Active Directory

Active Directory Nedir?

Active directory bir dizin servisidir.

İçerisinde server (sucunu), client, printer ve user gibi bilgileri tutar. Aynı zamanda veri tabanı görevi görür.

AD içerisinde yer alan Group Policy yönetim aracı ile çeşitli kısıtlamalar yapabilir veya tek bir noktadan istediğimiz uygulamanın dağıtımını gerçekleştirebiliriz.

Kaynakların kontrolünü sağlar, yönetiminin merkezileştirir ve kolaylaştırır. Bu yüzden çok tercih edilen bir servistir.

Active Directory hizmeti:

Diğer dizin servislerine erişmek için kullanılan LDAP ile ağdaki kullanıcı nesneleri, bilgisayarlar ve hizmetler hakkında bilgi sağlar. Bu bilgileri güvenli bir veri tabanında saklar ve dizini yönetmek ve aramak için araçlar sunar.

Kullanıcı hesaplarını ve kaynaklarını yönetmeye izin verir, bir kuruluşun ihtiyaç duyduğu şekilde tutarlı politikalar uygular.

Secure Sockets Layer (SSL) ve Kerberos tabanlı kimlik doğrulama ilkelerini kullanarak güvenlik protokolü uygular.

Daha iyi ölçeklenebilirlik sağlamak için eş zamanlı güncellemeleri olan birden fazla sunucuda veri kullanılabilirliği avantajlarını sağlar.

Active Directory Özellikleri

Yönetilebilirlik

Ölçeklenebilirlik

Genişletilebilirlik

Güvenlik Entegrasyonu

Diğer Dizin Servisleriyle Birlikte Çalışabilme

Güvenli Kimlik Doğrulama ve Yetkilendirme

Group Policy ile Yönetim

Dns ve Dhcp gibi Servislerle Birlikte Çalışabilme Özelliği

Active Directory Yapısı

Mantıksal Yapısı

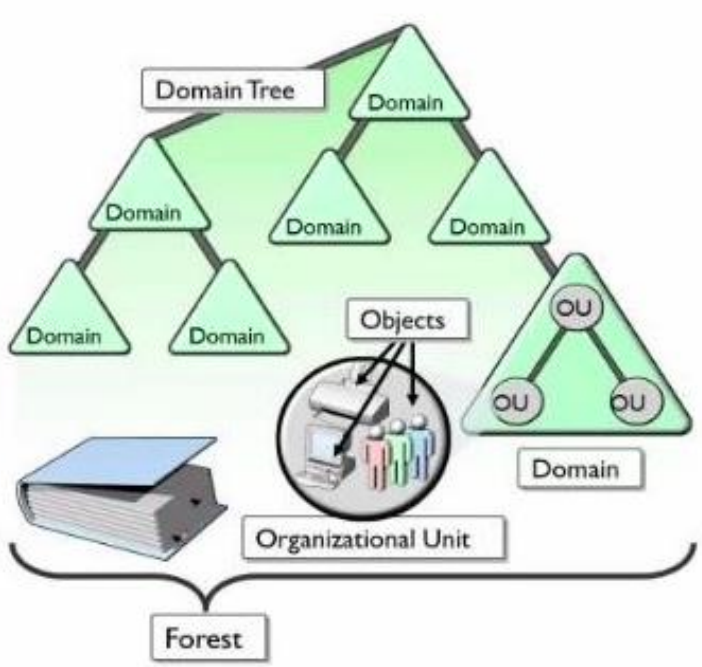
- Domain
- Organizational Unit
- Tree
- Forest
- Global Catalog
- Trust Relationship
- LDAP

Fiziksel Yapısı

- Domain Controller
- Sites

Mantıksal Yapısı

Mantıksal yapı AD içerisinde kullanıcı ve yönetici kapsamında hiyerarşik bir yapı kurulmasına olanak verir.



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

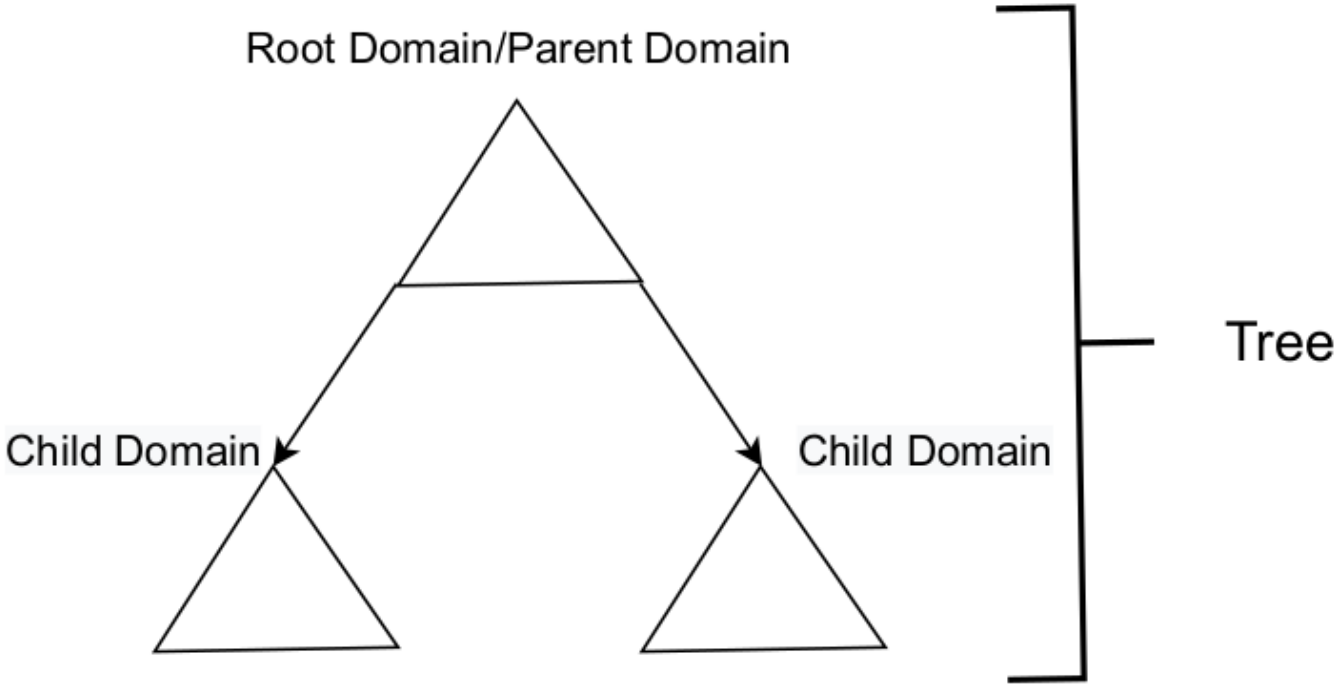
Domain

Active Directory’nin en temel bileşenidir. Domain sistem yöneticisi tarafından benzersiz bir isim seçilerek oluşturulmalıdır.

Tree

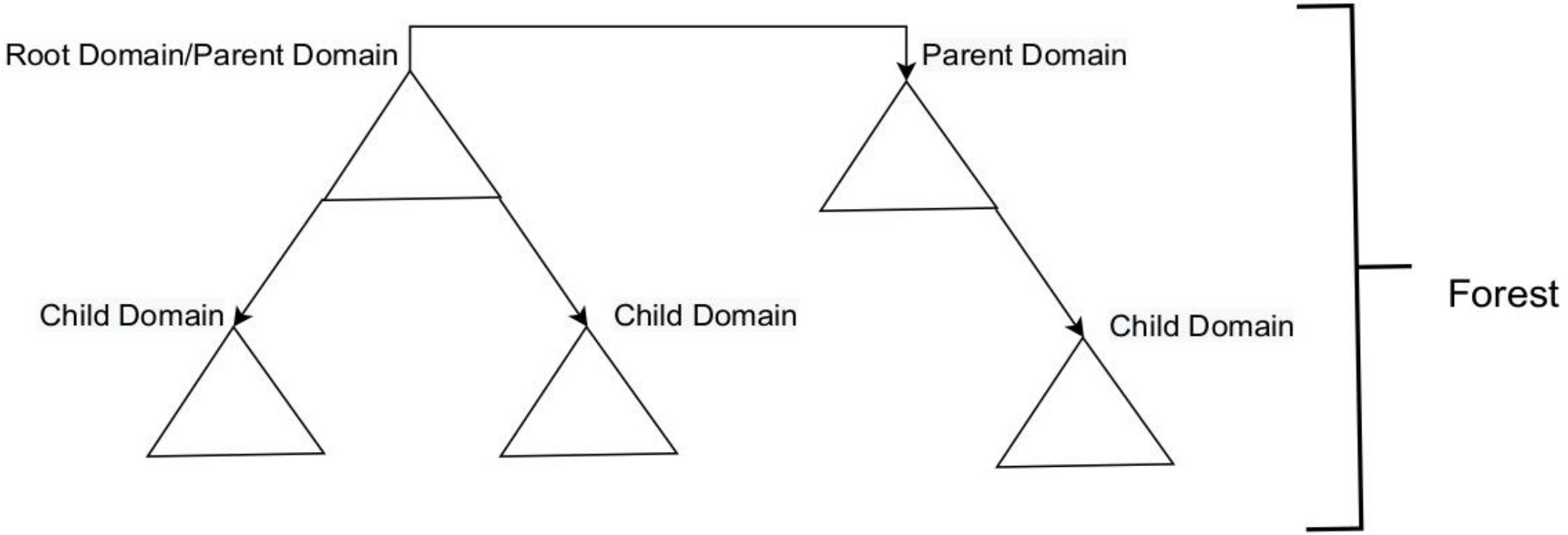
Yapısına yeni bir Domain eklendiği zaman, yeni eklenen Domain sondan eklendiği Domain'inin Child Domain'i durumunda olur ve eklendiği Domain de eklenen Domain için Parent Domain olur.

Yeni oluşturulan Child Domain'in ismi Parent Domain'den gelen isimle birleştirilir ve yeni oluşan Domain'in DNS ismi ortaya çıkar.



Forest

Birden fazla Tree’nin birleşmiş halidir.



OU (Organizational Unit)

Bir domain içerisindeki kullanıcıları, grupları veya bilgisayarları organize etmek amacıyla oluşturulmuş objelerdir. Organizasyonun ihtiyacını karşılamak ve yönetimi kolaylaştırmak noktasında objeleri gruplamak amacıyla kullanılır.

Global Catalog

Genelde ilk domain controller'dır. AD foresttaki her objeyi içerisinde bulundurur. Kullanıcıların foresttaki kaynakları bulmasına yardımcı olan dc'dir.

Trust Relationship

- One-way and two-way trusts
- Transitive and non-transitive trusts
- Tree-root trust
- Parent-child trust
- Shortcut trust
- External trust
- Forest trust
- Realm trust

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.

- Distinguished Name:
  Tüm Active Directory objeleri, network ortamında kendilerine ulaşılmasını sağlayan komple path içeren, distinguished name'e sahiptir.
  - CN=busrapc, OU=pardus, DC=pardus, DC=test DC=tr
  -
- Relative Distinguished Name:
  LDAP distinguished name içerisinde yer alır ve objeye ait eşsiz (unique) tanımlamayı içerir. Yani Active Directory içinde belirtilen Domain içinde tektir.
  - CN=busrapc, OU=pardus, DC=pardus, DC=test DC=tr

    pardus.test.tr içinde tek olan Relative Distingished Name busrapc'dir.

Fiziksel Yapısı

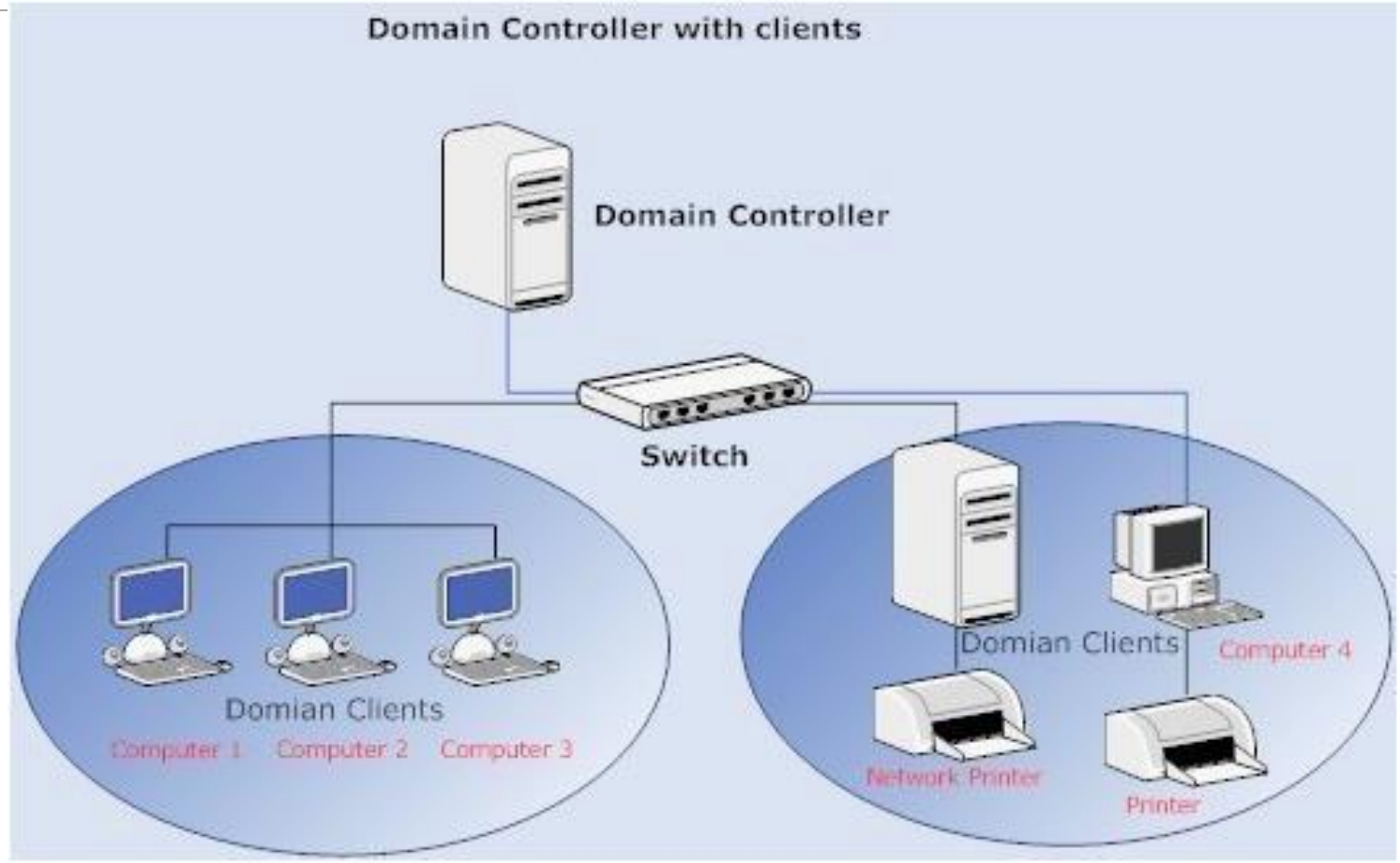
Active Directory'nin fiziksel yapısını; DC ve Site'lar oluşturur. Mantıksal yapı ile network kaynakları organize edilirken, fiziksel yapı ile network trafiğinin kontrolü ve konfigürasyonu gerçekleştirilebilir.

Domain Controller

Domain Controller, bilgisayar sistemlerindeki erişim isteklerini yanıtlayan ve sistemler üzerindeki kullanıcıları doğrulayan bir sistemdir.

Domain yapıları kullanıcıların ve kullanıcı bilgisayarlarının bir arada aynı ağ içerisinde hiyerarşik bir şekilde çalışmasını sağlayan yapılardır.

Domain yapısının beynidir.



Domain Controller’ın ana sorumlulukları ağa erişen kullanıcıların kim olduğunu, kullanıcıların doğrulanmasını ve hangi kullanıcının nereye erişebileceğini ya da erişemeyeceğini belirlemektir. Kullanıcılar, kendisine verilen yetki kadar sistemde hak sahibidir.

Domain Controller’ın önemli olmasının sebebi ağdaki akan verileri tanımlayan ve doğrulayan bir sistemdir. Bu verilerin içerisinde tüm bilgisayarların ismi, kullanıcı adları gibi önemli bilgiler vardır. Bu da Domain Controller’ı saldırganları kendisine çeken sistemlerden birisi haline getirmekte.

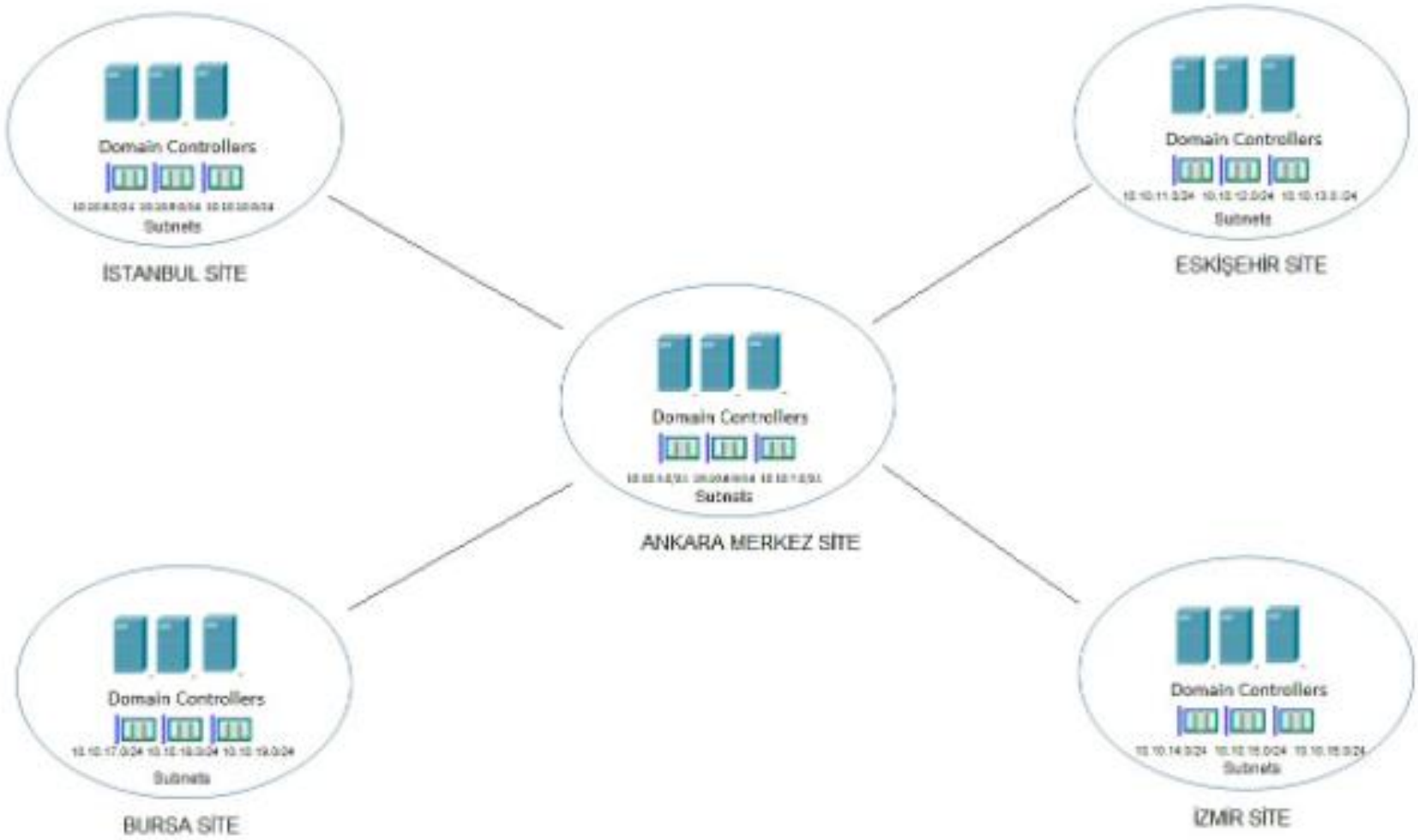
Domain Controller’ın avantajları;

- Merkezi bir kullanıcı yönetimi sağlar.
- Klasörler ve yazıcılar için kaynak paylaşımını aktifleştirir.
- Kullanıcı verilerini kriptolar.
- Geliştirilmiş güvenlik için kilitlenebilir ya da güvenlik önlemleri arttırılabilir.

Domain Controller’ın dezavantajları;

- Siber saldırı hedefi haline gelmektedir.
- Güvenliğinin sağlanmaması durumunda hacklenmesi söz konusu.
- Ağ, Domain Controller’ın ayakta kalmasına bağlıdır.

Sites


Domain Controllers
Subnets
İSTANBUL SİTE
Domain Controllers
Subnets
ESKİŞEHİR SİTE
Domain Controllers
Subnets
ANKARA MERKEZ SİTE
Domain Controllers
Subnets
BURSA SİTE
Domain Controllers
Subnets
İZMİR SİTE

Sites

Birbirlerine yüksek bant genişliğine sahip dış hatlarla bağlanmış bir veya birden fazla IP 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 esnasında en hızlı ve en güvenilir bağlantıyı kullanarak doğru Domain Controller'ı bulabilmeleri

AD FSMO (Flexible Single Master of Operation) Rolleri

Schema Master:

Active Directory içerisindeki objelerin özelliklerini düzenlememizi sağlar.

Active Directory şemasının yönetilmesinden ve tüm forestlardaki domainlerin DC'lerine replikasyonunun yapılmasından sorumludur. Her forest'da Schema Master rolünü üstlenen sadece bir DC bulunur.

Domain Naming Master:

- Domain isimlerini bünyesinde tutar. Domainlerin isimlerinin aynı olmasını engeller.

PDC Emulator:

Ağda bulunan dcler arasında replikasyon sağlar. Windows oturumlarını kontrol eder.

RID Master:

Ağda bulunan nesnelerin SID numarası vardır. Nesnelerin benzersiz SID numarası almasını sağlar ve çakışmayı önler.

Infrastructure Master:

Farklı domainden gelen kullanıcıların SID ayarlamalarını gerçekleştirir. Global catalog ile replikasyon sağlar.

Active Directory Authentication

Kimlik doğrulama, bir kullanıcının kimliğini tanıma ve kullanıcı bilgilerinin doğrulandığı bir süreçtir.

Kimlik doğrulama için kullanılan farklı protokoller vardır. Windows server işletim sistemleri

- Negitiote
- Kerberos Protokolü
- NTLM
- Schannel
- Digest

gibi kimlik doğrulama güvenlik desteği sağlayıcı arayüzleri (SSPI) uygular.

AD sunucu ile istemci arasında kimlik doğrulaması protokolü olarak Kerberos sürüm 5'i kullanır.

Kerberos Protokolü

Ağ üzerinde kullanıcıların şifrelerinin dolaşması güvenli olmadığı düşüncesiyle güvenlik zafiyeti oluşturacağı düşünülerek MIT tarafından geliştirilmiştir.

Kerberos, diğer sistemlerinde bağlı olduğu açık bir ağda, client ve server arasındaki kimlik doğrulamasını korumak için kullanılır.

Simetrik şifreleme anahtarını kullanır.

Kimlik doğrulama ticket'lar üzerinde gerçekleşir.

Ticket dağıtımını KDC (Key Distrubition Center) gerçekleştirir.

- UDP 88 portunu kullanır.

Kerberos Terimleri

Realm:

- Windows domainin Kerberos karşılığıdır.. Örneğin; PARDUS.TEST.TR

Principle:

- Windows domaindeki kullanıcıların karşılığıdır. Örneğin; busra.cagliyan@pardus.test.tr

KDC:

- Client ve server arasında güvenli bağlantı oluşturmada görevlidir. 3 bileşenden oluşur.
- **Veritabanı:** Tüm kimlik bilgileri veritabanı üzerinde tutulmaktadır.
- **Kimlik Denetim Sunucusu (AS):** Kimlik denetim işlemini başlatmakla sorumludur.
- **Ticket Granting Server(TGS):** Şifreli anahtarlar oluşturup kullanıcılara dağıtılmasını sağlar.

Ticket:

- Kullanıcıların ağa erişimlerini sağlar.

KERBEROS – ÇALIŞMA MEKANİZMASI

Kullanıcı

1.) Kullanıcı kimlik bilgilerini KDC'ye gönderip, TGT talebinde bulunur..

2.) Kimlik denetim servisi şifrelenmiş bir TGT ve oturum anahtarı gönderir.

3.) Kullanıcı, Ticket Granting Service (TGT) 'den sunucuya erişim talep eder.

4.) TGS şifrelenmiş oturum anahtarını ve bileti kullanıcıya gönderir.

Key Distribution Center

Veritabanı

5.) Kullanıcı bileti sunucuya gönderir.

6.) Sunucu, kullanıcının onayı için şifrelenmiş zaman damgasını gönderir.

Sunucu

Kerberos'un Çalışma Mantığı

1. Client makine kullanıcının username ve passwordünü şifreleyerek domain controllerdaki kdcye gönderir.
2. Kdc kendi veri tabanındaki bilgilerle kullanıcının bilgilerini karşılaştırır. eğer kullanıcının bilgileri varsa kdc kullanıcın üyesi olduğu grupların listesini çıkarır. global catalog üzerinden universal grouplarının listesi oluşturulur. Daha sonra session key ve ticket granting ticket üretir ve bunu kullanıcıya şifreleyerek gönderir.
3. TGT kullanıcının üye olduğu grupların listesi, kullanıcı adı ve ne kadar süre geçerli olacağı bilisini içerir. ve network üzerinde bir kaynağa erişmek istediğimizde ticket almak için kullanılır.
4. Böylece domaine logon olma işlemi tamamlanmıştır.
5. Client bilgisayar daha güvenli olması için sk ve tgt bilgilerini geçici hafıza üzerinde saklar.
6. Client bilgisayar aynı domaindeki bir server üzerindeki bağlantıya erişmek istediğinde elindeki tgt ile dc üzerindeki ticket granting service ile bağlantı kurar. TGS client pc ve server için session tickets üretir. Bu ticketler kaynağa erişmek isteyen bilgisayar, kaynağın üzerinde olduğu server, talebin ne zaman yapıldığı ve ticketlerin ne kadar süre geçerli olacağı bilgilerini içerir.
7. Client bu ticketı kullanarak kaynağa erişim sağlar. kaynağın bulunduğu serverda çalışan lsa(local security authority) servisi ticketı kullanarak bir access token oluşturur.
8. LSA kaynak üzerindeki access control list ile access tokendaki sidleri karşılaştırarak kullanıcının hangi haklara sahip olduğunu belirler.
9. LSA local ve auditing policy yönetimi, kullanıcılar için kimlik doğrulama ve access token oluşturma işlerinden sorumlu.