LDAP (Lightweight Directory Access Protocol)

LDAP, yani Hafif Dizin Erişim Protokolü, ağ üzerindeki dizin hizmetlerine erişmek ve bu hizmetleri yönetmek için kullanılan açık ve standart bir protokoldür. LDAP, özellikle kullanıcı bilgileri, kimlik doğrulama verileri, grup üyelikleri ve ağ kaynakları gibi bilgilerin merkezi bir dizin yapısında tutulmasını sağlar.

1. LDAP'ın Temel Amacı

LDAP'ın temel amacı, ağ üzerindeki kullanıcı ve kaynak bilgilerini merkezi bir dizin yapısında tutarak bu bilgilere hızlı, güvenli ve organize bir şekilde erişim sağlamaktır. Bu sayede sistem yöneticileri, kullanıcı hesaplarını, erişim izinlerini ve kaynakları tek bir merkezden yönetebilir.

2. LDAP'ın Tarihçesi

LDAP, 1990'lı yıllarda X.500 dizin hizmetlerinin daha hafif ve internet tabanlı bir versiyonu olarak geliştirilmiştir. X.500 protokolü karmaşık ve ağır bir yapıya sahipti; LDAP ise TCP/IP protokolü üzerinden çalışarak daha hızlı ve kolay bir kullanım sunmuştur.

3. LDAP'ın Yapısı

LDAP dizinleri hiyerarşik bir yapıya sahiptir. Bu yapı genellikle bir ağaç (tree) şeklinde organize edilir:

Root (Kök) Düğüm: Dizin yapısının en üst noktasıdır.

Organizasyon Birimleri (OU): Şirket departmanları, kullanıcı grupları gibi alt bölümleri temsil eder.

Nesneler (Entries): Kullanıcılar, bilgisayarlar, yazıcılar gibi varlıkları temsil eder.

Öznitelikler (Attributes): Her nesneye ait bilgiler (örneğin, ad, soyad, e-posta adresi, telefon numarası).

Her nesne, kendine özgü bir DN (Distinguished Name) ile tanımlanır.

4. LDAP Protokolü Nasıl Çalışır?

LDAP istemcisi, LDAP sunucusuna bağlanarak dizin verilerine erişim sağlar. Bu erişim şu işlemleri kapsar:

Arama (Search): Belirli kriterlere göre dizin içinde veri arama.

Okuma (Read): Belirli bir nesnenin özniteliklerini görüntüleme.

Yazma (Write): Yeni nesne ekleme veya mevcut nesneyi güncelleme.

Silme (Delete): Nesneleri dizinden kaldırma.

Kimlik Doğrulama (Bind): Kullanıcının kimliğini doğrulama işlemi.

5. LDAP Kullanım Alanları

LDAP, birçok farklı sistemde ve uygulamada kullanılmaktadır:

Kimlik Doğrulama: Kullanıcıların sisteme giriş yaparken doğrulanması.

Tek Noktadan Giriş (SSO): Bir kez giriş yaparak birden fazla uygulamaya erişim.

E-posta Sistemleri: Kullanıcı bilgilerini merkezi dizinden çekme.

Ağ Kaynaklarına Erişim: Yazıcılar, dosya sunucuları gibi kaynaklara erişim kontrolü.

Kurumsal Uygulamalar: CRM, ERP gibi sistemlerde kullanıcı yönetimi.

6. LDAP Sunucuları

LDAP protokolünü destekleyen birçok sunucu yazılımı mevcuttur:

Sunucu Adı	Açıklama
OpenLDAP	Açık kaynaklı ve yaygın kullanılan LDAP sunucusu
Microsoft Active Directory	LDAP protokolünü destekleyen Microsoft'un dizin hizmeti
Apache Directory Server	Java tabanlı açık kaynak LDAP sunucusu
389 Directory Server	Red Hat tarafından geliştirilen LDAP sunucusu

7. LDAP ve Güvenlik

LDAP, güvenli bağlantılar için SSL/TLS protokollerini destekler. Bu sayede veriler şifrelenerek iletilir ve kimlik doğrulama işlemleri güvenli hale gelir. Ayrıca erişim kontrol listeleri (ACL) ile hangi kullanıcıların hangi verilere erişebileceği belirlenebilir.

8. LDAP ile İlgili Kavramlar

DN (Distinguished Name): Her nesnenin dizin içindeki tam adresi.

RDN (Relative Distinguished Name): Nesnenin bulunduğu konuma göre göreli adı.

Schema (Şema): Dizin içinde hangi tür nesnelerin ve özniteliklerin bulunabileceğini tanımlar.

LDIF (LDAP Data Interchange Format): LDAP verilerinin dışa aktarımı ve içe alımı için kullanılan metin tabanlı format.

9. LDAP Sorgu Örneği

Bir LDAP sorgusu şu şekilde olabilir:

Code

```
ldapsearch -x -b "dc=example,dc=com" "(uid=ahmet)"
```

Bu sorgu, "example.com" alanında "ahmet" kullanıcı kimliğine sahip nesneyi arar.

10. Avantajları ve Dezavantajları

Avantajlar:

Merkezi yönetim sağlar.

Açık standarttır, birçok sistemle uyumludur.

Hızlı ve verimli arama yapısı sunar.

Dezavantajlar:

Yapılandırması karmaşık olabilir.

Güvenlik ayarları dikkatle yapılmalıdır.

Büyük dizinlerde performans sorunları yaşanabilir.