Windows Server

Active Directory

Mantıksal ve Fiziksel Mimarisi

Dizin servisi (Directory Service) Nedir?

Acıktığınızda ya da canınız yemek çektiğinde, telefon defterini açıp “yemek” yapan ünlü restoranların numaralarını bularak sipariş verirsiniz. İşte burada yemek ürününün üretildiği ve satıldığı restoranların adresini size veren telefon defteri bir directory service örneğidir. Directory service ulaşacağınız nesneye ait ihtiyacınız olan adres ve lokasyon bilgisini içerir. Telefon defteri örneğinde alfabetik bir sıralama söz konusudur. Bir diğer örnek, okuduğunuz bir kitapta ilginizi çeken bir konuyu bulmak için kitabın arka bölümündeki index kısmına bakarak konunun bulunduğu sayfayı öğrenir ve o sayfayı açıp konuyu okuyabilirsiniz. İşte kitap içerisinde aradığınız konunun adresini size veren index de bir başka directory service örneğidir. Bilgisayar üzerindeki directory service de hemen hemen aynı mantıkta çalışır.

ACTIVE DIRECTORY NEDİR?

Active Directory, Windows 2000 ve sonrasının bulunduğu, Network ortamlarında kullanılan bir directory servisidir. Bu servis Network içerisinde bulunan kaynakların isim, tanım, lokasyon, erişim, yönetim ve güvenlik bilgilerini depolamanın yanı sıra bu bilgileri, kullanıcılar ile uygulamaların hizmetine sunar. Active directory sunucuya bağlı bütün bilgisayarları ve kullanıcıları yönetmeyi sağlayan bir veritabanıdır.Bütün bilgisayar ve kullanıcılar bu veri tabanı içinde bir obje ve bir nesne.

Network ortamındaki fiziksel topoloji ile protokoller arası iletişimi sağlayarak kullanıcıların, aradıkları kaynaklara nerede ve nasıl Network'e dahil olduğunu bilmeksizin, ulaşmalarına olanak verir.

Directory Servisin Avantajları

- **Tek noktadan yönetim(Centralized Administration):** Active Directory sayesinde, kaynakların ve kullanıcıların bulunduğu konum ve aradaki mesafe önemli olmaksızın tek noktadan merkezi olarak yönetim yapılabilir. Kullanıcı, kaynak veya bilgisayar isterse dünyanın öbür ucunda olsun, Active Directory sayesinde, Active Directory üzerinden bu kaynakları ve bilgisayarları merkezi olarak yönetebiliriz.
- **Eşit Haklara Sahip Domain Controllerlar(Multimaster DC):** Aynı Active Directory domaini içerisindeki bütün DC'ler eşit haklara ve eşit veritabanına (database) sahiptirler. Dolayısıyla her DC master server rolünü alabilecek özelliğe sahiptir. Bir DC'de açılan bir kullanıcının özelliklerini başka bir DC'den kolaylıkla değiştirebilir ve bu değişikliği de diğer DC bilgisayarlarına güncelleyebilirsiniz.

Directory Servisin Avantajları

- **Genişletilebilme ve Büyütülebilme(Scalability):**Active Directory domain yapısını ihtiyacınıza göre istediğiniz kadar büyütebilirsiniz.Bir domain içerisinde milyonlarca obje barındırılabilir. NOT:Windows NT 4.0 domainlerinde domain veritabanının maksimum boyutu 40 MB'ı yani ortalama 40.000 kullanıcı hesabını geçemiyordu.
- **Internet İsim Yapısı Desteği:** Windows 2012/2008/2003/2000 Active Directory domain yapısı domain isimlendirmelerinde internet üzerinde kullanılan DNS isimlendirme yapısını(DNS namespace) kullanır. Bu isimlendirme yapısı sayesinde mail server gibi diğer yapıların yönetimi de daha esnek ve kolaylıkla yapılabilir.

Directory Servisin Avantajları

- **Dynamic DNS Desteği:**Windows 2012/ 2008/2003/2000 Active Directory sayesinde domaine katılan bir bilgisayar hesabının DNS(Domain Name System) veritabanında da otomatik olarak kayıtları oluşmuş olur. Windows 2012/2008/2003/2000 DNS'nin desteklediği Dynamic Update yani dinamik güncelleme sayesinde, ip adresi değişen bir client bilgisayarı bu değişikliği DNS'e bildirerek DNS veritabanını da güncellemiş olur.
- **Delegasyonlu Yönetim:**Active Directory içerisinde açılmış OU'lere delege ataması yapılarak domainin asıl yöneticisi olan administrator kullanıcısının yükü azaltılabilir. Böylece departman veya şube bazında işten anlayan junior adminlere temel görevler atanarak domain yönetimi kolaylaştırılabilir. Delegelerin yapacakları administrator'ın verdiği haklarla belirlenir.

ACTIVE DIRECTORY SCHEMA :

Active Directory Schema: Kullanıcı, grup, bilgisayar ve yazıcılar gibi bütün objelere ait bilgileri içerir. Windows 2000 ve sonrasında tüm Network yapınız (forest) içerisinde, sadece bir Schema bulunur ve bütün obje bilgileri Schema üzerine yazılır.

Schema yapısında, obje sınıfı ve niteliği tanımlanabilir.

Obje sınıfı: Bilgisayar, kullanıcı veya yazıcı olabilir. Nitelik: Schema içinde objelere ait bilgilerdir, bir kez tanımlandıktan sonra, arama(search) işlemlerinde kullanılabilir.

Örneğin: Kullanıcıların çalıştıkları bölümler, doğum yeri gibi.

Schema bilgileri: Active Directory veri tabanı(database) içerisinde depolanır.

Dolayısı ile;

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

Active Directory Yapısı

2 ye ayrılır:1_ Mantıksal Yapı

2_ Fiziksel Yapı

Active Directory içinde mantıksal yapı, fiziksel yapıdan bağımsız ve farklı bir yapıya sahiptir. Mantıksal yapı ile Network kaynaklarını organize ederken, fiziksel yapı ile Network trafiğini kontrol ve konfigüre edebilirsiniz.

Mantıksal Yapı Bileşenleri

Active Directory içerisindeki kaynakların organize edilmesi ve gruplandırılmasını içeren yapı mantıksal yapıdır. Active Directory içerisindeki mantıksal komponentleri genel olarak aşağıdaki şekilde sıralayabiliriz:

- Domain
- Organizational Unit
- Forest
- Tree
- Global Catalog
- Trust Relationship

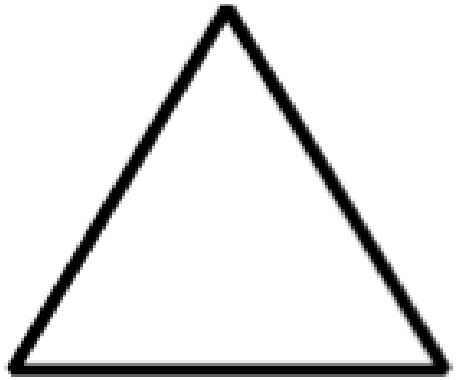
DOMAIN (ETKİ ALANI):

Domain: Yönetici(administrator) tarafından tanımlanmış ve ortak bir Database (veri tabanı) içerisinde paylaşıma sunulmuş bilgisayarları kapsar. Network ortamında eşsiz(unique) isime sahip olmalıdır. Domain yöneticisinin kullanıcı ve , grup hesaplarını denetlemesini merkezileştirmektedir.

Domain'ler ayrıca Replikasyon birimi olarak işlem yaparlar. Replikasyon iki yer arasında zaman uyumlaştırmayı (senkronizasyon) tanımlayan genel bir terimdir. Replikasyon süreklilik/devamlılık sağlamayı bazen de yedek kopya oluşturmayı sağlar Bu işlev, Domain içerisinde yer alan ve Domain Controllers(DC) olarak adlandırılan bilgisayar tarafından yapılır. Active Directory bilgilerindeki değişikliklerin, tüm Domain yapısına iletilmesi DC bilgisayarlar arası Replikasyon ile sağlanır.

DOMAIN

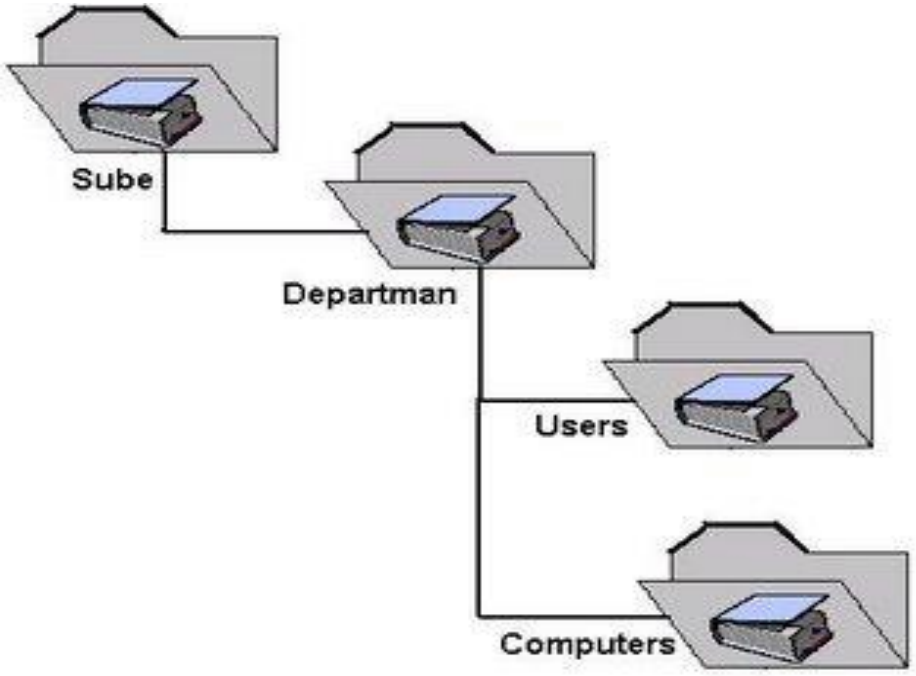
Bir Windows ağında merkezi yönetimi sağlamak amacıyla kurulan çekirdek yönetim birimine domain (etki alanı) adı verilir. Domain, aynı isim altında toplanmış objelerin oluşturduğu yapılara verilen isimdir.



Aynı domain içerisinde bulunan bütün objeler ortak bir veritabanı içerisinde depolanırlar. Windows 2012/2008/2003/2000 networkleri üzerinde domain yapısının oluşturulabilmesi için Active Directory domain servis rolünün Windows Server 2012/2008/2003/2000 sunucu ailesinden bir işletim sistemine sahip bilgisayar üzerine kurulması ve yapılandırılması gerekir.

ORGANIZATIONAL UNIT (OU)

Organizational unit (yapısal birim), domain içerisindeki objeleri organize etmeyi sağlayan birimlerdir. Organizational Unit'ler, kullanıcı hesapları(user accounts), grup hesapları(group accounts), bilgisayar hesapları (computer accounts), yazıcılar (printers), paylaştırılmış klasörler(shared folders) gibi nesneleri içerirler. Her domain içerisinde oluşturulan OU hiyerarşisi birbirinden bağımsızdır.



ORGANIZATIONAL UNIT (OU)

Nesneler organizational unit'ler içerisinde konumlandırılarak dağınıklık önlenmiş ve yönetim kolaylaştırılmış olur. Şirketiniz içerisinde, sahip olmuş olduğunuz departmanlar bazında OU'lar oluşturup, departmanlar içerisindeki nesneler için de ayrı ayrı alt OU'lar oluşturabilirsiniz. Mesela; muhasebe departmanı için bir OU oluşturup, bu OU altında da muhasebe departmanı içerisindeki bilgisayarlar için ayrı bir alt OU, kullanıcılar için ayrı bir alt OU oluşturarak düzenli bir yapı oluşturabilirsiniz. Bu işlemi şirket içerisindeki diğer departmanlar için tekrarladığınızda düzenli ve yönetimi kolay bir yapı oluşturmuş olacaksınız.

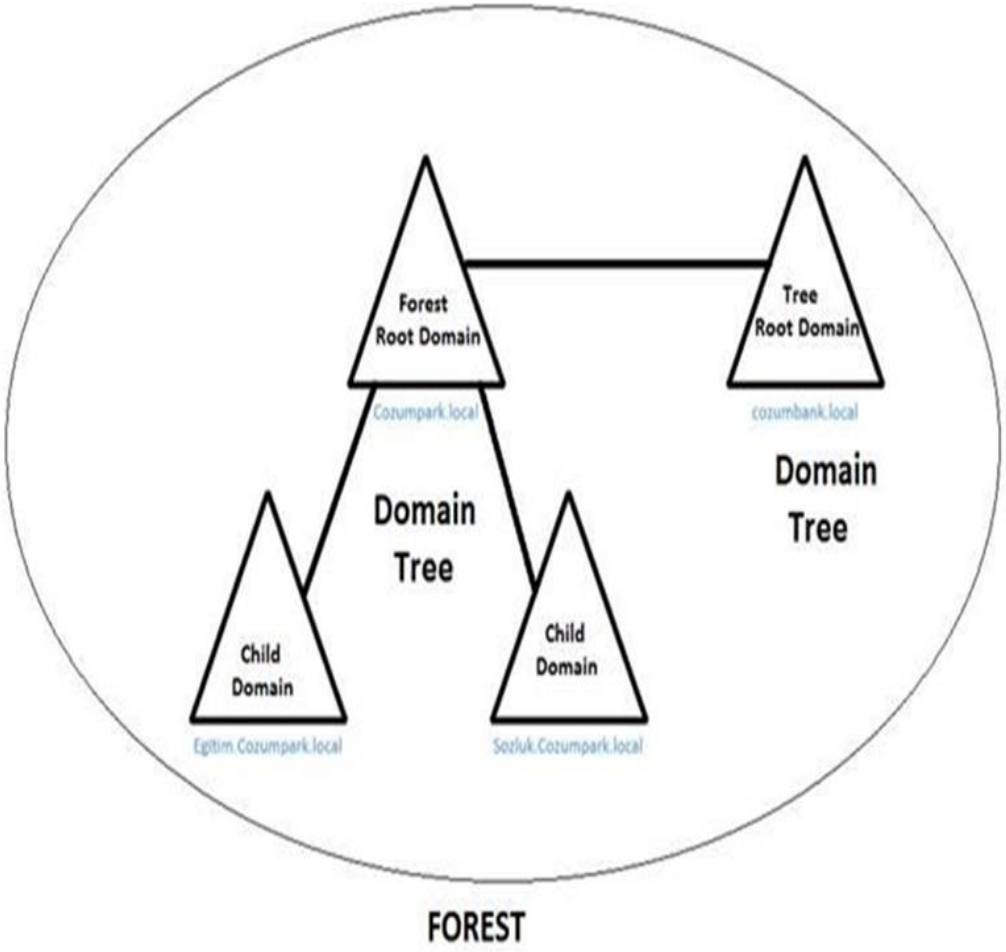
Organizational Unit'in sağladığı bir diğer avantaj da delegasyondur. Bir departman içerisindeki nesneler için yukarıda anlatmış olduğumuz model kullanılarak bir OU yapısı oluşturulduktan sonra, bu OU'lar altında yönetim amacıyla sistemdeki kullanıcıları delege olarak atayabilirsiniz. Kullanıcınızın delege atanması esnasında hangi yetkilere sahip olacağı belirlenmektedir. Bu sayede domain admin kullanıcısı üzerindeki yükün azalması ve temel görevlerle ilgili yönetimin kolaylaşması sağlanmış olacaktır.

FOREST

Forest, active directory domainlerinde mantıksal yapı içerisinde en dış katmandır. İçerisinde bir ya da daha fazla sayıda domain tree barındıran yapıya verilen isimdir. Aslında ilk kurulan domainden sonra o domaini içeren domain tree ile beraber en dış katmanda da forest yapısı oluşmuş demektir.

Forest içerisinde ilk kurulan domain'e "forest root domain' adı verilir. Forest yapısı da forest root domain adı ile anılır. Forest root domain altına ihtiyaca göre alt domainler (child domain) kurarak yapı genişletilebilir. Yine aynı forest içerisinde aynı grubun ya da organizasyonun içerisinde olan, fakat farklı isim alanına sahip ayrı domain ağaçları da kurularak yapı genişletilebilir. Her kurulan farklı isim alanındaki domain ağacının ilk domainine de tree-root-domain adı verilir.

FOREST



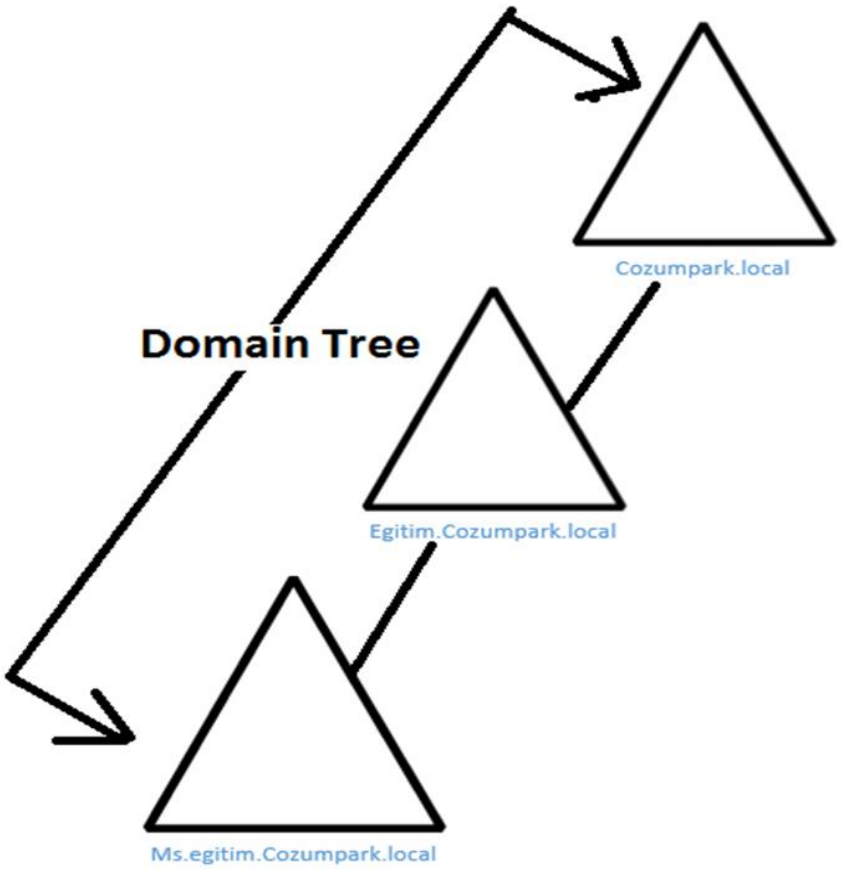
Forest, bir veya daha fazla Tree'den oluşur. Forest içindeki Tree'ler, aynı isim alanını kullanamazlar. Fakat forest içindeki tree'ler ortak bir Schema ve Global Catalog yapısını paylaşırlar. Forest içerisindeki tüm Tree Root Domain yapıları, Forest Root Domain ile geçişli güven ilişkisine sahiptir.

Forest içinde her tree, kendi eşsiz isim alanına(unique name space) sahiptirÖrneğin: Çözümpark haricinde, Çözümbank adıyla ayrı bir organizasyonu, yeni bir Active Directory Domain ismi ile kurmak istenebilir. Söz konusu iki organizasyon aynı isim alanını paylaşmamalarına rağmen, yeni Domain'i mevcut bir Forest altında yeni bir tree olarak yapılandırabiliriz. Sonuç olarak her iki organizasyon, birbirleri ile kaynaklarını veya yönetimsel fonksiyonlarını paylaşabilirler.

Domain Tree

Domain Tree, aynı isim altında toplanmış bir veya daha fazla sayıda Windows 2012/2008/2003/2000 domaininin hiyerarşik olarak oluşturduğu yapıya verilen isimdir. Diğer bir deyişle, aynı isim altında toplanan domainler topluluğuna "domain tree" adı verilir. Domain Tree, mevcut bir parent domain'e child domainlerin eklenmesi ile genişletilebilir. Aynı Domain Tree içerisindeki domainler hiyerarşik bir isim yapısını paylaşmaktadırlar. Domain Tree içerisinde bulunan child domainler, isim yapılarında parent domaininin ismini kendi domain isimlerinin sonuna soy isim gibi ekleyerek kullanırlar. Aynı domain tree içerisindeki domainler, ortak bir domain isim alanına(domain namespace) sahiptirler.

Domain Tree



Bir ortamda kurulan ilk domain ile esasında o domaine ait domain tree de oluşmuş olacaktır. Yapıyı yukarıda da bahsettiğimiz gibi alt child domainler kurarak genişletmek mümkündür. Bir domain tree içerisinde en tepede olan ve ilk kurulan domaine tree-root-domain, o domainin domain controller bilgisayarına da tree-root-DC adı verilir.

GLOBAL CATALOG

Active Directory içerisindeki tüm objelere ait niteliklerin tutulduğu yerdir. Kullanıcının ilk ismi, son ismi gibi sorgulamalarda sıklıkla kullanılan nitelik bilgileri, default olarak Global Catalog içerisinde depolanır.

Directory içerisindeki herhangi bir objenin tanımlanması için, gerekli bilgileri kapsar.

Forest içerisinde kendi domaininiz dışındaki bir domainde ya da farklı bir forest içerisindeki bir domainde bulunan bir kaynağa ya da objeye ulaşmak istediğinizde size o kaynağın ya da objenin adresini veren ya da o kaynağa ulaşmanız için gerekli yönlendirmeleri yapan domain controller sunucusu global katalog server olarak adlandırılır. Global Catalog Server forest yapısına ait kütüğü oluşturan, tutan, sanki bir "muhtar" gibi çalışan ve forest yapısının haritasını oluşturan bilgisayardır. Forest'da Global Catalog server rolü sadece forest root DC'ye yani forest içerisinde ilk kurulan Domain Controller bilgisayarına otomatik olarak atanır. İhtiyacınıza göre Global Catalog rolü forest yapısındaki diğer DC bilgisayarlarına da atanabilir. Kullanıcılar açısından iki önemli işlevi vardır:

- Verinin lokasyonunu bilmeksizin, tüm forest içerisinde, Active Directory bilgilerine ulaşım.
- Netvvork ortamına katılırken; universal group üyeliğinin kullanılabilmesi.

Güven İlişkileri(Trust Relationships)

Farklı iki domain arasında bilgi ve kaynak paylaşımı amacıyla kurulan ilişkiye güven ilişkisi(trust relationship) adı verilir.Windows 2012/ 2008/ 2003/2000 networkünde iki domain aynı forest içerisinde ise otomatik olarak bu iki domain arasında güven ilişkisi otomatik olarak oluşur. Aynı forest içerisindeki domainler arasında otomatik olarak oluşan güven ilişkilerinin iki önemli karakteristik özelliği vardır:

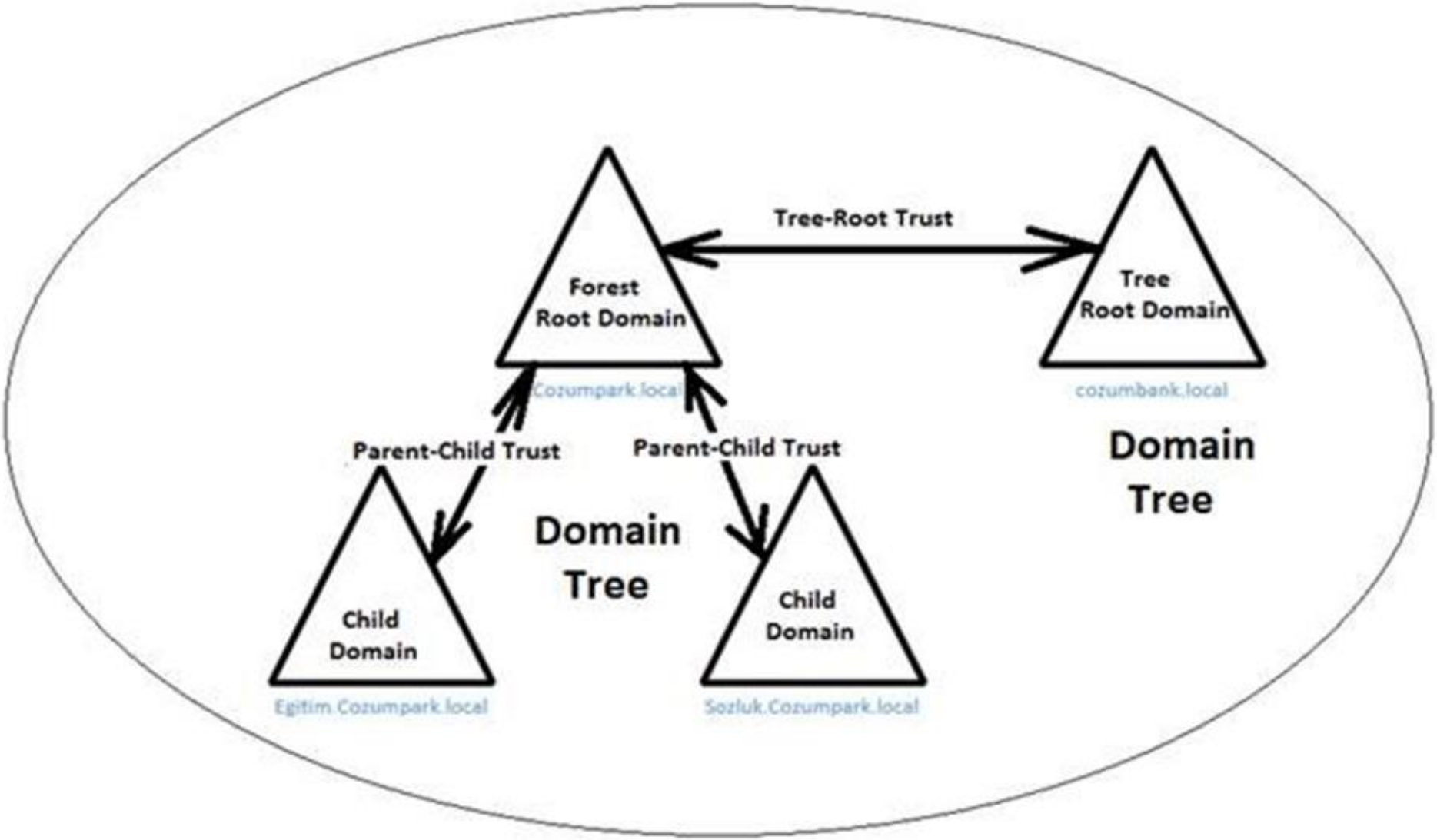
- Çift yönlü (two way)
- Geçişli (transitive)

Çift yönlü olması her iki tarafın da birbirinin kaynaklarına erişebilmesi anlamına gelmektedir. Geçişlilik ise, doğrudan güven ilişkisine sahip olmayan iki domainin her ikisinin parent domain ile kurdukları güven ilişkisi üzerinden birbirlerinin kaynaklarına erişmesi anlamına gelmektedir.

Diğer yandan aşağıdaki şekilde de görüldüğü gibi güven ilişkileri mantıksal olarak da kuruldukları yapılara göre de farklı isimlendirilmektedirler:

- Parent-Child Trust
- Tree-Root Trust

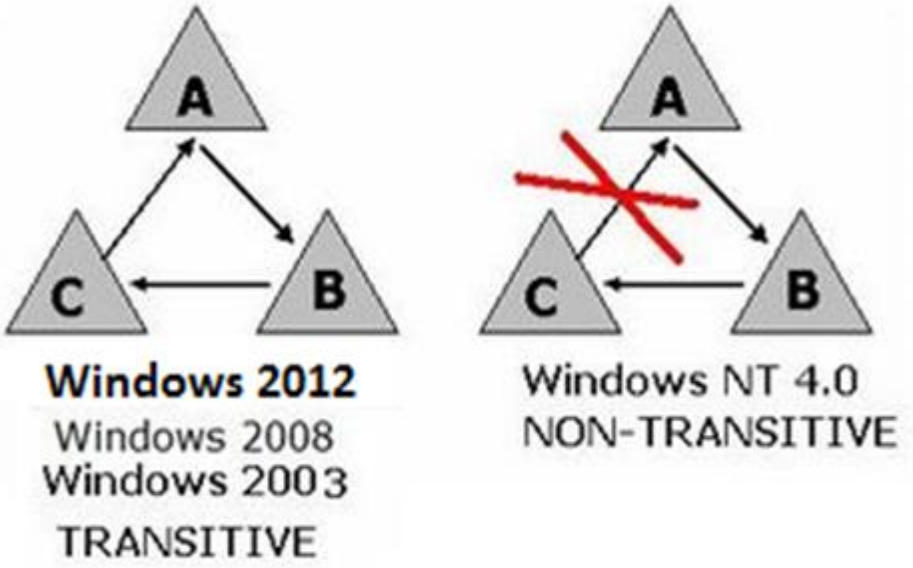
Parent-Child Trust---Tree-Root Trust



Parent-Child Trust, bir üst domain ile hemen o domain altındaki alt domain arasında kurulan güven ilişkisidir. Bu tip güven ilişkisi child domainden bakınca Parent Trust, parent yani üst domainden bakınca da Child Trust olarak görülecektir. Yani parent'ın child domaini ile ya da child domainin parent domaini ile kurduğu güven ilişkisi olacaktır. Bu güven ilişkisi çift yönlü ve geçişlilik özelliğine sahiptir. Örneğin yukarıdaki şekilde cozumpark.local isimli parent domain ile egitim.cozumpark.local ve sozluk.cozumpark.local domainleri arasındaki güven ilişkisi parent-child trust için güzel bir örnektir. Burada egitim ve sozluk domainlerinin doğrudan birbirleri arasında bir güven ilişkisi olmamasına rağmen geçişlilik özelliği ile birbirlerinin kaynaklarına erişebilirler.

Tree-Root Trust, forest root domain ile farklı isim alanı altında kurulmuş her domain tree'nin tree root domaini arasında oluşan güven ilişkisidir. Dolayısıyla aslında farklı domain tree'ler ve onların altındaki hiyerarşide kurulan child domainler yine aynı forest içerisindeki diğer domain tree altındaki child domainler tree-root trust hiyerarşisini kullanarak geçişlilik özelliği ile birbirlerinin kaynaklarına verilen yetkiler çerçevesinde ulaşabilirler. Dolayısıyla tree-root trust ilişkisi de yine çift yönlü ve geçişlilik özelliğine sahiptir.

Geçişlilik yani transitivity konusunu biraz daha açalım. Geçişli güven ilişkisi aşağıdaki şekildeki örnekte açık olarak görülmektedir.



A domaini B domainine güveniyor, B domaini de C domainine güveniyor. Böyle bir yapıda A domaini aynı zamanda C domainine de güvenmiş oluyor. Windows NT 4.0 domainlerinde kurulan güven ilişkisinde geçişlilik özelliği yoktu, yani NT 4.0 domainleri arasındaki güven ilişkisi non-transitive'dir. Dolayısıyla yukarıdaki örnekte A ve C domainlerinin birbirlerinin kaynaklarına erişebilmeleri için aralarında ayrıca güven ilişkisi kurulması gerekir.

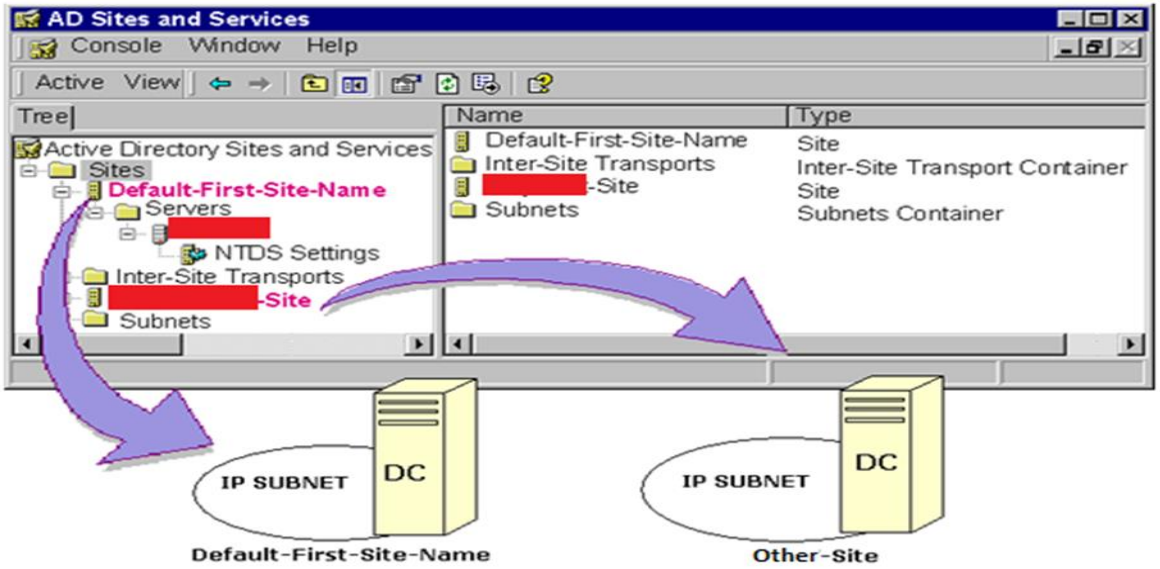
Fiziksel Yapı Bileşenleri

Active directory domainine ait fiziksel yapıyı ilgilendiren bileşenlerdir. Fiziksel yapıyı da iki ayrı kategoride inceleyeceğiz:

- Site
- Domain Controller

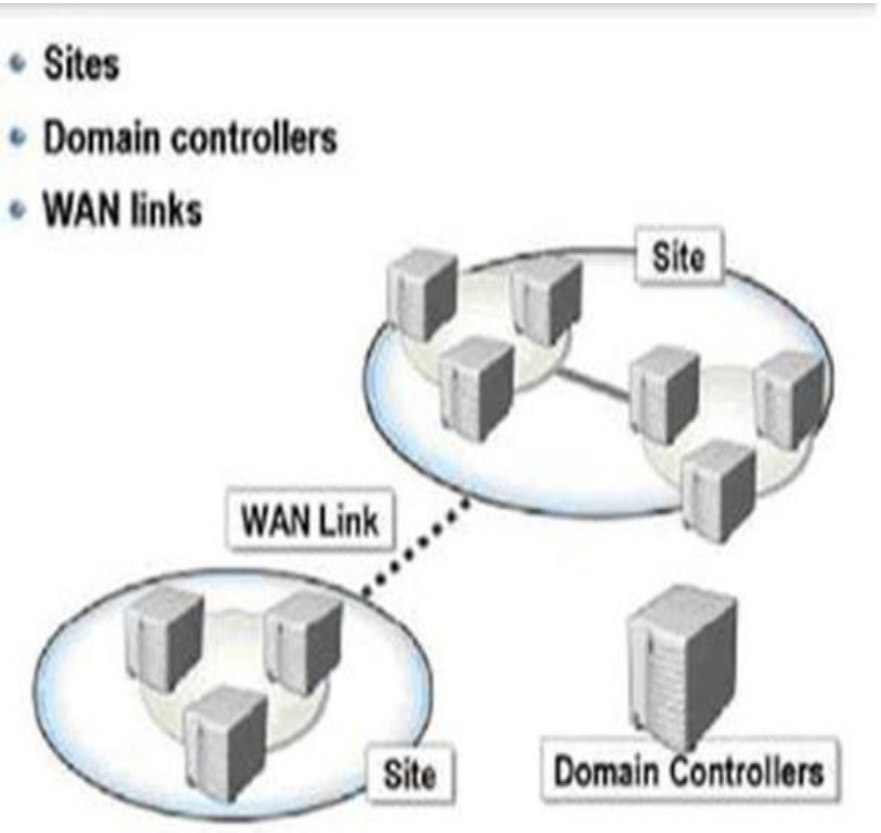
Site

Site, bir yada daha fazla ip subnetini içeren active directory yapılardır. Site, Windows 2012/2008/2003 domainleri içerisindeki, DC'ler arası replikasyon trafiğini ve süresini kontrol altına almak için oluşturulmuş yapılardır. Network içerisindeki ip subnetlerini siteler içerisinde tanımlayarak replikasyon trafiği de kontrol altına alınmış olur.



Active Directory kurulduktan sonra sitelerin yönetimi Administrative Tools içerisindeki Active Directory Sites and Services konsolu içerisinden yapılır.Site üzerinde yönetim yapma hakkı sadece Admins grubunun üyelerine aittir.

NOT:Active directory domainleri üçgen şekliyle, siteler de elips şekliyle gösterilirler.



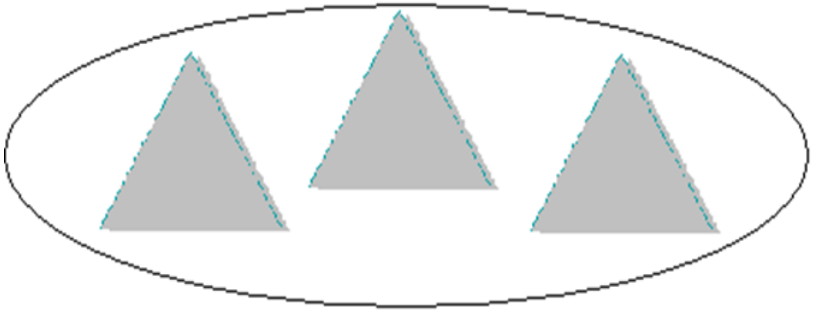
Bir Site, birbirlerine yüksek bant genişliğine sahip dış hatlarlar bağlanmış bir veya birden fazla IP (Internet Protocol) alt ağlarını ifade etmektedir. Site'ları doğru bir şekilde yapılandırarak kullanıcıların logon işlemlerinde oluşan ağ trafiğini ve replikasyon işlemleri sırasında oluşan yoğunluğu en aza indirgemek için Active Directory'nin alt ağlar arasındaki fiziksel bağlantıları en efektif şekilde kullanmasını sağlayabiliriz.

Site oluşturmaktaki başlıca sebepler şunlardır:

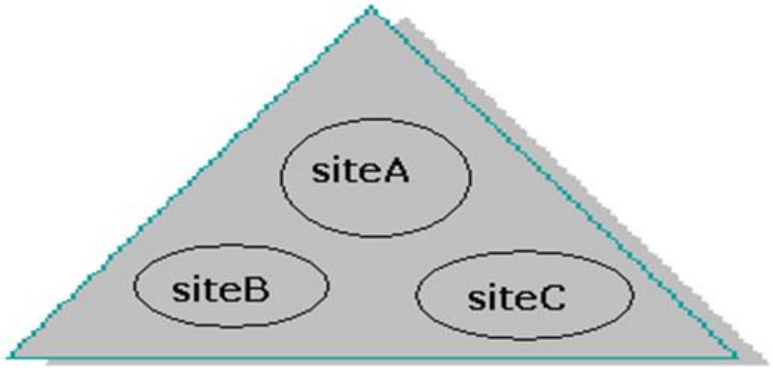
- Replikasyon trafiğinin optimize edilmesi
- Kullanıcıların logon olması esnasında en hızlı ve en güvenilir bağlantıyı kullanarak doğru Domain Controller'ı bulabilmeleri

Site

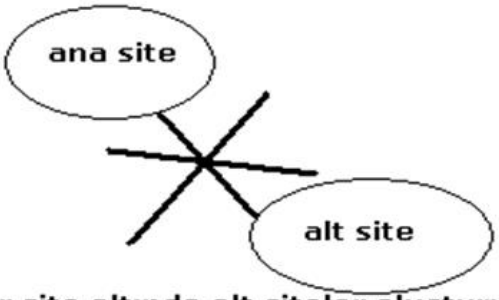
Yanda sitelerin karakteristiksel özellikleri listelenmiştir:



Bir site içerisinde birden fazla domain içerebilir.



Bir domain de birden fazla siteye bölünebilir



Bir site altında alt siteler oluşturulamaz.

Domain Controller

Domain yapısını kuran ve domain içerisindeki bütün objelerin ve kaynakların veritabanını depolayan bilgisayarlara DC(Domain Controller) adı verilir. DC, Active Directory bilgilerinin depolandığı, üzerinde Windows Server işletim sistemi çalışan bilgisayardır. Bir domain içerisinde kurulan bütün domain controller'lar üzerinde domain veritabanı bilgileri bulunur.DC'lerden biri üzerinde bir değişiklik yapıldığı zaman bu değişiklik aynı domain içerisindeki diğer DC bilgisayarlarına otomatik olarak çoğaltılır (replikasyon).Bir kullanıcı DC'lerden herhangi birisi üzerinde bir defaya mahsus oluşturulduktan sonra, bu diğer DC bilgisayarlarına replikasyon adı verilen bir mekanizma ile güncelleme yapılır.Bu mekanizma sayesinde domainde bulunan her DC bilgisayarı üzerinde domain bilgilerinin tutuldugu veritabanı kendini güncelleyerek diğer domain controller'ların bir kopyası oluşmuş olur. Dolayısıyla DC'lerden bir tanesi kapalı bile olsa kullanıcı domaine logon olmak istediğinde diğer DC'ler üzerinden kimlik kontrolü (authentication) yapılarak sisteme girmesi sağlanır.

Domain Controller

İlk domain controller'ın kurulumu ile domain yapısı oluşmuş olacaktır. Yedeklilik, ölçeklenebilme, yük dengeleme, yüksek erişilebilirlik gibi nedenlerden dolayı bir domainde en az iki adet domain controller olması gerekir. Dolayısıyla ilk kurulan domain controller'dan sonra bunun yanına additional domain controller rolüne sahip ilave domain controller'lar kurarak bu gereksinimler karşılanabilir. Domain controller ve additional domain controller sunucular hem yazılabilir hem de okunabilir özelliktedirler. DC:

1_Directory bilgilerinde değişiklik yapılmasına ve bu değişikliklerin aynı Domain içerisindeki diğer DC'ler ile replikasyonuna olanak sağlar.

2_Directory verilerini depolar.

3_Kullanıcıların logon işlemlerini yönetir.

4_Kimlik denetimi ile directory arama(search) işlemlerini gerçekleştirir.

Active Directory ve DNS

Active Directory ve DNS entegrasyonu Windows Server 2003 ile başlayan en önemli özelliklerinden biridir. Active Directory ve DNS, objelerin hem Active Directory objeleri hem de DNS domainleri ve kaynak kayıtları (Resource Records) olarak sunulabilecek şekilde benzer bir hiyerarşik isimlendirme yapısına sahiptirler. Bu entegrasyonun sonucu olarak Windows Server Ağındaki bilgisayarlar, Active Directory'ye özgü birtakım servisleri çalıştıran bilgisayarların yerini öğrenmek için DNS Sunucuları kullanmaktadırlar. Örneğin, bir client Active Directory'ye logon olmak veya herhangi bir kaynağı (yazıcı veya paylaşılmış bir klasör) dizin içerisinde aratmak için bilmesi gereken Domain Controller' IP adresini DNS Sunucu üzerinde SRV kayıtlarından öğrenmektedir. Active Directory'nin sorunsuz bir şekilde çalışması için DNS sunucuların SRV kayıtlarını eksiksiz bir şekilde barındırması gerekmektedir. SRV kayıtlarının amacı, client'lara logon esnasında veya herhangi bir kaynağa ulaşıyorken Domain Controller'ların yerlerini belirtmektir ve bu kayıtlar DNS sunucularda tutulur. SRV kayıtlarının olmadığı bir ortamda, client'lar Domain'e logon olamayacaklardır.

Ayrıca Windows Server , DNS bilgilerinin Active Directory veritabanı ile tümleşik olarak saklanmasına olanak vermektedir. Bu sayede DNS bilgilerinin replikasyonu daha efektif ve güvenli bir hale gelmektedir.

Windows Server , Active Directory organizasyonunu kurmadan, önce oluşturulacak olan Domain'in DNS altyapısını önceden oluşturmayı gerektirmektedir. Eğer oluşturulacak olan Domain'in DNS altyapısı kurulum öncesinden hazırlanmamışsa, kurulum esnasında da DNS altyapısı kurulabilir.