LKD
Şenlikleri
2002

# Kurumsal Yönetimde Dizinler, LDAP ve Yeni Dünya Düzeni!

**Oğuz YILMAZ**
**Teknoloji Danışmanı**
*oguz.yilmaz@gantek.com*



- Dizin nedir?
- Dizinler ve Veritabanları (VT)
- Dizin hizmetleri tarihçesi-X.500, LDAP
- LDAP Nedir?
- LDAP Veri Yapısı
- Neden LDAP?
- LDAP nasıl çalışır?
- Adlandırma ve şemalar
- Kurumsal Uygulama alanları
- Gelecekte LDAP
- İnternet bağlantıları

# *Dizin nedir?*

- "Belirli türden nesnelerin oluşturduğu küme ve bu küme üzerinde sorgulama imkanı sağlayan yapı"
  - Telefon rehberi
  - Personel kimlik bilgileri
  - Yerel ağ üzerindeki bilgisayarlara ilişkin kayıtlar
  - Kurumsal BT kullanıcı envanterleri

- Dizin Hizmeti:

  Nesneleri saklamak, sorgulamak ve yönetmek için kullanılan, bilgisayar ağındaki bir bilgi kaynağıdır.

- Veritabanı Nitelikleri:
  - Yapısal depolama
  - Depolanan nesneler arasında karmaşık ilişkiler(Relational)
  - Genellikle merkeziyetçi
  - Tümüyle kullanıcı tarafından tanımlanan şema(lar)
  - *Transaction* desteği
- Dizin Nitelikleri:
  - Yapısal depolama
  - Depolanan nesneler büyük ölçüde bağımsız; hiyerarşik düzenlenmiş
  - Genellikle dağıtık
  - Sabit çekirdek şema ve genişletilmesi imkanı

- Veritabanı Avantajları:
  - Nesneler arasında karmaşık ilişkilere imkan
  - Transaction desteği
  - Denenmiş teknolojiler ve gerçekleştirimler
  - Güncelleme ve ekleme ağırlıklı işlemlerde yüksek performans

- Dizin Avantajları:
  - Dağıtık yapısı
    - Uygun maliyetli dağıtık yapılar ve daha iyi replikasyon
  - Çekirdek şemanın varlığı
    - İstemciler dizinle ilgili “temel” bilgiye sahip
    - Ortak ve üretici-bağımsız dizin erişim protokolü mümkün

- Yazmadan daha çok okuma yapılan uygulamalarda.
- Uygulama doğası birisini seçmeye zorlayabilir:
  - Veriler arasında bağlara ihtiyaç duyan yapılar için VT
    - ERP, Muhasebe vb.
  - Dağıtık çalışmaya ihtiyaç duyan yapılar için Dizin
    - Kurumsal ya da küresel e-posta adres defteri
    - DNS sistemi
    - PKI altyapıları
- Bazı uygulamalar her ikisini de mümkün kılabilir:
  - Telefon rehberi

## *Dizin Hizmetleri Tarihçesi*

- ISO-ITU standardı: X.500 (1988,1993,1997)
  - Bu dizine erişim için de DAP(Directory Access Protocol) X.500 içinde tanımlı.
  - Örnek: Kanada Hükümeti. “Who’s Who” çalışan dizini. (Siemens Nixdorf DirX)
- LDAP(Lightweight Directory Access Protocol)
  - X.500 dizin erişim protokolünün hafifletilmişi (X.500.lite)
  - Michigan Üniversitesi’nde geliştirildi
  - Dizinlere erişim için IETF standart protokolü
  - Çeşitli üreticilerin ürettikleri LDAP-benzeri dizin erişim arabirimlerinin yanında bir endüstri standardı
  - X.500 bilgi modelini kullanıyor
  - RFC 1777 (LDAPv2) ve RFC 2251 (LDAPv3) ile tanımlı

# *LDAP Nedir?*

- LDAP(Lightweight Directory Access Protocol)
  - Dizindeki bilgiye erişim için bir protokol
  - Dizindeki bilginin karakterini ve formunu belirleyen bir bilgi modeli
  - Bilginin nasıl organize edildiğini belirleyen bir isim uzayı
  - Verinin nasıl dağıtılacağını ve bilgiye nasıl referans gösterilebileceğini gösteren bir dağıtık model

## *LDAP veri yapısı*

- Veri yapısı nesne tabanlı ve sıradüzensel
- Miras alma yolu ile çocuk sınıflar (*objectclass*) türetilebiliyor
- Her nesne, nitelikler(attribute) ve değerlerden(value) oluşuyor
- Her nitelik için birden fazla değerin atanması mümkün
- Nitelikler metin ya da *binary* olabiliyor
  - Büyük *binary* içerik yerine içeriğin URL' inin saklanması öneriliyor
- Depolanan her nesnenin biricik bir tanımlayıcısı (*distinguished name - DN*) var
  - DN'ler ülke, şehir, kurum, birim ve nesne ilk adı gibi bileşenlerden oluşuyor

dn: uid=oguz,ou=People,dc=ankara,dc=gantek,dc=com

## *Neden LDAP?*

- LDAP, IETF(Internet Engineering Task Force) değişim kontrolü altında. İnternet ihtiyaçlarına kolay adaptasyon.
- X.500 ün aksine TCP/IP destekler. =>internet
- Açık protokol. Dizini tutan sunucu tipi önemsiz.
- Protokol ve bilgi modeli genişletilebilir.
- LDAPv3 UTF-8 Evrensel Yazı tipi
- SASL yetkilendirme kütüphanesi üzerinden yetkilendirme

- LDAP şunları bilir:
  - Bağlan (bind)
  - Ara (search)
  - Karşılaştır (compare)
  - Yarat (create)
  - Ata (assign)
  - Değiştir (modify)
  - Sil (delete)

- Dizin sıradüzeni ve içeriği şema dosyaları ile tanımlanır.

  core.schema dosyasından:

  ***objectclass(2.5.6.6 NAME 'person' SUP top STRUCTURAL MUST ( sn $ cn ) MAY ( userPassword $ telephoneNumber $ seeAlso $ description ) )***

  ---

  ***attributetype ( 0.9.2342.19200300.100.1.1 NAME ( 'uid' 'userid' ) DESC 'RFC1274: user identifier' EQUALITY caseIgnoreMatch SUBSTR caseIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{256} )***

- Dizindeki her girdinin benzersiz(unique) olması beklenir.
- Dizindeki tüm girdiler, farklı birer dn(distinguished name)'e sahiptir.

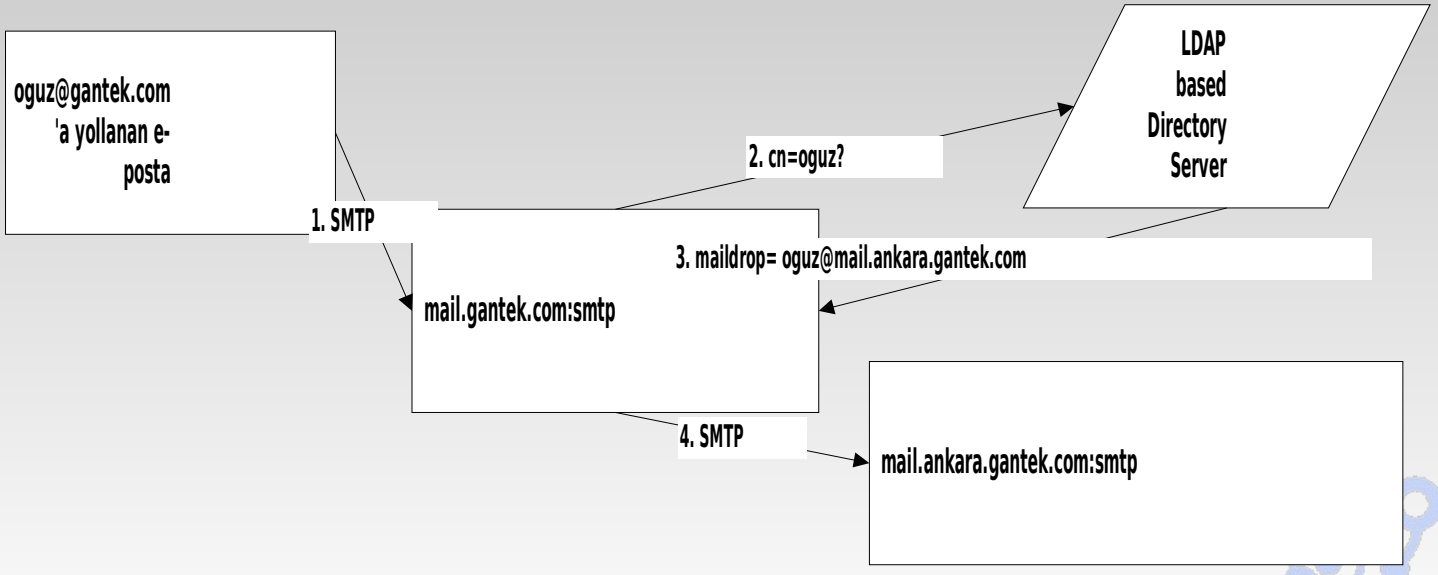
- LDIF(LDAP Data Interchange Format)
  Adres kitabı girdisi içeren örnek bir LDIF dosyası bölümü :

***dn:*** *cn=Oguz YILMAZ,ou=Staff,dc=ankara,dc=gantek,dc=com*
***cn:*** *Oguz YILMAZ*
***givenname:*** *Oguz*
***sn:*** *YILMAZ*
***title:*** *Sistem Destek Mühendisi*
***o:*** *GANTEK*
***ou:*** *Teknik Servis*
***telephonenumber:*** *(312)446 78 00*
***extension:*** *118*
***OfficeFax:*** *(312)446 36 66*
***mobile:*** *(532)xxx xx xx*
***roomnumber:*** *?*
***mail:*** *oguz.yilmaz@gantek.com*
***otherMailbox:*** *oguz@ieee.metu.edu.tr*
***postalAddress:*** *?*
***homepage:*** *http://oguz.ieee.metu.edu.tr/*
***objectClass:*** *gantek*
***objectClass:*** *person*
***objectClass:*** *organizationalPerson*
***objectClass:*** *inetOrgPerson*
*# Base64 encoded JPEG photo*
***jpegPhoto::*** */9j/4AAQSkZJRgABAAAAAQABAAD/2wBDABALD*
*A4MChAODQ4SERATGCgaGBYWGDEjJR0oOjM9PDkzODdASFxO*

- Bağlantı Yönetimi
  - Adres Kitapları
  - Kartvizitlikler
- Sistem Yönetimi:
  - /etc/{fstab, group, hosts, services...}
  - Microsoft Active Directory: Aygıtlar vb.
- Yetkilendirme:
  - LDAP üzerindeki tutulan şifreler üzerinden yetkilendirme
- Doküman Yönetimi:
  - Tüm dökümanlara uzaktan erişim
  - Aynı dökümandan birden fazla olmasını engeller

- Programlama:
  - Kod parçalarını LDAP sunucu üzerinde tut
  - SQL betiklerini dizine koy ve dünyanın istediğin yerinden çağır
- Netscape Roaming:
  - Kullanıcıların Netscape'deki kullanıcı ayarlarını ve sık ziyaret edilenlerini (bookmarks) sunucuda sakla
- Takvim Uygulamaları:
  - Sunucuda saklanan takvimler
  - Grup takvimleri
- Sayısal Sertifika Servisleri
- Yemek Kitabı:
  - : )

- Sendmail:
  - "/etc/mail/aliases" ve "/etc/mail/virtusertables ile yapılan ileti yönlendirmelerini LDAP ile yap. Sendmail 8.10 dan itibaren LDAP özellikleri mevcut.



- Birleştirilmiş veri (Unified data):
  - Kurumsal Yönetim
    - HR – insan kaynakları yönetimi
    - ERP – kurumsal kaynak planlaması
    - CRM – müşteri ilişkileri yönetimi
    - DM – döküman yönetimi
    - MM – dolaşabilirlik(mobility) yönetimi
    - Yetkilendirme – belirleme(identification) servisleri

- Bizim Çikolata A.Ş.:
  - 2000 çalışan
  - Her hafta 20 yeni çalışan
  - Merkez: Ankara
  - Bölge ofisler: İstanbul, İzmir
  - Fabrikalar: Aksaray, Konya
  - Satış ofisleri: Kırgızistan, Moskova, Suudi Arabistan

# *Uygulama Alanları – Bizim Çikolata*

- Sorunlar:
  - Hızlı büyüme
  - Sık insan değişimi, güvenlik kaygıları
    - Her bir insanın tüm çıkış işlerinin yapılması: 4 gün
  - Kullanıcı ihtiyaçları
    - Hangi oda?
    - Dahilisi ne idi?
  - 10'dan fazla internet-intranet sunucusu
    - Farklı hesaplar
  - İlerisi için 10,000 müşterileri için extranet kurmak istiyorlar
    - Müşteri bilgi güncelleme
    - Hesap durumları
    - Haberleşme
    - Stok vb.

- Sorunlar:
  - BiM Problemleri
    - Kullanıcı aliasları
    - İleti listeleri, gruplar
    - Sistem hesapları, kullanıcı bilişim bilgileri(şifre, PKI vb.)
  - Kurumsal kaynaklara erişim denetlemesi
    - Telefonlar
    - Giriş Çıkışlar
    - Dial-up erişimi
    - Buzdolabı !
  - Birimler arasında denetli veri paylaşımı
    - Yönetim – insan kaynakları – muhasebe – yerel yönetimler
  - Hiyerarşi ve buna göre politikalar

- Çözüm: **Dizin Tabanlı Kurumsal Yönetim**
  - Güvenilirlik ve yüksek edinilebilirlik ve bölge istekleri doğrultusunda coğrafyaya yayılmış dizin sunucular
  - Yalnızca istenen veriler coğrafyalara güncellenir. Çift taraflı.
  - BiM tüm sistemden sorumlu
  - Her bölge kendi bilgisinden sorumlu. Diğer bilgilere erişim denetli
  - İnsan Kaynakları ana verilerin girişini yapar.
  - Bim yalnızca görebileceklerini görür.
  - Kurum portalından tüm çalışanlar birbirlerinin uygun bilgilerine ulaşabilir.
  - Güvenlik sistemleri dizinde tanımlı erişim kontrol listeleri ile entegre edilir. (giriş, pbx ...)

- Çözüm: **Dizin Tabanlı Kurumsal Yönetim**
  - Tüm sistem sunucuları ve bilgisayarlara tek login. ACLler.
  - Bir çalışanın kurum sisteminden tamamen silinmesi: 5 dakika.
  - Veri paylaşımı ile BiM üzerindeki yük hafifler.
  - Her türlü veri denetli olarak dışarı aktarılabilir. (ERP...)

# Uygulama Alanları – Netscape Addressbook

- Netscape Adres Defteri
- Kullanılacaklar:

OpenLDAP 2.0.7 (www.openldap.org, www.rpm.org)
Netscape Communicator 4.75(www.netscape.com)
OpenLDAP 2 Administrators Guide

- **OpenLDAP kurulumu**
  - **ftp://ftp.rpmfind.net/linux/Mandrake-devel/cooker/cooker/Mandrake/RPMS/openldap-2.0.7-5mdk.i586.rpm**
  - **rpm –i openldap-2.0.7-5mdk.i586.rpm**
  - **/etc/openldap/slapd.conf ‘u düzenle:**

**değiştir:**

```
#suffix      "dc=dizin, dc=com“
#suffix      “o=dizin, c=TR”
suffix       "o=dizin“
#rootdn      "cn=Manager, dc=dizin, dc=com“
rootdn       "cn=Manager, o=dizin“

rootpw       123

# Indices to maintain
index cn,sn,uid pres,eq
index objectclass pres,eq
```



- **OpenLDAP kurulumu**
  - **ekle:**
    **include /etc/openldap/schema/cosine.schema**
    **include /etc/openldap/schema/inetorgperson.schema**
    **include /etc/openldap/schema/nis.schema**
    **include /etc/openldap/schema/misc.schema**
  - **yürüt:**
    **/etc/rc.d/init.d/ldap start**
  - **kontrol et:**
    **ps aux |grep slapd**

    **root 8890 0.0 0.3 3444 840 ? S Apr06 0:00 slapd**

# Uygulama Alanları – Netscape Addressbook

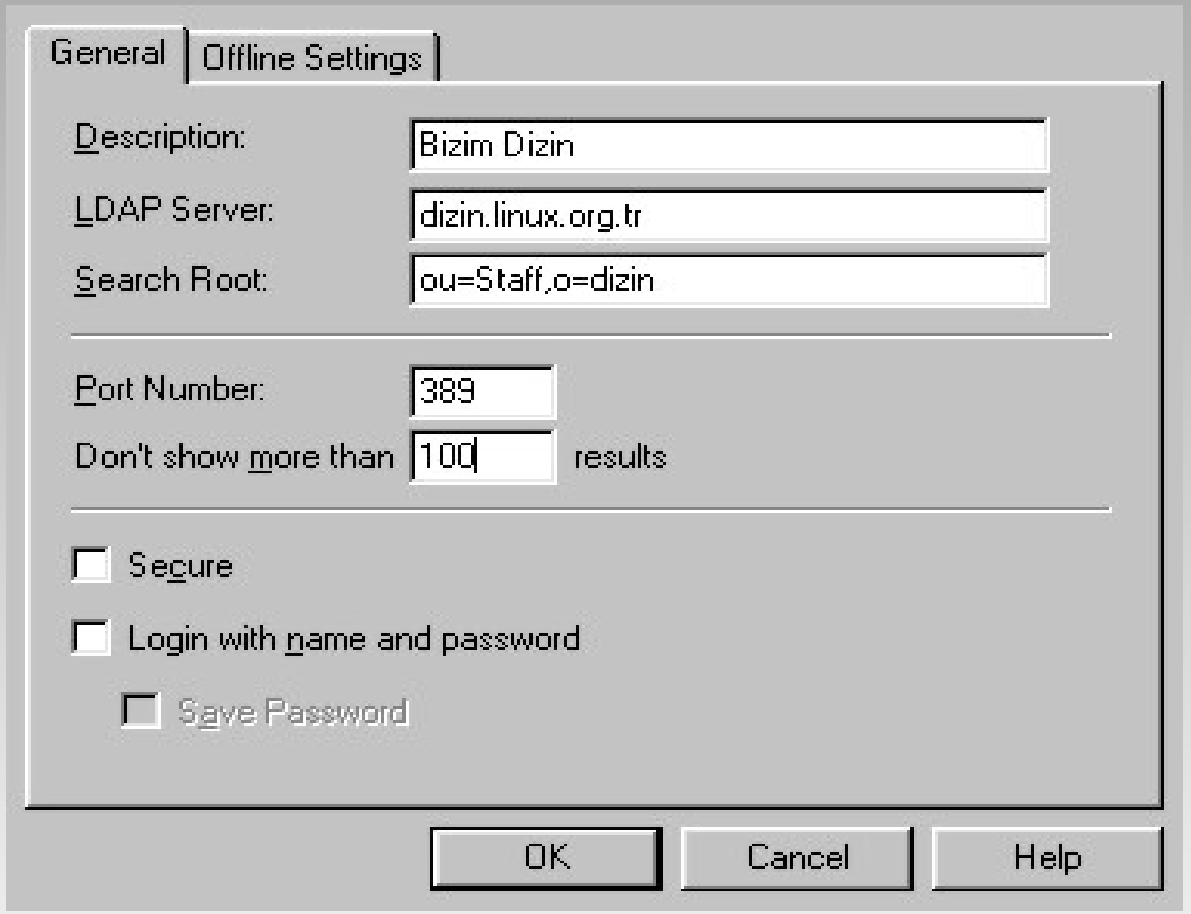
- **Ldif dosyası hazırla:**
  **dizin1.ldif isminde:**

```
dn: o=dizin
objectclass: dizin

dn: ou=Staff, o=dizin
objectclass: dizin
objectclass: organizationalUnit

dn: cn=Oguz Yilmaz,ou=Staff,o=dizin
cn: Oguz Yilmaz
givenname: Oguz Yilmaz
sn: Yilmaz
o: Dizin
ou: Teknik Servis
telephonenumber: (312) 446 78 00
roomnumber: ?
mail: oguz.yilmaz@gantek.com
othermailbox: oguz@ieee.metu.edu.tr
postaladdress: Kiz Kulesi 42-2 GOP/ANKARA
homepage: http://oguz.ieee.metu.edu.tr
objectclass: dizin
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
officefax: (312) 446 36 66
mobile: (532) xxx xx xx
extension: 118
```

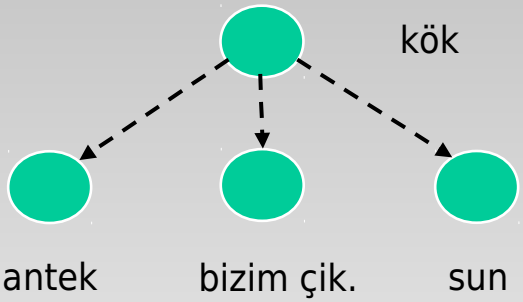
## *Uygulama Alanları – Netscape Addressbook*

- **Ldif dosyasını OpenLDAP'a aktar:**
  **ldapadd –D 'cn=Manager, o=dizin' –W –f dizin1.ldif**
- **Ve doğrula:**
  **ldapsearch -b 'ou=Staff, o=dizin' -L -D 'cn=Manager, o=dizin' -W**
- **Netscape'de:**
  **Communicator -> Address Book -> File -> New Directory...**

# Uygulama Alanları – Netscape Addressbook



- Alışılagelmiş iletişim teknolojilerinin yerini alacak
  - Telefon, pbx, fax vb. yok.
  - Bilgisayar ağları ve bunların düğüm noktaları var.
  - Tüm veri, tüm dünya tarafından, koşullu ulaşılabilir.




  - Sun “Webtone Switch” konsepti,
  - ProjectLiberty konsepti

- Transaction desteği
- LDAPv3 yenilemeleri
- Sayısal sertifikaların daha yoğun kullanımı
- Standart replikasyon
- Daha fazla LDAP arabirimi:
  - Şu an desteklenenler:
    · LDAP to X.500,X.500 to LDAP,
    · HTTP to LDAP,
    · WHOIS++ to LDAP,
    · FINGER to LDAP,
    · Email to LDAP,
    · ODBC to LDAP(çalışılmakta),
    · MDS to LDAP.

- LDAP destekli sunucudan bağımsız işlem:
  - Şu an Sun ve Microsoft'un sırasıyla JNDI ve ADSI program geliştirme arabirimleri mevcut.

    Veritabanlarındaki JDBC ve ODBC gibi.

# İnternet Bağlantıları

- http://www.ldap.org
- OpenLDAP http://www.openldap.org
- Understanding X.500 http://www.salford.ac.uk/its024/Version.Web/Contents.htm
- http://www.stanford.edu/~hodges/
- An LDAP Roadmap & FAQ http://www.kingsmountain.com/ldapRoadmap.shtml
- Customizing LDAP Settings for Communicator 4.0x http://developer.netscape.com/docs/manuals/communicator/custom.html
- http://www.umich.edu/~dirsvcs/ldap/index.html
- http://www.critical-angle.com/ldapworld/
- Sendmail'de LDAP kullanmak http://sendmail.net/?feed=donnellyldap01
- Linux LDAP HOW-TO



Sunum Powerpoint dosyasına ve bağlantılar listesine ***http://seminer.linux.org.tr/*** 'den ulaşabilirsiniz.

-o-

Tüm sorularınız için

**oguz.yilmaz@gantek.com**
**o.yilmaz@ieee.org**