

# OpenLDAP

Lucas Brasilino

<lucas.brasilino@gmail.com>

*Organização:*



**Training Tecnologia**  
Treinamentos e Consultoria em TI

*Apoio:*



*Patrocinadores:*



Universidade  
Católica de Brasília

# Agenda:

- Definindo serviços de diretórios
- O que é LDAP ?
- Implementações de servidores LDAP
- Características do OpenLDAP
- Exemplos de aplicações

*Organização:*



**Training Tecnologia**  
Treinamentos e Consultoria em TI

*Apoio:*

 **LINUX**



Linux  
Professional  
Institute

*Patrocinadores:*



Universidade  
Católica de Brasília

# Agenda:

- Configuração básica do OpenLDAP
- Arquivo LDIF
- Uso dos utilitários clientes
- Criação de um serviço de diretório

*Organização:*



**Training Tecnologia**  
Treinamentos e Consultoria em TI

*Apoio:*



*Patrocinadores:*



Universidade  
Católica de Brasília

# Definindo serviços de diretórios:

- É um banco de dados otimizado para leitura, procura e navegação
- Geralmente armazena informações em atributos
- Tais informações são descritivas de um dado item
- Cada item é único
- Estruturado em forma de árvores

*Organização:*



**Training Tecnologia**  
Treinamentos e Consultoria em TI

*Apoio:*



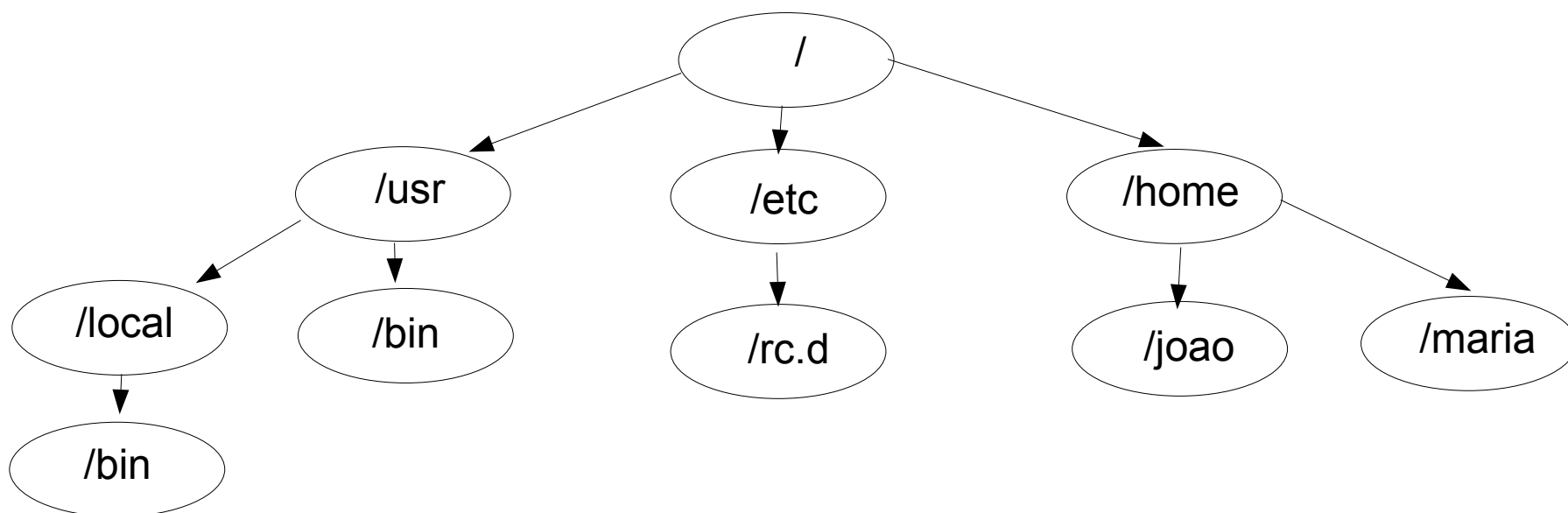
*Patrocinadores:*



Universidade  
Católica de Brasília

# Exemplos de diretórios:

## Sistema de arquivos



Organização:



**Training Tecnologia**  
Treinamentos e Consultoria em TI

Apoio:



Patrocinadores:



Universidade  
Católica de Brasília

# Sistema de arquivos:

```
$ echo "blabla" > /home/lucas/teste.txt
```

```
$ cat /home/lucas/teste.txt  
blabla
```

*Organização:*



**Training Tecnologia**  
Treinamentos e Consultoria em TI

*Apoio:*

 **LINUX**



Linux  
Professional  
Institute

*Patrocinadores:*



Universidade  
Católica de Brasília

# Sistema de arquivos:

```
$ stat /home/lucas/teste.txt
```

```
File: `/home/lucas/teste.txt'
```

```
Size: 7          Blocks: 8          IO Block: 4096  arquivo comum
```

```
Device: 304h/772d    Inode: 4652477    Links: 1
```

```
Access: (0644/-rw-r--r--) Uid: ( 500/  lucas)  Gid: ( 500/  lucas)
```

```
Access: 2006-11-30 23:14:35.0000000000 -0200
```

```
Modify: 2006-11-30 23:12:08.0000000000 -0200
```

```
Change: 2006-11-30 23:12:08.0000000000 -0200
```

Organização:



Training Tecnologia  
Treinamentos e Consultoria em TI

Apoio:

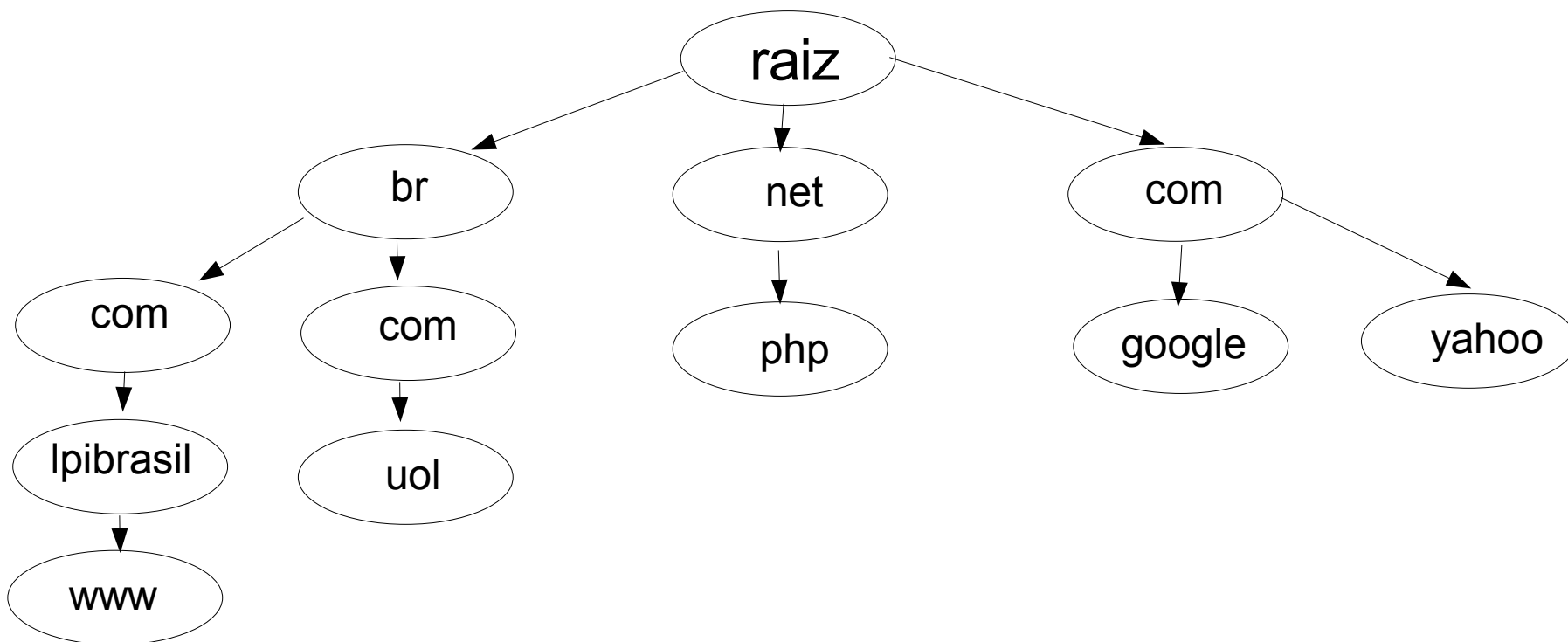


Patrocinadores:



Universidade  
Católica de Brasília

# Exemplos de diretórios: Sistema de DNS



Organização:



**Training Tecnologia**  
Treinamentos e Consultoria em TI

Apoio:



Patrocinadores:



Universidade  
Católica de Brasília

# O que é o LDAP?

- Lightweight Directory Access Protocol
- Derivado do X.500 DAP (IBM)
- Armazena dados utilizando o conceito de **objetos**
  - Contém atributos
  - É identificado pelo *Distinguished Name* (**DN**)

Organização:



Training Tecnologia  
Treinamentos e Consultoria em TI

Apoio:



Linux  
Professional  
Institute

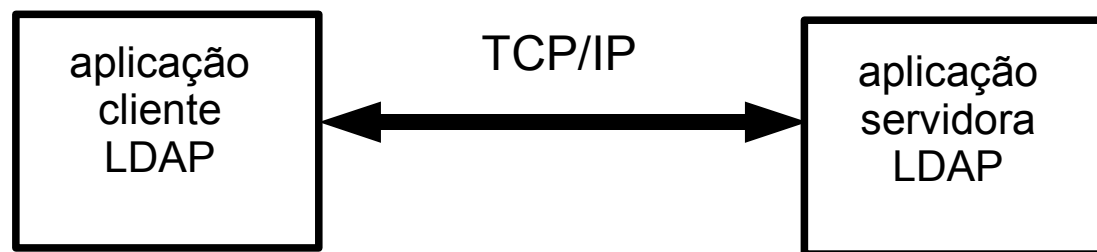
Patrocinadores:



Universidade  
Católica de Brasília

# O que é o LDAP?

- Arquitetura Cliente/Servidor
- Definido pela RFC 2251 (LDAPv3 – 1997)



# O que é o LDAP?

- Por ser descritivo é ideal para ser usado por:
  - Aplicações diversas  
Ex: Sistema de cadastro de funcionários
  - Sistema operacional  
Ex: Autenticação do usuário
  - Serviços de rede  
Ex: Servidor de email

*Organização:*



**Training Tecnologia**  
Treinamentos e Consultoria em TI

*Apoio:*



*Patrocinadores:*



Universidade  
Católica de Brasília

## Itens (objetos) do LDAP:

- Os atributos de cada objeto é determinado por esquemas (*schemas*)
  - Atributos requeridos (obrigatórios)
  - Atributos optativos (opcionais)
- Um atributo especial (*objectclass*) informa quais esquemas um objeto utiliza

Organização:



Training Tecnologia  
Treinamentos e Consultoria em TI

Apoio:



Linux  
Professional  
Institute

Patrocinadores:



Universidade  
Católica de Brasília

## Itens (objetos) do LDAP:

- Têm sua unicidade definida (e garantida) pelo *Distinguished Name* (DN)
- O DN é composto, a cada nível, de um dos atributos e seu valor
- Todo o conjunto de DN's forma o *Directory Information Tree* (DIT)

Organização:



Training Tecnologia  
Treinamentos e Consultoria em TI

Apoio:

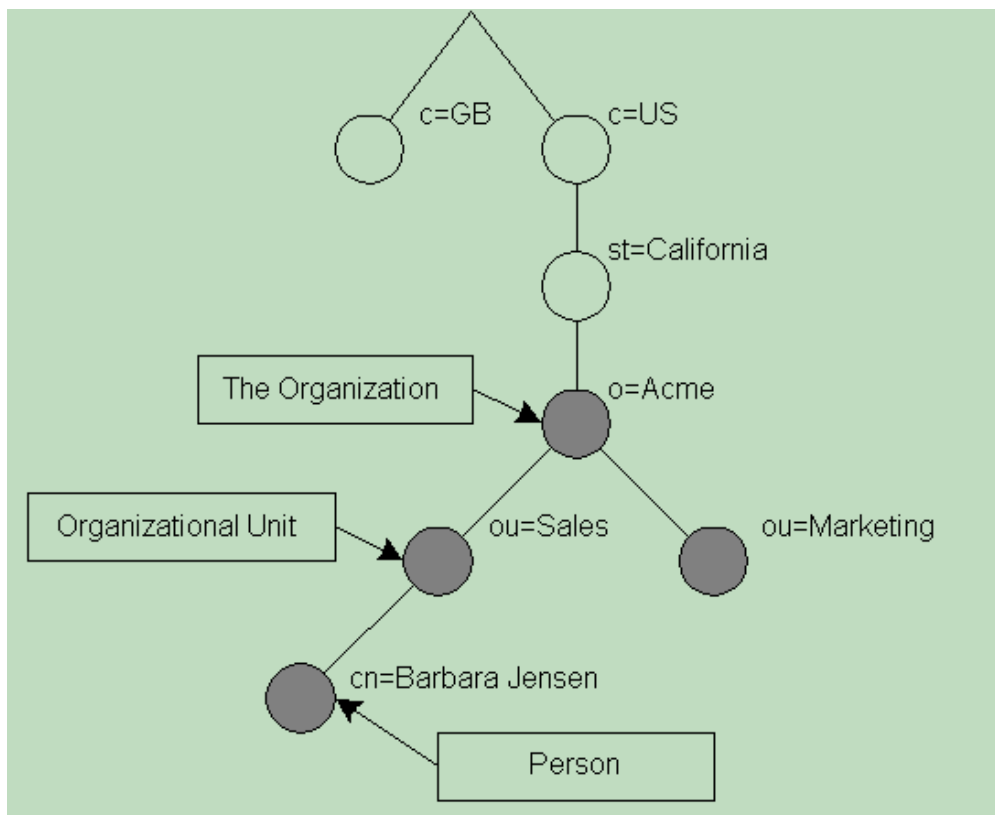


Patrocinadores:



Universidade  
Católica de Brasília

# Exemplo de implementação



Organização:



**Training Tecnologia**  
Treinamentos e Consultoria em TI

Apoio:



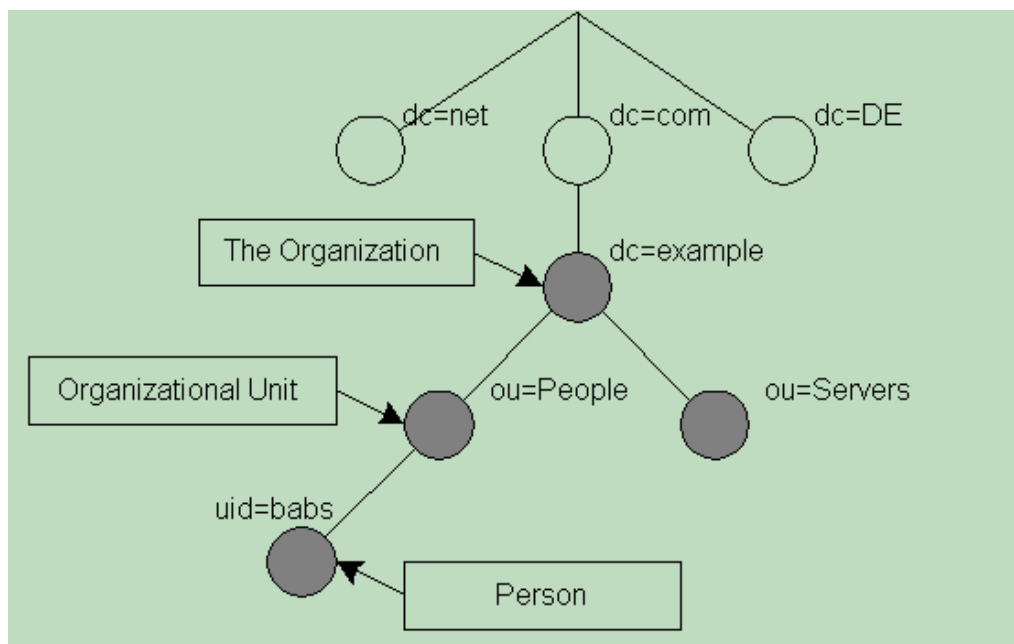
Linux  
Professional  
Institute

Patrocinadores:



Universidade  
Católica de Brasília

# Exemplo de implementação



`ou=People, dc=example, dc=com`  
`uid=babs, ou=People, dc=example, dc=com`

# Exemplo de esquema: **posixAccount**

## Atributos obrigatórios:

uid, cn, uidNumber, gidNumber, homeDirectory

## Atributos opcionais:

userPassword, loginShell, description, gecos

*Organização:*



**Training Tecnologia**  
Treinamentos e Consultoria em TI

*Apoio:*



Linux  
Professional  
Institute

*Patrocinadores:*



Universidade  
Católica de Brasília

# Exemplo de esquema: **inetOrgPerson**

Atributos obrigatórios:  
(nenhum)

Atributos possíveis:

uid, mail, userCertificate, photo, o, jpegPhoto,  
mobile, homePhone, etc...

Organização:



**Training Tecnologia**  
Treinamentos e Consultoria em TI

Apoio:

 **LINUX**



Linux  
Professional  
Institute

Patrocinadores:



Universidade  
Católica de Brasília

# Implementações de servidores LDAP:

- Netscape LDAP Server
- Fedora Directory Server
- Sun ONE Directory Server
- Microsoft Active Directory
- Novell eDirectory
- OpenLDAP

*Organização:*



**Training Tecnologia**  
Treinamentos e Consultoria em TI

*Apoio:*



*Patrocinadores:*



Universidade  
Católica de Brasília

# Característica do OpenLDAP:

- Desenvolvido sob licença OpenLDAP Public License
- Altamente configurável, inclusive com ACL's
- Suporta conexões seguras através dos protocolos SASL, TLS ou SSL
- Multi-threading

*Organização:*



**Training Tecnologia**  
Treinamentos e Consultoria em TI

*Apoio:*



*Patrocinadores:*



Universidade  
Católica de Brasília

# Característica do OpenLDAP:

- Suporta replicação (*replicas*), porém é *single-master*
- Permite a separação do DIT entre vários servidores (*referrals*)
- Suporta vários *backends*: BerkeleyDB, GDBM, LDAP (proxy), passwd, SQL, entre outros.
- Vasta API disponível: C/C++, Java, PHP, Perl, etc

Organização:



Training Tecnologia  
Treinamentos e Consultoria em TI

Apoio:



Linux  
Professional  
Institute

Patrocinadores:



Universidade  
Católica de Brasília

## Exemplos de aplicações:

- Servidores diversos:
  - Sendmail
  - Qmail
  - SAMBA
  - POP 3 / IMAP
- Clientes de Email:
  - Thunderbird
  - Evolution
- Sistemas de autenticação (Linux, Windows, etc)
- Aplicações diversas

Organização:



Training Tecnologia  
Treinamentos e Consultoria em TI

Apoio:



Patrocinadores:



Universidade  
Católica de Brasília

# Configuração básica do OpenLDAP

*Organização:*



**Training Tecnologia**  
Treinamentos e Consultoria em TI

*Apoio:*



*Patrocinadores:*



Universidade  
Católica de Brasília

Daemon:

slapd

Arquivo de configuração:

slapd.conf

Diretório padrão (Fedora Core):

/etc/openldap

*Organização:*



**Training Tecnologia**  
Treinamentos e Consultoria em TI

*Apoio:*



*Patrocinadores:*



Universidade  
Católica de Brasília

# Formato do slapd.conf:

opção    valor

Ex:

database    bdb

*Organização:*

*Apoio:*

*Patrocinadores:*

# Opções básicas:

## include <arquivo>

Carrega configurações adicionais antes de continuar a ler o arquivo de configuração. Usualmente utilizado para carregar os schemas

Organização:



**Training Tecnologia**  
Treinamentos e Consultoria em TI

Apoio:



Patrocinadores:



Universidade  
Católica de Brasília

# Opções básicas:

## database <backend>

Define uma instância do banco de dados de armazenamento da DIT e seu tipo de armazenamento.

Organização:



Training Tecnologia  
Treinamentos e Consultoria em TI

Apoio:



Patrocinadores:



Universidade  
Católica de Brasília

# Opções básicas:

suffix <dn>

Determina a partir de qual DN os objetos serão armazenados nesta instância da base de dados

*Organização:*



**Training Tecnologia**  
Treinamentos e Consultoria em TI

*Apoio:*



Linux  
Professional  
Institute

*Patrocinadores:*



Universidade  
Católica de Brasília

# Opções básicas:

`rootdn <dn>`

Indica o DN que não tem restrições de acesso à instância, ou seja, o que tem acesso a nível administrativo.

Organização:



**Training Tecnologia**  
Treinamentos e Consultoria em TI

Apoio:



Linux  
Professional  
Institute

Patrocinadores:



Universidade  
Católica de Brasília

# Opções básicas:

`rootpw <senha>`

Senha do rootdn. Pode estar definido em texto claro ou utilizando-se algum algoritmo hash.

Organização:



**Training Tecnologia**  
Treinamentos e Consultoria em TI

Apoio:

 **LINUX**



Linux  
Professional  
Institute

Patrocinadores:



Universidade  
Católica de Brasília

# Opções básicas:

`directory <caminho>`

Indica o diretório (no sistema de arquivos) onde a base de dados desta instância deve ser armazenada.

Organização:



Training Tecnologia  
Treinamentos e Consultoria em TI

Apoio:

 LINUX



Linux  
Professional  
Institute

Patrocinadores:



Universidade  
Católica de Brasília

# Opções básicas:

`index <atributo> <tipo>`

Define quais atributos terão índices e qual tipo de índices serão mantidos.

*Organização:*



**Training Tecnologia**  
Treinamentos e Consultoria em TI

*Apoio:*



*Patrocinadores:*



Universidade  
Católica de Brasília

# Arquivo LDIF (*LDAP Data Interchange Format*)

```
# comentário  
dn: <distinguished name>  
<atributo>: <valor>  
<atributo>: <valor>  
...
```

# Utilitários cliente OpenLDAP:

- Idapadd
- Idapsearch
- Idapdelete
- Idapmodify
- outros...

*Organização:*



**Training Tecnologia**  
Treinamentos e Consultoria em TI

*Apoio:*



Linux  
Professional  
Institute

*Patrocinadores:*



Universidade  
Católica de Brasília

Mãos à obra!!!

*Organização:*



*Apoio:*



*Patrocinadores:*



Universidade  
Católica de Brasília

Dúvidas???

Obrigado!!

Lucas Brasilino

<lucas.brasilino@gmail.com>

*Organização:*



**Training Tecnologia**  
Treinamentos e Consultoria em TI

*Apoio:*



*Patrocinadores:*



Universidade  
Católica de Brasília