Sunucu İşletim Sistemleri

-5-

Birden fazla bilgisayarı, kullanıcıları, paylaştırılmış ağ kaynakları olan büyük şirketlerin bu kaynakları daha verimli ve güvenli kullanabilmesi için işletim sistemleri içerisinde karmaşık yönetim yapılarına veya protokollerine ihtiyaç duyulmaktadır.

Windows sunucu işlerim sistemleri için ağ kaynaklarını verimli bir şekilde yönetebilmek için Active Directory yönetimsel yapısından faydalanılır.

Active Directory; kullanıcı hesaplarını, grupları, yazıcıları ve diğer birçok ağ kaynaklarını, merkezî olarak yöneten ve denetleyen; izinlerini belirleyen, kaynaklarla ilgili verileri tutan karmaşık ve güvenli bir yapıdır.

Active Directory, Microsoft tarafından özellikle Windows Server ve Client bilgisayar sistemleri için tasarlanmış olan içerisinde sunucu, client bilgisayar, kullanıcı ve yazıcı gibi bilgileri tutan bir dizin servisidir. Bahsi geçen verileri tuttuğu için bir veri tabanının aynısıdır. Bu servis içerisinde yer alan Group Policy yönetim aracı ile çeşitli kısıtlamalar yapabilir veya tek bir noktadan istediğimiz uygulamanın dağıtımını gerçekleştirebiliriz. Kaynakların kontrolü ve yönetiminin merkezileştirilmesi açısından büyük kolaylık sağladığı için çok tercih edilen bir servistir.

Active Directory ilk olarak Windows Server 2000 ile hayatımıza girdi. Zamanla 2003, 2008 ve 2012 sistemlerinde kendini geliştirerek günümüzdeki halini almıştır.

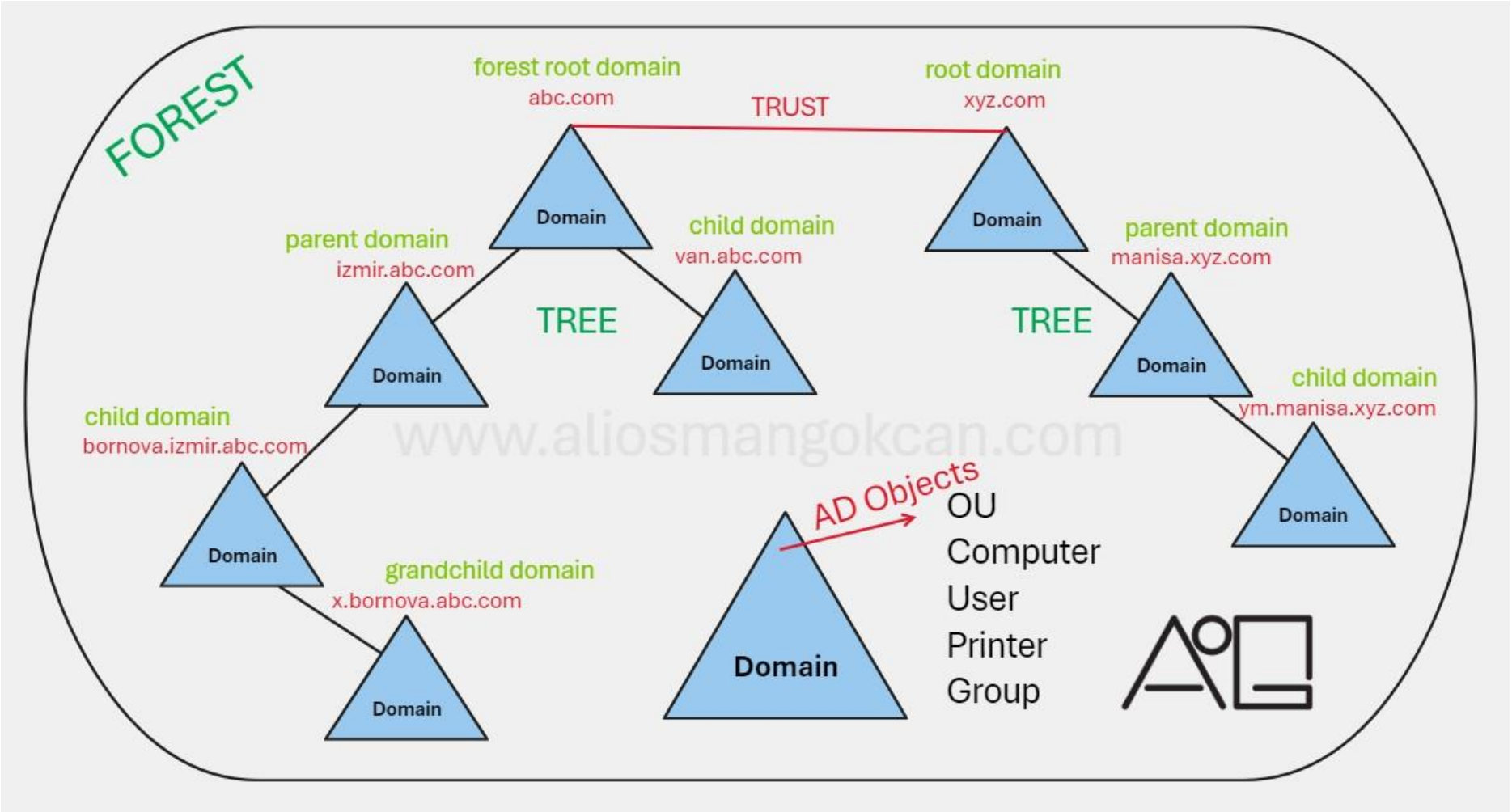
Active Directory Özellikleri;

1. Yönetilebilirlik
2. Ölçeklenebilirlik
3. Genişletilebilirlik
4. Güvenlik entegrasyonu
5. Diğer dizin servisleriyle birlikte çalışabilme
6. Güvenli kimlik doğrulama ve yetkilendirme
7. Group Policy ile yönetim
8. Dns ve Dhcp gibi servislerle birlikte çalışabilme özelliği

Domain: Active Directory'nin en temel bileşenidir. Domain sistem yöneticisi tarafından benzersiz bir isim seçilerek oluşturulmalıdır. Ayrıca Domain'ler güvenlik noktasında belli sınırlara sahiptir. Eğer sistem yöneticisi ayrıca bir izin belirlememişse, bir kullanıcının hakları sadece o Domain içerisinde geçerli olacaktır. Her bir Domain kendi güvenlik yapısına sahiptir.

Domain'ler ayrıca replikasyon birimi olarak adlandırılır. Bir Domain içerisinde, Active Directory veri tabanı kopyalarını bulunduran Domain Controller'lar bu kopyaları Domain içerisinde yapılan değişiklikleri birbirlerine kopyalayarak replikasyon yaparlar.

Active Directory Mantıksal Yapısı



Tree ve Forest

Oluşturulan ilk Windows Server Domain'i, Active Directory yapısındaki Kök Domain'i (Root Domain) ifade eder. Bundan sonra oluşturulacak olan yeni ek Domain'ler dizinin mantıksal Tree veya Forest yapısını oluşturacaktır.

Tree: Bir Tree yapısında yeni bir Domain eklendiği zaman, yeni eklenen Domain sondan eklendiği Domain'inin Child Domain'i durumunda olur ve eklendiği Domain de eklenen Domain için Parent Domain olur. Yeni oluşturulan Child Domain'in ismi Parent Domain'den gelen isimle birleştirilir ve yeni oluşan Domain'in DNS ismi ortaya çıkar.

Örneğin "cbu.edu.tr" bir Root Domain'dir. Bu Domain'e eklenecek yeni bir Domain "cbu.edu.tr" Domain'inin Child Domain'i olacaktır. Buna örnek olarak "turgutlumyo.cbu.edu.tr" Domain'ini gösterebiliriz. Bu örnekte turgutlumyo.cbu.edu.tr, cbu.edu.tr Domain'inin Child Domain'i olacaktır. cbu.edu.tr Domain'i ise Parent Domain konumundadır.

Forest: Forest, birden fazla Tree'nin birleşmiş halidir. Oluşturulan ilk Domain bir Tree'yi ifade eder ve ilk Tree'nin oluşturulmasıyla Forest'da oluşmuş olur. Sonradan bu Forest'a eklenecek olan Tree'ler, diğer Tree'lerle aynı isim aralığını paylaşmayacak olasalar da aynı Schema ve Global Catalog'a sahip olurlar. Forest oluşturulurken kurulmuş olan ilk Tree Forest-Root olarak bilinir ve diğer Tree'ler bu Forest Root altında toplanırlar.

Global Catalog (GC)

Global Catalog (GC), Active Directory Forest' ı içinde yer alan her objeyi bulunduran bir veritabanıdır ve Global Catalog Server' larda tutulur. Bu barındırılan özellikler, varsayılan olarak, sorgulamalar esnasında en sık kullanılan özelliklerdir. Global Catalog kullanıcılara şu hizmetleri sunar;

- ✓ Gereken verinin nerede olduğundan bağımsız olarak Active Directory objeleri hakkında bilgiler sunar.
- ✓ Bir ağa logon olunurken Universal Group Membership bilgisini kullanır.

Global Catalog Sunucusu Domain'deki bir Domain Controller'dır ve Domain'de oluşturulan ilk Domain Controller otomatik olarak Global Catalog seviyesine yükseltilir. Sonradan ek Global Catalog Sunucular eklenebilir.

Active Directory Schema

Kullanıcı, grup, bilgisayar ve yazıcılar gibi bütün objelere ait bilgileri içerir. Forest içerisinde, sadece bir Schema bulunur ve bütün obje bilgileri bu Schema üzerine yazılır. Kullanıcıların çalıştıkları bölümler ve doğum yeri gibi bilgileri buna örnek olarak verebiliriz. Schema bilgileri, Active Directory veritabanı (database) içerisinde depolanır.

- ✓ Kullanıcı uygulamaları için dinamik bir yapı sunar. Kullanıcıların obje araştırma işlemleri, Schema üzerinden gerçekleşir.
- ✓ Yeni oluşturulan veya değiştirilen obje dinamik olarak Schema içerisinde güncellenir.

- ✓ Obje sınıf ve niteliklerinin korunmasında, discretionary access control lists(DACLs) kullanılır.
- ✓ DACLs ile Schema üzerinde yalnızca yetkilendirilmiş kullanıcıların (authorized users) değişiklik yapabilmesi sağlanır.

Lightweight Directory Access Protocol (LDAP)

Tanım olarak LDAP, TCP/IP üzerinde çalışan dizin servislerini sorgulama ve değiştirme amacıyla kullanılan uygulama katmanı protokolüdür.

Active Directory mimarisi içerisinde ise sorgulama (query) ve güncelleme (update) için kullanılan, temel bir directory servis protokolüdür.

LDAP ile Active Directory objeleri, OU (Organizational Unit) ve CN (Common Name) kullanılarak Active Directory içerisinde yeniden tanımlanır. LDAP isimlendirme yöntemi; Active Directory objelerine erişimde kullanılır ve iki tanım içerir;

1. Distinguished Names
2. Relative Distinguished Names

Distinguished Names : Tüm Active Directory objeleri, network ortamında kendilerine ulaşılmasını sağlayan komple path içeren, distinguished name'e sahiptir. Örneğin;

CN=Ali Osman, OU=Teknik , DC=aliosman gokcan DC=com

Burada kullanılan CN Common Name, OU Organizational Unit, DC ise Domain Controller anlamındadır. DC, Domain hiyerarşisini belirler. Tüm DNS akışı tek tek yazılır. Örneğin; Domain adı aliosmangokcan .com ise, DC=aliosmangokcan , DC=com şeklinde belirtilir. Bir başka örnek verecek olursak eğer "AKIF" isimli kullanıcı, "BEYAZ" isimli OU içinde bulunsun ve bağlı bulunduğu Domain adı "aliosmangokcan.com" olsun. Bunun "Distingushed Name" yazılımı aşağıdaki şekilde olacaktır;

CN=AKIF, OU=BEYAZ, DC=aliosmangokcan, DC=com

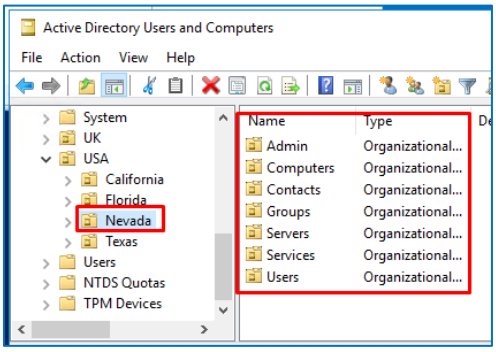
Relative Distinguished Name: LDAP distinguished name içerisinde yer alır ve objeye ait eşsiz (unique) tanımlamayı içerir. Yani Active Directory içinde belirtilen Domain içinde tektir. Örneğin;

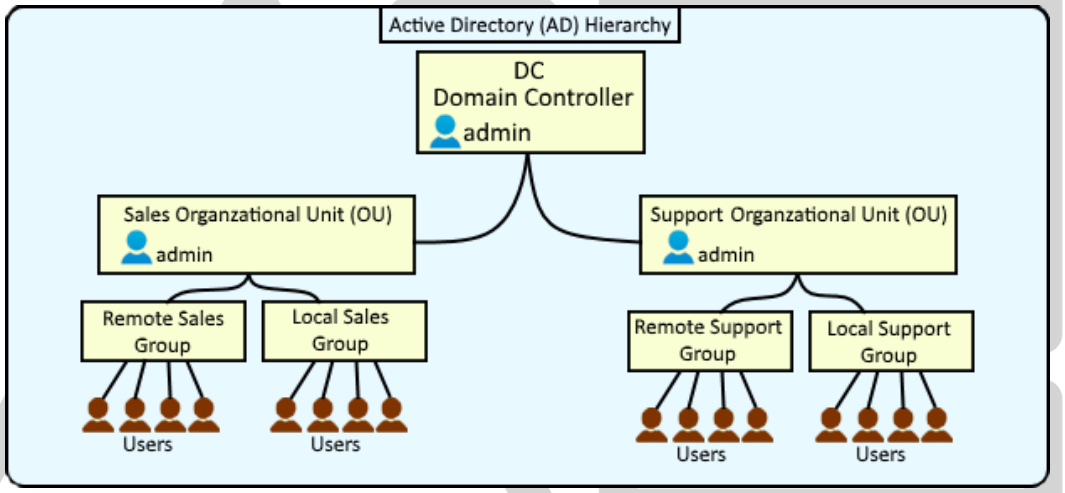
CN=AKIF, OU=BEYAZ, DC=aliosmangokcan, DC=com

yazımında aliosmangokcan.com içinde tek olan Relative Distingished Name AKIF 'dir. En son yazılan değer, her zaman tek değerdir. Ondan dolayı mükerrer olamaz.

Organizational Unit

Organizational Unit, bir Domain içerisindeki kullanıcıları, grupları veya bilgisayarları, yazıcıları organize etmek amacıyla oluşturulmuş objelerdir. Örnek olarak, objeleri gruplarken yönetimsel gereksinimler ön planda tutulabilir. Organizasyonda bir yönetici kullanıcılardan diğer yönetici ise bilgisayarlardan sorumlu olacaksa, biri kullanıcılar için biri de bilgisayarlar için iki adet OU oluşturulur ve kullanıcılar birinde bilgisayarlar da diğerinde toplanır. Son olarak ikisine de ayrı ayrı yönetciler atanabilir. Veya departmansal gruplandırmalar yapılabilir. Örneğin bir "Muhasebe" bir de "Pazarlama" departmanları için OU oluşturulur ve bu departmanlarda çalışan kullanıcılar ilgili OU'lara yerleştirildikten sonra departman şefleri bu birimlere yönetici olarak atanabilir. Bu işlemler aynı zamanda sistem yöneticilerinin işlerini kolaylaştıracaktır.





Ağ içerisindeki her Active Directory nesnesinin bir tanımlama bilgisi (distinguished name) bulunmaktadır.

Common Name (CN) : Active Directory nesnelerinin adını belirtir.

Organization Unit (OU) : Organizasyon biriminin adını belirtir.

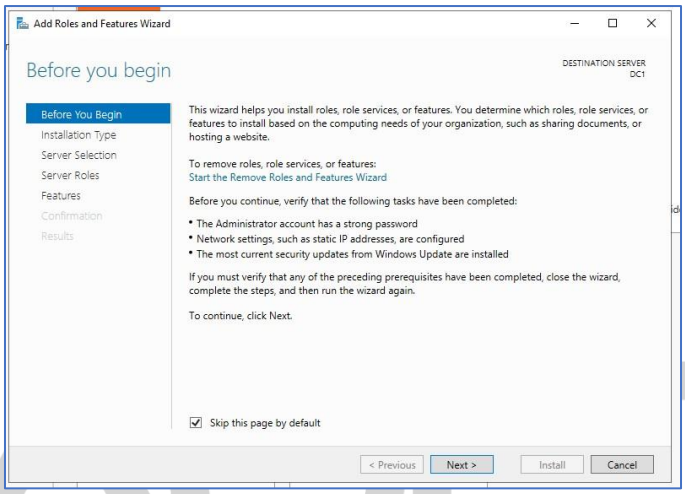
Domain Controller (DC): Etki alanının adını belirtir.

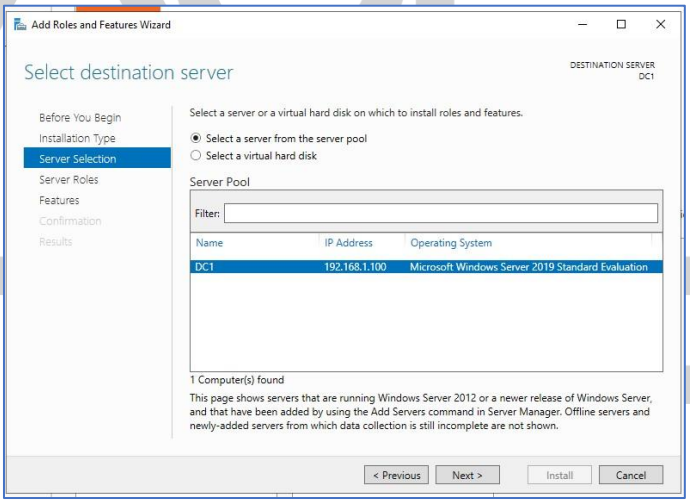
Örnek: sirketim.com domaini içerisinde "Pazarlama" organizasyon birimi içerisindeki "Lab_01" isimli bilgisayarın tanımlama bilgisi;

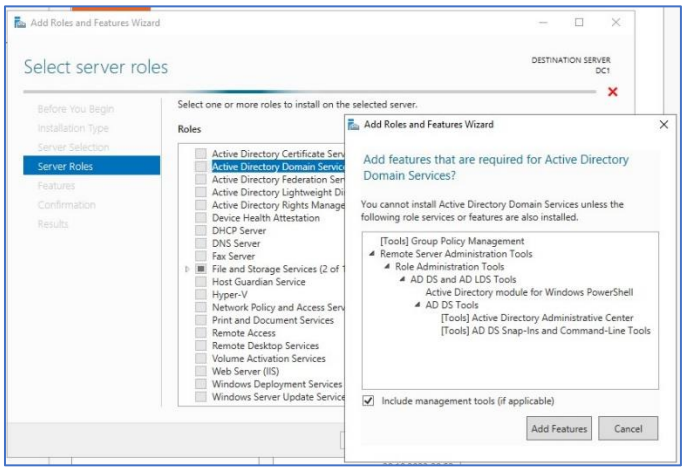
CN="Lab_01" **OU**="Pazarlama" **DC**="sirketim" **DC**="com"

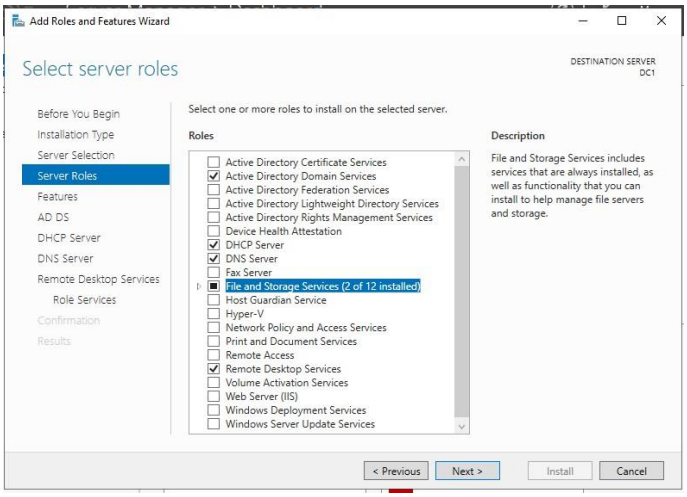
ACTIVE DIRECTORY (AD) KURULUMU

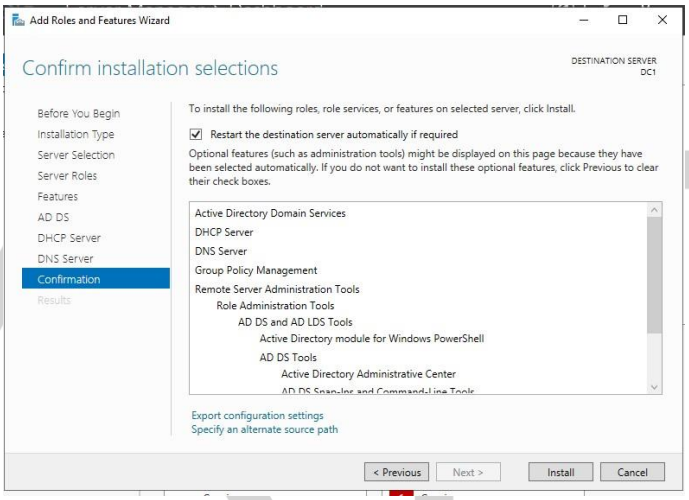
Windows Server 2012 işletim sistemine kadar ki versiyonlarda (2000,2003,2008,2008 R2) AD kurulumu DCPROMO komutu ile yapılıyordu. Hatta AD kurulumunu kaldırmak için de aynı komut kullanılmaktaydı. Server 2012 ve sonrasında AD kurulumu için Server Manager konsolu/ekranı kullanılmaktadır. Kurulum için aşağıdaki ekran görüntülerini sırasıyla uygulayabilirsiniz.

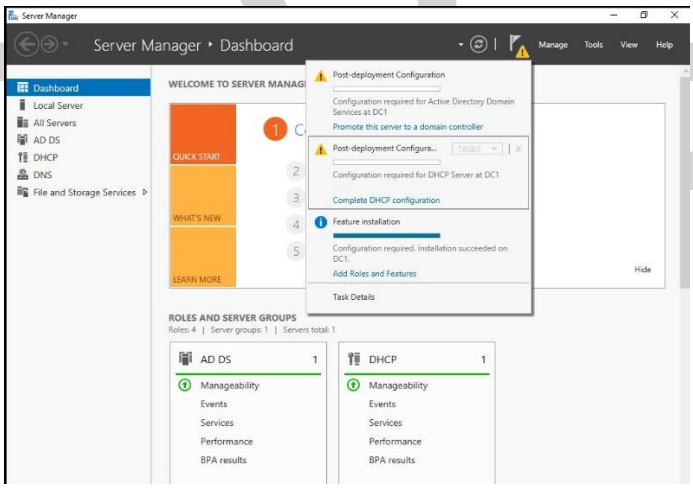


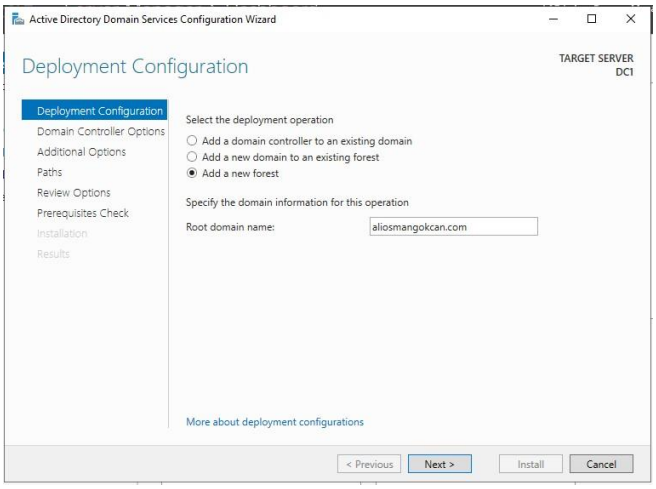


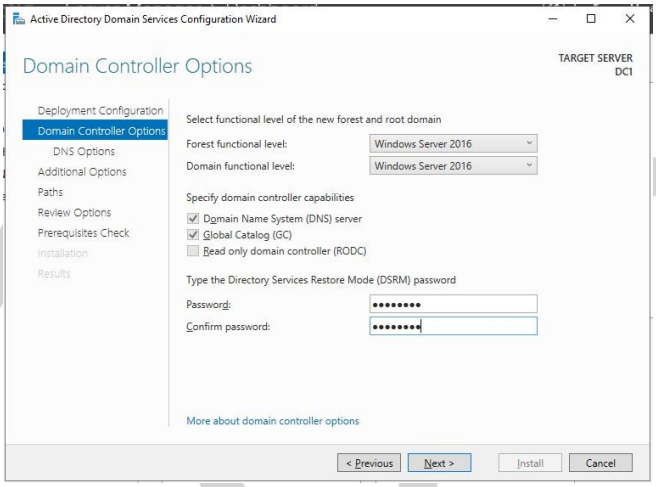


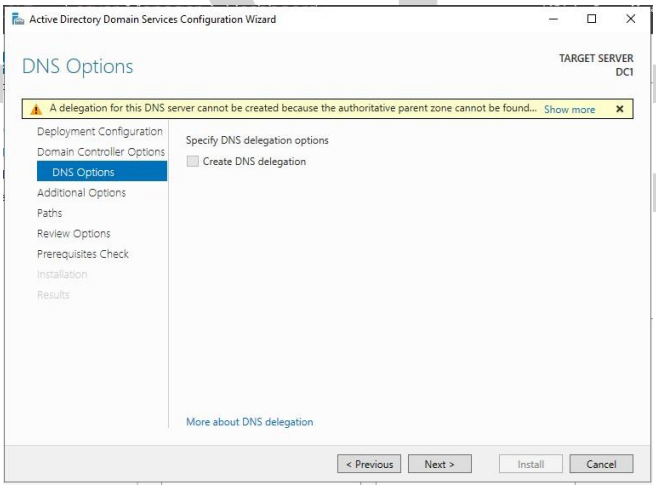

Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
DC1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
DHCP Server
DNS Server
Remote Desktop Services
Role Services
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Certificate Services
Active Directory Domain Services
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Device Health Attestation
DHCP Server
DNS Server
Fax Server
File and Storage Services (2 of 12 installed)
Host Guardian Service
Hyper-V
Network Policy and Access Services
Print and Document Services
Remote Access
Remote Desktop Services
Volume Activation Services
Web Server (IIS)
Windows Deployment Services
Windows Server Update Services
Description
File and Storage Services includes services that are always installed, as well as functionality that you can install to help manage file servers and storage.
< Previous
Next >
Install
Cancel

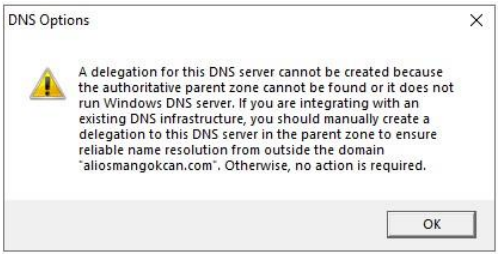

Add Roles and Features Wizard
Confirm installation selections
DESTINATION SERVER
DC1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
DHCP Server
DNS Server
Confirmation
Results
To install the following roles, role services, or features on selected server, click Install.
Restart the destination server automatically if required
Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.
Active Directory Domain Services
DHCP Server
DNS Server
Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
Active Directory Administrative Center
Export configuration settings
Specify an alternate source path
< Previous
Next >
Install
Cancel

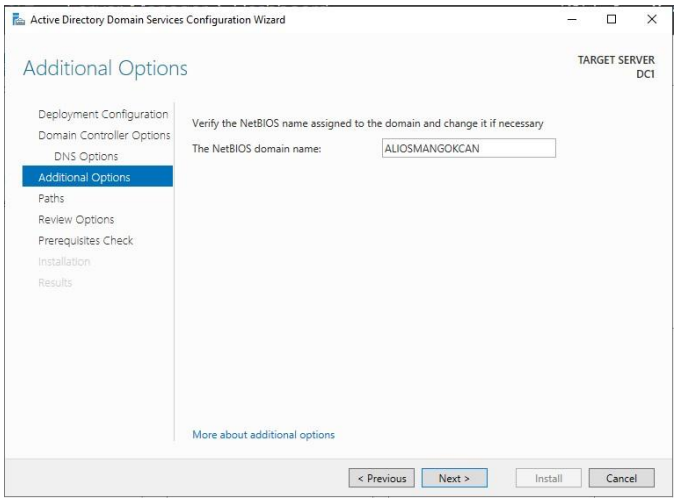

Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
DHCP
DNS
File and Storage Services
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
Post-deployment Configuration
Configuration required for Active Directory Domain Services at DC1
Promote this server to a domain controller
Post-deployment Configura...
Configuration required for DHCP Server at DC1
Complete DHCP configuration
Feature installation
Configuration required. Installation succeeded on DC1.
Add Roles and Features
Task Details
Hide
ROLES AND SERVER GROUPS
Roles: 4 | Server groups: 1 | Servers total: 1
AD DS
1
Manageability
Events
Services
Performance
BPA results
DHCP
1
Manageability
Events
Services
Performance
BPA results

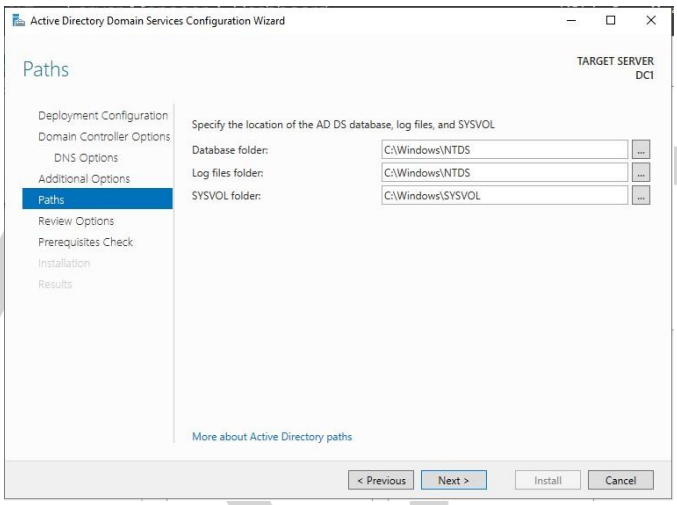

Active Directory Domain Services Configuration Wizard
Deployment Configuration
TARGET SERVER
DC1
Deployment Configuration
Domain Controller Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Select the deployment operation
Add a domain controller to an existing domain
Add a new domain to an existing forest
Add a new forest
Specify the domain information for this operation
Root domain name:
aliosmangokcan.com
More about deployment configurations
< Previous
Next >
Install
Cancel

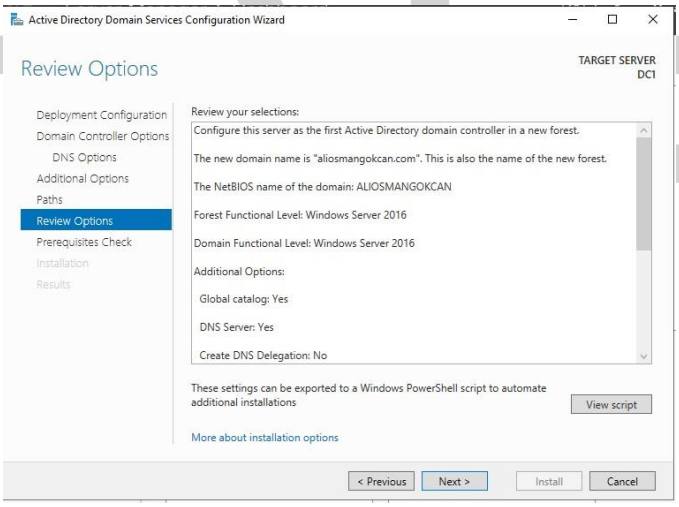

Active Directory Domain Services Configuration Wizard
Domain Controller Options
TARGET SERVER
DC1
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Select functional level of the new forest and root domain
Forest functional level:
Windows Server 2016
Domain functional level:
Windows Server 2016
Specify domain controller capabilities
Domain Name System (DNS) server
Global Catalog (GC)
Read only domain controller (RODC)
Type the Directory Services Restore Mode (DSRM) password
Password:
Confirm password:
More about domain controller options
< Previous
Next >
Install
Cancel

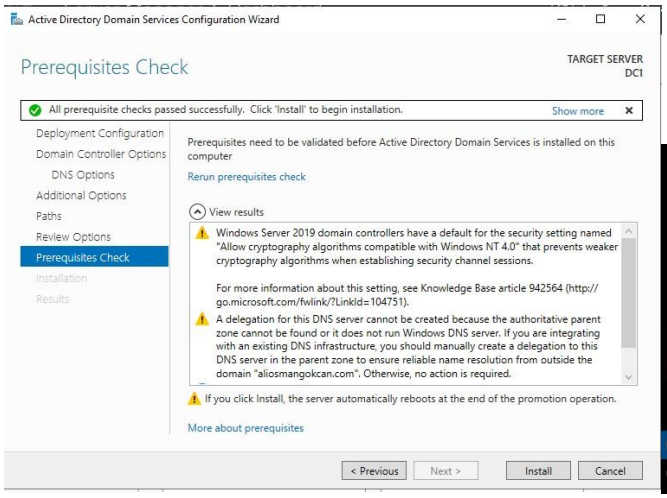

Active Directory Domain Services Configuration Wizard
DNS Options
TARGET SERVER
DC1
A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found...
Show more
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Specify DNS delegation options
Create DNS delegation
More about DNS delegation
< Previous
Next >
Install
Cancel

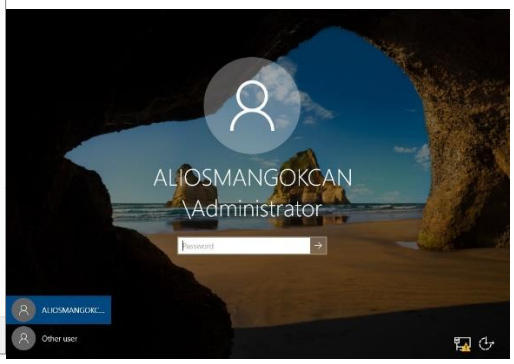

DNS Options
A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "aliosmangokcan.com". Otherwise, no action is required.
OK


Active Directory Domain Services Configuration Wizard
Additional Options
TARGET SERVER
DC1
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Verify the NetBIOS name assigned to the domain and change it if necessary
The NetBIOS domain name:
ALIOSMANGOKCAN
More about additional options
< Previous
Next >
Install
Cancel


Active Directory Domain Services Configuration Wizard
Paths
TARGET SERVER
DC1
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Specify the location of the AD DS database, log files, and SYSVOL
Database folder:
C:\Windows\NTDS
Log files folder:
C:\Windows\NTDS
SYSVOL folder:
C:\Windows\SYSVOL
More about Active Directory paths
< Previous
Next >
Install
Cancel


Active Directory Domain Services Configuration Wizard
Review Options
TARGET SERVER
DC1
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Review your selections:
Configure this server as the first Active Directory domain controller in a new forest.
The new domain name is "aliosmangokcan.com". This is also the name of the new forest.
The NetBIOS name of the domain: ALIOSMANGOKCAN
Forest Functional Level: Windows Server 2016
Domain Functional Level: Windows Server 2016
Additional Options:
Global catalog: Yes
DNS Server: Yes
Create DNS Delegation: No
These settings can be exported to a Windows PowerShell script to automate additional installations
View script
More about installation options
< Previous
Next >
Install
Cancel



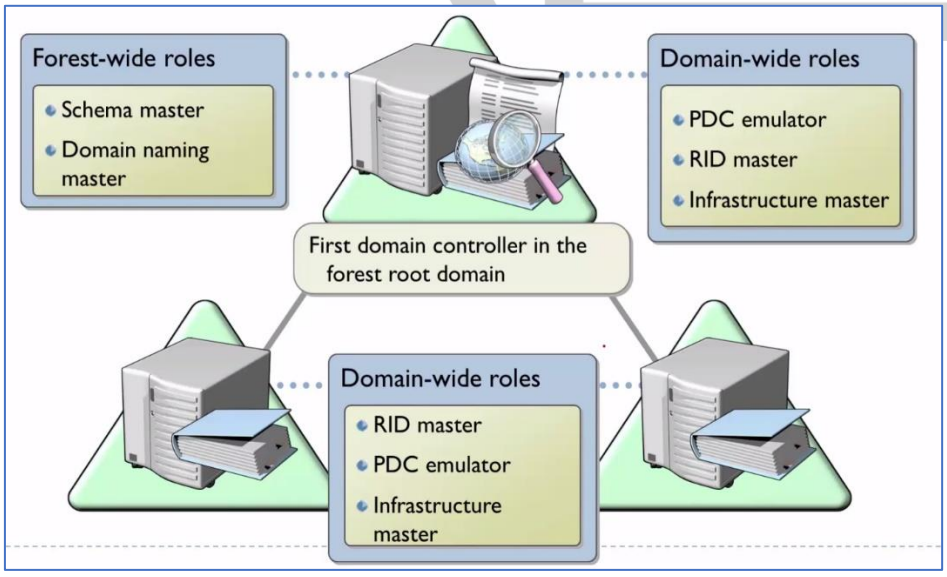


FSMO ROLLERİ

Active directory yapısında bulunan objelerin görevlerini yerine getirmeleri, çalışmalarının sağlıklı yürütülmesi için görev alan servisler ile beraber ayrıca bu servisleri yöneten roller bulunmaktadır. Bu rollere FSMO (Flexible Single Master Operation) rolleri denir. Bu roller içerisinde Forest bazında tek olanlar olabileceği gibi domain bazında tek olanlar da vardır. Bunlar;

a. Schema Master (Forest bazında tek)
b. Domain Naming Master (Forest bazında tek)
c. PDC Emulator,
d. RID Master,
e. Infrastructure Master

Bu 5 rol standart olarak ilk kurulan Forest içerisindeki ilk domain controller üzerinde bulunur.



- **Schema Master;**

Tüm güncelleme ve bilgiler Schema Master üzerinde tutulur. Forest bazında tektir. Active Directory Domain Services içerisinde, yapıdaki nesnelerin sahip olacağı özellikleri belirleyen bileşendir. Nesnelerin biçimsel yapısını belirler diyebiliriz. Örneğin, kullanıcı nesnesinde ad, soyad, şehir, görev gibi bilgilerin olacağını Schema belirler. Bu rol üzerinde sadece Domain Admins ve Enterprice Admins grubu üyelerinin yetkileri vardır. Diğer DC ler ile replike olur ve güncellemeleri yapar.

- **Domain Naming Master;**

Forest içerisinde tektir. Domain içerisine giren ve çıkan objelerin bilgilerini tutar ve yönetir. Domain (Etki alanı) isimlerini bünyesinde tutan rehberdir diyebiliriz. Yeni bir domain kurulacağı zaman isim onayını bu rol verir. İsim çakışmasını önler.

- **PDC Emulator;**

Saat senkronizasyonu, Şifre değişiklikleri ve şifre resetlemeleri, Group Policy ve sysvol paylaşım erişimlerini yönetir. Domain içerisinde tektir. En önemli roldür. Windows oturumlarını kontrol eder.

- **RID Master;**

Ağda bulunan tüm nesnelerin kendine has (benzersiz) bir SID numarası vardır. Nesnelerin benzersiz bir SID numarası almasını sağlar ve çakışmayı önler. Domain içerisinde tektir.

- **Infrastructure Master;**

Domainde tektir. Domainler arası bilgi transferini yapar ve güncel tutulmasını sağlar. Üzerindeki bilgi her daim günceldir.