Active Directory ------→**DOMAİN**
Windows 2000 den sora hayatımıa girmiş.

Microsoft tarafından özellikle Windows server ve client bilgisayar sistemleri için tasarlanmış olan içerisinde sunuvu client bilgisayar kullanıcı ve yazıcı gibi bilgileri tutan bir dizin servisidir.Bu servis içerisinde yer alan Group Policy yönetim aracı ile çeşitli kısıtlamalar yapabilir veya tek bir oktadan istediğimiz uygulamanın dağıtımını gerçekleştirebiliriz.

Active Directory servisi Domain controller olarak adlandırılan sunucu veya sunuvular üzerinde tutulur.

Veritabanı dosya ismi ntds.dit dosyasıdır.

Bununla birlikte tüm işlemlerin geçici olarak yer aldığı değişkenlerin veritabanına yazılmadan önce çeşitli sebeplerden ötürü saklandığı edb.log isimli dosyada Active Directory servisinin çalışmasında kritik yol oynar.

Özellikleri

Yönetilebilirlik
Genişletilebilirlik
Güvenlik entegresyonu
Diğer dizin servisleriyle birlikte çalışabilme
Güvenli kimlik doğulama ve yetkilendirme
Group policy ile yönetim
DNS ve Dhcp servislerle birlikte çalışabilme özellliği

Active Directory Mantıksal Yapısı

Veri deposunda bulunan bilgilerin nasıl görüleceğini belirler ve aynı zamanda o bilgilere erişimi denetler.İçerisinde kullanıcıc ve yönetici kapsamında hiyerarşik bir yapı kurulmasına olanak tanır.

LDAP:Tcp/ıp üzerinde çalışan servisleri sorguama değiştrme amacıyla kullanılan uygulama protokolü

Active Directory Fiziksel Yapısı

Active Directoryiçinde fiziksel yazpı mantıksal yapıdam bağımsız bir mimariye sahiptir.Mnatıksal yapı ile network kaynakları organze edilirken fiziksel yapı ile network trafiğinin kontrolü ve konfigürasyonu gerçekleştirilebilir.Act,ve directorynin fiziksel yapısını **DC(Domain Controller)** Ve **Site** lar oluşturur

Active Directory Güvenliği

Hesap Bilgilerinin Kontrol edilmesi ve değiştirilmesi
Kritik grup üyeliklerinin kontrol edilmesi
Yapı içerisindeki kullanıcıları hesaplarının takibi
Kimlik doğrulama
Lockout yöntemi

Active Directory Loglama
Yapılan tüm eylemlerin kayıt altına alınması Bu yapıyı belirli aralıklarla takip etmek gerekir.

Grpoup Policy Management
Group Policy istemci ve sunucu tarafında varsayılan olarak gelen bir özelliktir Group policy yönetilen sistemlerin ihtşyaçları doğrultusunda kullanılabilir.GPO(GROUP policy Object)Güvenlik sıkılaştırmaları ksııtlamalar ve benzeri işlemleri tek bir çatı altından yönetebileceğiniz bir active directory özelliğidir.

GPO da Ou(Oigaizational Unit) için policyler oluşturabilir veya tüm Ou lere aynı policyleri ekleyebilirsiniz Varsayılan olarak ise Default Domain Policy olarak gelmektedir.

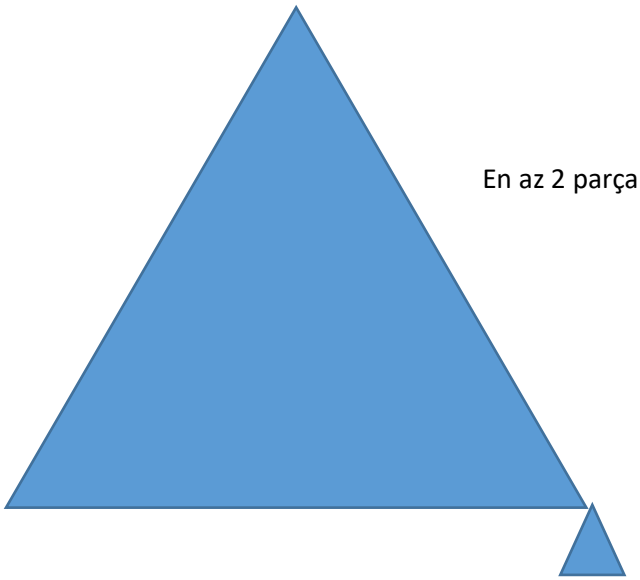
Kontrol paneline herkesin erişmemesi lazım
Bilgisayarlara takılan cihazların denetimi
yazılım yüklemesi denetimi
Parola kullanım süresi ve parola uzunluğu
komut satırı erişimi
Windows Exchange Server

Şirketlerin iletişim trafiğini yönetmesi için Microsoft tarafından geliştirilen iş birliği platformu
Epsota belgepaylaşım takvim rehber ve veri depolama gibi bir çok özelliği destekleyen sahip olduğu üstün güvenlik ve veri depoama özellikleri sayesinde şirketlerin iletişimtrafiğini mevzuatlara uygun ve güvenli şekilde yönetmelerine olanak tanır.

E posta istemcileri ve akıllı cihazlar ile etkileşimli bir şekilde çalışıyor kullanıcıların bir çok platformdan iletiişm kurulmasına verileri ise tek bir yerden depolanmasını sağlar ek olarak veri yedekleme veri kurtarma olanağı sağlar.
windoes Exchange server açıkları bulup saldırganlar;
1)keşif
2)Güvenlik açığı bulur ve sızar
3)Bilgi hırsızlığı
Güvenlik önlemleri
Exchange sunucularını güncel tutmalıyız
özel yardımcı programları kullanmalıyız
Güvenlik duvarlarını aktif hale getirmeliyi
Exchangi destekleyen ağ çevresini güvenli hale getirmeliyiz
Exchange sucunucuları izlenip ağ çevresini güvenli hale getirmeliyiz
izi verilenler ve engellenenler listesi oluşturmalıyız.Yönetici erişimini sınırlamalıyız.

Aslında bir database bir dosya .Dosyanın içerisinde bir sürü şey var.Oluşturduğumuz kullanıcılar gruplarvb
!!! Database in görevi Active Directory bilgisini saklamaktan sorumlu
Forest :Tüm treelerin bulunduğu yapı alt alta tree ayrı treee hepsi forestı kapsar

Tree :Alt alta dallanan yapı domainde
Organizational Unit
Domain
domain controller=Active directry databaseini üzerinde bulundurua nmakina .Domainle ilgili herşeyi üzerinde saklayan makine
global catalog
additional dc:zarralanma ihtimaline karşı aynı dc den bi tane daha yapma yedekleme.Her domain için bir DC şart

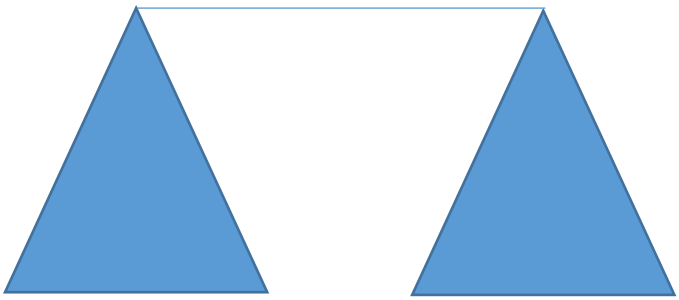


En az 2 parça isim ,Türkçe karaketer yok,benzersiz (unique) **PARENT**

Şubeler bağlantılar üçgene bağlı olmalı **CHİLD**

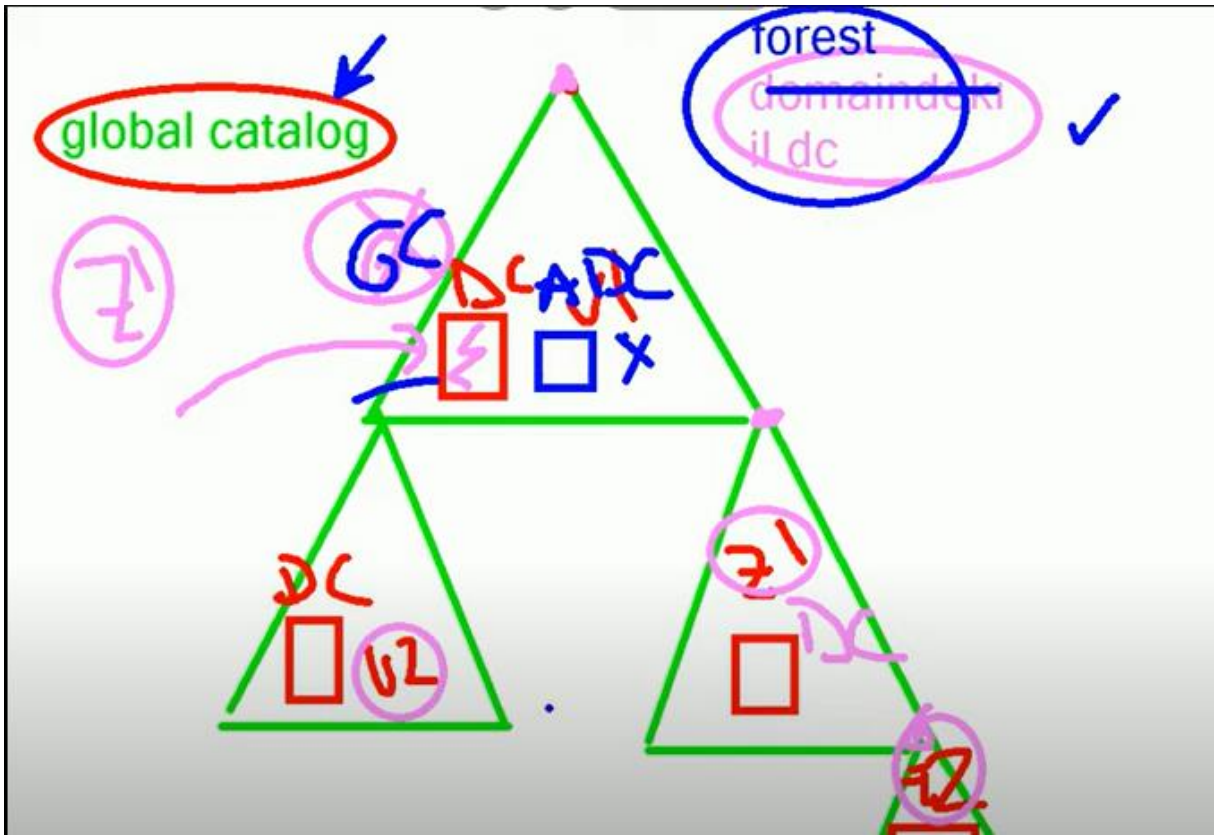
Domain Admins=Her domainin bir yöneticisi var ve domaine karışabiliyor.

Enterprise Admins=Tüm Domainlere karışabiliyor.Forestın ilk dc sinde
Merkeze bağımlı ismini üstten alıyor .



Yönetime bağımlı ama isimler değişik.Ekstra isimli bir domain istiyosak bu şekilde yapmamız lazım.

GLOBAL CATALOG:Active Directory ortamındaki her şeyi katologluyor.Foresttaki ilk DC.Altındaki kullancılar hakkında **sadece bilgisi** var



Organizational Unit OU: Folder mantığı ile aynı .işemleri klasörleyerek daha kolay işlem yapılmasını sağlar.

Bir domain kurma için neler şart?

1)Server işletim sistemi şart Server donanımı şart değil

2)Statik Ip şart

3)Subnet Mask şart Ip ile kullanmak zorundasın DG(Default Gateway)olmasada olur

4)DNS şart domain control edebilmek için Active directory dns ile çalışabilmek için ŞART

5)domain ismi ile makine ismi mantıklı olmalı

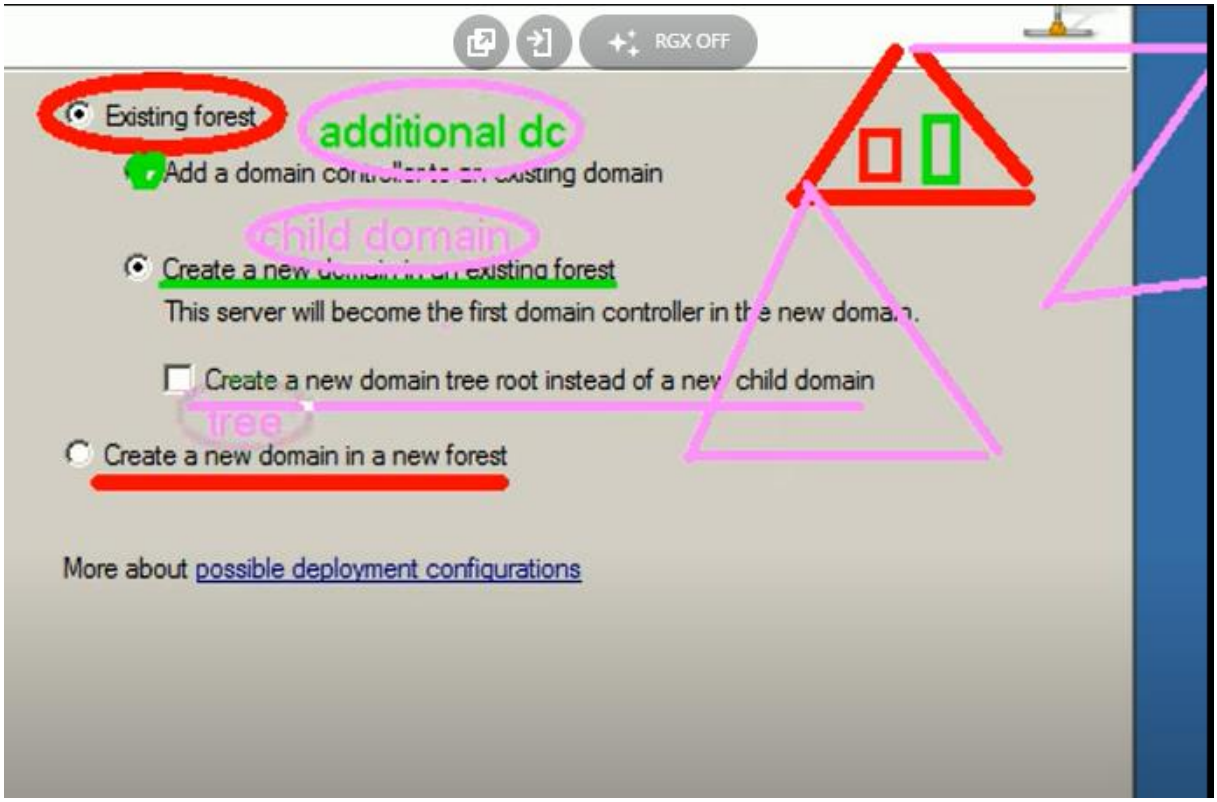
6)domain ismi kurallara uygun olmalı Türkçe karakter olmayacak en az iki parça çakışmayacak

Programda Add role diyip ekleme yaparken Active Directory Domain Services dersek domain kurabilmek için gerekli ortamı (file,register ayarları ,ekstra servisler)ayarlar.

Dcpromo=domain kurmak için kullanılan komut bunu direk konsoldan yazarak direk yazabiliriz.

Makineyi domain kontrol yapabilmek için Local Admin olmak lazım.

Domain kurarken gerekli olmayan duruma göre seçebiliriz.-→Use Advanced Mode ile



Forest root domain =en tepedeki domain

Forest Func Level Dc işletim sistemini belirler.

Domain Function Level=Domainlerin forestlerin farklı functınları olabilir.