

**T.C.  
MİLLÎ EĞİTİM BAKANLIĞI**

# **BİLİŞİM TEKNOLOJİLERİ**

## **ACTIVE DIRECTORY YÖNETİMİ**

**Ankara, 2015**

- Bu modül, mesleki ve teknik eğitim okul/kurumlarında uygulanan Çerçeve Öğretim Programlarında yer alan yeterlikleri kazandırmaya yönelik olarak öğrencilere rehberlik etmek amacıyla hazırlanmış bireysel öğrenme materyalidir.
- Millî Eğitim Bakanlığınca ücretsiz olarak verilmiştir.
- PARA İLE SATILMAZ.

# İÇİNDEKİLER

AÇIKLAMALAR .....	iii
GİRİŞ .....	1
ÖĞRENME FAALİYETİ-1 .....	3
1. ACTIVE DIRECTORY YAPISI.....	3
1.1. Etki Alanı Oluşturma .....	3
1.1.1. Etki Alanı Oluşturma (GUI) .....	3
1.1.2. Etki Alanı Oluşturma (Powershell 3.0).....	15
1.2. Active Directory DNS İlişkisi .....	15
1.3. Etki Alanı (Active Directory) .....	15
1.4. Etki Alanı İşlev Düzeyleri.....	16
1.4.1. Orman İşlev Düzeyleri.....	18
1.4.2. Etki Alanı İşlev Düzeyini Yükseltme .....	18
1.3. Site Yapısı ve Alt Ağlar .....	23
1.3.1. Sitelere Genel Bakış .....	23
1.3.2. Siteleri Kullanma .....	23
1.3.3. Siteleri Ve Alt Ağları İlişkilendirme .....	24
1.3.4. Sitelere Bilgisayar Atama .....	24
1.3.5. Etki Alanı Denetleyicilerini Siteye Göre Bulma .....	25
1.3.6. Site Bağlantılarıyla Siteleri Bağlama.....	25
1.4. Site Oluşturma .....	25
1.4.1. Alt Ağ Oluşturma .....	26
1.4.1. Site Bağlantısı Oluşturma .....	26
1.4.2. Site Bağlantısına Site Ekleme veya Site Kaldırma .....	27
1.5. Dizin Yapısı .....	28
1.5.1. Genel Katalog (Global Catalog) .....	28
1.5.2. LDAP (Lightweight Directory Access Protocol - Hafifletilmiş Dizin Erişim Protokolü) .....	28
UYGULAMA FAALİYETİ .....	31
ÖLÇME VE DEĞERLENDİRME .....	32
ÖĞRENME FAALİYETİ-2 .....	34
2. HESAP YÖNETİMİ.....	34
2.1. Hesap Çeşitleri .....	34
2.1.1. Active Directory’de Kullanıcı Hesabı Oluşturma .....	34
2.1.2. Active Directory’de Grup Hesabı Oluşturma .....	38
2.2. Active Directory ve Organizational Unit .....	40
2.2.1. Active Directory’de Organizational Unit Oluşturma.....	40
2.3. Parola İlkesi .....	43
2.3.1. Parola İlkesi Oluşturma .....	43
UYGULAMA FAALİYETİ .....	46
ÖLÇME VE DEĞERLENDİRME .....	47
ÖĞRENME FAALİYETİ-3.....	48
3. GELİŞMİŞ HESAP YÖNETİMİ .....	48
3.1. Kullanıcı Hesabı.....	48
3.1.1. General Tabı .....	48
3.1.2. Address Tabı.....	49
3.1.3. Account Tabı .....	49

---

3.1.4. Profile Tabı .....	51
3.1.5. Telephones Tabı .....	53
3.1.6. Organization Tabı .....	53
3.1.7. Remote Control Tabı .....	54
3.1.8. Remote Desktop Services Profile Tabı.....	54
3.1.9. COM+ Tabı.....	55
3.1.10. Member Of Tabı .....	55
3.1.11. Dial-in Tabı.....	56
3.1.12. Environment Tabı .....	56
3.1.13. Sessions Tabı.....	57
UYGULAMA FAALİYETİ .....	58
ÖLÇME VE DEĞERLENDİRME .....	59
MODÜL DEĞERLENDİRME .....	60
KAYNAKLAR.....	64

# AÇIKLAMALAR

<b>ALAN</b>	<b>Bilişim Teknolojileri</b>
<b>DAL/MESLEK</b>	<b>Bilgisayar Teknik Servis</b>
<b>MODÜLÜN ADI</b>	<b>Active Directory Yönetimi</b>
<b>MODÜLÜN TANIMI</b>	Etki alanı kurulumu nasıl yapılacağı, kullanıcı, grupları oluşturma, ileri seviye kullanıcı işlemleri hakkında becerilerin kazandırıldığı öğrenme materyalidir.
<b>SÜRE</b>	40/24
<b>ÖN KOŞUL</b>	
<b>YETERLİK</b>	Sunucu işletim sisteminin izin hizmetini yönetmek
<b>MODÜLÜN AMACI</b>	<b>Genel Amaç</b> Bu modül ile gerekli ortam sağlandığında; Active Directory hizmetlerini, grupları ve kullanıcıları yönergelere uygun ve etkin bir şekilde kullanarak sunucu işletim sisteminin izin hizmetini yönetebileceksiniz. <b>Amaçlar</b> <b>1.</b> Active Directory’i kullanabileceksiniz. <b>2.</b> Kullanıcı ve grup hesaplarını oluşturabileceksiniz. <b>3.</b> Kullanıcı ve grup hesaplarını ileri seviye yönetebileceksiniz.
<b>EĞİTİM ÖĞRETİM ORTAMLARI VE DONANIMLARI</b>	<b>Ortam:</b> Sunucu işletim sistemi kurulu bilgisayar ve laboratuvar ortamı <b>Donanım:</b> Projeksiyon, bilgisayar, anahtarlayıcı, dağıtıcı, ağ kartı
<b>ÖLÇME VE DEĞERLENDİRME</b>	Modül içinde yer alan her öğrenme faaliyetinden sonra verilen ölçme araçları ile kendinizi değerlendireceksiniz. Öğretmen modül sonunda ölçme aracı (çoktan seçmeli test, doğru-yanlış testi, boşluk doldurma, eşleştirme vb.) kullanarak modül uygulamaları ile kazandığınız bilgi ve becerileri ölçerek sizi değerlendirecektir.



# GİRİŞ

**Sevgili Öğrenci,**

Sunucu işletim sistemleri, ağ üzerindeki kaynakları kullanıcılara uygun izinlerle paylaştıran, yönetimde verimliliği hedefleyen güçlü sistemlerdir. Bir firmada bilgisayar ve kullanıcılar arttıkça bunların yönetimi ve denetimi zorlaşmaktadır. Bu gibi durumlarda yönetimi mantıksal birimlere bölmek ve her birime bir yönetici atamak gerekebilir. Ayrıca her yöneticiyi, ayrı kaynakların yönetimi için farklı yetkilerle donatabiliriz. Bu sayede yönetimi kolaylaştırmış ve verimliliği artırmış oluruz.

Yönetimi mantıksal birimlere bölmek için kullanılan organizasyon birimleri, kendi içerisinde bulunan sistem kaynaklarını basite indirgenmiş bir Resimde yönetmeyi hedefler. Organizasyon birimine atayacağımız yöneticiler ise birime bağlı kullanıcı hesaplarını, bilgisayar ve diğer kaynakları yöneterek sistemin ana yöneticisine düşen ağır yönetim yükünü hafifletmiş olur.

Bu modülde Active Directory tanımını ve kullanıcı, grup ve organizasyon birimlerinin oluşturulması ve yetkilendirilmesi, kullanıcılar için ne gibi hesap ayarları yapabileceğimizi, sistem yönetiminde güvenlik ilkeleri, sistem güvenliği için yapılacak ayarlamalar ve alınacak tedbirler, kullanıcı izinlerinin ve kısıtlamalarının düzenlenmesi gibi birçok güvenlik politikalarını öğrenecek ve uygulamalı olarak bu işlemleri gerçekleştireceksiniz.





# ÖĞRENME FAALİYETİ-1

## AMAÇ

Active Directory’i kurabilecek ve kullanabileceksiniz.

## ARAŞTIRMA

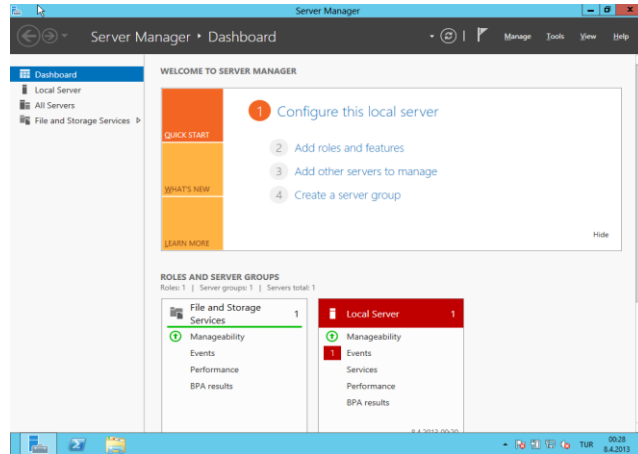
- Büyük şirketlerin Active Directory’i neden tercih ettiklerini, kurulumunun nasıl yapıldığını araştırınız. Topladığınız bilgileri rapor hâline getiriniz. Hazırladığınız raporu sınıfta öğretmeninize ve arkadaşlarınıza sununuz.

## 1. ACTIVE DIRECTORY YAPISI

### 1.1. Etki Alanı Oluşturma

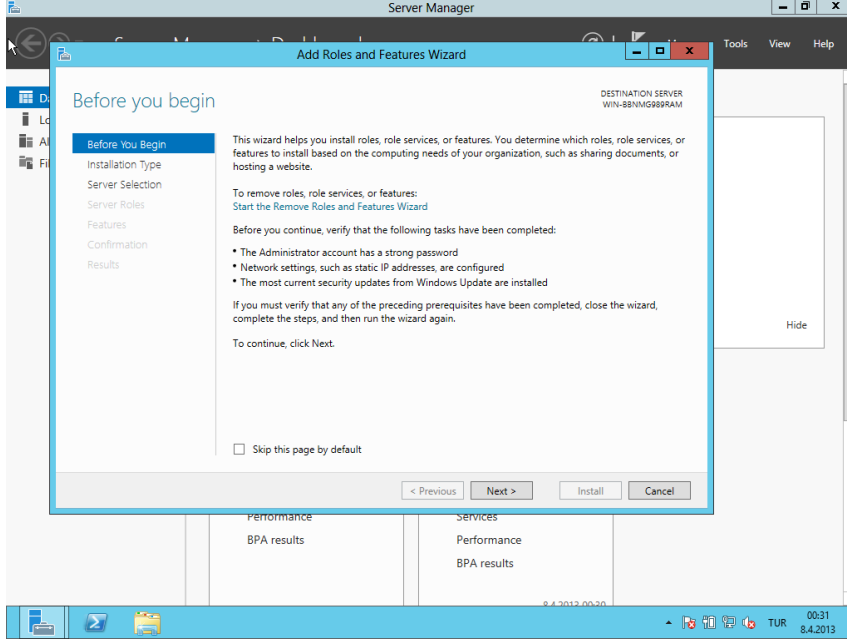
#### 1.1.1. Etki Alanı Oluşturma (GUI)

Süregelen Dcpromo komutu ile Active Directory (AD) kurulumu Windows Server 2012 ile son buldu. AD kurulumu artık Sunucu Yönetimi (Server Manager) penceresinden veya Powershell üzerinden ADDSDeployment komutları ile yapılabilir. Her AD kurulumunda olduğu gibi bilgisayara öncelikle bir sabit (static) IP verilmesi gerekmektedir. Ardından Sunucu Yönetimi (Server Manager) penceresinden Add roles and features seçeneği seçilir. Aynı işlem, pencerenin sağ üst tarafında yer alan Manage linki altında görülecek aynı isimli link ile de yapılabilir.



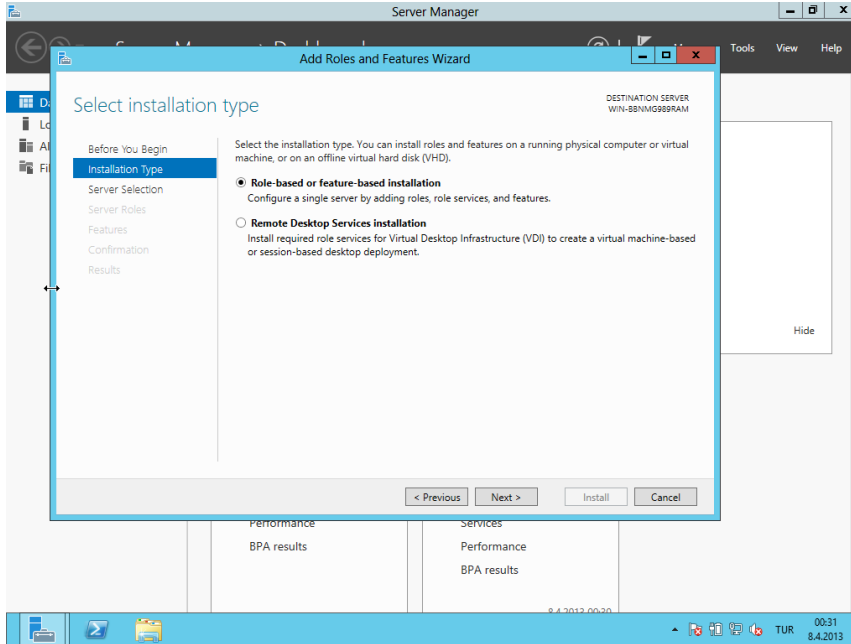
Resim 1.1: Metro kullanıcı arayüzü

Karşılaşılan aşağıdaki pencerede kurulum başlamadan önce bilinmesi gereken bilgiler yer almaktadır.



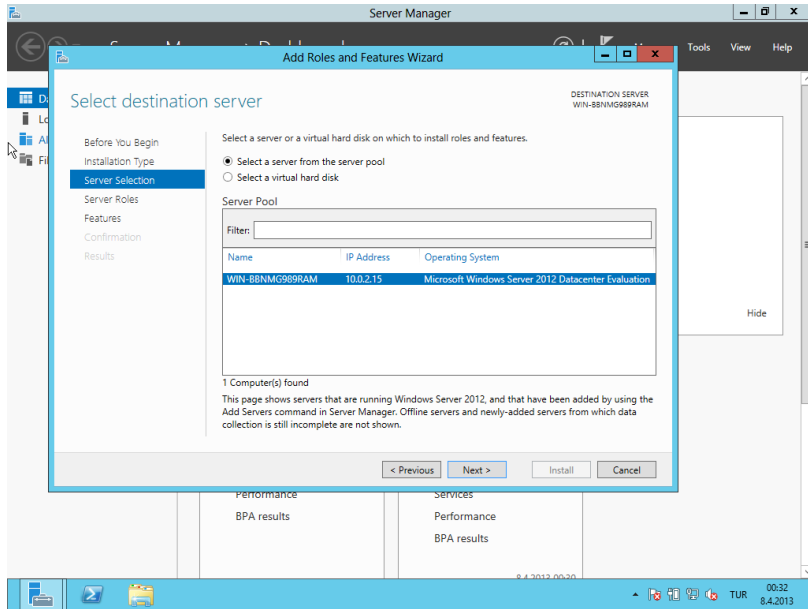
**Resim 1.2: Before you begin Penceresi**

Select Installation Type penceresinde Role-Based or Feature-Based Installation seçilir.



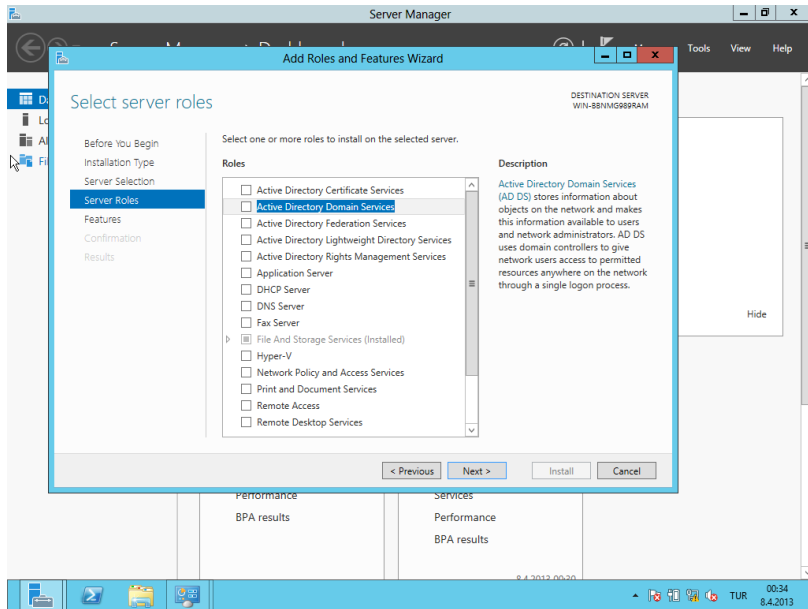
**Resim 1.3: Select Installation Type Penceresi**

Select destination server penceresinden kurulum yapılacak sunucu seçilir. Windows Server 2012 daha önceki sürümlerde olmayan özellikleri sayesinde bu pencere aracılığı ile aynı ağ'da yer alan başka bir sunucudaki sanal makine saklama dosyalarına (vhd) role ve özellik ekleme işlemini yapabilmektedir. (vhd'lere offline olarak da yapabilmektedir.) Bu pencereden sunucu seçilip kurulumu devam edilir.



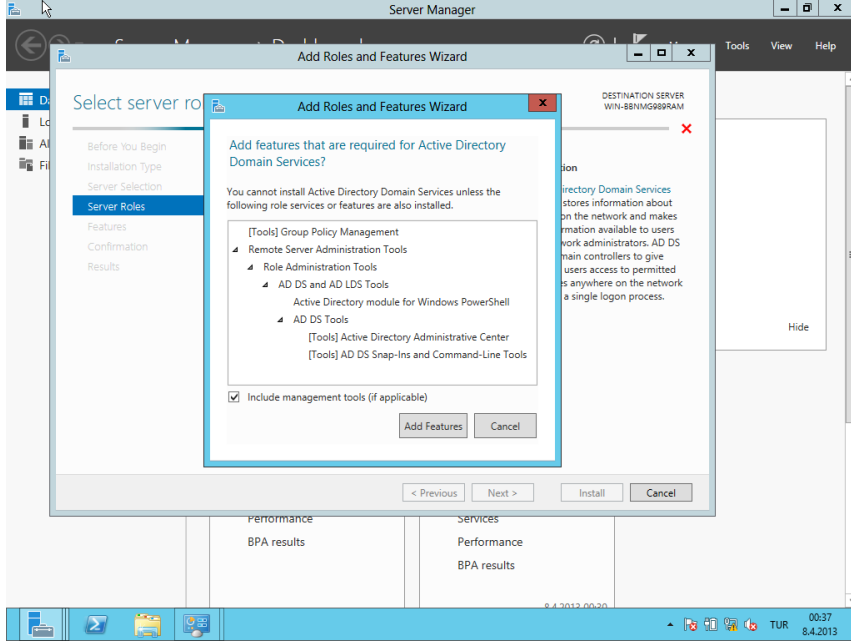
**Resim 1.4: Select Destination Server Penceresi**

Select server roles penceresinden “Active Directory Domain Services” seçilir.



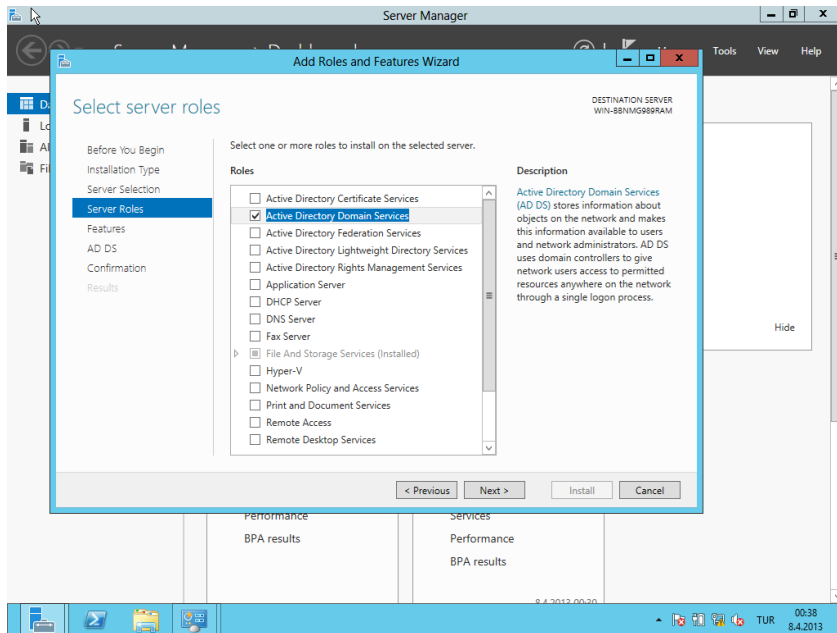
**Resim 1.5: Select Server Roles Penceresi**

Active Directory kurulumu için gerekli olan özelliklerin yer aldığı “Add Roles and Features Wizard” penceresindeki Add Features butonuna tıklanarak kurulumu devam edilir.



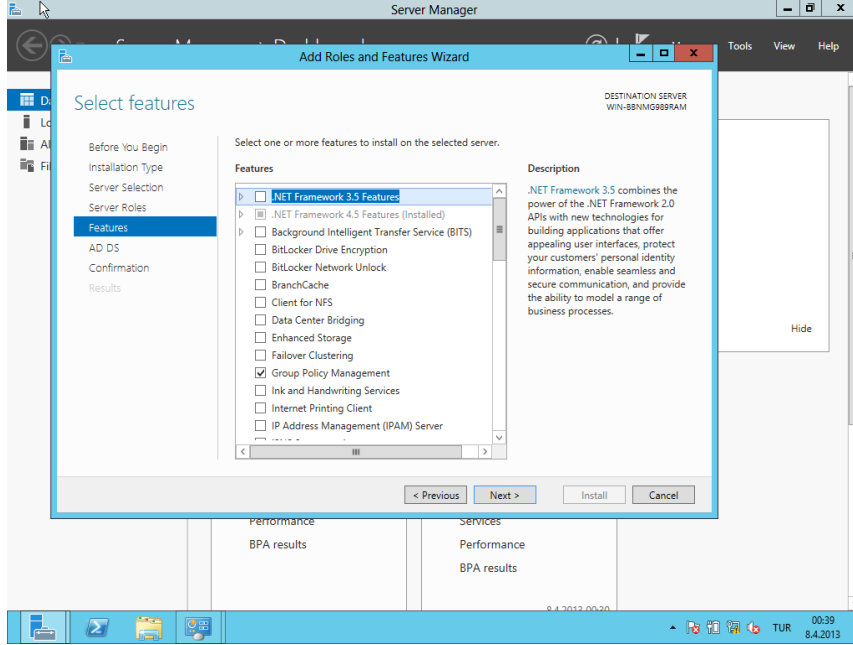
**Resim 1.6: Add Roles and Features Wizard Penceresi**

Özelliklerin kurulumu eklendiği Resim 1.6’den sonra Resim 1.7’de onaylama işlemi yapılır.



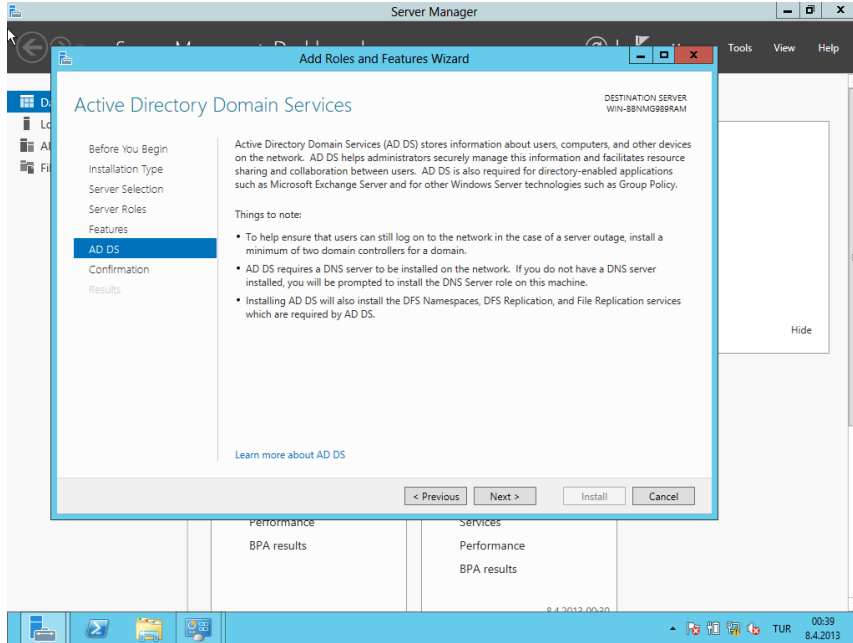
**Resim 1.7: Select Server Roles Penceresi**

Resim 1.8’de önceki pencerelerde yapılan özellik seçimleri görülmektedir. Next butonuna basılarak kurulumu devam edilir.



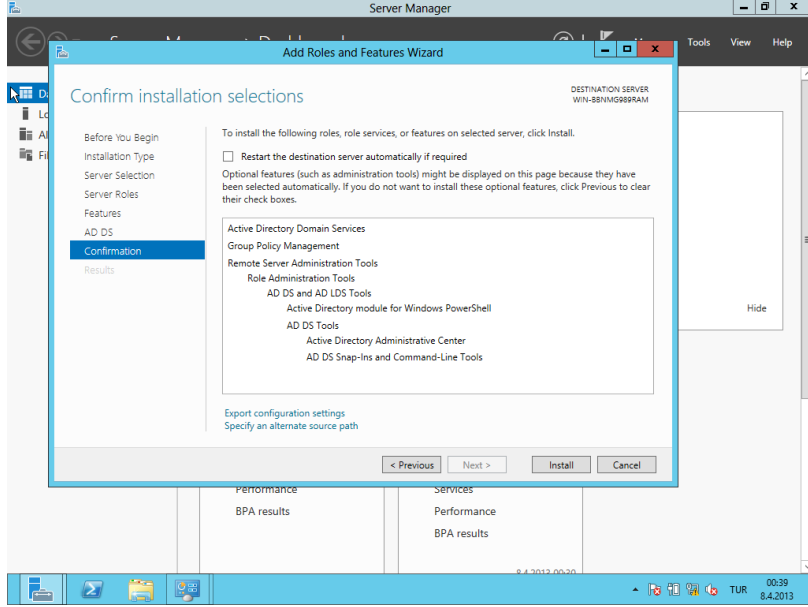
**Resim 1.8: Select Features Penceresi**

Resim 1.9’da Active Directory Domain Services ile ilgili bilgiler yer almaktadır.



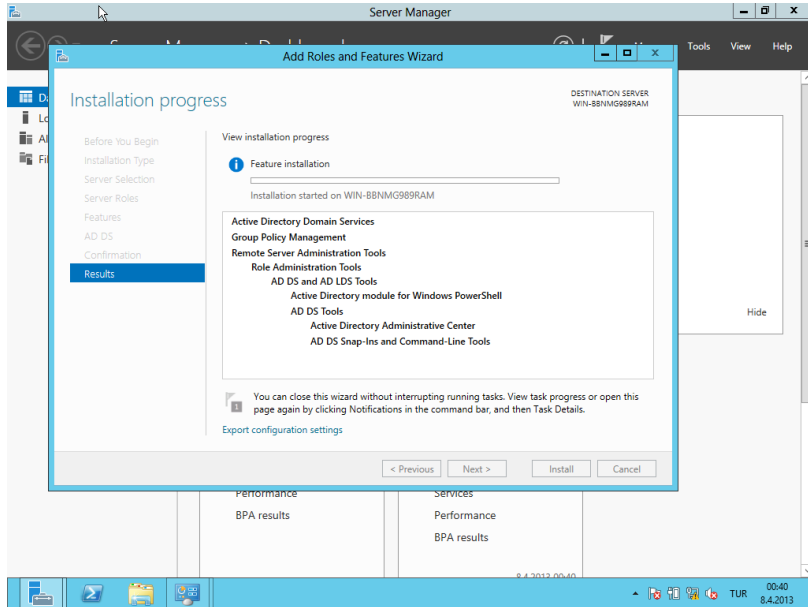
**Resim 1.9: AD DS Penceresi**

Resim 1.10'daki Install butonuna basilarak kurulum baslatilir. Eger kurulum bitiminde sistemin otomatik olarak restart etmesi isteniyor ise "Restart the destination Server automatically if required" checkbox'ı seçili duruma getirildikten sonra Install butonuna basilir.



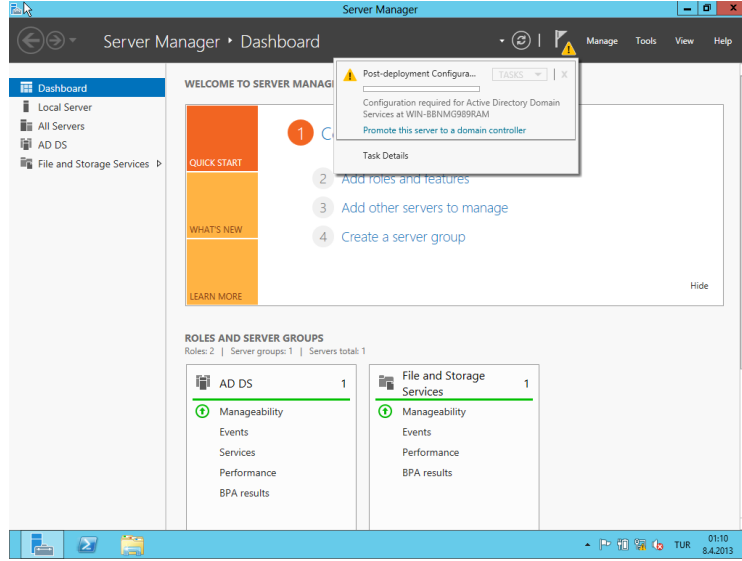
**Resim 1.10: Confirm Installation Selections Penceresi**

Resim 1.11'de Active Directory Domain Services kurulumunun başladığı görülmektedir.



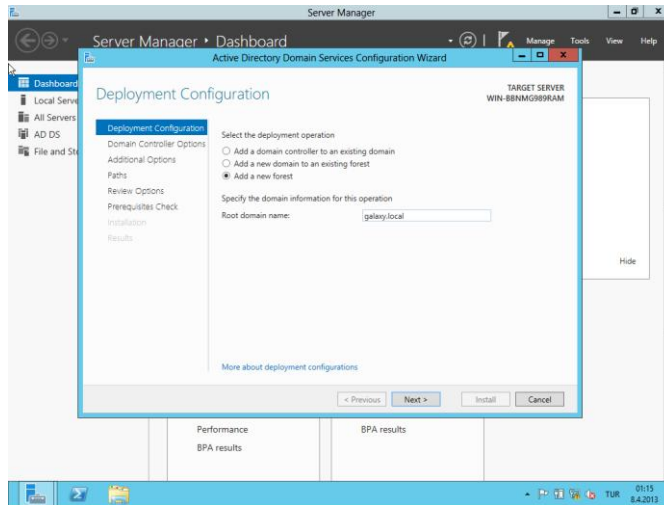
**Resim 1.11: Installation Progress Penceresi**

Sunucu açıldıktan hemen sonra Server Manager otomatik olarak tekrar açılacaktır. Resim 1.12’de görülen Notification ekranına tıkladıktan sonra “Configuration Required for Active Directory at Server adı” şeklinde bir uyarı görülecektir. Active Directory kurulumuna devam etmek için, “Promote this Server to a domain controller” linki tıklanmalıdır.



**Resim 1.12: Dashboard Penceresi**

Resim 1.13’te “Deployment Configuration penceresinde” nasıl bir etki alanı kurulacağı seçilir. “Add a domain controller to an existing domain” seçeneği ile var olan bir etki alanına etki, alanı yöneticisi ekleme işlemi, “Add a new domain to an existing forest” seçeneği ile var olan bir ormana yeni bir etki alanı ve son olarak da “Add a new forest” seçeneği ile yeni bir orman yapısı oluşturma işlemi yapılır. İlk defa kurulum yaptığımız için “Add a new forest” seçeneği aktifleştirilerek kurulumla devam edilir.

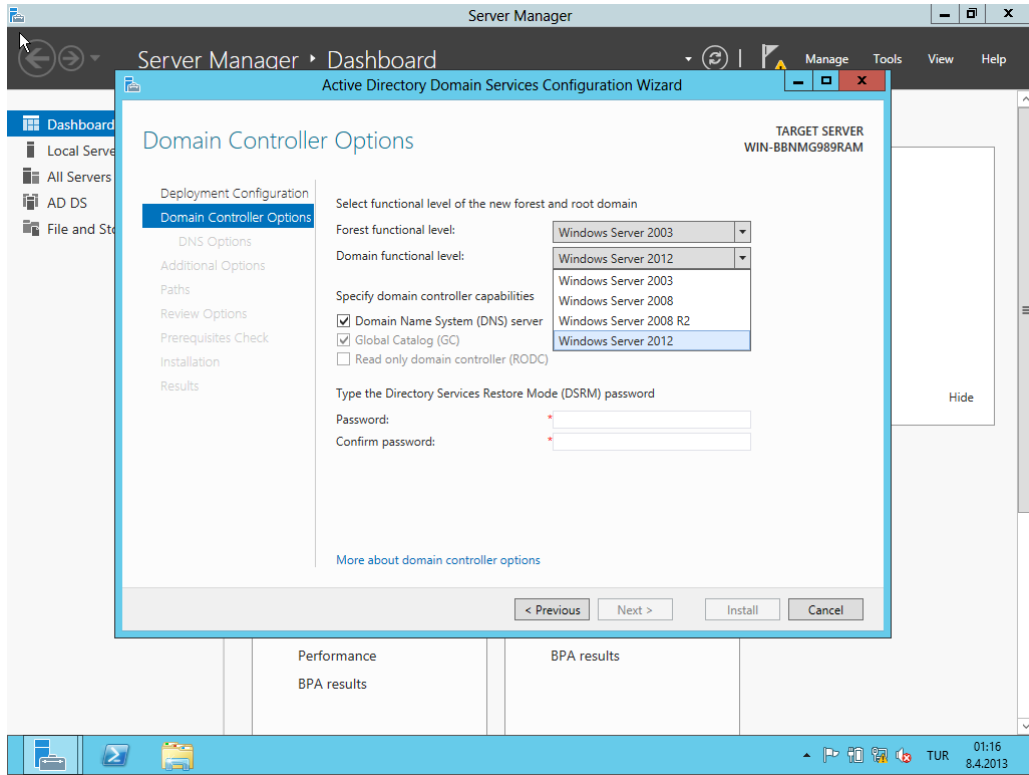


**Resim 1.13: Deployment Configuration Penceresi**

Resim 1.14'te yer alan Functional Level seçeneklerinden kurulacak orman yapısına, daha eski sunucu sistemlerinin eklenmesi durumu düşünülerek seçim yapılır. Burada eski sunucu işletim sistemi eklenecek ise eklenecek olan sunucu işletim sistemine uygun olan Functional level seçilerek diğer kurulum seçeneklerine geçilir.

“Specify domain controller capabilities” alanındaki “Domain Name System (DNS) server” seçeneği, ilk defa orman ve sunucu kurulumu yapılacağı için seçili olmalıdır.

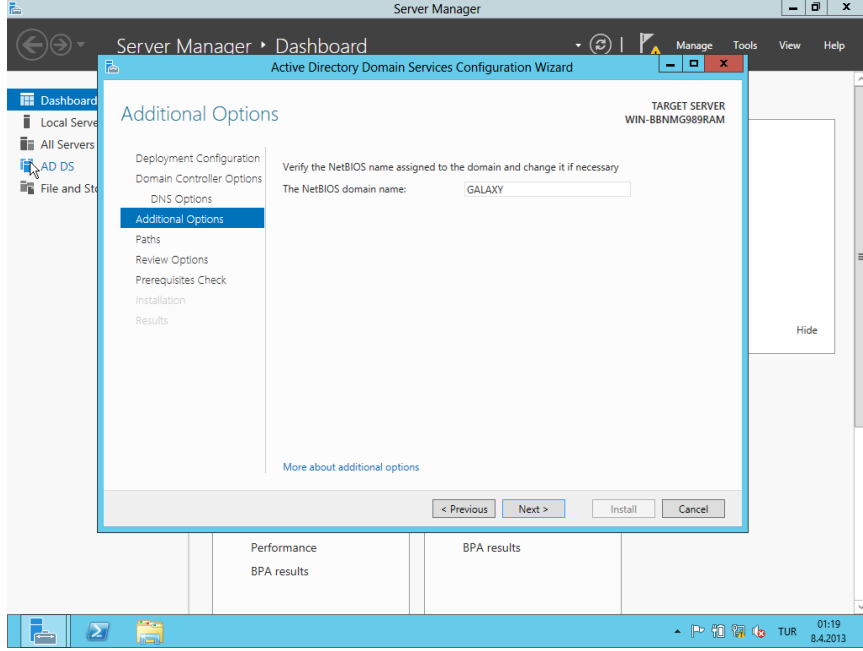
Resim 1.14'te görüldüğü üzere Global Catalog (GC) seçili gelmekte, değişim yapılamamaktadır, bu durumun sebebi ormanda ilk defa bir sunucu kuruluyor olmasıdır. “Type the Directory services Restore Mode (DSRM) password” kısmına bir şifre girilerek kurulumla devam edilir.



**Resim 1.14: Domain Controller Options Penceresi**

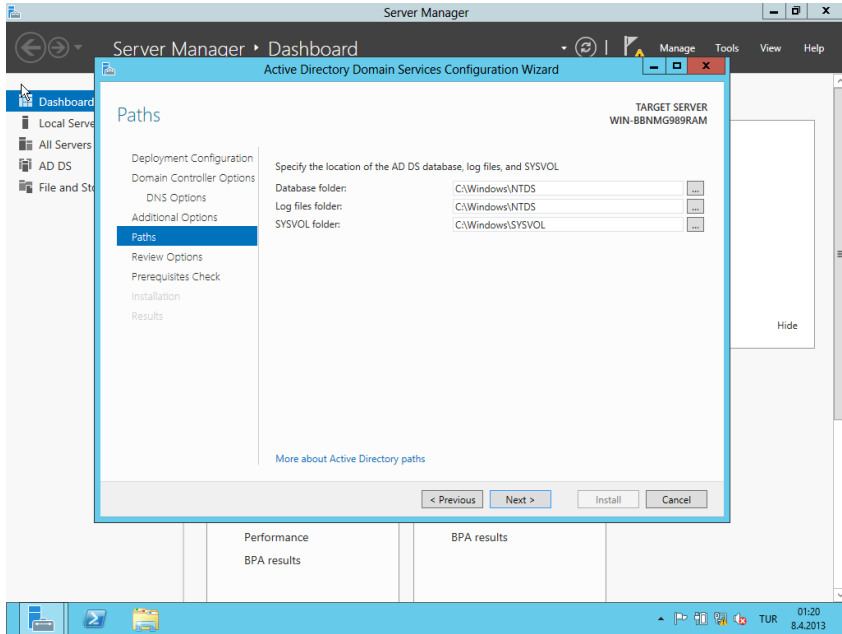


Resim 1.15'te etki alanı için kullanılacak Netbios ismi verilir.



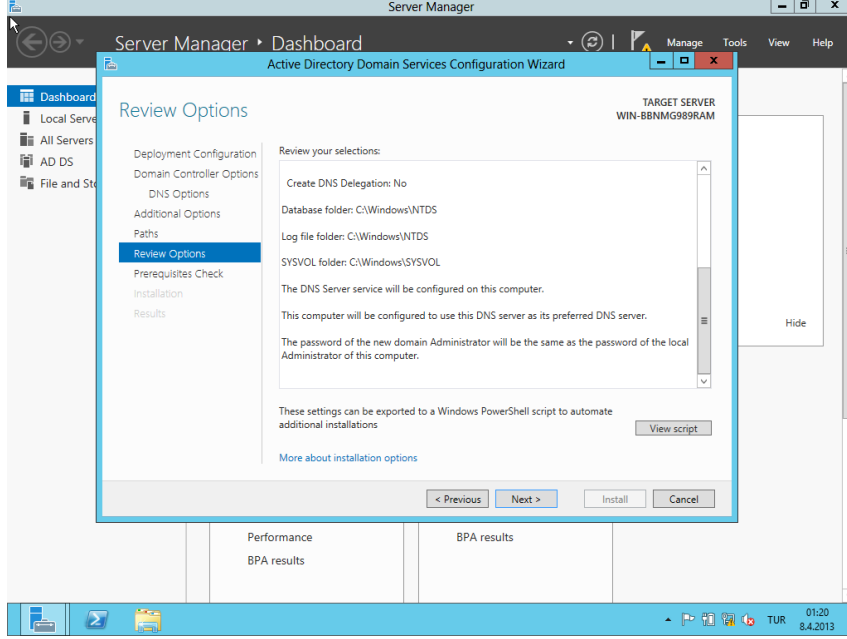
**Resim 1.15: Additional Options Penceresi**

Resim 1.16'da veritabanı, geçmiş klasörü ve Sysvol klasörünün barındırılacağı yerler seçilir. Bu klasör içerikleri, önemli olması sebebi ile geçerli gelen klasör yolu genelde bozulmaz.



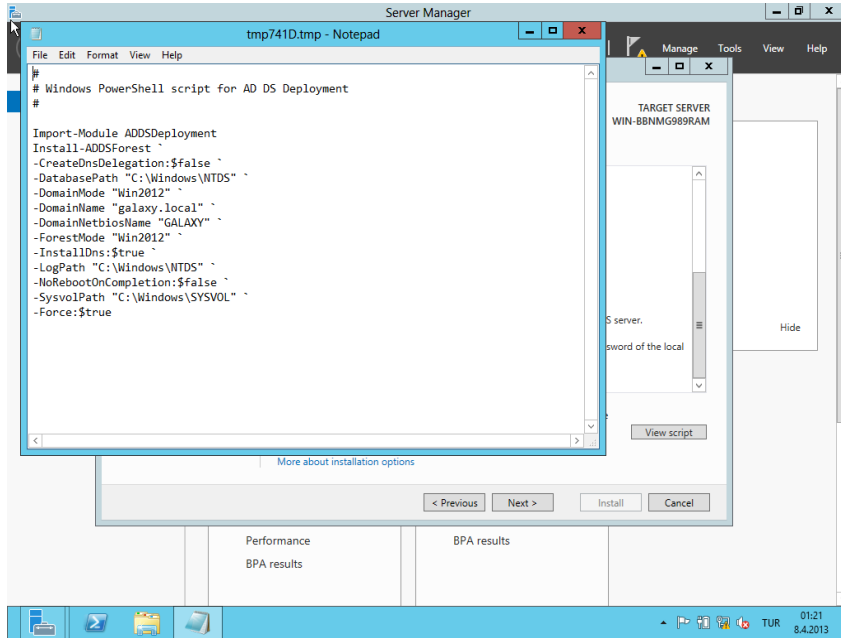
**Resim 1.16: Paths Penceresi**

Resim 1.17’de kurulumun başından beri yaptığımız ayarların özeti görüntülenmektedir.



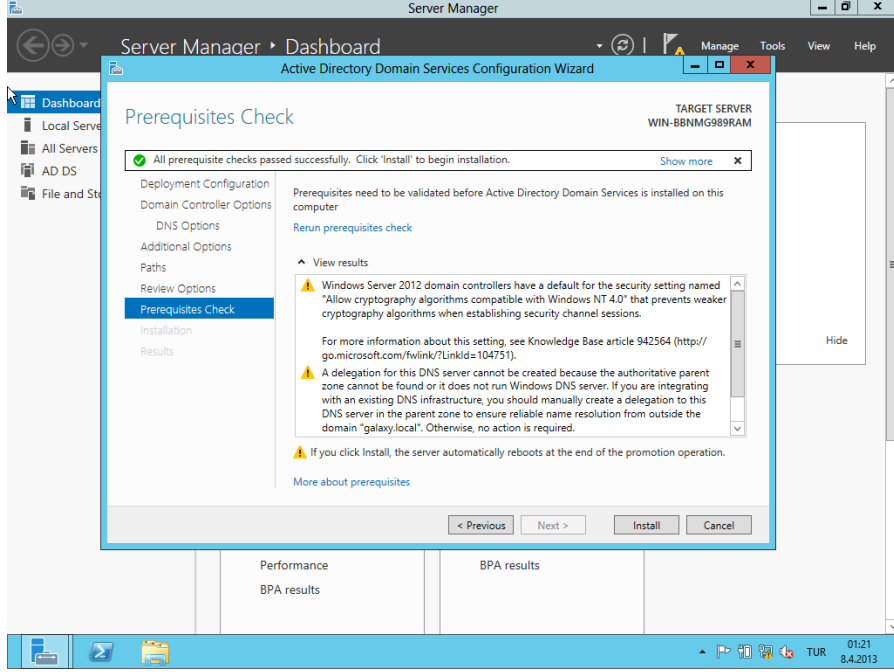
**Resim 1.17: Review Options Penceresi**

Resim 1.18’de Şekli 1.17’de görsel olarak görülen tüm ayarlar Powershell ortamında görülmektedir.



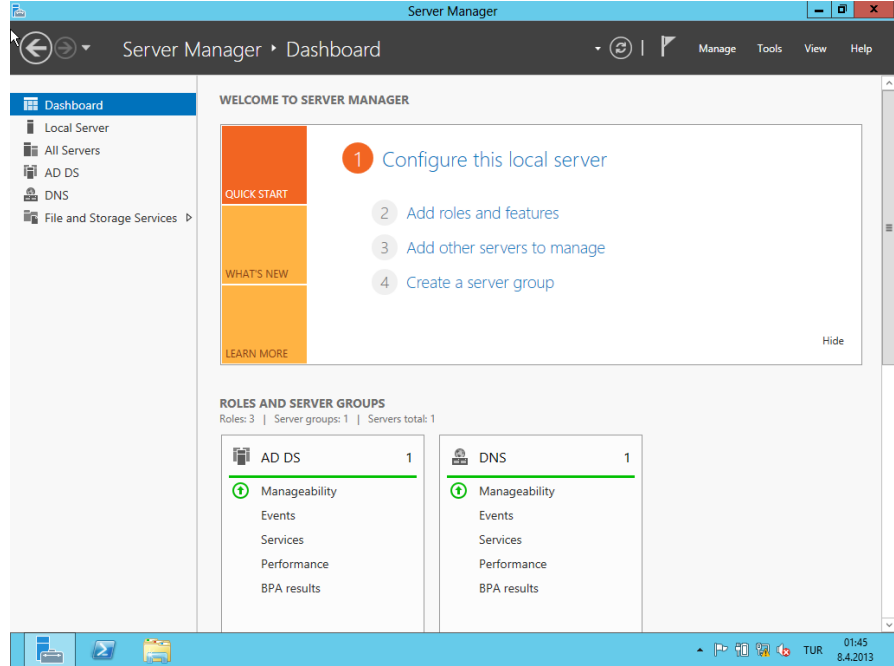
**Resim 1.18: Powershell Penceresi**

Resim 1.19’da Install butonuna basilarak kurulum baslatilir.

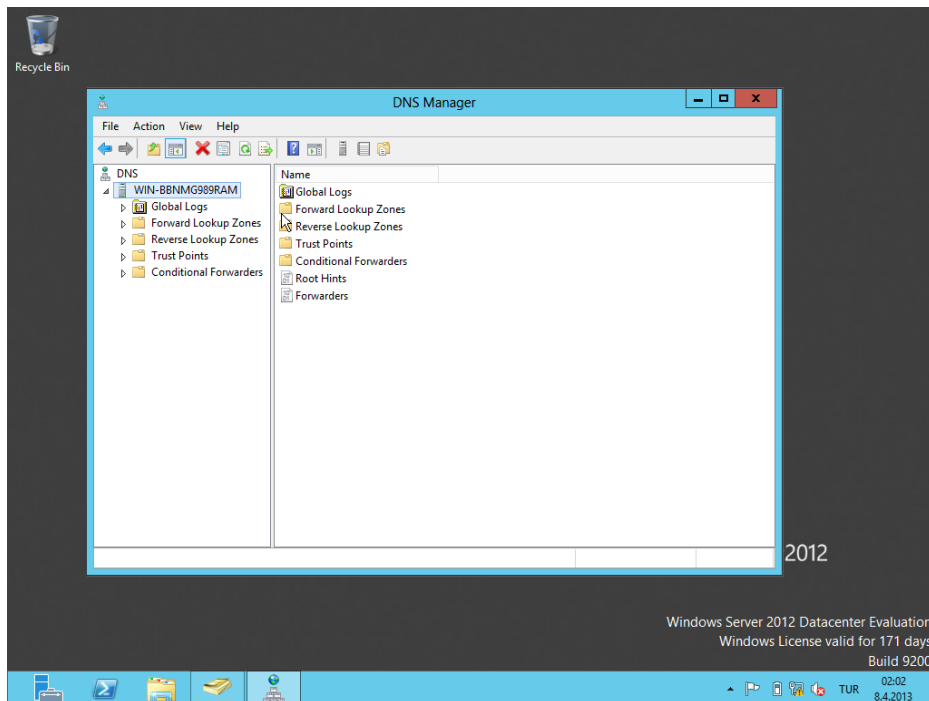


**Resim 1.19: Prerequisites Check enceresi**

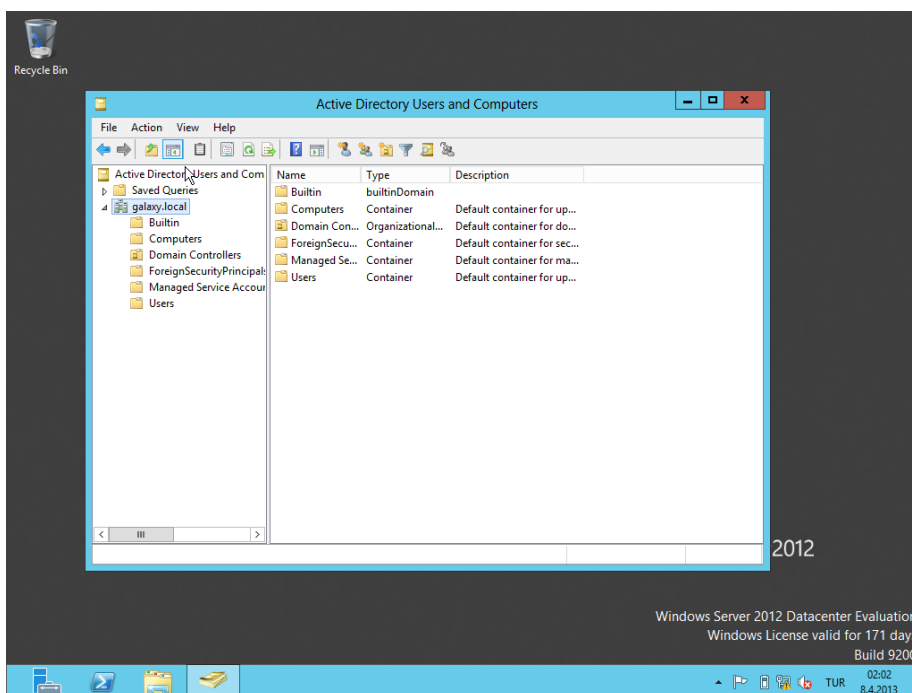
Resim 1.20, Resim 1.21, Resim 1.22’de kurulum sonrası ekranlar görölmektedir.



**Resim 1.20: Dashboard Penceresi**



**Resim 1.21: DNS Manager Penceresi**



**Resim 1.22: AD Users and Computers Penceresi**

### 1.1.2. Etki Alanı Oluşturma (Powershell 3.0)

Powershell 3.0 ekranına:

“PS C:\Users\Administrator> Add-WindowsFeature AD-Domain-Services – IncludeManagementTools” komutu yazılır.

İşlemler arka planda bilgisayarca yapıldıktan sonra; GUI’de görülen “Promote this server to a domain controller” penceresine eşdeğer noktaya gelinmiş olunur.

“Install-ADDSTForest –Domainname galaxy.local –CreateDNSDelegation:\$False – DataBasePath “C:\NTDS” –ForestMode Win2012 –DomainMode Win2012 – DomainNetBiosName galaxy –InstallDNS:\$True –LogPath “C:\NTDS” –SysvolPath “C:\NTDS\Sysvol” komutu yazılarak kurulumu devam edilir.

Kurulum sihirbazı tarafından “Directory Services Restore Mode” şifresi girilmesi istenen satıra şifre girilir. İşlemlerin ardından sistem restart eder ve sunucumuzda etki alanı kurulmuş olur.

## 1.2. Active Directory DNS İlişkisi

DNS, Active Directory için isimleri IP eşleşmelerini sağlayan servise verilen isimdir.

Örneğin: Tarayıcıya [www.meb.gov.tr](http://www.meb.gov.tr) yazdığımızda DNS bu adresin IP adresini istemci makineye göndererek işlevini yerine getirmiş olur.

DNS’te 2 çeşit alan vardır.

1. Forward Lookup Zones: İsmi IP adresine çevrilir. (SRV)
2. Reverse Lookup Zones: IP adresi isme çevrilir. (PTR)

## 1.3. Etki Alanı (Active Directory)

Etki alanı ve orman işlev düzeyleri, Active Directory Etki Alanı Hizmetleri (AD DS) ortamınızda etki alanı genelindeki veya orman genelindeki özellikleri etkinleştirmenize imkân tanıyan bir yoldur. Ağ ortamınıza bağlı olarak etki alanı ve orman işlevinin farklı düzeyleri kullanılabilir.

Etki alanınızdaki veya ormandaki tüm etki alanı denetleyicileri Windows Server’ın en son sürümünü çalıştırıyorsa ve etki alanı ve orman işlev düzeyi en yüksek değere ayarlanmışsa, etki alanı genelindeki ve orman genelindeki tüm özellikler kullanılabilir. Etki alanında veya ormanda Windows Server’ın eski sürümlerini çalışan etki alanı denetleyicileri varsa, AD DS özellikleri sınırlıdır.

## 1.4. Etki Alanı İşlev Düzeyleri

Etki alanı işlevselliği tüm etki alanını veya yalnızca söz konusu etki alanını etkileyen özellikleri etkinleştirir. Aşağıdaki tabloda, etki alanı işlev düzeyleri ve karşılık gelen etki alanı denetleyicileri listelenmiştir:

Etki Alanı İşlev Düzeyi	Desteklenen Etki Alanı Denetleyicisi İşletim Sistemleri
Windows Server 2003	Windows Server 2008 R2 Windows Server 2008 Windows Server 2003
Windows Server 2008	Windows Server 2008 R2 Windows Server 2008

Aşağıdaki tabloda etki alanı işlev düzeyleri için etkin olan etki alanı genelindeki özellikler tanımlanmıştır.

Etki Alanı İşlev Düzeyi	Etkinleştirilmiş Özellikler
Windows 2000 özgün	Varsayılan tüm Active Directory özellikleri ve aşağıdaki özellikler: <ul style="list-style-type: none"><li>➤ Evrensel gruplar hem dağıtım hem de güvenlik grupları için etkinleştirilir.</li><li>➤ Grupları iç içe geçirme</li><li>➤ Güvenlik grupları ve dağıtım grupları arasında dönüşümü mümkün kılan grup dönüşümü etkinidir.</li><li>➤ Güvenlik kimliği (SID) geçmiş</li></ul>
Windows Server 2003	Tüm varsayılan Active Directory özellikleri, Windows 2000 özgün etki alanı işlev düzeyinin tüm özellikleri ve aşağıdaki özellikler: <ul style="list-style-type: none"><li>➤ Etki alanı denetleyicisinin adını değiştirmeye hazırlık için, Netdom.exe etki alanı yönetim aracını kullanabilme</li><li>➤ Oturum açma zaman damgasının güncelleştirilmesi. <b>lastLogonTimestamp</b> özniteliği kullanıcı veya bilgisayarın en son oturum saatiyle güncelleştirilir. Bu öznitelik etki alanı içinde çoğaltılır.</li><li>➤ inetOrgPerson nesnesi ve kullanıcı nesnelerinde etkin parola olarak <b>userPassword</b> özniteliğini ayarlama yeteneği</li><li>➤ Kullanıcılar ve Bilgisayarlar kapsayıcılarını yeniden</li></ul>

	<p>yönlendirebilme yeteneği</p> <ul style="list-style-type: none"> <li>➤ Varsayılan olarak, bilgisayar ve kullanıcı/grup hesaplarını barındırmak için iki iyi bilinen kapsayıcı mevcuttur: cn=Bilgisayarlar,&lt;domain root&gt; ve cn=Kullanıcılar,&lt;domain root&gt;. Bu özellik, bu hesaplar için yeni ve iyi bilinen bir konum tanımlamaya olanak sağlar.</li> <li>➤ Yetkilendirme Yöneticisi, yetkilendirme ilkelerini AD DS'de depolayabilir.</li> <li>➤ Uygulamaların Kerberos kimlik doğrulama protokolü yoluyla kullanıcı kimlik bilgilerinin güvenli temsil avantajından yararlanmasına olanak sağlayan zorunlu temsilci seçme özelliği dâhildir. Yalnızca belirli hedef hizmetlere temsilci atanacak biçimde yapılandırabilirsiniz.</li> <li>➤ Güvenilen bir ormanda güvenen ormandaki kaynak sunucularında kimlik doğrulamasına izin verilen kullanıcı ve grupları belirtmeye olanak sağlayan seçmeli kimlik doğrulama desteklenir.</li> </ul>
Windows Server 2008	<p>Varsayılan tüm Active Directory özellikleri, Windows Server 2003 etki alanı işlev düzeyindeki tüm özellikler artı aşağıdaki özellikler:</p> <ul style="list-style-type: none"> <li>➤ SYSVOL içeriğinin daha sağlam ve ayrıntılı çoğaltılmasını sağlayan SYSVOL için Dağıtılmış Dosya Sistemi Çoğaltma desteği</li> <li>➤ Kerberos kimlik doğrulama protokolü için Gelişmiş Şifreleme Hizmetleri (AES 128 ve 256) desteği.</li> <li>➤ Bir kullanıcının başarılı olan son etkileşimli oturum açma saatini, bu işlemin hangi iş istasyonundan gerçekleştirildiğini ve son oturum açmanın ardından başarısız olan oturum açma girişimi sayısını görüntüleyen Son Etkileşimli Oturum Açma Bilgileri özelliği</li> <li>➤ Bir etki alanındaki kullanıcılar ve genel güvenlik grupları için parola ilkeleri ve hesap kilitleme ilkelerinin belirtilmesine olanak sağlayan iyi ayarlanmış parola ilkeleri</li> </ul>
Windows Server 2008 R2	<p>Tüm varsayılan Active Directory özellikleri, Windows Server 2008 etki alanı işlev düzeyinin tüm özellikleri ve aşağıdaki özellikler:</p> <ul style="list-style-type: none"> <li>➤ Her kullanıcının Kerberos belirtecinin içinde etki alanı kullanıcılarının kimliğini doğrulamak için kullanılan oturum açma yönteminin türü (akıllı kart veya kullanıcı adı/parola) hakkında bilgileri paketleyen kimlik</li> </ul>

	doğrulama mekanizması güvencesidir. Bu özellik, Active Directory Federasyon Hizmetleri (AD FS) gibi bir federal kimlik yönetimi altyapısının dağıtıldığı bir ağ ortamında etkinleştirildiğinde, bir kullanıcının oturum açma yöntemine dayalı kimlik doğrulamasını belirlemek üzere geliştirilen talep kullanan herhangi bir uygulamaya erişilmeye çalışıldığında, belirteçteki bilgiler ayıklanabilir.
--	---

#### 1.4.1. Orman İşlev Düzeyleri

Orman işlev düzeyleri ormanınızdaki tüm etki alanlarında özellikleri etkinleştirir. Aşağıdaki tabloda, orman işlev düzeyleri ve bunlara karşılık gelen etki alanı denetleyicileri listelenmiştir.

Orman işlev düzeyi	Desteklenen etki alanı denetleyicisi işletim sistemleri
Windows Server 2003	Windows Server 2008 R2 Windows Server 2008 Windows Server 2003
Windows Server 2008	Windows Server 2008
	Windows Server 2008 R2

#### 1.4.2. Etki Alanı İşlev Düzeyini Yükseltme

Active Directory Etki Alanı Hizmetleri'ni (AD DS) yüklediğinizde, bir grup temel Active Directory özelliği varsayılan olarak etkinleştirilir. Her etki alanı denetleyicisindeki temel Active Directory özelliklerine ek olarak, etki alanı veya ormandaki tüm etki alanı denetleyicileri Windows sunucusunun sonraki bir sürümünü çalıştırıyorsa, kullanılabilecek etki alanı çapında ve orman çapında Active Directory özellikleri vardır.

Etki alanı genelindeki tüm özellikleri etkinleştirmek için, etki alanındaki tüm etki alanı denetleyicilerinin Windows Server 2008 R2 ve sonraki sürümleri çalıştırıyor olması ve etki alanı işlev düzeyinin Windows Server 2008 R2 veya üzerine yükseltilmiş olması gereklidir. **Domain Admins** veya **Enterprise Admins** veya eşdeğer bir gruptaki üyelik, bu yordamı tamamlamak için gereken en düşük üyeliktir.



### **Etki alanı işlev düzeyini yükseltmek için:**

1. Active Directory Etki Alanları ve Güvenleri'ni açın. Active Directory Etki Alanları ve Güvenleri'ni açmak için, **Başlat'**ı tıklatın, **Yönetim Araçları'nın** üzerine gelin, sonra **Active Directory Etki Alanları ve Güvenleri'ni** tıklatınız.
2. Konsol ağacında, işlev düzeyini yükseltmek istediğiniz etki alanını sağ tıklatın ve ardından **Etki Alanı İşlev Düzeyini Yükselt'i** tıklatınız.
3. **Uygun bir etki alanı işlev düzeyi seçin** penceresinde değeri belirleyip **Yükselt** öğesini seçiniz.

#### **➤ Dikkat edilecek diğer noktalar**

- Etki alanı işlev düzeyini Active Directory Kullanıcıları ve Bilgisayarları ek bileşeninde etki alanını sağ tıklattıktan sonra **Etki Alanı İşlev Düzeyini Yükselt'i** tıklatarak da yükseltebilirsiniz.
- Geçerli etki alanı işlev düzeyi **Etki alanı işlev düzeyini yükselt** iletişim kutusunda **Geçerli etki alanı işlev düzeyi** altında görüntülenir.
- Bu yordamı gerçekleştirmek için, AD DS'de Domain Admins grubunun veya Enterprise Admins grubunun üyesi olmanız ya da uygun yetkilere sahip bir temsilci olmanız gerekir. En iyi güvenlik yöntemi olarak, bu yordam için **Farklı Çalıştır** kullanmayı dikkate alın. Daha fazla bilgi için Yardım ve Destek'te "farklı çalıştır komutunu kullanma" ifadesini aratınız.

Bu yordamdaki görevi Windows PowerShell™ için Active Directory modülü kullanarak da gerçekleştirebilirsiniz. Active Directory modülü uygulamasını açmak için, **Başlat'**ı tıklatın, **Yönetim Araçları'ı** ve ardından **Windows PowerShell için Active Directory Modülü** öğesini tıklatınız.

#### **1.2.1.3. Orman İşlev Düzeyini Yükseltme (Forest Functional Level)**

Active Directory Etki Alanı Hizmetleri'ni (AD DS) yüklediğinizde, bir grup temel Active Directory özelliği varsayılan olarak etkinleştirilir. Her etki alanı denetleyicisindeki temel Active Directory özelliklerine ek olarak, etki alanı veya ormandaki tüm etki alanı denetleyicileri Windows sunucusunun sonraki bir sürümünü çalıştırıyorsa, kullanılabilecek etki alanı çapında ve orman çapında Active Directory özellikleri vardır.

Tüm orman çapındaki özellikleri etkinleştirmek için, ormandaki tüm etki alanı denetleyicilerinin Windows Server 2008 R2 veya sonraki sürümleri çalıştırıyor olması ve orman işlev düzeyinin Windows Server 2008 R2 veya sonraki düzeye yükseltilmiş olması gereklidir.

**Enterprise Admins** veya eşdeğer bir gruba üyelik, bu yordamı gerçekleştirmek için en düşük gerekliliktir.

- Orman işlev düzeyini yükseltmek için;
  - Active Directory Etki Alanları ve Güvenleri'ni açınız. Active Directory Etki Alanları ve Güvenleri'ni açmak için, **Başlat'**ı tıklatınız, **Yönetim Araçları'**nın üzerine geliniz, sonra **Active Directory Etki Alanları ve Güvenleri'**ni tıklatınız.
  - Konsol ağacında **Active Directory Etki Alanları ve Güvenleri'**ni sağ tıklatın ve **Orman İşlev Düzeyi Artırma'yı** tıklatınız.
  - **Uygun bir orman işlev düzeyi seçin** penceresinde değeri belirleyip **Yükselt** öğesini seçiniz.

Windows Server'ın eski bir sürümünü çalıştıran etki alanı denetleyicileriniz varsa ya da olacaksa, orman işlev düzeyini daha yüksek bir değere yükseltmeyiniz.

- Dikkat edilecek diğer noktalar
  - Bu yordamı gerçekleştirmek için, AD DS'de Enterprise Admins grubunun üyesi olmanız veya doğru yetkilere sahip bir temsilci olmanız gerekir. En iyi güvenlik yöntemi olarak, bu yordam için **Farklı Çalıştır** kullanmayı dikkate alınız. Daha fazla bilgi için Yardım ve Destek'te "farklı çalıştır komutunu kullanma" ifadesini aratınız.
  - Orman işlev düzeyini yükselte miyorsanız, ormandaki hangi etki alanı denetleyicilerin sonraki sürüme yükseltilmesi gerektiğini belirten bir günlük dosyası kaydetmek için **Orman İşlev Düzeyini Yükselt** iletişim kutusunda **Farklı Kaydet**'i tıkatabilirsiniz.
  - Geçerli orman işlev düzeyi, **Orman İşlev Düzeyini Yükselt** iletişim kutusunda **Geçerli orman işlev düzeyi** altında görüntülenir.

Bu yordamdaki görevi Windows PowerShell için Active Directory modülü kullanarak da gerçekleştirebilirsiniz. Active Directory modülü uygulamasını açmak için, **Başlat'**ı tıklatınız, **Yönetim Araçları'**ı ve ardından **Windows PowerShell için Active Directory Modülü** öğesini tıklatınız.

- Kullanıcı asıl adı, son ekleri ekleme;

Varolan kullanıcı hesabı için kullanıcı asıl adı (UPN) soneki eklemek için Active Directory Etki Alanları ve Güvenleri'ni kullanabilirsiniz. Kullanıcı hesabı için varsayılan UPN soneki, kullanıcı hesabını içeren etki alanının Etki Alanı Adı Sistemi (DNS) etki alanı adıdır. Tüm kullanıcılar için tek bir UPN soneki belirterek yönetim ve kullanıcı

oturum açma işlemlerini kolaylaştırmak için, alternatif UPN sonekleri ekleyebilirsiniz. UPN soneki yalnızca Active Directory ormanı içinde kullanılır ve geçerli bir DNS etki alanı olmak zorunda değildir.

**Domain Admins** veya **Enterprise Admins** veya eşdeğer bir gruptaki üyelik, bu yordamı tamamlamak için gereken en düşük üyeliktir.

- UPN sonekleri eklemek için;
  - Active Directory Etki Alanları ve Güvenleri'ni açınız. Active Directory Etki Alanları ve Güvenleri'ni açmak için, **Başlat'**ı tıklatın, **Yönetim Araçları'**nın üzerine geliniz, sonra **Active Directory Etki Alanları ve Güvenleri'**ni tıklatınız.
  - Konsol ağacında **Active Directory Etki Alanları ve Güvenleri'**ni sağ tıklatın ve ardından **Özellikler'i** tıklatınız.
  - **UPN Sonekleri** sekmesinde, orman için alternatif bir UPN soneki yazınız ve ardından **Ekle'**yi tıklatınız.
  - Daha fazla alternatif UPN soneki eklemek için 3. adımı yineleyiniz.
- Dikkat edilecek diğer noktalar
  - Bu yordamı gerçekleştirmek için, Active Directory Etki Alanı Hizmetleri'nde (AD DS) Domain Admins grubunun veya Enterprise Admins grubunun üyesi olmanız ya da uygun yetkilere sahip bir temsilci olmanız gerekir. En iyi güvenlik yöntemi olarak, bu yordam için **Farklı Çalıştır** kullanmayı dikkate alın. Daha fazla bilgi için Yardım ve Destek'te "farklı çalıştır komutunu kullanma" ifadesini aratınız.
  - UPN sonekleri, geçerli karakterler ve sözdizimi açısından DNS kurallarına uymalıdır.

Bu yordamdaki görevi Windows PowerShell için Active Directory modülü kullanarak da gerçekleştirebilirsiniz. Active Directory modülü uygulamasını açmak için, **Başlat'**ı tıklatın, **Yönetim Araçları'**ı ve ardından **Windows PowerShell için Active Directory Modülü** ögesini tıklatın.

#### 1.2.1.4. Etki Alanı Roller ve İşlevleri

Active Directory içerisindeki rol sunucu özellik ve yeteneklerin mantıklı bölümlere ayrılmış hâli olarak tanımlanabilir. Active directory de 5 adet Rol bulunmaktadır.

➤ Bu roller;

- 1-Domain Naming Master
- 2-Schema Master
- 3-RID Pool Manager
- 4-PDC Emulator Master
- 5-Infrastructure Master

Yukarıdaki rollerin hepsi aynı sunucuda da olabilir ayrı ayrı sunuculara paylaştırılarak sunucuların yükleri hafifletilebilir. Bu roller kendi aralarında Forest seviyesi ve Domain seviyesi olarak ikiye ayrılır.

#### **1.2.1.5. Forest Seviyesi Roller**

##### **1.2.1.5.1. Domain Naming Master**

Bu rolün görevi Forest içerisine Domain eklenmesi veya Domain kaldırılması görevini üstlenir. Bu role sahip sunucu sayısı her forest için sadece 1 tane olabilir.

##### **1.2.1.5.2. Global Catalog**

Active Directory Veri Tabanı üzerinde işlem yapabilen kısımdır, active directory için veri tabanı ile iletişim kurar.

##### **1.2.1.5.3. Schema Master**

Active Directory veri tabanı üzerinde doğrudan erişimi olan roldür veri tabanın motoru olarak çalışır.

Schema master rolünün schema üzerinden doğrudan erişim yetkisi vardır kullanıcı açma, grup oluşturma veya silme gibi hertürlü işlem bu rol sayesinde yapılır, Active Directory üzerinde kullanıcı açamıyorsanız ise Schema master rolünün ayakta olup olmadığına bakmak gerekir.

#### **1.2.1.6. Domain Seviyesi Roller**

##### **1.2.1.6.1. Rid Pool Manager**

Domain üzerinde SID numaraları oluşturmaktan sorumludur ,SID numaraları domain içerisindeki her grup,kullanıcı bilgisayar gibi nesnelere atanmış benzersiz bir numaradır. Bu rol çalışmazsa nesnelere SID numarası verilemeyeceğinden herhangi bir nesnede oluşturulamaz.

#### **1.2.1.6.2. Pdc Emulator Master**

Bu rol kullanıcıların şifre değişikliklerini yapmaktan ve değişiklikleri bütün domain controller bilgisayarlarda güncellemekten sorumludur .Bu rol domain controller bilgisayarlar için şifre değişikliklerini ve girilen şifrelerin doğru olup olmadığını konusunda bilgi sağlar. Diğer domain controllerlardan bilgisayarlar için bir Time server görevi yapar ve domain controller bilgisayarlar arasında zaman eşitlemesinden sorumludur.

#### **1.2.1.6.3. Infrastructure Master**

Bu rol domaindeki nesnelerin güncellenmesinden ve güncel kalmasından sorumludur. Domain controllerin Kütüphanesi gibi çalışır.

### **1.3. Site Yapısı ve Alt Ağlar**

Siteleri, alt ağları ve site bağlantılarını kavramak siteleri ve Active Directory Etki Alanı Hizmetleri'nde (AD DS) uygulanışını verimli bir şekilde yönetmenize yardımcı olur.

#### **1.3.1. Sitelere Genel Bakış**

AD DS'deki siteler ağınızın fiziksel yapısını veya topolojisini temsil eder. AD DS en etkili çoğaltma topolojisini oluşturmak için, dizinde site, alt ağ ve site bağlantısı nesneleri olarak depolanan ağ topolojisi bilgilerini kullanır. Çoğaltma topolojisinin kendisi, bir kaynak etki alanı denetleyicisinden bağlantı nesnesini depolayan hedef etki alanına gelen çoğaltmaya olanak veren bir takım bağlantı nesnelerinden oluşur. Bilgi Tutarlılığı Denetleyicisi (KCC) bu bağlantı nesnelerini her etki alanı denetleyicisinde otomatik olarak oluşturur.

Bir arada toplanarak çoğaltma topolojisini etkileyen site, alt ağ ve site bağlantısı nesnelerini yönetmek için Active Directory Siteleri ve Hizmetleri ek bileşenini kullanabilirsiniz.

Site ve etki alanlarını ayırt edebilmek önemlidir. Etki alanları kuruluşunuzun mantıksal yapısını temsil ederken, siteler ağınızın fiziksel yapısını temsil eder. Site nesneleri ve içerikleri ormanda, etki alanı veya siteden bağımsız olarak tüm etki alanı denetleyicilerine çoğaltılır.

#### **1.3.2. Siteleri Kullanma**

Site kullanan etki alanı denetleyicileri ve diğer sunucular, sitelerin sağladığı iyi bağlantı özelliklerinden yararlanmak için AD DS'de sunucu nesneleri yayımlar. Etki alanı denetleyicilerini sitelere, etki alanı verilerine nerede gereksinim duyulduğuna göre yerleştirirsiniz. Örneğin, bir etki alanındaki hiçbir kullanıcı fiziksel olarak bir sitede bulunmuyorsa, söz konusu etki alanı için bu siteye etki alanı denetleyicisi yerleştirmenin anlamı yoktur.

- Siteler aşağıdaki gibi bazı etkinlikleri kolaylaştırır:
  - **Çoğaltma.** AD DS, veriler her güncelleştirildiğinde bir site içinde ve yapılandırılabilir bir zamanlama uyarınca siteler arasında bilgileri çoğaltarak, güncel dizin bilgilerine duyulan gereksinim ile bant genişliğini en uygun Resimde kullanma gereksinimi arasında denge kurar.
  - **Kimlik doğrulaması.** Site bilgileri kimlik doğrulamayı daha hızlı ve etkili kılmaya yardımcı olur. Bir istemci bir etki alanında oturum açtığında, kimlik doğrulaması için önce yerel sitesinde bir etki alanı denetleyicisi isteğinde bulunur. Siteler belirleyerek, istemcilerin kimlik doğrulama için kendilerine en yakın etki alanı denetleyicilerini kullanmasını sağlayabilirsiniz; bu da kimlik doğrulama işlemindeki gecikmeleri ve geniş alan ağı (WAN) bağlantıları üzerindeki trafiği azaltır.
  - **Hizmet konumu.** Active Directory Sertifika Hizmetleri (AD CS), Exchange Server ve Message Queuing gibi diğer hizmetler, istemcilerin en yakın hizmet sağlayıcıları kolayca bulmasına olanak sağlayan site ve alt ağ bilgilerini kullanabilen nesneleri depolamak için AD DS'yi kullanır.

### 1.3.3. Siteleri Ve Alt Ağları İlişkilendirme

AD DS'deki bir alt ağ nesnesi komşu bilgisayarları gruplar; bu grupta, yakın posta adreslerinin posta kodlarıyla gruplanmasına çok benzer. Bir siteyi bir veya daha fazla alt ağla ilişkilendirerek, siteye birtakım IP adresleri atarsınız.

Bir ormanda ilk etki alanı denetleyicisini oluşturmak için Active Directory Etki Alanı Hizmetleri sunucu rolünü eklediğinizde, AD DS'de varsayılan bir site (Varsayılan-İlk-Site-Adı) oluşturulur. Bu site dizindeki tek site olduğu sürece, ormana eklediğiniz tüm etki alanı denetleyicileri bu siteye atanır. Ancak, ormanınızda birden fazla site olacaksa, tüm ek sitelerin yanı sıra Varsayılan-İlk-Site-Adı'na IP adresleri atayan alt ağlar oluşturmanız gerekir.

### 1.3.4. Sitelere Bilgisayar Atama

Sunucu nesneleri AD DS'de uygulamalara veya hizmetlere göre oluşturulur ve IP adreslerine göre bir siteye yerleştirilirler. Bir sunucuya Active Directory Etki Alanı Hizmetleri sunucu rolünü eklediğinizde, sunucunun IP adresinin eşleştiği alt ağı içeren AD DS sitesinde bir sunucu nesnesi oluşturulur. Etki alanı denetleyicisinin IP adresi ormandaki herhangi bir siteyle eşleşmezse, etki alanı denetleyicisinin sunucu nesnesi, AD DS için çoğaltma kaynağını sağlayan etki alanı denetleyicisinin sitesinde oluşturulur.

Bir istemci için site ataması, oturum açma sırasındaki IP adresine ve alt ağ maskesine göre dinamik olarak belirlenir.

### 1.3.5. Etki Alanı Denetleyicilerini Siteye Göre Bulma

Etki alanı denetleyicileri, Etki Alanı Adı Sistemi'nde (DNS), site adlarını tanımlayan hizmet (SRV) kaynağı kayıtlarına kaydolur. Etki alanı denetleyicileri ayrıca DNS'de, IP adreslerini tanımlayan ana bilgisayar (A) kaynağı kayıtlarına da kaydolur. Bir istemci etki alanı denetleyicisi istediğinde, DNS'ye site adını sağlar. DNS bu site adını, söz konusu sitede (veya istemciye en yakın bir sonraki sitede) bir etki alanı denetleyicisi bulmak için kullanır. DNS bundan sonra, etki alanı denetleyicisine bağlanması için istemciye etki alanı denetleyicisinin IP adresini sağlar. Bu nedenle, bir etki alanı denetleyicisine atadığınız IP adresinin, ilgili sunucu nesnesinin sitesiyle ilişkilendirilen bir alt ağla eşleştiğinden emin olmanız gerekir. Aksi takdirde, bir istemci etki alanı denetleyicisi istediğinde, döndürülen IP adresi uzaktaki bir sitede bulunan bir etki alanı denetleyicisinin IP adresi olabilir. Bir istemci uzaktaki bir siteye bağlandığında, bu durum performansın yavaş olması ve pahalı WAN bağlantıları üzerinde trafiğin gereksiz yere artmasıyla sonuçlanabilir.

### 1.3.6. Site Bağlantılarıyla Siteleri Bağlama

Ağlar genellikle WAN'lar ile bağlanan birtakım yerel ağlardan (LAN) oluşur. AD DS'de, site bağlantı nesneleri siteler arasındaki WAN bağlantılarını temsil eder. Site içinde çoğaltma işlemleri dizin güncelleştirmeleri oluştuğunda otomatik olarak gerçekleşirken, siteler arası çoğaltma işlemi (daha yavaş ve daha pahalı olan WAN bağlantıları üzerinden yapılır.) 3 saatte bir gerçekleşecek şekilde zamanlanır. WAN bağlantısı trafiği üzerinde denetim kurabilmek için, varsayılan zamanlamayı belirttiğiniz dönemlerde ve belirttiğiniz aralıklarla gerçekleşecek şekilde değiştirebilirsiniz.

## 1.4. Site Oluşturma

Ortamınızda yeni siteler oluşturmak için Active Directory Siteleri ve Hizmetleri ek bileşenini kullanabilirsiniz.

Bu yordamı tamamlamak için en azından ormandaki **Enterprise Admins** grubuna veya orman kök etki alanındaki **Domain Admins** grubuna ya da eşdeğerine üye olmanız gerekir.

- Site oluşturmak için;
  1. Active Directory Siteleri ve Hizmetleri'ni açın. Active Directory Siteleri ve Hizmetleri'ni açmak için, **Başlat'**ı tıklatınız, **Yönetim Araçları'nın** üzerine geliniz, sonra **Active Directory Siteleri ve Hizmetleri'ni** tıklatınız. işletim sisteminde Active Directory Siteleri ve Hizmetleri'ni açmak için, **dssite.msc**.
  2. Konsol ağacında, **Siteler'i** sağ tıklatınız ve sonra **Yeni Site'yi** tıklatınız.
  3. **Ad** alanına, yeni sitenin adını yazınız.
  4. **Bağlantı Adı** alanında, bir site bağlantı nesnesini tıklatın ve **Tamam'**ı tıklatınız.

### 1.4.1. Alt Ağ Oluşturma

Yeni alt ağlar oluşturmak için Active Directory Siteleri ve Hizmetleri ek bileşenini kullanabilirsiniz.

Bu yordamı tamamlamak için en azından ormandaki **Enterprise Admins** grubuna veya orman kök etki alanındaki **Domain Admins** grubuna ya da eşdeğerine üye olmanız gerekir.

- Alt ağ oluşturmak için
  - Active Directory Siteleri ve Hizmetleri'ni açınız. Active Directory Siteleri ve Hizmetleri'ni açmak için, **Başlat'**ı tıklatın, **Yönetim Araçları'nın** üzerine gelin, sonra **Active Directory Siteleri ve Hizmetleri'ni** tıklatınız. işletim sisteminde Active Directory Siteleri ve Hizmetleri'ni açmak için, **dssite.msc**.
  - Konsol ağacında, **Siteler'i** çift tıklatınız, **Alt Ağlar'**ı sağ tıklatın ve **Yeni Alt Ağ'**ı tıklatınız.
  - **Önek'e**, IP sürüm 4 (IPv4) veya IP sürüm 6 (IPv6) alt ağının önekini yazınız.
  - **Bu örnek için bir site nesnesi seçin** alanında, bu alt ağla ilişkilendirilecek siteyi tıklatın ve sonra **Tamam'**ı tıklatınız.

### 1.4.1. Site Bağlantısı Oluşturma

Yeni site bağlantıları oluşturmak için Active Directory Siteleri ve Hizmetleri ek bileşenini kullanabilirsiniz.

Bu yordamı tamamlamak için en azından ormandaki **Enterprise Admins** grubuna veya orman kök etki alanındaki **Domain Admins** grubuna ya da eşdeğerine üye olmanız gerekir.

- Site bağlantısı oluşturmak için:
  - Active Directory Siteleri ve Hizmetleri'ni açınız. Active Directory Siteleri ve Hizmetleri'ni açmak için, **Başlat'**ı tıklatın, **Yönetim Araçları'nın** üzerine geliniz, sonra **Active Directory Siteleri ve Hizmetleri'ni** tıklatınız. işletim sisteminde Active Directory Siteleri ve Hizmetleri'ni açmak için, **dssite.msc**.



- Konsol ağacında, site bağlantısının kullanmasını istediğiniz siteler arası aktarım protokolünü sağ tıklatınız.
- **Yeni Site Bağlantısı'nı** tıklatınız.
- **Ad** alanına, site bağlantısının adını yazınız.
- **Bu site bağlantısında olmayan siteler** alanında, site bağlantısına eklenecek bir siteyi tıklatın ve ardından **Ekle**'yi tıklatın. Site bağlantısına başka siteler de eklemek için bunu tekrarlayın. Site bağlantısından bir siteyi kaldırmak için, **Bu bağlantıdaki siteler**'de siteyi tıklatın ve **Kaldır**'ı tıklatınız.
- Bu site bağlantısıyla bağlanmasını istediğiniz siteleri ekledikten sonra **Tamam**'ı tıklatınız.

#### 1.4.2. Site Bağlantısına Site Ekleme veya Site Kaldırma

Ormanınıza siteler ve site bağlantıları eklediğinizde, aynı sitenin iki site bağlantısına eklenmesi gibi durumlara neden olabilirsiniz. Site bağlantı üzerinden çoğaltma yapılması gereken tüm sitelerin bir site bağlantısında bulunmaması gibi durumlara da neden olabilirsiniz. Site bağlantılarına site eklemek veya site bağlantılarından site kaldırmak için Active Directory Siteleri ve Hizmetleri ek bileşenini kullanabilirsiniz.

Bu yordamı tamamlamak için en azından ormandaki **Enterprise Admins** grubuna veya orman kök etki alanındaki **Domain Admins** grubuna ya da eşdeğerine üye olmanız gerekir.

- Site bağlantısına site eklemek veya site kaldırmak için:
  - Active Directory Siteleri ve Hizmetleri'ni açınız. Active Directory Siteleri ve Hizmetleri'ni açmak için, **Başlat**'ı tıklatın, **Yönetim Araçları**'nın üzerine gelin, sonra **Active Directory Siteleri ve Hizmetleri**'ni tıklatınız.
  - işletim sisteminde Active Directory Siteleri ve Hizmetleri'ni açmak için, **dssite.msc**.
  - Konsol ağacında, site ekleyeceğiniz veya kaldıracağınız site bağlantısını içeren siteler arası aktarım klasörünü tıklatınız.
  - Ayrıntılar bölmesinde, bir site eklemek veya kaldırmak istediğiniz site bağlantısını sağ tıklatın ve sonra **Özellikler**'i tıklatınız.
  - İlgili listede, bu site bağlantısına eklemek veya kaldırmak istediğiniz siteyi tıklatınız ve **Ekle** veya **Kaldır**'ı tıklatınız.

## 1.5. Dizin Yapısı

Dizin yapısı, ulaşmak istediğiniz objeye ait olan adres bilgisini içerir.

### 1.5.1. Genel Katalog (Global Catalog)

Çoklu Active Directory Etki Alanı Hizmetleri (AD DS) ormanındaki her etki alanında her nesnenin aranabilir, kısmi gösterimini içerir dağıtılmış bir veri deposudur. Kısaca içerisinde etki alanına ait her bilginin, özelliklerin, niteliklerin tutulduğu yapıdır. Genel katalog, genel katalog sunucuları olarak atanmış ve çoğaltma yoluyla dağıtılır etki alanı denetleyicileri üzerinde depolanır. Farklı etki alanı denetleyicileri alışları içermeyen çünkü genel kataloğa yönlendirilir aramalar hızlıdır.

Yapılandırma ve sema dizini bölümü çoğaltmalarını ek olarak, ormandaki her etki alanı denetleyicisi tek bir etki alanı dizin bölümünün tam, yazılabilir çoğaltma depolar. Bu nedenle, etki alanı denetleyicisi, etki alanı sadece nesneleri bulabilir. Farklı bir etki olarak bir nesne konumlandırılması kullanıcı ya da uygulamanın istenen nesnenin etki sağlamak için gerekli olacaktır.

Genel katalog etki alanı adını bilmek zorunda kalmadan herhangi bir etki alanından nesneleri bulmak için yeteneği sağlar. Bir genel katalog sunucusu tam, yazılabilir etki alanı dizini bölümü çoğaltma yanı sıra, aynı zamanda ormandaki tüm diğer etki alanı dizin bölümleri kısmi, salt okunur bir kopyasını saklar, bir etki alanı denetleyicisi. Öznitelikleri yalnızca sınırlı bir dizi her nesne için yer alması nedeniyle ek bir etki alanı dizini bölümleri kısmi vardır. Çoğu arama için kullanılan yalnızca öznitelikleri dahil ederek, hatta en büyük ormandaki her etki alanında her nesnenin tek bir genel katalog sunucusu veritabanında temsil edilebilir.

### 1.5.2. LDAP (Lightweight Directory Access Protocol - Hafifletilmiş Dizin Erişim Protokolü)

Elektronik ortamda belirli türden nesneleri içerisinde bulunduran ve bu nesneler arasında arama yapma imkânı veren yapıdır. Dizinlere örnek olarak; tutulan kişi listeleri, telefon rehberi, bir ağa dahil olan bilgisayarların listeleri ve bir şirkette çalışan personele dair tutulan kayıtlar verilebilir. Dizinlerin genel özellikleri incelendiğinde ise, yapısal depolama yaptıkları, bu depolamanın genellikle dağınık olduğu, içerdiği nesnelerin genellikle birbirlerinden bağımsız oldukları ve hiyerarşik bir düzende sıralandıkları görülecektir.

Dizin standartları 1988 yılında ISO-ITU tarafından X.500 standardı ile belirlenmiştir. X.500 standardı dizinlerin kullanımı ve erişimi ile ilgili dört farklı protokolü içerisinde barındırmaktadır. Bunlar; DAP (Directory Access Protocol - Dizin Erişim Protokolü), DSP (Directory System Protocol - Dizin Sistemi Protokolü), DISP (Directory Information Shadowing Protocol - Dizin Bilgileri Gölgeleme Protokolü) ve DOP (Directory Operational Bindings Management Protocol - Dizin İşlemsel Bağlantı Yönetim Protokolü) 'dür.

LDAP (Lightweight Directory Access Protocol – Hafifletilmiş Dizin Eriřim Protokolü) ise Michigan Üniversitesi'nde geliştirilen, son kullanıcıların kullanımı açısından oldukça karmařık bir yapıya sahip olan X.500 standardına uygun olarak oluşturulmuş dizinlere erişimde kullanılan DAP protokolünün hafifletilmiş biçimidir. LDAP in bir başka oluşturulma amacı ise ilk zamanlarda DAP protokolünün sadece OSI (Open System Interconnection) referans modelini kullanmasıdır. LDAP protokolü ise TCP/IP protokolünü kullandığından dizinlere Web üzerinden de erişim imkânı sunmaktadır. Bir diğer önemli LDAP protokolü özelliğı ise açık bir protokol olmasıdır. Bu sayede protokolün bilgi modeli geliştirilebilmekte ve verileri tutan sunucu çeşidinden bağımsız olarak verilere erişim sağlanabilmektedir.

LDAP açık bir protokol olması nedeniyle, günümüzde farklı uygulamalarda sıklıkla kullanılmaktadır. Linux işletim sistemlerinde OpenLDAP programı aracılığıyla kullanılan LDAP protokolü; Windows işletim sistemlerinde ise orta ve büyük ölçekli işletmelerde yaygın kullanıma sahip olan Aktif Dizin (Active Directory) hizmeti olarak yer almaktadır. Active Directory, yaptığı birçok işlemde (yeni kullanıcı ve yeni grup tanımlama, hâlihazırdaki kullanıcı bilgilerine erişme ve bu bilgileri güncelleme, nesneler arasında esnek sorgulama yapılabilmesi gibi işlemler) arka planda LDAP protokolünü kullanmaktadır. Ayrıca, Active Directory sunucusuna bağlanarak ihtiyaç duyulan verilerin alınması ve bu verilen düzenlenebilmesi LDAP aracılığıyla sağlanmaktadır.

LDAP veri yapıları incelendiğinde ise 3 temel özellik göze çarpmaktadır. Bunlardan birincisi LDAP verilerinin alt sınıflara ve hiyerarşik bir yapıya sahip olması, yani nesne tabanlı ve sıradüzensel bir yapıda olmasıdır. İkinci önemli özellik ise her nesnenin kendine özgü nitelik(attribute) ve değerlerden (value) meydana gelmiş olmasıdır. Bu nitelik ve değerler nesneyi dizinde bulunan diğer nesnelerden farklı kılmakta ve nesneyi tanımlamaktadır. Bu nedenle nesnelere ait nitelikler birden fazla değere sahip olabilmekte ve bu değerler metin ya da ikilik sistem verileri olabilmektedir. Üçüncü önemli özellik ise depolanan her nesneyi tanımlayan tek bir belirleyici ismin (distinguished name - DN) olmasıdır.

LDAP verileri hiyerarşik düzeni, oluşturulan nesnelerin içerdikleri farklı nitelikler sayesinde sağlanmaktadır. Belirli niteliklere sahip nesnelerin hiyerarşik bir düzende bir araya gelerek oluşturdukları yapıya ağaç (tree) adı verilmektedir. Bir ağaçta bulunan yapılar nasıl farklı dallar aracılığıyla gövdeye ve sonrasında köke bağlanıyorsa, LDAP nesneleri de kendi içlerinde birbirlerinden farklı olsalar da ortak noktaları sebebiyle aynı grup içerisinde yer alabilmektedirler. Bu ağaç yapısının en üst kısmında kök (Root) dizin yer almaktadır. Kök dizin, organizasyonun dahil olduğu temel dizindir. Dizin hizmeti veren bir sunucunun belirleyici ismi (distinguished name) ise etki alanı öğeleri (Domain Component - DC) tarafından belirlenmektedir. Etki alanı öğeleri bir anlamda ağaç yapısının ana kimlik bilgilerini oluşturmaktadır ve bu ağaç yapısı içerisinde bulunan tüm nesneler için ortaktır. Hiyerarşik yapıda etki alanı öğelerinden sonra gelen yapılar ise organizasyon üniteleridir (Organizational Unit - OU). Organizasyon üniteleri oluşturulan nesnelerin daha kolay ve daha esnek yönetimi amaçlı oluşturulmuş yapılardır. Bu organizasyon üniteleri kendi içlerinde yine amaca yönelik olarak başka organizasyon üniteleri de bulundurabilmektedirler. Organizasyon üniteleri altına oluşturulan nesneler ise kendilerine özgü ortak adlarla (Common Name - CN) birbirlerinden ayrılmaktadırlar. Yine bu ortak

adlarla birbirlerinden ayrılan nesneler kendi içlerinde farklı niteliklere sahip olabilmektedirler (soyadı, kullanıcı adı, telefon numarası, sicil numarası, IP Numarası... gibi). Aşağıdaki tabloda LDAP nesnelerine ait olan bazı nitelikler ve bu niteliklerin kodları görülmektedir.

LDAP Niteliği	Nitelik Kodu	Nitelik Açıklaması
Organizasyon	o	Organizasyon adı
Etki alanı ögesi	dc	DNS ögesi
Organizasyon ünitesi	ou	Organizasyon ünitesi adı
Ortak ad	cn	Oluşturulan girdinin ortak adı
Soyad	sn	Kullanıcı soyadı
Kullanıcı ID	uid	Sistem giriş kimlik adı

## UYGULAMA FALİYETİ

İşlem Basamakları	Öneriler
➤ Sunucu olarak kurulum yapılacak bilgisayarın Ip adresinin statik olup olmadığını kontrol ediniz.	➤ Ağ bağlantılarına ve çeşitlerine dikkat ediniz.
➤ Galaxy.local adında bir etki alanı oluşturunuz.	➤ Etki alanı isminin yazılışına dikkat ediniz.

### KONTROL LİSTESİ

Bu faaliyet kapsamında aşağıda listelenen davranışlardan kazandığınız beceriler için **Evet**, kazanamadığınız beceriler için **Hayır** kutucuğuna (X) işareti koyarak kendinizi değerlendiriniz.

Değerlendirme Ölçütleri	Evet	Hayır
1. Active Directory kurulumunu yapmak için sunucu bilgisayarı hazırlayabildiniz mi?		
2. Active Directory kurulumunu yapabildiniz mi?		
3. Kullanıcı, Grup ve OU tanımlarını anlayabildiniz mi?		

### DEĞERLENDİRME

Değerlendirme sonunda “**Hayır**” şeklindeki cevaplarınızı bir daha gözden geçiriniz. Kendinizi yeterli görmüyorsanız öğrenme faaliyetini tekrar ediniz. Bütün cevaplarınız “**Evet**” ise “Ölçme ve Değerlendirme”ye geçiniz.

## ÖLÇME VE DEĞERLENDİRME

Bu faaliyet sonunda kazandıklarınızı aşağıdaki soruları cevaplandırarak ölçünüz.

**Aşağıdaki soruları dikkatlice okuyarak doğru seçeneği işaretleyiniz.**

1. Sunucu üzerine Active Directory nasıl kurulabilir?
  - a) Sunucu Yönetimi Penceresinden
  - b) Manage seçeneği altından
  - c) Powershell üzerinden ADDSDeployment komutları ile
  - d) Server Manager Penceresinden
  - e) Hepsi
2. Active Directory kurulum işleminde yöneticinin yapması gereken ilk adım nedir?
  - a) Sunucuya Statik ip vermek
  - b) Sunucuya dinamik ip vermek
  - c) Add roles and features linkine basmak
  - d) Role Based linkine basmak
  - e) Hiçbiri
3. Select server roles penceresinde Active Directory kurulumu yapmak için hangi seçenek aktifleştirilir?
  - a) Active Directory Certificate Services
  - b) Active Directory Domain Services
  - c) Active Directory Federation Services
  - d) DNS Server
  - e) Hyper-V
4. Active Directory ormanda ilk defa kurulacak ise Deployment Configuration penceresinden hangi seçenek seçilmelidir?
  - a) Add a domain controller to an existing domain
  - b) Add a new domain to an existing forest
  - c) Add a new forest
  - d) Add a new domain controller to an existing forest
  - e) Add a new forest to an existing forest
5. Hazır bulunan etki alanına, etki alanı yöneticisi kurulacak ise Deployment Configuration penceresinden hangi seçenek seçilmelidir?
  - a) Add a domain controller to an existing domain
  - b) Add a new domain to an existing forest
  - c) Add a new forest
  - d) Add a new domain controller to an existing forest
  - e) Add a new forest to an existing forest

6. Aşağıdakilerden hangisi Windows Server 2012'in desteklediği Forest functional level'larından biri değildir?
  - a) Windows Server 2012
  - b) Windows Server 2003
  - c) Windows Server 2008
  - d) Windows Server 2008 R2
  - e) Windows Server 2003 R2
7. Aşağıdakilerden hangisi Windows Server 2012 üzerinde ön tanımlı olarak gelen veritabanı saklanan klasördür?
  - a) C:\Windows\NTDS
  - b) C:\Program Files\NTDS
  - c) C:\Program Files (x86)\NTDS
  - d) C:\Windows\SYSVOL
  - e) C:\Program Files\SYSVOL

## DEĞERLENDİRME

Cevaplarınızı cevap anahtarı ile karşılaştırınız. Doğru cevap sayınızı belirleyerek kendinizi değerlendiriniz. Yanlış cevap verdiğiniz ya da cevap verirken tereddüt yaşadığınız sorularla ilgili konuları faaliyete dönerek tekrar inceleyiniz.

Tüm sorulara doğru cevap verdiyseniz diğer faaliyete geçiniz.

## ÖĞRENME FAALİYETİ-2

### AMAÇ

Active Directory’de kullanıcı ve grup işlemlerini yapabileceksiniz.

### ARAŞTIRMA

- Active Directory’de kullanıcı ve grup işlemlerini araştırınız. Topladığınız bilgileri rapor hâline getiriniz. Hazırladığınız raporu sınıfta öğretmeninize ve arkadaşlarınıza sununuz.

## 2. HESAP YÖNETİMİ

### 2.1. Hesap Çeşitleri

Kullanıcı hesapları, kimlik doğrulamak, kaynaklara erişim yetkisi vermek veya erişimi reddetmek ve ağınızdaki bağımsız kullanıcıların etkinliklerini denetlemek için kullanılır. Grup hesabı, birden çok kullanıcıya eş zamanlı olarak izinler ve haklar kümesi atayabilmek üzere kullanılan, kullanıcı hesaplarından oluşan bir gruptur. Bir grup aynı zamanda kişileri, bilgisayarları ve diğer grupları da içerebilir. Etki alanı kullanıcılarını yönetmek üzere Active Directory’de kullanıcı hesapları ve grup hesapları oluşturabilirsiniz. İlgili bilgisayara özel kullanıcıları yönetmek üzere yerel bilgisayarda da kullanıcı ve grup hesapları oluşturabilirsiniz.

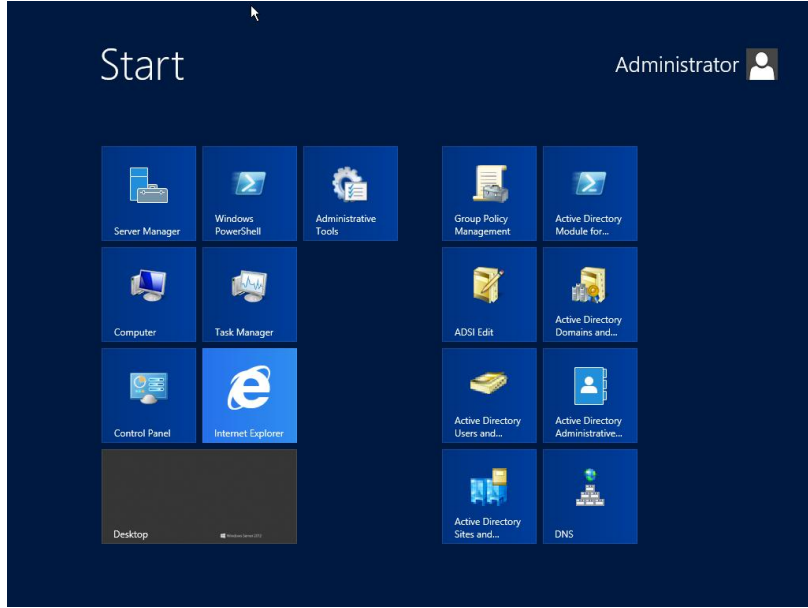
En yaygın kullanılan görevler: Active Directory’de kullanıcı hesapları oluşturma, Active Directory’de grup hesapları oluşturma, yerel bilgisayarda kullanıcı hesapları oluşturma ve yerel bilgisayarda grup hesapları oluşturmaktır.

Active Directory’yi veya Yerel grupları komut satırından yönetmede, kullanıcı ve grup hesabı oluşturmak için Powershell’i de kullanabilirsiniz.

#### 2.1.1. Active Directory’de Kullanıcı Hesabı Oluşturma

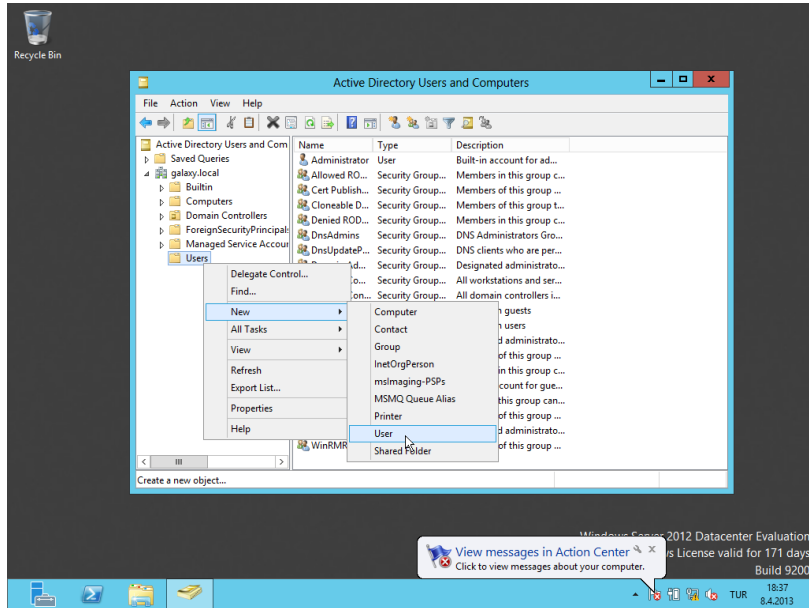
Active Directory’de kullanıcı hesabı oluşturmak için metro arayüzünden (Resim 2.1) “Active Directory Users and Computers” linkine tıklayınız.





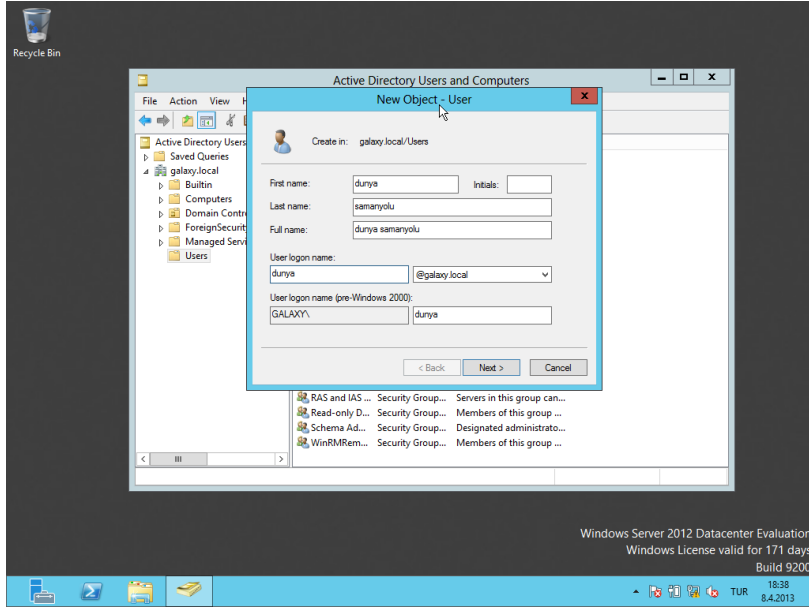
**Resim 2.1: Metro UI**

Resim 2.2’de Users üzerinde farenin sağ butonuna basılır, açılan menüden New-User seçeneği seçilir.



**Resim 2.2: Active Directory Users and Computers Penceresi**

Resim 2.3’te gerekli alanlar doldurulur. “User logon name” kısmı kullanıcının sisteme giriş yaparken kullanacağı isim olduğu için önemlidir.



**Resim 2.3: New Object-User Penceresi**

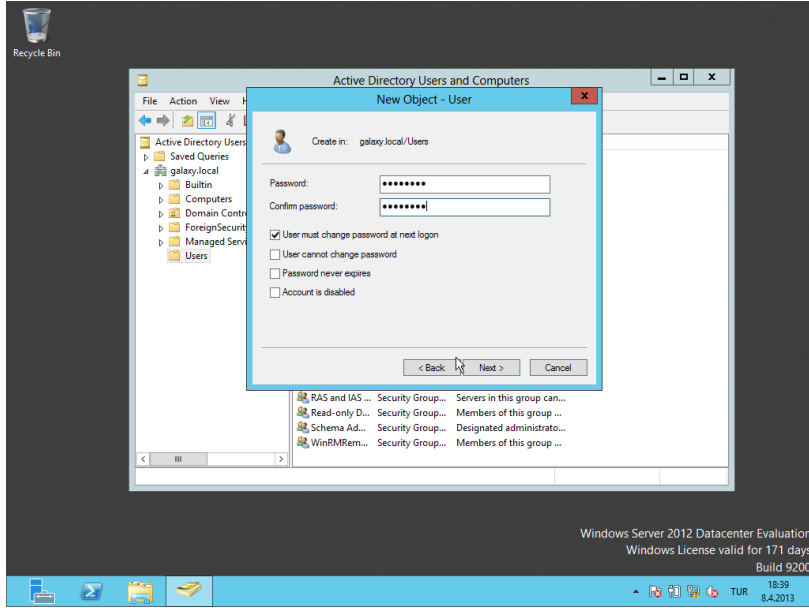
Resim 2.4’te “Password” alanına Complex (Büyük Harf, Küçük Harf, Rakam, Simgeden oluşan) bir şifre girilir.

“User must change password at next logon” seçeneği seçilir ise kullanıcı sisteme ilk giriş yaptığıında şifresini değiştirmesi istenecektir.

“User cannot change password” seçeneği seçilir ise kullanıcı asla şifresini değiştiremez.

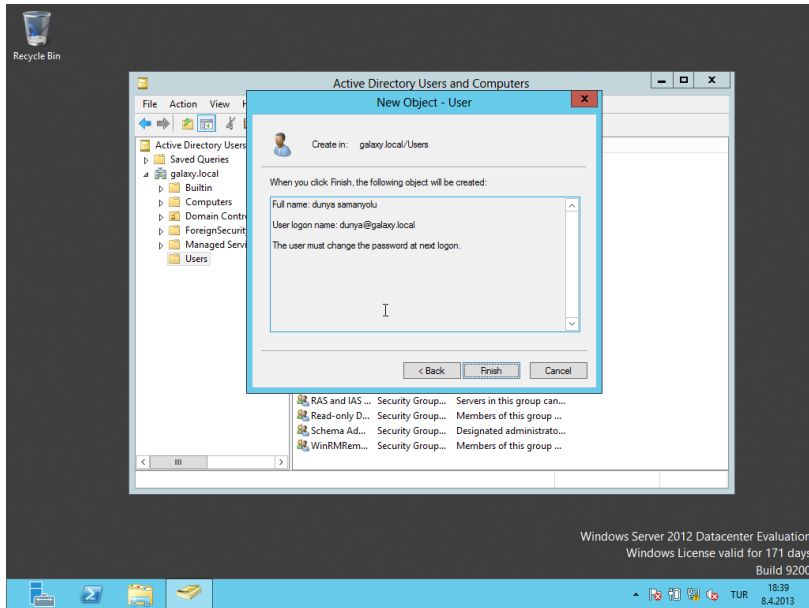
“Password never expires” seçeneği seçilir ise belirlenen şifrenin geçerlilik süresi dolmayacağından kullanıcının yeni bir şifre belirlemesi hiçbir zaman istenmeyecektir.

“Account is disabled” seçeneği seçilir ise kullanıcı hesabı pasif duruma getirilmiş olur, kullanıcı adı ile sisteme giriş yapılamaz.

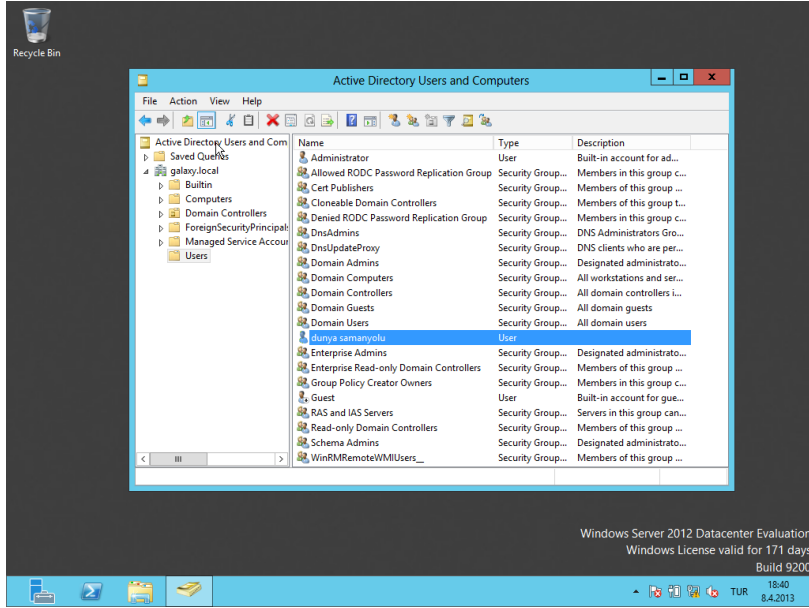


**Resim 2.4: New Object-User Penceresi**

Resim 2.5'te Finish butonuna basilarak Resim 2.6'da görüldüğü üzere Active Directory'ye bir kullanıcı eklenmiş olur.



**Resim 2.5: New Object-User Penceresi**



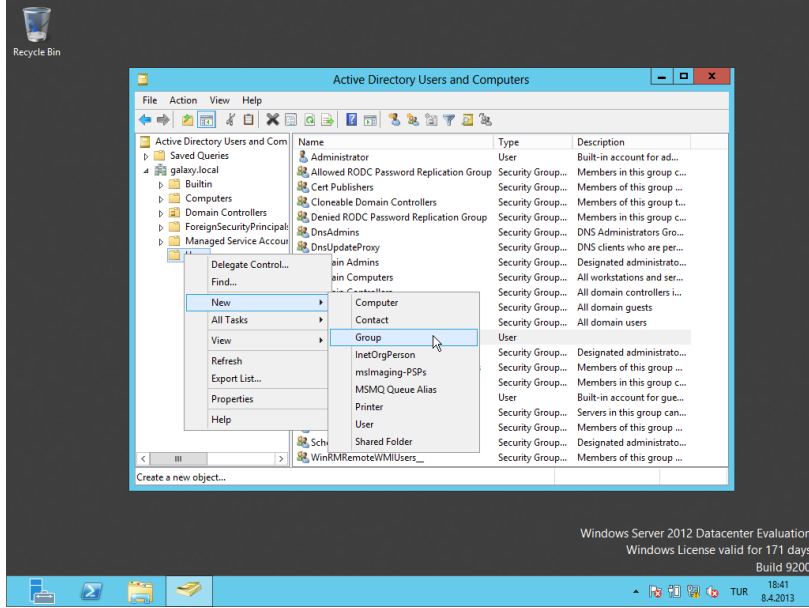
**Resim 2.6: Active Directory Users and Computers Penceresi**

### 2.1.2. Active Directory’de Grup Hesabı Oluşturma

Gruplar AD’de aynı amaca yönelik kullanıcı, bilgisayar vb. bir arada tutulduğu yapılara verilen isimdir.

- AD’de 2 tip grup vardır.
  - Security (Güvenlik) Group: Kullanıcı ve Bilgisayarların izin işlemleri için kullanılır.
  - Distribution (Dağıtım) Group: Genel olarak mail atmak için oluşturulan gruptur. (Genellikle Exchange server bulunan domainlerde kullanılır)
- Bu belirtilen 2 tip grubun altında 3 alt yapı bulunmaktadır.
  - Domain Local: Aynı domain yapısında bulunan kaynaklara erişim izin ayarları için kullanılır.
  - Global : Aynı ağ ihtiyacını taşıyan, benzer paylaşımları olan yapılarda kullanılır.
  - Universal: Birden fazla domain’e üye olan grubu aynı anda yönetimi için kullanılır.

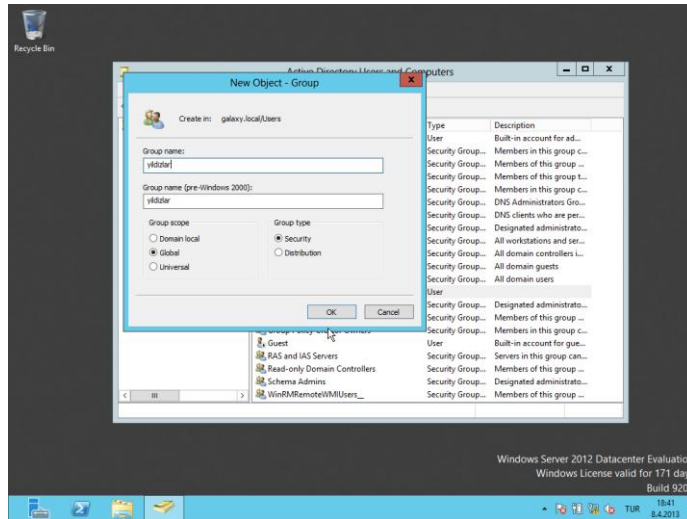
Metro UI'den Active Directory Users and Computer seçildikten sonra grubun oluşturulmak istendiği nesne üzerinde Resim 2.7'de görüldüğü üzere farenin sağ butonuna basılır.New-Group yolu izlenir.



**Resim 2.7: Active Directory Users and Computers Penceresi**

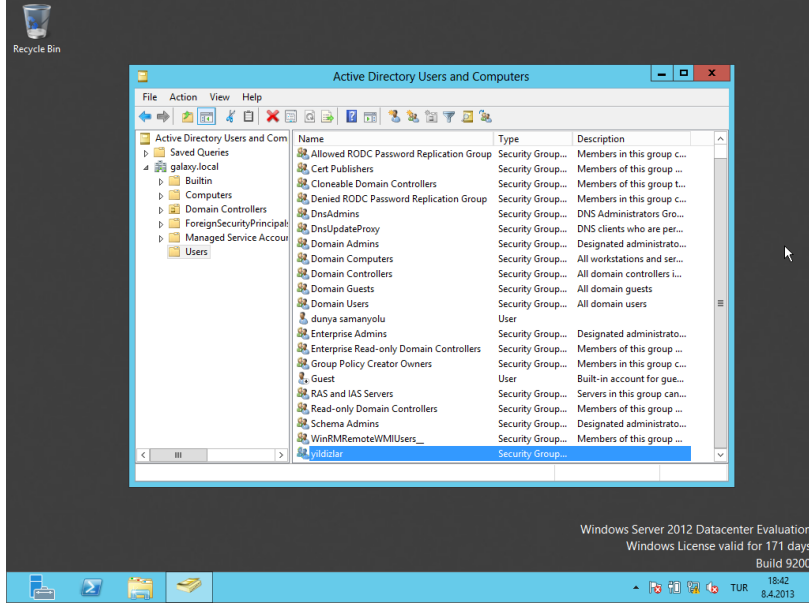
Resim 2.8'de Grup Name alanına grubun ismi yazılır. Eğer etki alanınızda Windows Server 2000 öncesi yapılar var ise Grup name (pre-Windows 2000) alanı doldurulabilir.

Group scope ve Group type alanlarında yukarıda bahsedildiği tanımlar doğrultusunda, ihtiyacı karşılayacak seçim yapılır.



**Resim 2.8: New Object-Group Penceresi**

Resim 2.9’da görüldüğü gibi grup oluşturulmuş oldu.



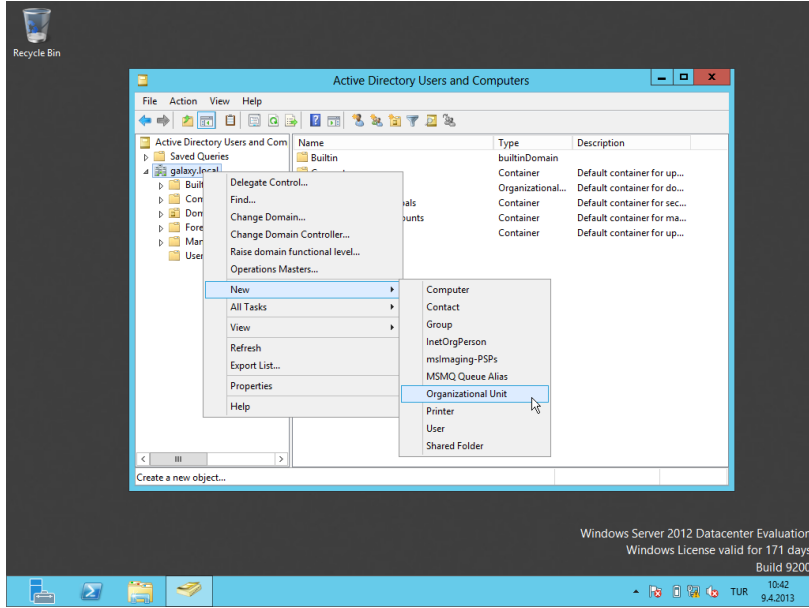
Resim 2.9: New Object-Group Penceresi

## 2.2. Active Directory ve Organizational Unit

Genel olarak Etki alanı (Active Directory) işlemlerinde kullanıcı, bilgisayar ve grupları bir amaca yönelik olarak bir araya getirmek ve kolay yönetimlerini sağlamak için Organization al Unit’ler (OU) kullanılır. Bir OU başka bir OU’ın bünyesinde olabilir. Bölgesel yapılarda yönetim için tercih edilir. Sistem yöneticileri yeni bir etki alanı oluşturmak yerine OU oluşturmayı ve yönetimi bu şekilde sağlamayı tercih ederler.

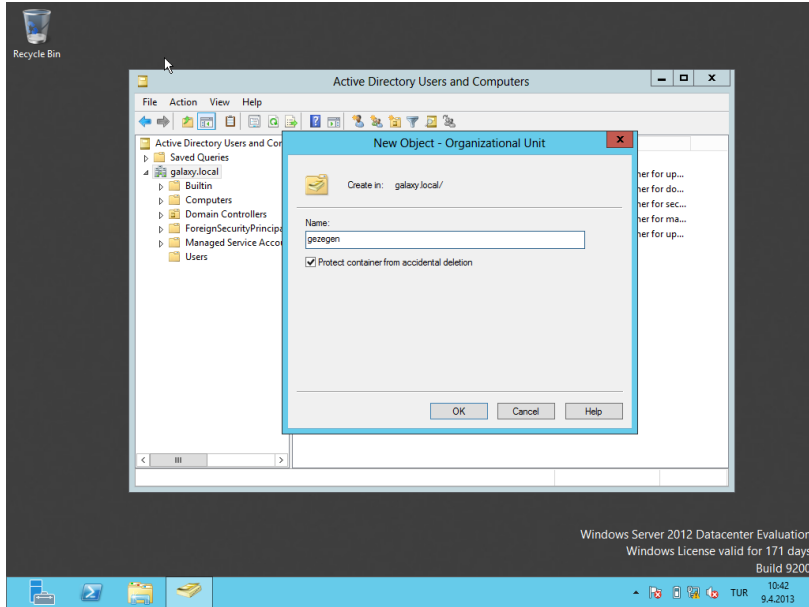
### 2.2.1. Active Directory’de Organizational Unit Oluşturma

Domain ismi üzerine Resim 2.10’de görüldüğü gibi fare ile gelinerek sağ butonuna basılır. New OU yolu izlenerek “New Object – Organizational Unit” penceresi aktifleştirilir.



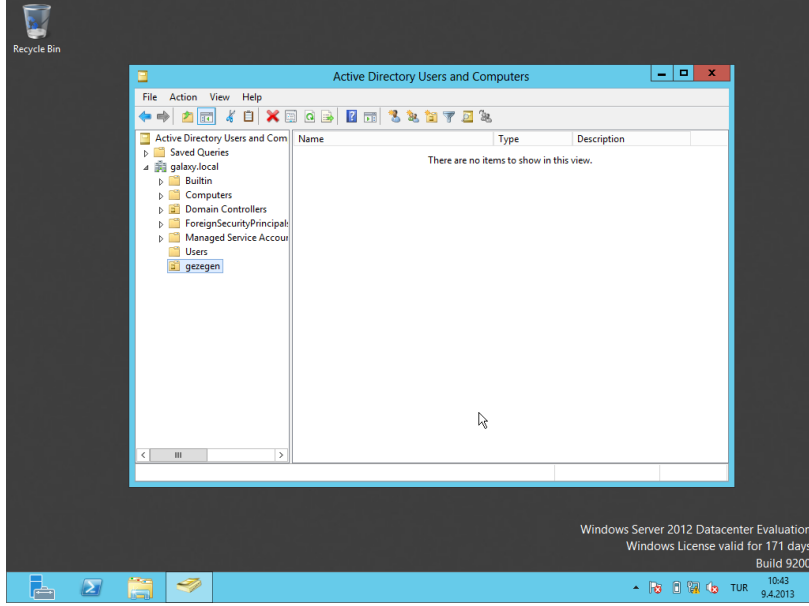
**Resim 2.10: Active Directory Users and Computers Penceresi**

Resim 2.11 penceresinde oluşturulacak OU'ya verilecek isim belirlenir.



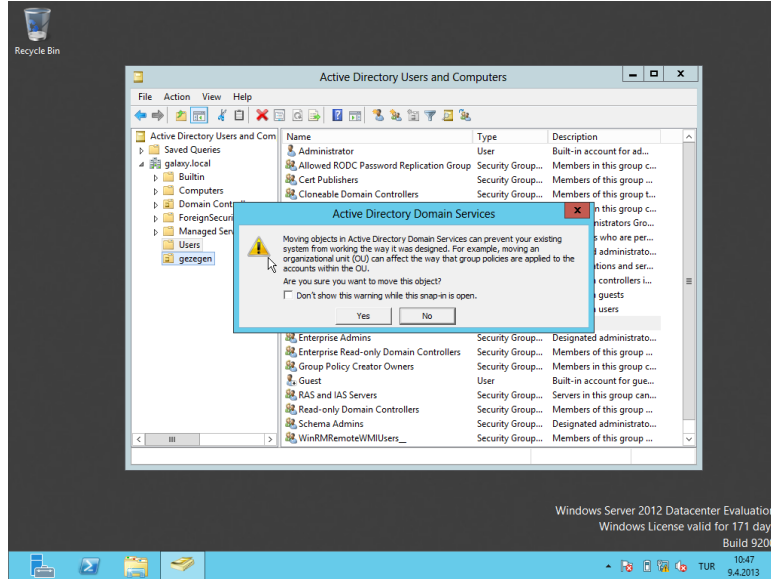
**Resim 2.11: New Object-Group Penceresi**

Resim 2.12’de görüldüğü üzere yeni OU oluşturuldu.



**Resim 2.12: Active Directory Users and Computers Penceresi**

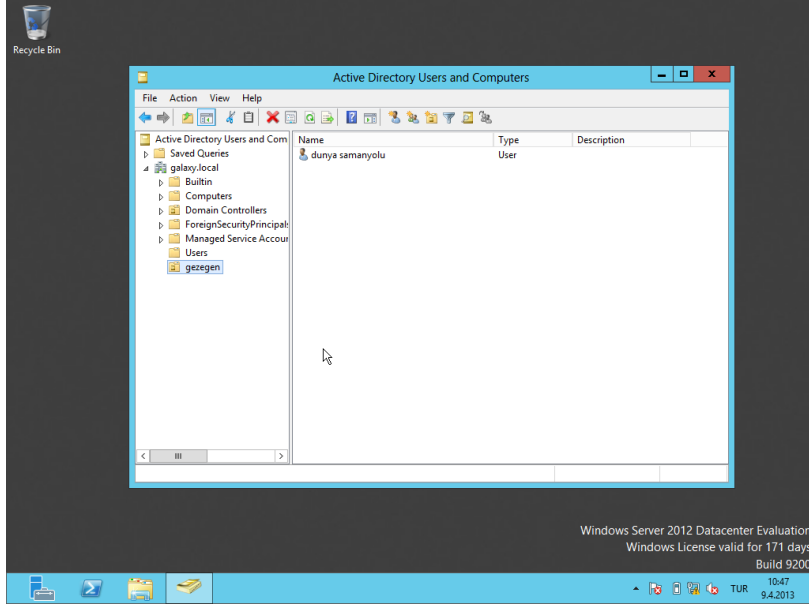
OU’ları yönetim amaçlı kullanacağımızı belirtmiştik. OU’lara yüklenen Group Policy ayarları içerilerinde bulunan Kullanıcı, Bilgisayar ve gruplara etki eder. Resim 2.13’te önceden oluşturduğumuz “dünya samanyolu” kullanıcısını “gezegen” OU’suna taşıırken karşılaşılan pencere görülmektedir. Bu pencerede eğer kullanıcı taşınır ise kullanıcının OU için hazırlanmış olan tüm yönetimsel ayarları taşıyacağı belirtiliyor.



**Resim 2.13: Active Directory Domain Services Penceresi**



Resim 2.14’te görüldüğü gibi artık kullanıcı gezegen OU’suna yönetici tarafından tanımlanmış tüm hak, kısıtlamaları taşıyacaktır.



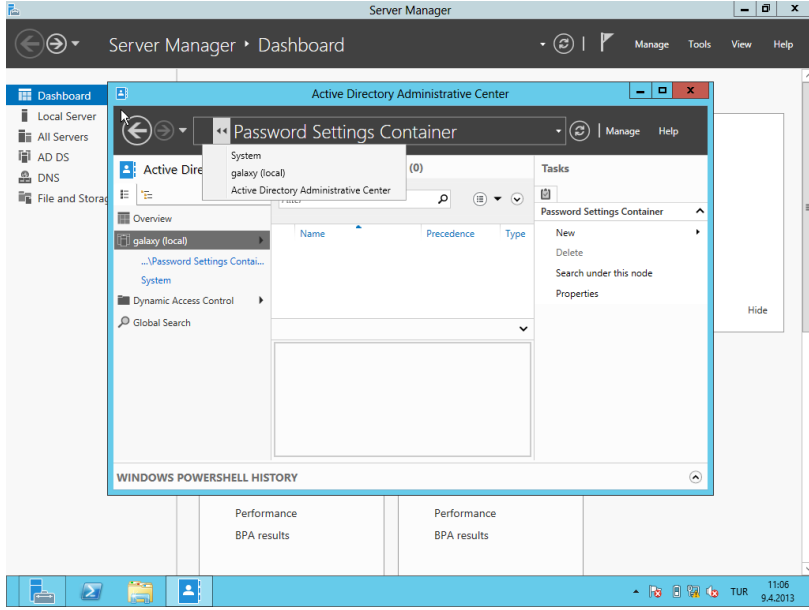
**Resim 2.14: Active Directory Users and Computers Penceresi**

## 2.3. Parola İlkesi

Parola ilkesi (Fine Grained Password Policy) istenen bir yapı içerisindeki objelerin (kullanıcı ve grup) şifrelerinin ne gibi özellikler taşıması gerektiğinin, uzunluğunun ne kadar olması gerektiğinin vb. belirlendiği ilkedir.

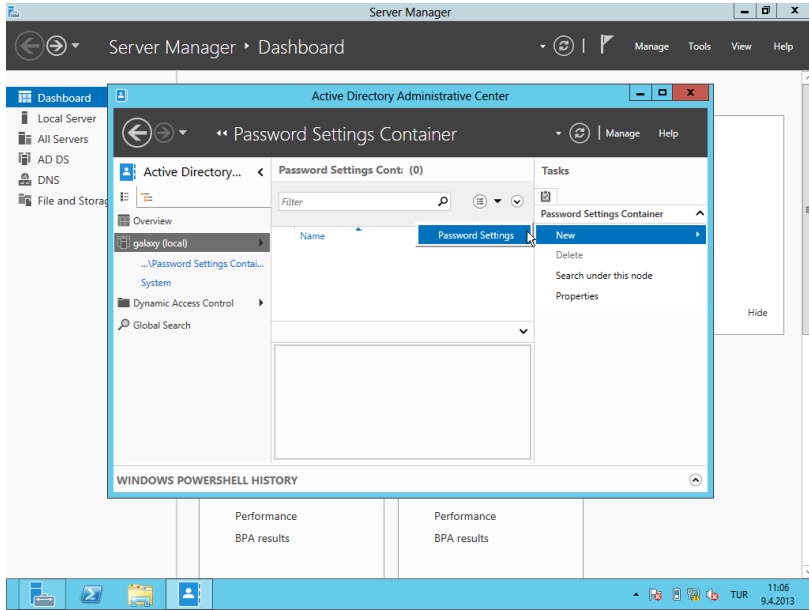
### 2.3.1. Parola İlkesi Oluşturma

Resim 2.15’te görülen yol izlenerek yeni bir parola ilkesi oluşturulmasını sağlayacak pencereye ulaşılır.



**Resim 2.15: Active Directory Administrative Center Penceresi**

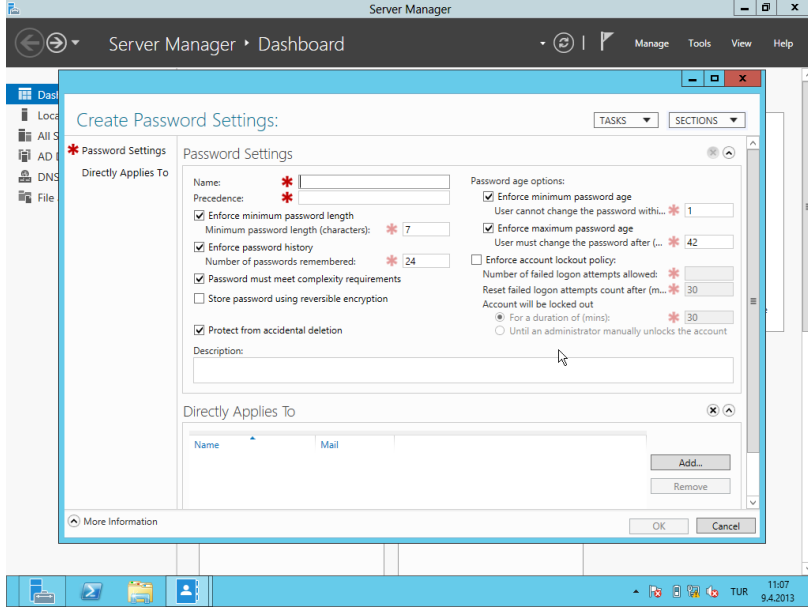
Resim 2.16’da görüldüğü üzere şifre ayarlarının belirleneceği pencere (Resim 2.17 New - Password Settings yolu izlenerek ekrana getirilir.



**Resim 2.16: Active Directory Administrative Center Penceresi**

Resim 2.17’de yeni şifre ayarları (Minumum şifre uzunluğu, kaç adet geriye dönük şifrenin hatırlanması gerektiği, kaç gün boyunca şifrenin değiştirilemeyeceği vb.)

yapıldıktan ve bu ayarların hangi kullanıcı ve/veya grup'lar tarafından kullanılacağı "Directly Applies to" alanında seçildikten sonra mutlaka Powershell'de gpupdate komutu kullanılmalıdır. Komutun işletilmesini takiben yapılan ayarlar geçerli olacaktır.



**Resim 2.17: Create Password Settings Penceresi**

## UYGULAMA FAALİYETİ

İşlem Basamakları	Öneriler
➤ Tanımlanacak kullanıcı isimlerini belirleyiniz.	➤ Kullanıcı adının etki alanı içersinde benzersiz olmasına dikkat ediniz. Şifresini karmaşık yapıda girmeyi unutmayınız.
➤ Tanımlanacak grup isimlerini belirleyiniz. ➤ Tanımlanacak bir OU ismi belirleyiniz.	➤ Oluşturacağınız grup ve OU isimlerinin benzersiz olmasına ve ihtiyaçları karşılamasına dikkat ediniz.
➤ Tanımladığınız bir kullanıcıyı OU içine taşıyınız.	➤ Taşıma işlemi fare ile yaparken dikkatli olunuz. Kullanıcının OU altında tüm haklarından yararlanmasını sağlayınız.

### KONTROL LİSTESİ

Bu faaliyet kapsamında aşağıda listelenen davranışlardan kazandığınız beceriler için **Evet**, kazanamadığınız beceriler için **Hayır** kutucuğuna (X) işareti koyarak kendinizi değerlendiriniz.

Değerlendirme Ölçütleri	Evet	Hayır
1- Active Directory yapısına yeni bir kullanıcı ekleyebildiniz mi?		
2- Active Directory yapısına yeni bir grup ekleyebildiniz mi?		
3- Active Directory yapısına yeni bir OU ekleyip, kullanıcıyı içersine taşıyabildiniz mi?		

### DEĞERLENDİRME

Değerlendirme sonunda “**Hayır**” şeklindeki cevaplarınızı bir daha gözden geçiriniz. Kendinizi yeterli görmüyorsanız öğrenme faaliyetini tekrar ediniz. Bütün cevaplarınız “**Evet**” ise “Ölçme ve Değerlendirme”ye geçiniz.

## ÖLÇME VE DEĞERLENDİRME

Bu faaliyet sonunda kazandıklarınızı aşağıdaki soruları cevaplandırarak ölçünüz.

**Aşağıdaki soruyu dikkatlice okuyarak doğru seçeneği işaretleyiniz.**

8. Aşağıdakilerden hangisi genel olarak mail atmak için oluşturulan gruptur?
- a) Security group
  - b) Distribution group
  - c) Domain local group
  - d) Global group
  - e) Universal group

**Aşağıdaki cümleleri dikkatlice okuyarak boş bırakılan yerlere doğru sözcüğü yazınız.**

9. Aynı ağ ihtiyacını taşıyan, benzer paylaşımları olan yapılarda ..... grup kullanılır.
10. Aynı domain yapısında bulunan kaynaklara erişim izin ayarları için ..... grubu kullanılır.
11. Eski (Windows Server 2000 öncesi) sistemlere giriş için kullanılan oturum açma adı .....olarak adlandırılır.

**Aşağıdaki soruyu dikkatlice okuyarak doğru seçeneği işaretleyiniz.**

12. Hesap yönetiminde en yaygın kullanılan görevlere örnek hangisi verilebilir?
- a) Active Directory’de kullanıcı hesabı oluşturma
  - b) Active Directory’de grup hesabı oluşturma
  - c) Lokalde kullanıcı hesabı oluşturma
  - d) Local’de grup hesabı oluşturma
  - e) Hepsi

## DEĞERLENDİRME

Değerlendirme sonunda “Hayır” şeklindeki cevaplarınızı bir daha gözden geçiriniz. Kendinizi yeterli görmüyorsanız öğrenme faaliyetini tekrar ediniz. Bütün cevaplarınız “Evet” ise bir sonraki öğrenme faaliyetine geçiniz.

# ÖĞRENME FAALİYETİ-3

## AMAÇ

Active Directory’de gelişmiş kullanıcı işlemlerini yapabileceksiniz.

## ARAŞTIRMA

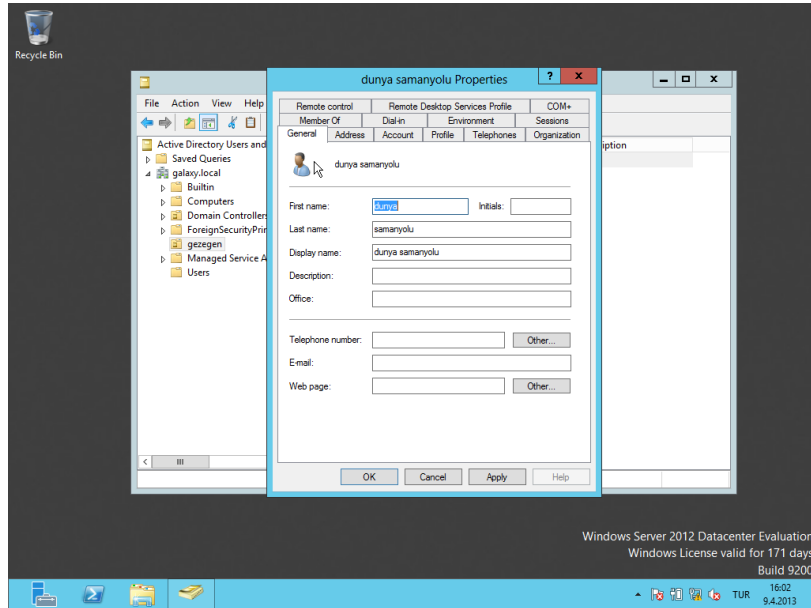
- Active Directory’de gelişmiş kullanıcı işlemlerini araştırınız. Topladığınız bilgileri rapor hâline getiriniz. Topladığınız bilgileri rapor hâline getiriniz. Hazırladığınız raporunuzu sınıfta sununuz.

## 3. GELİŞMİŞ HESAP YÖNETİMİ

### 3.1. Kullanıcı Hesabı

#### 3.1.1. General Tabı

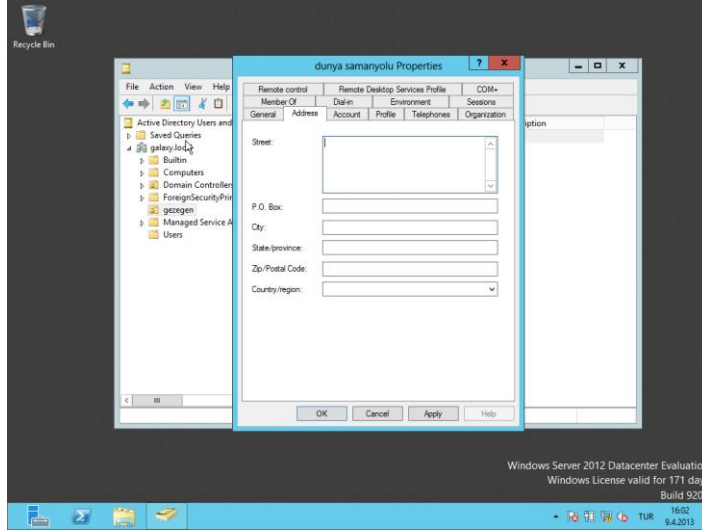
Ad, Soyad, e-posta vb. genel kullanıcı bilgilerinin belirtildiği penceredir.



Resim 3.1: Kullanıcı özellikleri penceresi General Tabı

### 3.1.2. Address Tabı

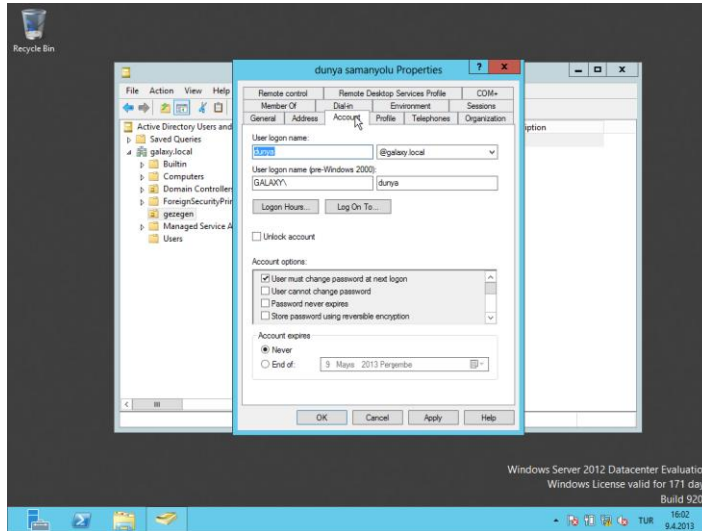
Sokak, Şehir, Ülke vb. bilgilerin bulunduğu penceredir.



Resim 3.2: Kullanıcı özellikleri penceresi Address Tabı

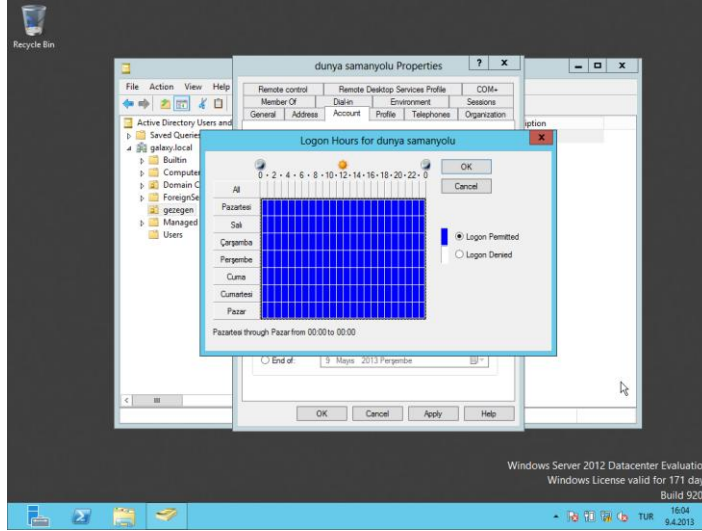
### 3.1.3. Account Tabı

- Kullanıcı hesabı ile ilgili bilgiler içerir.



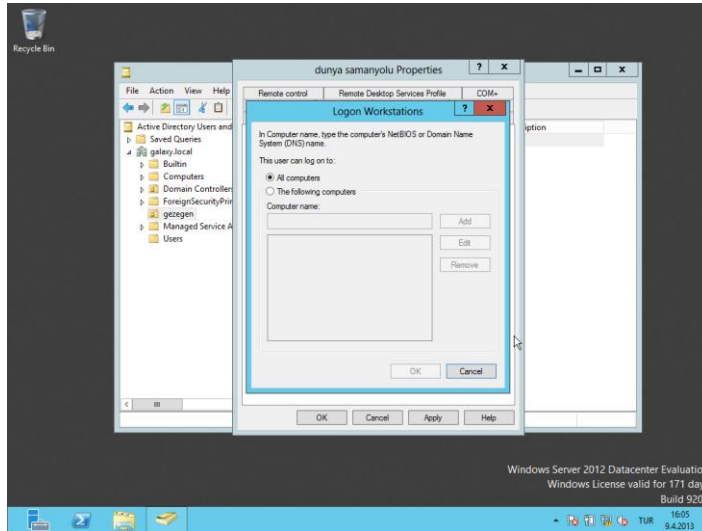
Resim 3.3: Kullanıcı özellikleri penceresi Account Tabı

- User logon name : Kullanıcının oturum açacağı isim burada bulunur.
- User logon name (pre-Windows 2000): WS 2000 öncesi işletim sistemlerindeki oturum açma ismi burada bulunur.
- Logon Hours : Bu hesabın hangi saatler arasında aktif olacağını belirttiği alandır.



**Resim 3.4 : Logon Hours Penceresi**

- Log On To: Bu hesabın hangi bilgisayarlar ile oturum açabileceği burada belirlenir.



**Resim 3.5: Logon Workstations Penceresi**

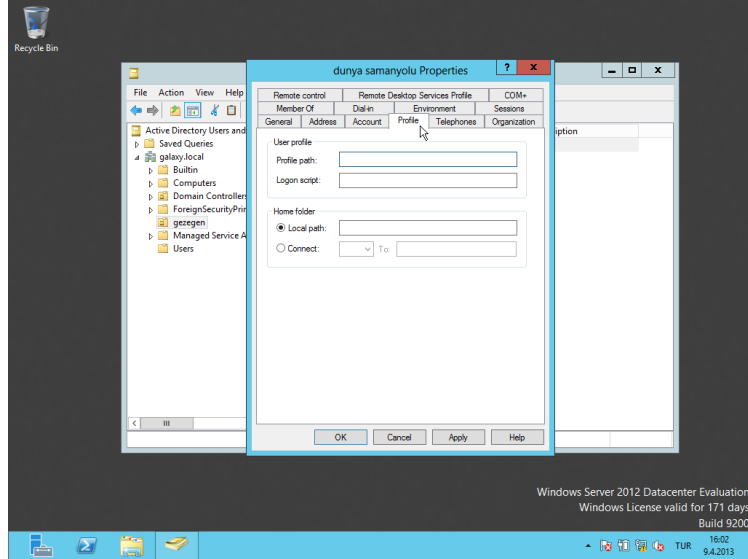
- Unlock account: Kilitlemiş hesabı aktif hâle getirmek için kullanılır.



- Account options alanı: Bu alanda en çok kullanılan özellikler aşağıdadır.
- User must change password at next logon: Kullanıcının hesaba oturum açtığı anda şifresini değiştirmesi gerektiğinin belirtildiği alandır.
  - User cannot change password: Bu seçenek işaretlenir ise kullanıcı asla şifresini değiştiremez.
  - Password never expires: Bu seçenek seçilir ise atanan şifrenin değiştirilmesi gerektiğine dair kullanıcı bir uyarı almaz.
  - Store password using reversible encryption: Kullanıcı şifresinin bir algoritma ile şifrelenerek saklanması sağlanır.
  - Account is disabled: Hesabı pasif hâle getirmek için seçilmesi gereken alandır.
  - Account expires: Hesabın ne zaman pasif durumu alınması gerektiğinin belirtildiği alandır. Örneğin stajyerlerin hesaplarının sistemde kaldırılma tarihleri belli olacağından tercih edilir.

### 3.1.4. Profile Tabı

- Kullanıcı dosyalarının bulunduğu alan ile alakalı alandır.



**Resim 3.6: Kullanıcı özellikleri penceresi Profile Tabı**

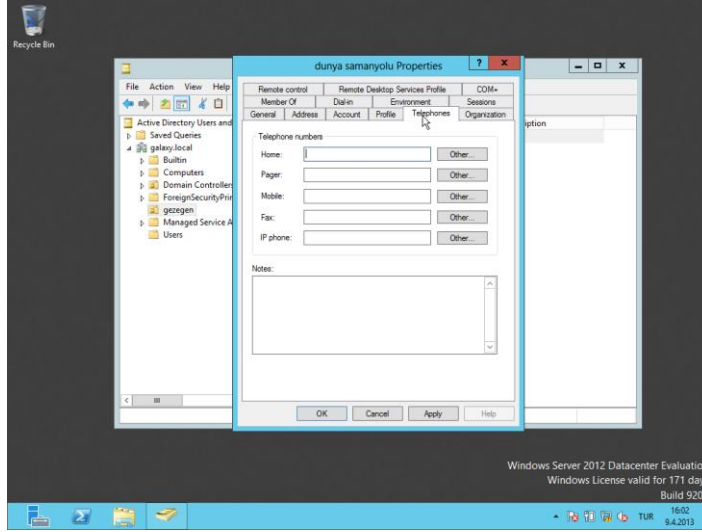
- Roaming Profile: Kullanıcının kendi oturum açma adı ile etki alanındaki tüm bilgisayarlarda oturum açabilmesi ve her oturumda aynı dosyalarına ulaşabilmesi için geliştirilmiş profile verilen addır.
  - Gezici profil yapmak için öncelikle sunucu üzerinde bir klasör oluşturulur.
  - Bu kalsör paylaşımına açılarak gezici profil olacak kullanıcı adının bu klasör üzerinde tam yetkiye sahip olması sağlanır.
  - Profile Path alanına \\serveradi\paylasimadi\%username% yazılır.

Bu işlemler sonucunda gezici profil oluşturulmuş olur. Test etmek için gezici profil adı ile bir sefer oturum açılır ve sunucu üzerinde oluşturulan klasör içinde oturum adı açılan kullanıcı dosyaları görülür ise işlemin doğruluğu kanıtlanmış olur.

- Mandatory Profile: Mandatory profile’de roaming gibi farklı bilgisayarlarda oturum açmak isteyen kullanıcılar için kullanılan bir yöntemdir. Roaming’den farkı kullanıcının her oturum açtığında aynı dosyaları görmesi, üzerlerinde değişiklik yapsa da oturumu kapadığında bu değişikliklerin silinmesidir. Mandatory Profile yapmak için; sunucu içerisinde Roaming profile olarak oluşturulan kullanıcı adı ile aynı isimde olan klasör içerisinde yer alan NTUSER.DAT dosyasının adı NTUSER.MAN yapılır.
- Logon Script: Kullanıcı oturum açtığı zaman bir dosya yada script çalıştırılmak isteniyor ise kullanılır.
- Home Folder: Kullanıcı dosyalarının belirlenen bir alanda tutulması için kullanılır. Connect kısmında Home Folder uygulaması yapılan sunucuya diğer bilgisayarlar tarafından kolaylıkla ulaşılabilmesi için kullanılır.

### 3.1.5. Telephones Tabı

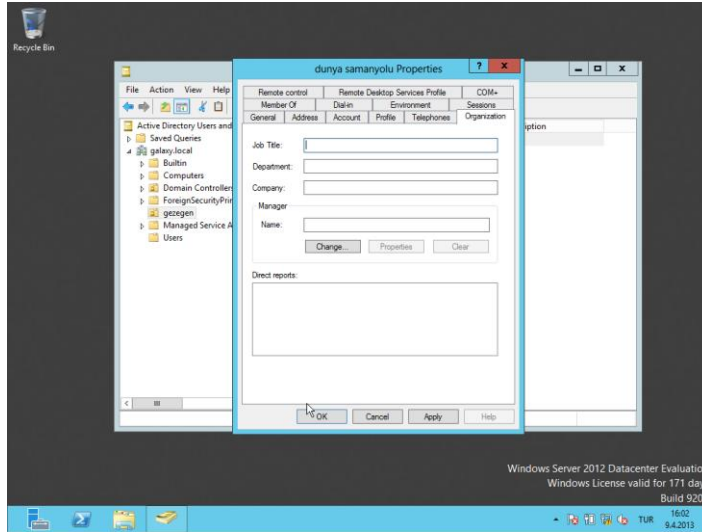
Kullanıcı telefon bilgilerinin yer aldığı alandır.



Resim 3.7: Kullanıcı özellikleri penceresi Telephones Tabı

### 3.1.6. Organization Tabı

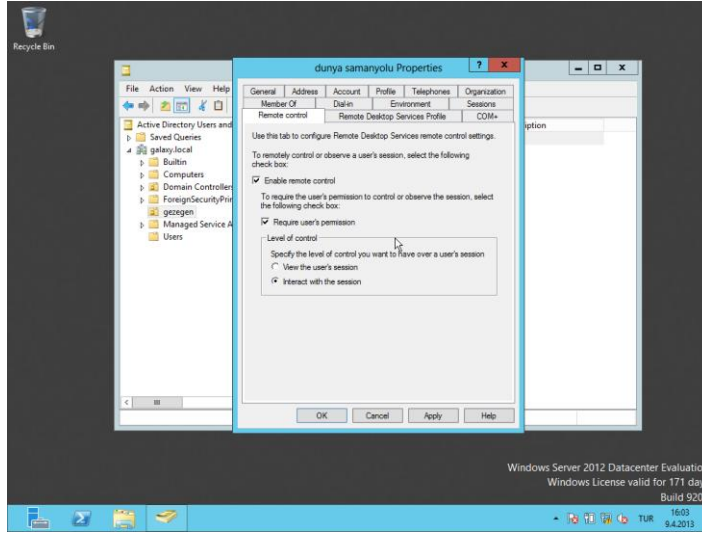
Kullanıcı iş bilgilerinin yer aldığı alandır.



Resim 3.8: Kullanıcı özellikleri penceresi Organization Tabı

### 3.1.7. Remote Control Tabı

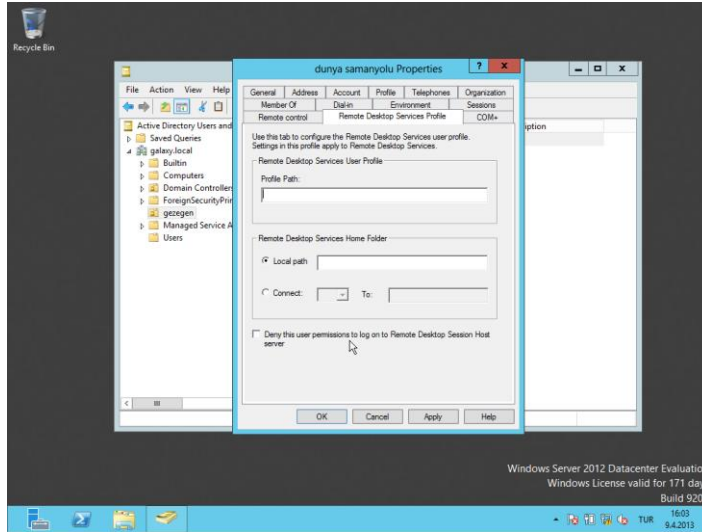
Kullanıcı profilinin uzaktan erişim ile ilgili ayarlarının yapıldığı alandır.



Resim 3.9: Kullanıcı özellikleri penceresi Remote Control Tabı

### 3.1.8. Remote Desktop Services Profile Tabı

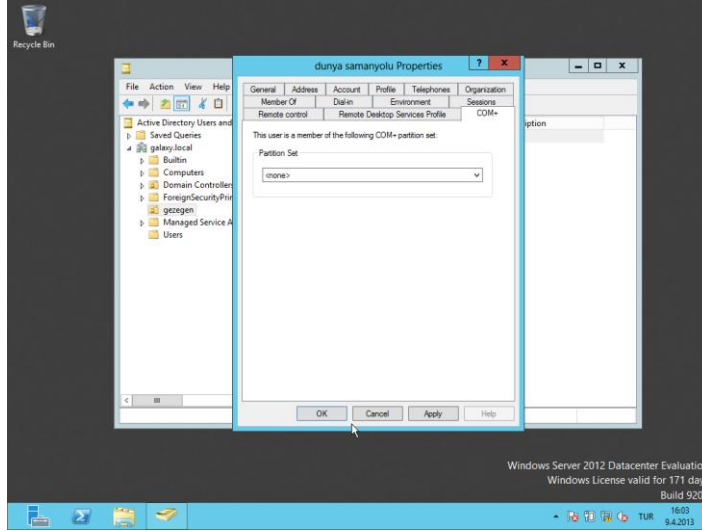
Kullanıcının masaüstüne uzaktan erişimle ilgili ayarlarının yapıldığı alandır.



Resim 3.10: Kullanıcı özellikleri penceresi Remote Control Services Profile Tabı

### 3.1.9. COM+ Tabı

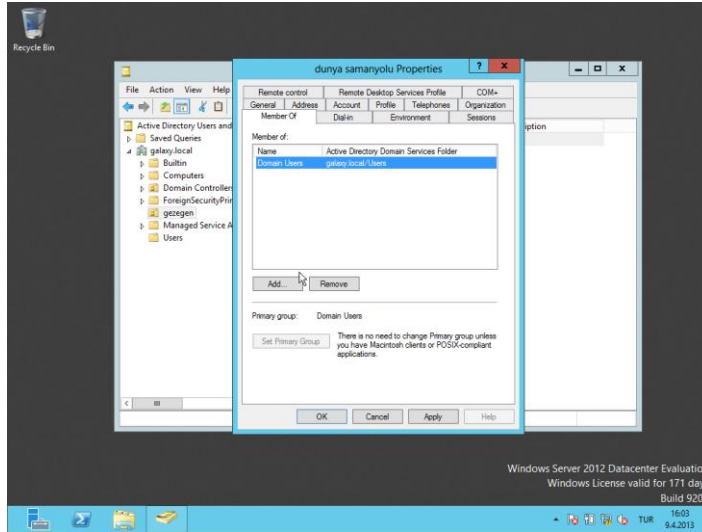
Eğer kullanıcı Com+ alanının üyesi ise bu üyelik ayarlarının yapıldığı alandır.



Resim 3.11: Kullanıcı özellikleri penceresi COM+ Tabı

### 3.1.10. Member Of Tabı

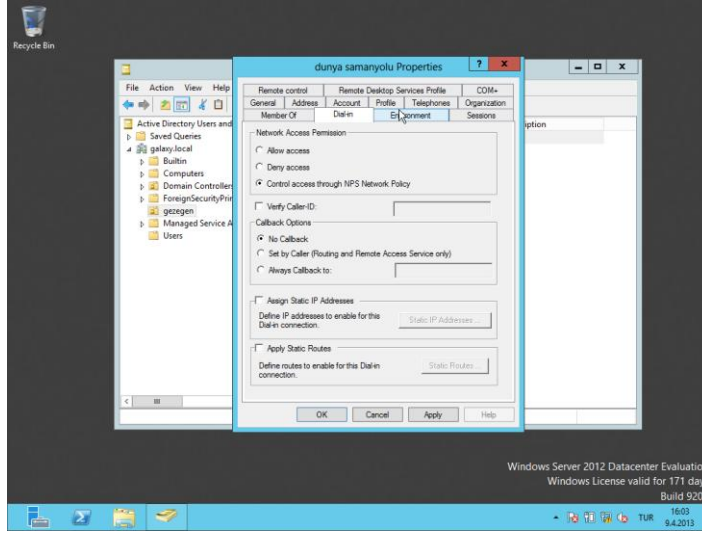
Kullanıcının üyelik ayarlarının yapıldığı alandır.



Resim 3.12 : Kullanıcı özellikleri penceresi Member Of Tabı

### 3.1.11. Dial-in Tabı

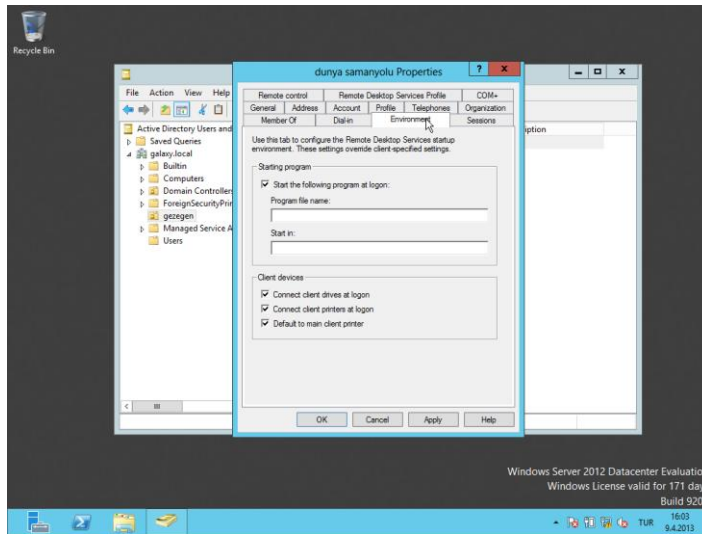
Kullanıcı hesabının dial-up bağlantı ile sunucu üzerinde oturum açması işlemleri ile ilgili işlemlerin yapıldığı alandır.



Resim 3.13: Kullanıcı özellikleri penceresi Dial-in Tabı

### 3.1.12. Environment Tabı

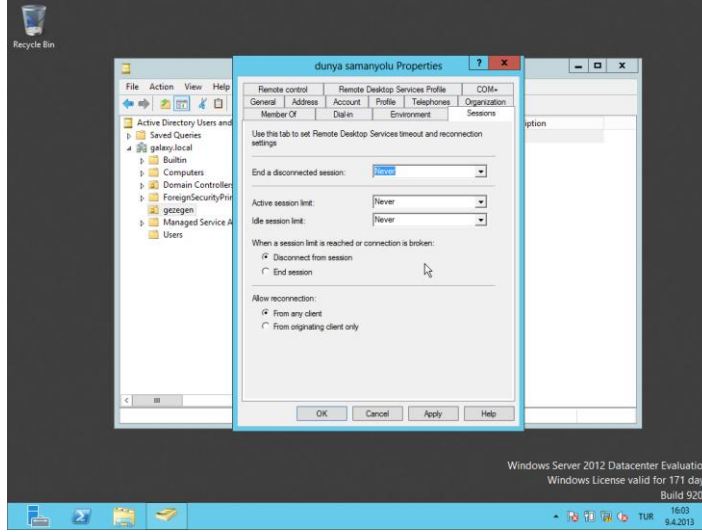
Kullanıcı oturum açtığı anda bir program çalıştırılmak isteniyorsa kullanılan alandır.



Resim 3.14: Kullanıcı özellikleri penceresi Environment Tabı

### 3.1.13. Sessions Tabı

Kullanıcının oturum işlemlerinin yapıldığı alandır.



**Resim 3.15: Kullanıcı özellikleri penceresi Sessions Tabı**

## UYGULAMA FAALİYETİ

İşlem Basamakları	Öneriler
➤ Yeni bir kullanıcı oluşturunuz.	➤ Kullanıcı hesabı oluştururken şifreyi ilk girişte değiştirmesi seçeneğini seçmeyi unutmayınız.
➤ Oluşturduğunuz kullanıcının oturum açabileceği saatleri hafta içi 08:00-17:00 olarak ayarlayınız.	➤ Fare ile ayarlama yaparken dikkat ediniz.
➤ Kullanıcının roaming profil'e sahip olmasını sağlayınız.	➤ Mandatory ve Roaming profilleri karıştırmamak için dikkatli olunuz.
➤ Kullanıcının takip eden ilk oturum açışında herhangi bir programın istemci bilgisayara otomatik olarak yüklenmesini sağlayınız.	➤ Yükleyeceğiniz program uzantısının *.msc olmasına dikkat ediniz.

## KONTROL LİSTESİ

Bu faaliyet kapsamında aşağıda listelenen davranışlardan kazandığınız beceriler için **Evet**, kazanamadığınız beceriler için **Hayır** kutucuğuna (X) işareti koyarak kendinizi değerlendiriniz.

Değerlendirme Ölçütleri	Evet	Hayır
1- Active Directory yapısına yeni bir kullanıcı ekleyebildiniz mi?		
2- Kullanıcının oturum açma saatlerini ayarlayabildiniz mi?		
3- Roaming profil işlemini başarılı bir resimde yapabildiniz mi?		
4- Oturum açma işlemini takiben istemci bilgisayara program kurulumu yapabildiniz mi?	5-	

## DEĞERLENDİRME

Değerlendirme sonunda “**Hayır**” şeklindeki cevaplarınızı bir daha gözden geçiriniz. Kendinizi yeterli görmüyorsanız öğrenme faaliyetini tekrar ediniz. Bütün cevaplarınız “**Evet**” ise “Ölçme ve Değerlendirme”ye geçiniz.



## ÖLÇME VE DEĞERLENDİRME

Bu faaliyet sonunda kazandıklarınızı aşağıdaki soruları cevaplandırarak ölçünüz.

**Aşağıdaki soruları dikkatlice okuyarak doğru seçeneği işaretleyiniz.**

1. Aşağıdakilerden hangisi kullanıcı özellikleri altında yer alan General sekmesinde yer almaz?
  - a) First name
  - b) Last name
  - c) Surname
  - d) Description
  - e) Telephone Number
2. Kullanıcının oturum açabileceği saatlerin ve hangi bilgisayarlarda oturum açabileceğinin ayarlandığı sekme (tab) hangisidir?
  - a) General
  - b) Address
  - c) Account
  - d) Profil
  - e) COM+
3. Roaming profilinde yapılabildiği sekme hangisidir?
  - a) General
  - b) Address
  - c) Account
  - d) Profil
  - e) COM+
4. Oturum açılmasını takiben kullanıcının bilgisayarında bir program çalıştırılmak isteniyor ise bu işlem hangi sekmeden yapılabilir?
  - a) Dial-in
  - b) Environment
  - c) Account
  - d) Profil
  - e) Sessions

## DEĞERLENDİRME

Cevaplarınızı cevap anahtarıyla karşılaştırınız. Yanlış cevap verdiğiniz ya da cevap verirken tereddüt ettiğiniz sorularla ilgili konuları faaliyete geri dönerek tekrarlayınız. Cevaplarınızın tümü doğru ise “Modül Değerlendirme”ye geçiniz.

# MODÜL DEĞERLENDİRME

Bu faaliyet sonunda kazandıklarınızı aşağıdaki soruları cevaplandırarak ölçünüz.

**Aşağıdaki soruları dikkatlice okuyarak doğru seçeneği işaretleyiniz.**

1. Sunucu üzerine Active Directory nasıl kurulabilir?
  - a) Sunucu Yönetimi Penceresinden
  - b) Manage seçeneği altından
  - c) Powershell üzerinden ADDSDeployment komutları ile
  - d) Server Manager Penceresinden
  - e) Hepsi
2. Active Directory kurulum işleminde yöneticinin yapması gereken ilk adım nedir?
  - a) Sunucuya Statik ip vermek
  - b) Sunucuya dinamik ip vermek
  - c) Add roles and features linkine basmak
  - d) Role Based linkine basmak
  - e) Hiçbiri
3. Select server roles penceresinde Active Directory kurulumu yapmak için hangi seçenek aktifleştirilir?
  - a) Active Directory Certificate Services
  - b) Active Directory Domain Services
  - c) Active Directory Federation Services
  - d) DNS Server
  - e) Hyper-V
4. Active Directory ormanda ilk defa kurulacak ise Deployment Configuration penceresinden hangi seçenek seçilmelidir?
  - a) Add a domain controller to an existing domain
  - b) Add a new domain to an existing forest
  - c) Add a new forest
  - d) Add a new domain controller to an existing forest
  - e) Add a new forest to an existing forest
5. Hazır bulunan etki alanına, etki alanı yöneticisi kurulacak ise Deployment Configuration penceresinden hangi seçenek seçilmelidir?
  - a) Add a domain controller to an existing domain
  - b) Add a new domain to an existing forest
  - c) Add a new forest
  - d) Add a new domain controller to an existing forest
  - e) Add a new forest to an existing forest

6. Aşağıdakilerden hangisi Windows Server 2012'in desteklediği Forest functional level'lerinden biri değildir?
- a) Windows Server 2012
  - b) Windows Server 2003
  - c) Windows Server 2008
  - d) Windows Server 2008 R2
  - e) Windows Server 2003 R2
7. Aşağıdakilerden hangisi Windows Server 2012 üzerinde ön tanımlı olarak gelen veritabanı saklanan klasördür?
- a) C:\Windows\NTDS
  - b) C:\Program Files\NTDS
  - c) C:\Program Files (x86)\NTDS
  - d) C:\Windows\SYVOL
  - e) C:\Program Files\SYVOL
8. Aşağıdakilerden hangisi genel olarak mail atmak için oluşturulan gruptur?
- a) Security group
  - b) Distribution group
  - c) Domain local group
  - d) Global group
  - e) Universal group

**Aşağıdaki cümleleri dikkatlice okuyarak boş bırakılan yerlere doğru sözcüğü yazınız.**

9. Aynı ağ ihtiyacını taşıyan, benzer paylaşımları olan yapılarda ..... grup kullanılır.
10. Aynı domain yapısında bulunan kaynaklara erişim izin ayarları için ..... grubu kullanılır.
11. Eski (Windows Server 2000 öncesi) sistemlere giriş için kullanılan oturum açma adı .....olarak adlandırılır.

**Aşağıdaki soruları dikkatlice okuyarak doğru seçeneği işaretleyiniz.**

12. Hesap yönetiminde en yaygın kullanılan görevlere örnek hangisi verilebilir?
- a) Active Directory'de kullanıcı hesabı oluşturma
  - b) Active Directory'de grup hesabı oluşturma
  - c) Lokalde kullanıcı hesabı oluşturma
  - d) Local'de grup hesabı oluşturma
  - e) Hepsi

13. Aşağıdakilerden hangisi kullanıcı özellikleri altında yer alan General sekmesinde yer almaz?
- a) First name
  - b) Last name
  - c) Surname
  - d) Description
  - e) Telephone Number
14. Kullanıcının oturum açabileceği saatlerin ve hangi bilgisayarlarda oturum açabileceğinin ayarlandığı sekme (tab) hangisidir?
- a) General
  - b) Address
  - c) Account
  - d) Profil
  - e) COM+
15. Roaming profilinde yapılabildiği sekme hangisidir?
- a) General
  - b) Address
  - c) Account
  - d) Profil
  - e) COM+
16. Oturum açılmasını takiben kullanıcının bilgisayarında bir program çalıştırılmak isteniyor ise bu işlem hangi sekmeden yapılabilir?
- a) Dial-in
  - b) Environment
  - c) Account
  - d) Profil
  - e) Sessions

# CEVAP ANAHTARLARI

## ÖĞRENME FAALİYETİ-1 CEVAP ANAHTARI

1	E
2	A
3	B
4	C
5	A
6	E
7	A

## ÖĞRENME FAALİYETİ-2 CEVAP ANAHTARI

8	B
9	GLOBAL
10	DOMAIN LOCAL
11	NEYBIOS
12	E

## ÖĞRENME FAALİYETİ-3 CEVAP ANAHTARI

13	C
14	C
15	D
16	B

## MODÜL DEĞERLENDİRME CEVAP ANAHTARI

1	E
2	A
3	B
4	C
5	A
6	E
7	A
8	B
9	GLOBAL
10	DOMAIN LOCAL
11	NEYBIOS
12	E
13	C
14	C
15	D
16	B

## KAYNAKLAR

- GÜR Murat, M. İbrahim KANTAR, Volkan ŞAYF, Ali YÜKSEL, **Windows Server 2012**, 1.Baskı, Kodlab Yayıncılık, İstanbul, Mart, 2013.
- İNAN Yüksel, Nihat DEMİRLİ, **Sistem Mühendisliği Windows Server 2003 ve Windows Xp**, 4.Baskı, Palme Yayıncılık, Ankara, 2006.
- MESEP- Bilişim Teknolojileri alanı **Sunucu İşletim Sistemi 1 Modülü**. Ankara. 2008.
- MESEP- Bilişim Teknolojileri alanı **Sunucu İşletim Sistemi 2 Modülü**. Ankara. 2008.
- MESEP- Bilişim Teknolojileri alanı **Sunucu İşletim Sistemi 3 Modülü**. Ankara. 2011.
- MESEP- Bilişim Teknolojileri alanı. **Sunucu İşletim Sistemi 4 Modülü**. Ankara. 2011.
- MESEP- Bilişim Teknolojileri alanı **Sunucu İşletim Sistemi 5 Modülü**. Ankara. 2011.
- MESEP- Bilişim Teknolojileri alanı. **Sunucu İşletim Sistemi 6 Modülü**. Ankara. 2011.
- YILDIRIMOĞLU Murat, **Windows Server 2008 R2**, 1.Baskı, Pusula Yayıncılık, İstanbul, Mart, 2010.