

I took the red pill

-

zentrale Adressbuchverwaltung

Why ???

- Ähm, ja... anderer Pc?
- Mal wieder der "falsche" Rechner
- Öh, wohin soll ich das jetzt Mailen
- Platte gestorben ... deine Freunde auch
- Shared Address book

Die Erleuchtung - LDAP

- Zentrale Lösung
- Adressen können gemeinsam genutzt werden
- Rechteverwaltung
- Beliebige Datenobjekte

Long way down

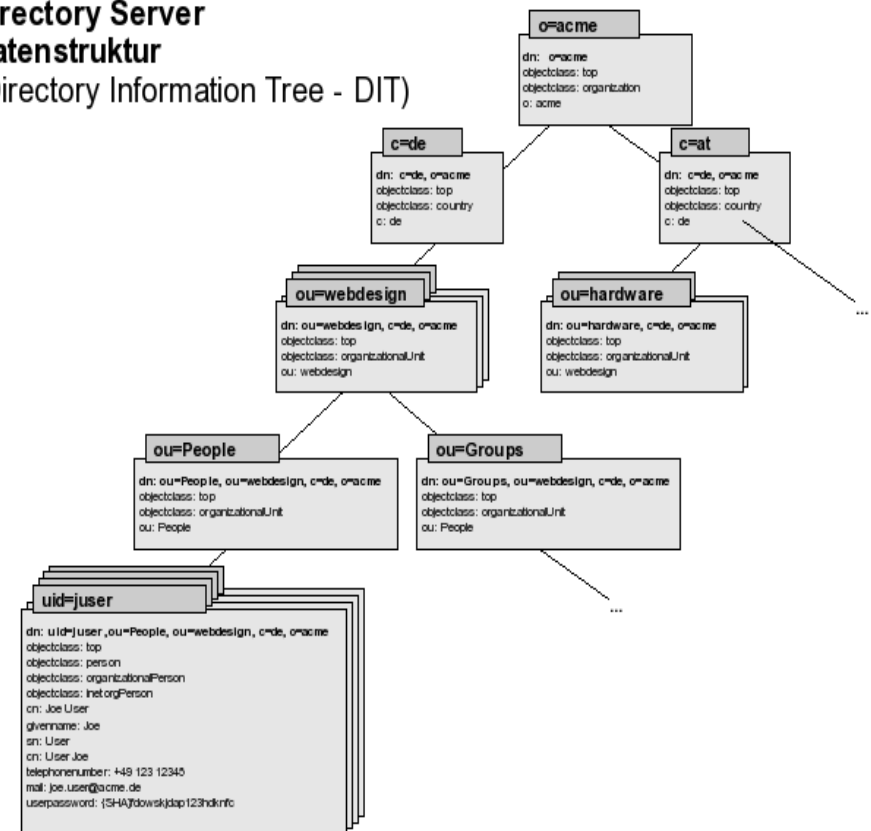
- LDAP Struktur
- ja, richtig: Verschlüsselung
- LDAP Schemas
- Client der das LDAP befüttern kann

wachs Bäumchen wachs

- LDAP hat eine Baumstruktur
- suchen in bestimmten Ästen
- oo Ansatz ...
angeblich sowas wie Vererbung möglich,
hab ich noch nie getroffen

Directory Server Datenstruktur

(Directory Information Tree - DIT)



Struktur ... für Leute ohne Chaos

- DN = Distinguished Name

Muss eindeutig sein, sprich gleiche Objekte können in unterschiedlichen Ästen existieren, aber der Pfad muss eindeutig sein.

cn=admin,dc=test,dc=de

cn=admin,ou=people,dc=test,dc=de

- CN = Common Name

- OU = Organizational Unit

Schema F

- Ein Schema beschreibt eine Objektklasse
- Ein Schema beinhaltet die Attribute einer Objektklasse
- OID = Object Identifier -> IANA
- Neue Schema kann man von bestehenden Objekten ableiten

inetOrgPerson

The inetOrgPerson represents people who are associated with an
organization in some way. It is a structural class and is derived
from the organizationalPerson which is defined in X.521 [X521].

objectclass (2.16.840.1.113730.3.2.2

NAME 'inetOrgPerson'

DESC 'RFC2798: Internet Organizational Person'

SUP organizationalPerson

STRUCTURAL

MAY (

audio \$ businessCategory \$ carLicense \$ departmentNumber \$
displayName \$ employeeNumber \$ employeeType \$ givenName \$
homePhone \$ homePostalAddress \$ initials \$ jpegPhoto \$
labeledURI \$ mail \$ manager \$ mobile \$ o \$ pager \$
photo \$ roomNumber \$ secretary \$ uid \$ userCertificate \$
x500uniqueIdentifier \$ preferredLanguage \$
userSMIMECertificate \$ userPKCS12)

)

LDIF

```
dn: cn=John Doe,dc=example,dc=com
cn: John Doe
givenName: John
sn: Doe
telephoneNumber: +1 888 555 6789 telephoneNumber: +1
888 555 1234
mail: john@example.com
manager: cn=Barbara Doe,dc=example,dc=com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
```

Directory Server Eintrag

Distinguished Name

```
dn: uid=juser,ou=People, ou=web design, c=de, o=acme
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetorgPerson
cn: Joe User
givenname: Joe
sn: User
cn: User Joe
telephonenumber: +49 123 12345
mail: joe.user@acme.de
userpassword: {SHA}fdowskjdap123hdknfc
```

User-Nutzdaten

Schema-Definition des Eintrags

Tools ... Kettensägen und ähnliches

- slapcat
- ldapadd
- qg
- apt-get

openLDAP

- slapd – LDAP Daemon
- slurpd – Replikations Daemon
- client tools

configure the bitch - part1

`/etc/ldap/slapd.conf`

einbinden der Schema Files

```
include      /etc/ldap/schema/core.schema
include      /etc/ldap/schema/cosine.schema
include      /etc/ldap/schema/nis.schema
include      /etc/ldap/schema/inetorgperson.schema
```

configure the bitch - part2

TLSCertificateFile /etc/ldap/cert/server.crt
Zertifikatsfile angeben

TLSCertificateKeyFile /etc/ldap/cert/server.key
privater Schlüssel

TLSCACertificateFile /etc/ldap/cert/server.crt
CA Zertifikat

TLSVerifyClient never
Keine Client Authentifizierung

configure the bitch - part3

suffix "dc=ditzy,dc=biz"

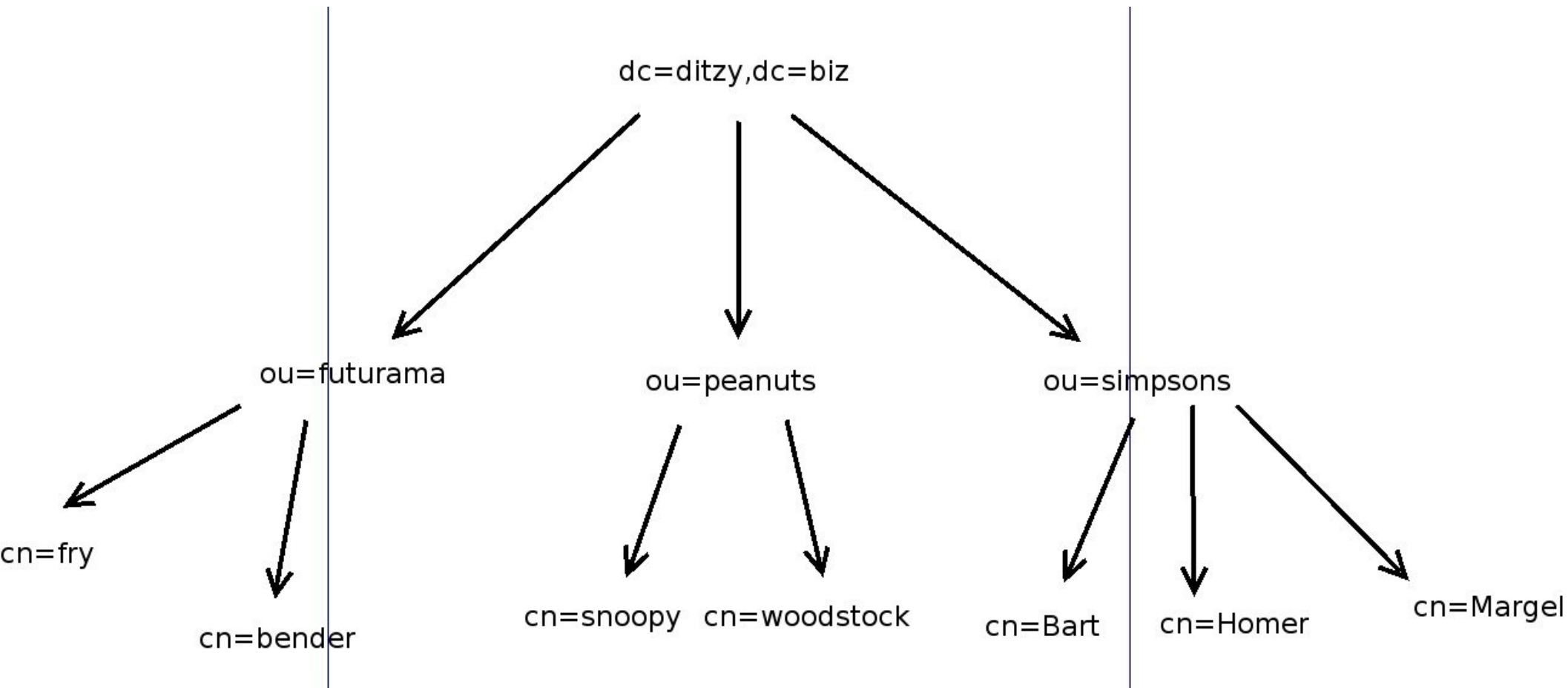
einstellen für welche root, suffix das LDAP zuständig ist

rootdn "cn=admin,dc=ditzy,dc=biz"

rootpw f00b4r

einstellen des initialen root Passworts fürs LDAP

Address book structure



bitch's client ... safersex

/etc/ldap/ldap.conf

TLS_CACERT /etc/ldap/server.crt

Serverzertifikat importieren - pitfall