



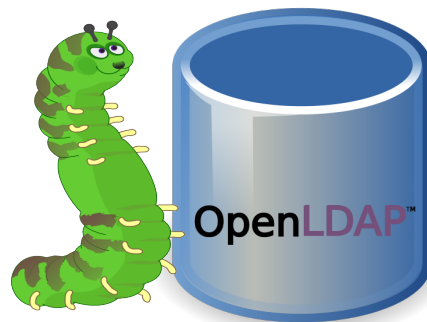
## Curso 452

# Linux Security Servers in Cloud

Versão 2015\_3.0

## Servidor OpenLDAP

---



**LDAP**

**Lightweight Directory Access Protocol**

**Protocolo Leve de Acesso a Diretórios**

### Fundamentação

LDAP (Lightweight Directory Access Protocol ou Protocolo Leve de Acesso a Diretórios) “Padrão aberto capaz de facilitar, de forma flexível, o compartilhamento, a manutenção e o gerenciamento de grandes volumes de informações, definindo um método padrão de acesso e atualização de informações dentro de um diretório.” (TUTTLE 2009)“

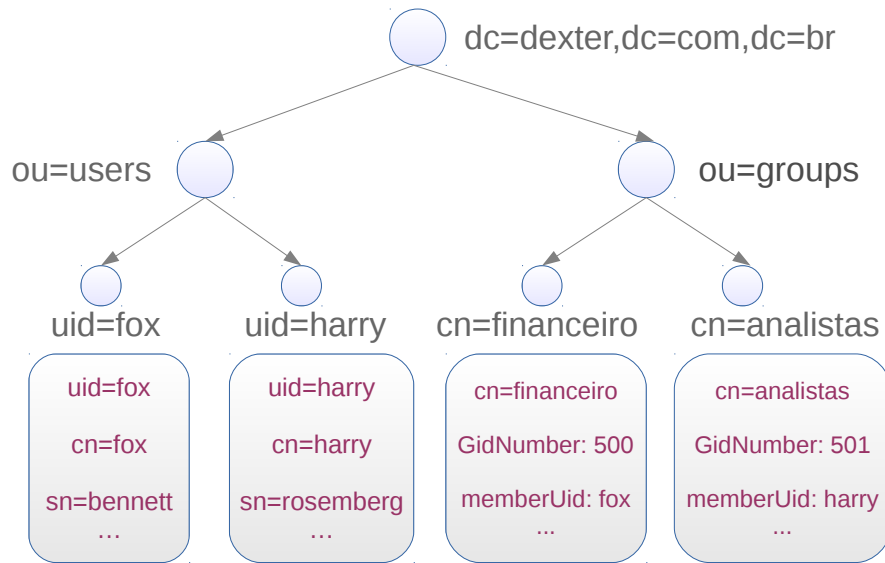


## Aula 07

- 

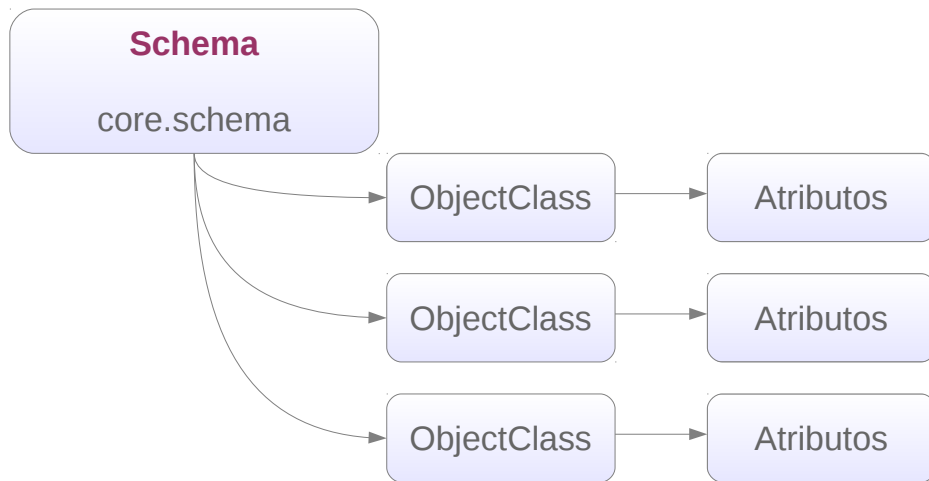
[illegible]

## Servidor OpenLDAP



O LDAP é um protocolo de rede que roda sobre o TCP/IP que permite organizar os recursos de rede de forma hierárquica, como uma árvore de diretório, onde temos primeiramente o diretório raiz, em seguida a rede da empresa, o departamento e por fim o computador do funcionário e os recursos de rede (arquivos, impressoras, etc.) compartilhados por ele. A árvore de diretório pode ser criada de acordo com a necessidade.

## Servidor OpenLDAP



Uma das principais vantagens do LDAP é a facilidade em localizar informações e arquivos disponibilizados. Pesquisando pelo sobrenome de um funcionário é possível localizar dados sobre ele, como telefone, departamento onde trabalha, projetos em que está envolvido e outras informações incluídas no sistema, além de arquivos criados por ele ou que lhe façam referência. Cada funcionário pode ter uma conta de acesso no servidor LDAP, para que possa cadastrar informações sobre si e compartilhar arquivos.

# Servidor OpenLDAP

---

## Centralização de serviços na rede:

Diagrama de uma arquitetura de rede centralizada. No topo, um servidor OpenLDAP (representado por um ícone de servidor com uma placa de identificação "John Doe") está conectado a uma barra horizontal. Abaixo desta barra, há seis servidores cliente. Cada servidor cliente possui um ícone específico: o primeiro tem um ícone de DNS; o segundo, um ícone de e-mail; o terceiro, um ícone de Internet; o quarto, o logotipo do Windows; o quinto, um ícone de navegador web; e o sexto, um ícone de FTP.

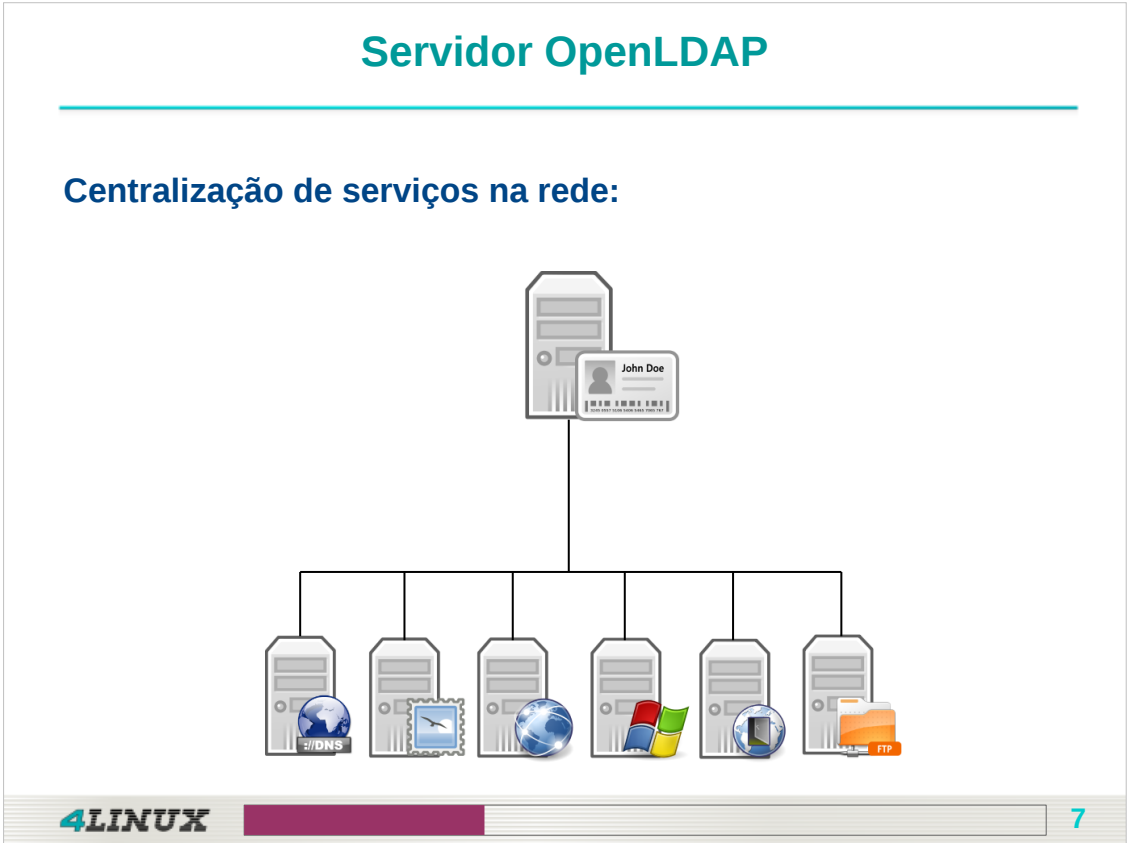
4LINUX

7

# Servidor OpenLDAP

---

## Centralização de serviços na rede:



# Servidor OpenLDAP

---

## Centralização de serviços na rede:

Diagrama de uma arquitetura de rede centralizada. No topo, um servidor OpenLDAP (representado por um ícone de servidor com uma placa de identificação "John Doe") está conectado a uma barra horizontal que distribui a conexão para seis servidores cliente na base. Cada servidor cliente possui um ícone específico: o primeiro tem um ícone de DNS; o segundo, um ícone de e-mail; o terceiro, um ícone de Internet; o quarto, o logotipo do Windows; o quinto, um ícone de navegador web; e o sexto, um ícone de FTP.

4LINUX

7

# Servidor OpenLDAP

---

## Centralização de serviços na rede:

Diagrama ilustrando a centralização de serviços na rede. Um servidor central (OpenLDAP) está conectado a uma barra horizontal que distribui a conexão para seis servidores cliente. Cada servidor cliente possui um ícone específico: o primeiro tem um ícone de DNS; o segundo, um ícone de e-mail; o terceiro, um ícone de Internet; o quarto, o logotipo do Windows; o quinto, um ícone de navegador; e o sexto, um ícone de FTP.

4LINUX

7

notações:

notações:

# Servidor OpenLDAP

---

## Diretórios vs DBMS:

- Fortemente otimizados para leituras;
- Dados podem ser redundantes;

The diagram illustrates the performance characteristics of Directory Servers versus Database Management Systems (DBMS) for read and write operations. It is divided into two main sections: 'Diretórios' (Directories) on the left and 'DBMS' on the right.

**Diretórios (Directories):** This section shows a server icon with a user card overlay labeled 'John Doe'. Four purple arrows point down to the server, labeled 'Leitura' (Read). One orange arrow points up from the server, labeled 'Escrita' (Write).

**DBMS:** This section shows a server icon with a database cylinder overlay. Four purple arrows point down to the server, labeled 'Leitura' (Read). Three orange arrows point up from the server, labeled 'Escrita' (Write).

The visual representation indicates that Directory Servers are optimized for read operations (multiple read arrows, single write arrow), while DBMS are optimized for write operations (multiple write arrows, single read arrow).

## This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.



## Servidor OpenLDAP

**Servidor: DataCenter**

### Atributos:

- c** - Representa país (country);
- o** - Representa uma organização como uma empresa (organization);
- ou** - Representa um departamento (organization unit);
- cn** - Representa um nome (common name);
- uid** - Representa a identidade de um usuário (user ID);
- gn** - Representa o nome próprio de uma pessoa (given name);
- sn** - Representa o sobrenome de uma pessoa (surname).

### Anotações:

[illegible]

## Servidor OpenLDAP

**Servidor: DataCenter**

## ➤ Instalando o OpenLDAP:

```
1# apt-get install slapd ldap-utils
```

< Irá solicitar a senha do Administrador LDAP >

## ➤ Configurando a base LDAP:

```
2# dpkg-reconfigure slapd
```

## 1 – Omitir as Configurações: Não

## 2 – Domínio DNS: **dexter.com.br**

3 – Nome da Empresa: **Dexter Courier**

4 – Senha do Admin: **4linux**

5 – Confirme a Senha: **4linux**

## 6 – Método de Armazenamento: **HDB**



10

### Anotações:

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

## Servidor OpenLDAP

**Servidor: DataCenter**

➤ **Consulta simples ao LDAP:**

```
i# ldapsearch -x -LLL -h 127.0.0.1 -b
dc=dexter,dc=com,dc=br
```

➤ **Consulta sendo Administrador da Base LDAP:**

```
2# ldapsearch -x -LLL -h 127.0.0.1 -b
dc=dexter,dc=com,dc=br -D
"cn=admin,dc=dexter,dc=com,dc=br" -W
```

**-x** → Autenticação Básica

**-b** → Qual a base de consulta

- LLL → Limpar a Busca

**-D** → Usuario Admin do LDAP

**-h** → Especificar o Host do LDAP

**-W** → Senha do Admin LDAP

### Anotações:

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

## Servidor OpenLDAP

**Servidor: DataCenter**

## ➤ Configurando o LDAP:

```
1# cd /etc/ldap/
2# vim ldap.conf
8 BASE      dc=dexter,dc=com,dc=br
9 URI       ldap://127.0.0.1
```

## Consultando o LDAP:

```
3# ldapsearch -x -LLL
```

### Anotações:

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

## Servidor OpenLDAP

*Servidor: DataCenter*

### Inserindo dados na base do LDAP Proxy usando LDIF:

```
1# cd /etc/ldap/  
2# cp /root/ldap/ldifs.tar.gz .  
3# tar zxvf ldifs.tar.gz  
4# cd ldifs/ ; ls  
  
group.ldif  ou.ldif  user.ldif  modify.ldif
```

LDIF → São arquivos usados para alterar/inserir a base do LDAP.

### O que é um LDIF?

LDIF (LDAP Data Interchange Format) é o formato de arquivo de entrada padrão do OpenLDAP. É desta maneira que os dados devem ser incluídos no sistema LDAP quando não temos nenhuma ferramenta de administração.

## Servidor OpenLDAP

**Servidor: DataCenter**

➤ Criando as OU (organization unit) da Dexter, Users e Groups:

```
1# vim ou.ldif
2# ldapadd -x -D "cn=admin,dc=dexter,dc=com,dc=br" -f
ou.ldif -W
3# ldapsearch -x -LLL -b dc=dexter,dc=com,dc=br
```

## ➤ Criando os Usuários da Dexter no LDAP:

```
1# vim user.ldif

< Modifique os Campos para DN, UID, SN, CN, homeDirectory e mail para
o seu Nome e Sobrenome >

2# ldapadd -x -D "cn=admin,dc=dexter,dc=com,dc=br" -f
user.ldif -W
```

### Anotações:

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

## Servidor OpenLDAP

**Servidor: DataCenter**

## ➤ Criando os Grupos:

```
1# vim group.ldif
< Ajuste o campo nome.sobrenome para seu usuário >
2#ldapadd -x -D "cn=admin,dc=dexter,dc=com,dc=br" -f
group.ldif -W
```

## ➤ Apagando o Usuário Fox Bennet:

```
1# ldapdelete -x -D "cn=admin,dc=dexter,dc=com,dc=br"  
uid=fox.bennett,ou=users,dc=dexter,dc=com,dc=br -W
```

Para deletar informações da Base é necessário ser Administrador.

### Anotações:

[illegible]

## Servidor OpenLDAP

**Servidor: DataCenter / Linux Interna**

## Alterando um registro existente:

```
1# vim modify.ldif
2# ldapmodify -x -D "cn=admin,dc=dexter,dc=com,dc=br" -f
modify.ldif -W
```

Iremos utilizar uma ferramenta para administrar o LDAP Proxy:

## ApacheDirectoryStudio – Acesse pela máquina Linux Interna em /usr/apacheds/ApacheDirectoryStudio

### Anotações:

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.



## Servidor OpenLDAP

**Servidor: Linux Interna**

## ETAPA 1

New LDAP Connection

LDAP

Network Parameter

Please enter connection name and network parameters.

Connection name:

LDAP Proxy

Network Parameter

Hostname:

192.168.200.131

Port:

389

Encryption method:

No encryption

Server certificates for LDAP connections can be managed in the ['Certificate Validation'](#) preference page.

Provider:

Apache Directory LDAP Client API

Check Network Parameter

☐ Read-Only (prevents any add, delete, modify or rename operation)

### Anotações:

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

## Servidor OpenLDAP

**Servidor: Linux Interna**

## ETAPA 2

New LDAP Connection

Authentication

Please select an authentication method and input authentication data.

LDAP

Authentication Method

Simple Authentication

Authentication Parameter

Bind DN or user: cn=admin,dc=dexterproxy,dc=com,dc=br

Bind password: .....

☒ Save password

Check Authentication

▶ SASL Settings

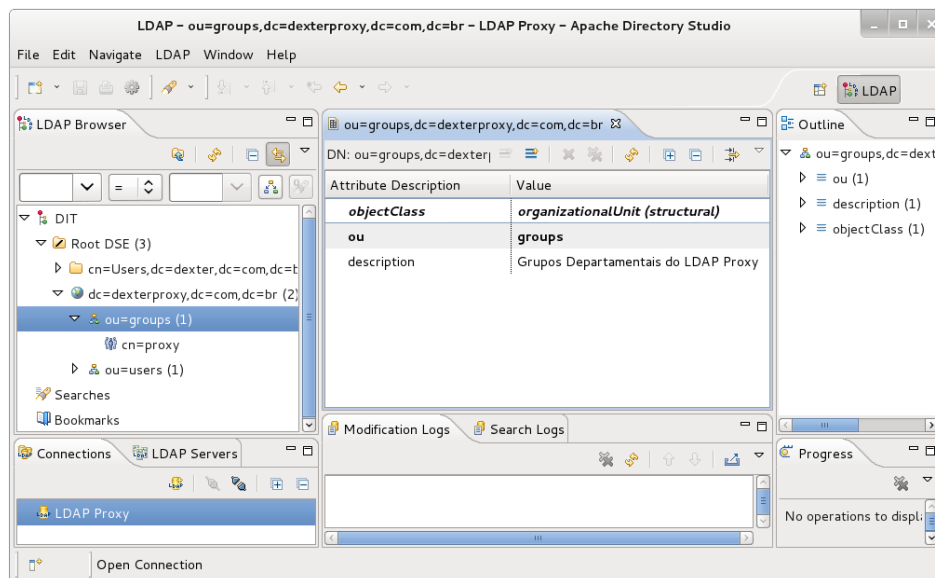
▶ Kerberos Settings

### Anotações:

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

## Servidor OpenLDAP

**Servidor: Linux Interna**



### Anotações:

[illegible]

## Servidor OpenLDAP

**Servidor: DataCenter**

## Fazendo BACKUP do LDAP:

```
1# ls /var/lib/ldap/
2# /etc/init.d/slapd stop
3# slapcat -l /etc/ldap/backup.base.ldap
4# rm -rf /var/lib/ldap/*
5# /etc/init.d/slapd start
6# ldapsearch -x -LLL
7# /etc/init.d/slapd stop
8# slapadd -l /etc/ldap/backup.base.ldap
9# /etc/init.d/slapd start
```

### Anotações:

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

## Próximos Passos

---

Para que você tenha um melhor aproveitamento do curso, participe das seguintes atividades disponíveis no Netclass:

- Executar as tarefas do **Practice Lab**;
- Resolver o **Desafio Appliance Lab** e postar o resultado no Fórum Temático;
- Responder as questões do **Teste de Conhecimento** sobre o conteúdo visto em aula.

**Mãos à obra!**

# 4LINUX

OPEN SOFTWARE SPECIALISTS



**ESPECIALISTA EM "JUNTAR AS PEÇAS" DO MUNDO OPEN SOURCE**

[WWW.4LINUX.COM.BR](http://WWW.4LINUX.COM.BR)