FACULDADE DE TECNOLOGIA DO NORDESTE
GRADUAÇÃO TECNOLÓGICA EM REDES DE COMPUTADORES
ADMINISTRAÇÃO DE SISTEMAS OPERACIONAIS RC30 2015.2

OUTROS TRABALHOS EM:

www.projetoderedes.com.br

OPENLDAP: AUTENTICAÇÃO CENTRALIZADA

FORTALEZA
2015

MARIA THAYNA DO NASCIMENTO DE BRITO
MIKAEL RITLAY NOGUEIRA DE ALMEIDA
DIEGO MOISES DA SILVA
LEONARDO HEITOR RIBEIRO PITANGA
CARLOS EDUARDO LOUPO DA SILVA

OPENLDAP: AUTENTICAÇÃO CENTRALIZADA

Trabalho de OpenLDAP apresentado na disciplina de Adminsitração de Sistemas Operacionais, turma RC30 no semestre 2015.2 da Faculdade de Tecnologia do Nordeste (FATENE), como requisito de obtençao da nota da segunda avaliação (N2).

Orientador: Prof^{o} Esp. Gilberto Gonzaga Figueredo

FORTALEZA
2015

TRABALHO ACADÊMICO
FACULDADE DE TECNOLOGIA DO NORDESTE
GRADUAÇÃO TECNOLÓGICA EM REDES DE COMPUTADORES

Às_____horas do dia_____ do mês de_____ do ano de_____, na sala_____, compareceram para defesa pública do trabalho de conclusão de curso de graduação, requisito parcial para a obtenção do título de Bacharel em <grau desejado> o aluno (a): <Nome do aluno> tendo como título da Trabalho Acadêmico, OpenLDAP: Autenticação Centralizada.

Constituíram a banca examinadora os professores:

Professor (a) _____ (orientador (a)),

Professor (a) _____ (examinador (a)), e

Professor (a) _____ (examinador (a)).

Após a apresentação e as observações dos membros da banca avaliadora, ficou definido que o trabalho foi considerado _____ com nota_____.

Eu, _____ Coordenador(a) do Graduação Tecnológica em Redes de Computadores, lavrei a presente ata que segue assinada por mim e pelos demais membros da Banca Examinadora.

Observações:

_____

_____

_____

_____

_____

Fortaleza, ____ de _____de 2015.

_____ _____

Profª. Me. Danielle Christina Costa Amorim
Coordenador

Profº Esp. Gilberto Gonzaga Figueredo
Orientador

A imaginação é mais importante que o conhecimento.

Albert Einstein

RESUMO

Este documento tem por objetivo sintetizar e discorrer sobre o protocolo LDAP, demonstrar suas origens, seus pontos fracos e fortes, bem como, destacar a importância do mesmo para a administração de uma rede, tanto para uma administração centralizada, evitando redundância e retrabalhos, quanto no âmbito da segurança das informações, baseando-se em métodos criptográficos atuais como o SSL e TLS que são capazes de assegurar um alto nível de segurança em uma consulta LDAP. Será discriminado também as principais soluções disponíveis hoje no mercado, as quais, implementam o protocolo. A principal abordagem desse documento se dará em soluções livres que possuem todas as principais funcionalidades disponíveis em soluções proprietárias, porém sem a necessidade de despender recursos na compra de licenças. Será apresentado um estudo de caso em um ambiente com sistemas operacionais mistos (Windows® e Linux) onde será feita a autenticação com as mesmas credenciais.

Palavras-chave: OpenLDAP, LDAP, Autenticação, Sistemas Operacionais

LISTA DE FIGURAS

LISTA DE DESENHOS

LISTA DE GRÁFICOS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
ACL	do inglês, *Access control list*, Lista de controle de acesso
AD	do inglês, Active Directory
AIX	do inglês, Advanced Interactive eXecutive
APT	do inglês, Advanced Packaging Tool
BDB	do inglês, Berkeley´s Data Base
BSD	do inglês, Berkeley Software Distribution
CCITT	do inglês, Consultative Committee for International Telegraphy and Telephony
DAP	do inglês, Directory Access Protocol
DNS	do inglês, Domain Name System
FTP	do inglês, File Transfer Protocol
GPO	do inglês, Group Policy Objects
HP-UX	do inglês, Hewlett Packard UniX
HTTP	do inglês, HyperText Transfer Protocol
IEC	do Inglês, *International Electromechanical Commission*, Comissão Internacional de Eletrotécnica
IETF	do inglês, Internet Engineering Task Force
IMAP	do inglês, Internet Message Access Protocol
IP	do inglês, Internet Protocol
ISO	do Inglês, *International Standardization Organization*, Organização Internacional para Padronização

LDAP	do inglês, Lightweight Directory Access Protocol
LDIF	do inglês, LDAP Interchange Format
MTA	do inglês, Mail Transfer Agent
NBR	Prefixo utilizado para Normas Brasileiras, emitidas pela ABNT
NT	do inglês, New Technology
OSI	do inglês, Open Systems Interconnection
POP	do inglês, Post Office Protocol
RFC	do inglês, Request for Comments
SMTP	do inglês, Simple Mail Transfer Protocol
SNMP	do inglês, Simple Network Management Protocol
SQL	do inglês, Structured Query Language
SSH	do inglês, Secure Shell
SSL	Secure Socket Layer
SSO	Single Sign On
TCP	Transmission Control Protocol
TSL	Transport Layer Security
RAID	do inglês, *Redundant Array of Independent Disks*

LISTA DE SÍMBOLOS

$\Re$	Conjunto dos números reais
π	Número PI
μ	submúltiplo do SI, equivale a $x10^{-6}$
©	do Inglês, Copyright, denota que o nome ou marca em questão possui direitos de cópia reservados
®	Símbolo de marca registrada usado para identificar uma empresa, produto ou serviço

SUMÁRIO

1 INTRODUÇÃO

Este documento tem por objetivo orientar e discorrer sobre um protocolo que, apesar de ser muito utilizado, sendo um padrão em empresas de médio a grande porte, são poucos os que realmente conhecem suas funcionalidades mais avançadas. Isso ocorre visto que soluções proprietárias tendem a abstrair esse nível de configuração, engessando um protocolo extremamente flexível, limitando-os a apenas frações de suas funcionalidades.

No decorrer desse material o leitor será encaminhado por uma introdução sobre os conceitos que são necessários para o entendimento do protocolo, passando pelas implementações dessa ferramenta, hoje disponíveis no mercado; um exemplo de estudo de caso, onde a partir de uma necessidade inicial de um cliente é desenvolvido um estudo de quais ferramentas mais se adequariam aos requisitos, sempre focando a centralização das informações em uma única base LDAP.

No capítulo 1, intitulado “O PROTOCOLO LDAP”, temos a parte introdutória do trabalho, onde são apontadas as origens, influências do protocolo LDAP, as diferenças do mesmo e seu antecessor o X.500, além da conceituação de diretórios, estrutura do LDAP, métodos de organização da árvore e conceituação de *schemas* e arquivos LDIF.

No capítulo 2, intitulado “IMPLEMENTAÇÕES DO PROTOCOLO LDAP”, são abordadas as principais soluções baseadas no protocolo, identificando suas principais características e dando uma maior ênfase a solução *OpenSource* de nome OpenLDAP , sendo demonstrado os seus métodos de replicação, criptografia, modelos de banco de dados compatíveis e método de trabalho com as ACLs.

No capítulo 3, intitulado “ESTUDO DE CASO”, é apresentado um estudo de caso fictício de uma empresa de nome Secure Info Ltda, onde a mesma define uma série de requisitos para a implementação de um sistema que atenderá sua estrutura tanto interna quanto externa. Estes requisitos são trabalhados durante todo o capítulo. Com os requisitos em mãos, será assim iniciada a definição dos softwares mais adequados para o atendimento aos mesmos, após essas definições serão demonstradas as instalações dos principais softwares que se relacionam diretamente com o servidor LDAP, visto que esse é o foco principal do trabalho.

Finalmente, conclui-se que este documento é elaborado, principalmente, para pessoas envolvidas diretamente em manutenção e gerenciamento de redes e para estudantes da área de tecnologia.

2 O PROTOCOLO LDAP

2.1 ORIGEM DO LDAP

No início da década de 80, ao se unirem a ISO e o CCITT com o objetivo de criar um serviço de mensagens, surgiu a necessidade de desenvolver um protocolo que tivesse a capacidade de organizar entradas em um serviço de nomes de forma hierárquica, capaz de suportar grandes quantidades de dados e com uma enorme capacidade de procura de informações. Esse serviço criado pelas duas instituições, foi apresentado em 1988, sendo denominado X.500, juntamente com um conjunto de recomendações e normas ISO 9594. O X.500 especificava que a comunicação entre o cliente e o servidor do diretório deveria usar o *Directory Access Protocol* (DAP) que era executado sobre a pilha de protocolos do modelo OSI.

Devido à alta complexidade e o custo elevado, pesquisadores da Universidade de Michigan criaram um servidor LDAP, o *slapd*, que atuava sobre os protocolos TCP/IP. Este servidor foi apresentado como uma alternativa ao protocolo DAP em 1993, como citado por (GOUVEIA,2009), disponibilizando as fontes na Internet e criando listas de discussão para divulgar e aperfeiçoar esse novo protocolo. Assim a evolução do mesmo foi acompanhada por pessoas do mundo inteiro, e o mesmo deixou de ser uma mera alternativa para o protocolo DAP, tornando-se um serviço de diretório completo, agora competindo diretamente com o X.500.

O LDAP é um protocolo especializado em organizar os recursos de rede de forma hierárquica, através de uma árvore de diretórios, que roda sobre os protocolos TCP/IP, diferente do protocolo no qual foi baseado, o DAP, o qual roda sobre o modelo OSI. Para (BARTH,2009) essa foi uma das principais causas da adoção em larga escala do protocolo, visto que com essa nova plataforma foi possível reduzir consideravelmente o *overhead*[1] de camadas superiores do modelo OSI.

Segundo (GOUVEIA,2009) o LDAP ganhou força após o ano de 1997, quando foi lançada sua terceira versão, além de uma fundação a qual mantém uma solução *OpenSource* a *OpenLDAP Foudation*, várias outras empresas como *Novell*, *Microsoft* e *Netscape* começaram a oferecer produtos baseados nessa nova plataforma.

---

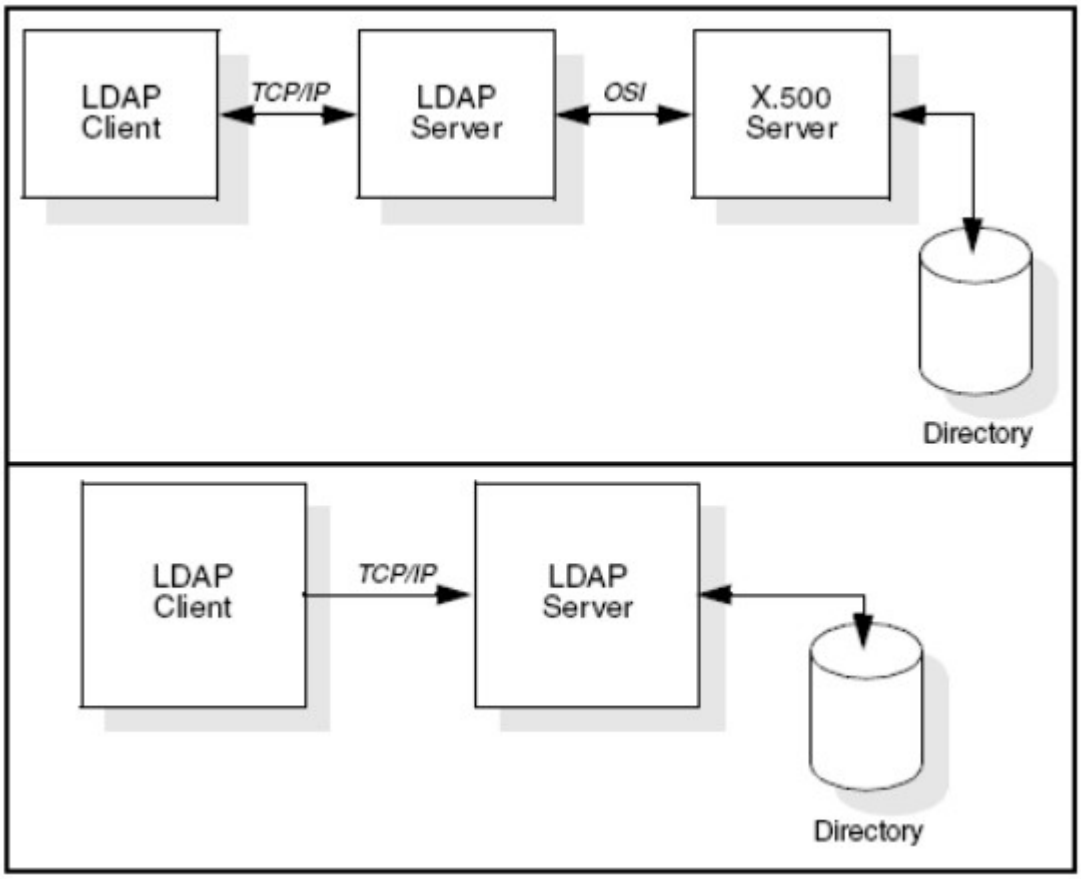
[1] *Overhead* é geralmente considerado qualquer processamento ou armazenamento em excesso, seja de tempo de computação, de memória, de largura de banda ou qualquer outro recurso que seja requerido para ser utilizado ou gasto para executar uma determinada tarefa.

2.2 PROTOCOLO X.500 VS LDAP

Segundo (TRIGO,2007), o LDAP possui as seguintes simplificações em relação ao X.500:

- É executado diretamente sobre o TCP/IP;
- A maioria dos elementos de dados são representados como cadeias de caracteres, processadas de modo mais fácil que os dados na representação estruturada *Abstract Syntax Notation One* (ASN.1) usada pelo X.500;
- Codifica dados para transporte em redes usando uma versão simplificada das mesmas regras de codificação usadas pelo X.500;
- Elimina características pouco usadas e também operações redundantes do X.500.

Figura 1: Aplicação LDAP



Fonte: (OpenLDAPFoundation,2009)

2.3 NOÇÕES TEÓRICAS SOBRE LDAP

2.3.1 Definições de diretórios

(TRIGO,2007) descreve que diretório é literalmente definido como “algo usado para indicar direções”, ou seja, para indicar um caminho para se chegar àquilo que se procura.

Segundo a definição de (TUTTLE,2009):

> “Diretório é uma lista de informações sobre objetos organizados ou catalogados em uma ordem, e que fornece o acesso aos dados dos objetos. São os diretórios que permitem que usuários ou aplicações encontrem recursos no ambiente com as características necessárias para um tipo de tarefa particular.”

Diretórios nos cercam a todo tempo, seja em uma lista telefônica, na estrutura de pastas do computador, em blogs, em serviços de buscas, além de vários outros lugares. Outro exemplo de diretório é o DNS o qual possui uma relação de nomes de *host*[2] e seu respectivo IP.

Segundo (TRIGO,2007) é muito comum ocorrer confusão com o uso de diretórios, pois apesar de ser possível fazer com eles praticamente qualquer coisa, desde salvar informações como um banco de dados, salvar arquivos como um sistema de arquivos e disponibilizar arquivos como um sistema FTP, não se justifica o mesmo, pois para cada uma dessas funções existe um sistema que foi desenvolvido para fazer somente essa tarefa, assim sem dúvida, o fará muito melhor do que o diretório.

2.3.2 Características do LDAP

Segundo (TRIGO,2007), o LDAP foi padronizado em junho de 1993, no RFC 1487 da IETF.

O LDAP, segundo (BARTH,2009) foi projetado para resolver problemas de distribuição de diretórios pela rede, contando com nove aspectos que lhe garantiram essa habilidade, sendo eles:

- Seu desenho genérico
- Simplicidade do protocolo
- Arquitetura distribuída

[2] No contexto abordado host é qualquer máquina ou computador conectado a uma rede

- Segurança
- Padrão aberto
- Solicitação de funcionalidades e esquemas do servidor
- Internacionalização
- Suporte ao IPv6
- Berkeley´s Data Base

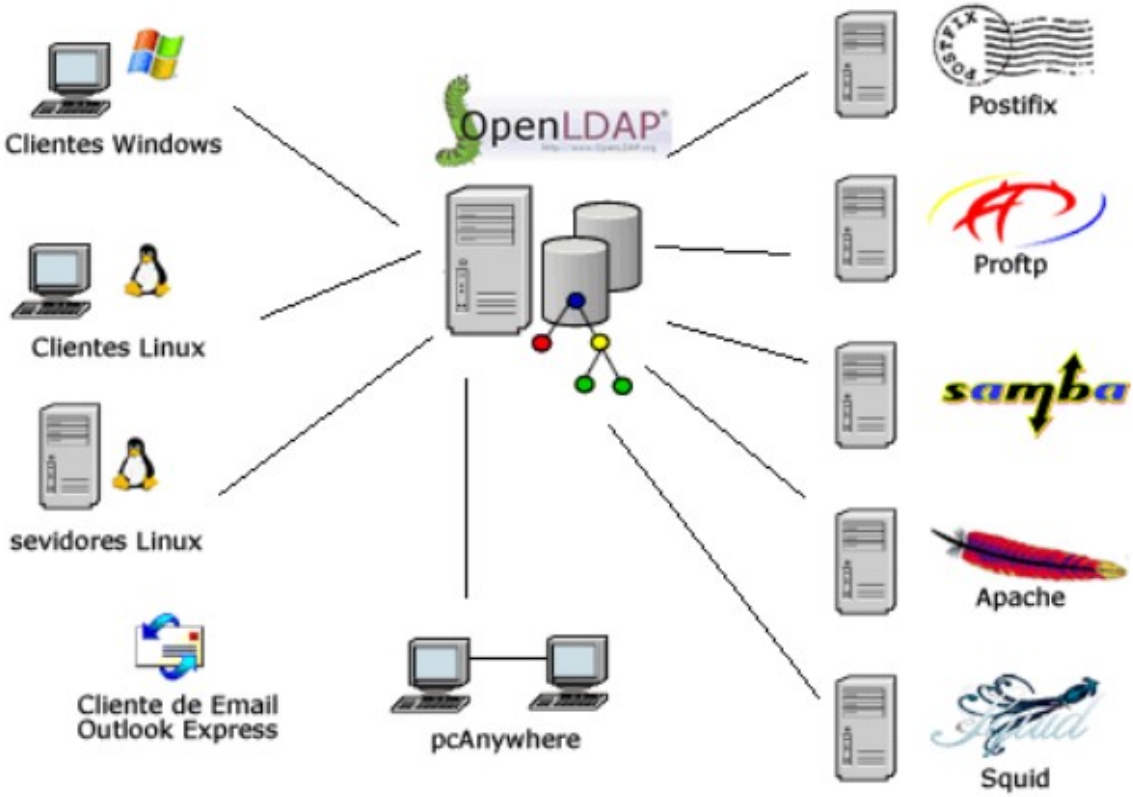
Ainda segundo (BARTH,2009) uma aplicação que o LDAP disponibiliza é o conceito de *Single Sign On* (SSO), ou seja, autenticação unificada, possibilitando e facilitando a integração com diversos outros serviços, assim o usuário tem apenas um *userid* ou identificação única na rede e com esse pode acessar diversos recursos da mesma.

(TUTTLE,2009) afirma que o LDAP é um 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.

A principal característica do LDAP é a integração com outros serviços, complementando assim a infra-estrutura de redes, fornecendo novos recursos e, especialmente, maior integração, diferentemente de outros protocolos e linguagens estabelecidos como exemplo: SNMP, HTTP, SMTP, IMAP ou SQL.

Abaixo a Figura 2 representa essa característica.

Figura 2: Característica do LDAP



Fonte: OpenLDAP Foudation

2.3.3 Estrutura do LDAP

(TRIGO,2007) afirma que o grande fator responsável pela flexibilidade do LDAP é a sua organização de forma hierárquica. A árvore de informações possui um elemento-raiz, por onde começa a busca das informações. A partir daí, o sistema vai percorrendo os nós filhos até que consiga encontrar o elemento desejado. A raiz e os ramos da árvore são os diretórios os quais podem conter outros diretórios. Abaixo desses diretórios estão os elementos ou também chamados de entradas. Para cada entrada podemos ter um ou mais valores associados a ela. A Tabela 1 abaixo mostra os principais atributos e suas descrições.

Tabela 1: Exemplos de atributos, com suas respectivas descrições

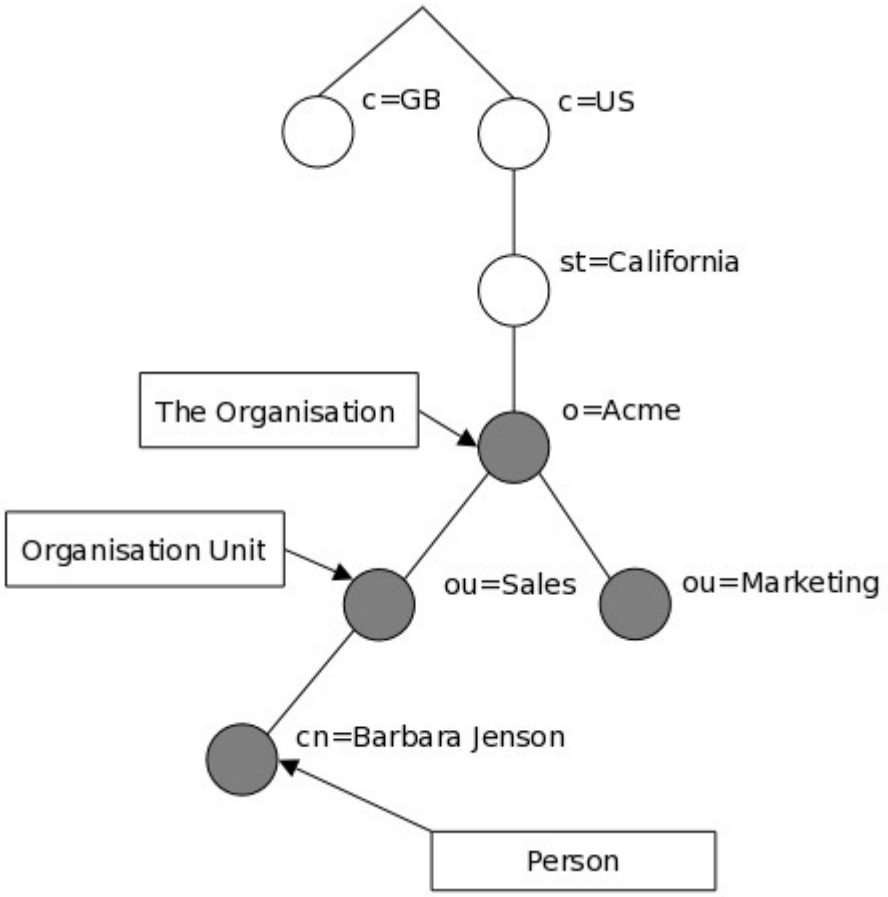
Atributo	Descrição
dc	Identificação única do Objeto (do inglês *Domain Component*)
ou	Unidade Organizacional (do inglês *Organization Unit*)
cn	Nome comum (do inglês *Common Name*)
dn	Nome distinto (do inglês *Distinguished Name*)
c	País (do inglês *Country*)
o	Organização (do inglês *Organization*)

Atributo	Descrição
st	Estado (do inglês *State*)

Fonte: Autoria própria

Segundo (TRIGO,2007), existem duas maneiras de organizar uma árvore de diretórios; no estilo X.500 onde a estrutura da árvore de diretórios é baseado em regiões, como é demonstrado na Figura 3 e no estilo DNS, no qual, os dados são organizados como se fossem domínios. A grande vantagem de se usar o estilo DNS é o fato de poder configurar o serviço de LDAP para uma empresa a partir de um nome de domínio válido, garantindo o caráter único da identidade quando disponibilizado através da Internet.

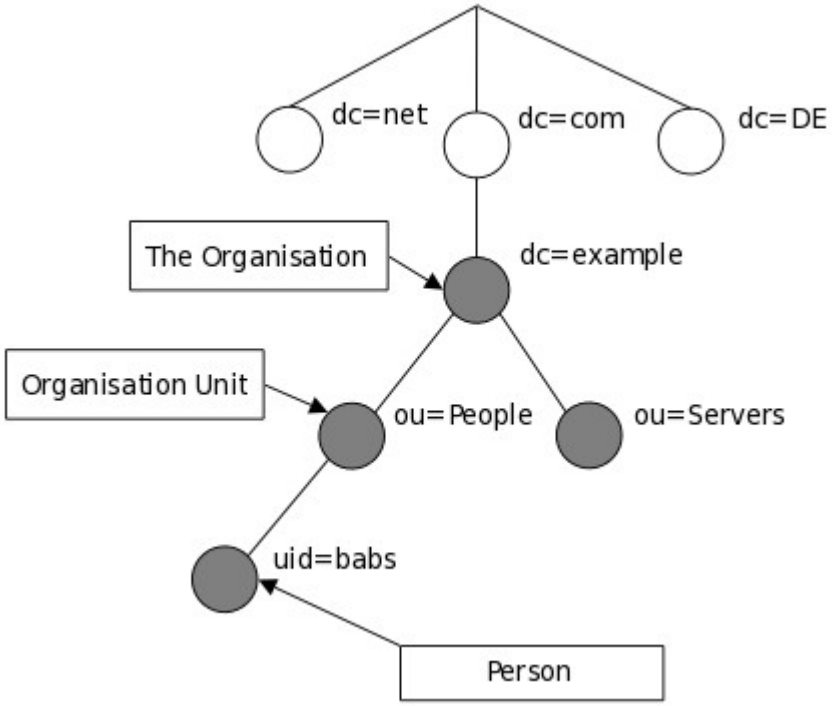
Figura 3: Estrutura geográfica



Fonte: (OpenLDAPFoundation,2009)

Na Figura 4 abaixo podemos visualizar uma estrutura baseada na forma organizacional.

Figura 4: Estrutura organizacional



Fonte: (OpenLDAPFoundation,2009)

2.3.4 Schema

Segundo (GOUVEIA,2009), os *schemas* são responsáveis por manter a integridade dos dados do diretório. São extensíveis, possibilitando a adição de atributos ou classes de acordo com a necessidade.

Schemas definem quais *object class* podem ser inseridos no diretório, quais os atributos de uma determinada *object class* e quais os valores possíveis para esses atributos. Assim, caso um objeto não obedeça às regras do *schema*, não poderá ser inserido no mesmo.

2.3.5 Arquivos LDIF

Segundo (TRIGO,2007), arquivos LDIFs são arquivos de texto puro, usados para importar, modificar e exportar informações. Esse formato de arquivo é o único meio de entrada de dados em um servidor LDAP; mesmo programas que trabalham diretamente com o servidor LDAP, inserindo e removendo registros, como é o caso do PHPMyAdmin, utilizam-se de arquivos LDIF para suas transações. Abaixo é colocado dois arquivos LDIF onde o primeiro é responsável pela inserção de um usuário em uma base, e o seguinte pela modificação do valor do atributo *userPassword*, no caso, a senha do usuário.

Exemplo de um arquivo LDIF: base.ldif

```
dn: dc=fatene,dc=edu,dc=br
objectClass: top
```

```
objectClass: dcObject
objectClass: organization
o: fatene.edu.br
dc: fatene

dn: cn=admin,dc=fatene,dc=edu,dc=br
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword:: e1NTSEF9SGFKQTdDQjhEMHVnYXorSCtKUGoyaDhKZGVRQ0c5OGY=

dn: ou=Usuarios,dc=fatene,dc=edu,dc=br
ou: Usuarios
objectClass: organizationalUnit
objectClass: top

dn: cn=Administrador,ou=Usuarios,dc=fatene,dc=edu,dc=br
uid: administrador
cn: Administrador
sn: Administrador
mail: administrador@fatene.edu.br
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
userPassword: {crypt}
$6$6IaRKR8Y$zZsqvVTHlcIDoLbObi5zgOsuSmBQBgCJPhBN3CgcNGhB8hLJBlva18A6zP6m7YW
Qw1hSgTW2GfgWka.9xU4EW1
shadowLastChange: 16749
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/bash
uidNumber: 1000
gidNumber: 1000
homeDirectory: /home/administrador
gecos: Administrador,,,
```

Fonte: Autoria própria

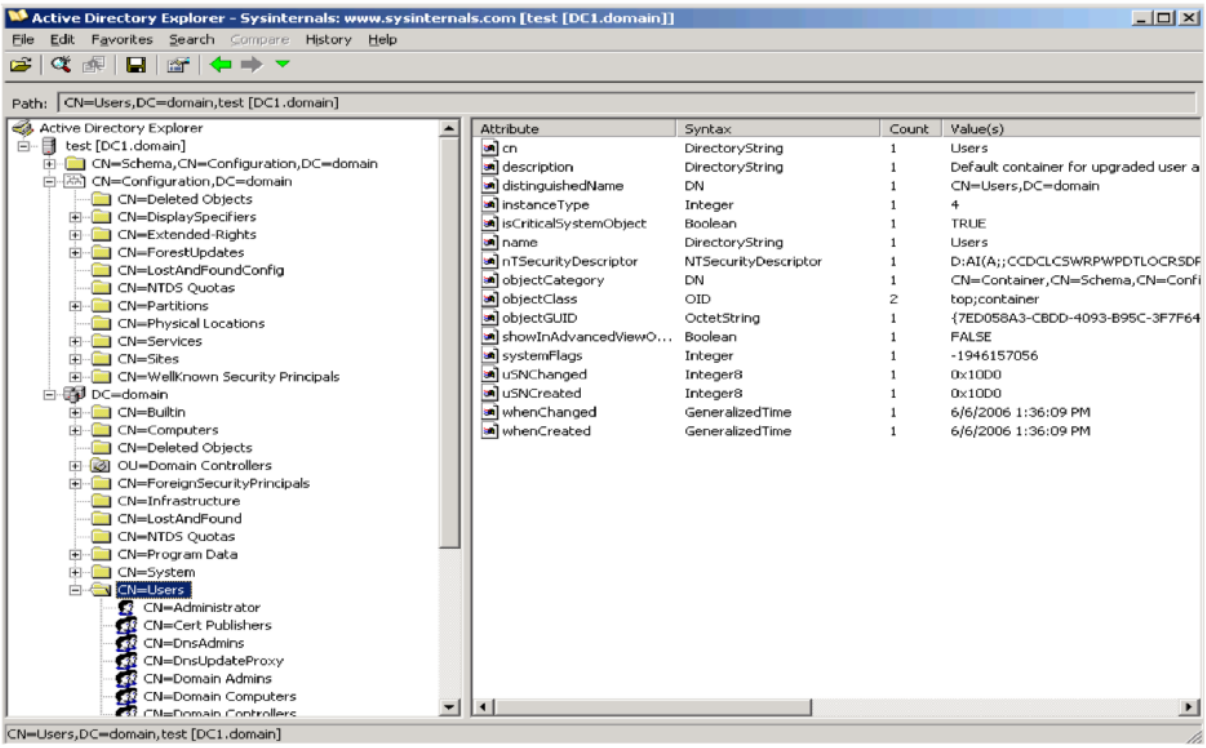
3 IMPLEMENTAÇÕES DO PROTOCOLO LDAP

Como mencionado anteriormente, o protocolo LDAP é apenas um conjunto de conceitos e definições que possibilitam uma padronização na troca de informações entre diversas soluções baseadas no protocolo. Assim os métodos utilizados para armazenar as informações internamente e de replicação, por exemplo, são peculiaridades de cada implementação. Abaixo é apresentado algumas características dessas principais implementações.

3.1 *ACTIVE DIRECTORY*

Objetos como usuários, grupos, membros dos grupos, senhas, contas de computadores, relações de confiança, informações sobre o domínio, unidades organizacionais, etc., ficam armazenados no banco de dados do AD que além de armazenar esses vários objetos em seu banco de dados, disponibiliza vários serviços, como: autenticação de usuários, replicação do seu banco de dados, pesquisa dos objetos disponíveis na rede, administração centralizada da segurança utilizando GPO, entre outros. Esses recursos tornam a administração do AD bem mais fácil, sendo possível administrar todos os recursos disponíveis na rede centralizadamente.

Figura 5: Exemplo de implementação do *Active Directory*

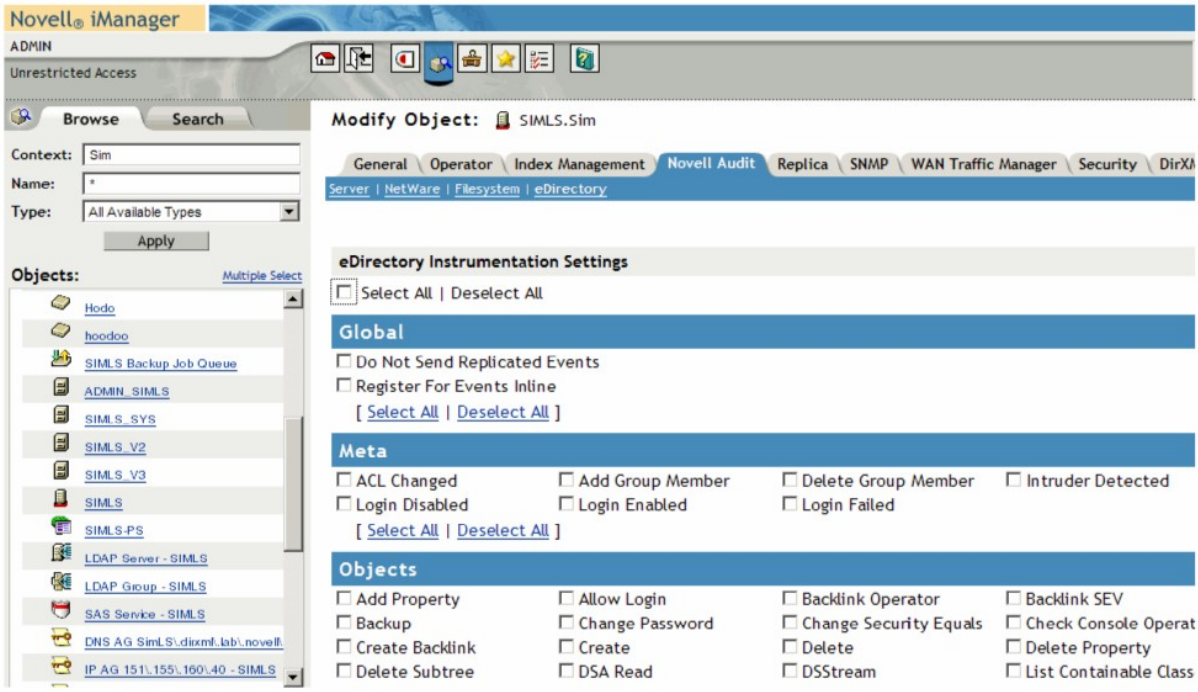


Fonte: *(MENEGUITE,2009)*

3.2 *EDIRECTORY*

Assim como a Microsoft, a Novell também disponibiliza uma implementação do LDAP, o eDirectory, que é a base de identidade que vincula os usuários e seus direitos de acesso aos recursos, dispositivos e políticas de segurança da empresa. Ele oferece a compatibilidade, segurança, confiabilidade, escalabilidade e gerenciabilidade necessárias para distribuições internas e de Internet. O *eDirectory* possui características muito próximas do *Active Directory* da Microsoft.

Figura 6: Exemplo de implementação do eDirectory



Fonte: Novel 2009

3.3 OPENLDAP

O OpenLDAP é uma implementação do LDAP desenvolvida pela Universidade de Michigan e mantido pelo Projeto OpenLDAP , possui como principais características: suporte ao IPv4 e IPv6, autenticação, segurança no transporte usando SSL e TSL, controle de acessos, alta performance em múltiplas chamadas e a replicação de base. O OpenLDAP tem uma licença específica chamada de The OpenLDAP *Public License* (OpenLDAP *Project*, 2009) e é independente de plataforma, assim várias distribuições Linux já disponibilizam o mesmo em seus repositórios. Além do Linux o OpenLDAP é também compatível com AIX, variantes de *BSD*, *HP-UX*, *Mac OS X*, *Solaris e Microsoft Windows* (Baseados na tecnologia NT).

3.3.1 Replicação

A replicação é um método muito utilizado quando trabalhamos em um ambiente corporativo, onde existe a necessidade de alta disponibilidade nos serviços. É na verdade a manutenção de uma cópia, seja parcial ou total, dos dados em outros servidores. No OpenLDAP existem duas técnicas distintas de replicação, as quais são o *slurpd* e o *syncrepl*, sendo que a *slurpd*, é uma técnica mais antiga a qual foi descontinuada na versão 2.4 do OpenLDAP , por possuir uma série de limitações que foram supridas por sua sucessora a *syncrepl*. As principais limitações eram as limitações para replicar uma base parcialmente e a utilização de mais de um servidor Master.

Quando trabalhamos com o *syncrepl* o servidor LDAP pode assumir duas posturas quanto à replicação, Master ou Slave. Quando Master o servidor assume todas as funções de um servidor OpenLDAP , desde a inserção, atualização e consulta dos dados. Porém quando slave o servidor só aceitará execuções de consultas em sua base de dados quando originadas de máquinas clientes, assim para que qualquer informação seja alterada, a solicitação deverá ser feita ao servidor Master o qual se encarregará de replicar as alterações para seus servidores slaves.

3.3.1.1 Master x Slave

Nesse método de replicação temos um único servidor Master o qual tem seu conteúdo replicado em todos os seus servidores escravos. Nesses servidores slaves não ocorre entrada de dados, apenas replicam passivamente os dados de um servidor principal. Esse método de replicação é o mais comum e atende a grande parte das demandas de servidores LDAP.

3.3.1.2 Master x Master

Replicação multimaster é um método de replicação mais recente no OpenLDAP , porém já implementado no *Active Directory* desde sua primeira versão. Esta é uma replicação que atende a demandas muito singulares e apesar de funcionar muito bem ainda é pouco difundida e aplicada. Esta replicação consiste na utilização de dois ou mais servidores Masters, independentes, os quais possuem todas as suas funcionalidades ativadas, porém é criado por parte dos servidores um controle interno para que seja possível manter a integridade dos dados, algo que era muito mais simples de controlar quando existia uma única entrada de dados.

3.3.1.3 Diretórios distribuídos

Utilizando o OpenLDAP com o método de replicação *syncrepl* podemos não somente criar uma cópia da árvore de diretórios em outros servidores, mas também criar políticas de replicação e replicar a cada servidor somente aquilo que se pretende que o mesmo tenha acesso, assim por exemplo, quando temos uma empresa com sede em Minas Gerais e filial em São Paulo, a mesma não precisa replicar toda sua base para a filial, apenas aqueles usuários que a pertençam, evitando assim um tráfego desnecessário na rede além de aumentar a segurança.

3.3.2 Criptografia

Fazendo-se uso da definição de (FADEL,2009):

> "O termo Criptografia tem origem grega e surgiu da fusão das palavras "*kryptós*" e "*graphein*", que significam "oculto" e "escrever", respectivamente. Trata-se de um conjunto de conceitos e técnicas que visa codificar uma informação de forma que somente o emissor e o receptor possam acessá-la, evitando que um intruso consiga interceptá-la."

Segundo (TRIGO,2007), na maioria das vezes, o servidor LDAP é utilizado para armazenar dados de usuários, como senha de autenticação, por exemplo, assim segurança é algo fundamental. Para aumentarmos a segurança no transporte de dados é possível criptografá-los, usando TLS ou SSL, assim mesmo que alguém consiga interceptar os dados, não conseguirá visualizar o que está sendo trafegado.

3.3.3 Módulo de Banco de Dados

Como mencionado anteriormente o LDAP é apenas um protocolo de comunicação entre um cliente e um serviço de diretórios. A definição do armazenamento das informações da árvore de diretórios é independente do mesmo, assim cada implementação do protocolo é responsável por fazer essa definição, podendo variar desde um simples arquivo texto até um banco de dados relacional completo. Segundo (TRIGO,2007), o OpenLDAP possui dois bancos de dados nativos, o LDBM e o BerkeleyDB, sendo que o segundo é para ele a melhor opção quanto ao desempenho.

3.3.4 Listas de Controle de Acesso (ACLs)

ACL é a definição de todos os recursos de acesso controlado e todos aqueles usuários que têm acesso a eles. Segundo (CARTER,2009), as ACLs disponibilizadas pelo OpenLDAP possuem uma sintaxe simples, além de serem também muito flexíveis e robustas em sua

implementação. A ideia básica das ACLs é definir quem tem acesso a quê. Abaixo é exposto um exemplo de ACL no OpenLDAP :

```
access to attrs=userPassword,shadowLastChange
        by dn="cn=admin,dc=fatene,dc=edu,dc=br" write
        by anonymous auth
        by self write
        by * none
# ACL de acesso de leitura da base.
access to dn.base="" by * read
# O admin dn tem acesso FULL de escrita
access to *
by dn="cn=admin,dc=fatene,dc=edu,dc=br" write
by * read
```

Fonte: Autoria própria

A ACL acima tem a função de permitir que apenas o dono tenha acesso de escrita no campo *userPassword*, ou seja, só ele pode mudar sua senha, que o usuário "cn=admin,dc=fatene,dc=edu,dc=br" consiga gravar esses atributos e que todos os demais deverão se autenticar como um usuário com permissão de acesso a esse atributo.

Resumidamente a sintaxe das ACLs no OpenLDAP é:

access to <o que> by <quem> <controle>

3.3.5 Backups e Restauração

O backup e restauração de uma base LDAP é extremamente fácil, como demonstrado com os comandos abaixo:

Para efetuarmos Backup de toda a base:

```
# ldapsearch -x -D cn=admin,dc=fatene,dc=edu,dc=br -b
dc=fatene,dc=edu,dc=br -LLL -W > backup.ldif
```

Fonte: Autoria própria

Para restaurar a base:

```
Pare o OpenLdap e remova a base danificada.

# service slapd stop ; rm /var/lib/ldap/*

Start o OpenLdap e copie o arquivo de exemplo DB_CONFIG

# service slapd start ; cp /usr/share/slapd/DB_CONFIG /var/lib/ldap/

Pare o OpenLdap e Restaure a base

# service slapd stop ; slapadd -l backup.ldif

Faça a indexação da Base, arrume as permissões e Inicie o Ldap

# slapindex -v
# chown openldap:openldap /var/lib/ldap/*
# service slapd start
```

Fonte: Autoria própria

Existem outras maneiras de fazer os procedimentos acima relacionados. Por exemplo, usando o *ldapadd*, não precisamos parar o serviço do *OpenLDAP* para efetuarmos o retorno dos dados, porém precisaremos ter um usuário com permissão administrativa para inserir os mesmos, diferente do *slapcat* o qual só precisa ter acesso ao diretório do banco de dados do *OpenLDAP* no caminho /var/lib/ldap/. Saber definir qual o procedimento mais adequado para a necessidade do cliente é extremamente importante.

4 ESTUDO DE CASO

4.1 LEVANTAMENTO DOS REQUISITOS

Para demonstração prática sobre o tema foi feito um estudo de caso de uma empresa com máquinas em *DualBoot* com sistemas operacionais *Microsoft Windows 7® Professional* 64 bits e *Ubuntu 14.04 64 bits* onde a autenticação é feita de forma centralizada através de um usuário e senha. O ambiente atual possui os seguintes usuários e grupos:

Tabela 2: Usuários e Grupos da empresa

Nome	Identificação	Grupo
Ana Paula	ana.p	Administrativo
Claudio Tezzi	claudio.t	Administrativo
Dayane Santos	dayane.s	Pessoal
Andreia Pereira	andreia.p	Pessoal
Gabriela Vieira	gabriela.v	Financeiro
Marcos Rauber	marcos.r	Financeiro
Bruno dos Santos	bruno.s	Compras
Karla Soares	karla.s	Compras

Fonte: Autoria própria

Iremos criar diretórios de acordo com a que serão usado para o armazenamento de arquivos que será usado por cada setor. Esses diretórios poderão ser usado para serem exportados pelo servidor NFS (Network File System) que é um protocolo de rede para compartilhamento de diretórios e arquivos entre sistemas GNU/Linux.

Tabela 3: Diretórios do servidor de arquivos

Diretório	Dono:Grupo	Permissões
/arquivos/	root:root	775
/arquivos/administrativo/	root:administrativo	3770
/arquivos/pessoal/	root:pessoal	3770
/arquivos/financeiro	root:financeiro	3770
/arquivos/compras	root:compras	3770

Fonte: Autoria própria

Outra estrutura de diretórios será criada para o armazenamento das lixeiras dos arquivos pessoais dos usuários.

Tabela 4: Diretórios das lixeiras dos usuários

Diretório	Dono:Grupo	Permissões
/arquivos/LIXEIRAS	root:root	755
/arquivos/LIXEIRAS/ana.p	ana.p:ana.p	0755
/arquivos/LIXEIRAS/claudio.t	claudio.t:claudio.t	0755
/arquivos/LIXEIRAS/dayane.s	dayane.s:dayane.s	0755
/arquivos/LIXEIRAS/andreia.p	andreia.p:andreia.p	0755
/arquivos/LIXEIRAS/gabriela.v	gabriela.v:gabriela.v	0755
/arquivos/LIXEIRAS/marcos.r	marcos.r:marcos.r	0755
/arquivos/LIXEIRAS/bruno.s	bruno.s:bruno.s	0755
/arquivos/LIXEIRAS/karla.s	karla.s:karla.s	0755

Fonte: Autoria própria

Para esta implementação foi definido como requisito a integração da autenticação entre os serviços, assim não deverá haver redundância de informações cadastrais dos usuários e lista de contatos, outro requisito é a utilização de soluções *OpenSource* de maneira a não dispor de recursos na aquisição de novas licenças com sistemas operacionais servidores.

Este documento abordará somente a instalação e configuração dos servidores LDAP, informações sobre a instalação dos outros serviços citados podem ser encontradas no próprio *website* dos respectivos desenvolvedores, onde normalmente já disponibilizam materiais com instruções para a instalação, como também nos livros de (TRIGO,2007) e (CARTER,2009).

4.2 DEFINIÇÃO DOS SOFTWARES A SEREM UTILIZADOS

4.2.1 Sistemas operacionais

Para a implementação destes servidores o primeiro item a ser definido é o sistema operacional que será usado, pois todos os softwares definidos posteriormente dependerão diretamente dessa definição.

Diversos sistemas foram considerados nessa implementação, porém alguns como o *Windows Server* e *Unix* foram descartados por termos como requisito, um sistema *OpenSource* o qual não demande custo de licenças, o que não é o caso dos mesmos. Assim se enquadram nesse perfil os sistemas *GNU/Linux*, porém os mesmos possuem uma infinidade

de derivações, denominadas distro ou distribuições, as quais se diferenciam em diversos casos muito uma da outra, assim escolher uma distribuição que se enquadre melhor aos requisitos do projeto é fundamental para o sucesso do mesmo.

Servidor:

- GNU/Linux Debian 7 64 bits;

Clientes:

- *Microsoft Windows 7® Professional*;
- *GNU/Linux Ubuntu 14.04 64 bits*;

Definimos o Debian 7 como a solução a ser implementada, pois trata-se de um sistema robusto, leve, possui um gerenciador de pacotes extremamente poderoso, o APT, além de contar com um sistema massivo de testes que garantem que os softwares disponibilizados para o mesmo, estarão realmente maduros, sendo esse seu principal diferencial.

4.2.2 NFS

O NFS será usado para compartilhamento dos arquivos entre os setores centralizando o armazenamento de arquivos podendo ser estendido ao uso de *Storages* (FreeNAS) com vários discos com nível de RAID.

4.2.3 SAMBA

O SAMBA será usado para integração do sistema operacional *Microsoft Windows 7®* com o servidor *GNU/Linux Debian 7* para o compartilhamento de arquivos, controlador de domínio e autenticação.

4.2.4 PhpLDAPadmin

Para facilitar o gerenciamento e administração da nossa base OpenLdap, iremos instalar a aplicação PhpLdapAdmin no servidor, utilizando Apache e Php e assim gerenciar a base OpenLDAP via web.

O PhpLdapAdmin é uma ferramenta com interface web, desenvolvida em PHP para o gerenciamento da base LDAP. Ela permite visualizar, modificar e excluir atributos ou objetos da árvore ldap, simplificando a administração e permitindo uma melhor visão da árvore como um todo.

4.2.5 Gerenciador de domínio e autenticação

Para essa definição foram considerados as três principais implementações do protocolo LDAP, o *Active Directory*, *eDirectory* e uma solução integrada entre OpenLDAP + Samba, porém a única solução que cumpre os requisitos é a junção SAMBA integrado ao OpenLDAP,

já que os outros são proprietários e demandam um investimento alto na aquisição de suas licenças.

4.3 INSTALAÇÃO DO SERVIDOR OPENLDAP

Antes da instalação do servidor do OpenLDAP é preciso ajustar alguns parâmetros importantes no sistema, os quais, farão grande diferença no ato de instalação do servidor OpenLDAP.

O primeiro parâmetro a ser verificado é *hostname* e FQDN no servidor, para isso devemos acessar o arquivo /etc/hosts e incluir as linhas a abaixo:

Arquivo /etc/hosts

```
172.25.0.100    master.fatene.edu.br    master
172.25.0.200    slave.fatene.edu.br     slave
```

Fonte: Autoria própria

Arquivo: /etc/hostname

```
master
```

Fonte: Autoria própria

Agora execute os seguintes comandos:

```
#/etc/init.d/hostname.sh ; /bin/bash
# hostname ; hostname -f
# ping -c3 master.fatene.edu.br
```

Fonte: Autoria própria

A saída do último comando deve ser:

```
PING master.fatene.edu.br (127.0.1.1) 56(84) bytes of data.
64 bytes from master.fatene.edu.br (127.0.1.1): icmp_req=1 ttl=64
time=0.022 ms
64 bytes from master.fatene.edu.br (127.0.1.1): icmp_req=2 ttl=64
time=0.036 ms
64 bytes from master.fatene.edu.br (127.0.1.1): icmp_req=3 ttl=64
time=0.036 ms

--- master.fatene.edu.br ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.022/0.031/0.036/0.008 ms
```

Fonte: Autoria própria

Agora faça a instalação do pacote *slapd*

```
# aptitude install slapd
```

Fonte: Autoria própria

No momento da instalação o gerenciador de pacotes vai pedir para que seja definida uma senha para ao usuário administrador da base LDAP. Defina uma senha e prossiga com a instalação. Ao terminar verifique se já existe uma base criada:

```
# slapcat |more
```

Fonte: Autoria própria

Veja a saída do comando acima:

```
dn: dc=fatene,dc=edu,dc=br
objectClass: top
objectClass: dcObject
objectClass: organization
o: fatene.edu.br
dc: fatene
structuralObjectClass: organization
entryUUID: cb24882c-2344-1035-88db-c71b55d41cf3
creatorsName: cn=admin,dc=fatene,dc=edu,dc=br
createTimestamp: 20151119200641Z
entryCSN: 20151119200641.358191Z#000000#000#000000
modifiersName: cn=admin,dc=fatene,dc=edu,dc=br
modifyTimestamp: 20151119200641Z

dn: cn=admin,dc=fatene,dc=edu,dc=br
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword:: e1NTSEF9SGFKQTdDQjhEMHVnYXorSCtKUGoyaDhKZGVRQ0c5OGY=
structuralObjectClass: organizationalRole
entryUUID: cb261700-2344-1035-88dc-c71b55d41cf3
creatorsName: cn=admin,dc=fatene,dc=edu,dc=br
createTimestamp: 20151119200641Z
entryCSN: 20151119200641.368407Z#000000#000#000000
modifiersName: cn=admin,dc=fatene,dc=edu,dc=br
modifyTimestamp: 20151119200641Z
```

Fonte: Autoria própria

Terminada a instalação do OpenLDAP, vamos agora configuração.

4.3.1 Configuração do OpenLDAP

Existem 2 modos de configuração do servidor OpenLDAP: através do arquivo */etc/ldap/slapd.conf* ou com o *cn=config* que é uma forma de fazer alterações *on-line*. Os sistemas atuais não utilizam o arquivo *slapd.conf* e sim o c*n=config* por padrão , então para reativar a utilização o arquivo *slapd.conf*.

Primeiramente para o serviço principal do OpenLDAP (*slapd*) copie o arquivo de exemplo slapd.conf no /etc/ldap/ e depois declare-o no /etc/default/slapd.

```
# service slapd stop
# cp /usr/share/slapd/slapd.conf /etc/ldap
# vim /etc/default/slapd
SLAPD_CONF = “/etc/ldap/slapd.conf”
```

Fonte: Autoria própria

Agora vamos editar o arquivo principal de configuração do OpenLDAP (/etc/ldap/slapd.conf):

```
# Servidor LDAP - FATENE - Administracao de Sistemas Operacionais
#
```

```
# Fatene @2015
#
# Desenvolvido por Mikael Ritlay <mikaelritlay@gmail.com>
# Creditos: Rafael Cristaldo <rafael@rafaelcristaldo.com.br>
#######################################################################
# Diretivas Globais:

# Compatibilidade com ldapv2
allow bind_v2

# Definicoes de Schema e objectClass
include         /etc/ldap/schema/core.schema
include         /etc/ldap/schema/cosine.schema
include         /etc/ldap/schema/nis.schema
include         /etc/ldap/schema/inetorgperson.schema

# Local de armazenamento do PID
pidfile         /var/run/slapd/slapd.pid

# Lista de argumentos passados ao servidor na inicialização

argsfile        /var/run/slapd/slapd.args

# Nivel de log
loglevel        none

# Local de armazanamento dos modulos
modulepath      /usr/lib/ldap
moduleload      back_hdb

# Numero maximo de entradas que podem retorar de uma pesquisa
sizelimit 500

# Quantos threads disponíveis para o servidor ldap - CPU
tool-threads 1

#######################################################################
# Diretiva específica do Backend HDB :
backend         hdb

#######################################################################
# Diretiva da base de dadosdatabase        hdb

# Base do servidor de diretorio LDAP - Domain Component - Raiz
suffix          "dc=fatene,dc=edu,dc=br"

# Diretiva que especifica o super usuario rootdn
rootdn          "cn=admin,dc=fatene,dc=edu,dc=br"
rootpw          {SSHA}VrJugOnxYhn13waH2NDK+/u+JRxYCxr/

# Arquivos da base de dados sao armazenados - BASE LDAP
directory       "/var/lib/ldap"

# Valores do arquivo DB_CONFIG
# Tamanho do cache
dbconfig set_cachesize 0 2097152 0
# Numero de objetos que podem ser travados ao mesmo tempo.
dbconfig set_lk_max_objects 1500
```

```
# Numero de travas
dbconfig set_lk_max_locks 1500
# Numbero de travadores
dbconfig set_lk_max_lockers 1500

# Opcoes de Indexacao para a base de dados
index           objectClass,uid,userPassword eq,pres
index           default                                 eq


# Salva o tempo das modificações de entrada na base de dados
lastmod         on

# Checkpoint a base BerkeleyDB database periodicamente em caso de falhas do
systema
checkpoint      128 5

# Configuracoes de ACL
# Permite que os usuários possam trocar de senha
access to attrs=userPassword,shadowLastChange
        by dn="cn=admin,dc=fatene,dc=edu,dc=br" write
        by anonymous auth
        by self write
        by * none

# ACL de acesso de leitura da base.
access to dn.base="" by * read

# O admin dn tem acesso FULL de escrita
access to *
        by dn="cn=admin,dc=fatene,dc=edu,dc=br" write
        by * read
```

Fonte: Autoria própria

Após a configuração do arquivo slapd.conf, devemos remover o diretório /etc/ldap/slapd.d e testar a nova configuração:

```
Pare o servidor OpenLDAP
# service slapd stop
Remova o diretório slapd.d
# cd /etc/ldap ; rm -rf slapd.d
Teste o arquivo de configuração com o slaptest e inicie o serviço:
# slaptest
565dc4ec /etc/ldap/slapd.conf: line 93: rootdn is always granted unlimited
privileges.
565dc4ec /etc/ldap/slapd.conf: line 101: rootdn is always granted unlimited
privileges.
config file testing succeeded
Inicie o servidor OpenLDAP
# service slapd start
[ ok ] Starting OpenLDAP: slapd.
```

Fonte: Autoria própria

4.3.1.1 Configuração de logs

Por padrão o *slapd* envia os registros de atividade de *log* para o arquivo de *log* padrão do sistema. Vamos definir um arquivo chamado *slapd.log*.

```
Abra o arquivo /etc/default/slapd e adicione o LOCAL em:
SLAPD_OPTIONS="-l LOCAL4"
Abra o arquivo /etc/rsyslog.conf e adicione a linha:
local4* /var/log/slapd.log
Restarte o serviço do rsyslog e do slapd.
# service rsyslog restart ; service slapd restart
[ ok ] Stopping enhanced syslogd: rsyslogd.
[ ok ] Starting enhanced syslogd: rsyslogd.
[ ok ] Starting OpenLDAP: slapd.
```

Fonte: Autoria própria

O OpenLDAP já está instalado e configurado no servidor.

4.4 INSTALAÇÃO DO PHPLDAPADMIN

Primeiro, vamos instalar o servidor apache, o php e outras dependências.

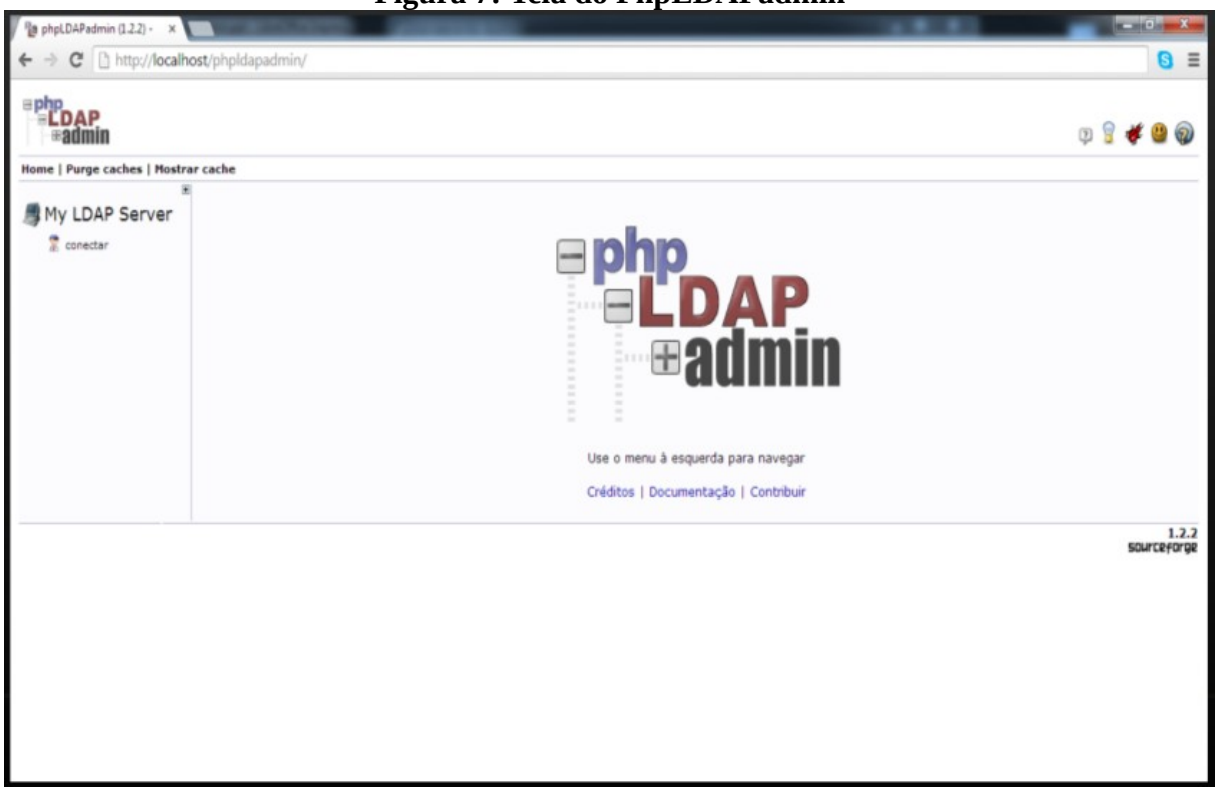
```
# aptitude update
# aptitude install apache2 libapache2-mod-php5 php5 php5-ldap
Agora instale o PhpLdapAdmin
# aptitude install phpldapadmin
```

Fonte: Autoria própria

Acesse o servidor usado o endereço:

http://172.25.0.100/phpldapadmin

Figura 7: Tela do PhpLDAPadmin



Fonte: Autoria própria

4.4.1 Configuração do phpldapadmin

Por padrão, o *phpldapadmin* utiliza alguns *templates*, os quais não vamos utilizar neste curso. Faça as alterações conforme segue:

```
Renomeie os .xml para desabilitar os templates
# cd /etc/phpldapadmin/templates/modification/
# mv inetOrgPerson.xml inetOrgPerson.xml.disable
# mv posixGroup.xml posixGroup.xml.disable
Abra o arquivo de configuração e descomente a linha abaixo:
# vim /etc/phpldapadmin/config.php
Linha 161
$config->custom->appearance['hide_template_warning'] = true;
Linha 286
$servers->setValue('server','name','Master LDAP Server');
Linha 300
$servers->setValue('server','base',array('dc=matrix'));
Linha 326
$servers-
>setValue('login','bind_id','dn="cn=admin,dc=fatene,dc=edu,dc=br"');
Vamos adicionar a opção Login shell /bin/bash e arrumar a opção do
HomeDirectory, removendo o /home/users
# /etc/phpldapadmin/templates/creation/posixAccount
Linha 41
<attribute id="uid">
<display>User ID</display>
+ <onchange>=autoFill(homeDirectory;/home/%uid%)</onchange>
Linha 69
<attribute id="loginShell">
<value id="/bin/sh">/bin/sh</value>
<value id="/bin/csh">/bin/csh</value>
<value id="/bin/tsh">/bin/tsh</value>
+ <value id="/bin/bash">/bin/bash</value>
```

Fonte: Autoria própria

Vamos configurar um novo *Vhost* para o *phpldapadmin* e fazer com que ele responda somente na porta 443.

```
Remova o link do http
# unlink /etc/apache2/conf.d/phpldapadmin
Vamos criar um certificado SSL
# mkdir -p /etc/apache2/ssl
# cd /etc/apache2/ssl
# openssl req -x509 -nodes -days 365 -newkey rsa:2048 -subj
"/C=BR/ST=Ceara/L=Fortaleza/O=Fatene/CN=master.fatene" -keyout fatene.key
-out fatene.pem
# vim /etc/apache2/sites-available/phpldapadmin
<IfModule mod_ssl.c>
<VirtualHost _default_:443>
ServerName master.fatene
ServerAdmin webmaster@fatene
DocumentRoot /usr/share/phpldapadmin/htdocs
ErrorLog /var/log/apache2/master.fatene-error.log
CustomLog /var/log/apache2/master.fatene-access.log common
SSLEngine on
SSLCertificateFile /etc/apache2/ssl/fatene.pem
SSLCertificateKeyFile /etc/apache2/ssl/fatene.key
</VirtualHost>
</IfModule>
Agora precisamos ativar o módulo ssl
# a2enmod ssl
Ative o site phpldapadmin e restart o apache2
```

```
# a2ensite phpldapadmin
# service apache2 restart
```

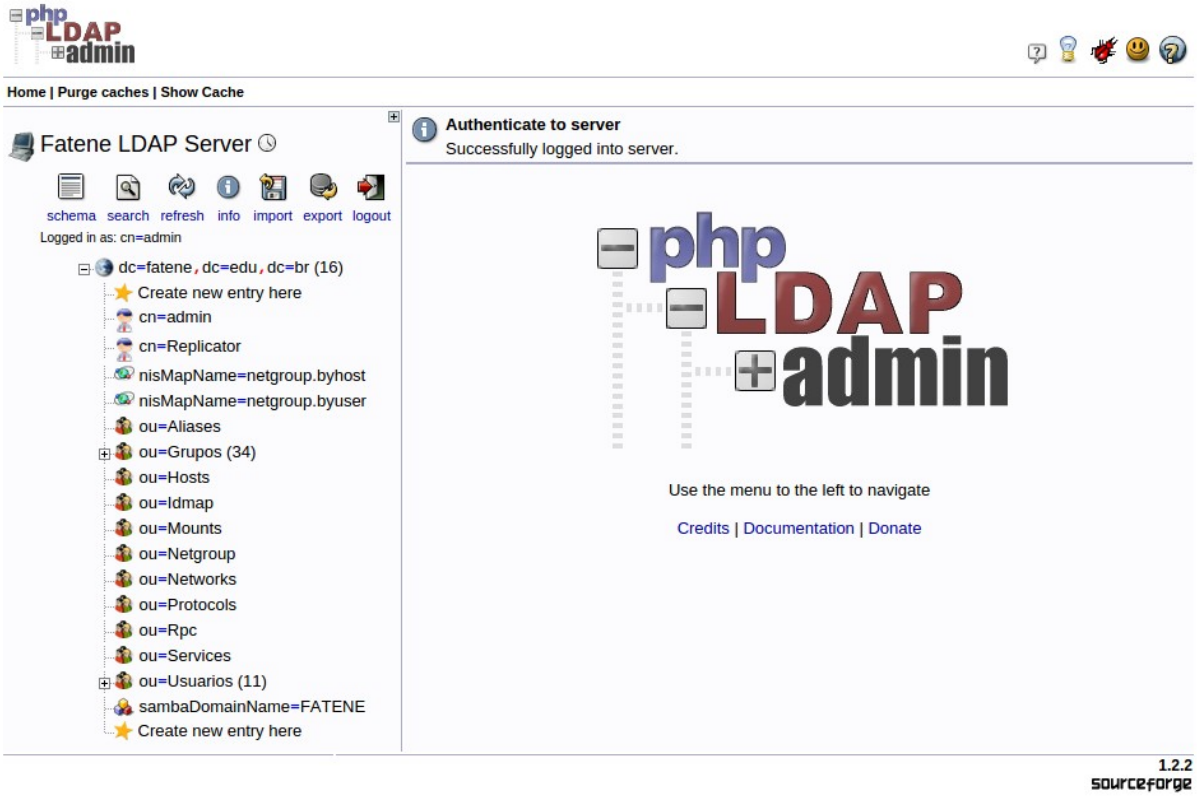
Fonte: Autoria própria

Teste o novo acesso SSL:

https://172.25.0.100/phpldapadmin

Agora estamos com a aplicação *phpLdapAdmin* instalada e configurada, sendo possível administrar o OpenLDAP via interface *web*, assim facilitando a criação de novos usuários e grupos.

Figura 8: Acesso a base com Phpldapadmin



Fonte: Autoria própria

5 CONCLUSÃO

Este trabalho tem por objetivo apresentar um protocolo extremamente importante quando falamos em centralização de aplicativos conectados em rede, o LDAP, demonstrando que este é uma ótima solução por contar com uma arquitetura distribuída, métodos nativos de segurança, contar com padrão aberto, internacionalização e suporte ao ipv6, além de diversas outras funcionalidades. Também foi demonstrado nesse trabalho o quanto flexível o protocolo LDAP pode ser, possibilitando uma gama de possibilidades para o uso do mesmo. Este foi focado na solução livre *OpenLDAP* , a qual, apresentou características compatíveis com ferramentas proprietárias e, em alguns casos, até mesmo os superando, isso sem a necessidade de desprendermos recursos para aquisição de licenças.

Acredita-se que este servirá como instrumento de referência para estudantes e profissionais da área de tecnologia que pretendem se aprofundar nesse protocolo, que a longa data é utilizado, massivamente, em empresas de médio a grande porte de todo o mundo.

6 REFERÊNCIAS

GOUVEIA,2009: B. Gouveia, LDAP para iniciantes, 2009, http://www.ldap.org.br/

Douglas Graciano Barth, Vanderson Siewert; Conceituação de DNS. : , 2009.

Clodonil Honório Trigo; OpenLDAP - Uma Abordagem Integrada. : Novatec, 2007.

OpenLDAPFoundation,2009: OPENLDAP FOUNDATION, OpenLDAP Software 2.4 Administrator's Guide, 2009, http://www.openldap.org/doc/admin24/

TUTTLE,2009: S. EHLENBERGER TUTTLE, , Understanding LDAP: Design and Implementation, 2009, http://www.redbooks.ibm.com/

RONALDO LOURO MENEGUITE;LDAP – AUTENTICAÇÃO CENTRALIZADA., CATAGUASES: 2009.

FADEL,2009: Désirée Faria Fadel, Cripografia RSA, 2009, http://www.ime.unicamp.br/~ftorres/ENSINO/MONOGRAFIAS/desi_RSA.pdf

Gerald Carter; LDAP - Administração de Sistemas. Rio de Janeiro: Alta Books, 2009.

7 GLOSSÁRIO

FreeWare — O termo é geralmente ligado a softwares que são disponibilizados de forma gratuita aos usuários.

General Public License (GPL) — Termo de designação, do Inglês, dado à Licença Pública Geral, criada pela *Free Software Foundation* (FSF), cujo fundador é Richard Stallman, em 1984. Esta licença encerra em si um acordo legal de uso de software no qual o usuário, tem acesso garantido ao código fonte, sendo convidado a alterá-lo e assim contribuir para seu desenvolvimento. A principal garantia é de que esta licença tem propriedade “virótica”, ou seja, ao se integrar a outros códigos, todos obrigatoriamente devem passar a serem licenciados sob a GPL, e portanto o autor deve disponibilizar os códigos fonte de tudo.

LibreOffice — Pacote de aplicativos para computadores, aplicável a diversas plataformas com soluções para escritório e finalidade acadêmica

Normas — Conjunto de regras editadas por instituições responsáveis por compor e publicar padrões internacional e nacionais

Open Source — É uma classificação que se dá a softwares que têm seu código fonte público. Difere do *Freeware*, pois o este pode ser gratuito, mas em geral o código não é disponível a público. Já o *OpenSource*, em geral é licenciado sob a *General Public License* (GPL), ou outras licenças, que se caracterizam por deixar livre a sua utilização, alteração e até revenda, sem custos.

GNU — É um acrônimo recursivo para *GNU is Not Unix*. GNU é um sistema operacional tipo Unix cujo objetivo desde sua concepção é oferecer um sistema operacional completo e totalmente composto por software livre, isto é, que respeita a liberdade dos usuários.

Apêndice A – Exemplo de arquivos integração com do SAMBA com OpenLDAP

Arquivo de configuração principal do SAMBA como PDC: /etc/samba/smb.conf:

```
[global]
        workgroup = FATENE
        netbios name = master
        server string = Servidor de Domínio FATENE
        printing = cups
        load printers = Yes
        log level = 1
        log file = /var/log/samba/samba.log.%m
        max log size = 10000
        passwd program = /usr/sbin/smbldap-passwd -u %u
passwd chat = *Enter\snew\s*\spassword:* %n\n *Retype\snew\s*\spassword:*
%n\n *password\supdated\ssuccessfully* .
        encrypt passwords = yes
        ldap password sync = yes
        domain master = yes
        wins support = yes
        time server = yes
        domain logons = yes
        logon path = \\%L\%U\profile
        logon drive = H:
        logon home = \\%L\%U
        logon script = logon.bat
        preferred master = yes
os level = 200
        enable privileges = yes
        admin users = root
        # Integração do Samba com Ldap
        username map = /etc/samba/smbusers
        add user script = /usr/sbin/smbldap-useradd -m "%u"
        add machine script = /usr/sbin/smbldap-useradd -t 0 -w "%u"
        add group script = /usr/sbin/smbldap-groupadd -p "%g"
        add user to group script = /usr/sbin/smbldap-groupmod -m "%u" "%g"
        delete user script = /usr/sbin/smbldap-userdel "%u"
        delete group script = /usr/sbin/smbldap-groupdel "%g"
        delete user from group script = /usr/sbin/smbldap-groupmod -x "%u"
"%g"
        set primary group script = /usr/sbin/smbldap-usermod -g "%g" "%u"
        passdb backend = ldapsam:ldap://master.fatene.edu.br
        ldap suffix = dc=fatene,dc=edu,dc=br
        ldap machine suffix = ou=Hosts
        ldap user suffix = ou=Usuarios
        ldap group suffix = ou=Grupos
        ldap admin dn = cn=admin,dc=fatene,dc=edu,dc=br
        ldap ssl = off
        security = user
        username level = 2
        hide unreadable = yes
        veto files = /*.mp3/*.mkv/*.avi/
        hide files = /*.ini/*.log/
        interfaces =  lo eth0
        bind interfaces only = yes
```

```
        preserve case = Yes
        default case = lower
        display charset = UTF8
        unix charset = UTF8
        dos charset = 850
        vfs objects = recycle, full_audit
        # Lixeiras
        recycle:keeptree = True
        recycle:touch = True
        recycle:versions = True
        recycle:noversions = .doc| .xls| .pdf| .html| .ppt| .txt
        recycle:repository = /srv/LIXEIRAS/%U
        recycle:exclude = *.tmp *.log *.obj ~*.* *.bak
        recycle:exclude_dir = tmp, cache
        recycle:maxsize = 10000000

        #Auditoria
        full_audit:success = open, opendir, write, unlink, rename, mkdir,
rmdir, chmod
        full_audit:prefix = %u|%I|%S
        full_audit:failure = none
        full_audit:facility = local5
        full_audit:priority = notice
#================ Definições de Compartilhamento ======================#

[LIXEIRAS]
        comment = LIXEIRAS DOS USUARIOS
        path = /arquivos/LIXEIRAS/%U
        writable = yes
[homes]
        comment = Diretorio Home
        root preexec = /etc/samba/scripts/mkhomdir.sh %S
        browseable = no
        writable = yes
        create mask = 0640
        directory mask = 0750
        valid users = %S
        vfs object = recycle
        recycle:keeptree = True
        recycle:touch = True
        recycle:versions = True
        recycle:noversions = .doc| .xls| .pdf| .html| .ppt| .txt
        recycle:repository = .Trash/%U
        recycle:exclude = *.tmp, *.log, *.obj, ~*.*, *.bak
        recycle:exclude_dir = tmp, cache
        recycle:maxsize = 10000000
[netlogon]
        path = /home/netlogon
        browseable = no
        read only = yes
[printers]
        comment = Samsung ML-2010
        browseable = yes
        path = /var/spool/samba
        writable = no
```

```
        guest ok = yes
        print ok = yes
[administrativo]
        comment = Diretorio Administrativo
        path = /arquivos/samba/administrativo
        available = yes
        writable = yes
        write list = @administrativo
[compras]
        comment = Diretorio Compras
        path = /arquivos/samba/compras
        available = yes
        writable = yes
        write list = @compras
[financeiro]
        comment = Diretorio Financeiro
        path = /arquivos/samba/financeiro
        available = yes
        writable = yes
        write list = @financeiro
[pessoal]
        comment = Diretorio Pessoal
        path = /arquivos/samba/pessoal
        available = yes
        writable = yes
        write list = @pessoal
```

Fonte: Autoria própria

Arquivo de configuração do smbldap-tools: /etc/smbldap-tools/smbldap.conf

```
SID="S-1-5-21-1424700921-664739437-2864376241"
sambaDomain="fatene"
masterLDAP="master.fatene.edu.br"
masterPort="389"
ldapTLS="0"
ldapSSL="0"
verify="none"
suffix="dc=fatene,dc=edu,dc=br"
usersdn="ou=Usuarios,${suffix}"
computersdn="ou=Hosts,${suffix}"
groupsdn="ou=Grupos,${suffix}"
idmapdn="ou=Idmap,${suffix}"
sambaUnixIdPooldn="sambaDomainName=${sambaDomain},${suffix}"
scope="sub"
password_hash="SSHA"
password_crypt_salt_format="%s"
userLoginShell="/bin/bash"
userHome="/home/%U"
userHomeDirectoryMode="700"
userGecos="System User"
defaultUserGid="513"
skeletonDir="/etc/skel"
shadowAccount="1"
defaultMaxPasswordAge="45"
userSmbHome="\\%L\homes\%U"
userProfile="\\%L\%U\profile"
```

```
userHomeDrive="H:"
userScript="logon.bat"
mailDomain="fatene.edu.br"
with_smbpasswd="0"
smbpasswd="/usr/bin/smbpasswd"
with_slappasswd="0"
slappasswd="/usr/sbin/slappasswd"
```

Arquivo de configuração do smbldap-tools: /etc/smbldap-tools/smbldap_bind.conf

```
slaveDN="cn=admin,dc=fatene,dc=edu,dc=br"
slavePw="senha"
masterDN="cn=admin,dc=fatene,dc=edu,dc=br"
masterPw="senha"
```

Fonte: Autoria própria

ÍNDICE