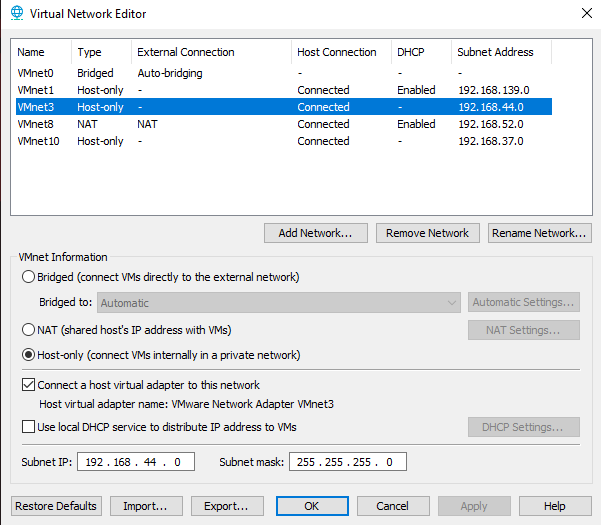
**Roma Lokasyonu:** Roma lokasyonunda Client ve DC kuruldu, DC üzerine AD DS(Active Directory Domain Server), DNS(Domain Name Server) kuruldu.

**Berlin Lokasyonu:** Berlin lokasyonunda Client ve W19 Server kuruldu, W19 Server üzerine DHCP kuruldu.

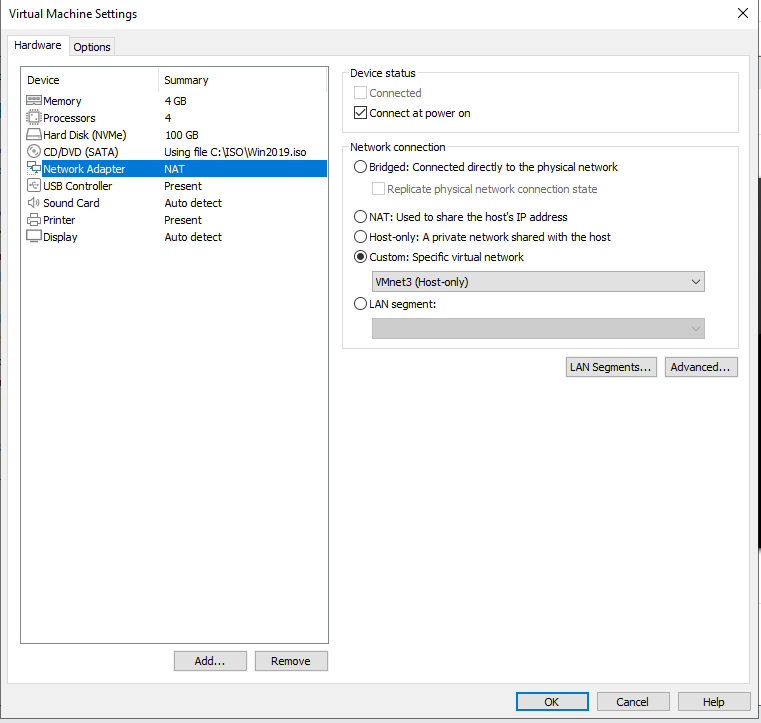
**Tokyo Lokasyonu:** Tokyo lokasyonunda Client ve W19 Server kuruldu.

**PROJE DETAYLARI**

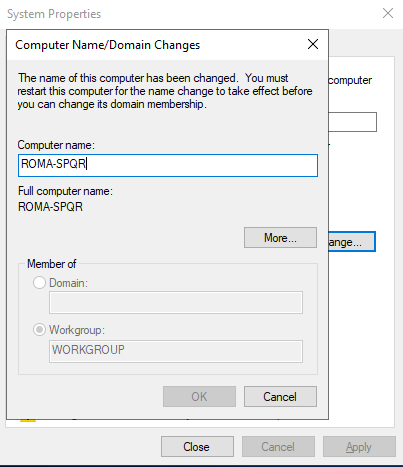
* Her bir lokasyon için Ip Network belirlendi.
* Merkez lokasyonda belirlendi bir DC konumlandırıldı: ROMA
* Konumlandırılan DC üzerine verilen Görevler: ADDC, GC ve DNS



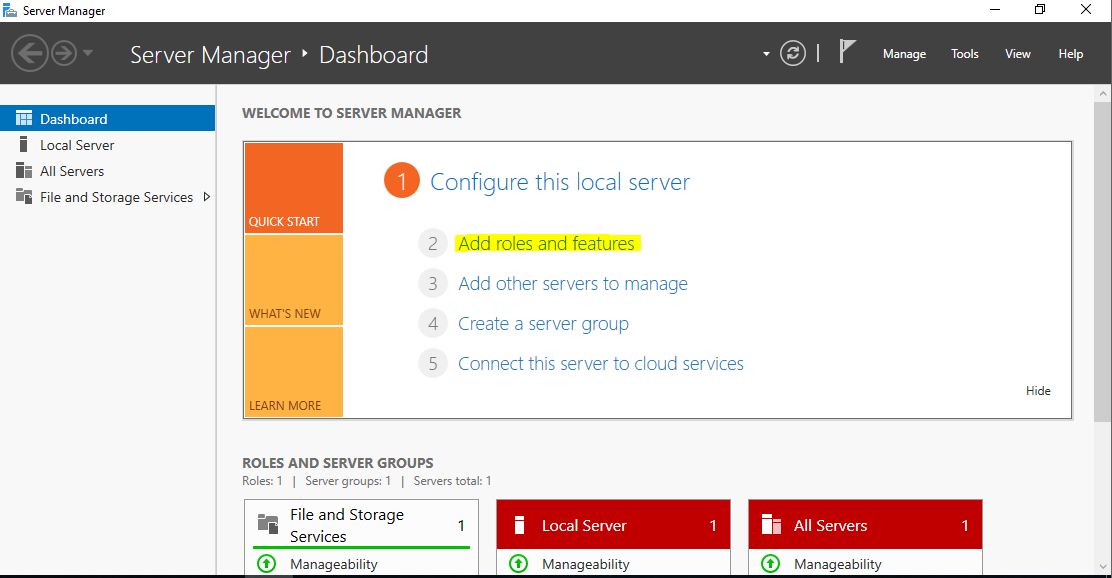
1. Virtual network adaptör olarak Vm3 kullanıldı



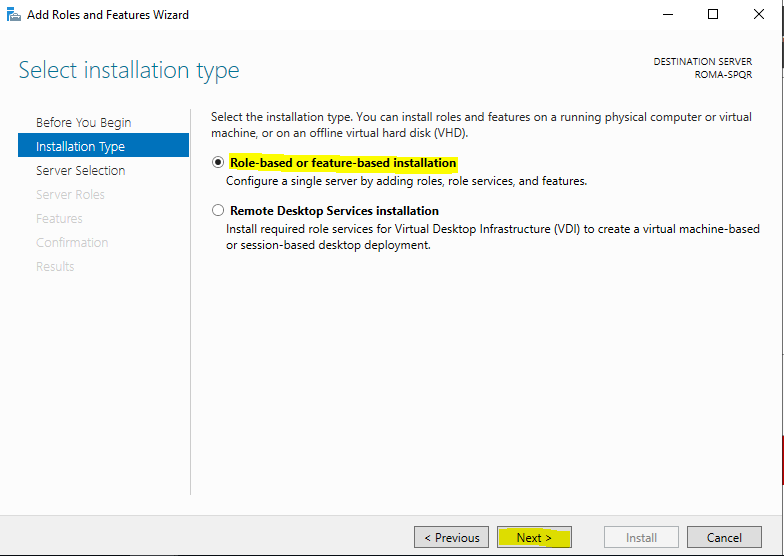
1. Vmnet 3 adaptörü takıldı



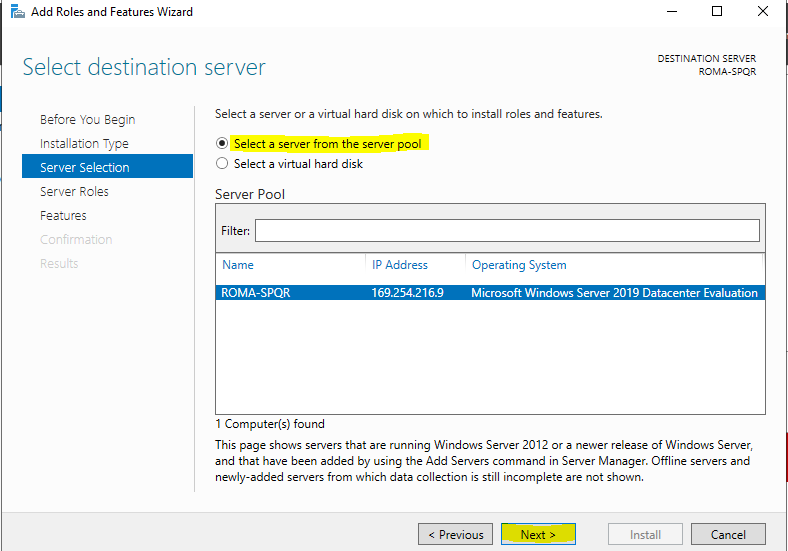
1. Bilgisayarın ismi ROMA-SAPQR olarak değiştirildi



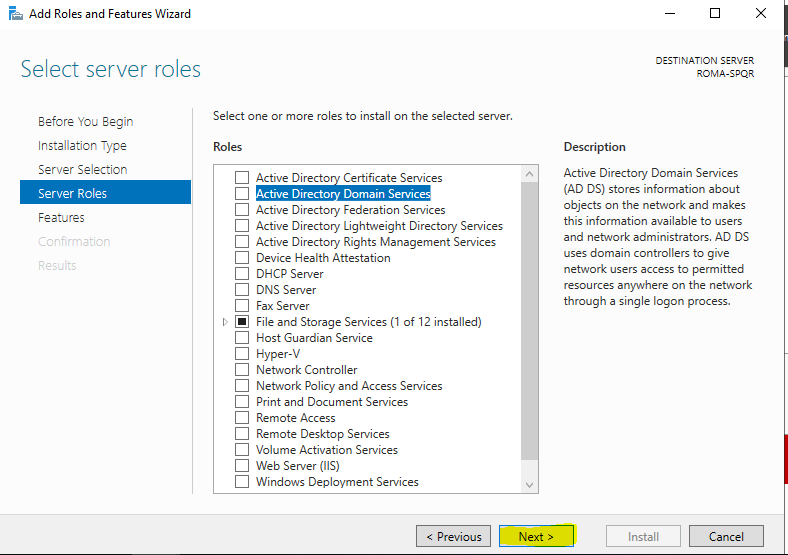
1. Add roles and features kısmından Active Directory site and services rolü eklemek için tıklıyoruz



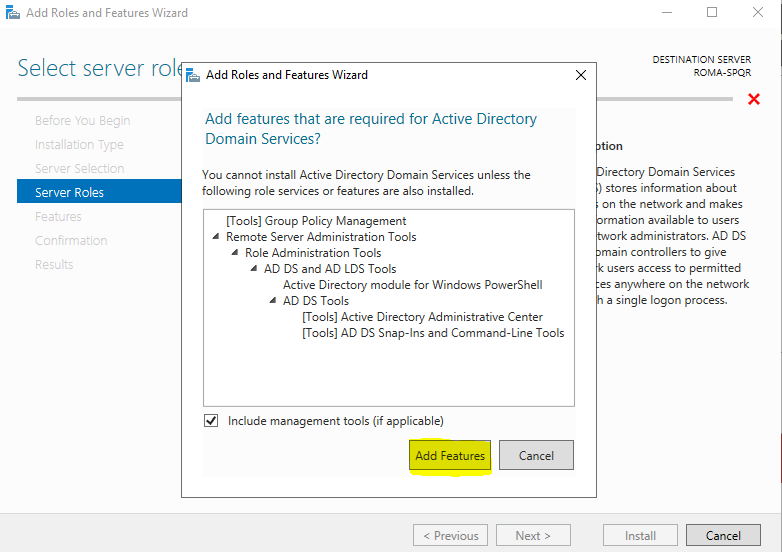
1. Uzaktan bağlanarak değil basit kurulum yaparak ilerleyeceğiz



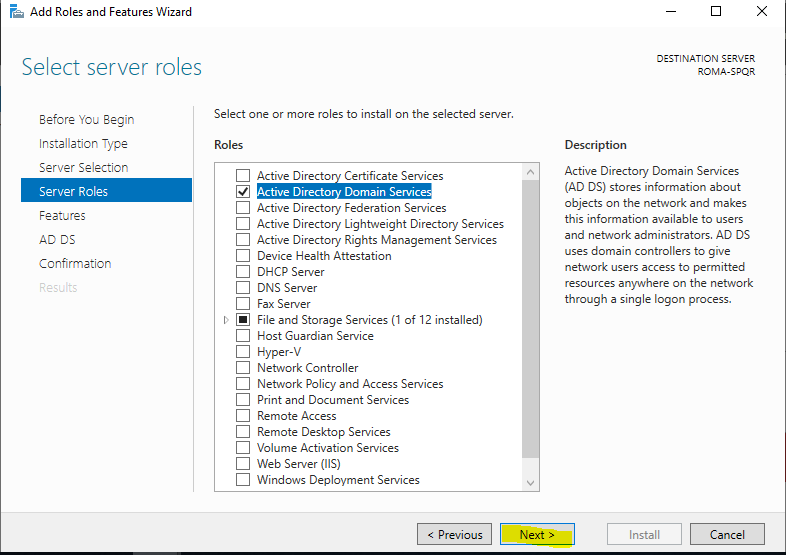
1. Server poolundan kendi serverımızı seçiyoruz



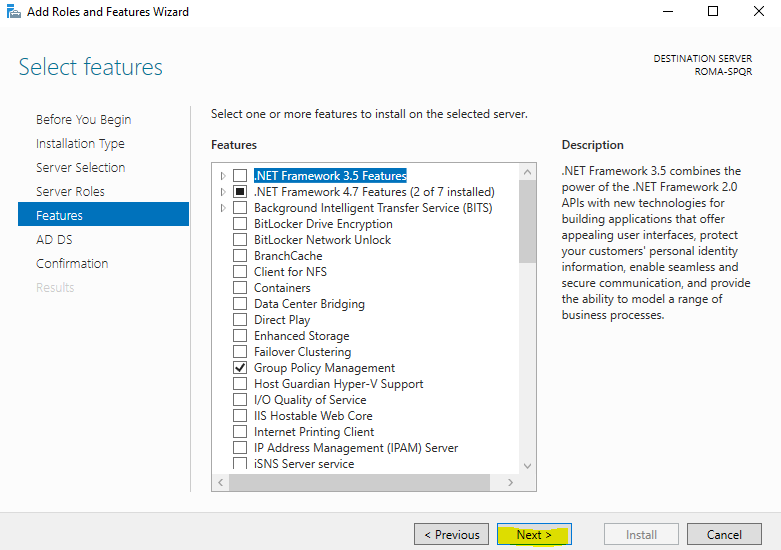
1. Server rollerden Active Directory Domain Services seçildi



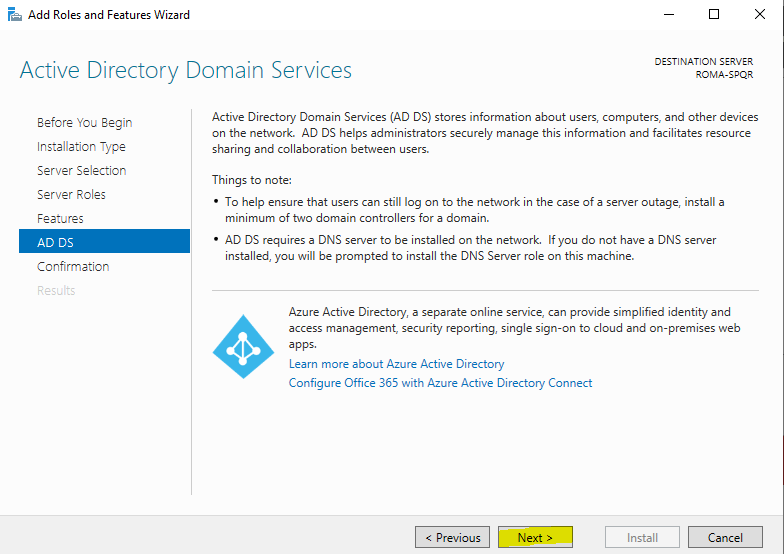
1. Eklemiş olduğumuz tüm toollar bilgilendirme olarak karşımıza çıkıyor Add featuresa tıklayıp sonlandırıyoruz.



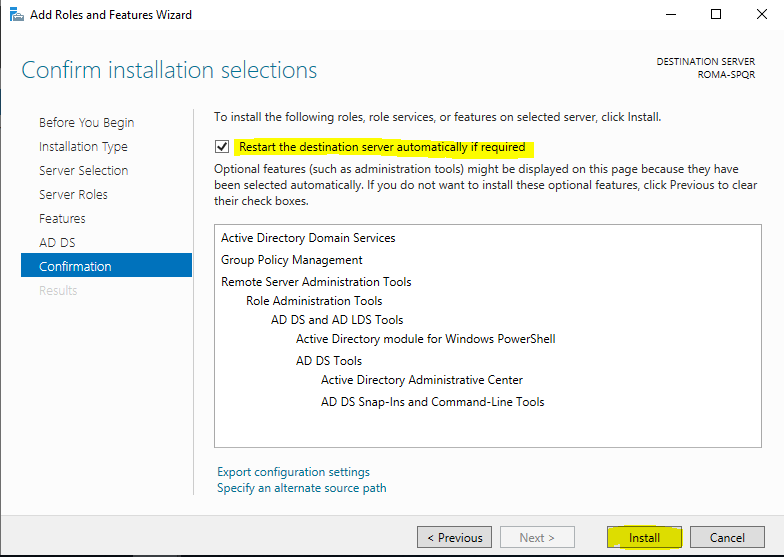
1. Rollerden Active Directory Services rolünü seçiyoruz.



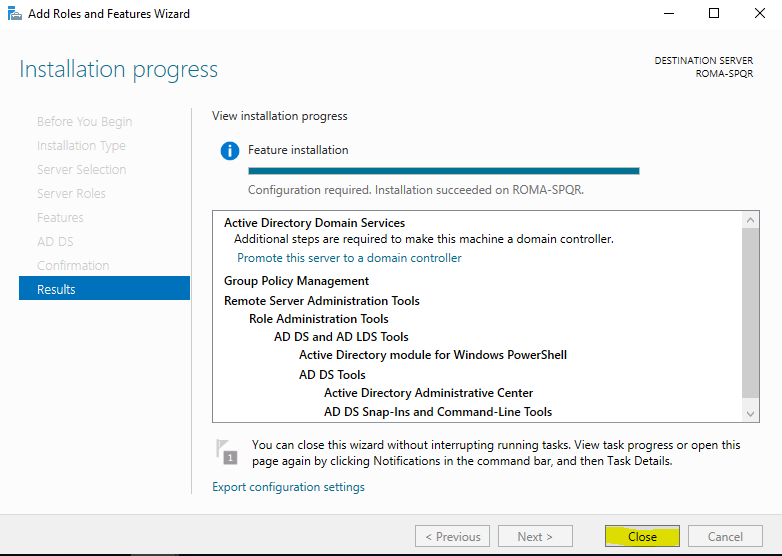
1. Features kısmından otomatik olarak gelen rollerle devam ediyoruz.



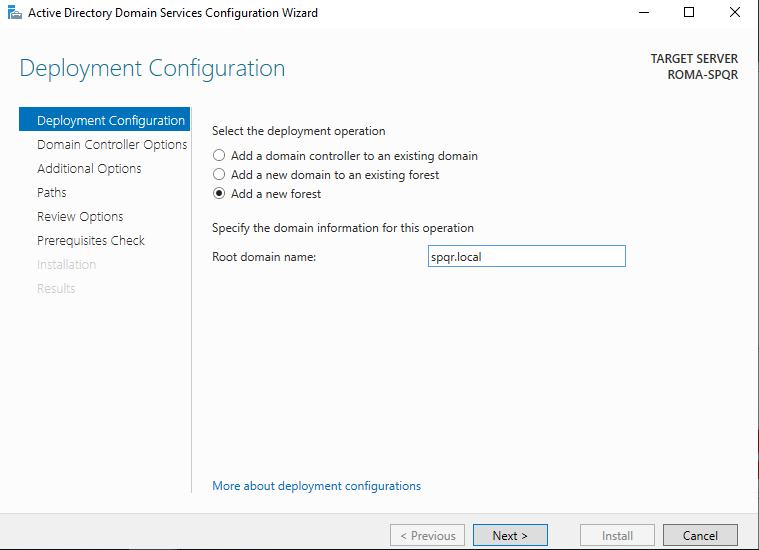
1. Kurmuş olduğumuz serverı Azure ile birlikte çalıştırmak için yapabileceğimiz ayar kısmı
2. Azure server bağlantısı yapmıyacağız



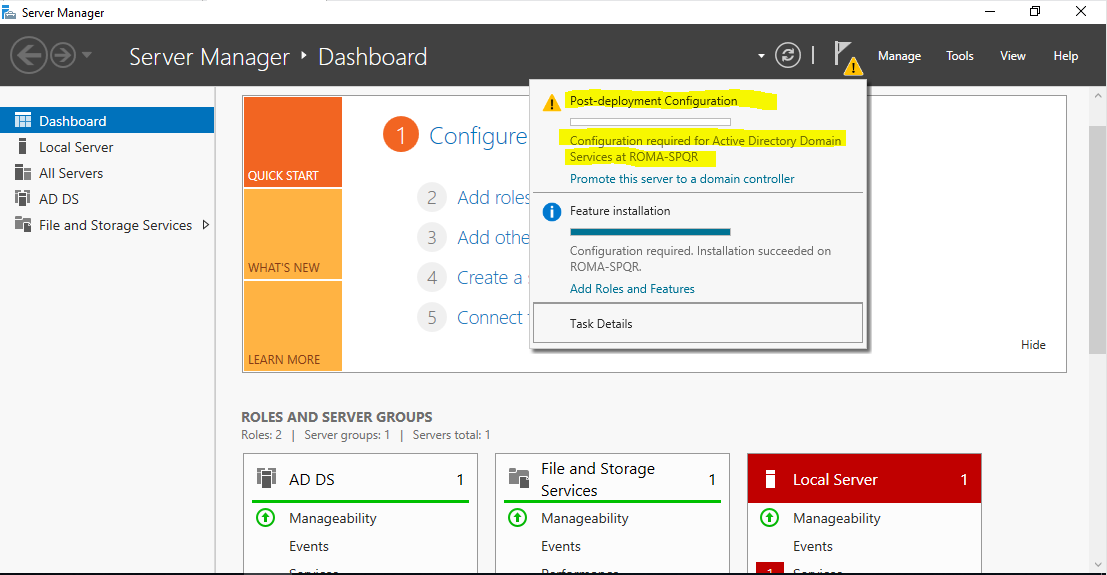
1. Active Directory Domain Services rolünü ekledikten sonra beraber gelen özellikleri özet olarak bize sunuyor ardından role eklendikten sonra restart edilmesi için yukarıdaki kutucuğu işartetliyoruz.



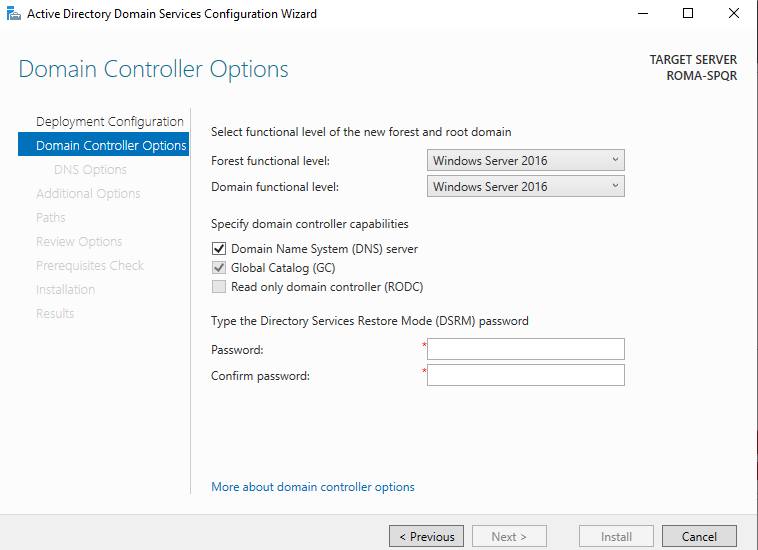
1. Rol kurulumu tamamlandı



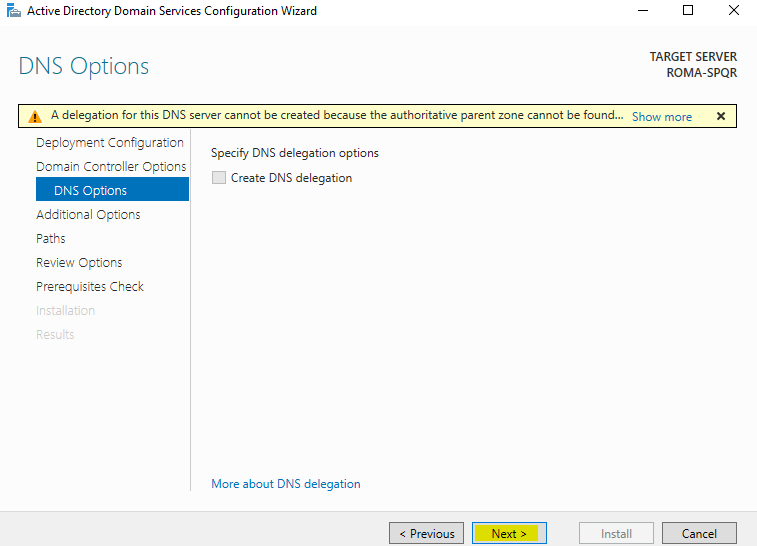
1. Domain ismimizi “spqr.local “olarak veriyoruz



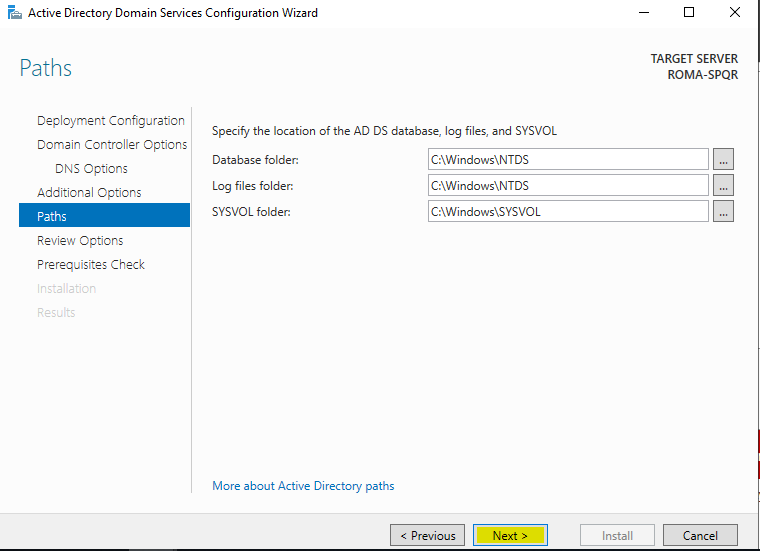
1. Ardından promete etmek için flags kısmından ilerliyoruz.



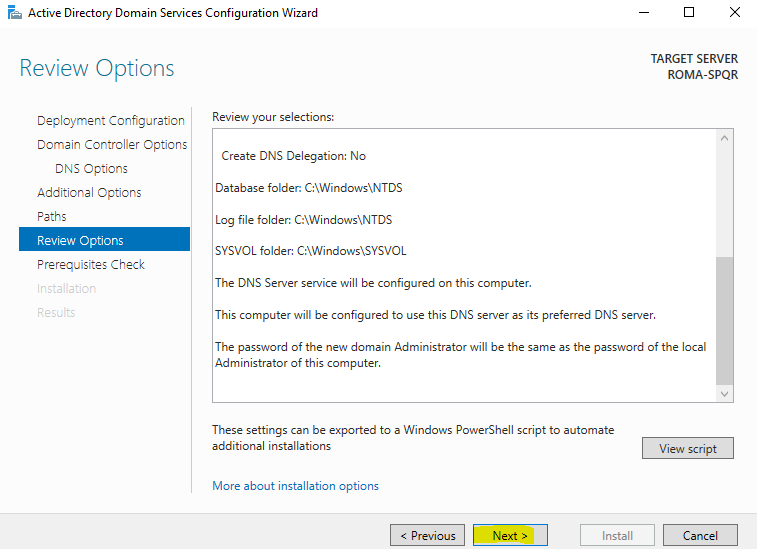
1. Domain control ayarları olarak forest function level Windows server 2016
2. Domain functional level Windows Server 2016 seçiyoruz
3. Domain ayarları yapılırken Dns Server ve Global katalog kurulumu gerçekleşmesi için kutucukları işaretliyoruz.



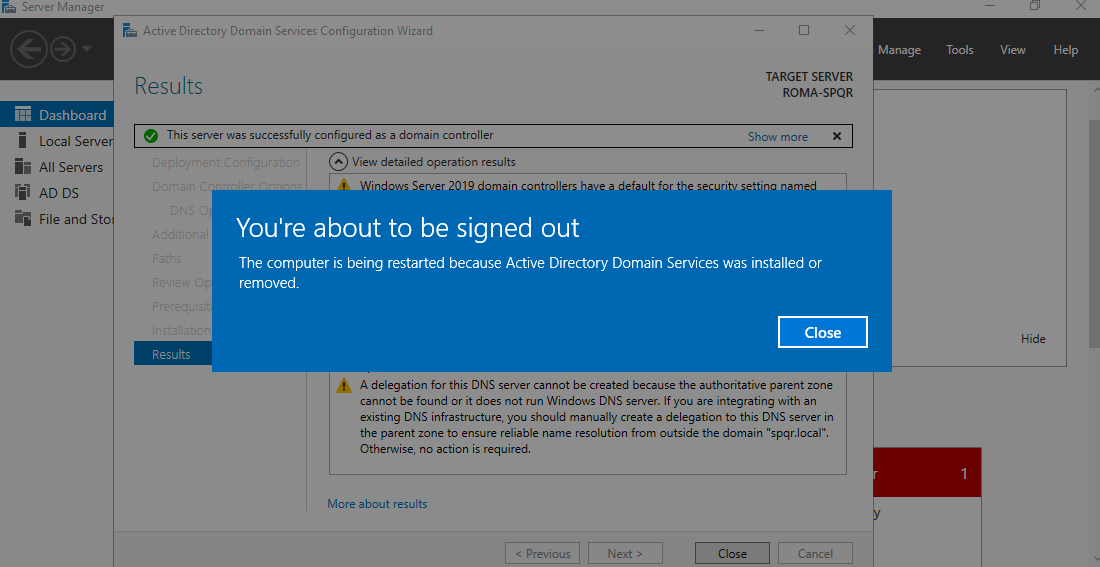
1. Dns ayarları yapmıyoruz



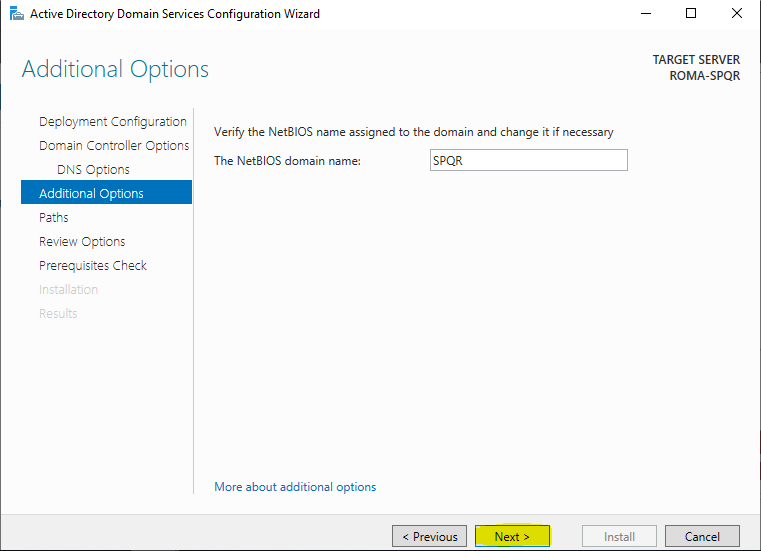
1. Databese folder dosya yolu olarak C\\Windows\NTDS
2. Log files folder dosya yolu olarak C\\Windows\NTDS
3. SYSVOL folder dosya yolu olarak C\\Windows\SYSVOL
4. Dosya yolları belirlendi



1. Yaptığımız ayarları özet olarak görüyoruz istersek yaptığımız ayarların powerchell kodları olarak View Scripts kısmından alabilriz.



1. Ardından oturumdan düşüyoruz.



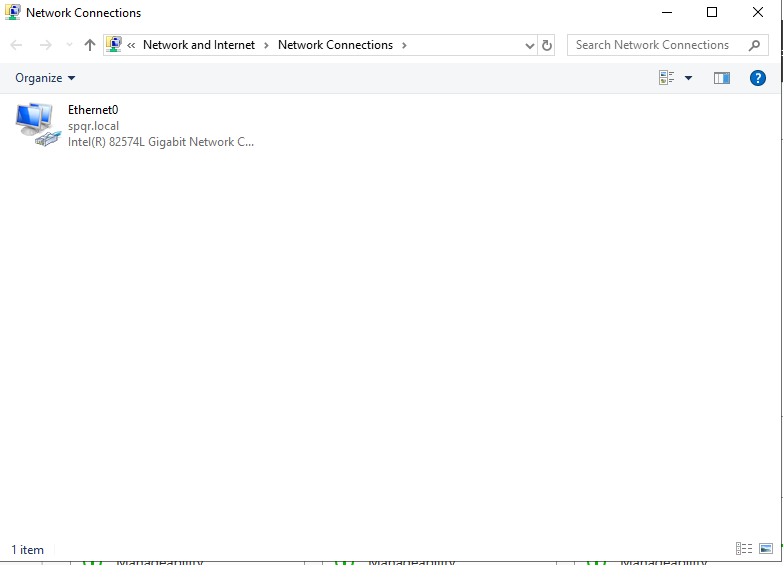
1. NetBIOS domain name SPQR olarak oluşturuldu



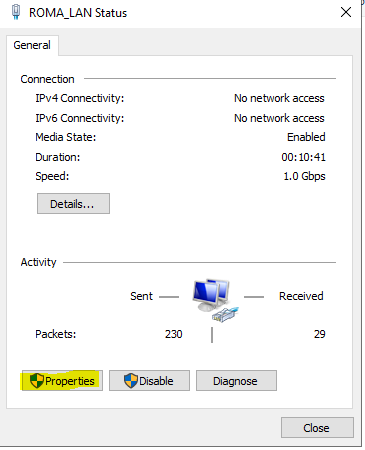
1. Yaptığımız ayarlar servera uygulanıyor.



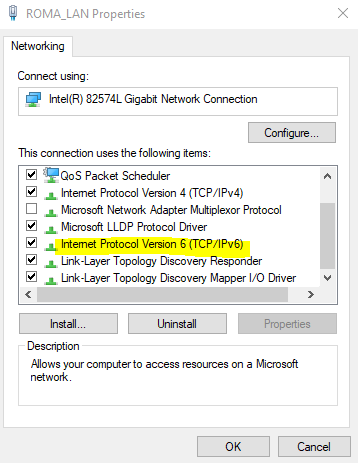
1. Oturum açılışı yapılıyor
2. Network ayarları



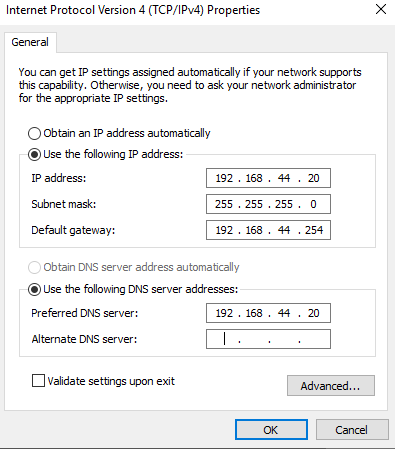
1. Ethernet0 “RomaLan olarak değiştiriliyor.



1. Poroperties kısmına tıklıyoruz.



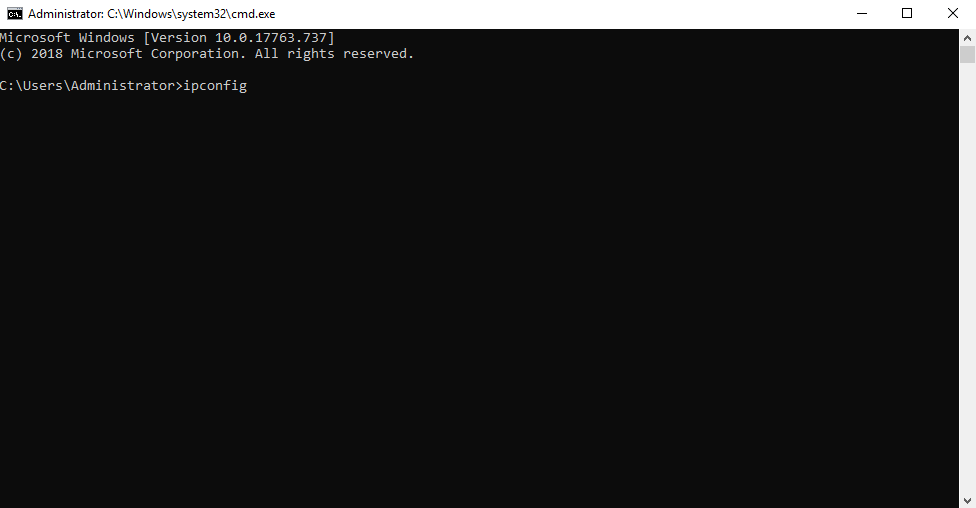
1. Internet Protocol Version 6 (TCP/IPv6) kapatılıyor.
2. Ardından Internet Protocol Version 4 (TCP/IPv4) ün içine giriliyor.



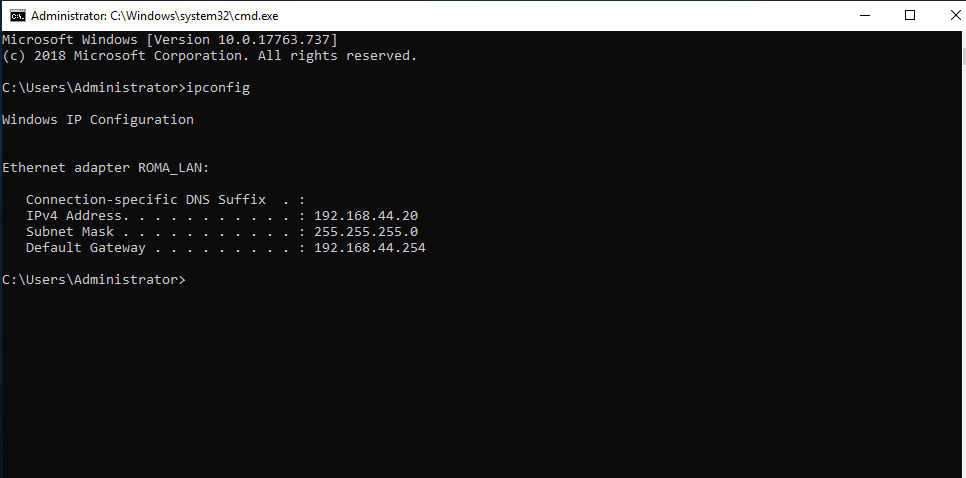
1. Network ayarları static olarak giriliyor.



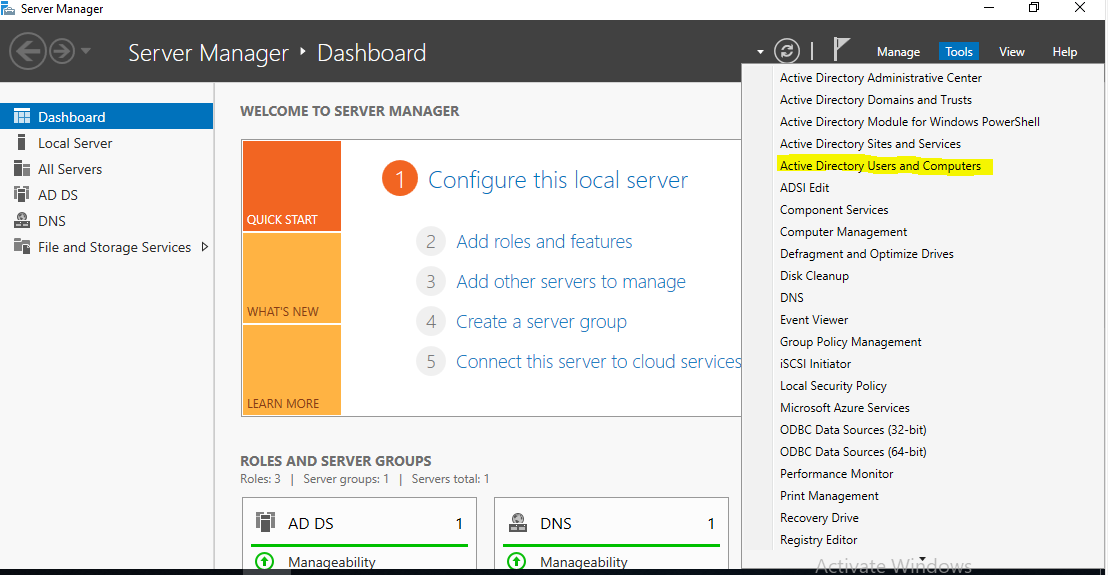
1. Ardından cmd çalıştırılıyor.



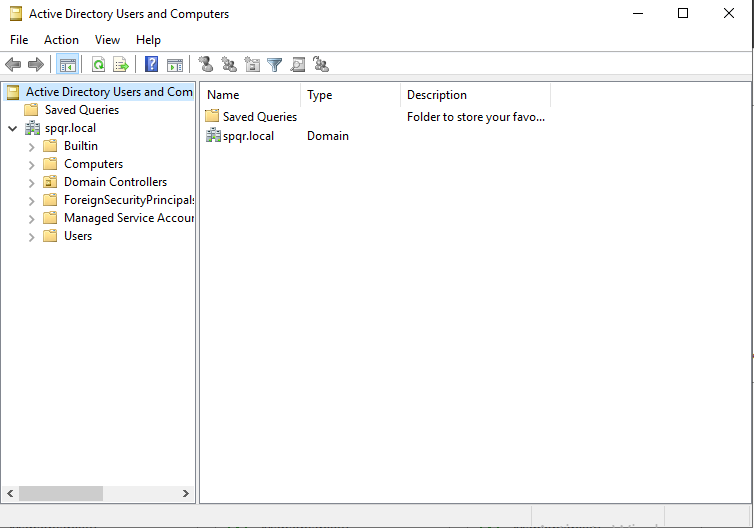
1. Komut ekranında İpconfig komutu ile network bilgilerimizi çağrıyoruz.



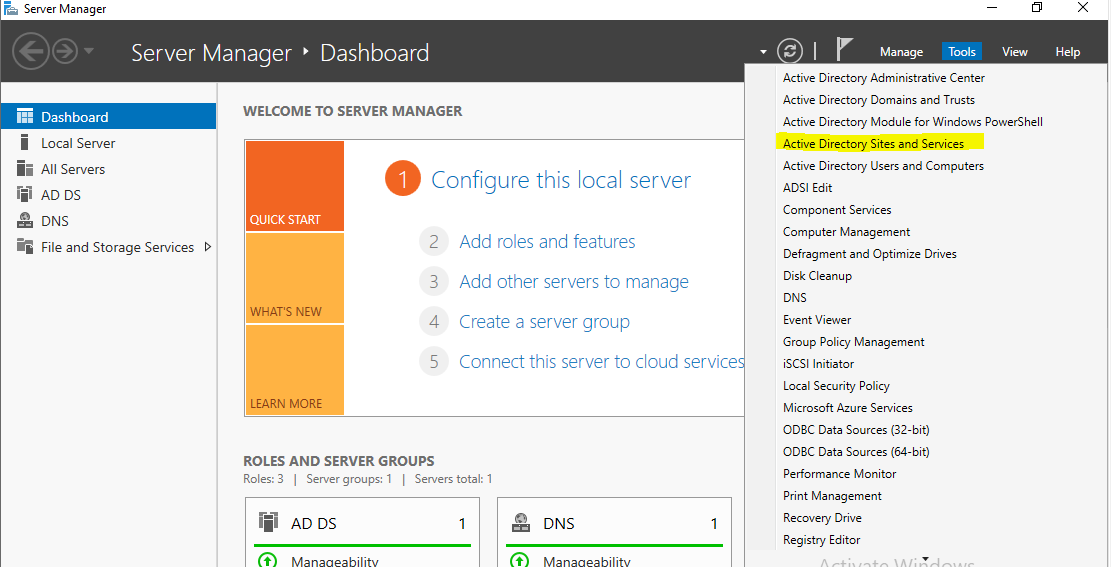
1. Ardından komut ekranında beliren network bilgilerini doğruluyoruz.



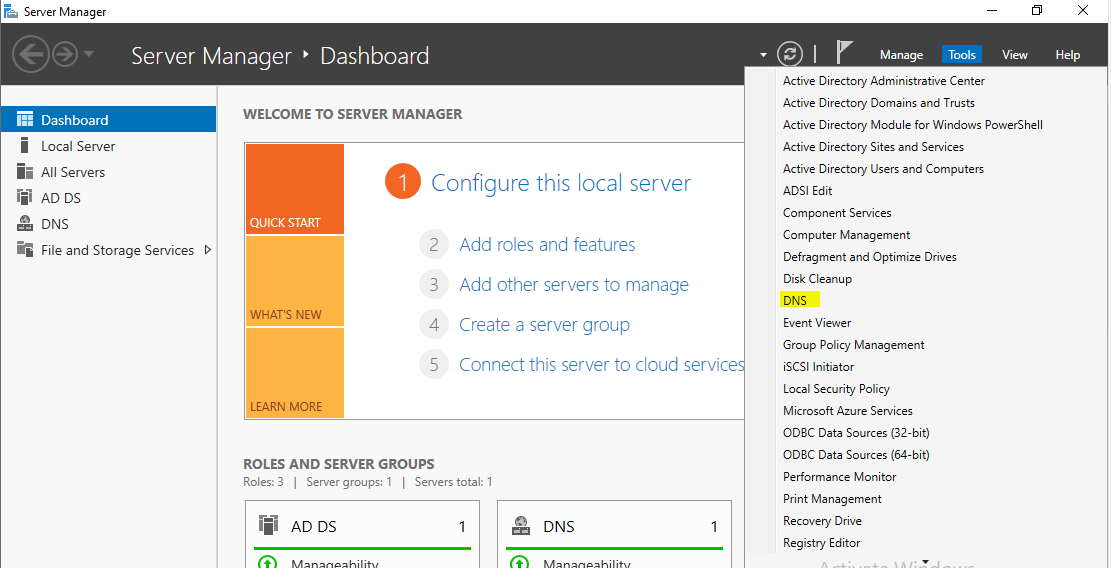
1. Tools kısmından Active Directory Users and Computers bölümüne giriyoruz.



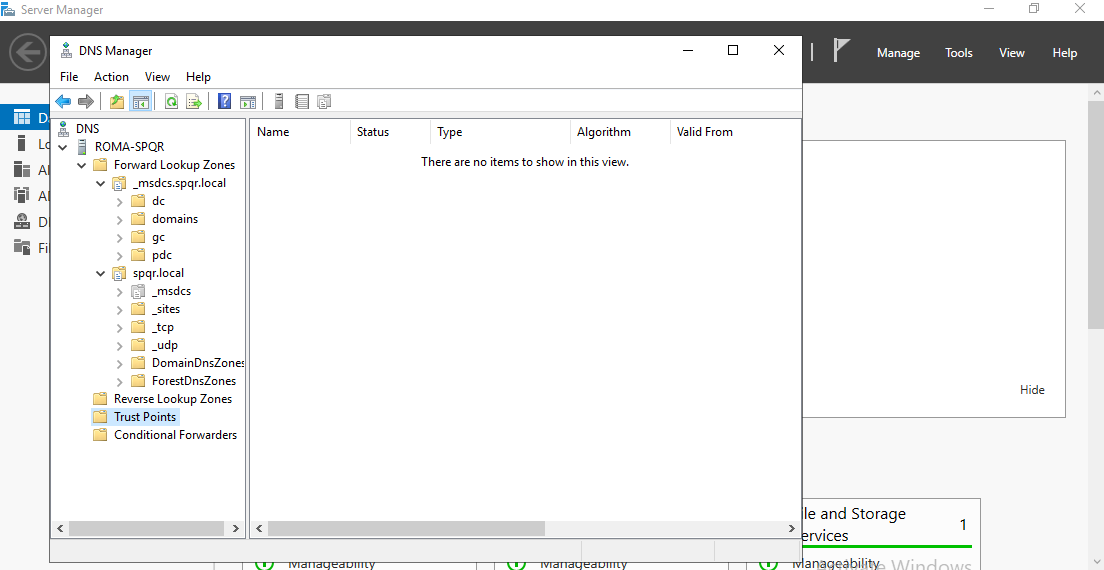
1. Serverımızın Active Directory Users and Computers kısmı resimde görüldüğü gibidir.



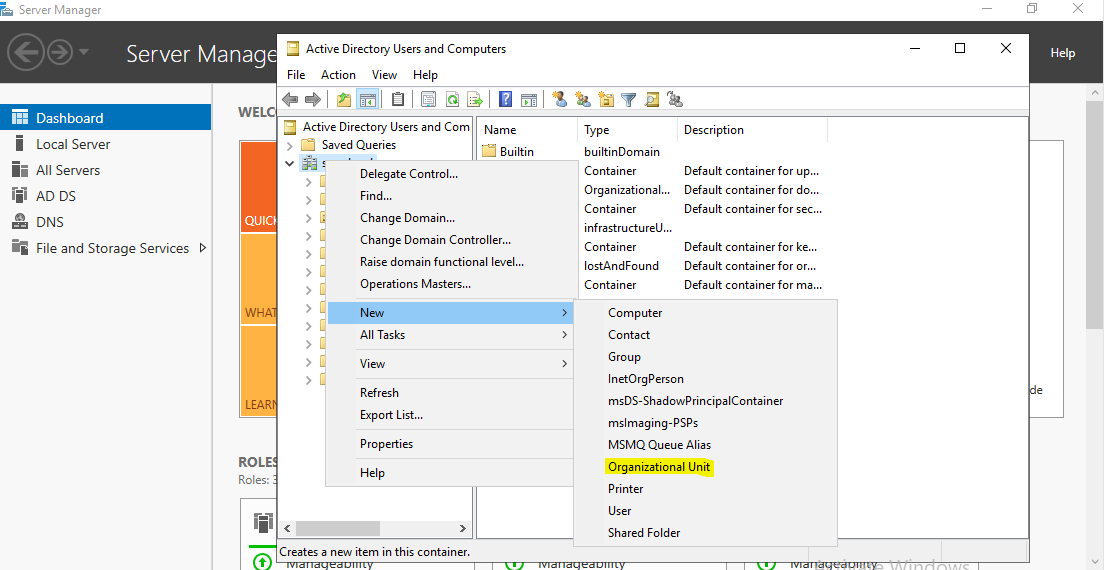
1. Tools Active Directory Site and Services kısmına geçiş yapabiliriz.



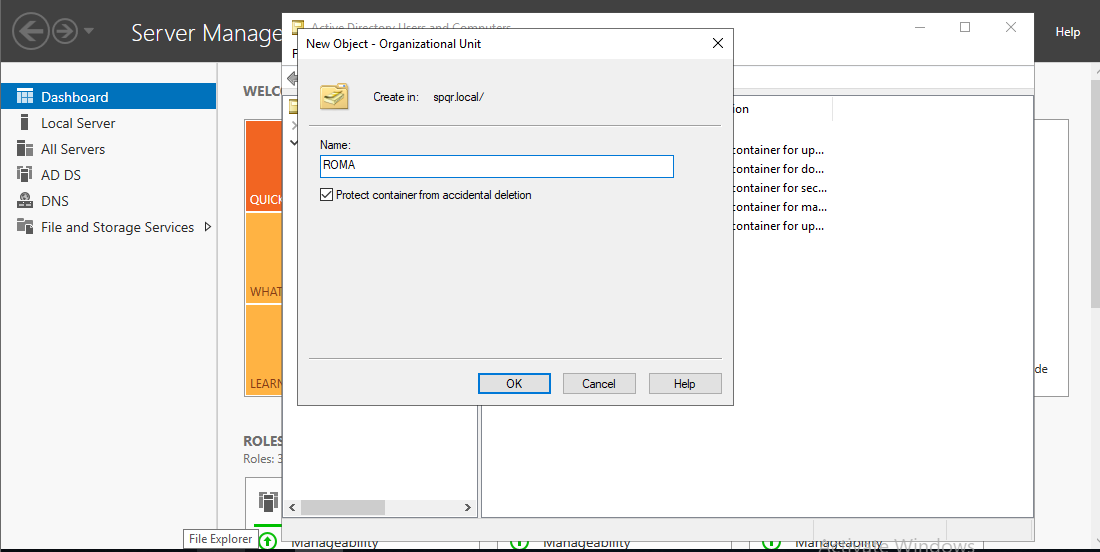
1. Tools Dns kısmından dns ekranına geçiş yapabiliriz.



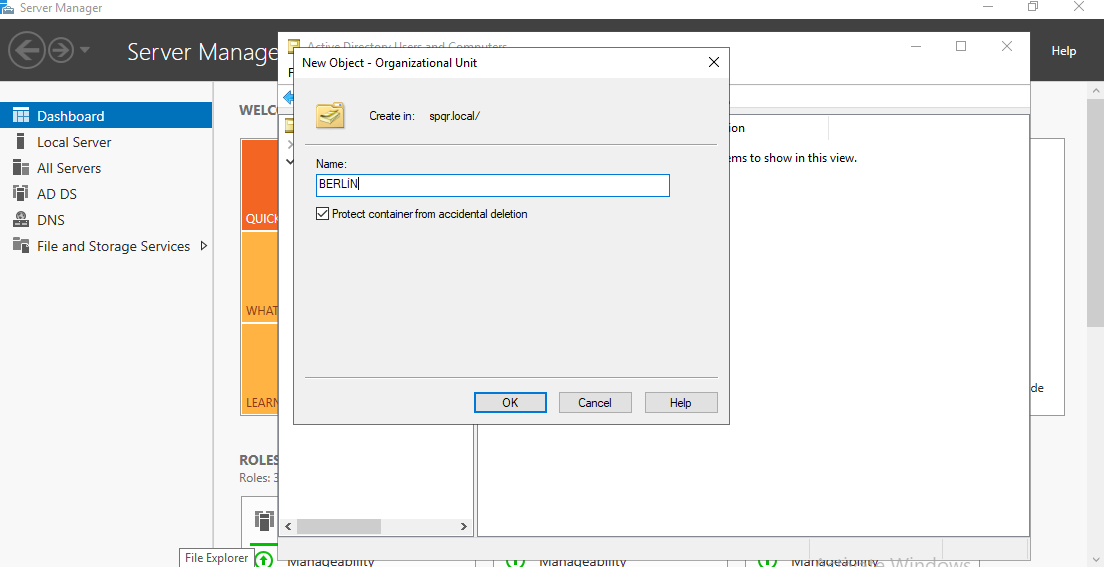
1. Dns Manager ekranımız.



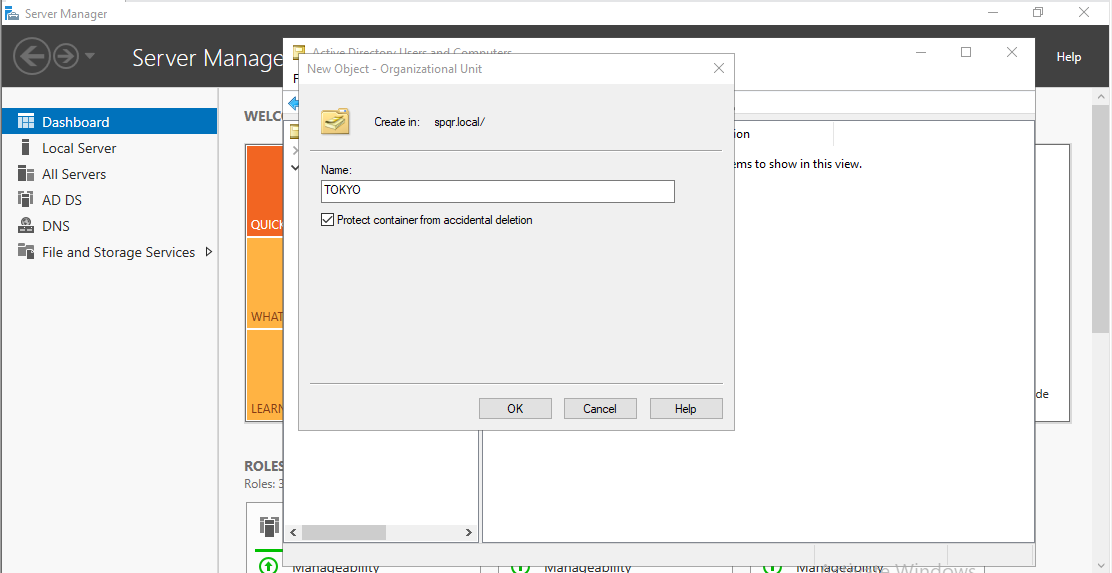
1. Yeni bir organizational Unit oluşturuyoruz.



1. Roma isimli organize unit oluşturuldu



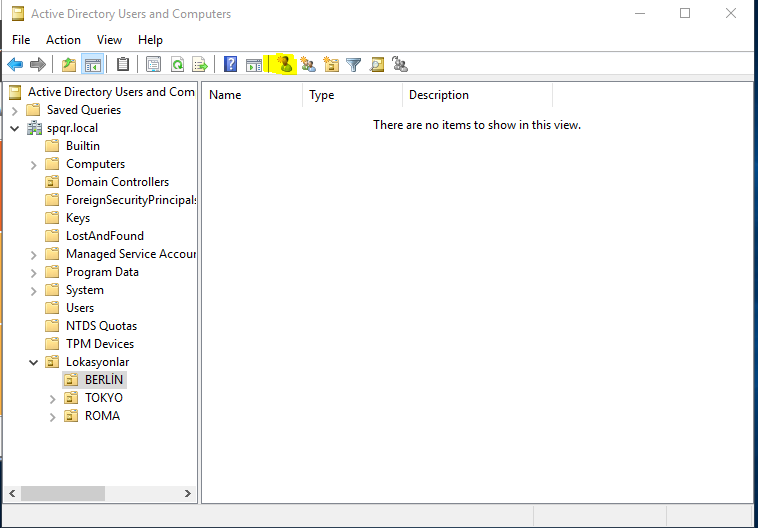
1. Berlin adlı organize unit oluşturuldu.



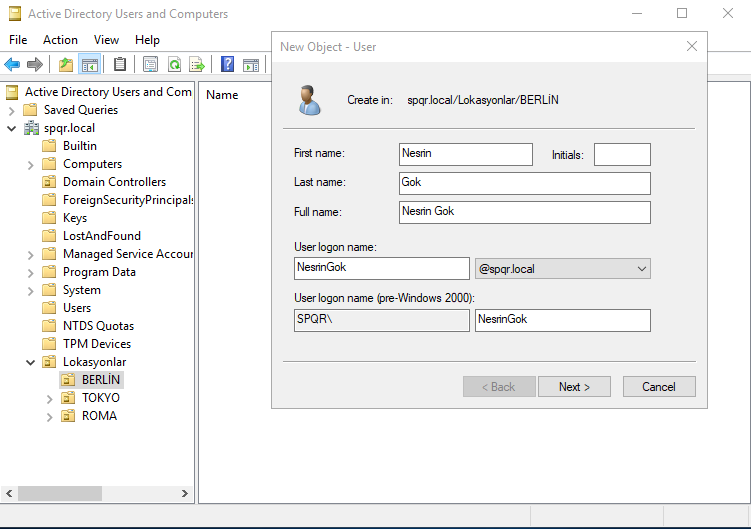
1. Tokyo adlı organize unit oluşturuldu.



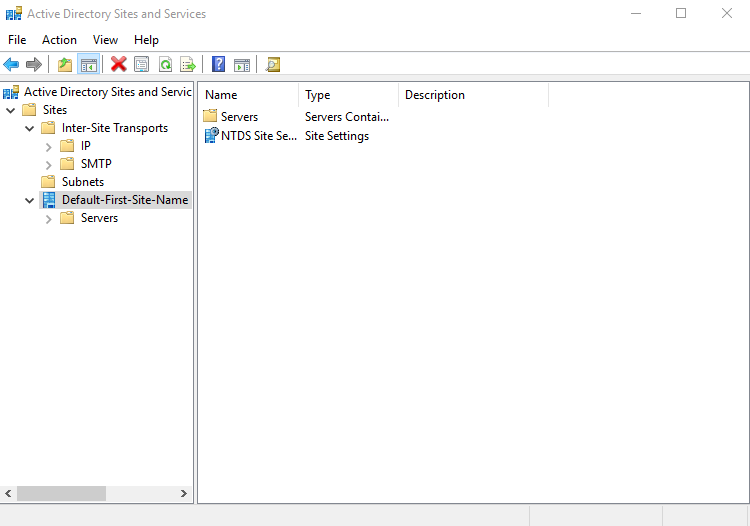
1. Lokasyonlar ekranda görüldüğü gibidir.



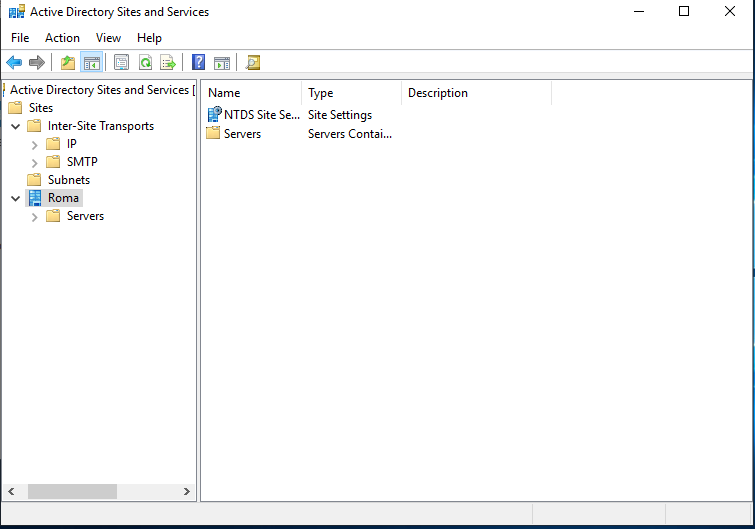
1. Berlin lokasyon içerisine yeni kullanıcı oluşturmak için sarı renkle belirtilen user add kısmına tıklıyoruz.



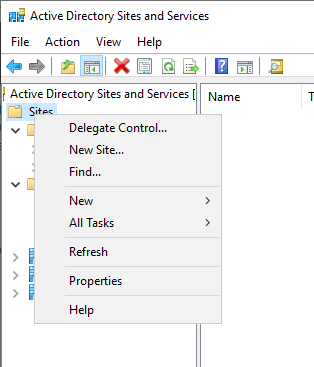
1. Berlin Nesrin gök adlı kullanıcı oluşturuldu.
2. Roma Yunus Maman adlı kullanıcı oluşturuldu.
3. Tokyo Alptug adlı kullanıcı oluşturuldu.



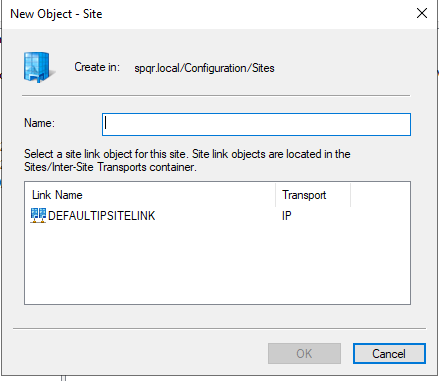
1. Active Directory Sites and Services kısmında Default-First Name değiştiriliyor.



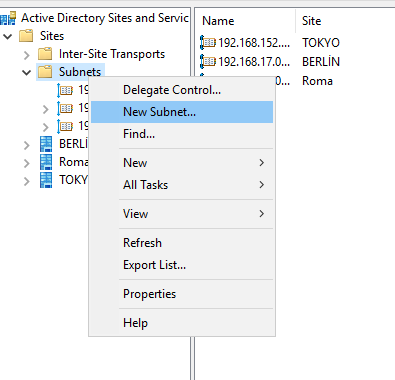
1. Active Directory Sites and Services kısmında Default-First Name Roma olarak değiştirildi.



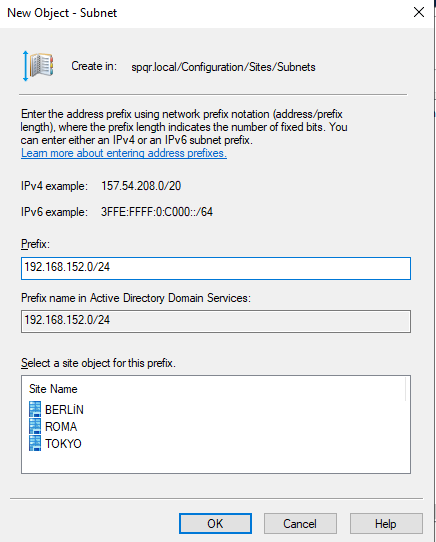
1. Sites kısmından yeni site oluşturuyoruz.



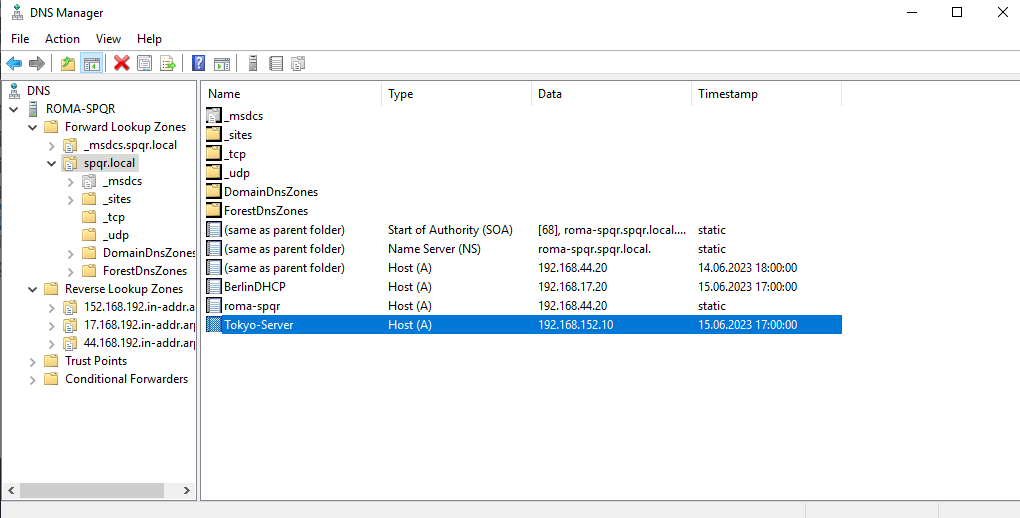
1. Oluşturacağımız Site’nin ismini yazıyoruz ve DEFAULTIPSITELINK’i seçiyoruz, ardından ok diyoruz ve sitemiz oluşuyor.



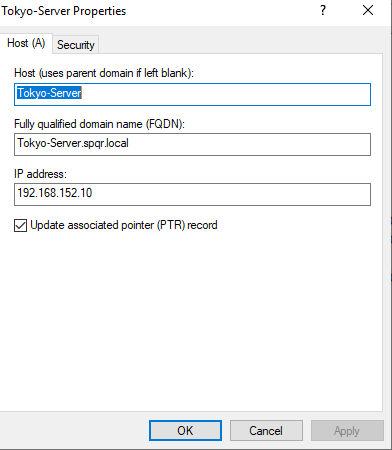
1. Sitemizi oluşturduktan sonra site’nin subnet’ini oluşturmamız gerekiyor ve Subnet klasörüne sağ tıklayıp ‘New Subnet’ seçeneğine tıklıyoruz.



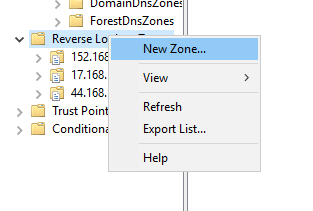
1. Ardından Prefix bölümüne Site’nin network adresini yazıyoruz, sitemizi seçiyoruz arından ok diyoruz.



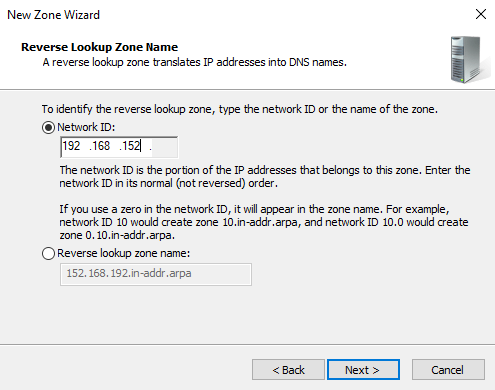
1. Daha sonrasında DNS konfigürasyonu için DNS Manager’e giriyoruz ve A kayıtlarını kontrol ediyoruz.



1. Serverlarımızın ‘PTR’ kayıtları için bir ‘A’ kaydına sağ tıklayıp arından properties’e tıklıyoruz, ‘PTR’ kayıtlarını oluşturmak için ‘Update associated pointer (PTR) record’u tikliyoruz ve ok diyoruz.

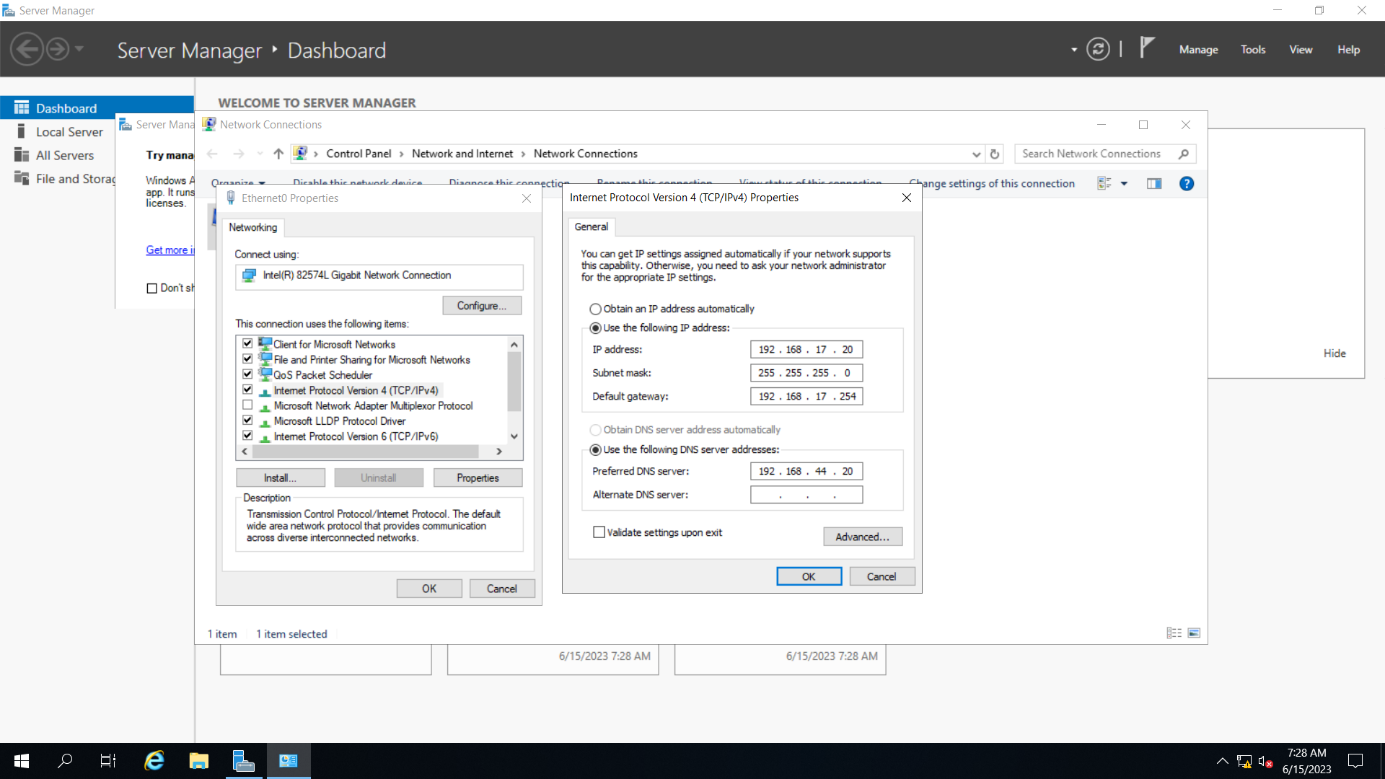
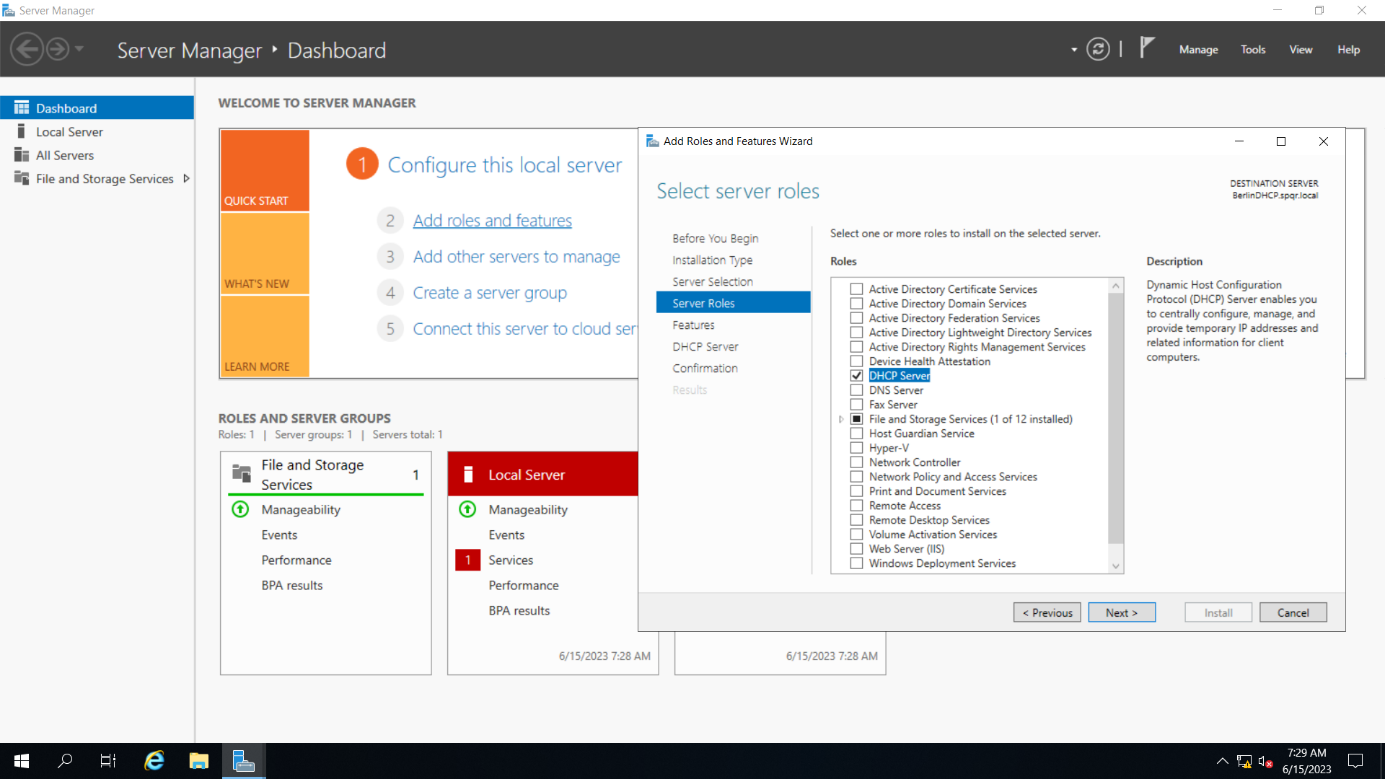
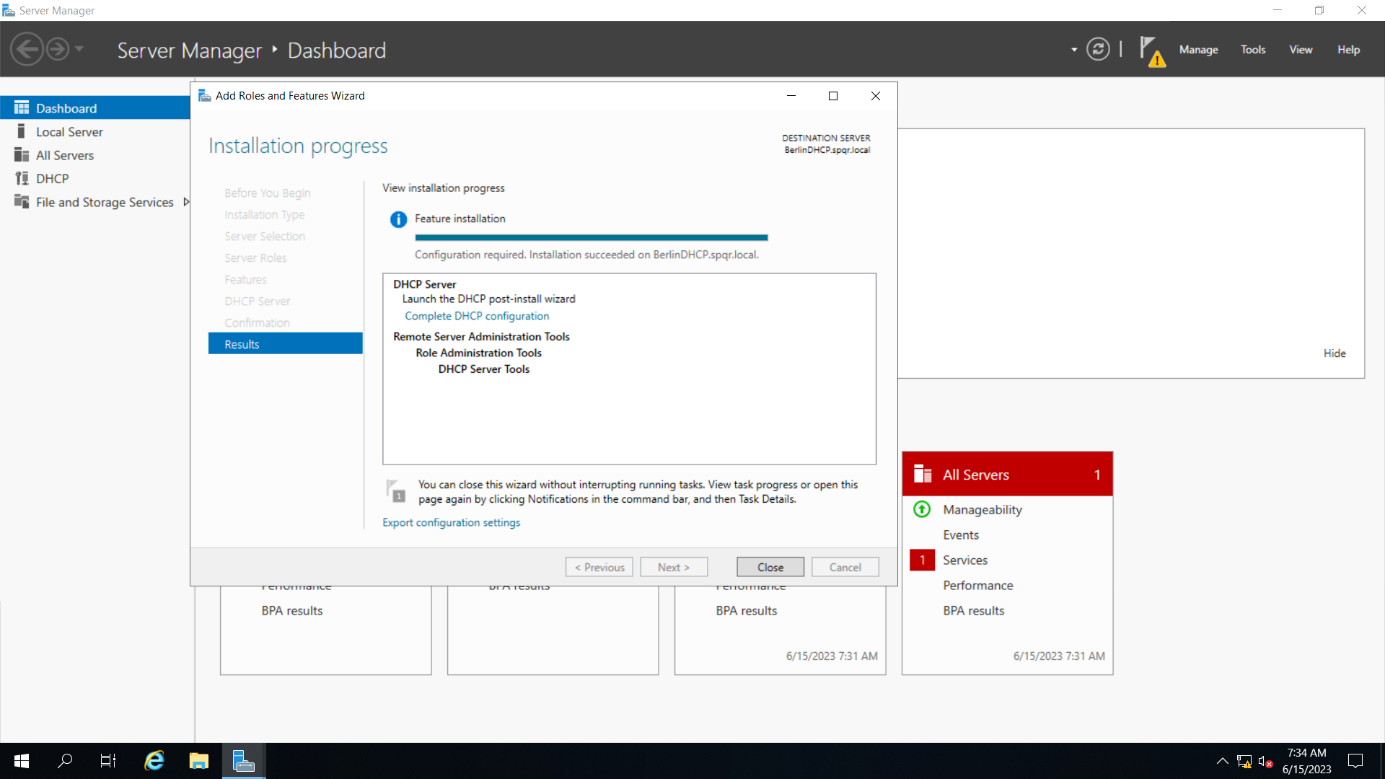
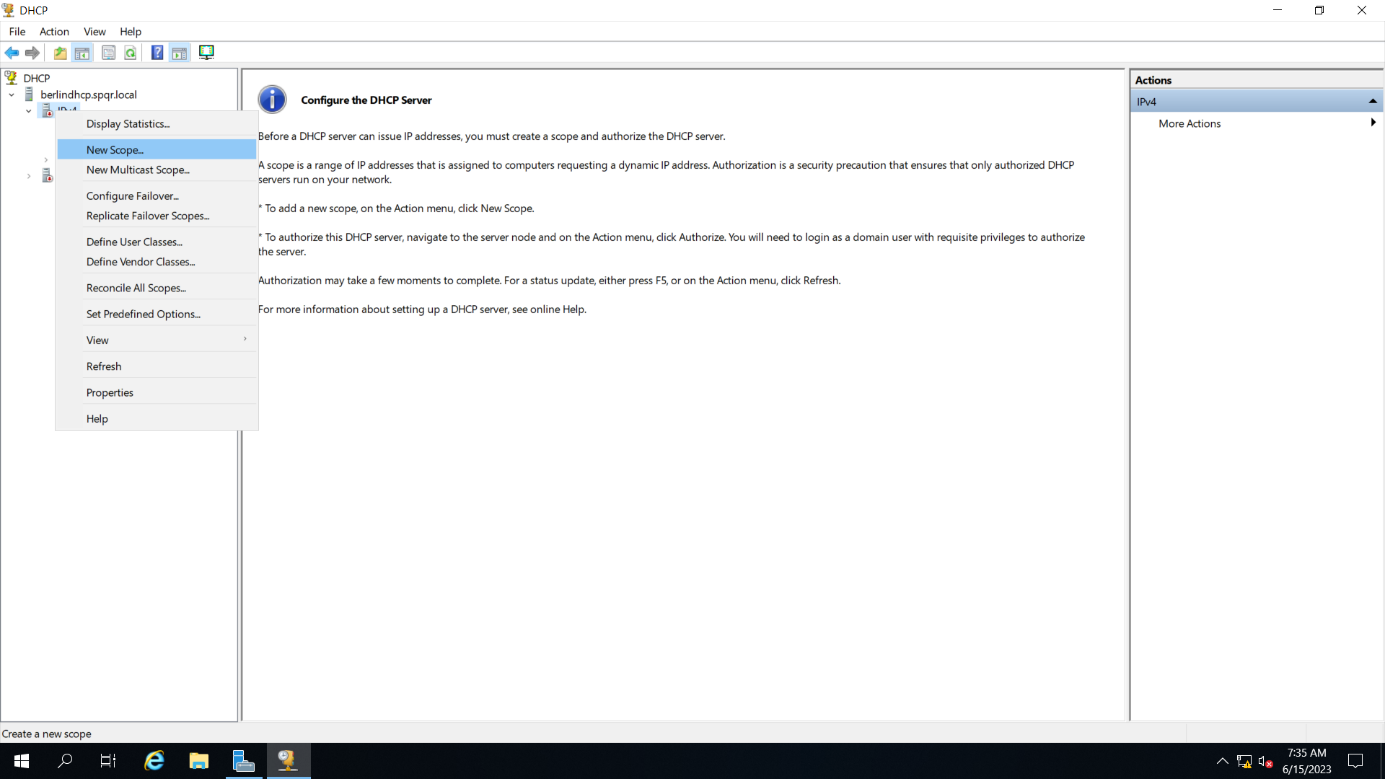
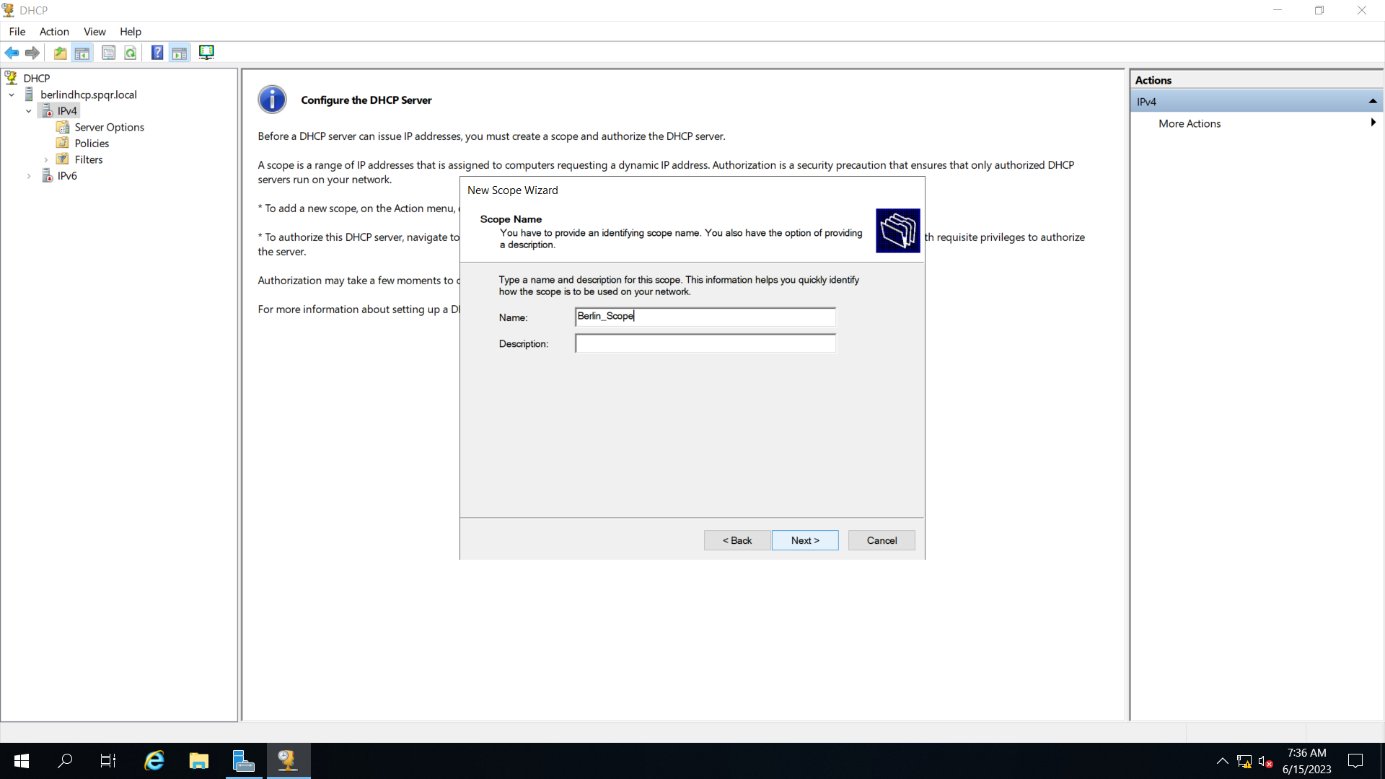
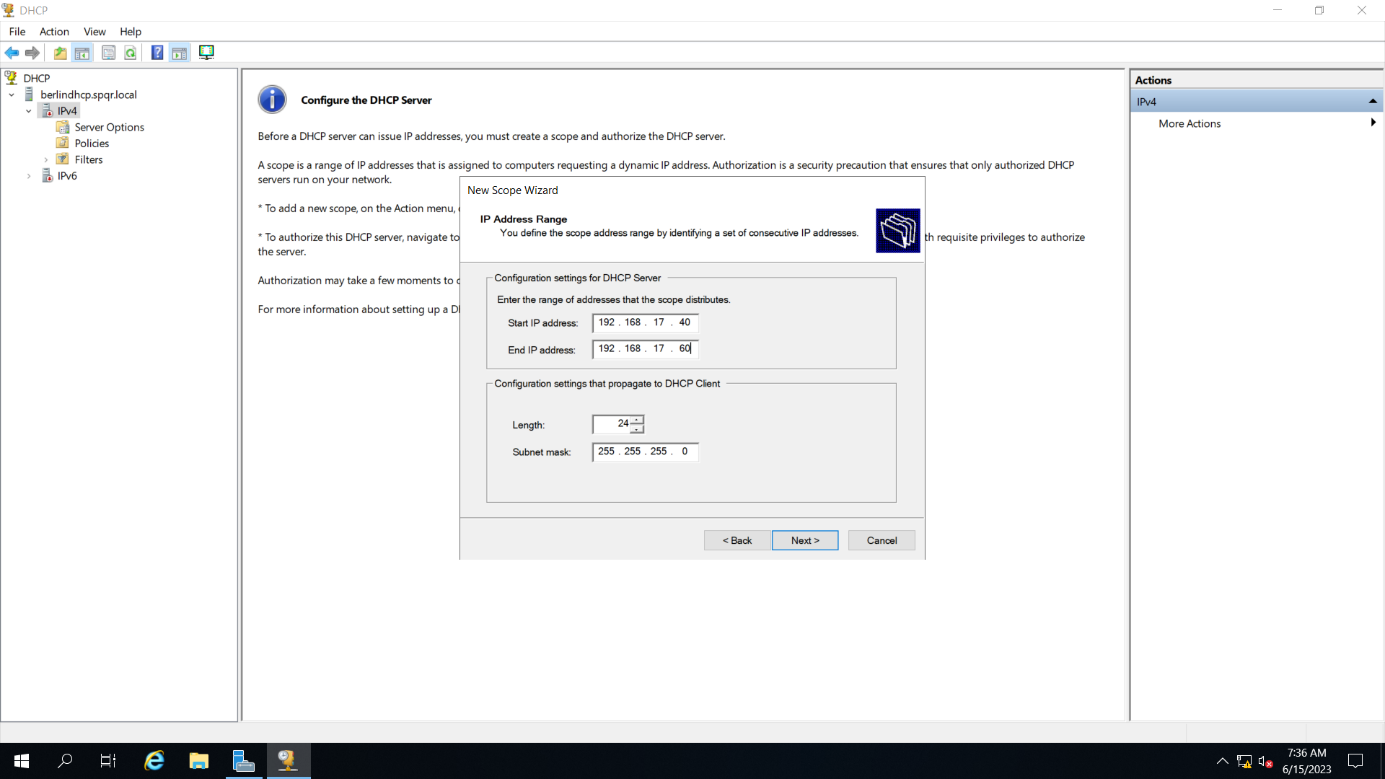


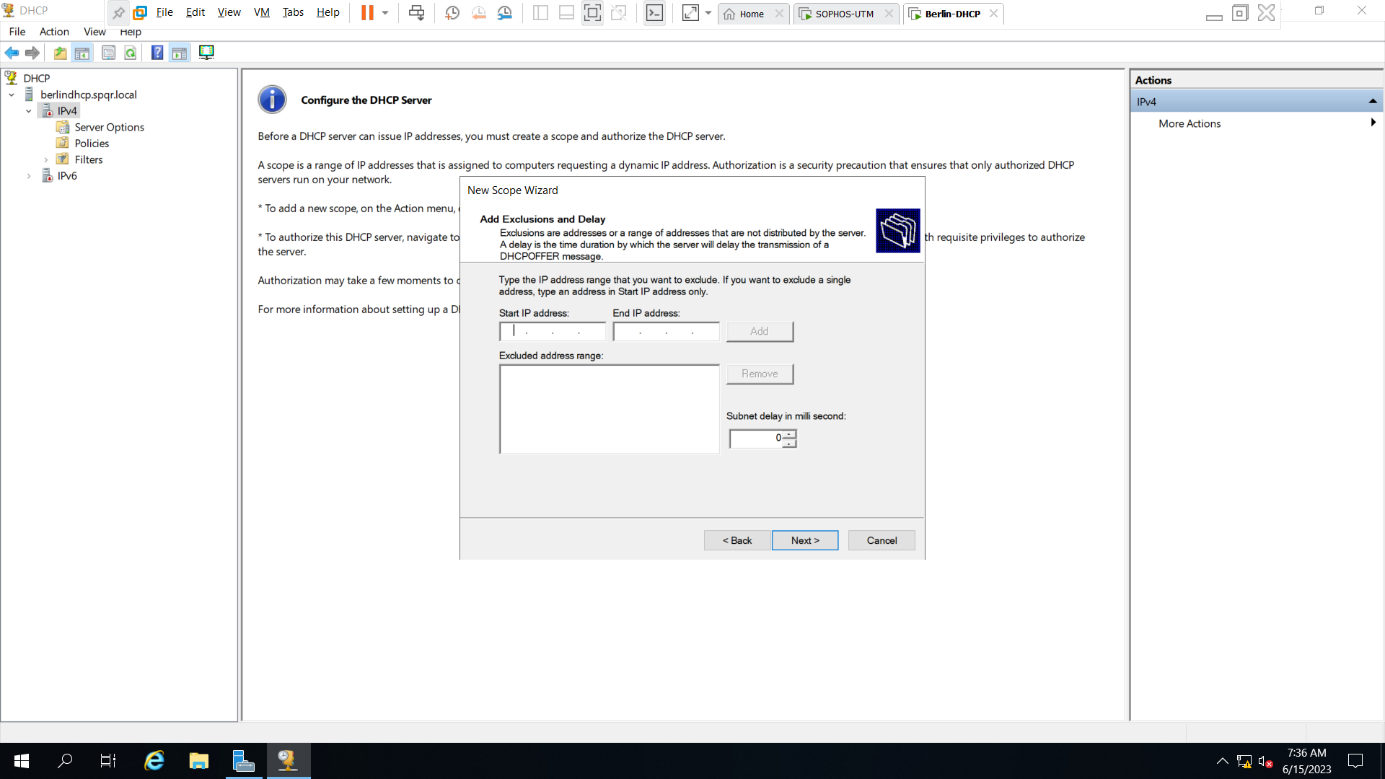
1. ‘PTR’ kayıtlarımızın düşmesi için Reverse Lookup Zone’dan ‘New Zone’ oluşturuyoruz.

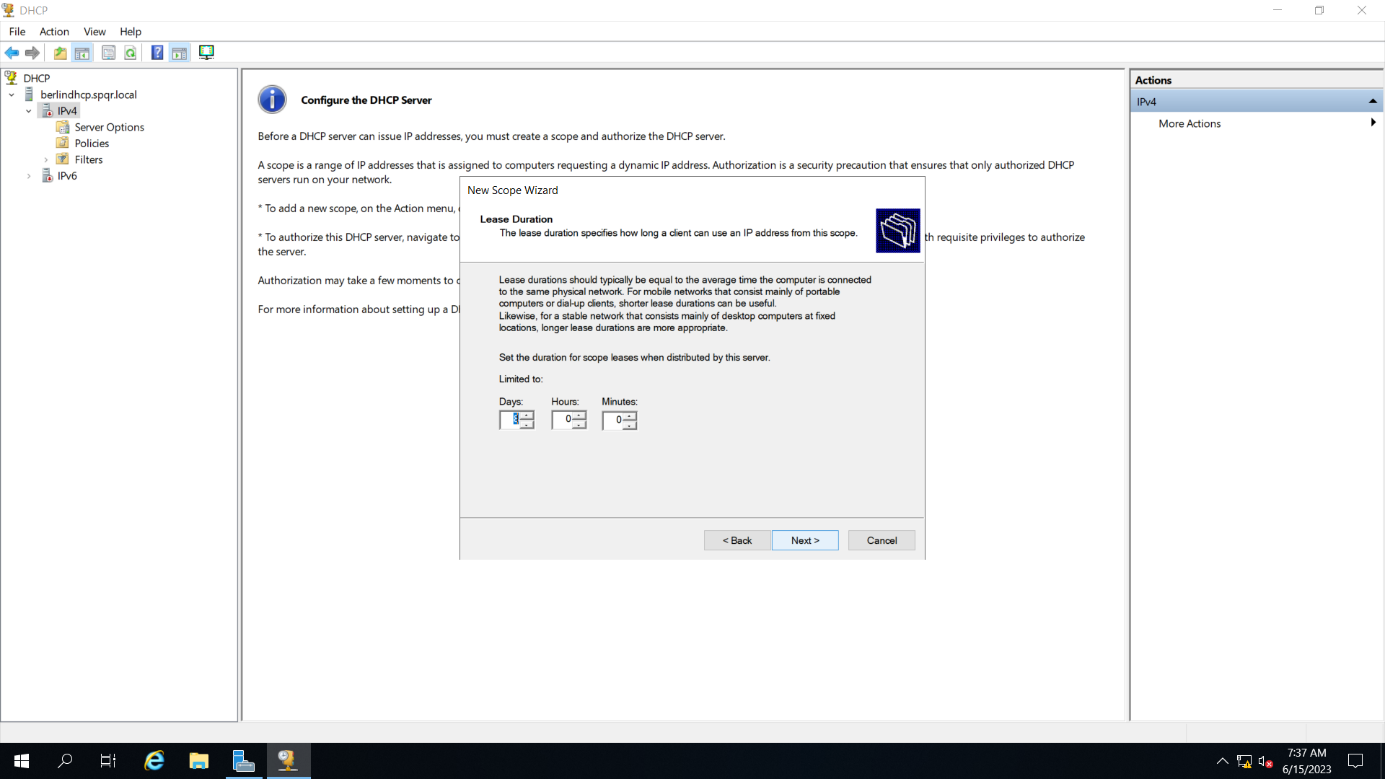
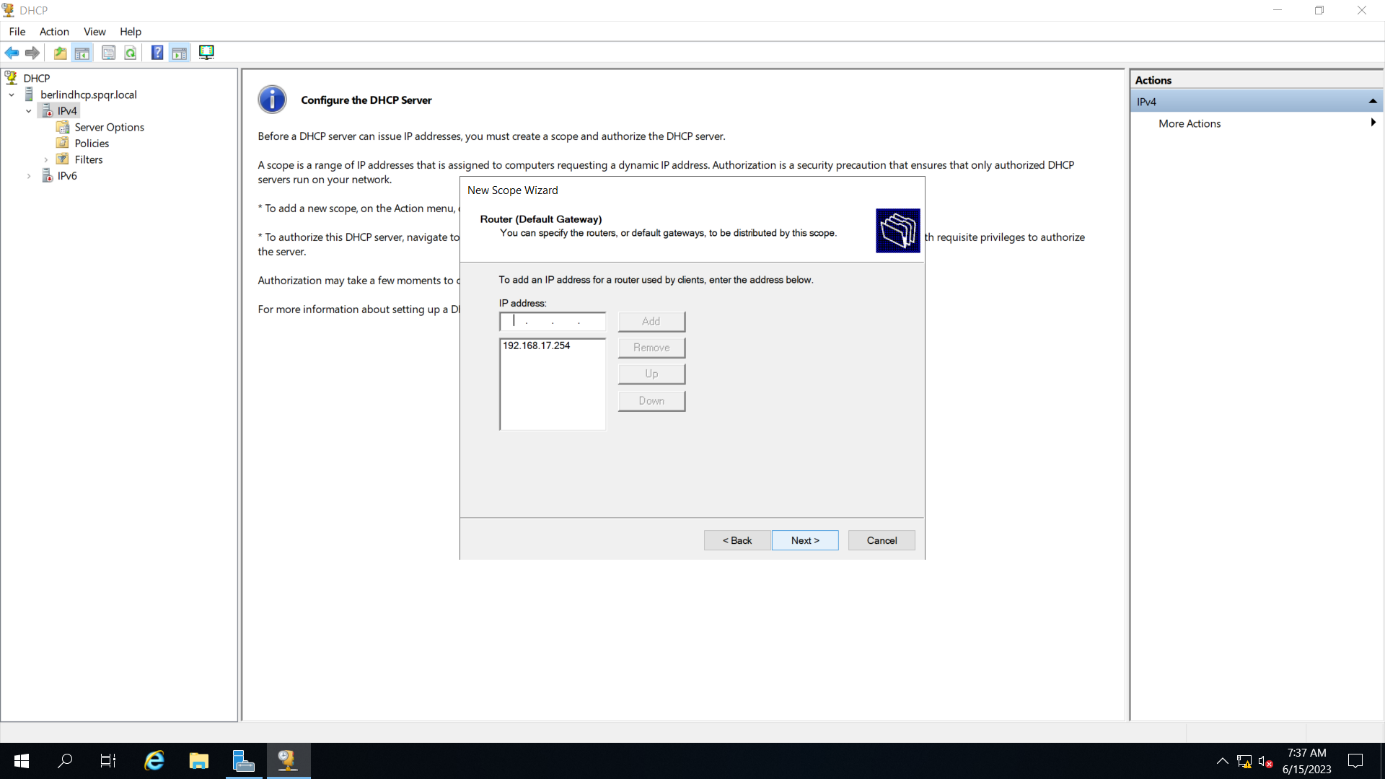
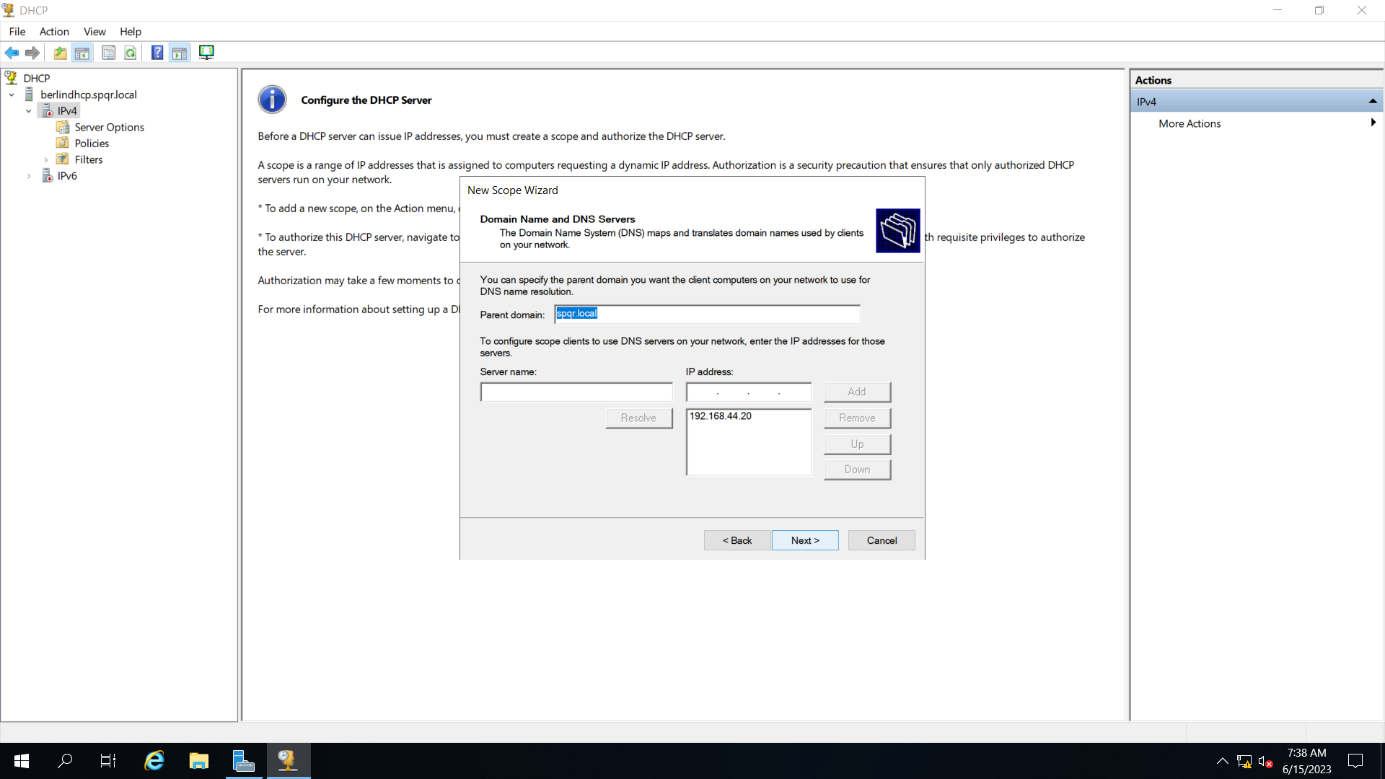
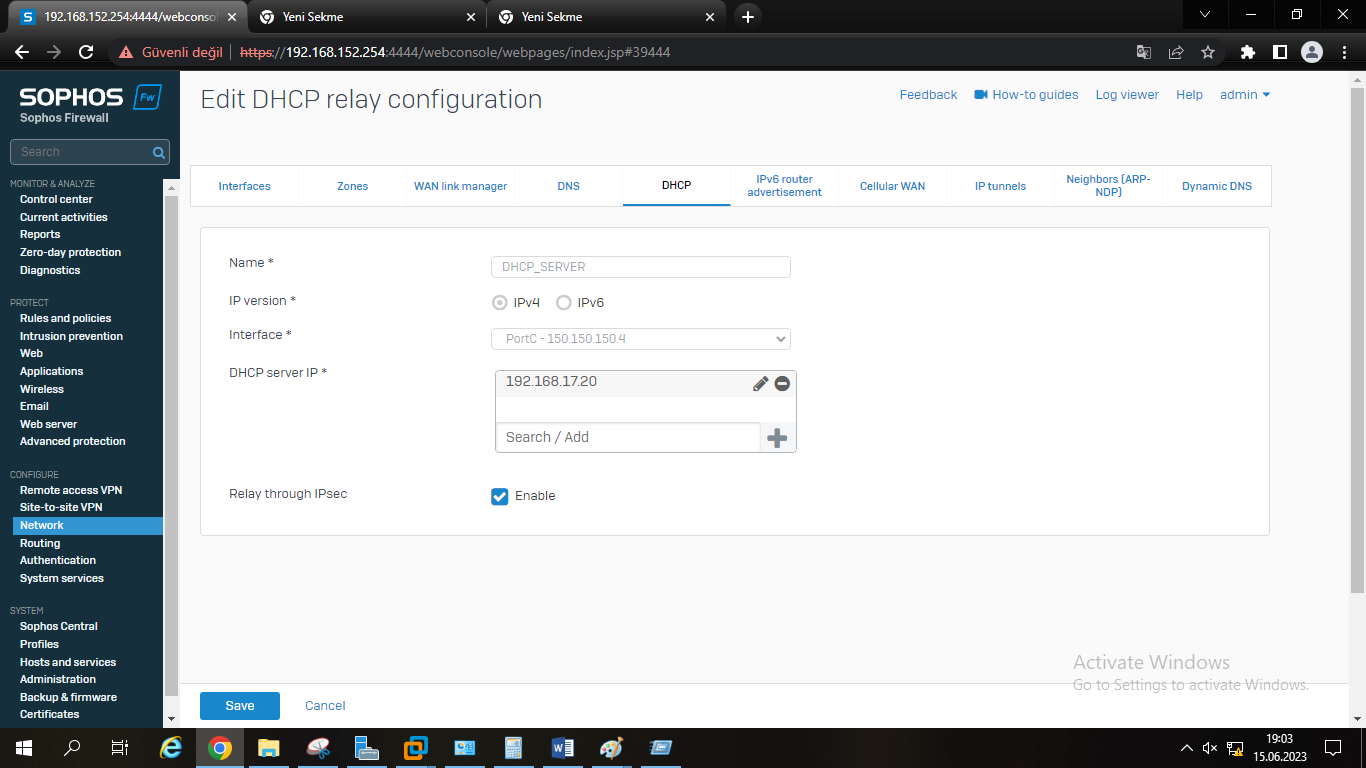


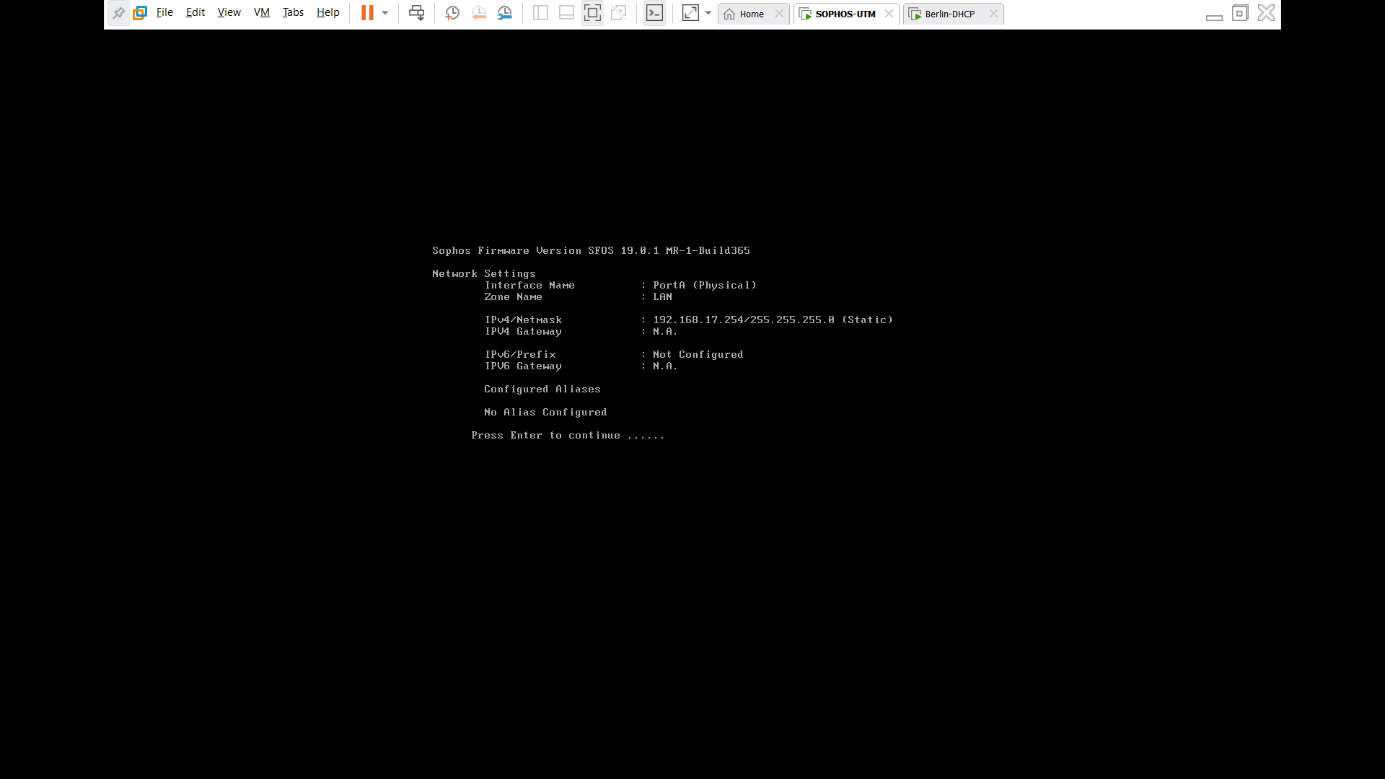
1. New Zone oluştururken oluşturacağımız Lan’ın Network adresini yazıyoruz.

* Berlin lokasyonunda konumlandırılan Server görevi: DHCP

1. **Konumlandırılan server kurulumu yapıldıktan sonra static olarak ip verildi. Hostname bilgisi verildi ve Roma üzerinde kurulan domaine “spqr.local” katıldı.**
2. **DHCP server üzerinde Server / add roles and feature bölümünde DHCP rolü yüklendi.**
3. **DHCP set edildikten sonra her lokasyon için scoplar oluşturuldu.**
   1. **Scop oluştururken öncellikle DHCP server’ın bulunduğu konum için ilk Scop oluşturulur daha sonra diğer lokasyonlar için Scoplar oluşturulur.**
   2. **Yapılan işlem: IPv4 üzerinde sağ tıklayarak new scope sekmesinden, ilk scop için isim belirlendi.**
   3. **LAN başlangıç ve bitiş IP’leri belirlendi.**
   4. **Daha sonra belirlenen aralıkta kullanılması istenmeyen ipler belirnedi.**

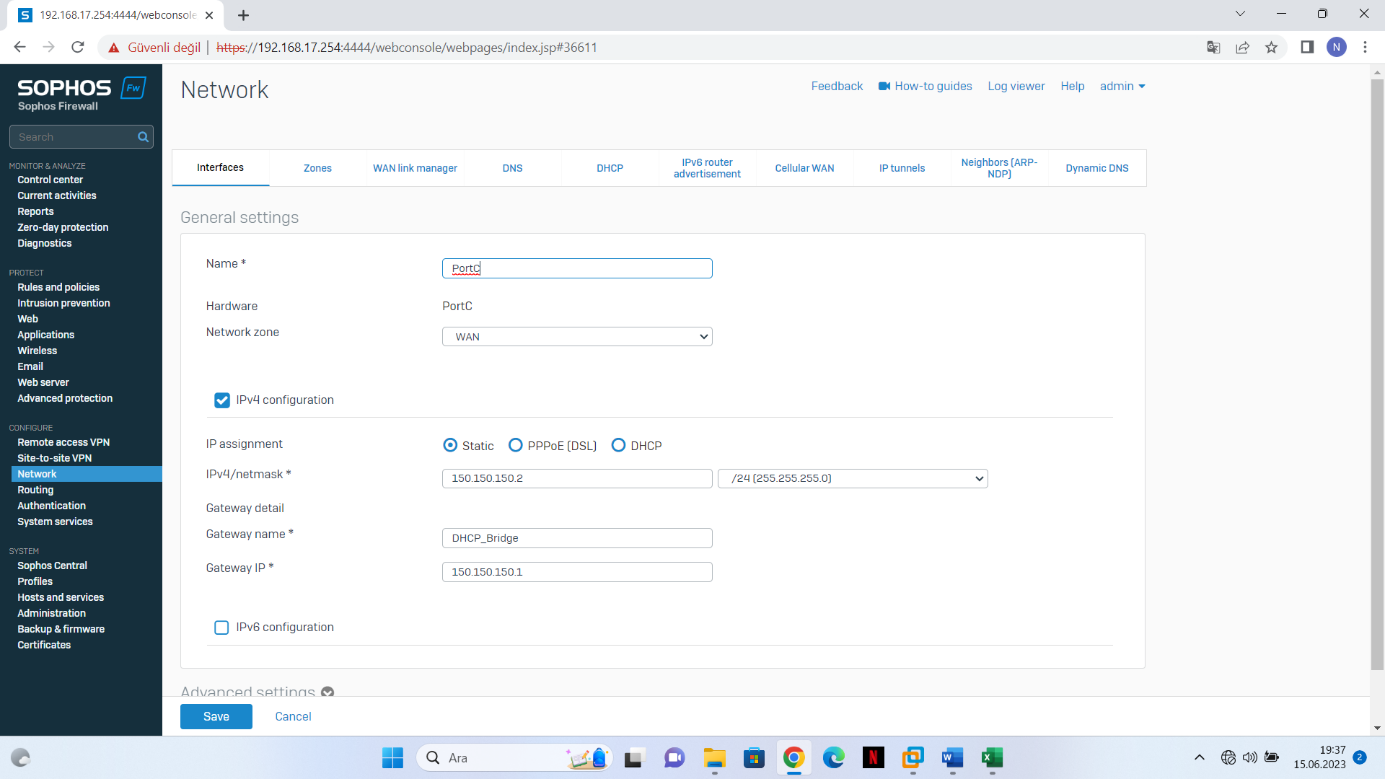


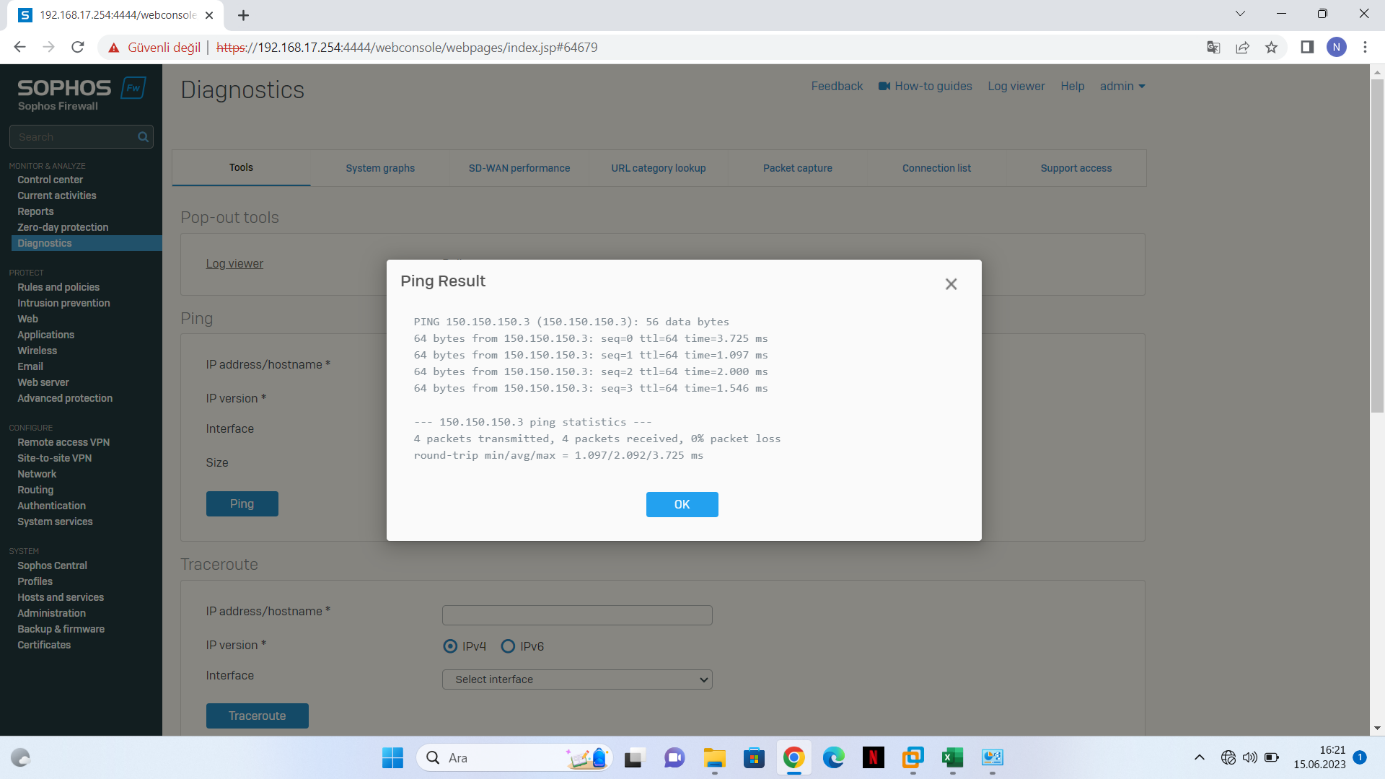
* 1. **Kiralanan iplerin kiralanma süresi belirtildi.**
  2. **Gateway verildi.**
  3. **DNS Belirtildi ve kaydedildi.**
  4. **Diğer lokasyonlar içinde oluşturulduktan sonra farklı LAN da bulunan Client’lar için Lokasyonların UTM’lerinde Relay tanımlanması yapıldı.**
* Merkez ve her bir şubeye Sophos UTM konumlandırıldı ve kurulumları yapıldı.

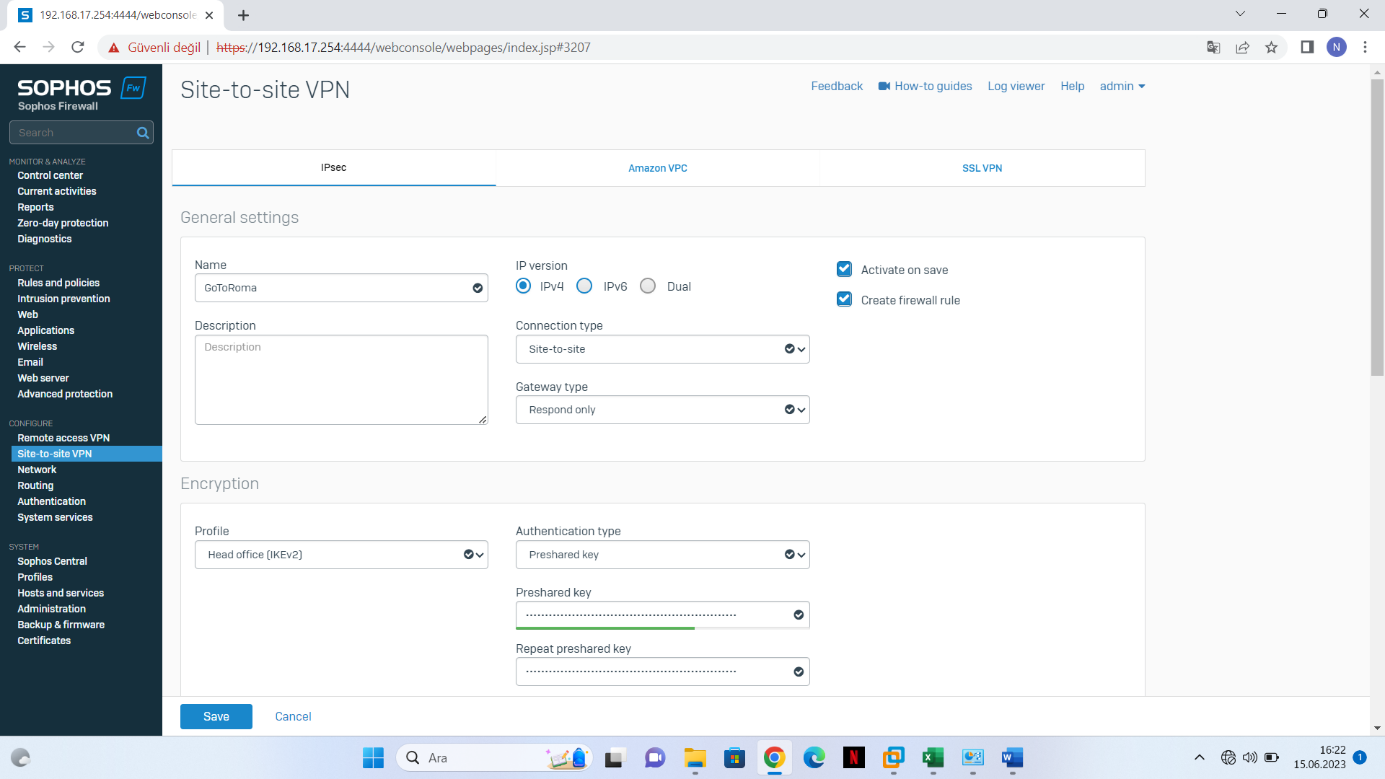
1. SopHos Ip adres tanımlandı.
2. Arayüzden açılarak update yapıldı.

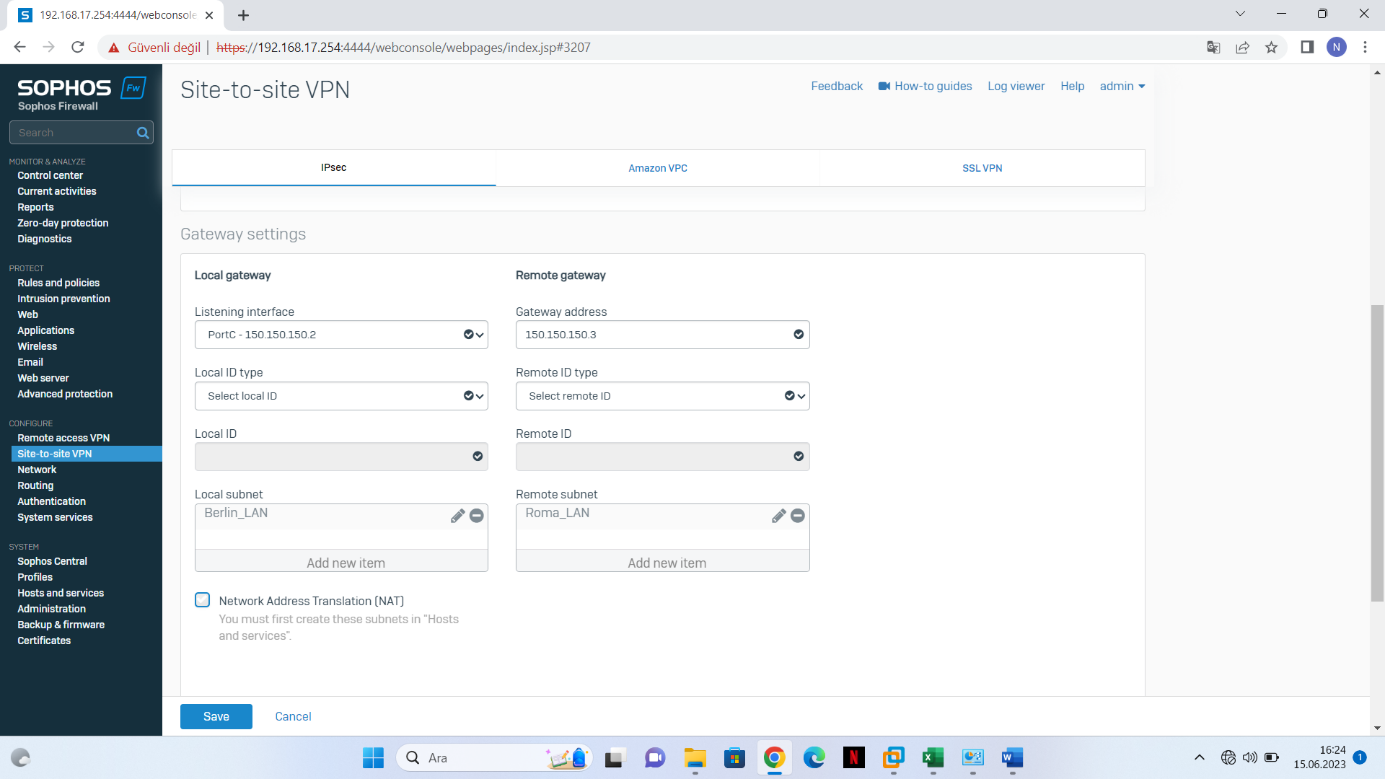
metin, ekran görüntüsü, yazılım, bilgisayar simgesi içeren bir resim

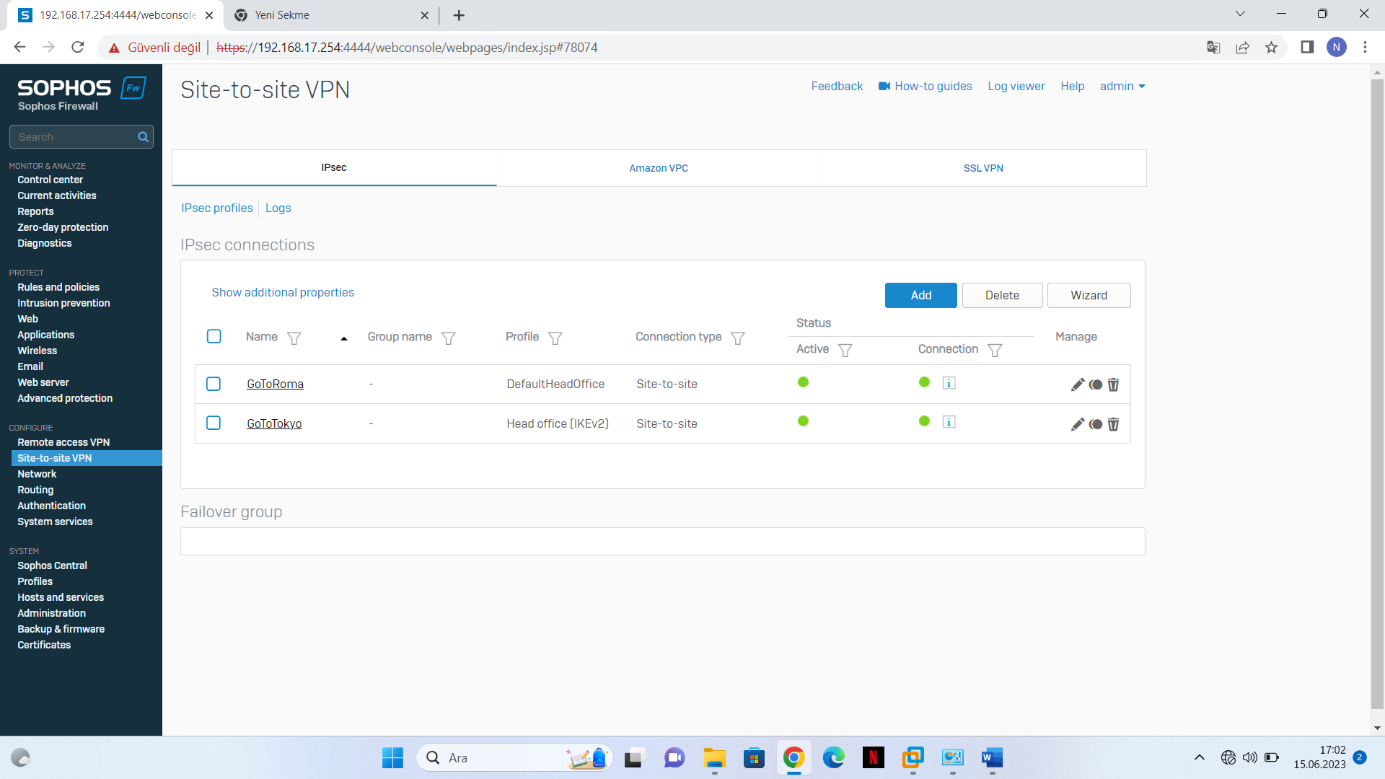
Açıklama otomatik olarak oluşturuldu

1. Arayüzden portC static ip verildi ve kontrol sağlandı.



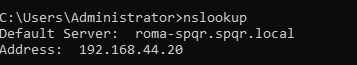
1.  Her şube arasında IpSec VPN tanımlarını yapın ve kontrol edin.



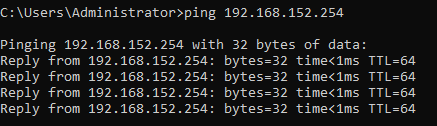


**PROJE TEST**

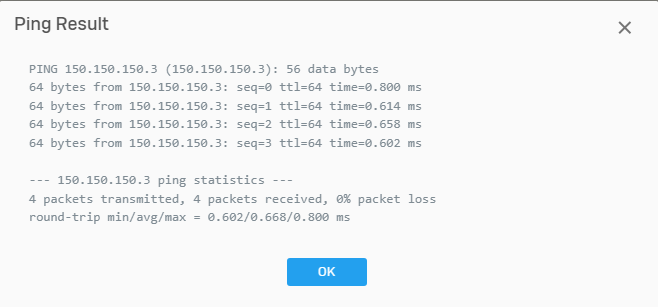
1-Windows 2019 Server’i Domain’e almamız için nslookup sorgusu yapıyoruz.



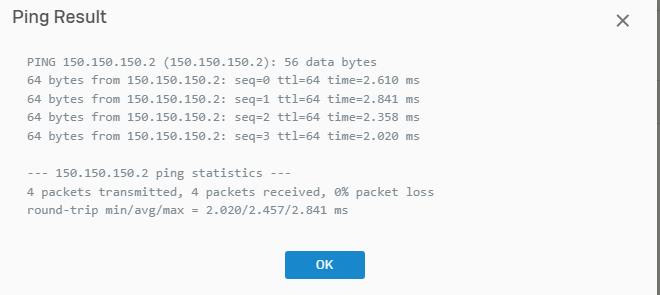
2- W19 Serverdan UTM’e ping atıyoruz.



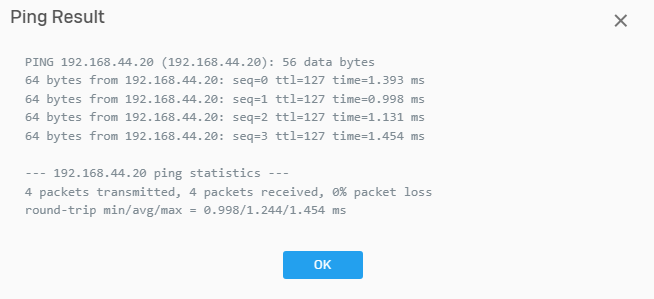
3-UTM’den DC’nin bulunduğu UTM’in bağlantı kontrolünü yapıyoruz. Böylelikle UTM’ler arası bağlantı var mı yok mu? Kontrolünü yapıyoruz.



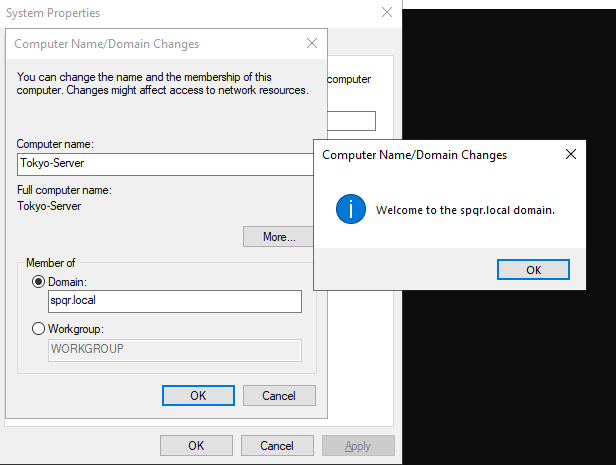
4- UTM’den DHCP’nin bulunduğu UTM’in bağlantı kontrolünü yapıyoruz. Böylelikle UTM’ler arası bağlantı var mı yok mu? Kontrolünü yapıyoruz.



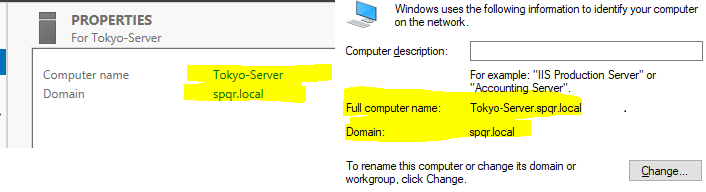
4- VPN kontrolü yapıyoruz, karşı LAN’a ping atıyoruz. Böylelikle VPN’in üzgün çalışıp çalışmadığını anlıyoruz.



5-Gerekli kurulum, konfigürasyonlar ve VPN bağlantısı testleri yapıldıktan sonra Windows 2019 server’imiz domaine katılıp katılmadığını kontrol ediyoruz.



6- Sysdm.cpl ve Server Manager’den domain’e giriş yaptığımızı kontrol ediyoruz.



7-DNS launch nslookup sorgusu yapıyoruz. DNS’in doğru oluşup oluşmadığını kontrol ediyoruz.

\\192.168.41.150\paylaş\121213.PNG