FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Guilherme Berbelini

Demonstrando Autenticação Centralizada com o OpenLDAP

Americana, SP

2017

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Guilherme Berbelini

Demonstrando Autenticação Centralizada com o OpenLDAP

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação do Professor Ricardo Kiyoshi Batori.

Área de concentração: Administração de Sistemas Operacionais de Redes

Americana, SP.

2017

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

B427d BERBELINI, Guilherme

Demonstrando autenticação centralizada com o OpenLDAP. / Guilherme Berbelini. – Americana, 2017.

49f.

Monografia (Curso de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Profa. Ms. Ricardo Kiyoshi Batori

1 Segurança em sistemas de informação 2. Autenticação de acesso 3. Redes de computadores I. BATORI, Ricardo Kiyoshi II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: 681.518.5

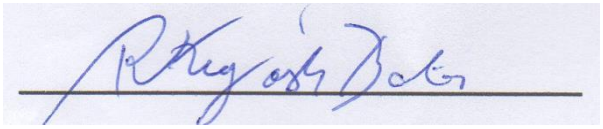
681.519

Demonstrando Autenticação Centralizada com o OpenLDAP

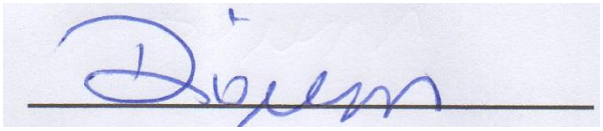
Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Administração de Sistemas Operacionais de Redes

Americana, 13 de dezembro de 2017.

Banca Examinadora:



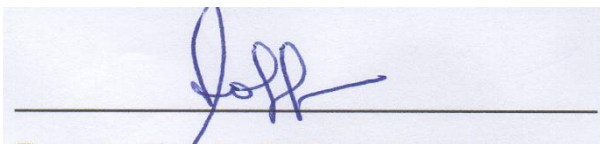
Ricardo Kiyoshi Batori (Presidente)
Mestre
Faculdade de Tecnologia de Americana



Diógenes de Oliveira (Membro)

Mestre

Faculdade de Tecnologia de Americana



Renato Kreid Soffner (Membro)

Doutor

Faculdade de Tecnologia de Americana

AGRADECIMENTOS

Em primeiro lugar, agradeço a Deus por ter me proporcionada sabedoria e saúde nesta caminhada, aos meus pais que me incentivaram todos esses anos, ao Professor Orientador Ricardo Kiyoshi Batori e aos meus amigos que participaram diretamente e indiretamente nesta monografia.

RESUMO

O objetivo desta monografia é a demonstração de um servidor com o software de código aberto *OpenLDAP*, que serve para armazenar, atualizar e pesquisar informações de objetos, como pessoas, computadores, periféricos, entre outros. Neste trabalho de Conclusão de Curso utiliza-se o *OpenLDA*P na montagem de um diretório para prover autenticação centralizada em serviços de rede, demonstrando ser uma solução estratégica e livre para o ambiente de sistemas da informação da Faculdade de Tecnologia de Americana.

Palavras Chave: Autenticação Centralizada; *OpenLDAP*; Demonstração.

ABSTRACT

The purpose of this monograph is to demonstrate a server with OpenLDAP open source software, which is used to store, update and search for information about objects such as people, computers, peripherals, among others. In this work, OpenLDAP is used in the assembly of a directory to provide centralized authentication in network services, proving to be a strategic and free solution for the information systems environment of the Faculty of Technology of Americana.

Keywords: *Centralized Authentication; OpenLDAP; Demonstration.*

GLOSSÀRIO

ACL: *Access Control List*, lista que define as permissões de acesso de um usuário a um determinado serviço.

Daemon: é um programa de computador que executa como um processo em plano de fundo.

Hostname: Nome do terminal de rede.

Intranet: Rede de computadores privada.

OpenSSL: Implementação livre e de código aberto que implementa os protocolos *SSL* e *TLS*.

Print *Screen*: Captura de imagem presente na tela.

SASL: *Simple Authentication and Security Layer*, *framework* para autenticação e segurança de dados em protocolos da Internet.

SSL: *Secure Sockets Layer*, protocolo de segurança.

Schemas: Regras em relação à organização das informações.

Script: Linguagem de programação.

Software: Sequência de instruções escritas para serem interpretadas por um computador com o objetivo de executar tarefas específicas.

TLS: *Transport Layer Security*, protocolo de segurança.

Web: ***World Wide Web***, rede mundial de computadores.

Login: Acesso a um sistema.

Usernames: Nome do usuário.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

1 INTRODUÇÃO

Atualmente, em qualquer organização, é praticamente necessário centralizar a autenticação dos usuários, com o objetivo de reduzir custos e facilitar a administração do Administrador de Sistemas, pois gerenciar as contas dos vários serviços de rede exige muito empenho, tempo e infraestrutura.

Segurança é outro ponto chave para centralizar a autenticação, com o número reduzido de credenciais, ou seja, uma credencial de acesso para vários serviços, viabiliza ao Administrador de Sistemas estabelecer e gerenciar uma única política de acesso para as credenciais, por exemplo, o uso de uma senha forte, a troca periódica de senha e a expiração das credenciais, além de simplificar e centralizar o controle de acesso. Outro fator que contribui para a segurança é a redução de possíveis pontos de falhas com as diversas bases dos dados contendo informações sigilosas dos usuários.

Possuir um Diretório ultrapassou a barreira de Boas Práticas em TI, segundo Silva (2010) “Esta solução provê recursos que atendem aos princípios de autenticidade e não-repúdio”, desse modo nesta monografia usaremos o OpenLDAP em alternativa aos serviços de diretórios comerciais, tal como, o *Active Directory*, na montagem de um diretório fictício com o domínio “fatec.br” para centralizar a autenticação e interagir com os serviços de rede, apesar que o uso de Diretórios é bem mais amplo que isto.

Em primeiro plano, abordaremos a conceptualização e definição do software, posteriormente os comandos de gerenciamento e administração da ferramenta e pôr fim a configuração técnica do *OpenLDAP* e a integralização do mesmo com os serviços de rede, entre os serviços de redes com suporte a Autenticação ao *OpenLDAP*, citaremos especificamente a autenticação nos softwares, *ProFTPD* (Servidor de *File Transfer Protocol*) e Apache (*Web Server*), além do próprio Linux.

A escolha do serviço de diretório *OpenLDAP* as demais opções, é totalmente inteligível, o software é *Open-Source*, isto é, uma opção totalmente gratuita com um amplo suporte da comunidade pela Internet.

Para plataforma de teste deste ambiente, adotamos como distribuição no servidor que provém os serviços e nos clientes o *Ubuntu Server* 16.04.3 LTS.

2 Autenticação Centralizada

Segundo Sócrates Filho (2009), o conceito de autenticação conforme a Segurança da Informação é o processo que busca a identidade digital do usuário de um sistema no momento que ele requisita um *login*, que é comumente formado por um nome e uma senha. Na pluralidade cada serviço e sistema possuí seu método particular de autenticação, desta forma, a monografia busca reunir todos os dados necessários dos usuários para a autenticação (nome e senha) em uma única base de dados, de modo que interaja e centralize a autenticação nos sistemas e serviços.

2.1 Porque Centralizar a Autenticação?

Quase todos os serviços utilizam *login*, a quantidade de serviços e usuários está cada vez maior e a equipe de TI cada vez menor, o que se torna insustentável administrar uma base de dados para cada serviço.

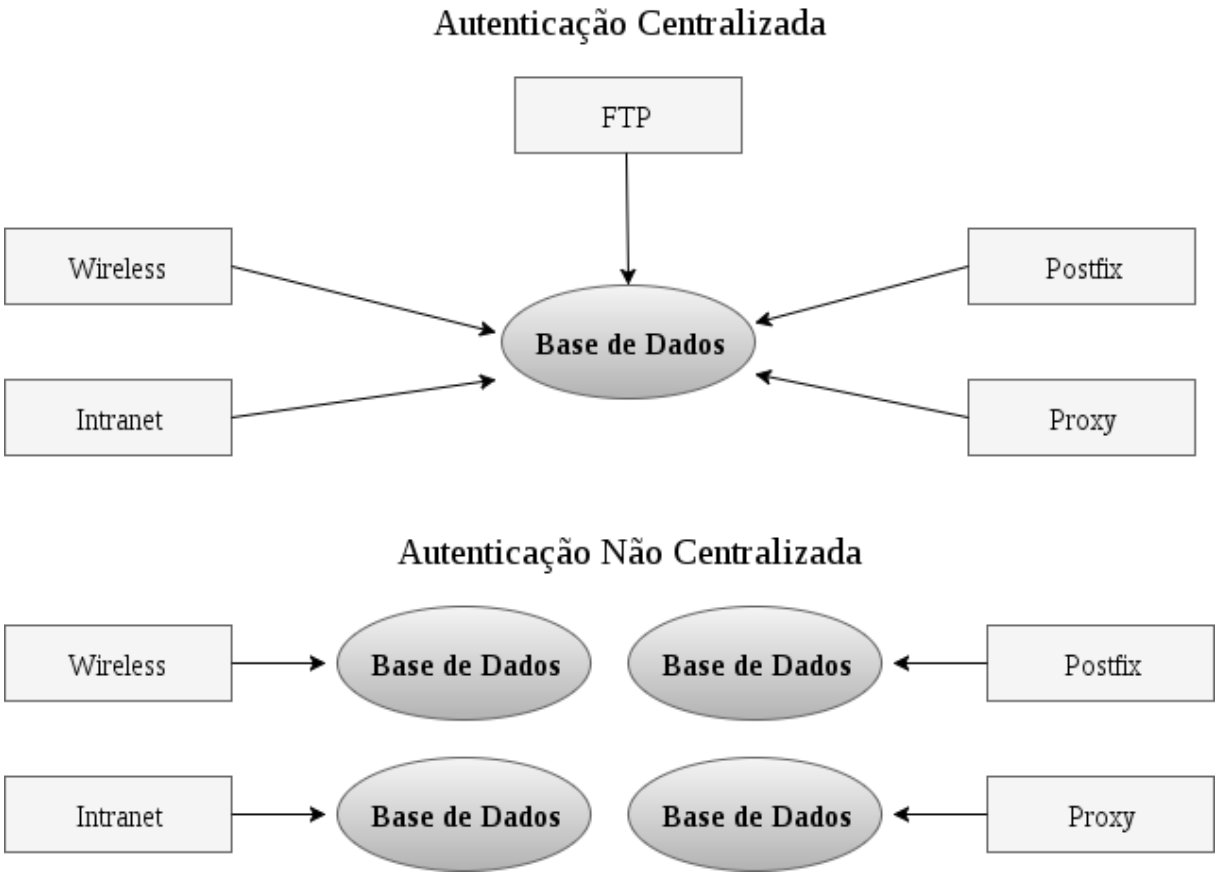
2.2 Vantagens da Autenticação Centralizada

Com a autenticação centralizada, os usuários podem acessar vários sistemas diferentes por meio de uma única credencial, ou seja, o usuário gerencia apenas uma credencial, facilitando a memorização. Por meio da Autenticação Centralizada é possível realizar a Autorização Centralizada, por exemplo, o Usuário “X”, do grupo Funcionários, é permitido a utilizar somente serviços definidos pelo seu grupo.

Facilita o Backup das credenciais de acesso, em razão dos dados estarem centralizados e proporciona seguir e gerir uma política de segurança, como o tamanho das senhas, complexidade das senhas e o formato de *login* dos usuários com maior facilidade.

A figura 1 ilustra as diferenças da autenticação centralizada e da autenticação não centralizada.

Figura 1 – Autenticação Centralizada e Não Centralizada.



Fonte: Figura elaborada pelo próprio autor.

3 Serviço de Diretório

De acordo com Trigo:

> "[...]diretório significa, literalmente, algo usado para indicar direções, ou seja, algo que indica um caminho para se chegar aquilo que se procura; no caso de uma lista telefônica, você se utiliza do nome da pessoa ou da empresa para achar seu número de telefone – ou endereço. (TRIGO ,2007, p.17)"

Isto é, podemos definir um diretório como uma estrutura de armazenamento e compartilhamento de dados. O serviço de diretório é uma aplicação que armazena e organiza as informações do ambiente hierarquicamente, possibilitando o administrador gerenciá-las de forma centralizada.

O serviço é utilizado para armazenar informações de usuários, periféricos, serviços e redes, como senhas e usernames, computadores, impressoras, entre outros; Diretórios são otimizados para leitura, possuí sofisticados métodos de busca, alto desempenho em altos volumes de busca, otimiza o tempo de resposta com réplicas e permite a distribuição das informações. O exemplo de um serviço de diretório é o protocolo LDAP, exemplificado no próximo capitulo.

3.1 *Lightweight Directory Access Protocol*

O *Lightweight Directory Access Protocol* é protocolo leve de acesso a diretórios baseado no modelo cliente/servidor ilustrado na figura 2. Criado em 1993 por pesquisadores da Universidade de Michigan o protocolo atua sobre o modelo *TCP/IP* e opera nas portas 389 (Padrão) e 636 (Suporte a criptografia).

O *LDAP* se encontra em sua terceira versão, com a adição dos seguintes recursos: Autenticação com criptografia, autenticação com o *SASL*, resolução de *Schemas* e extensões (novas funcionalidades).

Figura 2: Modelo Cliente/Servidor LDAP.

Fonte: Figura elaborada pelo próprio Autor.

3.2 Operações no *Lightweight Directory Access Protocol*

As operações básicas do protocolo *LDAP* são:

•*Bind*: Especifica a versão *LDAP* e autentica;

•*Search*: Procura por entradas no diretório;

•*Compare*: Testa o valor do atributo;

•*Add*: Adiciona uma nova entrada;

•*Delete*: Apaga uma entrada;

•*Modify*: Modifica uma entrada;

•*Unbind*: Fecha a sessão (*Logout*);

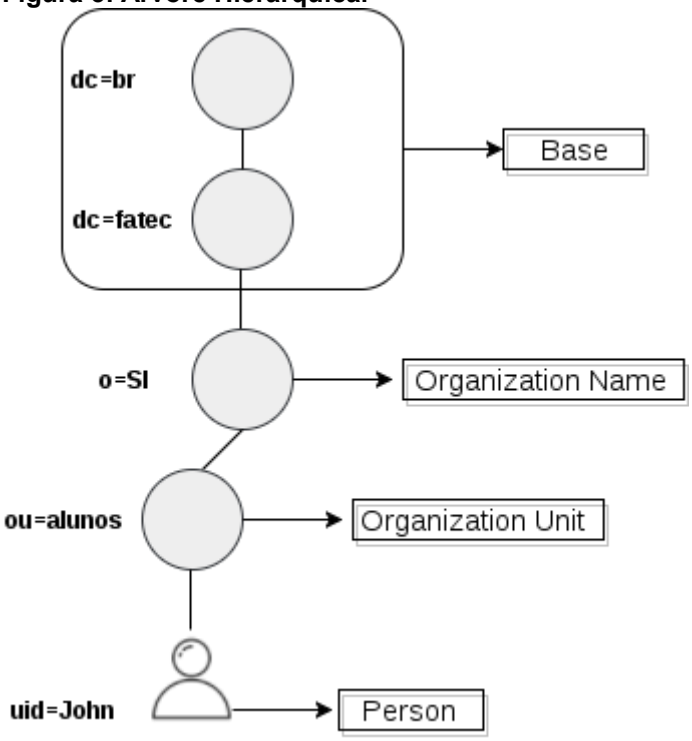
3.3 *Directory Information Tree*

No *LDAP*, as entradas de registros são organizadas em uma estrutura de árvore hierárquica denominado *Directory Information Tree (DIT)*, formada por nós ou entradas que se caracterizam pelo atributo "*objectClass*", definindo as regras que determinada entrada deverá respeitar.

A entrada ou nó no DIT é identificada através do *Distinguised Name* (*DN*), que é utilizado para identificar de forma única uma entrada na árvore; fazendo analogia com o Banco de Dados Relacional, então seria o campo “CHAVE”.

Por exemplo, na figura 3, a entrada do usuário John possuí um *DN* de *uid*=John, *o*=SI,*ou*=alunos,dc=fatec,dc=br.

Figura 3: Arvore Hierárquica.



Fonte: Figura elaborada pelo próprio Autor.

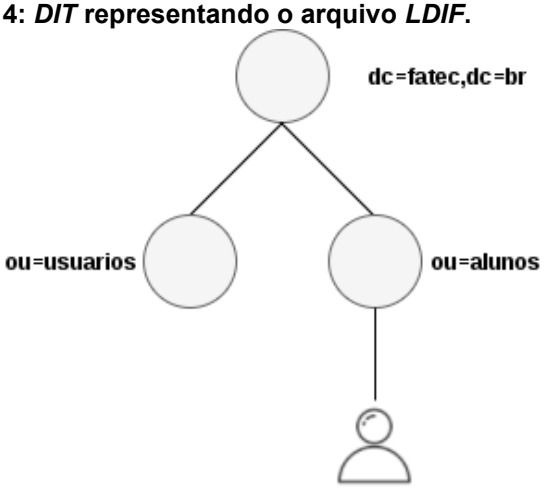
3.4. *LDAP Data Interchange Format*

O *LDAP Data Interchange Format (LDIF)* é um formato de troca de dados em texto puro, que contém diretivas que representam o conteúdo de uma base *LDAP*. O arquivo *.ldif* é utilizado para importar novos dados e atualizar os existentes no diretório *LDAP*, outra utilidade é o uso para backup.

O ANEXO A representa o arquivo *LDIF* aplicado na monografia.

A seguir, a figura 6 introduz o modelo de diretório (*DIT*) a partir do modelo *LDIF* do ANEXO A:

Figura 4: *DIT* representando o arquivo *LDIF*.



Fonte: Figura elaborada pelo autor.

3.5 Entradas e Atributos

No serviço de diretório LDAP as entradas, identificadas *pelo Distinguished Name* (DN) Carter (2003), são um conjunto de informações que caracterizam um objeto, seja ele, pessoas, organizações, servidores, periféricos, entre outros. De acordo com GIL o atributo (2012, p.27), pode-se definir o atributo como sendo a parte do serviço do diretório onde a informação está sendo armazenada de fato, ou seja, que possuí valor ou dado.

As entradas são compostas por um conjunto de atributos que contêm informações sobre o objeto, cada atributo é definido por uma sintaxe, que indica as informações e valores que podem ser armazenadas.

3.6 Classes de Objetos

De acordo com Sungaila:

> "[..]cada entrada pertence a uma ou mais classes de objetos que identificam quais dados podem ser armazenados naquela entrada. A classe de objetos especifica atributos obrigatórios e atributos opcionais que podem ser associados a cada entrada daquela classe. (SUNGAILA, 2008, p.59)"

Ressalta-se que as classes de objetos ou *obejectClass* se organizam hierarquicamente, em razão disso, o *objectClass* top deve estar obrigatoriamente no topo da estrutura do diretório, pelo fato da classe ser a pai das outras.

3.7 *OpenLDAP*

O projeto *OpenLDAP* é uma suíte de softwares *Open-source* que oferece serviços de diretório *LDAP*. De acordo com Luis Henrique Carrara e Marcos Augusto Bellezi o software pode ser executado em vários sistemas operacionais, dentre eles *BSD*, Solaris, Windows e distribuições Linux. O projeto é amplamente utilizado em ambientes comerciais, sendo utilizado como alternativa às implementações pagas existentes (*Microsoft Active Directory*, *Sun Java System Directory Server*). O suporte é gerenciado por uma comunidade mundial de voluntários que usam a Internet para se comunicar, planejar e desenvolver a ferramenta. As principais atrações do *OpenLDAP* são:

• A versão atual 2.4.45 acessada em Junho de 2017 implementa o LDAPv3.

• Suporte aos protocolos *IPV4* e *IPV6*.

• Várias opções de segurança, como *TLS, SSL e SASL*.

• Replicação da Base

• Solução *Open-source* com amplo suporte pela Internet.

De acordo com Ribeiro Junior (2008) a suíte de softwares do *OpenLDAP* é composta pelos seguintes módulos:

•*Slapd – stand-alone LDAP daemon*, responsável por oferecer um servidor de serviço de diretório *LDAP*.

•*Slurpd – stand-alone LDAP update replication daemon*, responsável por oferecer a replicação de dados do servidor *LDAP*.

•*Syncrepl – LDAP sync replication*, de modo genérico, o *daemon syncrepl* é responsável também pela replicação da base, porém, de acordo com Ribeiro Junior

(2008), “A replicação de base é mais flexível e tem mais recursos que o *slurpd,* mas só funciona nas versões mais novas do *OpenLDAP*.

•Ferramentas administrativas, são responsáveis na administração das bases *LDAP*.

•Bibliotecas do protocolo *LDAP*.

A configuração do *OpenLDAP* é conduzida basicamente pelos arquivos, *cn=config* e *ldap.conf*. O *cn=config* é a configuração do *daemon slapd*, explanado anteriormente, enquanto, o arquivo *ldap.conf* é utilizado para configuração dos clientes que vão ter acesso a base LDAP.

O projeto está disponível para download em http://www.openldap.org/.

3.8 *Software* de Código Aberto

Os softwares de código aberto ou *Open-Source* são softwares desenvolvidos pela comunidade de usuários, para a comunidade de usuários, ou seja, qualquer um pode utilizar, compartilhar, incrementar e modificar o mesmo. Como o próprio nome sugere, os softwares de código aberto apresentam o código fonte aberto para a comunidade, de modo que os mesmos contribuem para o aperfeiçoamento e suporte do software, em vista disso, diversos diálogos, fóruns, tutoriais são disponibilizados na Internet pela e para a própria comunidade de usuários.

De acordo com a *Open Source Iniciative*, os softwares de código aberto devem obedecer aos seguintes critérios:

• Distribuição livre da licença do software;

• Distribuição livre do código fonte, inclusive do código fonte compilado;

• Permissão para modificação do software;

• Integridade do autor do código fonte;

• Não discriminação contra pessoas, grupos e área de atuação;

• A licença não deve restringir e ser específica a um software

• A licença deve ser tecnologia neutra.

3.9 Comandos de gerenciamento *LDAP*

O *LDAP* dispõe de vários comandos para gerenciamento e administração do serviço, especificamente neste capitulo aborda-se os comandos *LDAP* para manipulação de dados. Reforçando a ideia, Pinheiro (2012) diz que, [...] a forma padrão de administração é feita via linha de comando com os comandos providos pelo pacote "*ldap-utils*".

Os comandos *LDAP* podem ser executados remotamente e não precisam da permissão Root para executa-los.

• *ldapadd*: O comando possibilita que seja feito adições de entradas no servidor *LDAP*.

Exemplo: Inserir um arquivo *LDIF* qualquer na base *LDAP*.

• *ldapsearch*: O comando possibilita localizar uma entrada no diretório *LDAP*.

Exemplo: Buscar o usuário "Jack" na base *LDAP* pelo atributo *uid*.

• *ldapmodify*: O comando possibilita que seja feito modificações nas entradas do diretório *LDAP*.

• *ldapcompare*: O comando possibilita que seja feito comparações entre dois atributos em uma entrada no diretório *LDAP*. Se o valor dos atributos coincidir, o comando retornará *TRUE*, se não, retornará *FALSE*.

• *ldapdelete*: O comando possibilita deletar objetos da base.

Exemplo: Buscar o usuário "Jack" na base *LDAP* pelo atributo *uid*.

3.9.1 Parâmetros dos comandos *LDAP*

A tabela 1 ilustra as opções dos comandos *LDAP* e suas especificações.

Tabela 1: Opções dos comandos *LDAP*.

Comandos:	**Funções**:
-h	*Host* onde está a Base *LDAP*
-p	Porta na qual irá se conectar, a padrão do *LDAP* é a 389
-x	Autenticação Simples
-w	Pede a senha do *admin* na linha de comando
-W	Pede a senha do *admin* em um prompt
-ZZ	Força a conexão segura com o TLS, se não fecha a conexão
-Z	Tenta a conexão segura com o TLS, se não tenta com outros meios de autenticação
-D	*DN* do usuário que será utilizado para autenticar

Fonte: Tabela elaborada pelo Autor.

3.10 Comandos de administração *SLAP*

Os comandos *SLAP* são utilizados para adicionar entradas na base *LDAP* a partir de arquivos *.ldif* e são indicados para manutenção de grandes bases, pois estes comandos são rápidos.

Em oposição aos comandos *LDAP* devem ser executados com a base *LDAP* paralisada.

Obs.: É recomendado criar um backup da base antes de executar qualquer ação com os comandos *SLAP*.

• *slapadd*: O comando é operado para adicionar objetos na base de dados *LDAP*, por meio de arquivos. ldif.

• *slapcat*: Permite visualizar a base de dados *LDAP* e quando usada com parâmetros possibilita exportar uma base de dados *LDAP* para um arquivo *.ldif*.

• *slappasswd*: O comando gera *hash's* de senhas em diferentes formatos, como, {*MD5*}, {*SMD5*}, {*CRYPT*}, {*SHA*} e {*SSHA*}.

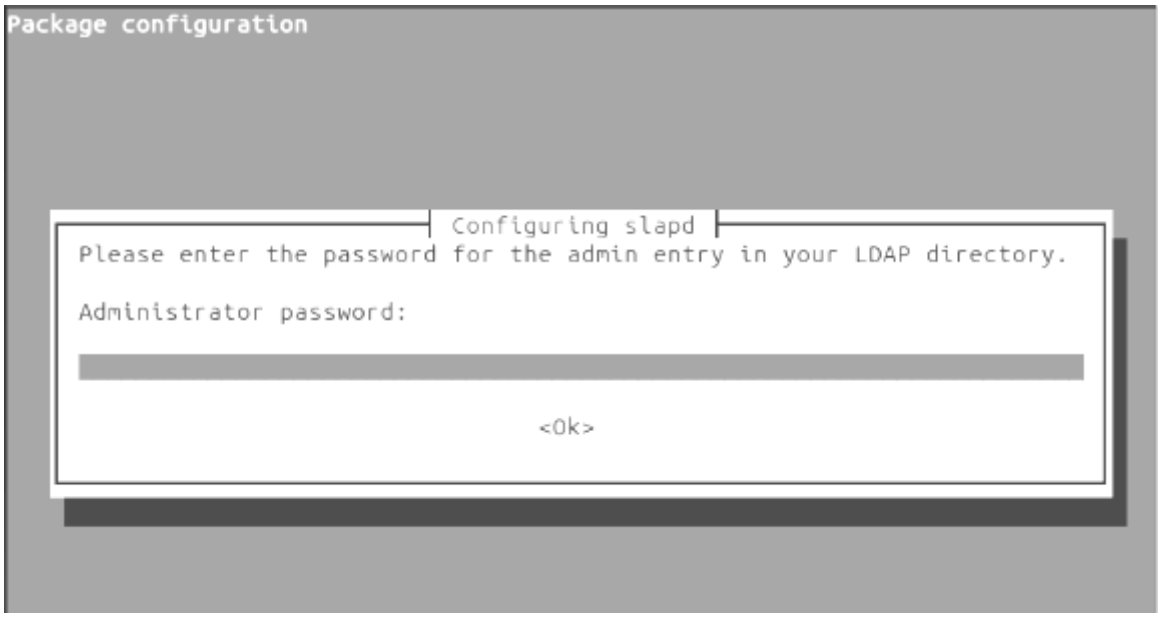
• *slaptest*: É utilizado para verificar se existem erros no arquivo de configuração *cn=config*.

Os parâmetros para os comandos *SLAP*, podem ser consultados no manual do *OpenLDAP*, no seguinte endereço: https://www.openldap.org/software/man.cgi.

4 Instalação e Configuração do Servidor *OpenLDAP*

A instalação do servidor de serviço de diretório *OpenLDAP* se dá a partir de pacotes pré-compilados de acordo com a distribuição Linux utilizada, no Ubuntu Server 16.04.3 LTS o pacote é intitulado *slapd*. A única requisição na instalação do servidor *OpenLDAP* ilustrado na figura 4 é a escolha de uma senha para o administrador da base de dados.

Figura 5: *Admin Password*.



Fonte*: Print Screen* de tela.

O OpenLDAP utiliza como configuração uma base de dados *LDAP* chamada de "*cn=config*", que reúne todas as informações do diretório, por exemplo: Toda a estrutura (*dc=fatec,dc=br*) do diretório, o usuário e senha do administrador da base de dados (*cn=admin,dc=fatec,dc=br*), o local de armazenamento dos dados *(/var/lib/ldap*), as *ACL´S* padrões do *OpenLDAP*, os módulos e os *schemas*, que é onde estão armazenado os atributos.

5 Instalação e Configuração dos Clientes *OpenLDAP*

Para instalação do cliente *OpenLDAP*, utiliza-se os mesmos pacotes pré-compilados do servidor, porém de acordo com a distribuição Linux utilizada.

No arquivo *ldap.conf* encontra-se as opções de configuração "*client*" para acesso no servidor *OpenLDAP*, a figura 5 abaixo ilustra o arquivo de configuração *ldap.conf*.

Figura 6: *ldap.conf*.

```
# LDAP Defaults
#

# See ldap.conf(5) for details
# This file should be world readable but not world writable.

BASE    dc=fatec,dc=br
URI     ldap://192.168.122.152

#SIZELIMIT      12
#TIMELIMIT      15
#DEREF          never

# TLS certificates (needed for GnuTLS)
TLS_CACERT      /etc/ldap/tls/cacert.pem
TLS_REQCERT     allow

~
~
```

Fonte: *Print Screen* de tela.

5.1 Parâmetro *BASE*

Especifica o *Distinguished Name* (DN) da base *LDAP*, quer dizer, o caminho na base a ser usadas nas operações *LDAP*.

5.2 Parâmetro *URI*

É o endereço do servidor *LDAP* que deve ser conectado.

5.3 Parâmetro *TIMELIMIT*

Tempo máximo de uma única busca.

5.4 Parâmetro *SIZELIMIT*

É o número de entradas pesquisadas em uma única busca.

5.5 Parâmetro *DEREF*

Não permite consultas em outros servidores.

5.6 Parâmetro *TLS_CACERT*

Especifica o local do arquivo que contém o a agência certificadora que o cliente reconhecerá.

5.7 Parâmetro *TLS_REQCERT*

Especifica o local do arquivo que contém o certificado do cliente.

6 Backup no *OpenLDAP*

A cópia de segurança é uma poderosíssima ferramenta na continuidade do negócio em caso de falhas, perda ou roubo de dados. É tão importante como manter o servidor online, bem configurado, é zelar uma política adequada de backup.

O Backup ou cópia de segurança segundo Faria (2014, p 1), “consiste na cópia de dados específicos (redundância) para serem restaurados no caso da perda dos originais. ”

Para realizar o backup no *OpenLDAP* é necessário criar um usuário com permissão de leitura em toda a base, incluindo as senhas dos usuários, a figura 6 consiste na *ACL* para dar permissões necessárias ao usuário backup.

Figura 7: *ACL* usuário Backup.

```
#Remove as ACLs padrao:
dn: olcDatabase={1}hdb,cn=config
changetype: modify
delete: olcAccess

# 1. ACL
dn: olcDatabase={1}hdb,cn=config
changetype: modify
add: olcAccess
olcAccess: {0}to attrs=userPassword,shadowLastChange
        by self write
        by anonymous auth
        by dn="cn=admin,dc=fatec,dc=br" write
        by dn="cn=backup,dc=fatec,dc=br" read
        by * none

# 2. ACL
dn: olcDatabase={1}hdb,cn=config
changetype: modify
add: olcAccess
olcAccess: {1}to dn.base=""
        by * read

# 3. ACL
dn: olcDatabase={1}hdb,cn=config
changetype: modify
add: olcAccess
olcAccess: {2}to *
        by self write
        by dn="cn=admin,dc=fatec,dc=br" write
        by dn="cn=backup,dc=fatec,dc=br" read
        by * read
```

Fonte: Print Screen de tela.

6.1 *Access Control List* 1:

Define os atributos que serão controlados, no cenário os atributos *userPassword* e *shadowLastChange*, indicam respectivamente a senha do usuário e a última vez que a senha do usuário foi modificada.

Define o usuário que tem acesso (usuário backup, permissão de leitura) a determinado atributo e em seguida qual tipo de acesso.

Ativa a permissão de autenticação, ou seja, o acesso aos atributos somente será mediante autenticação e define que todos os usuários não possuam acesso ao conteúdo dos atributos.

6.2 *Access Control List* 2:

Indica que qualquer usuário, até mesmo os anônimos podem acessar a raiz da base *LDAP*.

6.3 *Access Control List* 3:

Permite acesso a todos os usuários, define que o usuário *admin* pode escrever na base LDAP e o usuário backup e os demais usuários podem ler o conteúdo da base.

7 Conexão segura com o *OpenLDAP*

O *OpenLDAP* contempla a segurança com o protocolo *Transport Layer Security* (TLS) e *Secure Socket Layer* (SSL) para fornecer a identidade do servidor *OpenLDAP* e a criptografia no tráfego de dados. O protocolo TLS utiliza a porta padrão do serviço (389) e somente a comunicação entre os hosts são encriptadas, enquanto o SSL opera em uma porta diferente do padrão (636), pelo fato do protocolo gerar um canal de comunicação totalmente encriptado, desde o processo de estabelecimento de conexão até o trafego de dados em si. O protocolo de segurança TLS e SSL são fornecidos pelo pacote *OpenSSL*.

É de suma importância implantar o protocolo de segurança no *OpenLDAP*, pois em um ambiente operacional, o Servidor *OpenLDAP* fornece atributos contendo informações privadas dos usuários, como, *login*, rg, cpf, e-mail, data de nascimento, entre outros para o funcionamento de aplicações, autenticações e até mesmo pesquisas.

8 As informações do Servidor *LDAP* que devemos compreender para atender a integração com os serviços

Para integração de algum serviço com o *OpenLDAP* é importante estar atento nas informações abaixo:

- IP ou *Hostname* do Servidor;
- Porta: *ldap* (389) ou *ldaps*(636)
- Sufixo da Base (*dc=fatec,dc=br*);
- Versão do protocolo *LDAP*;
- DN do usuário;
- Senha;

É fundamental as informações acima para a configuração dos serviços.

9 *File Transfer Protocol*: Autenticação *LDAP*

O *File Transfer Protocol* ou FTP é um protocolo de transferência de dados, ou seja, um protocolo que permite que os usuários possam enviar ou receber arquivos, seja na Internet ou nas redes internas. De acordo com Sungaila (2008, p.97), “o *File Transfer Protocol* ainda é largamente utilizado”.

Atualmente encontram-se vários servidores FTP baseados em Linux. Para a integralização com o *OpenLDAP*, a solução que apresenta maior facilidade na configuração, amplo suporte na Internet, além de segurança por oferecer suporte a criptografia, é o software *Proftpd*.

O *Proftpd* oferece diversos módulos para a autenticação de usuários, neste caso, utiliza-se o módulo *mod_ldap* para autenticação na base *LDAP*, por padrão o módulo *mod_ldap* não vem compilado no pacote *proftpd*.

9.1 Configuração do *ProFTPD*

Considerando o ambiente da monografia, o pacote *Proftpd* já está instalado na máquina ftp.fatec.br, desta maneira, parte-se da instalação do módulo *LDAP*.

No Ubuntu Server 16.04 LTS o pacote do módulo *LDAP* é nomeado como, *proftpd-mod-ldap*.

O arquivo contendo todas diretivas de configuração do *Proftpd* é o */etc/proftpd/proftpd.conf*, nele encontra-se a opção para habilitar o arquivo de configuração para autenticar usuários da base *LDAP* no *proftpd*, deste modo, desmarque a diretiva:

```
Include /etc/proftpd/ldap.conf
```

Edite o arquivo */etc/proftpd/modules.conf* contendo todos os módulos para autenticação dos usuários e desmarque para ativar o módulo de autenticação na base *LDAP* (*mod_ldap*):

```
LoadModule mod_ldap.c
```

No arquivo */etc/proftpd/ldap.conf* inclua os parâmetros da base *LDAP* para a autenticação no serviço:

```
LDAPServer “10.0.2.15”

LDAPBindDN “cn=admin,dc=fatec,dc=br” “abcde”

LDAPUsers ou=Users,dc=fatec,dc=br (&(uid=u%)(title=ftp)) (uidNumber=u%)

LDAPUseTLS on
```

O parâmetro *LDAPServer* indica o Servidor *LDAP* para autenticação.

O parâmetro *LDAPBindDN* é necessário quando o acesso “anônimo” a base não é permitida, neste caso usa-se o usuário “admin”.

O parâmetro *LDAPUsers* indica o diretório que armazena os usuários para autenticação no serviço, neste caso, somente os usuários do diretório *Users* com o atributo *title=ftp* devem autenticar.

E o parâmetro *LDAPUseTLS* ativa o suporte a criptografia do protocolo *TLS*.

Exemplo Autenticação no *FTP*:

```
Connected to ldap.fatec.br

220 ProFTPD 1.3.5a Server (Debian) [::ffff:10.0.2.15]

Name (ldap.fatec.br:root): jack

331 Password required for jack

Password:

230 User jack logged in

Remote system type is UNIX.

Using binary mode to transfer files.

ftp>
```

Saída do *log* representada abaixo:

```
Set 17 14:32:26 ldap slapd[1125]: conn=1048 fd=21 ACCEPT from IP=127.0.0.1:60300 (IP=0.0.0.0:389)

Set 17 14:32:26 ldap slapd[1125]: conn=1048 op=0 EXT oid=1.3.6.1.4.1.1466.20037
```

Set 17 14:32:26 ldap slapd[1125]: conn=1048 op=0 STARTTLS

Set 17 14:32:26 ldap slapd[1125]: conn=1048 op=0 RESULT oid= err=0 text=

Set 17 14:32:26 dap slapd[1125]: conn=1047 op=3 SEARCH RESULT tag=101 err=0 nentries=1

text=

Set 17 14:32:26 ldap slapd[1125]: conn=1048 fd=21 TLS established tls_ssf=128 ssf=128

Set 17 14:32:26 ldap slapd[1125]: conn=1048 op=1 BIND dn="cn=Jack,ou=Users,dc=fatec,dc=br" method=128

10 Apache: Autenticação *LDAP*

Apache HTTP é um Servidor Web mais utilizado no mundo, de acordo com Silva o Apache:

> "[...]é responsável por disponibilizar páginas, fotos, ou qualquer outro tipo de objeto ao navegador do cliente. (SILVA, 2010)"

Além do mais segundo Silva (2010), "O Apache é um servidor Web extremamente configurável, robusto e de alta performance desenvolvido por uma equipe de voluntários"

O software é disponível para diversos sistemas operacionais, como, Linux e Unix, MAC OS, Windows e outros. No momento do desenvolvimento deste trabalho de conclusão de curso, a última versão estável do Apache é a 2.4.77

O Objetivo do projeto é fornecer para o usuário uma janela de *login* contendo usuário e senha já definidos na base de dados armazenada no servidor *OpenLDAP* para acesso a uma determinada *Intranet*. Para isso, usa-se o módulo "*libapache2-authnz-ldap*" para autenticação Apache no diretório *LDAP*.

10.1 Configuração Apache

Supondo que o Apache já foi instalado no ambiente, será apenas necessário a ativação do módulo *libapache2-authnz-ldap*. O *Ubuntu* fornece um *script* designado *a2enmod* para ativação de diversos módulos específicos no Apache2, por ventura a ativação do *módulo libapache2-authnz-ldap* desfruta desta facilidade:

```
# a2enmod authnz_ldap

Considering dependency ldap for authnz_ldap:

Enabling module ldap.

Enabling module authnz_ldap.

To activate the new configuration, you need to run:

service apache2 restart

# service apache2 restart
```

```
service apache2 restart

* Restarting web server apache2
```

Para o desenvolvimento da *Intranet*, o exemplo abaixo deve ser copiado para o diretório */etc/apache2/sites-avaible/*.

```
<VirtualHost *:80>
    #Informaçoes do Servidor WEB
    ServerAdmin admin@fatec.br
    ServerName intranet.fatec.br
    DocumentRoot /var/www/intranet

<Directory /var/www/intranet>
    #Conteudo da Intranet
    Options Indexes FollowSymLinks MultiViews
    AllowOverride None
    AuthType Basic
    AuthName "Autenticação LDAP"
    AuthBasicProvider ldap
    #Endereço do Servidor OpenLDAP e diretorio que está armazenado os usuarios
    AuthLDAPURL "ldap://192.168.122.52:389/ou=Users,dc=fatec,dc=br?uid"
   #Qualquer usuario que deter Nome e Senha consegue autenticar
    require valid-user
    Order allow,deny
    allow from all
</Directory>

ErrorLog /var/log/apache2/ldap-error.log
# Possible values include: debug, info, notice, warn, error, crit,
```

```
# alert, emerg.

LogLevel warn

CustomLog /var/log/apache2/ldap-access.log combined
ServerSignature Off
</VirtualHost>
```

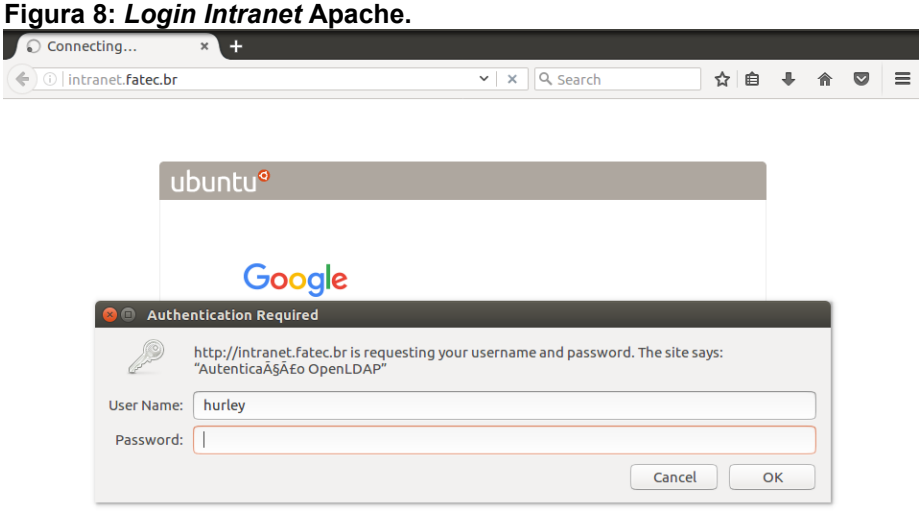
Crie o diretório da *Intranet* e um arquivo *index.html* contendo a mensagem de boas-vindas ao usuário:

```
# mkdir /var/www/intranet/
# echo "Intranet: Autenticação LDAP" > /var/www/intranet/index.html
```

Finalize, habilitando o site da *Intranet* com o módulo *a2ensite*.

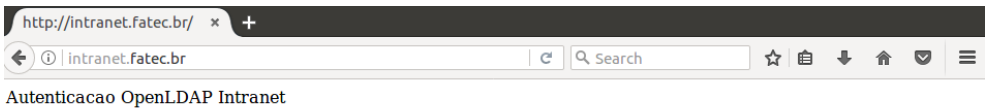
As figuras 7 e 8 relata a autenticação *LDAP* do usuário Hurley na *Intranet*:

Figura 8: *Login Intranet* Apache.



Fonte: *Print Screen* de tela.

Figura 9: Autenticação do usuário Hurley com sucesso na *Intranet* Apache.



Fonte: *Print Screen* de tela.

11 Estações Linux: Autenticação *LDAP*

Uma das possíveis integralizações do *OpenLDAP* é próprio Linux. Por regra, o Linux usa sua base de dados local para autenticação, neste projeto o propósito é empregar a base dados *LDAP* compreendendo os usuários da *ou=Users* para autenticação nas estações Linux *Ubuntu 16*.04 LTS, simulando um laboratório e expondo a excelente opção do *LDAP* para a administração deste ambiente.

Vale ressaltar que o foco é apenas apresentar e simular a autenticação via *LDAP* nas estações Linux, em que o dado dos usuários tem dê ser armazenados localmente. Porém em um ambiente real de laboratório, outros métodos e serviços, como *o Network File System*, podem ser incrementados para implementação e aprimoramento deste ambiente.

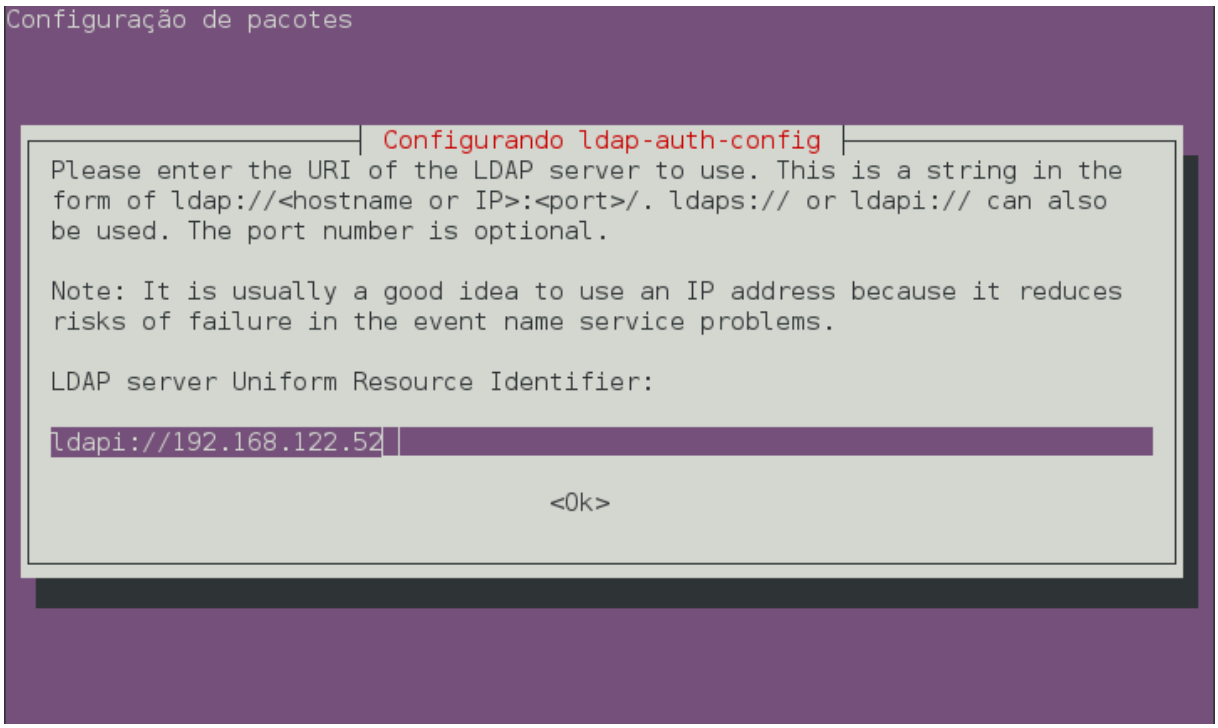
O Ubuntu apresenta um meta-pacote denominado *ldap-auth-client* que incorpora todos os pacotes e ferramentas necessárias para autenticação no *OpenLDAP Server*. Hartley (2015) intitula, os metas pacotes como “uma maneira conveniente de instalar aplicações, bibliotecas e documentação em massa”.

Outro pacote fundamental para a autenticação nas estações Linux é o *daemon nscd*, que provê cache de acesso do *passwd*, hosts e *group* nas estações Linux que consequentemente reduz a necessidade de acesso ao *OpenLDAP*, evitando o congestionamento do tráfego de dados por meio de menos requisições entre as estações Linux e o *OpenLDAP Server*.

11.1 Configuração Estações Linux

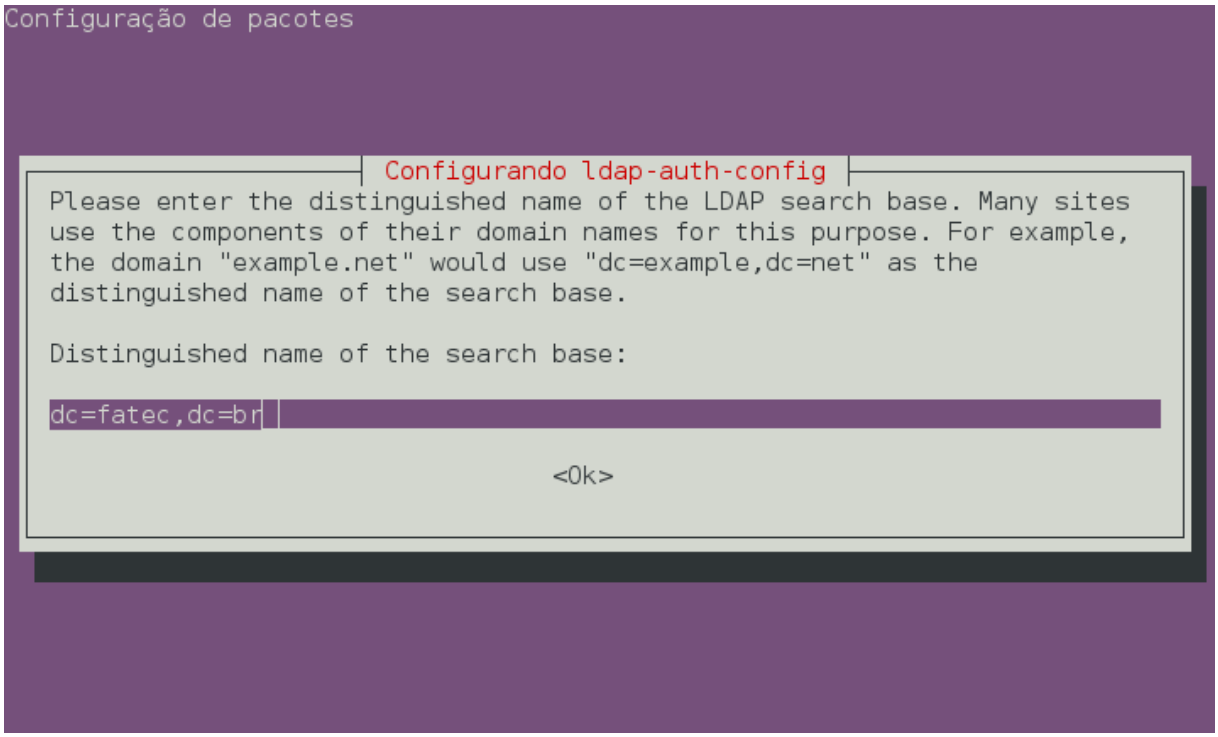
Instalação do meta-pacotes *ldap-auth-client* já citado acima através das figuras 10, 11, 12,13.

Figura 10: *IP* do Servidor *LDAP*.



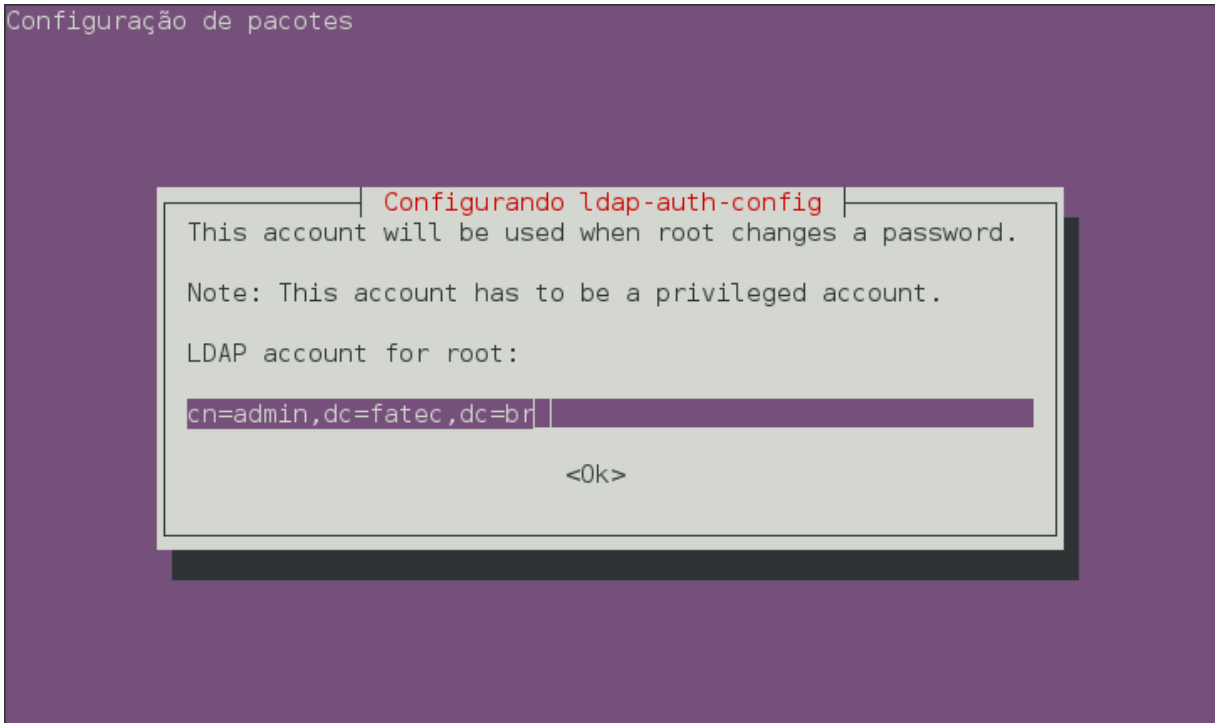
Fonte: *Print Screen* de tela.

Figura 11: Base de dados responsável pela Autenticação dos usuários.



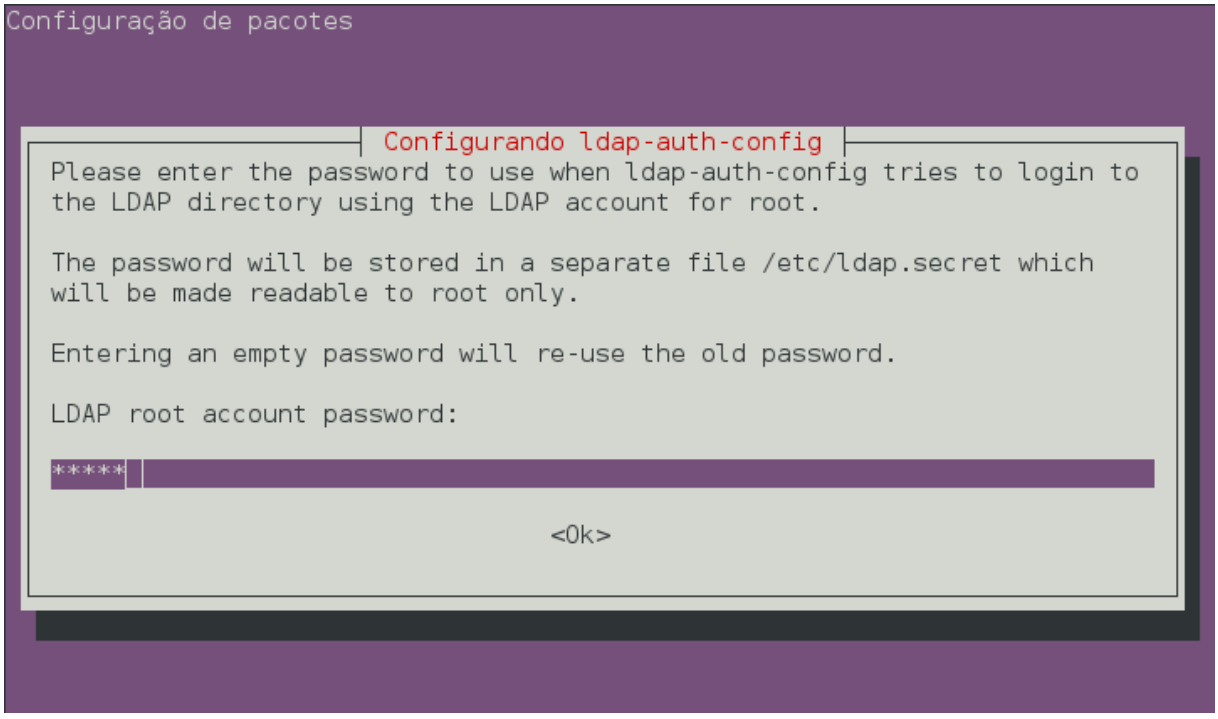
Fonte: *Print Screen* de tela.

Figura 12: Administrador do *LDAP*.



Fonte: *Print Screen* de tela.

Figura 13: Senha do Administrador do *LDAP*.



Fonte: *Print Screen* de tela.

É determinante para concluir a autenticação *LDAP* em estações Linux, a configuração do arquivo */etc/nsswitch.conf* que define segundo Thomaz (2008), "[...]a ordem das buscas realizadas quando uma certa informação é requisitada", ou seja, o arquivo *passwd* que contém todos os usuários que podem acessar o sistema, o arquivo *group* que define os grupos que cada usuário pertence e o arquivo *shadow* que contém as senhas dos usuários, são priorizadas as buscas na base *LDAP*, ilustrado na figura 13.

Figura 14: Arquivo */etc/nsswitch.conf*.

```
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc-reference' and `info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.

# pre_auth-client-config # passwd:         compat
passwd: files ldap
# pre_auth-client-config # group:          compat
group: files ldap
# pre_auth-client-config # shadow:         compat
shadow: files ldap
gshadow:        files

hosts:          files dns
networks:       files

protocols:      db files
services:       db files
ethers:         db files
rpc:            db files

# pre_auth-client-config # netgroup:       nis
netgroup: nis
~
```

Fonte: *Print Screen* de tela.

As figuras 14, 15, 16 e 17 relata a autenticação do usuário Hurley e Kate providos da base LDAP na máquina client.fatec.br.

Figura 15: Autenticação Hurley.

```
administrador@client:~$ su hurley
Senha:
```

Fonte: *Print Screen* de tela.

Figura 16: Autenticação concluída com sucesso Usuário Hurley.

Fonte: *Print Screen* de tela.

Figura 17: Autenticação Kate.

Fonte: *Print Screen* de tela.

Figura 18: Autenticação concluída com sucesso Usuário Kate.

Fonte: *Print Screen* de tela.

12 Considerações Finais

Anteriormente ao ambiente com os serviços integrados com a autenticação centralizada via *OpenLDAP*, as autenticações nos serviços eram de forma descentralizadas, isto é, cada serviço possuía seus meios para autenticação, ocasionando segundo Sócrates Filho (2009), a perda da padronização de acesso às informações, e a possibilidade de superposição de direitos, que causam furos de segurança.

Desta maneira o *OpenLDAP* se mostra uma alternativa *Open-Source* de simples implementação e eficaz a estes métodos por englobar de forma centralizada diversas informações, tal como, a identidade dos usuários, a título de exemplo o gerenciamento de usuários, como criar usuários, excluir usuários, fornece permissões, alterar informações do usuário são tarefas usuais dos Administradores de Sistema, pressupondo um ambiente com diversos serviços, o gerenciamento de usuário de apenas um usuário acarretaria na remodelação e manutenção de todos os serviços.

Outro fator que estimula a implementação da Autenticação Centralizada é uso de apenas uma credencial de acesso a todos os serviços de tecnologia da informação ofertados pela instituição, agilizando conforme citado acima o gerenciamento de usuários, a administração dos controles de acesso e a administração do sistema em si, direcionando o tempo poupado para a execução de novas tarefas.

Vale salientar que o *OpenLDAP* é um software *Open-Source*, ou seja, a ferramenta apresenta custo zero para licenciamento e manutenção do mesmo, em tempos de crise, na qual a redução de custos é uma busca constante de qualquer instituição, o corte de gastos com licenças de software é necessário, portanto o *OpenLDAP* se retrata como alternativa livre a tais software, além de contribuir com o estudo e análise do conteúdo disponibilizado pela comunidade de software livre.

Para trabalhos futuros comparados a esta monografia, é recomendado uma pesquisa mais aprofundada relacionando replicação*, ACL's* e ferramentas administrativas gráficas, de forma que alcance um nível para efetivamente planejar a implementação do serviço em um ambiente real de produção.

REFERÊNCIAS BIBLIOGRÁFICAS

ALBUQUERQUE, Erick. **Tipos de autenticação no FTP**. Disponível em: <https://iisbrasil.wordpress.com/2011/04/07/tipos-de-autenticacao-no-ftp/>. Acesso em: 24 out. 2017.

FARIA, Heitor Medrado de. **Bacula:** Ferramenta livre de backup. 2. ed. Rio de Janeiro: Brasport, 2014.

GIL, Anahuac de Paula.**OpenLDAP**:Extreme. Rio de Janeiro: Brasport, 2012. 249 p.

HARTLEY, Matt**. What Are Linux Meta-packages?** 2015. Disponível em: <https://www.linux.com/blog/what-are-linux-meta-packages>. Acesso em: 28 set. 2017.

INITIATIVE, Open Source. *The Open Source Definition*. Disponível em: <https://opensource.org/osd>. Acesso em: 19 out. 2017.

MACHADO, Erich Soares; MORI JUNIOR, Flavio da Silva. **Autenticação Integrada Baseada em Serviço de Diretório LDAP.** 2006. 78 f. TCC (Graduação) - Curso de Bacharelado em Ciência da Computação, Ime-Usp, Universidade de São Paulo, São Paulo, 2006.

PINHEIRO, Ricardo. **Comandos de gerenciamento do LDAP.** 2012. Disponível em: <http://www.cooperati.com.br/2012/02/14/comandos-de-gerenciamento-do-ldap/>. Acesso em: 31 out. 2016.

RIBEIRO JUNIOR, Jaime. **OpenLDAP:** a chave é a centralização. 2008. Disponível em: <https://www.vivaolinux.com.br/artigo/OpenLDAP-a-chave-e-a-centralizacao?pagina=1>. Acesso em: 1 nov. 2016.

SILVA, Alexandro. **Implantando autenticação centralizada e segura usando Openldap**. 2010. Disponível em: <http://www.dicas-l.com.br/arquivo/implantando_autenticacao_centralizada_e_segura_usando_openldap.php#.WeTzL3Xyvdc>. Acesso em: 16 out. 2017

SILVA, Gleydson Mazioli da. **Guia Foca GNU/Linux Avançado**. 2010. Disponível em: <http://www.guiafoca.org/?page_id=242>. Acesso em: 03 out. 2017.

SÓCRATES FILHO, **Segurança da Informação:** Autenticação. 2009. Disponível em: <http://waltercunha.com/blog/index.php/2009/08/19/seguranca-da-informacao-autenticacao/>. Acesso em: 14 nov. 2017.

SUNGAILA, Marcos. **Autenticação Centralizada com OpenLDAP.** São Paulo: Novatec, 2008. 230 p.

THOMAZ, Ygor. NIS (nsswitch.conf). 2008. Disponível em: <https://www.vivaolinux.com.br/etc/nsswitch.conf-controlc>. Acesso em: 25 out. 2017.

TRIGO, Clodonil Honório. **OpenLDAP: uma abordagem integrada.** São Paulo: Novatec, 2007. 239 p.

ANEXO A – Representação do arquivo *LDIF*

dc=fatec,dc=br

objectClass: top

objectClass: dcObject

objectClass: organization

o: fatec.br

dc: fatec

structuralObjectClass: organization

dn: cn=admin,dc=fatec,dc=br

objectClass: simpleSecurityObject

objectClass: organizationalRole

cn: admin

description: LDAP administrator

userPassword: {SSHA}CEO86UmJFw3iaVa6W1vZAPavzOBdOI30

structuralObjectClass: organizationalRole

dn: ou=Users,dc=fatec,dc=br

ou: Usuarios

objectClass: organizationalUnit

objectClass: top

dn: ou=Alunos,dc=fatec,dc=br

ou: Alunos

objectClass: organizationalUnit

objectClass: top

dn: cn=John,ou=Users,dc=fatec,dc=br

uid: john

cn: John

sn: John

givenName: John

objectclass: inetOrgPerson

objectclass: posixAccount

objectclass: shadowAccount

homeDirectory: /home/john

loginShell: /bin/bash

uidNumber: 5001

gidNumber: 5001

userPassword: {SSHA}4A/oHilFJnhqti2Gdfh8EL5jip8ATaWM

dn: cn=Jack,ou=Users,dc=fatec,dc=br

uid: jack

cn: Jack

sn: Jack

title: ftp

givenName: Jack

objectclass: inetOrgPerson

objectclass: posixAccount

objectclass: shadowAccount

homeDirectory: /home/jack

loginShell: /bin/bash

uidNumber: 5002

gidNumber: 5002

userPassword: {SSHA}vVdEvtZzx30Qk1CNAUqdVgMmHHshfv4/

dn: cn=Kate,ou=Users,dc=fatec,dc=br

uid: kate

cn: Kate

sn: Kate

givenName: Kate

objectclass: inetOrgPerson

objectclass: posixAccount

objectclass: shadowAccount

homeDirectory: /home/kate

loginShell: /bin/bash

uidNumber: 5003

gidNumber: 5003

userPassword: {SSHA}GC+WbbjnurwLZGoNZ4uYYgs57Vycp5KG

dn: cn=Hurley,ou=Users,dc=fatec,dc=br

uid: hurley

cn: Hurley

sn: Hurley

givenName: Hurley

objectclass: inetOrgPerson

objectclass: posixAccount

objectclass: shadowAccount

homeDirectory: /home/hurley

loginShell: /bin/bash

uidNumber: 5004

gidNumber: 5004

userPassword: {SSHA}s/8uY/hoegvz5ujeAT1iCD+m422lXhW