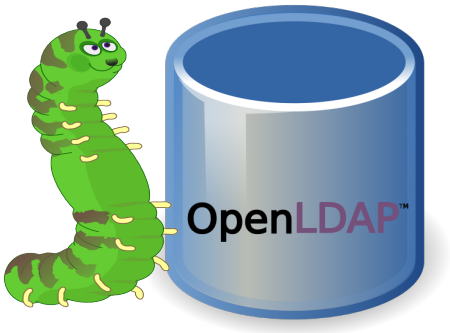
Curso 452

Linux Security Servers in Cloud

Versão 2015_3.0

Servidor OpenLDAP



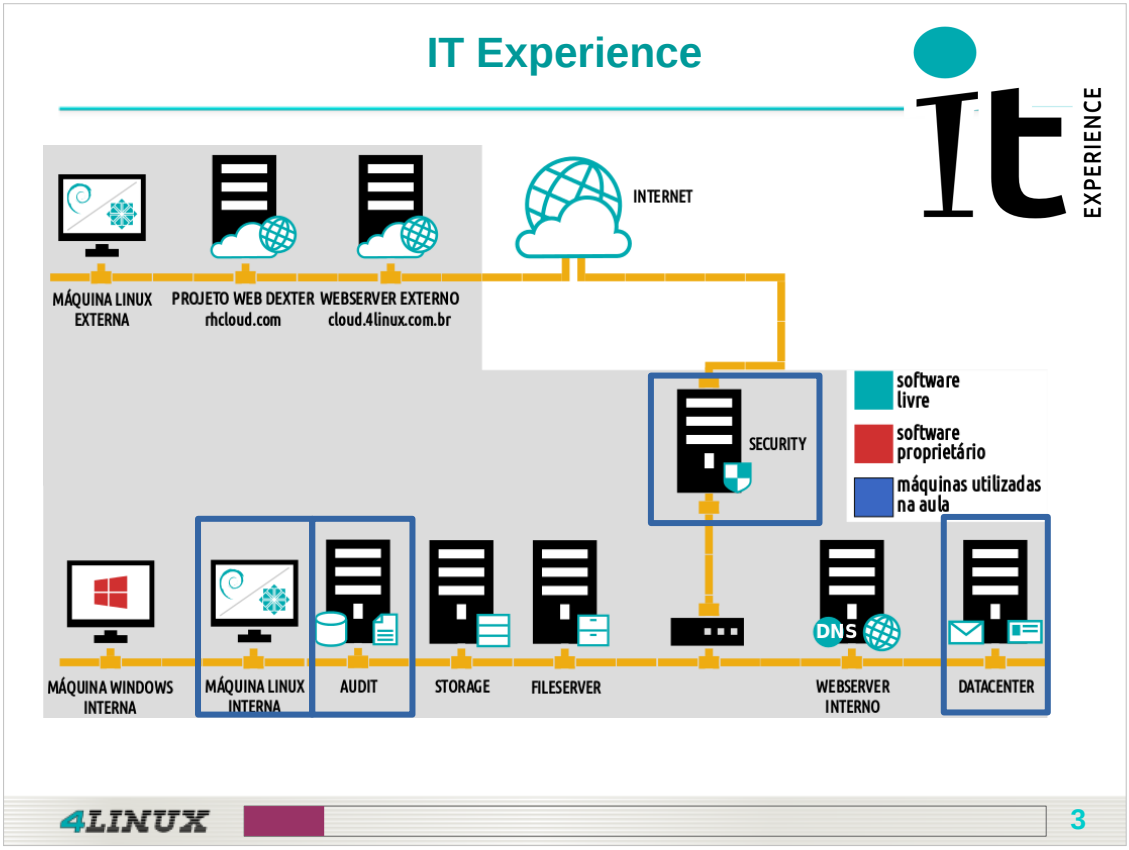
LDAP

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)“


IT Experience
IT EXPERIENCE
INTERNET
MÁQUINA LINUX EXTERNA
PROJETO WEB DEXTER rhcloud.com
WEBSERVER EXTERNO cloud.4linux.com.br
SECURITY
software livre
software proprietário
máquinas utilizadas na aula
MÁQUINA WINDOWS INTERNA
MÁQUINA LINUX INTERNA
AUDIT
STORAGE
FILESERVER
DNS
WEBSERVER INTERNO
DATACENTER
4LINUX
3

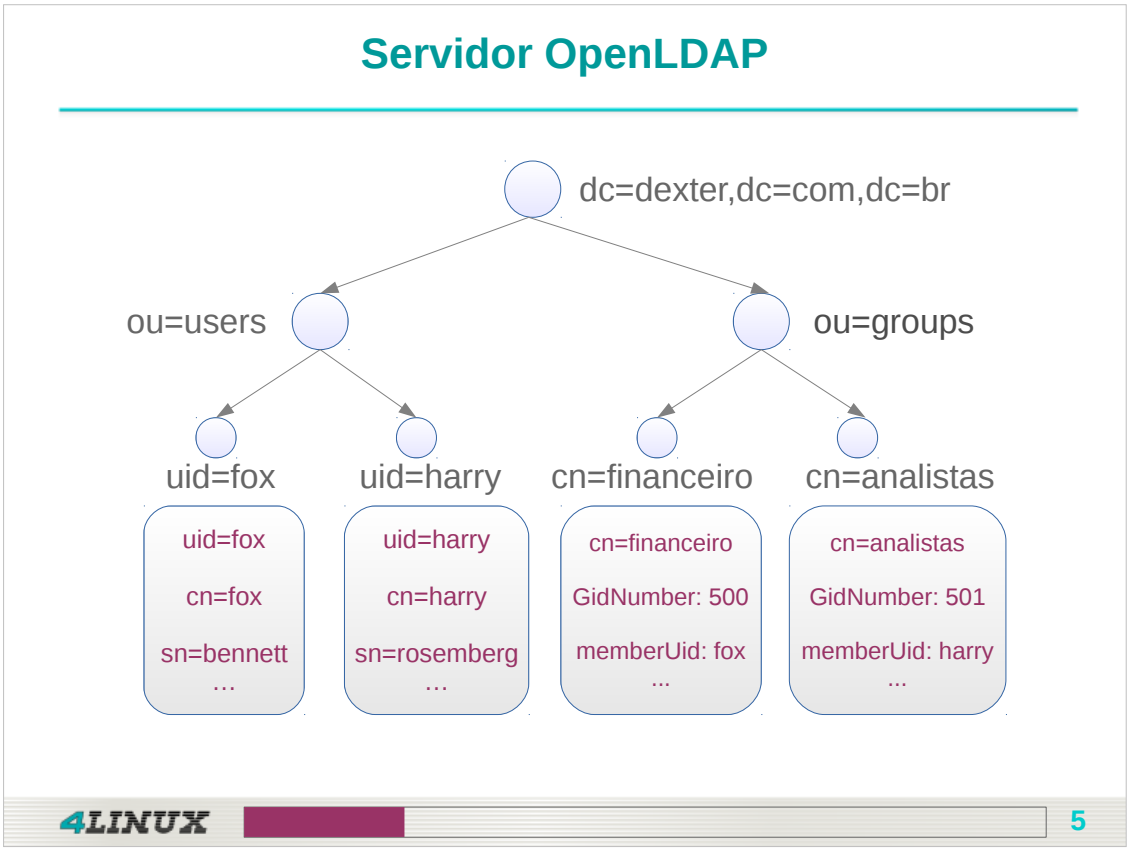
Anotações:

Objetivos da Aula

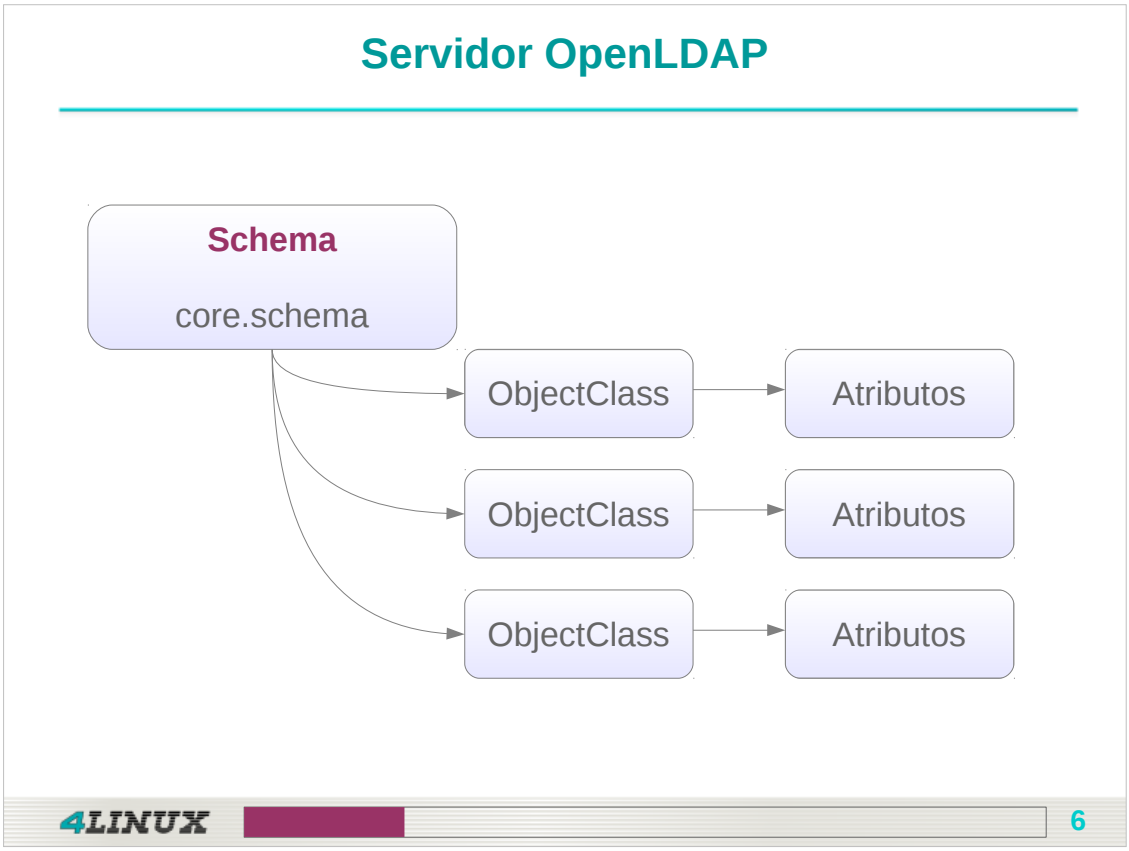
Aula 07

- Entender a estrutura do LDAP;
  - Schemas;
  - ObjectClass;
  - Atributos;
- Inserir e modificar dados com arquivos LDIF;
- Administrando o LDAP com ApacheDirectoryStudio;
- Fazendo backup da base LDAP.

Anotações:



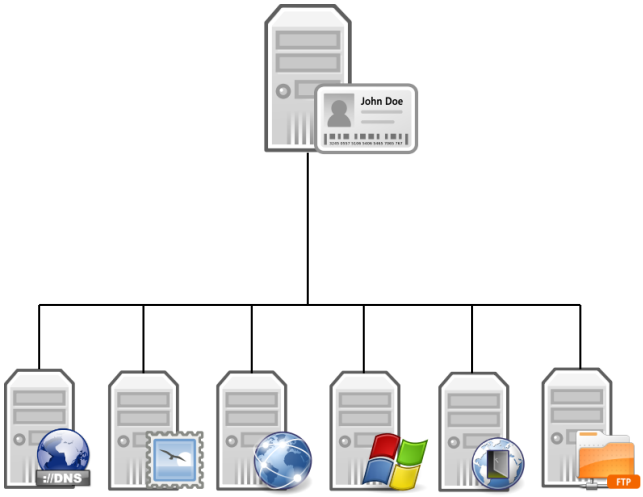
O LDAP é um protocolo de rede que roda sobre o TCP/IP que permite organizar os recursos de rede de forma hierárquica, como uma árvore de diretório, onde temos primeiramente o diretório raiz, em seguida a rede da empresa, o departamento e por fim o computador do funcionário e os recursos de rede (arquivos,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



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:

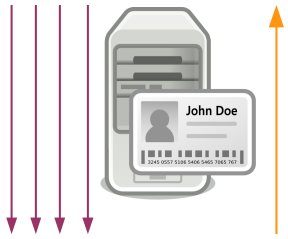


Anotações:

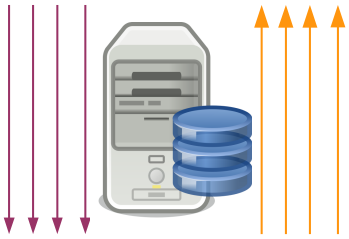
Servidor OpenLDAP

Diretórios vs DBMS:

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



Leitura Escrita



Leitura Escrita

Anotações:

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:

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**

Anotações:

Servidor OpenLDAP

Servidor: DataCenter

- **Consulta simples ao LDAP:**

```
1# 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:

Servidor OpenLDAP

Servidor: DataCenter

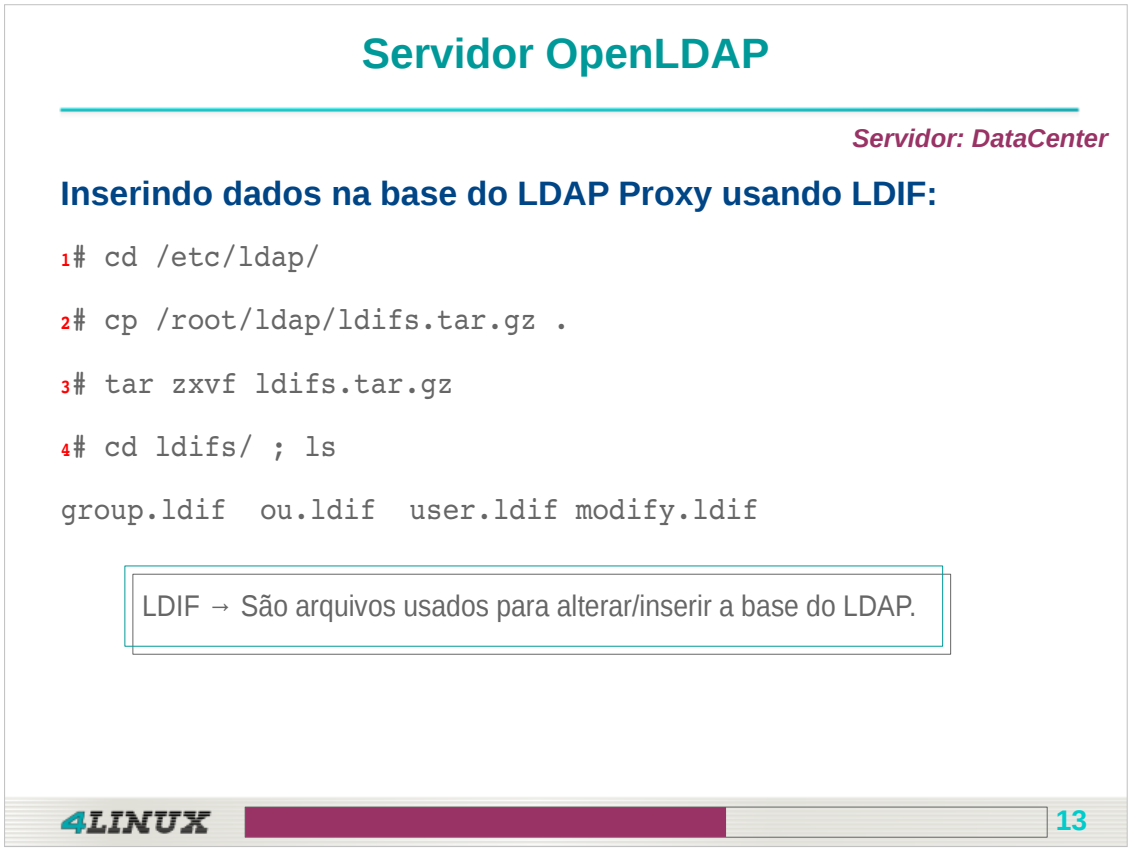
- **Configurando o LDAP:**

```
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:



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:

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:

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:

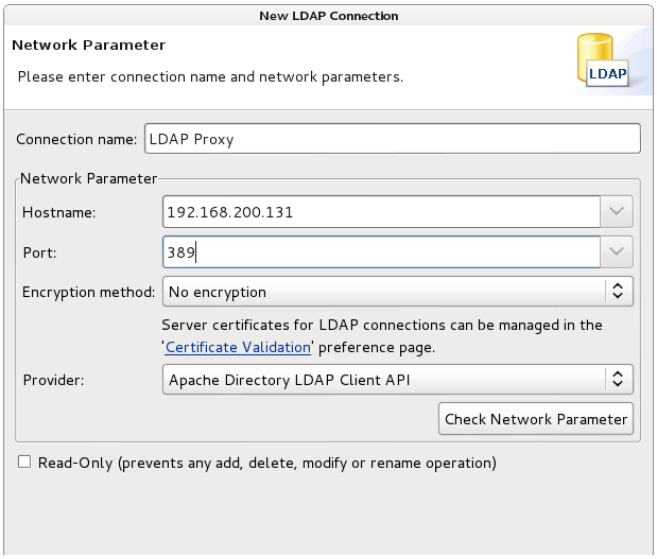
ApacheDirectoryStudio – Acesse pela máquina Linux Interna em /usr/apacheds/ApacheDirectoryStudio

Anotações:

Servidor OpenLDAP

Servidor: Linux Interna

ETAPA 1

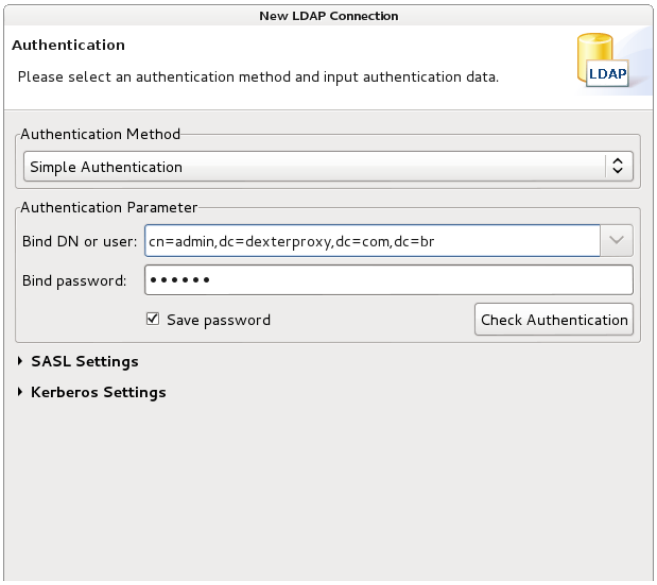


Anotações:

Servidor OpenLDAP

Servidor: Linux Interna

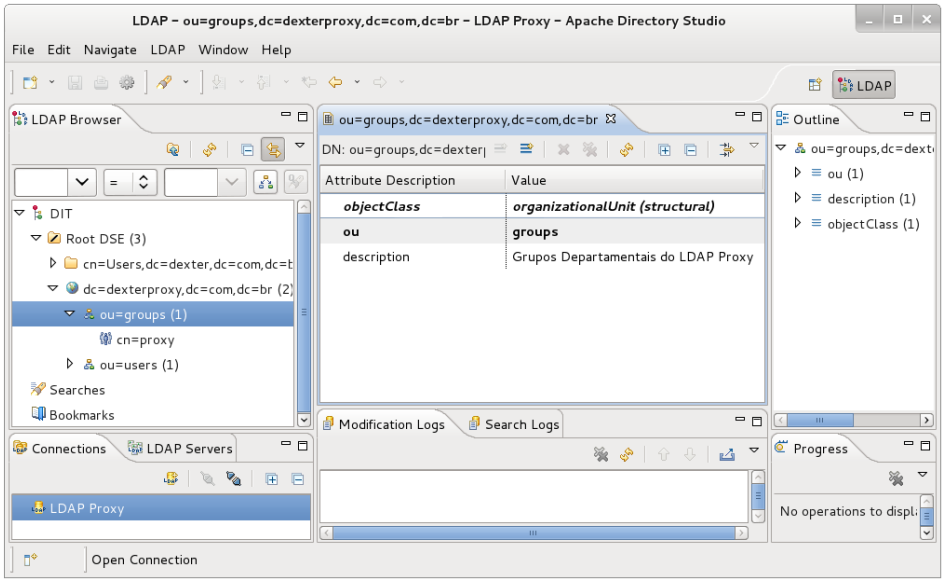
ETAPA 2



Anotações:

Servidor OpenLDAP

Servidor: Linux Interna



Anotações:

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:

Próximos Passos

Para que você tenha um melhor aproveitamento do curso, participes 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!