RONALDO LOURO MENEGUITE

LDAP – AUTENTICAÇÃO CENTRALIZADA

BACHARELADO EM SISTEMAS DE INFORMAÇÃO

FACULDADES UNIFICADAS DOCTUM DE CATAGUASES
CATAGUASES – MG – BRASIL
2009

RONALDO LOURO MENEGUITE

LDAP – AUTENTICAÇÃO CENTRALIZADA

Trabalho de Conclusão de Curso apresentado à Banca Examinadora das Faculdades Unificadas Doctum de Cataguases como requisito parcial para a obtenção do título de Bacharel em Sistemas de Informação, sob a orientação do Profª. Marília das Dores de Barros.

FACULDADES UNIFICADAS DOCTUM DE CATAGUASES
CATAGUASES – MG – BRASIL
2009

RONALDO LOURO MENEGUITE

LDAP – AUTENTICAÇÃO CENTRALIZADA

Trabalho de Conclusão de Curso apresentado à Banca Examinadora das Faculdades Unificadas Doctum de Cataguases como requisito parcial para a obtenção do título de Bacharel em Sistemas de Informação.

BANCA EXAMINADORA

_____

Profa. Marília das Dores de Barros. – Orientadora
Faculdades Unificadas Doctum de Cataguases

_____

Prof. Norberto da Silva Prado
Faculdades Unificadas Doctum de Cataguases

_____

Prof. Frands de Souza Franco
Faculdades Unificadas Doctum de Cataguases

CATAGUASES – MG – BRASIL
2009

Dedico este trabalho à memória de meu querido avô Olívio Silveira Louro, que certamente foi fundamental para tornar esta graduação possível.

AGRADECIMENTOS

Agradeço a Deus.

À minha noiva e companheira Mara, por sua compreensão e dedicação em todos os momentos.

Aos meus pais e família que, com muito carinho e apoio, não mediram esforços para que eu chegasse até esta etapa de minha vida.

À professora e orientadora Marília Barros por seu apoio e inspiração no amadurecimento dos meus conhecimentos e conceitos que me levaram a execução e conclusão desta monografia.

À professora Fabiana S. N. Menta por sua dedicação e zelo quanto às revisões deste trabalho.

Ao amigo Samuel Honorato, que sempre se manteve disponível para os meus questionamentos, apoiando e incentivando a busca de novos conhecimentos.

Aos professores Norberto, Miriam e Maria Aparecida por suas contribuições, mesmo quando este ainda era apenas um projeto.

“Uma mente que se abre a uma nova idéia jamais volta ao seu tamanho original”.
(**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. Teremos nesse também, um estudo de caso fictício, com uma análise de soluções disponíveis de todos os principais serviços implementados internamente em empresas de pequeno a médio porte, gerando uma solução completa baseada em softwares OpenSource e sempre com foco na centralização gerada pela implementação do protocolo LDAP.

Palavras-chave: LDAP, OpenLDAP , Centralização, Criptografia e OpenSource

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

SIGLAS	SIGNIFICADOS
ACL	*Access control list*
AD	*Active Directory*
AIX	*Advanced Interactive eXecutive*
APT	*Advanced Packaging Tool*
BDB	*Berkeley´s Data Base*
BSD	*Berkeley Software Distribution*
CCITT	*Consultative Committee for International Telegraphy and Telephony*
DAP	*Directory Access Protocol*
DNS	*Domain Name System*
FTP	*File Transfer Protocol*
GPO	*Group Policy Objects*
HP-UX	*Hewlett Packard UniX*
HTTP	*HyperText Transfer Protocol*
IETF	*Internet Engineering Task Force*
IMAP	*Internet Message Access Protocol*
IP	*Internet Protocol*
ISO	*International Organization Standardization*
LDAP	*Lightweight Directory Access Protocol*
LDIF	*LDAP Interchange Format*
MTA	*Mail Transfer Agent*
NT	*New Technology*
OSI	*Open Systems Interconnection*
POP	*Post Office Protocol*
RFC	*Request for Comments*
SMTP	*Simple Mail Transfer Protocol*
SNMP	*Simple Network Management Protocol*
SQL	*Structured Query Language*
SSH	*Secure Shell*

SSL	*Secure Socket Layer*
SSO	*Single Sign On*
TCP	*Transmission Control Protocol*
TSL	*Transport Layer Security*

SUMÁRIO

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.

O presente documento divide-se em capítulos.

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.

1. O PROTOCOLO LDAP

1.1 Origens 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 (2005), 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 e SIEWERT (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 overhead1 de camadas superiores do modelo OSI.

Segundo GOUVEIA (2005) 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.

1.2 Protocolo LDAP vs X.500

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.

[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.

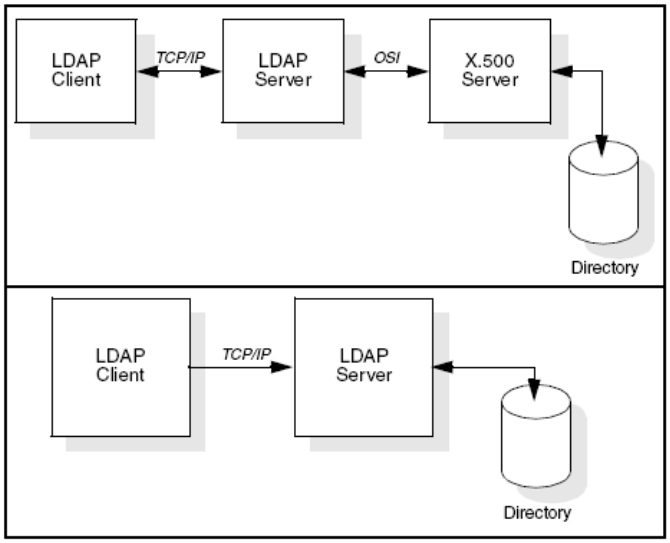

Figura 1: Aplicação LDAP
Fonte: OpenLDAP Foundation (2009)

1.3 Noções teóricas sobre o LDAP

1.3.1 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.

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

O LDAP, segundo BARTH e SIEWERT (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
- Segurança
- Padrão aberto
- Solicitação de funcionalidades e esquemas do servidor
- Internacionalização
- Suporte ao IPv6
- *Berkeley´s Data Base* (BDB)

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

Ainda segundo BARTH e SIEWERT (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.

Para LOSANO (2009) 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.

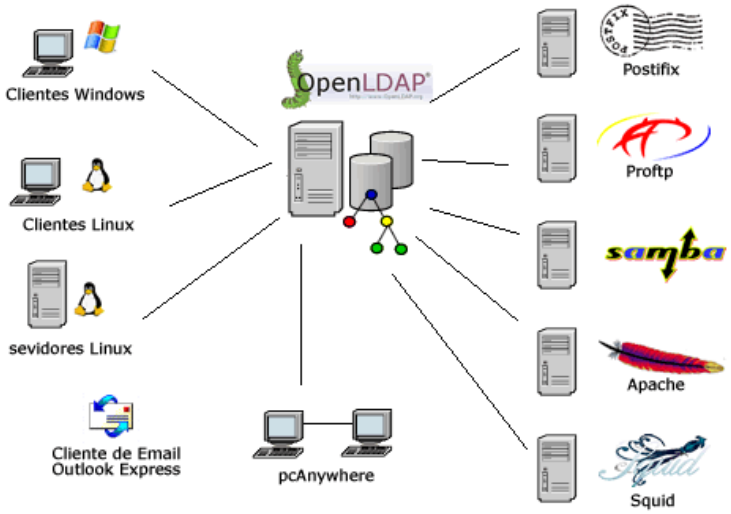

Figura 2: Característica do LDAP
Fonte: OpenLDAP Foundation (2009)

1.3.3 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:
Fonte: Própria

Atributo	Descrição
Dc	Identificação única do Objeto (do inglês *Distinguished Name*)
C	Para diretórios que representam países (do inglês *country*)
O	Para o nome da empresa (do inglês *organization*)
Ou	Para departamento (do inglês *organization unit*)
Cn	Como atributo de Nome (do inglês *common name*)
Uid	Identidade do usuário (do inglês *user id*)
Gn	Nome próprio da pessoa (do inglês *given name*)

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.

Na figura 4 abaixo podemos visualizar uma estrutura baseada nesse estilo.

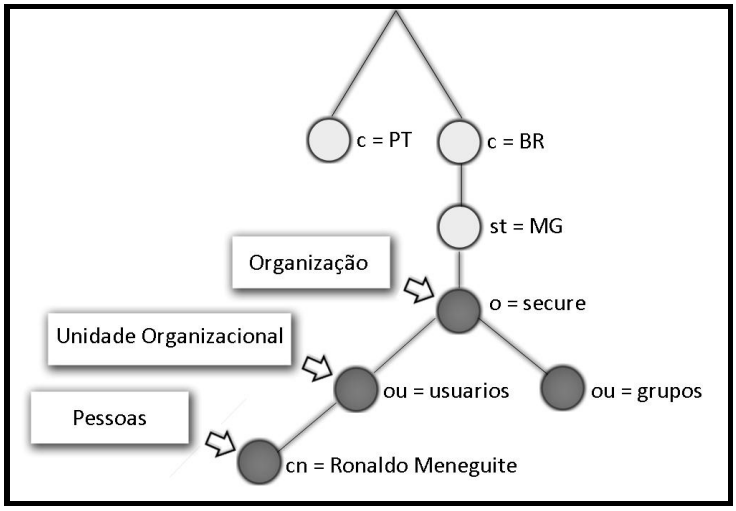

Figura 3: Estrutura no estilo X.500

Fonte: Própria

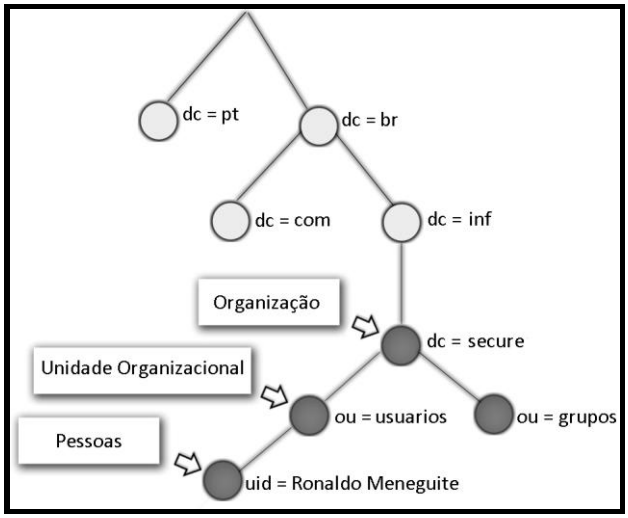

Figura 4: Estrutura no estilo DNS

Fonte: Própria

1.3.4 *Schema* – Segundo GOUVEIA (2005), 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.

S*chemas* 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.

1.3.5 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.

Arquivo insereUser.ldif

```
dn: cn=ronaldo,dc=secure,dc=inf,dc=br
cn: ronaldo
objectClass: simpleSecurityObject
objectClass: organizationalRole
userPassword: {SSHA}4P4F2gCtCh7PthUlS1AJ+DOMXOI0iUpH
description: Usuario Ronaldo
```

Arquivo atualizaUser.ldif

```
dn: cn=ronaldo,dc=secure,dc=inf,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}tNnd/KF/Rg/dCTq4S1yo7OEiUK4aFk9g
```

2. 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.

2.1 Active Directory

O Active Directory é uma implementação do serviço de diretório utilizando o protocolo LDAP que armazena informações sobre objetos em redes de computadores e disponibiliza essas informações a usuários e administradores desta rede. É um software da Microsoft utilizado em ambientes *Windows* e que segundo SANTANA (2009) surgiu juntamente com o *Windows* 2000 *Server*.

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.

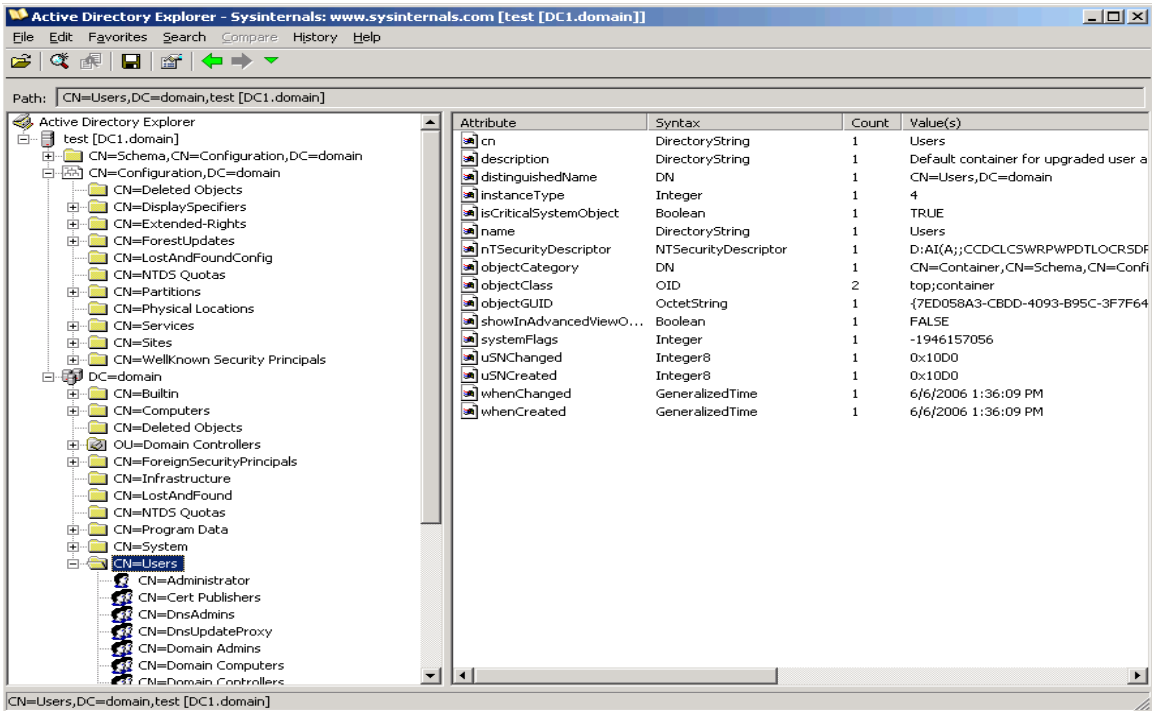

Figura 5: Exemplo de implementação do Active Directory
Fonte: Própria

2.2 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.

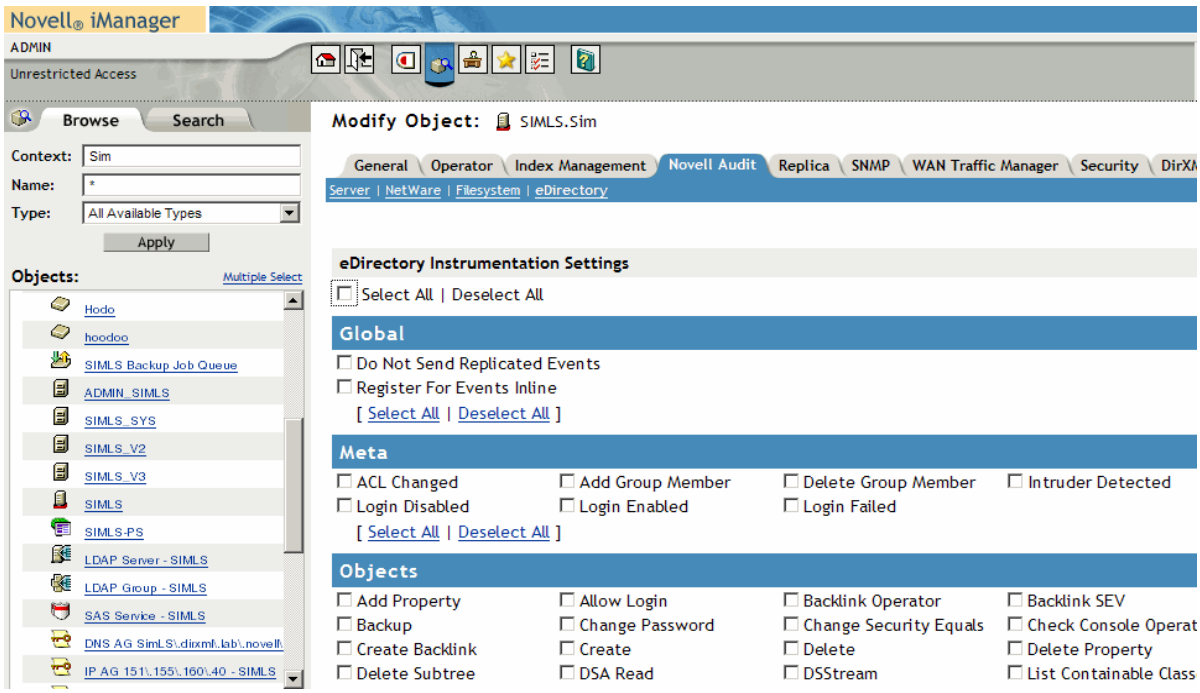

Figura 6: Exemplo de implementação do eDirectory
Fonte: Novel (2009)

2.3 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).

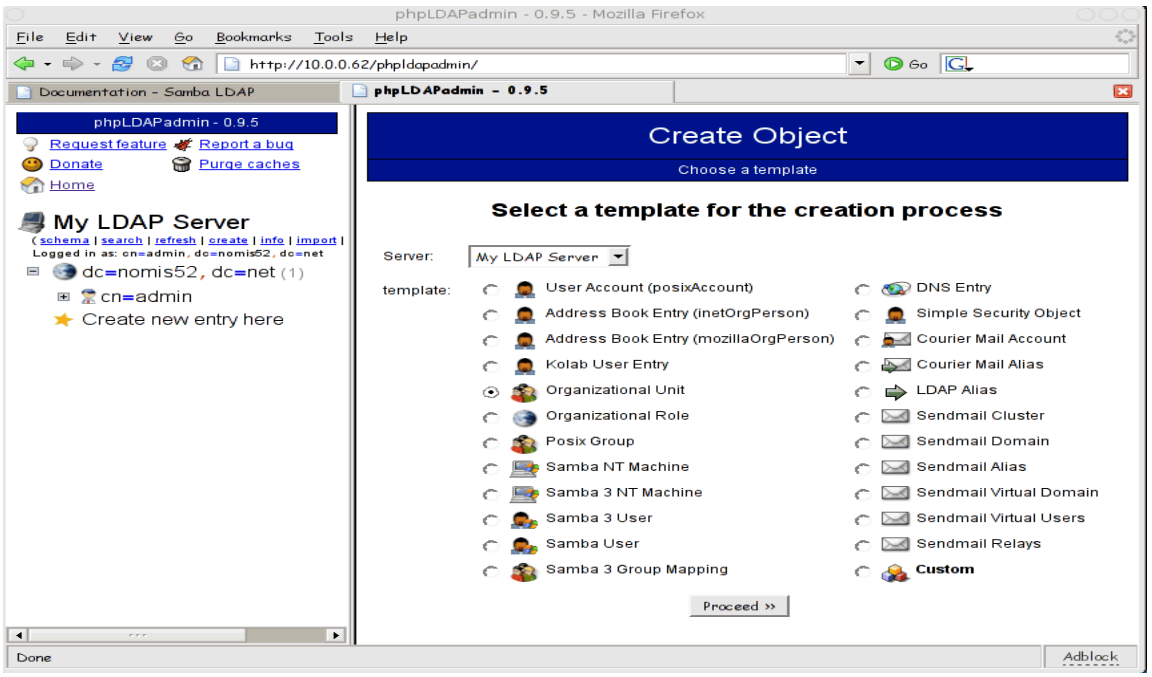

Figura 7: Implementação do LDAP + phpLDAPAdmin

Fonte: Própria

2.3.1 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*.

2.3.1.1 Replicação 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.

2.3.1.2 Replicação *Master* x *Master* (*multimaster*) – 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.

2.3.1.3 Diretórios Distribuídos – Utilizando o OpenLpad 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.

2.3.2 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.

2.3.3 Módulos 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.

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

```
# ACL do Atributo userPassword
Access to attrs=userPassword
        by      self                                    write
        by      cn=backup,dc=secure,dc=inf,dc=br        read
        by      *                                       auth
```

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=backup,dc=secure,dc=inf,dc=br consiga apenas ler esse atributo 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>

2.3.5 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:

slapcat > backup.ldif

Retornar o backup (é necessário estarmos com a base parada)

slapadd –l backup.ldif

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.

3. ESTUDO DE CASO

3.1 Levantamento de requisitos

Para uma demonstração prática sobre o tema foi feito um estudo de caso da empresa Secure Info Ltda, uma empresa de consultoria na área de segurança da informação a qual está se preparando para entrar no mercado. A Secure Info possui demanda de uma série de serviços os quais pretende prover internamente, sendo eles:

Servidor interno de e-mail (com soluções SMTP, POP e IMAP);

Sistema gerenciador de domínio e autenticação (máquinas Windows e Linux);

Servidor FTP;

Sistema de Webmail;

Servidor de Proxy;

Servidor Web;

Servidor SSH;

Servidor de Arquivos.

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.

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 do desenvolvedor, onde normalmente já disponibilizam materiais com instruções para a instalação, como também nos livros de CARTER (2009) e TRIGO (2007).

3.2 Definição de Softwares a serem usados

3.2.1 Sistema operacional – 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 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.

As distribuições avaliadas foram:

Suse Linux Enterprise 11;
OpenSuse 11.1;
RedHat Enterprise 5.4;
Fedora 11;
Unbutu Server 8.04 LTS;
Debian 5;

Diante das distribuições avaliadas, duas inicialmente já foram descartadas por se tratarem de distribuições comerciais as quais demandam um custo elevado para aquisição da licença de uso, são elas: Suse Linux Enterprise 11 e RedHat Enterprise 5.4. Das demais, todas cumpririam os pré-requisitos identificados, assim definimos o Debian 5 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.

3.2.2 Sistema 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 OpenLDAP + Samba, já que os outros são proprietários e demandam um investimento alto na aquisição de suas licenças.

3.2.3 Sistema de e-mail – Diversos sistemas gerenciadores de e-mails também conhecidos como MTA estão disponíveis hoje no mercado, os principais são Microsoft Exchange, Qmail e Postfix. O Microsoft Exchange é um sistema muito bom, porém não é compatível com o sistema operacional adotado, assim restam-nos duas soluções o Qmail e PostFix, diante das mesmas optaremos pela solução Postfix a qual conta com um desenvolvimento bem mais ativo que o Qmail, além de possuir material de apoio muito bom e amplo.

3.2.4 Servidor FTP – Existe hoje uma infinidade de opções em soluções FTP, como por exemplo, proftpd, pureftp e o vsftpd, porém as mesmas possuem características muito similares sendo assim optaremos pela implementação da solução proftpd a qual atende os requisitos e possui uma maior compatibilidade de integração com o servidor de autenticação baseada no OpenLDAP .

3.2.5 Servidor de Arquivo – Para servidor de arquivo utilizaremos o SAMBA por atender os requisitos iniciais do projeto além de já estar disponível no sistema devido a necessidade do mesmo para autenticarmos os usuários na rede.

3.3 Definição da divisão dos serviços entre os servidores

Para esta implementação usaremos a seguinte estrutura:

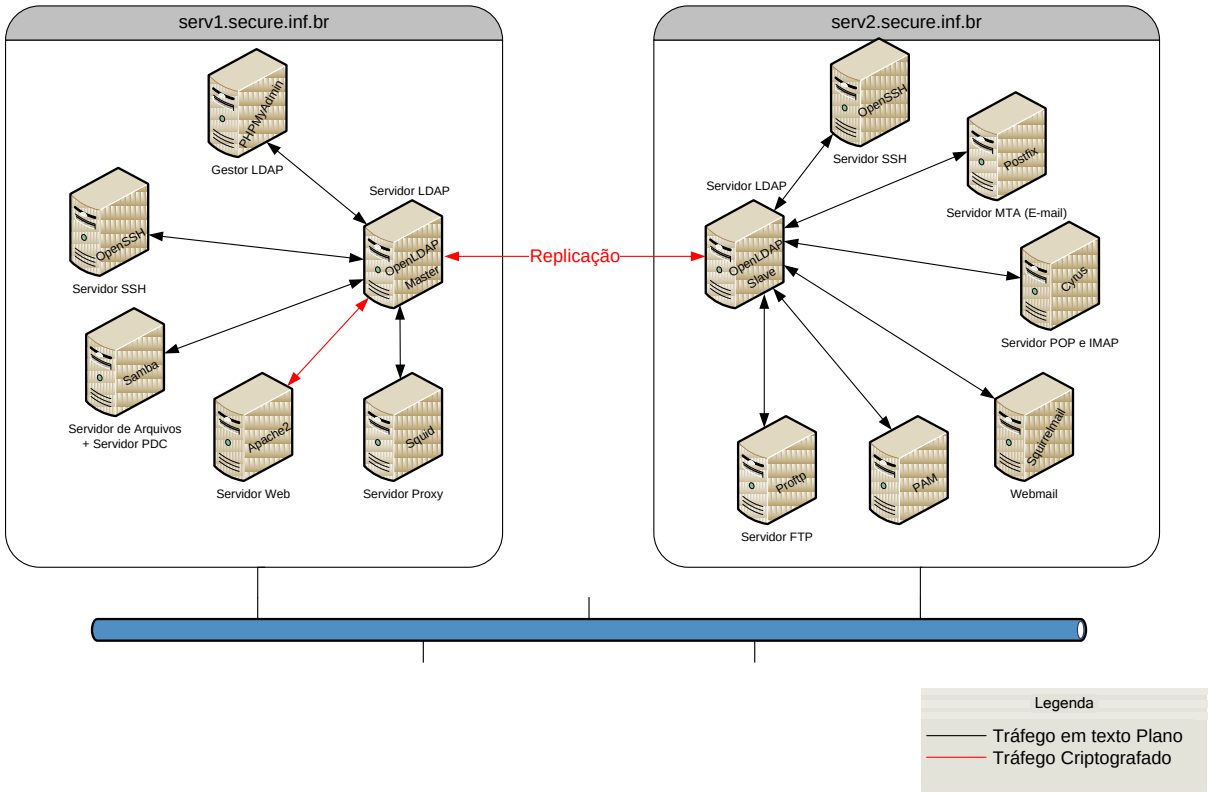

Figura 8: Estrutura de divisão dos serviços entre os servidores

Fonte: Própria

Cada figura de servidor representa um serviço rodando dentro do respectivo servidor.

3.4 Instalação do Servidor OpenLDAP

3.4.1 Requisitos para a instalação do OpenLDAP - O primeiro procedimento adotado foi a atualização dos repositórios instalados com o comando:

- *apt-get update*

Logo depois a atualização dos pacotes instalados:

- *apt-get upgrade*

Antes de iniciar a instalação verificamos alguns parâmetros importantes no sistema, os quais, farão grande diferença no ato da instalação do OpenLDAP .

O primeiro parâmetro verificado se encontra no arquivo /etc/hosts, onde deverá ser informado o IP do servidor, nome, domínio e apelido da máquina.

Foram inseridos os seguintes parâmetros logo abaixo da linha, que referencia o localhost.

```
127.0.0.1           serv1.secure.inf.br   serv1
192.168.239.134     serv1.secure.inf.br   serv1
```

O segundo parâmetro verificado foi no arquivo /etc/hostname onde substituímos o nome serv1 para seu nome completo serv1.secure.inf.br.

Com esses parâmetros configurados cumprimos os requisitos básicos para iniciarmos a instalação.

3.4.2 Instalação do OpenLDAP e seus utilitários - Para a instalação do OpenLDAP e seus utilitários utilizamos o seguinte comando:

- apt-get install slapd ldap-utils

Na instalação inicial, o próprio debian cria baseado nos parâmetros os quais foram alterados anteriormente uma estrutura previa da árvore, assim não precisamos fazer esse processo manualmente.

Nesta instalação a árvore em formato DNS foi criada com a raiz "dc=secure,dc=inf,dc=br", parâmetro esse que servirá de base para todos os itens que o sucederem.

O arquivo de configuração principal do OpenLDAP é o /etc/ldap/slapd.conf, este é algo como um centro de controle do OpenLDAP e é nele que faremos várias configurações durante todo o processo de instalação do servidor.

Com a base montada procedemos com o seguinte comando para verificar se o servidor OpenLDAP está de fato configurado corretamente:

- ldapsearch -x -h localhost -b "dc=secure,dc=inf,dc=br"

O retorno foi:

dn: dc=secure,dc=inf,dc=br
objectClass: top
objectClass: dcObject
objectClass: organization
o: secure.inf.br
dc: doctum

dn: cn=admin,dc=secure,dc=inf,dc=br
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator

Com esse retorno demos sequência à instalação inserindo alguns objetos na árvore, de maneira a povoá-la adequadamente. Como descrito anteriormente, a única maneira de transferir dados a um servidor LDAP é fazendo uso de arquivos do tipo ldif, assim prosseguiremos criando um arquivo, o qual será o responsável por criar alguns grupos em nossa árvore.

Abaixo podemos visualizar o conteúdo do arquivo grupos.ldif :

dn: ou=grupos,dc=secure,dc=inf,dc=br
ou: Grupos
objectClass: organizationalUnit
objectClass: top

```
dn: ou=usuarios,dc=secure,dc=inf,dc=br
ou: Grupos
objectClass: organizationalUnit
objectClass: top

dn: ou=ti,ou=usuarios,dc=secure,dc=inf,dc=br
ou: ti
objectClass: organizationalUnit
objectClass: top

dn: ou=base_teste,ou=usuarios,dc=secure,dc=inf,dc=br
ou: base_teste
objectClass: organizationalUnit
objectClass: top

dn: ou=administracao,ou=usuarios,dc=secure,dc=inf,dc=br
ou: administracao
objectClass: organizationalUnit
objectClass: top
```

Para inserirmos esses grupos em nossa árvore faremos uso do seguinte comando:

- ldapadd -h localhost -x -D cn=admin,dc=secure,dc=inf,dc=br -w senha -f grupos.ldif

Para a inserção de usuários usaremos o arquivo usuarios.ldif descrito abaixo:

```
dn: uid=ronaldo,ou=ti,ou=usuarios,dc=secure,dc=inf,dc=br
uid: ronaldo
cn: Ronaldo Meneguite
sn: Meneguite
objectClass: inetOrgPerson
objectClass: posixAccount
homeDirectory: /home/ronaldo
loginShell: /bin/bash
uidNumber: 1000
gidNumber: 1000
userPassword: {SSHA}sZmrhpFA7XTkVGVrljx7QiUqU8kFLMlo
dn: cn=replicator,dc=secure,dc=inf,dc=br
cn: replicator
objectClass: simpleSecurityObject
objectClass: organizationalRole
userPassword: {SSHA}sZmrhpFA7XTkVGVrljx7QiUqU8kFLMlo
description: LDAP Replicator

dn: uid=estagio,ou=ti,ou=usuarios,dc=secure,dc=inf,dc=br
uid: estagio
```

cn: Estagiario
sn: Estagiaro
objectClass: inetOrgPerson
objectClass: posixAccount
homeDirectory: /home/estagio
loginShell: /bin/bash
uidNumber: 1002
gidNumber: 1000
userPassword: {SSHA}sZmrhpFA7XTkVGVrljx7QiUqU8kFLMlo

Para inserirmos esses grupos em nossa árvore faremos uso do seguinte comando:

- ldapadd -x -D cn=admin,dc=secure,dc=inf,dc=br -w senha -f usuarios.ldif

Com o comando abaixo, podemos verificar se os grupos e usuários foram inseridos com sucesso.

- ldapsearch –x –b =secure,dc=inf,dc=br

Com sucesso nos comandos acima, foi listado todo o conteúdo do diretório LDAP inclusive com os grupos e usuários inseridos anteriormente, tendo assim em mãos um servidor OpenLDAP configurado e pronto para usar.

Para o segundo servidor o serv2.secure.inf.br foi efetuado o mesmo procedimento de instalação do serviço, não inserindo os usuários e grupos como no servidor principal, visto que os mesmos serão replicados quando configurarmos a replicação.

3.5 Ativando suporte a criptografia

O servidor OpenLDAP suporta trabalhar com dois esquemas de criptografia sendo eles, o SSL ou TLS onde a diferença entre eles é que o SSL por ser uma camada de segurança, tem sua porta alterada para uma porta diferente da padrão, a 389, enquanto no TLS, a criptografia é feita na camada de transporte, o que propicia ser ativado sem alteração da porta do serviço.

A resistência da criptografia quando em ataque, tanto na SSL quanto do TLS é basicamente a mesma, visto que ambos são fornecidos pelo OpenSSL. Para este estudo de caso utilizaremos o TLS como método de criptografia.

3.5.1 Ativando suporte a TLS – Para ativar o suporte a TLS será usado a seguinte sequência de comandos:

Instalar o OpenSSL

- apt-get install openssl

Criar o diretório para armazenamento da chave

- mkdir /etc/ldap/tls
- cd /etc/ldap/tls

Criando a agência certificadora

- /usr/lib/ssl/misc/CA.sh –newca

Criando certificado do servidor:

- openssl req –new –nodes –keyout newreq.pen –out newreq.pem

Assinando o certificado do servidor com o da agência certificadora criada:

- /usr/lib/ssl/misc/CA.sh –sign

Alterando os nomes dos certificados gerados para facilitar a identificação:

- mv newcert.pem srvcert.pem
- mv newreq.pem srvkey.pem

Copiando o certificado da agência certificadora para o mesmo diretórios dos outros:

- cp demoCA/cacert.pem .

3.5.2 Ativando TLS no OpenLDAP – Para ativarmos o suporte a TLS no OpenLDAP devemos adicionar no arquivo /etc/ldap/slapd.conf as seguintes linhas logo após a inclusão dos schemas:

```
TLSCertificateFile /etc/ldap/tls/srvcert.pem
TLSCertificateKeyFile /etc/ldap/tls/srvkey.pem
TLSCACertificateFile /etc/ldap/tls/cacert.pem
```

Após a inserção das linhas acima mencionadas reiniciamos o servidor com o seguinte comando:

- /etc/init.d/slapd restart

Para testarmos a comunicação criptografada, prosseguimos com a configuração do cliente LDAP, sendo ele instalado junto com o servidor, de maneira que o mesmo possa utilizar TLS, bastando para isso inserirmos no final do arquivo a seguinte linha:

```
TLS_CACERT /etc/ldap/tls/cacert.pem
```

Para visualizamos o funcionamento da criptografia, faremos uso do seguinte comando:

- ldapsearch –x –ZZ

Para futuro uso copiaremos os certificados gerados para a pasta /etc/ldap/tls/ do serv2.secure.inf.br.

3.6 Replicação

Como descrito anteriormente existe hoje duas maneiras de fazermos uma replicação utilizando o OpenLDAP , uma é usando o slurpd e outra usando o syncrepl, porém o slurpd foi descontinuado na versão 2.4 do OpenLDAP , além de possuir uma série de limitações. Assim foi definido a utilização do syncrepl.

3.6.1 Configurando o serv1.secure.inf.br (MASTER) – Foi iniciado a configuração do servidor Master alterando o arquivo de configuração /etc/ldap/slapd.conf, alterando o parâmetro modulepath para syncprov e inserindo as seguintes linhas logo abaixo da opção "índex":

```
overlay syncprov
syncprov-checkpoint 100 10
syncprov-sessionlog 100
```

Inserimos também junto a ACL responsável pelos atributos de senha, *userPassword* e *shadowLastChange* a seguinte linha:

```
by dn="cn=replicator,dc=secure,dc=inf,dc=br" read
```

Assim inserimos a permissão para o usuário replicador ler os campos de senha dos usuários, pois sem o acesso a leitura ele não conseguiria efetuar a replicação completa da base. Neste ponto foi reiniciado o servidor com o comando:

- /etc/init.d/slapd restart

3.6.2 Configurando o serv2.secure.inf.br (*SLAVE*) – Iniciamos a configuração do servidor *slave* editando o arquivo de configuração /etc/ldap/slapd.conf e removendo o caracter # antes da linha "rootdn", e logo após inserimos as seguintes linhas abaixo de "index":

```
syncrepl rid=1
        provider=ldap://serv1.secure.inf.br:389
        type=refreshAndPersist
        retry="5 + 5 +"
        interval=00:00:00:10
        searchbase="dc=secure,dc=inf,dc=br"
        filter="(objectClass=*)"
        scope=sub
        attrs="*"
        schemachecking=on
```

```
bindmethod=simple
binddn="cn=replicator,dc=secure,dc=inf,dc=br"
credentials=doctum2009
```

Após os procedimentos acima citamos, inserimos a linha “TLS_CACERT /etc/ldap/tls/cacert.pem” no aquivo /etc/ldap/ldap.conf , paramos o servidor OpenLDAP , removemos os diretórios e novamente iniciamos o servidor, para isso utilizamos as seguintes linhas de comando:

- /etc/init.d/slapd stop
- rm /var/lib/ldap/*
- /etc/init.d/slapd start

Assim temos agora os dois servidores configurados, sendo que os dados do serv1.secure.inf.br estão sendo replicados para o servidor serv2.secure.inf.br, porém o mesmo não tem autoridade sobre os dados fazendo com que para alterarmos qualquer informação na base, teremos que fazer isso no serv1.secure.inf.br e essa atualização será replicada de imediato para o serv2.secure.inf.br.

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.

REFERÊNCIAS BIBLIOGRÁFICAS

BARTH, D. G.; SIEWERT, V. C. **Conceituação de DNS**. Disponível em: <http://artigocientifico.uol.com.br/uploads/artc_1148560980_24.pdf>. Acesso em: jun. 2009.

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

FADEL, D.. **Criptografia RSA.** Disponível em: < http://www.ime.unicamp.br/~ftorres/ENSINO/MONOGRAFIAS/desi_RSA.pdf>. Acesso em: nov. 2009.

GOUVEIA, B.. **LDAP para iniciantes**. Disponível em: <http://www.ldap.org.br/>. Acesso em: jun. 2009.

LOSANO, F.. **Integração de Rede com Diretórios LDAP**. Disponível em: <http://www.revistadolinux.com.br/ed/025/assinantes/rede.php3>. Acesso em: mar. 2009.

NOVELL**. Novell Documentation: Novel Audit 2.0.** Disponível em: <http://www.novell.com/documentation/novellaudit20/index.html?page=/documentation/novellaudit20/novellaudit20/data/b27qg60.html>. Acesso em: abr. 2009.

OPENLDAP FOUNDATION. **OpenLDAP Software 2.4 Administrator's Guide.** Disponível em: <http://www.openldap.org/doc/admin24/>. Acesso em: mai. 2009.

SANTANA, F.. **Instalação do Active Directory**. Disponível em: <http://www.fabianosantana.com.br/windows-2000/287-ad>. Acesso em: mai 2009.

TRIGO, C. H. **OpenLDAP: Uma abordagem integrada.** São Paulo: Novatec Editora, 2007.

TUTTLE, S. EHLENBERGER, A.; GORTHI, R. **Understanding LDAP: Design and Implementation**. Disponível em: <http://www.redbooks.ibm.com/>. Acesso em: abr. 2009.