

UNIVERSIDADE CATÓLICA DE PELOTAS

RONALDO CUNHA

PROTOCOLO LDAP

Pelotas

2021

Introdução

Este trabalho não tem o intuito de aprofundar o conteúdo sobre o LDAP, mas mostrar uma visão geral do que é o LDAP, para que serve, e como damos inicio a instalação e configuração do servidor. Deixando também referências e bibliografias da confecção do mesmo para quem deseja saber mais sobre o assunto.

LDAP

LDAP (*Lightweight Directory Access Protocol*). Traduzindo, é um Protocolo leve de acesso a diretórios

O que são serviços de diretórios?

Segundo a Wikipédia: “Um **serviço de diretório** é um software que armazena e organiza informações sobre recursos e os usuários de uma rede de computadores, e que permite aos administradores de rede gerenciar o acesso de usuários e sistemas a esses recursos. Além disso, os serviços de diretório atuam como uma camada de abstração entre os usuários e esses recursos. A palavra directory em inglês poderia ser melhor traduzida por catálogo, no sentido de uma lista ordenada com descrição curta dos itens, não necessariamente arquivos”

Esta definição deixa claro como são gerenciados o conteúdo de uma rede de computadores através deste serviço.

O que faz este serviço?

Centraliza a gestão de recursos, ou seja, simplifica o uso para a sua finalidade que é gerenciar aplicações clientes, como por exemplo, autenticar usuários e leitores de e-mail, onde será solicitado informações para que possam ser acessados estes serviços na rede. Neste ponto podemos até confundir com uma banco de dados, mas, não podemos esquecer que estas informações estão no servidor LDAP, este por sua vez é controlado por gerenciadores criados com regras especificas para este fim, ou seja, o uso de diretório.

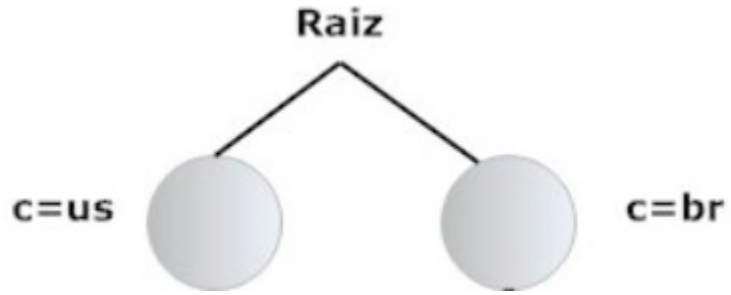
Podemos citar algumas aplicações que fazem uso do LDAP:

- Gerenciar logins na rede através de usuários e senhas;
- Login para estações que usam Windows que utilizam Samba ou estações com Linux;

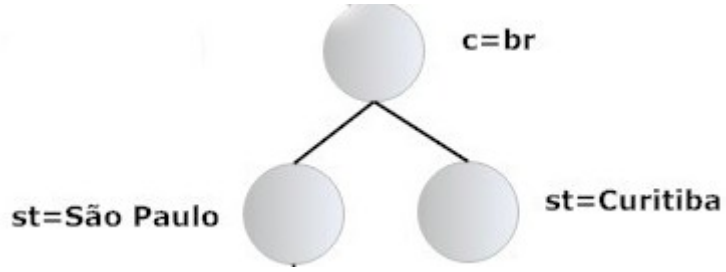
- Serviços de e-mail(IMAP, POP3, SMTP);
- Acesso à internet com uso do proxy;
- Cadastro de cliente;
- Cadastro de ;
- Permissões para acesso e administração do Diretório ou partes dele.

Funcionamento da estrutura de um Diretório

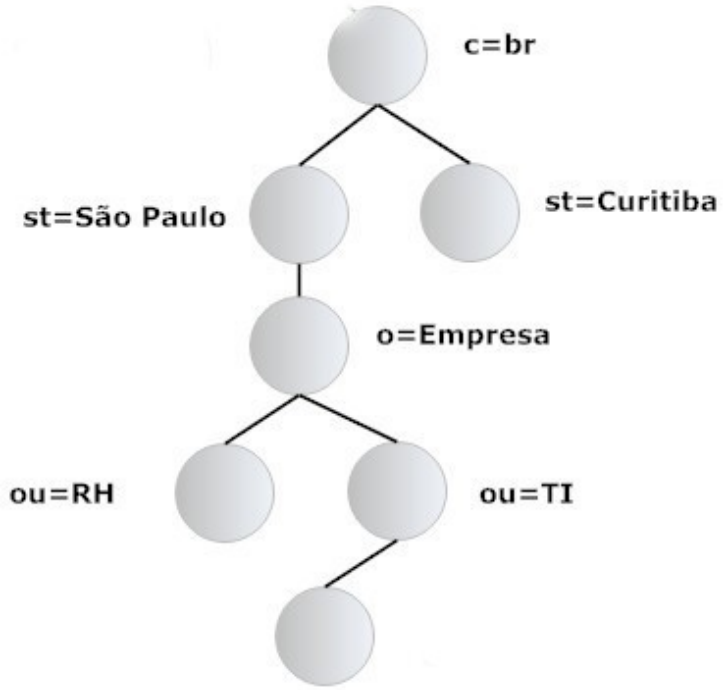
Podemos dizer que no LDAP a estrutura nos lembra uma árvore, esta estrutura serve para organizar e representar também limites. Nesta figura [1] esta representando as entradas de países que representam o topo da estrutura.



Abaixo (figura [2]) esta mostrando o seguimento da estrutura, ou seja, após os países temos os estados.



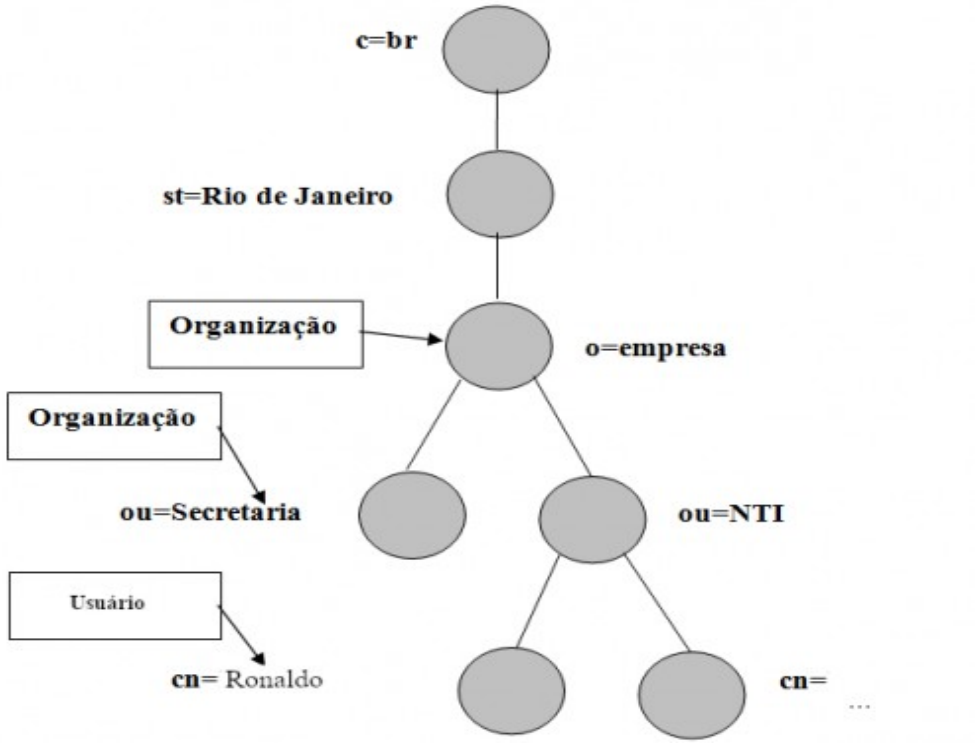
Na continuação notamos que, em cada país esta divida nos territórios e suas respectivas empresas, ou seja, temo no Brasil, Curitiba, a empresa separadas pelos seus setores, na imagem (figura [3]) abaixo mostra claramente .



Neste modelo, temos a estrutura e a representação de suas entradas:

Entrada	**Significado**
c	*country - país*
st	*stateOrProvinceName - estado*
l	*localityName - cidade*
street	*streetAddress - endereço*
o	*organizationName - organização*
ou	*organizationalUnit - unidade organizacional*

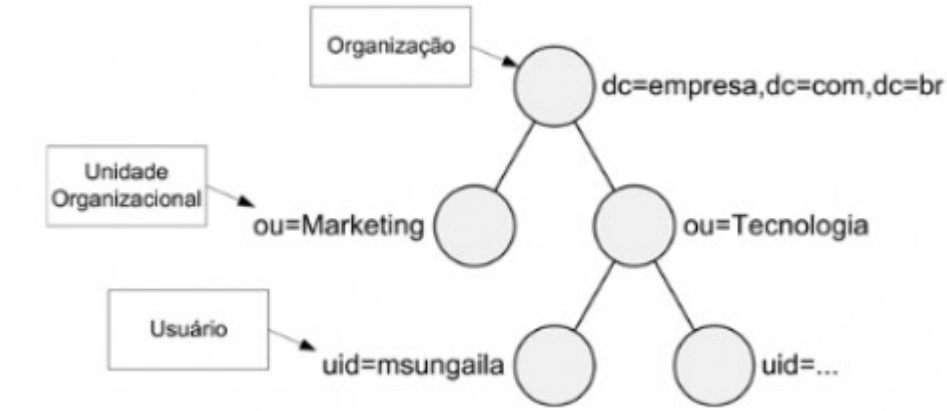
Na figura [4] temos um modelo de diretório baseado na estrutura de localidade



O armazenamento de dados no servidor de Diretórios segue a hierarquia a qual pertence. Neste exemplo, temos algo assim:

```
cn=Ronaldo
ou=Secretaria
o=empresa
st=Rio de Janeiro
c=br
```

Chamamos este tipo de identificação de DN (Distinguished Name) ou nome único. O DN serve para indicar todos os ramos da árvore LDAP, desde sua base, que no nosso exemplo é (c=br) até sua parte final, o usuário. Nesta construção de árvore, podemos também usar os Diretórios para usar domínios Internet (dc). Sendo assim, poderá utilizar o serviço para localizar os domínos utilizados. Como exemplo temos a figura [5],



Neste exemplo podemos notar mudança na entrada, note o DN.

```
uid=msungalia
ou=usuarios
dc=empresa
cd=com
c=br
```

Resumindo

Com base em (GIL, 2012), o LDAP funciona parecido com diretórios de sistema sem nenhuma ligação com base, ou seja, ele não armazena arquivos e sim recursos. No armazenamento é utilizado objetos e atributos que chamamos de schema, que nada mais é do que um arquivo texto lido pela base LDAP quando usado. Temos também atributos opcionais e obrigatórios que é o ObjectClass. Este atributo conterá o tipo de armazenamento. Com estas definições, notamos que no LDAP os registros são únicos, isso quer dizer que não haverá registros iguais no mesmo diretório.

Implementando LDAP através do OpenLDAP

Sempre quando vamos implementar algo novo, existem algumas dúvidas. Falando do LDAP, vemos que existem várias alternativas para implantação do mesmo em software proprietário, ou seja, software pago. Também temos alternativa de software aberto, o OpenLDAP.

Pré-requisitos – OpenLDAP

Sempre quando vamos implementar algo novo podem existir pré-requisitos para o funcionamento do mesmo, no caso do LDAP algumas instalações básicas serão necessárias. Instalações estas que são necessárias para o funcionamento do servidor LDAP. Serão abordados aqui um método que serve para qualquer distribuição. Pois no caso no *Debian*, há uma ferramenta do próprio *Debian*, o *apt-get* ou o *aptitude*. Lembrando que para compilar pacotes temos que ter alguns softwares instalados. Lembrando que a maioria das distribuições já trás programas para compilação por padrão.

O básico para esta etapa:

- Ferramenta para geração de executáveis - *GNU make*;
- Compilador *C* padrão *ISO/ANSI*;
- Compactadores *bzip2* e *gzip*
- *TAR* - Utilitário para extração de pacotes-fonte
- *PATCH* - Utilitário para correções e recursos adicionais

Na distribuição Debian basta executar o comando abaixo para instalação.

```
# apt-get install build-essential
```

Lembrando que os pacotes baixados e que forem compilados, devem estar no diretório /usr/src*, pois geralmente é local para compilação dos programas.*

OpenSSL

Outro detalhe é a criptografia do sistema, o OpenSSL disponibiliza ferramentas para tal, disponíveis no site http://www.openssl.org/

Na maioria das distribuições já vem tal ferramenta nativamente, mas, caso haja necessidade do código fonte, basta baixar, compilar e instalar com os comandos a seguir:

```
# cd /usr/src
# tar -xf openssl-1.0.2o.tar.gz
# cd openssl-1.0.2o
# ./config –prefix=/usr/local/ssl –openssldir=/usr/local/ssl
shared zlib
# make
# make test
# make install
# ldconfig -v
```

Não esquecendo que em distribuições *Debian*, basta usar o comando abaixo para instalação do pacote openssl

```
# apt-get install openssl libssl-1.0.2o
```

Berkeley DB

As informações serão armazenadas em alguma base, para este exemplo será usado o Berkeley que pode ser obtido no da Oracle. Como já dito anterior, aqui também, as distribuições oferecem o gerenciador de pacotes nativamente. Então, tendo necessidade, basta baixar e instalar com estes comandos:

```
# cd /usr/src
# tar -xf db-4.6.19.tar.gz
# cd db-4.6.19/build_unix
# ../dist/configure –prefix=/usr/local
# make
# make install
# ldconfig
```

No caso do *Debian* basta usar o comando a seguir:

```
# apt-get install db4.2-util
```

No uso do apt-get, será instaladas dependências necessárias ao funcionamento correto desta.

Cyrus-SASL

O conceito de SASL segundo o site ArcGIS - Simple Authentication and Security Layer, é uma estrutura para autenticação e segurança de dados em protocolos de internet.

Na maioria das distribuições são oferecidas essa ferramenta de forma nativa, mas, caso haja necessidade de instalação das mesmas, baixe e instale conforme comandoas abaixo:

```
# cd /usr/src
# tar -xf cyrus-sasl-2.1.27.tar.gz
# cd cyrus-sas-2.1.27
# ./configure –prefix=/usr –enable-static –mandir=/usr/share/man –
infodir=/usr/share/info
# make
# make install
```

Instalação do OpenLDAP

Lembrando que antes de fazer a instalação, verifique se sua distribuição já não possui o pacote de instalação. Caso não tenha, ficam aqui os passos a serem seguidos para baixar, compilar e instalar o OpenLDAP. Não esqueça sempre de baixar e instalar de sites oficiais. No nosso caso, use o site oficial do OpenLDAP.Há tambem a opção de baixar o Guia do Administrador

Abaixo como compilar e instalar o OpenLDAP da última versão disponível em outubro de 2021.

```
# cd /usr/src
# tar -xf openldap-2.5.8.tgz
# cd openldap-2.5.8
# ./configure –with-threads –with-tls
# make depend
# make
# make install
```

Se você utiliza o Debian poderá instalar os pacotes como este comando:

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

Mas, atenção, durante a instalação, você deverá criar uma senha para usuário `admin`. Isto é apenas um detalhe para o inicio da configuração da instalação.

Configuração do OpenLDAP

Desde momento em diante irá começar a configuração do servidor, onde serão definidos o conteúdo que será armazenado, como será armazenado e em qual formato, e também a senha para acessar o servidor.

Para realizar esta configuração, deve ser utilizado um editor de texto e criar o arquivo com configurações com o nome de `slapd.conf` que está localizado no diretório `etc/ldap`. Primeiramente deve-se definir a base de dados a ser utilizada, neste exemplo vamos utilizar o formato BDB, junto será definido uma senha também para o administrador desta base de dados, abaixo configuração do arquivo (SUNGAILA, 2008, p. 28). Abaixo o conteúdo do arquivo baseado :

```
# /etc/ldap/sldap.conf
# Versão de protoclo utilizado para conexão pelo clientes
allow bind_v2
# Schema e definições de classes de objeto
include/etc/ldap/schema/core.schema
include/etc/ldap/schema/cosine.schema
include/etc/ldap/schema/nis.schema
include/etc/ldap/schema/inetorgperson.schema
# Arquivos de controle dos processos do servidor
pidfile/var/run/slapd/slapd.pid
argsfile /var/run/slapd/slapd.pid
# Modulos
modulepath /usr/lib/ldap
moduleload back_bdb
# Parâmetros especificos do tipo de base
backend bdb
# Base de dados
database bdb
# Estrutura de diretório e administrador
suffix “dc=empresa,dc=com,dc=br
rootdn “cn=Manager,dc=empresa,dc=com,dc=br
rootpw senhasecreta
# Local armazenamento de dados
directory /var/lib/ldap
```

Significado dos itens do arquivo:

Entrada	Significado
include	inclusão de arquivos com tipo de dados
pidfile	contém o número do processo slapd
argsfile	contém argumentos passados ao servidor na inicialização
modulepath	local dos módulos para o backends para armazenamento de dados
moduleload	carga do módulo para o backend
backend	definição de parametros para o backend BDB
database	definição do database com informações do OpenLDAP na base Berkeley DB
suffix	parte da estrutura que definirá a hierarquia que serão armazenados o serviço de diretório
rootdn	administrador da base, não é o mesmo root do sistema, geralmente usado **Manager** ou **admin**
rootpw	senha de acesso ao servidor LDAP, devendo ser usado **slappasswd** para criptografar a senha
directory	localização dos arquivos binários com a base do servidor

Arquivos LDIF

Sabemos que o LDAP não possue um gerenciador que possamos manibular tabelas como em um banco de dados. Para podermos manipular os dados, são criados arquivos textos, estes são utilizados para inserir novos dados na base, chamamos estes arquivos de LDIF. Para criarmos um arquivo LDIF devemos utilizar um editor de textos para criação do mesmo com o seguinte conteúdo (SUNGAILA, 2008, p. 32):

```
# arquivo empresa.ldif
dn: dc=empresa,dc=com,cd=br
objectClass: dcObject
objectClass: organization
o: Empresa Ltda
dc: empresa
```

Após criar o arquivo, este deve ser incluído na base, para fazermos isto, devemos utilizar o comando *ldapadd* que deve ser executado como administrador.

Abaixo o comando a ser utilizado:

```
$ ldapadd -x -D “cn=Manager,dc=empresa,dc=com,dc=br” -W -f
empresa.ldif
Enter LDAP Password:
adding new entry “dc=empresa,dc=com,dc=br”
```

Com o servidor instalado, vimos a necessidade da manipulação de arquivos LDIF, é nele que ativamos a sincronização e, indicados alguns atributos, definimos filtros de pesquisa, bem como a configuração de usuários.

Ainda há uma série de configurações que podem ser realizadas, mas, não será tópico aqui desta pesquisa, pois estou apenas demonstrando o inicio de uma implementação deste protocolo.

No modo avançado, segundo (SUNGAILA, 2008), será possível modificar dados em um diretório, mesmo não sendo um tarefa muito comum, mas, podemos utilizar a ferramenta *ldapmodify* processando um arquivo LDIF que contém os dados a serem alterados. Onde podemos indicar o tipo de ação a ser realizada, podemos acrescentar atributos, remover valores de um determinado atributo, ou mesmo substituir um valor do atributo.

Além de mudanças, podemos também utilizar o LDAP numa associação com catálogo de endereços de e-mail compartilhado, não sendo mais necessário uma distribuição de uma lista para todos usuários de uma empresa contendo seus respectivos e-mails.

Completando os exemplos anteriores, podemos também utilizar *schemas* em diretório LDAP, que é um conjunto de regras que define atributos, classe de objetos e controles indicando onde cada dado pode ser armazenado. O protocolo LDAPv3 define um *schema* básico para os objetos comuns de uma rede como país, cidade, organizações, usuários, pessoas e grupos e dispositivos.

Vimos até o momento foi mostrado exemplos do que podemos realizar na base LDAP para criação de usuários com o uso de arquivos LDIF, mas, notamos que seria muito trabalhoso e pouco produtivo. Sendo assim, podemos utilizar scripts para várias etapas, tornando assim menos trabalhoso a manipulação dos dados com LDAP.

A seguir 2 exemplos de *scripts* , adicionando e excluindo (SUNGAILA, 2008)

add_users_passwd.sh

```
#! /bin/bash

I="1"

while [ "$I" -lt "21" ] ; do
        useradd usuario$I -p `echo usuario$I | mkpasswd -s -H md5` -m -d /home/usuario$I -c "Fulano$I da Silva"
        echo "User usuario$I has been added..."
        I=`expr $I + 1`
done
```

del_users_passwd.sh

```
#! /bin/bash

I="1"

while [ "$I" -lt "21" ] ; do
        userdel -r usuario$I
        echo "User usuario$I has been removed..."
        I=`expr $I + 1`
done
```

CONCLUSÃO

O protocolo LDAP pode ser utilizado em diversas áreas, pode ser utilizado para inúmeros serviços tanto em pequenas empresas como em grandes corporações.
Na minha opinião, o OpenLDAP é uma das melhores opções, pois além de ser um software GNU, é também um protocolo que pode ser integrado com diversos serviços.

Como pode ser visto, este trabalho foi traçado com o intuito de dar uma visão geral sobre o que é o LDAP, a utilização do OpenLDAP e, consequentemente criarmos uma visão de onde partir para nos aprofundar no assunto. Com certeza a partir deste trabalho, juntamente com todas referências aqui deixadas, será possível para aquele que tiver interesse aprender mais sobre o assunto deste protocolo de grande valia para nossas redes de computadores.

Referências e bibliografias:

Imagens [1], [2] e [3] foram compiladas pelo autor, coletadas do site Blog Stato, acesso em out. de 2021.

Imagem [4] foi compilada pelo autor, coletadas do site DevMedia, acesso em out. de 2021.

Imagem [5] Utilizada do site Novatec Marcos Sungalia - OpenLDAP, aceso em out. de 2021.

SSL - Disponível em https://github.com/openssl/openssl, acesso em out. de 2021.

GNU - Disponível em https://www.gnu.org/, acesso em out. de 2021.

OpenSSL - Disponível em https://www.howtoforge.com/tutorial/how-to-install-openssl-from-source-on-linux/, acesso em out. de 2021.

Berkeley DB - Disponível em https://www.oracle.com/database/berkeley-db/index/, acesso em out. de 2021.

OpenLDAP - Disponível em https://www.openldap.org, acesso em out. de 2021.

ArcGis - Disponível em https://enterprise.arcgis.com, acesso em out. de 2021.

CARTER, Gerald. LDAP Administração de Sistemas. Rio de Janeiro: Alta Books, 2009.*

GIL, A. P. . OpenLDAP Extreme. 1. ed. Rio de Janeiro: Brasport, 2012.*

SUNGAILA, Marcos. Autenticação Centralizada com OpenLDAP. 1. ed. São Paulo: Novatec, 2008.*

Introdução ao OpenLDAP - Disponível em https://www.linux.ime.usp.br/~cef/mac499-06/monografias/erich/html/ch01s09.html, acesso em out. de 2021.

Instalando o OpenLDAP, disponível em https://www.vivaolinux.com.br/topico/OpenLdap/Instalando-OpenLDAP, acesso em out. de 2021.

** Conteúdo criado de acordo com referências e bibliografias citadas acima. Que também podem ser utilizadas de maneira avançada na implementação e manipulação do OpenLDAP*