OpenLDAP

Developer Conference 2011

PRESENTED BY:

Jan Včelák

Red Hat

topics

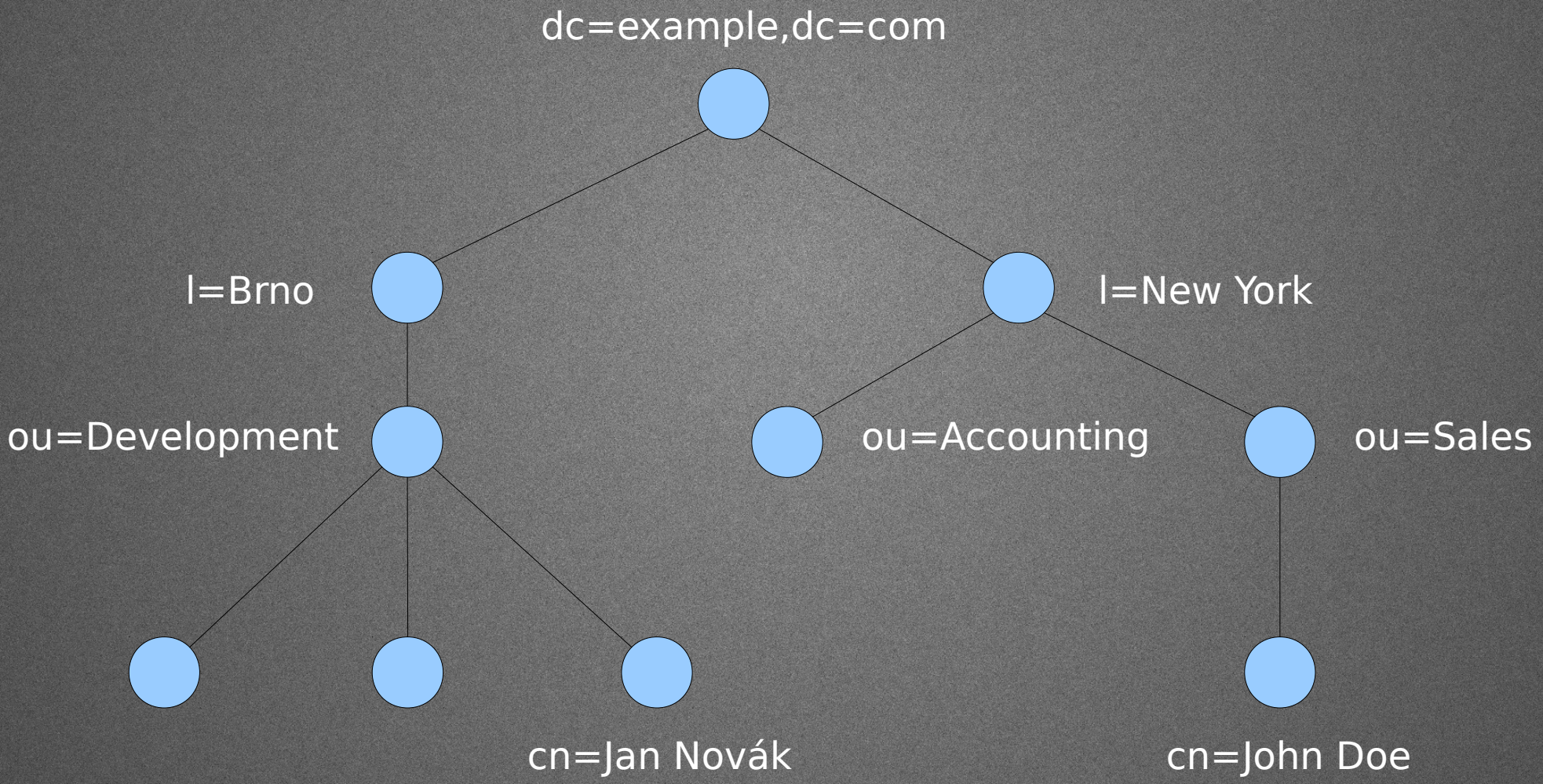
- what is LDAP
- database structure
- difference from other Dbs
- server architecture
- data distrubution
- configuration

LDAP

- Lightweight Directory Access Protocol
  - X.500 (DAP, DSP, DISP, DOP)

- address book
- user management
- authentication (password, SSH key, ...)
- central configuration (DNS, DHCP, autofs, ...)
- authentication backend (Kerberos, Radius, ...)
- ....

Directory Information Tree



entries

- DN (Distinguish Name)
- RDN (Relative Distinguish Name)

cn=John Doe,ou=Sales,
l=New York,dc=example,dc=com

LDIF

```
dn: uid=jdoe,dc=example,dc=com
objectClass: top
objectClass: person
objectClass: inetOrgPerson
cn: John Doe
sn: Doe
uid: fbar
givenName: John
userPassword: secret
departmentNumber: 2220
mobile: +1 213 151-5816
mail: fbar@example.com
usercertificate;binary:: MIIBvjCCASegAwIBAgIBAjANBgkqhki
 G9w0BAQQFADAnMQ8wDQYDVQQDEwZjb25maWcxFDASBgNVBAMTC01NUi
 BDQSBDZXJ0MB4XDTAxMDQwNTE1NTEwNloXDTExMDcw...
```

schema – classes

```
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 )
    )
```

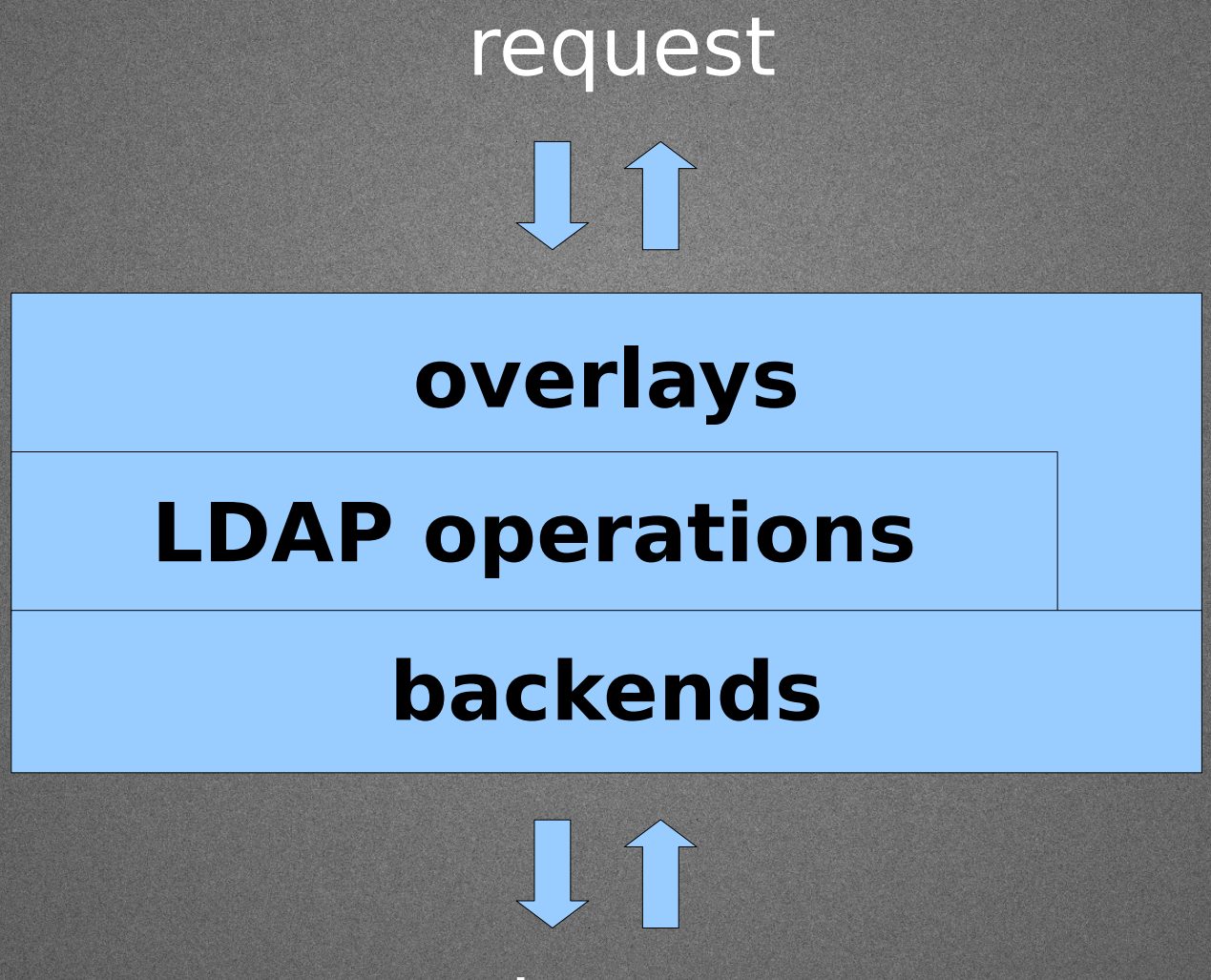
schema – attributes

```
attributetype ( 2.16.840.1.113730.3.1.39
    NAME 'preferredLanguage'
    DESC 'RFC2798: preferred written or spoken
          language for a person'
    EQUALITY caseIgnoreMatch
    SUBSTR caseIgnoreSubstringsMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
    SINGLE-VALUE )
```

difference from other DBs

- data organization
- data operations
- referential integrity
- transactions
- distribution by design
- schema

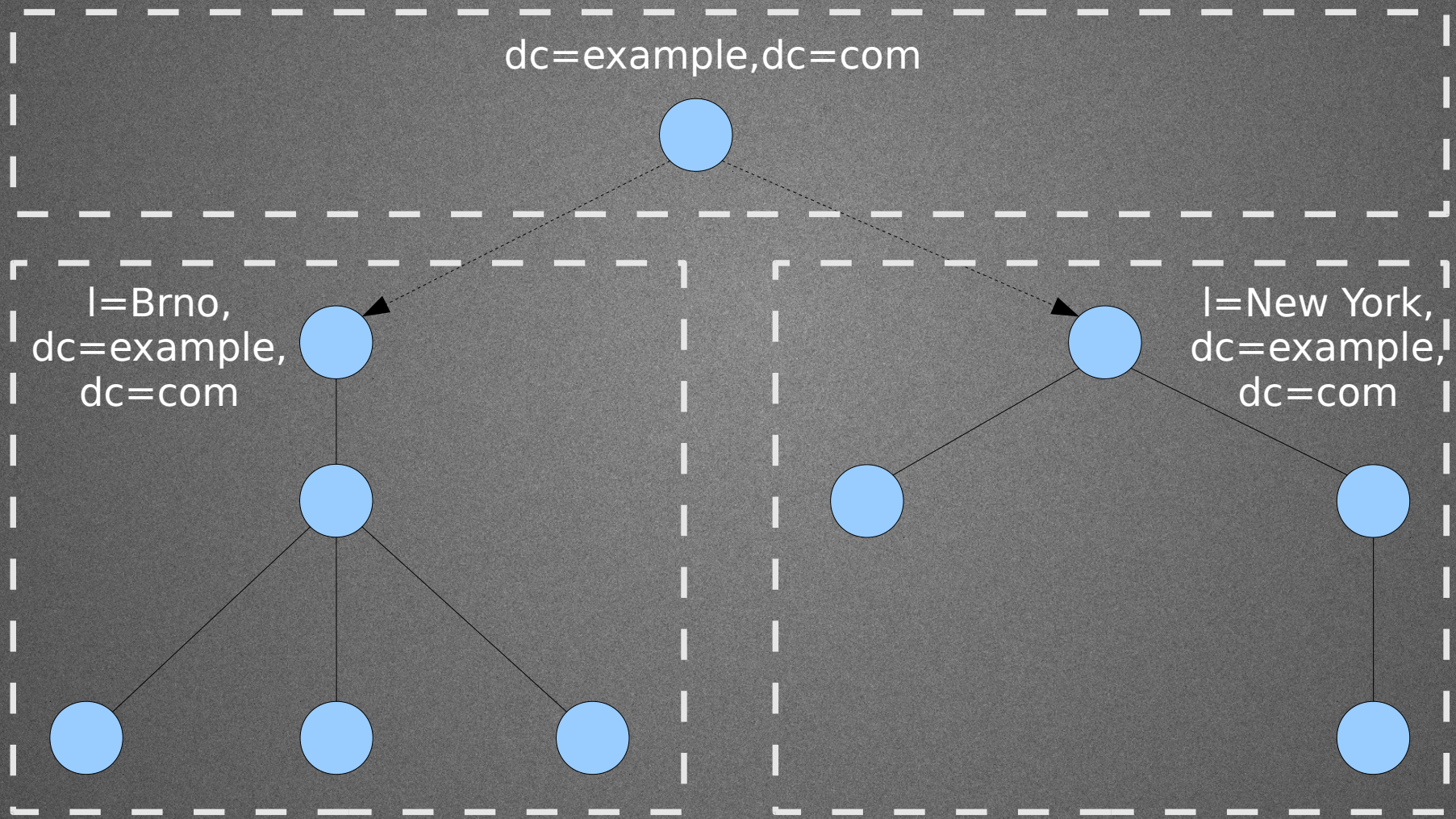
OpenLDAP server architecture



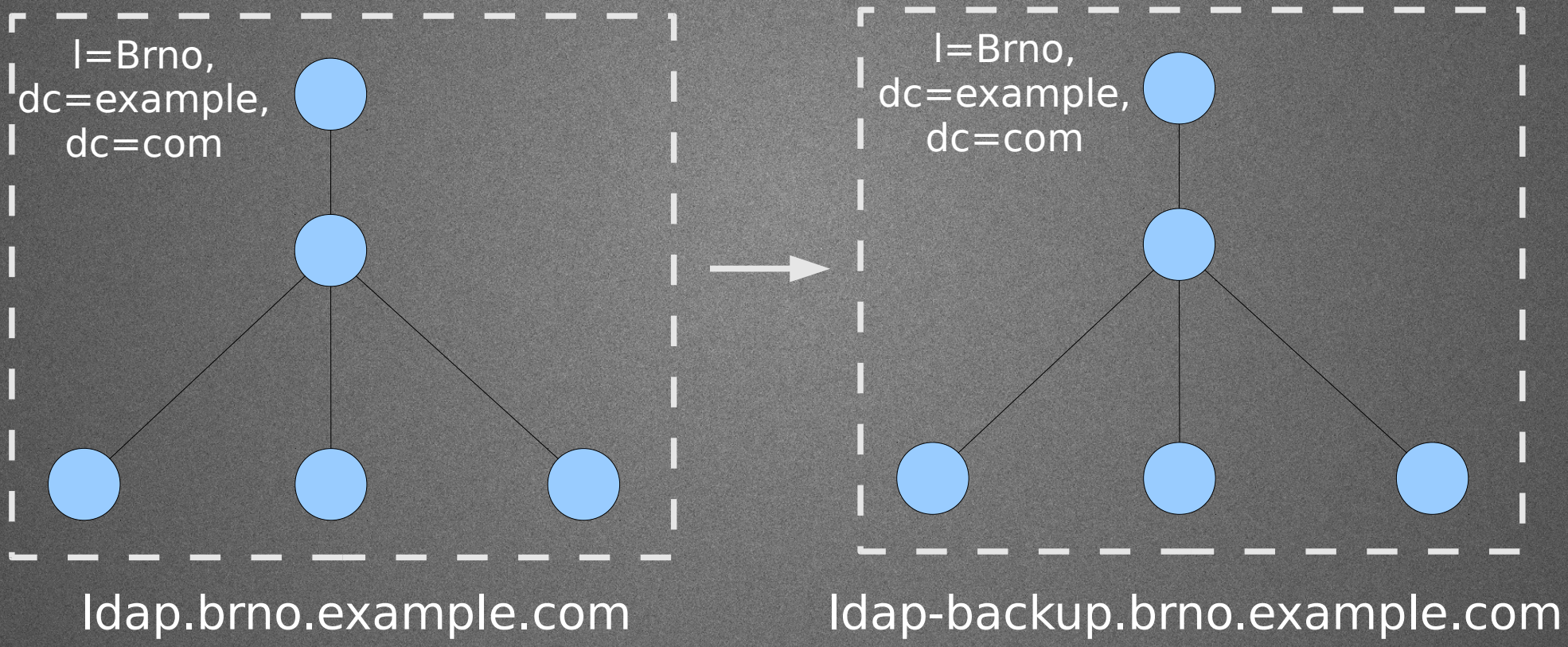
available modules

accesslog
auditlog
back_sql
chain
collect
constraint
dds
deref
dyngroup
dynlist
memberof
pbind
pcache
ppolicy
refint
retcode
rwm
seqmod
smbk5pwd
sssvlv
syncprov
translucent
unique
valsort

data distribution - referrals

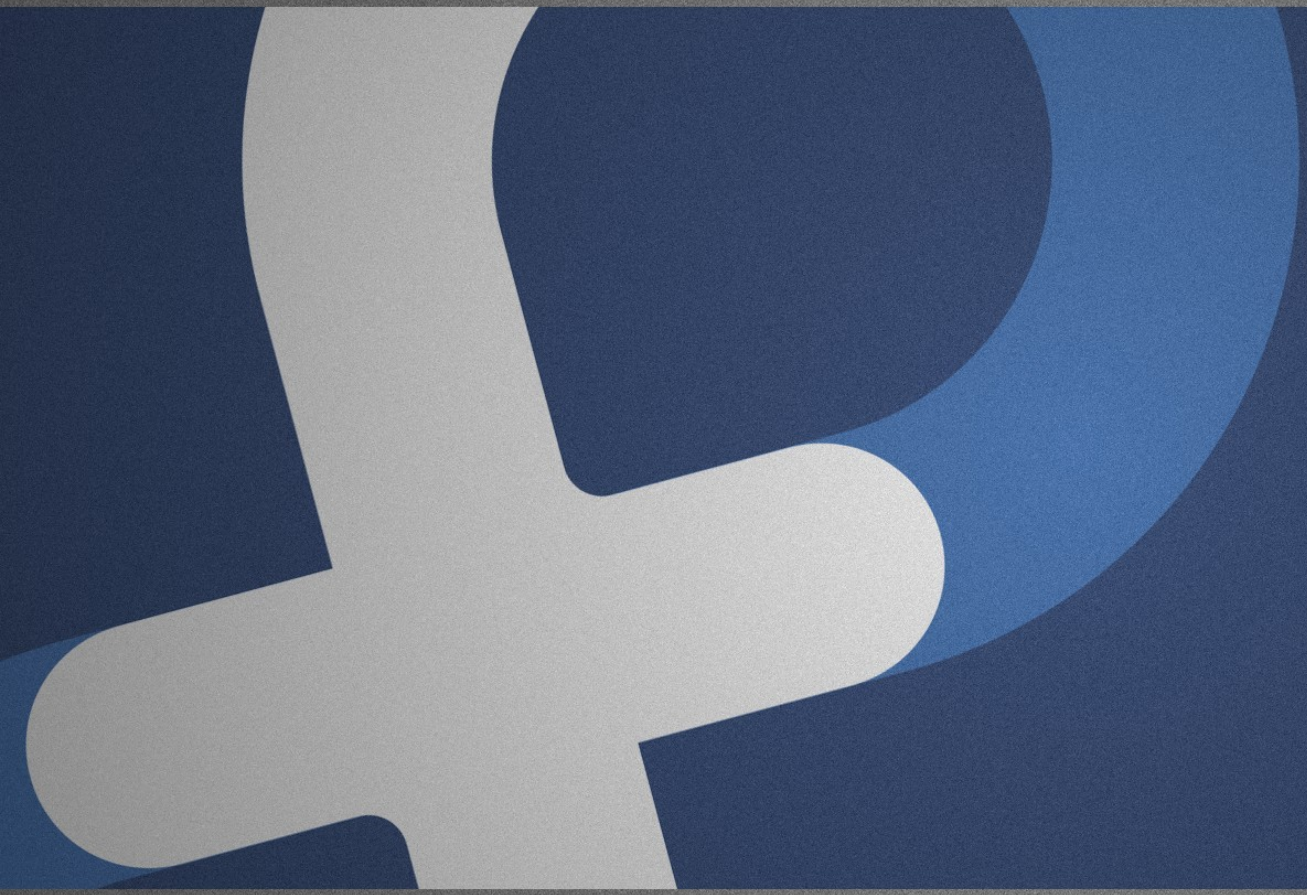


data distribution - replication



configuration

- cn=config
  - since 2.3
  - LDIF backend - /etc/openldap/slapd.d
  - on-the-fly modification
  - man slapd-config
- ~~/etc/openldap/slapd.conf~~
  - works – but please, do not use
  - man slapd.conf



Questions?

CONTACT:
jvcelak@redhat.com