A sua Inteligência em Linux

# LDAP

**1 Encontro Nacional GUS – LinuxChix**
**3 e 4 de Maio de 2003**



**Alessandro Kenji Urakawa**
**Consultor**
**alessandro@4linux.com.br**

A sua Inteligência em Linux

# LDAP

**Lightweight Directory Access Protocol -**
**Protocolo Leve de Acessos a Diretórios**

# LDAP

- Conceitos:
  - Ldap
  - Serviço de Diretórios
  - X.500
- Projeto OpenLdap
- Características
- Autenticações
- LDIF (Ldap Interchange Format)
- ObjectClass e Atributos
- Schemas
- Réplica de Bases
- Passo a passo
- Aplicações

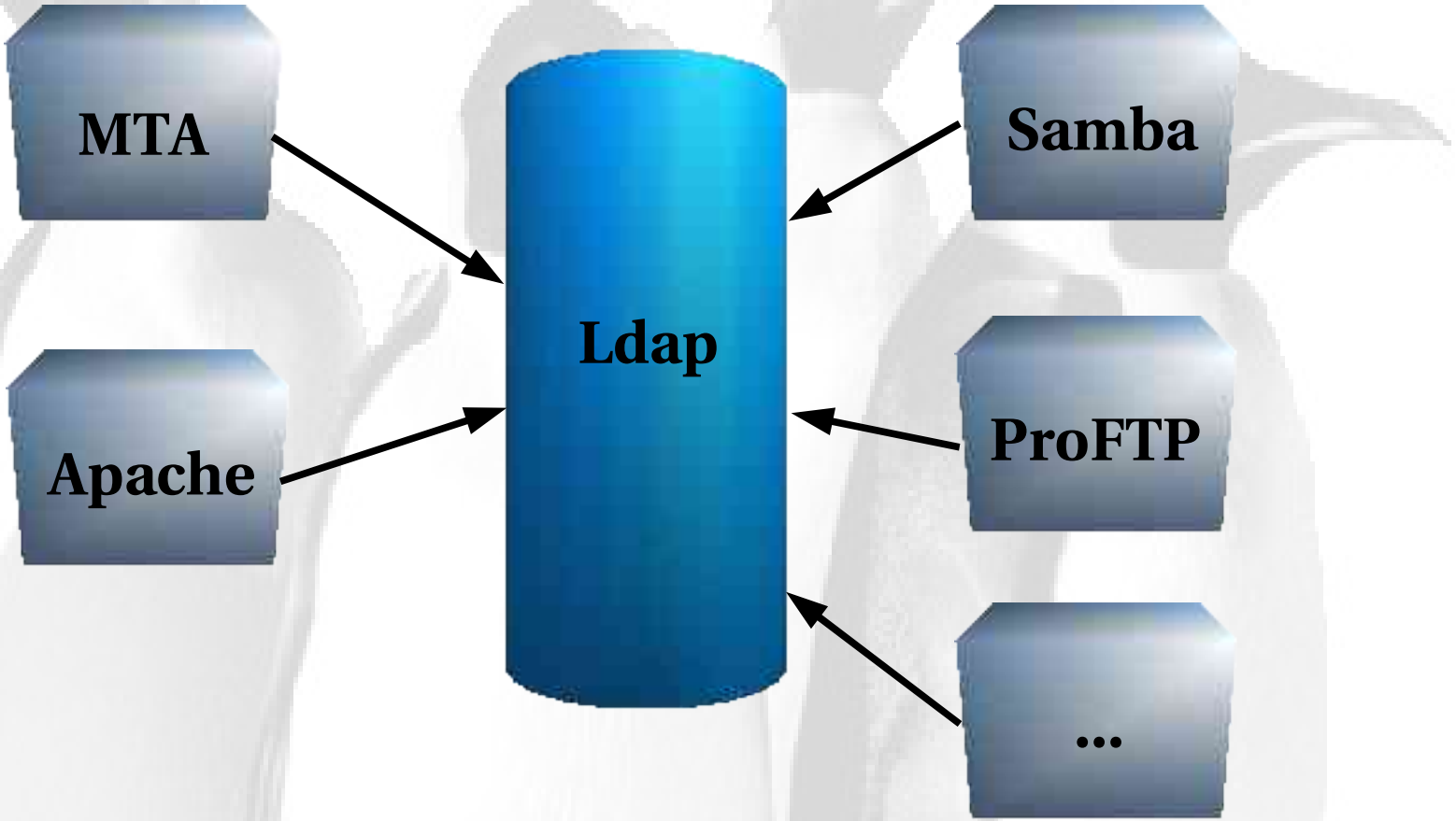
# LDAP

**O LDAP é um protocolo para acessos a diretórios que foi desenvolvido a partir do X.500.**

**Uma de suas principais utilidades é a de centralizar as informações dos usuários.**


Banco de Dados

# LDAP



# LDAP

## O que é um serviço de Diretórios ?

- Banco de Dados otimizado para leitura;
- Suporta sofisticados métodos de busca;
- Ajustados para dar respostas rápidas para procuras em altos volumes;
- Um exemplo é o DNS (Domain Name System);

# LDAP

**Modelo X.500 ?**

- **Mais conhecido como DAP (Directory Access Protocol)**
- **Modelo que dita como as transações ocorrem em um serviço de Diretórios;**
- **Desenvolvido no modelo OSI.**


## Projeto OpenLdap

- O LDAP comecou a ser desenvolvido pela Universidade de Michigan;
- Baseado no modelo X.500.
- Roda em cima da pilha TCP/IP.

# LDAP

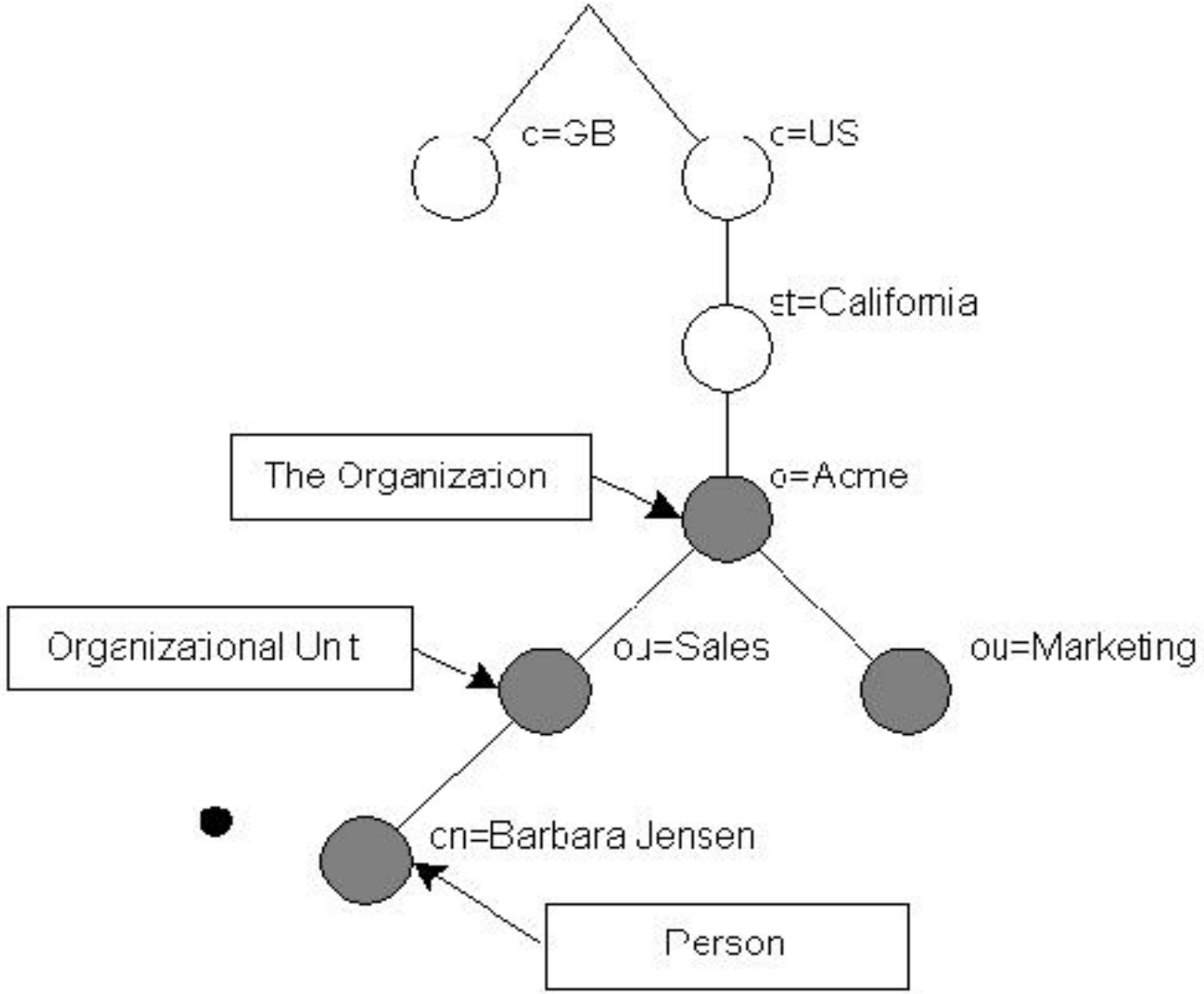
**Que tipo de informações podem ser guardadas em um diretório ?**

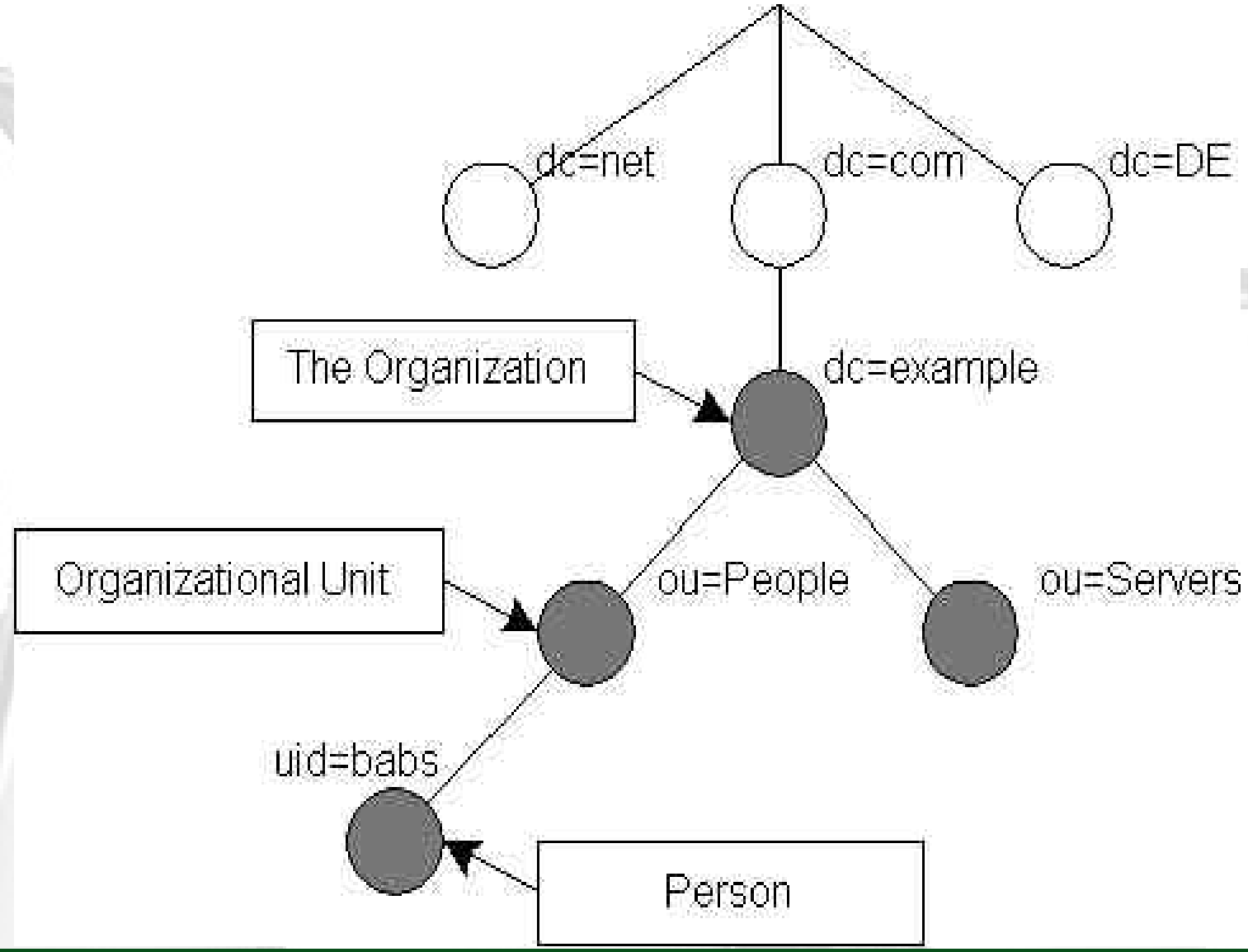
- **Nome;**
- **UID (user ID);**
- **Passwords;**
- **E-mails e Alias;**
- **Fotos;**
- **Local de trabalho;**
- **...**

# LDAP

**Como as informações são organizadas ?**

- **Estrutura hierárquica em árvore;**


c=GB
c=US
st=Califomia
The Organization
o=Acme
Organizational Unt
ou=Sales
ou=Marketing
cn=Barbara Jensen
Person


dc=net
dc=com
dc=DE
The Organization
dc=example
Organizational Unit
ou=People
ou=Servers
uid=babs
Person

# LDAP

**Como as informações são referenciadas ?**

- **dn: uid=alessandro,ou=Consultoria,o=4Linux,c=BR**

**RFC 2253 - LADPv3 Distinguished Names**

| | |
|---|---|
| **CN** | **commonName** |
| **L** | **localityName** |
| **ST** | **stateOrProvinceName** |
| **O** | **organizationName** |
| **OU** | **organizationalUnitName** |
| **C** | **countryName** |
| **STREET** | **streetAddress** |
| **DC** | **domainComponent** |
| **UID** | **userid** |

# LDAP

**Como é feito uma busca ?**

- **Critérios de busca;**
- **Busca em determinadas áreas ou na árvore inteira;**
- **Filtros;**

# LDAP

**Como protejo as informações para acessos não autorizados ?**

- **Autenticação;**
- **Controle em listas de acessos;**

# LDAP

## Ldif – Ldap Interchange Format

- **Formato para Importar / Exportar informações no Ldap;**
- **Arquivo texto;**
- **Cuidado com acentos, cedilha e principalmente com espaços em branco no final de cada linha;**

# LDIF

```
dn: uid=alessandro,ou=Consultoria,o=4Linux, c=BR
objectClass: top
objectClass: organizationalperson
objectClass: inetOrgPerson
objectClass: qmailuser
uid: alessandro
o: 4Linux
ou: Consultoria
cn: Alessandro Kenji Urakawa
sn: Urakawa
userPassword:: 1WlVnbEQzQ1pKVDRsQnM9
mail: alessandro@4linux.com.br
Title: Consultor Técnico
PhoneNumber: +55 (11) 3889-0108
```

# Schemas

- Define os Objetos e Atributos;
- Tipo de dado que será guardado no Atributo;
- Cada objeto ou atributo possui um número de controle (OID), registrado no IANA;
- Pode ser criado para suprir eventuais necessidades;

# ObjectClass

- Que atributos são requeridos e quais podem ser utilizados quando o objeto for declarado;
- Determinam a classe e o tipo de informações que você deseje guardar no registro;
- Ldap Schema Viewer - http://ldap.akbkhome.com
- RCF-2252 - Object Class Description - ftp://ftp.isi.edu/in-notes/rfc2252.txt

# Características

- Suporte a IPV4 e IPV6;
- Autenticação (Cyrus SASL – Kerberos V, GSSAPI, Digest-MD5);
- Segurança no transporte (SSL e TLS);
- Controle de acessos;
- Escolha entre banco de dados (GDBM ou BerkeleyDB);
- Pode atender a múltiplos bancos ao mesmo tempo;
- Alta perfomance em múltiplas chamadas;
- Replicação de Bases;

A sua Inteligência em Linux

# Perfomance

| Performance numbers for Active Directory and Open LDAP | | | |
|---|---|---|---|
| Product | Load time (Record/sec) | Messaging test with one client (Operation / sec) | Messaging test with 10 clients (Operation / sec) |
| Open LDAP on Linux | 23.5 | 4.6 | 47.7 |
| Active Directory on Win 2000 | 99.3 | 9.5 | 1,536 |
| Product | Addressing (wildcard) test with one client (Operation / sec) | Addressing (wildcard) test with 10 clients (Operation / sec) | Searchable test with one client (Operation / sec) |
| Open LDAP on Linux | 5.9 | 46.6 | 4.5 |
| Active Directory on Win 2000 | 2.0 | 11.0 | 993 |
| Product | Search Rate test with 10 clients (Operation / sec) | | Modify test (Operation / sec) |
| Open LDAP on Linux | 18.2 | | 9.3 |
| Active Directory on Win 2000 | 2,199 | | 27.7 |

**Fonte: Network Word Fusion**

# Ldap

# Instalação

# Passo a Passo

**1 – Remova todos os pacotes do BerkeleyDB v1, v2 ou v3 que esteja instalado no servidor;**

**2- Faça o download dos fontes:**
**Cyrus Sasl 2.1.13 -**
**http://ftp.andrew.cmu.edu/pub/cyrus-mail/cyrus-sasl-2.1.13.tar.gz**

**BerkeleyDB 4.1.25 -**
**http://www.sleepycat.com/update/snapshot/db-4.1.25.tar.gz**

**OpenLdap – 2.1.17 - Stable**
**ftp://ftp.OpenLDAP.org/pub/OpenLDAP/openldap-stable/openldap-20030410.tgz**

# Passo a Passo

**3 – Compile e instale o BerkeleyDB:**

**'# tar xvfz db-4.1.25.tar.gz'**
**'# cd db.4.1.25/build_unix'**
**'# ../dist/configure'**
**'# make'**
**'# make install '**
**'# echo "/usr/local/BerkeleyDB.4.1/lib" >> /etc/ld.so.conf '**
**'# ldconfig'**

**O BerkeleyDB será instalado em /usr/local/ BerkeleyDB.4.1**

# Passo a Passo

## 4 – Compile e instale o Cyrus-Sasl:

```
'# tar xvfz cyrus-sasl-2.1.13.tar.gz'
'# cd cyrus-sasl-2.1.13'
'# ./configure –with-bdb-libdir=/usr/local/BerkeleyDB.4.1/lib \
   --with-bdb-incdir=/usr/local/BerkeleyDB.4.1/include \
   --enable-krb4=no '
'# make'
'# make install '
'# ln -s /usr/local/lib/sasl2 /usr/lib/sasl2'
'# ldconfig'
```

**O Cyrus-Sals será instalado em /usr/local**

# Passo a Passo

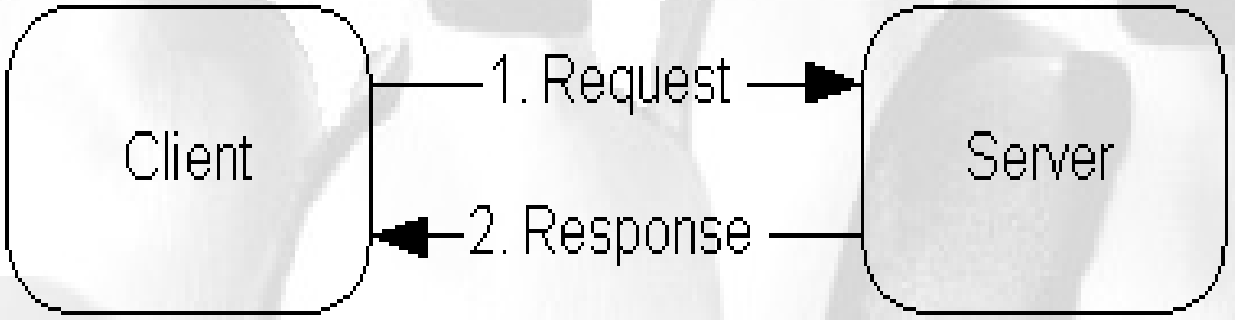
## 5 – Compile e instale o OpenLdap

```
'# tar xvfz openldap-stable-20030410.tar.gz'
'# cd openldap-2.1.17'
'# env CPPFLAGS=-I/usr/local/BerkeleyDB.4.1/include  \
   LDFLAGS=-L/usr/local/BerkeleyDB.4.1/lib  \
   ./configure '
'# make depend'
'# make '
'# make test' - Opcional
'# make install'
```

**O OpenLdap será instalado em /usr/local**

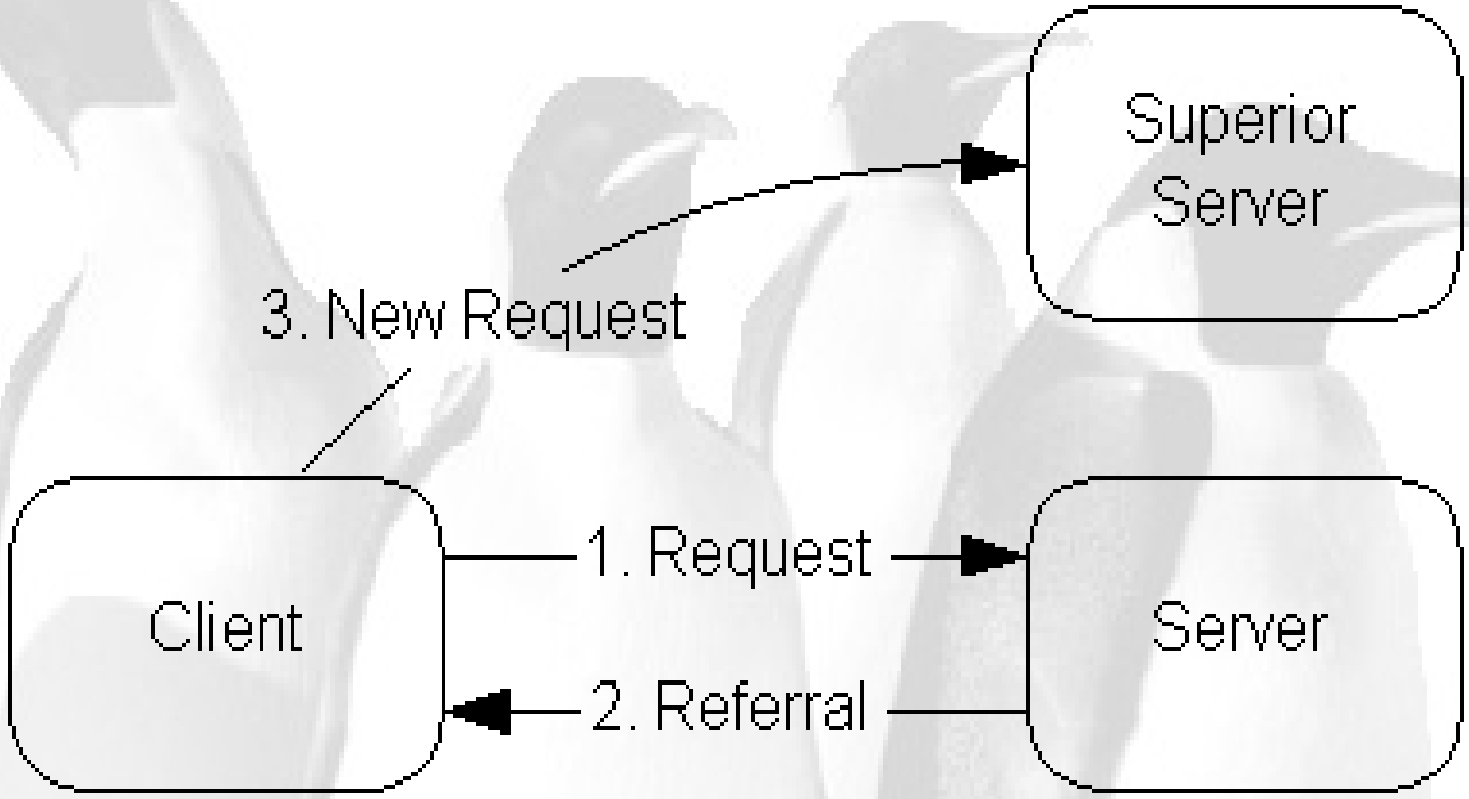
# Passo a Passo

**6 – Escolha de que forma você vai estruturar a base de acordo com a sua necessidade:**



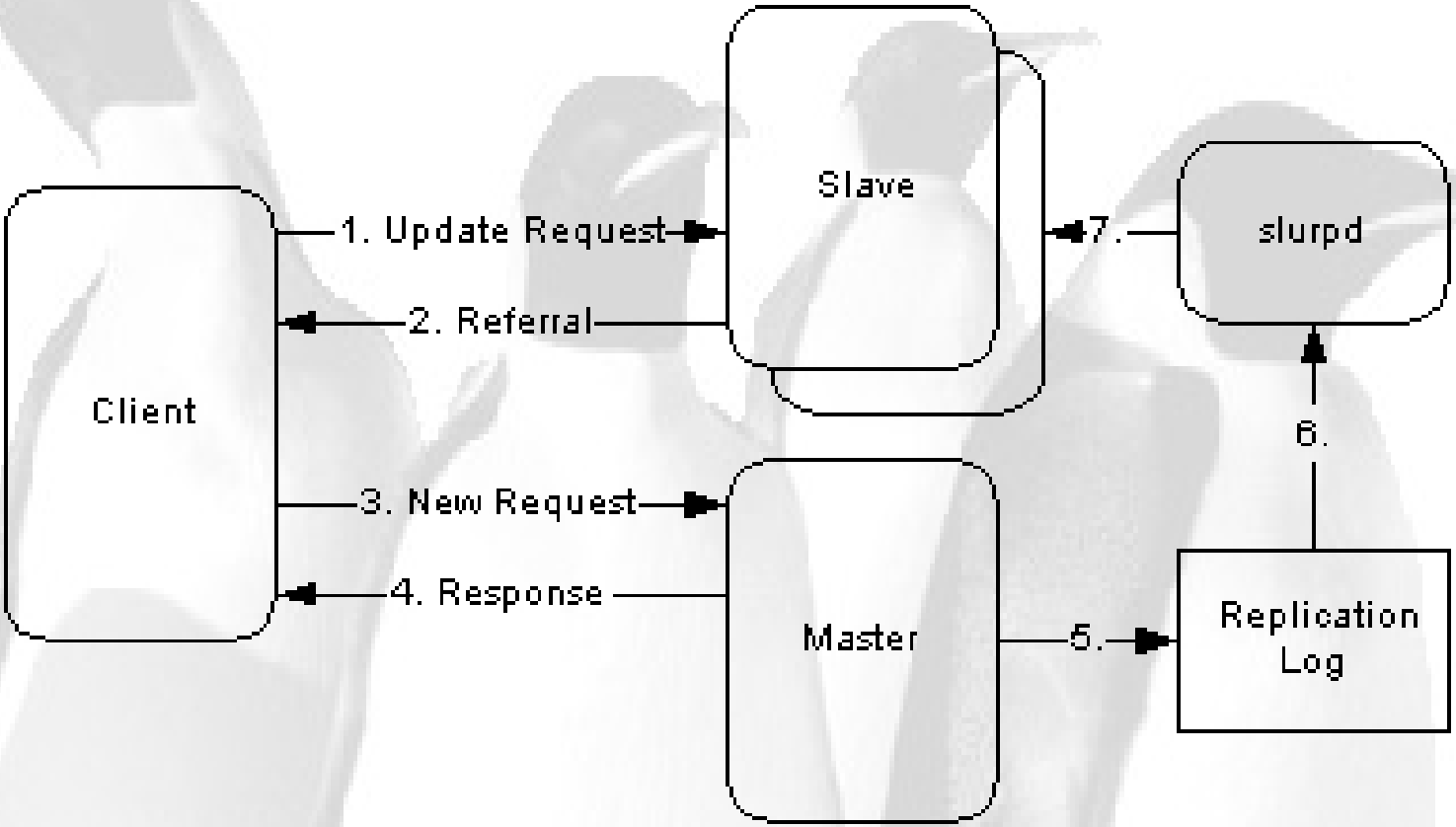

**Servidor com serviços locais**

# Passo a Passo




**Servidor com referência**

# Passo a Passo




**Servidor com réplica**

A sua Inteligência em Linux

# Passo a Passo

## 7 – Edite o arquivo /usr/local/etc/openldap/slapd.conf

```
include     /usr/local/etc/openldap/schema/core.schema
include     /usr/local/etc/openldap/schema/cosine.schema
include     /usr/local/etc/openldap/schema/inetorgperson.schema
include     /usr/local/etc/openldap/schema/nis.schema
pidfile     /usr/local/var/slapd.pid
argsfile    /usr/local/var/slapd.args

database      bdb
suffix        "o=4linux,c=BR"
rootdn        "cn=Manager,o=4linux,c=BR"
rootpw        secret
directory     /usr/local/var/openldap-data
index  objectClass    eq
```

# Passo a Passo

**8 – Suba o daemon do Servidor ldap:**
**'# /usr/local/libexec/slapd'**

**9 – Crie um arquivo texto no formato ldif, contendo:**

**dn: o=4linux,c=BR**
**objectClass: organization**
**o: 4Linux**

**dn: ou=Consultoria, o=4linux,c=BR**
**objectClass: organizationalUnit**
**ou: Consultoria**
**description: Consultoria 4Linux**

# Passo a Passo

**10 – Carrege este primeiro ldif na base:**

```
'# ldapadd -x -v -W -D"cn=Manager,o=4linux,c=BR"  \
   -f  primeiro.ldif'
```

**onde: -x = Autenticação Simples**
**-v = verbose**
**-W = pedir a senha do usuário**
**-D = usuário que vai fazer a conexão**
**-f = arquivo no formato ldif a ser adicionado**

# Passo a Passo

**11 – Crie um segundo arquivo texto no formato ldif, contendo:**

```
dn: uid=alessandro,ou=consultoria,o=4linux,c=BR
objectClass: top
objectClass: inetOrgPerson
uid: alessandro
userPassword: {MD5}!$HKASDJK#$@NBKMNCKA#(JASD
ou: Consultoria
o: 4linux
cn: Alessandro Kenji Urakawa
sn: Urakawa
mail: alessandro@4linux.com.br
title: Consultor
phoneNumber: +55 (11) 3889-0108
```

# Passo a Passo

**12 – Inclua este usuário na base com o mesmo procedimento do anterior:**

```
'# ldapadd -x -v -W -D"cn=Manager,o=4linux,c=BR"  \
   -f  segundo.ldif'
```

**13 – Para efetuar uma pesquisa para ver se está tudo ok:**

```
'# ldapsearch -x -b'o=4linux,c=BR' '(objectClass=*)'
```

**onde: -x = autenticação simples**
**-b = base a ser efuata a pesquisa**
**(objecClass=*) = critério da busca**

# Passo a Passo

**14 – Ok ! Agora você já tem os exemplos de como incluir as empresas, departamentos (areas), e pessoas dentro da base ldap ... O resto agora é com vocês.**

# Informações Adicionais

**Para criptografar as senhas do usuários:**

**'# slappasswd -h {MD5}'**

**onde: -h = tipo de criptografia (SHA,SSHA,CRIPT, MD5, ..)**
**-w = senha a ser criptografada**

**Este comando te retornará a senha criptografada, copie e coloque no atributo userPassword do seu usuário.**

# Informações Adicionais

**Para modificar algum dado já cadastrado:**

**Crie um aquivo ldif com o dn e os campos a serem modificados, por exemplo:**

```
dn: uid=alessandro,ou=Consultoria,o=4linux,c=BR
title: Consultor / Instrutor
```

**Agora utilize o comando:**

```
'# ldapmodify -x -v -W -D"cn=Manager,o=4linux,c=BR" \
-f modificar.ldif '
```

**Os parâmetros são os mesmo do ldapadd.**

# Informações Adicionais

**Para deletar alguma entrada no ldap:**

**'# ldapdelete -x -v -W -D"cn=Manager,o=4linux,c=BR" **
**"uid=alessandro,ou=consultoria,o=4linux,c=BR"**

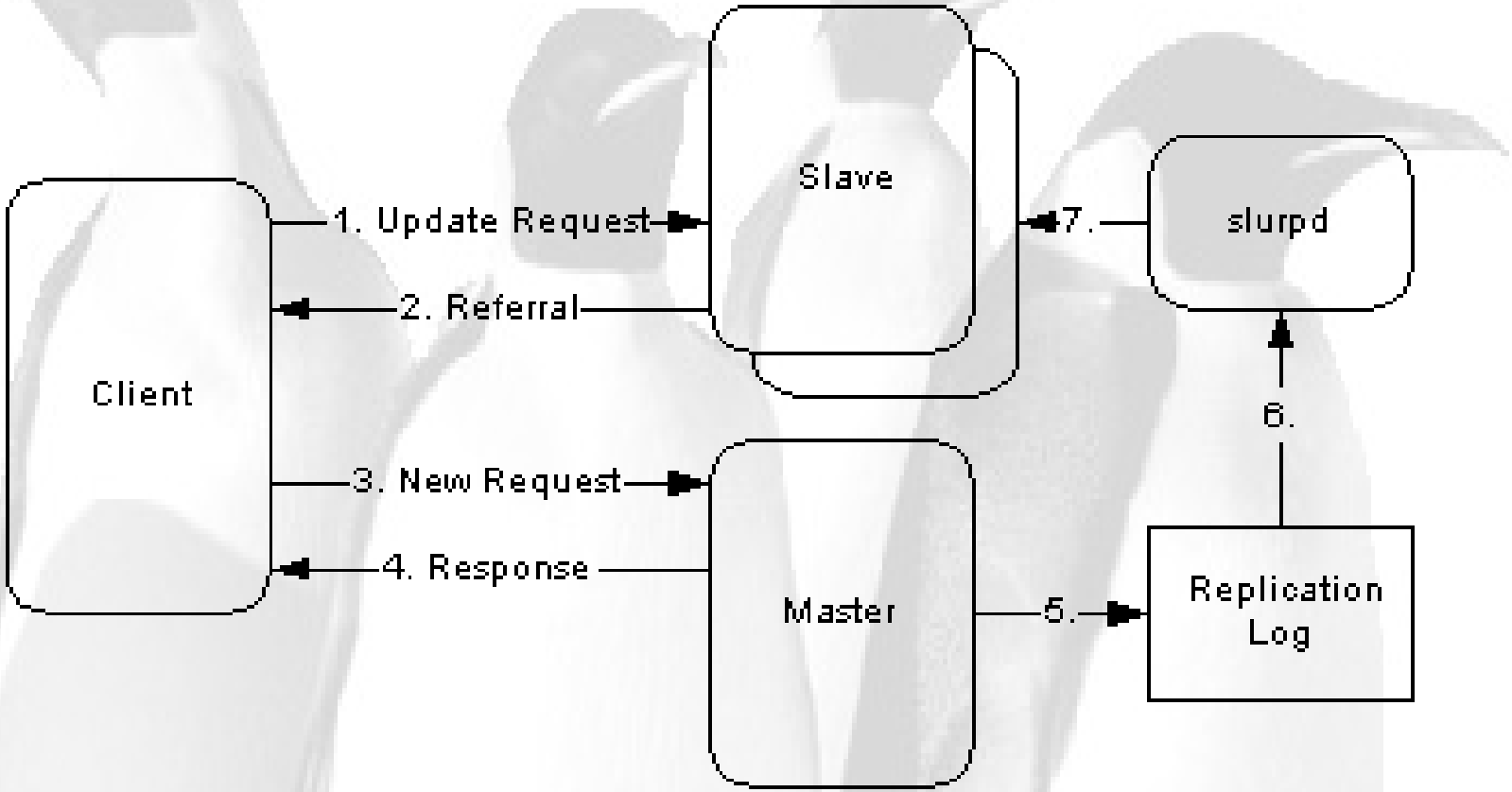
**Os parâmentro são iguais a do ldapadd.**

**Ao invés de passar o dn inteiro como no exemplo você pode criar uma lista das entradas, uma a cada linha, e usar o parâmetro -f.**

# Réplica

- Algumas vezes necessitamos ter mais do que um servidor LDAP para atender a todas as requisições;
- Junto com o DNS, conseguimos fazer o balanceamento de carga;
- O Daemon responsável pela réplica é o Slurpd

# Réplica


Slave
slurpd
1. Update Request
2. Referral
7.
Client
6.
3. New Request
4. Response
Master
5.
Replication Log

# Réplica

1- Os dois servidores (Master e Slave) devem ter o servidor slapd devidamente configurado;

2- Adicione as seguintes linhas no slapd.conf do servidor master:

```
replica host=slave.example.com:389
binddn="cn=Manager,dc=example,dc=com"
bindmethod=simple credentials=secret

replogfile /usr/local/var/replog.log
```

# Réplica

**3- Adicione as seguintes linhas no slapd.conf do servidor slave:**

**updatedn "cn=Manager,dc=example,dc=com"**
**updateref ldap://master.example.net**

**4 – Pare o servidor Master**

**5 – Copie a base do Master para o Slave.**

# Réplica

**6- Suba o slapd dos servidores master e slave;**

**7 – Suba o daemon slurpd no servidor master;**

**Ok !! Agora faça alguma modificação na base master e veja através dos logs se a réplica funcionou corretamente.**

# Criação de Schemas

**1 – Obtenha o OID - http://www.iana.org/cgi-bin/enterprise.pl**

**2 – Crie um arquivo local do seu schema**

**3- Defina os seus atributos (se necessário)**

**4 – Defina os seus objectClass**

# Criação de Schemas

| OID | Assignment |
|---|---|
| 1.1 | Organization's OID |
| 1.1.1 | SNMP Elements |
| 1.1.2 | LDAP Elements |
| 1.1.2.1 | AttributeTypes |
| 1.1.2.1.1 | myAttribute |
| 1.1.2.2 | ObjectClasses |
| 1.1.2.2.1 | myObjectClass |

# Criação de Schemas

**AttributeType ( 2.5.4.41 NAME 'name'**
**DESC 'name(s) associated with the object'**
**EQUALITY caseIgnoreMatch**
**SUBSTR caseIgnoreSubstringsMatch**
**SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{32768} )**

**attributeType ( 2.5.4.3 NAME ( 'cn' 'commonName' )**
**DESC 'common name(s) assciated with the object'**
**SUP name )**

# Criação de Schemas

| Name | OID | Description |
|---|---|---|
| boolean | 1.3.6.1.4.1.1466.115.121.1.7 | boolean value |
| distinguishedName | 1.3.6.1.4.1.1466.115.121.1.12 | DN |
| directoryString | 1.3.6.1.4.1.1466.115.121.1.15 | UTF-8 string |
| IA5String | 1.3.6.1.4.1.1466.115.121.1.26 | ASCII string |
| Integer | 1.3.6.1.4.1.1466.115.121.1.27 | integer |
| Name and Optional UID | 1.3.6.1.4.1.1466.115.121.1.34 | DN plus UID |
| Numeric String | 1.3.6.1.4.1.1466.115.121.1.36 | numeric string |
| OID | 1.3.6.1.4.1.1466.115.121.1.38 | object identifier |
| Octet String | 1.3.6.1.4.1.1466.115.121.1.40 | arbitary octets |
| Printable String | 1.3.6.1.4.1.1466.115.121.1.44 | printable string |

**Principais tipos de SYNTAX**

| Name | Type | Description |
|---|---|---|
| booleanMatch | equality | boolean |
| octetStringMatch | equality | octet string |
| objectIdentiferMatch | equality | OID |
| distinguishedNameMatch | equality | DN |
| uniqueMemberMatch | equality | Name with optional UID |
| numericStringMatch | equality | numerical |
| numericStringOrderingMatch | ordering | numerical |
| numericStringSubstringsMatch | substrings | numerical |
| caseIgnoreMatch | equality | case insensitive, space insensitive |
| caseIgnoreOrderingMatch | ordering | case insensitive, space insensitive |
| caseIgnoreSubstringsMatch | substrings | case insensitive, space insensitive |
| caseExactMatch | equality | case sensitive, space insensitive |
| caseExactOrderingMatch | ordering | case sensitive, space insensitive |
| caseExactSubstringsMatch | substrings | case sensitive, space insensitive |
| caseIgnoreIA5Match | equality | case insensitive, space insensitive |
| caseIgnoreIA5OrderingMatch | ordering | case insensitive, space insensitive |
| caseIgnoreIA5SubstringsMatch | substrings | case insensitive, space insensitive |
| caseExactIA5Match | equality | case sensitive, space insensitive |
| caseExactIA5OrderingMatch | ordering | case sensitive, space insensitive |
| caseExactIA5SubstringsMatch | substrings | case sensitive, space insensitive |

**Principais tipos de EQUALITY**

# Criação de Schemas

```
Objectclass ( 1.1.2.2.2 NAME 'myPerson'
    DESC 'my person'
    SUP inetOrgPerson
    MUST ( myUniqueName $ givenName )
    MAY myPhoto )
```

# Aplicações


**Uid;**
**Senha;**
**Onde estão armazenadas as mensagens no servidor;**
**Cotas;**
**Tamanho máximo de mensagens;**
**Status da conta**

# Aplicações


# Aplicações


# Dúvidas ?