LDAP (Lightweight Directory Access Protocol) Nedir ve Ne İçin Kullanılır?

I. Tanım ve Temel Kavramlar

LDAP (Lightweight Directory Access Protocol), Türkçe karşılığıyla **Hafif Dizin Erişim Protokolü** anlamına gelir. TCP/IP protokolü üzerinde çalışan, bir ağ üzerindeki dizin hizmetlerine erişmek, bu hizmetlerdeki bilgileri sorgulamak ve yönetmek için kullanılan bir uygulama katmanı protokolüdür.

A. Dizin Hizmeti (Directory Service) Nedir?

LDAP'ı anlamak için öncelikle **dizin hizmeti** kavramını anlamak gerekir. Dizin hizmeti, ağ üzerindeki kaynaklara (kullanıcılar, gruplar, bilgisayarlar, yazıcılar, e-posta adresleri, telefon numaraları vb.) ait bilgileri merkezi ve hiyerarşik bir yapıda depolayan bir veritabanı türüdür.

Bu dizin, geleneksel veritabanlarından farklıdır; **okuma ve arama (Read/Search)** işlemlerini çok hızlı gerçekleştirmek üzere optimize edilmiştir, ancak **yazma/güncelleme (Write/Update)** işlemleri daha az sıklıkta yapılır.

B. Neden "Hafifletilmiş" (Lightweight)?

LDAP, daha eski ve karmaşık olan **X.500 DAP (Directory Access Protocol)** protokolünün daha basit ve TCP/IP ağlarına uygun, daha az sistem kaynağı tüketen bir versiyonu olarak tasarlanmıştır. Bu sadeleştirme sayesinde masaüstü bilgisayarlardan mobil cihazlara kadar geniş bir alanda kullanılabilmektedir.

II. LDAP'ın Yapısı ve Çalışma Prensibi

LDAP, bilgileri geleneksel veritabanlarındaki gibi tablolar halinde değil, bir ağaç yapısı veya ters çevrilmiş bir ağaç yapısı (hiyerarşi) olarak organize eder. Buna **Dizin Bilgi Ağacı (Directory Information Tree - DIT)** denir.

A. Hiyerarşik Yapı (DIT)

Bilgiler, kök düğümden başlayarak dallanan ve yapraklanan bir hiyerarşi ile tutulur. Bu yapı, gerçek dünya organizasyonlarını taklit eder:

- **Kök Düğüm:** Ağacın en tepesi.

- **Organizasyonel Birim (OU):** Departmanlar, kullanıcılar veya gruplar gibi alt kategorileri temsil eder.
- **Etki Alanı Bileşeni (DC):** Alan adlarını (domain) tanımlar (ör: `dc=sirketim, dc=com`).
- **Girdi (Entry):** Ağaçtaki bireysel nesnelerdir (ör: bir kullanıcı, bir yazıcı). Her girdi, onu tanımlayan niteliklere (Attributes) sahiptir (ad, soyad, e-posta, parola).
- **Ayırt Edici Ad (Distinguished Name - DN):** Ağaçtaki bir girdinin benzersiz ve tam yoludur (ör: `cn=Ahmet Yilmaz, ou=Muhasebe, dc=sirketim, dc=com`).

B. İstemci-Sunucu Mimarisi

LDAP, bir istemci-sunucu protokolüdür:

1. **LDAP Sunucusu (DSA - Directory System Agent):** Dizin hizmetini barındırır ve DIT verisini saklar. (Örn: Microsoft Active Directory, OpenLDAP). Varsayılan olarak TCP 389 portunu kullanır.
2. **LDAP İstemcisi:** Uygulamalar veya sistemlerdir. Sunucuya bağlanır ve arama, kimlik doğrulama veya veri değiştirme taleplerini LDAP protokolü üzerinden gönderir.

III. LDAP Ne İçin Kullanılır?

LDAP'ın birincil kullanım amacı, **merkezi kimlik doğrulama (Authentication)** ve **yetkilendirme (Authorization)** sağlamaktır.

1. Merkezi Kimlik Doğrulama (Single Sign-On - SSO)

LDAP'ın en önemli görevi budur. Bir kullanıcı, farklı uygulamalara (e-posta, ERP, CRM, intranet) giriş yaparken her biri için ayrı bir kullanıcı adı/şifre yerine, **tek bir merkezi hesap** kullanabilir.

- Kullanıcı sisteme giriş yapmak istediğinde, uygulama (istemci) LDAP sunucusuna sorgu gönderir.
- LDAP sunucusu (dizin hizmeti), kullanıcının kimlik bilgilerini (parola dahil) dizinde arar ve doğrular.
- Doğrulama başarılı olursa, uygulama kullanıcıya erişim izni verir.

2. Dizin Bilgisi Yönetimi

Kullanıcıların veya diğer ağ kaynaklarının tüm bilgilerini (telefon numarası, ofis konumu, güvenlik grupları) tek bir yerde tutmak ve gerektiğinde uygulamalara sunmak. Bu, ağ yönetimini büyük ölçüde kolaylaştırır.

3. Yetkilendirme

Kimlik doğrulamasının ötesinde, kullanıcının hangi güvenlik gruplarının (Group) üyesi olduğunu sorgular ve uygulamalar bu bilgiye dayanarak kullanıcıya hangi kaynaklara erişim izni vereceğine karar verir.

4. Diğer Kullanımlar

- **E-posta İstemcileri:** Adres defterlerini dizin hizmetinden çekmek.
- **Otomatik Ağ Yapılandırması:** IP atama sistemlerinin (DHCP) ve ağ cihazlarının kullanıcı bilgilerini merkezi dizinden alması.

IV. Güvenlik Notu: LDAP vs. LDAPS

LDAP protokolü, varsayılan olarak şifreleme kullanmaz (TCP 389). Bu durum, ağdaki dinleme saldırılarına karşı hassas olduğu anlamına gelir. Bu nedenle, parolaların ve hassas bilgilerin güvenli bir şekilde iletilmesi için genellikle **LDAPS (LDAP over SSL/TLS)** kullanılır. LDAPS, iletişimi şifreleyerek veri gizliliğini ve bütünlüğünü sağlar (Varsayılan olarak TCP 636 portunu kullanır).