

**LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RN
ESPECIALIZAÇÃO EM REDES DE COMPUTADORES**

**IMPLANTAÇÃO DE UM SERVIDOR DE ARQUIVOS SAMBA
UTILIZANDO UM SERVIÇO DE DIRETÓRIO LDAP COM BASES REPLICADAS**

JOSÉ MARIA AMORA DA SILVA JÚNIOR

NATAL/RN

2011

JOSÉ MARIA AMORA DA SILVA JÚNIOR

**IMPLANTAÇÃO DE UM SERVIDOR DE ARQUIVOS SAMBA
UTILIZANDO UM SERVIÇO DE DIRETÓRIO LDAP COM BASES REPLICADAS**

**Monografia apresentada ao curso de
Especialização em Redes de
Computadores da Faculdade
Natalense para o Desenvolvimento do
Rio Grande do Norte como requisito
parcial para a obtenção do título de
Especialista em Redes de
Computadores.**

**Orientador:
Aluizio Ferreira da Rocha Neto**

NATAL/RN

2011

Silva Junior, José Maria Amora da
Implementação de um servidor de arquivos samba
utilizando um serviço de diretório LDAP com bases replicadas. / José Maria
Amora da Silva Junior – Natal: FARN, 2011.
35 f.

Orientador: Aluizio Ferreira da Rocha Neto (Msc.)
Monografia (Especialização em Redes de Computadores) –
Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte.

1. Programas de Computadores – Monografia. 2. Servidor de arquivo
LDAP – Monografia. 3. Diretório LDAP – Monografia. I. Título.

**LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RN
ESPECIALIZAÇÃO EM REDES DE COMPUTADORES**

JOSÉ MARIA AMORA DA SILVA JÚNIOR

**IMPLANTAÇÃO DE UM SERVIDOR DE ARQUIVOS SAMBA
UTILIZANDO UM SERVIÇO DE DIRETÓRIO LDAP COM BASES REPLICADAS**

Monografia apresentada e aprovada em ____ de _____ de ____, pela banca examinadora
composta pelos seguintes membros

Aluizio Ferreira da Rocha Neto, M.Sc.
Orientador

Membro examinador

Membro examinador

Natal/RN, ____ de _____ de ____.

Sumário

1 INTRODUÇÃO	10
1.1 MINISTÉRIO PÚBLICO DO TRABALHO	11
1.2 PROBLEMA DE PESQUISA	11
1.3 OBJETIVOS.....	11
1.4 JUSTIFICATIVA	12
2 REFERENCIAL TEÓRICO	13
2.1 SOFTWARE LIVRE	13
2.2 SAMBA	13
2.2.1 Arquivo de configuração do samba.....	15
2.3 OPENLDAP	16
2.4 SMBLDAP-TOOLS	17
2.5 REPLICAÇÃO DE BASE LDAP	18
2.5.1 Replicação Master x Slave	19
2.5.2 Replicação Master x Master (multimaster)	19
2.5.3 Diretórios Distribuídos	19
3 DESENVOLVIMENTO DA SOLUÇÃO	20
3.1 AJUSTES NO SERVIDOR PDC SAMBA.....	21
3.2 AJUSTES NOS ARQUIVOS DO SMBLDAP-TOOLS.....	24
3.2.1 Arquivo smbldap.conf	24
3.2.2 Arquivo smbldap_bind.conf.....	25
3.3 AJUSTES NO SERVIDOR LDAP DO PDC	26
3.3.1 Arquivo slapd.conf	26
3.3.2 Arquivo ldap.conf.....	27
3.4 AJUSTES NO SERVIDOR BDC SAMBA	29
3.4.1 Ajustes no aplicativo smbldap-tools do BDC.....	30
3.4.2 Ajustes no servidor LDAP do BDC	30
3.5 SERVIÇO DE REPLICAÇÃO DE DIRETÓRIOS	30
3.6 SINCRONIZAÇÃO DOS SERVIDORES PDC E BDC	33
4 CONCLUSÕES E RECOMENDAÇÕES.....	34
5 REFERÊNCIAS BIBLIOGRÁFICAS	35

LISTA DE FIGURAS

Figura 1.1: Parque de informática da PRT 21ª Região.....	9
Figura 3.1: Pacotes necessários.....	15
Figura 3.2: Parâmetros dos servidores.....	16
Figura 3.3: Parâmetros principais do arquivo smb.conf do servidor PIPA.....	18
Figura 3.4: Exemplo de compartilhamento criado no servidor PIPA.....	18
Figura 3.5: Script de logon para o grupo Informatica.....	19
Figura 3.6: Parâmetros principais para integração Samba e LDAP.....	22
Figura 3.7: Parâmetros do arquivo ldap.conf.....	23
Figura 3.8: Arquivo nsswitch.conf.....	23
Figura 3.9: Saída comando id.....	23
Figura 3.10: Dados do arquivo de log do LDAP.....	24
Figura 3.11: Parâmetros do smb.conf do BDC PONTANEGRA.....	25
Figura 3.12: Alteração no servidor BDC PONTANEGRA.....	25
Figura 3.13: Parâmetros do servidor Master PIPA que habilitam a replicação da base LDAP.....	26
Figura 3.14: Parâmetros do servidor Master PONTANEGRA que habilitam a replicação da base LDAP.....	27
Figura 3.15: Instrução do cron.....	28
Figura 3.16: Script de backup.....	28

LISTA DE ABREVIATURAS, SIGLAS E SÍMBOLOS

CIFS	Common Internet File System
FTP	File Transfer Protocol
GPL	General Public License
LDAP	Lightweight Directory Access Protocol
NetBEUI	NetBIOS Extended User Interface
NetBIOS	Network Basic Input/Output System
SMB	Server Message Block
SSH	Secure Shell
WINS	Windows Internet Name Service

RESUMO

Este trabalho apresenta uma proposição para utilização de ferramentas de código aberto com o objetivo de criar um ambiente centralizado de autenticação de usuários em uma rede heterogênea de computadores. Baseia-se em um caso real da Procuradoria Regional do Trabalho – 21ª Região, localizada em Natal, capital do Estado do Rio Grande do Norte, onde vários servidores Samba/LDAP atuam como PDC de redes distintas. São discutidos os detalhes de implementação dos serviços de autenticação de usuário em base LDAP, replicação de diretório e gerenciamento de arquivos para máquinas Windows e Linux.

Palavras-chaves: LDAP, Samba, Linux, Windows, Replicação de Diretórios

ABSTRACT

This paper presents a proposition for use of open source tools with the goal of creating a centralized environment authentication of users in a heterogeneous network of computers. It is based on a real case of the Procuradoria Regional do Trabalho - 21 Região, located in Natal, capital of Rio Grande do Norte, where multiple servers Samba / LDAP to act as PDC in separate networks. We discuss the implementation details of services for user authentication based on LDAP, replication of directory and file management for Windows and Linux machines.

Keywords: LDAP, Samba, Linux, Windows, Replication of directory

1 INTRODUÇÃO

A Procuradoria Regional do Trabalho – 21ª Região é uma instituição recente, criada em 23 de abril de 1992. Da sua criação até hoje teve um aumento considerável no número de computadores conectados à rede institucional, o que gerou uma maior complexidade na administração dos usuários e serviços disponíveis. Na figura 1.1 pode-se ter uma noção da complexidade deste parque de informática, que é formado, além da sede, por duas unidades descentralizadas, uma no município de Mossoró e outra em Caicó. Ambas tem redes distintas, porém todos os usuários, tanto da sede como nas filiais, possuem uma única identificação.

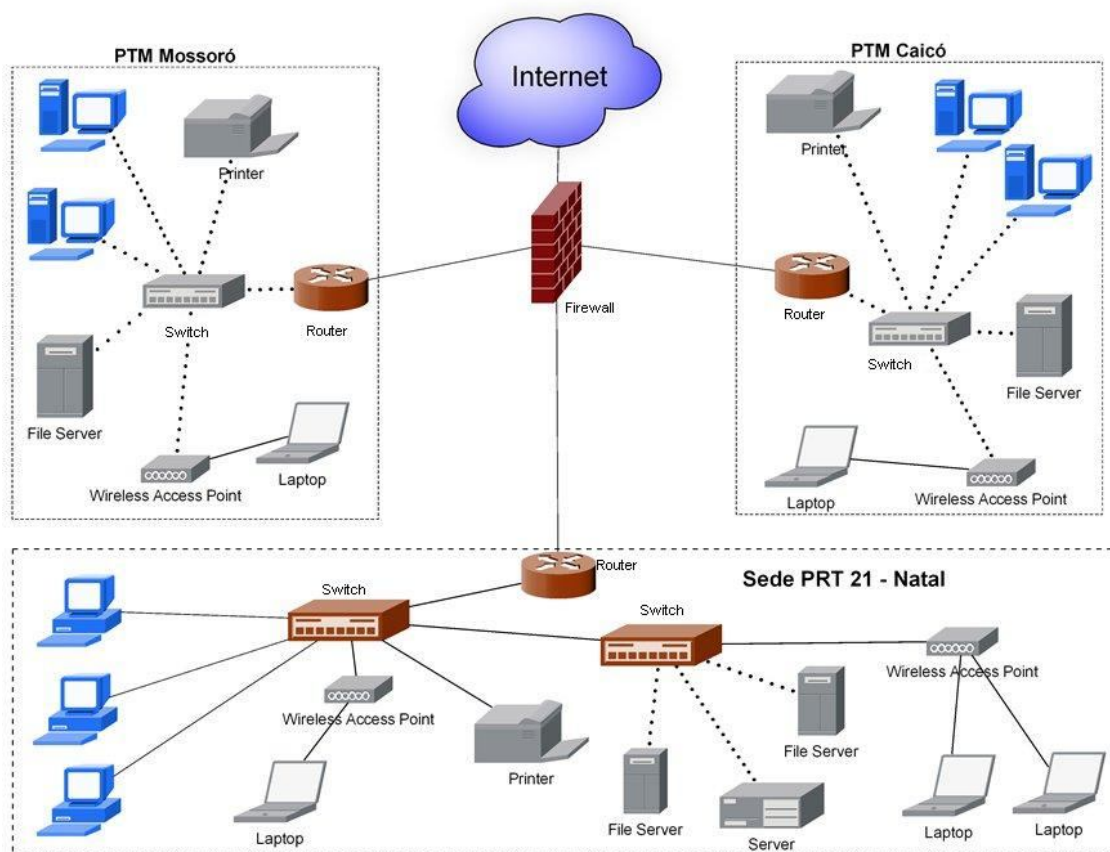


Figura 1.1: Parque de informática da PRT 21ª Região

Soma-se ao já exposto o fato de o Ministério Público do Trabalho ter adotado novas políticas de informática, ficando proibidas as aquisições de aplicativos de código fechado, exceto se não houver outra alternativa.

Com o intuito de solucionar esses problemas decidiu-se implementar no nosso

ambiente de trabalho um sistema centralizado de autenticação de usuários, juntamente com o serviço de gerenciamento e compartilhamento de arquivos, utilizando ferramentas de código aberto.

1.1 MINISTÉRIO PÚBLICO DO TRABALHO

O Ministério Público é uma instituição permanente, essencial à função jurisdicional do Estado, sendo responsável pela defesa da ordem jurídica, do regime democrático e dos interesses sociais e individuais indisponíveis.

Possui independência e autonomia, com orçamento, carreira e administração próprios. Aparece na Constituição Federal no capítulo das funções essenciais à Justiça, sem vinculação funcional com quaisquer dos Poderes do Estado.

Possui como princípios institucionais a unidade, a indivisibilidade e a independência funcional.

Compõe, juntamente com o Ministério Público Federal, Ministério Público Militar e o Ministério Público do Distrito Federal e Territórios, o Ministério Público da União.

É composto pela Procuradoria-Geral, com sede em Brasília/DF, 24 Procuradorias Regionais instaladas nas capitais dos Estados e 100 Procuradorias do Trabalho nos Municípios instalados em cidades do interior.

1.2 PROBLEMA DE PESQUISA

O problema de pesquisa abordado por este trabalho consiste em mostrar a implementação de um ambiente centralizado de autenticação de usuários utilizando o protocolo LDAP, através do software livre OpenLDAP, juntamente com o sistema de gerenciamento e compartilhamento de arquivos – SAMBA –, e o sistema operacional CentOS/Linux para substituir o Windows NT 4.0, este ainda utilizado em nossa instituição.

Far-se-á também uma replicação da base de dados do OpenLDAP, para caso de falha no sistema principal.

1.3 OBJETIVOS

Com este trabalho pretende-se mostrar como utilizar programas de código aberto para gerenciar uma rede de computadores, substituindo, assim, aplicações fechadas e que possuem um custo muito alto de aquisição e manutenção. Para isso será implementado um ambiente de

testes com servidores Linux/CentOS, os quais serão responsáveis por autenticar os usuários da rede e prover serviços de gerenciamento e compartilhamento de arquivos para clientes Windows e Linux.

1.4 JUSTIFICATIVA

O que motivou a realização deste trabalho foi a necessidade de esta Procuradoria ter uma rede de computadores configurada com novas tecnologias e que atendesse às suas necessidades operacionais. Sabe-se que a redução de custos é um fator preponderante para o serviço público, motivo pelo qual optou por utilizar ferramentas sem custo de aquisição e/ou manutenção, mantendo um alto grau de satisfação por parte dos usuários.

O presente trabalho tem também como objetivo servir como uma base de consulta para os administradores de rede da instituição acima mencionada, que pretendam adotar nossa estratégia em seus ambientes de trabalho.

2 REFERENCIAL TEÓRICO

2.1 SOFTWARE LIVRE

Software Livre, ou Free Software, conforme a definição de software livre criada pela *Free Software Foundation*¹, é o software que pode ser usado, copiado, estudado, modificado e redistribuído sem restrição. A forma usual de um software ser distribuído livremente é sendo acompanhado por uma licença de software livre (como a GPL ou a BSD), e com a disponibilização do seu código-fonte.

Software Livre se refere à existência simultânea de **quatro tipos de liberdade** para os usuários do software, definidas pela Free Software Foundation.

As 4 liberdades básicas associadas ao software livre são:

- A liberdade de executar o programa, para qualquer propósito (liberdade nº 0).
- A liberdade de estudar como o programa funciona, e adaptá-lo para as suas necessidades (liberdade nº 1).
- A liberdade de redistribuir cópias de modo que você possa ajudar ao seu próximo (liberdade nº 2).
- A liberdade de aperfeiçoar o programa, e liberar os seus aperfeiçoamentos, de modo que toda a comunidade se beneficie (liberdade nº 3).

Para que essas liberdades sejam reais, elas tem de ser irrevogáveis desde que não se faça nada errado; caso o desenvolvedor do software tenha o poder de revogar a licença, mesmo que o usuário não tenha dado motivo, o software não é livre.

2.2 SAMBA

O SAMBA é um servidor e conjunto de ferramentas com a função de permitir que máquinas Linux e Windows se comuniquem entre si, compartilhando serviços (arquivos, diretório, impressão) através do protocolo SMB (Server Message Block)/CIFS (Common Internet File System), equivalentes a implementação NetBEUI no Windows. O SAMBA é uma das soluções em ambiente UNIX capaz de interligar redes heterogêneas.

Com o SAMBA, é possível construir domínios completos, fazer controle de acesso a

¹ A **Free Software Foundation (FSF, Fundação para o Software Livre)** é uma organização sem fins lucrativos, fundada em 1985 por Richard Stallman e que se dedica à eliminação de restrições sobre a cópia, redistribuição, estudo e modificação de programas de computadores – bandeiras do movimento do software livre, em essência.

nível de usuário, compartilhamento, montar um servidor WINS, servidor de domínio, impressão, etc. Na maioria dos casos o controle de acesso e exibição de diretórios no samba é mais minucioso e personalizável que no próprio Windows.

Segue abaixo algumas funcionalidades importantes de aplicações do samba e seu conjunto de ferramentas:

- Montar um servidor de compartilhamento de impressão no Linux que receberá a impressão de outras máquinas Windows da rede.
- Compartilhamento de arquivos entre máquinas Windows e Linux ou de máquinas Linux (sendo o servidor SAMBA) com outro Sistema Operacional que tenha um cliente NetBEUI (Macintosh, OS/2, LanManager, etc).
- Controle de acesso aos recursos compartilhados no servidor através de diversos métodos (compartilhamento, usuário, domínio, servidor).
- Controle de acesso leitura/gravação por compartilhamento.
- Controle de acesso de leitura/gravação por usuário autenticado.
- Possibilidade de definir contas de "Convidados", que podem se conectar sem fornecer senha.
- Possibilidade de uso do banco de dados de senha do sistema (/etc/passwd), autenticação usando o arquivo de dados criptografados do samba, LDAP, PAM, etc.
- Controle de cache e opções de tuning por compartilhamento.
- Permite ocultar o conteúdo de determinados diretórios que não quer que sejam exibidos ao usuário de forma fácil.
- Possui configuração bastante flexível com relação ao mapeamento de nomes DOS => UNIX e vice versa, página de código, acentuação, etc.
- Permite o uso de aliases na rede para identificar uma máquina com outro nome e simular uma rede NetBIOS virtual.
- O samba possibilita ajuste fino nas configurações de transmissão e recepção dos pacotes TCP/IP, como forma de garantir a melhor performance possível de acordo com suas instalações.

- Permite o uso do gerenciador de mensagem do Linux (Linpopup) para a troca de mensagens com estações Windows via NetBios. Com a flexibilidade do samba é possível até redirecionar a mensagem recebida via e-mail ou pager.
- Possui suporte completo a servidor WINS (também chamado de *NBNS - NetBios Name Service*) de rede. A configuração é bastante fácil.
- Faz auditoria tanto dos acessos a pesquisa de nomes na rede como acesso a compartilhamentos. Entre os detalhes salvos estão a data de acesso, IP de origem, etc.
- Suporte completo a controlador de domínio Windows (PDC).
- Suporte quase completo a backup do controlador de domínio (BDC). Até a versão 2.2 do samba, o suporte a BDC é parcial. Este código provavelmente estará estável até a versão 3.0.
- Permite montar unidades mapeadas de sistemas Windows ou outros servidores Linux como um diretório no Linux.
- Permite a configuração de recursos simples através de programas de configuração gráficos, tanto via sistema, como via web.
- Permite executar comandos no acesso ao compartilhamento ou quando o acesso ao compartilhamento é finalizado.
- Com um pouco de conhecimento e habilidade de administração de sistemas Linux, é possível criar ambientes de auditoria e monitoração até monitoração de acesso a compartilhamento em tempo real.
- Entre outras possibilidades.

2.2.1 Arquivo de configuração do samba

Toda a configuração relacionada com nomes, grupo de trabalho, tipo de servidor, log, compartilhamento de arquivos e impressão do samba é colocada no arquivo de configuração `/etc/samba/smb.conf`. Este arquivo é dividido em seções e parâmetros.

Uma seção no arquivo de configuração do samba (`smb.conf`) é definido por um nome entre "[]". As seções têm o objetivo de organizar os parâmetros pra que tenham efeito

somente em algumas configurações de compartilhamento do servidor (exceto os da seção [global] que não especificam compartilhamentos, mas suas diretivas podem ser válidas para todas os compartilhamentos do arquivo de configuração). Alguns nomes de seções foram reservados para configurações específicas do samba, eles são os seguintes:

[global]

Define configurações que afetam o servidor samba como um todo, fazendo efeito em todos os compartilhamentos existentes na máquina. Por exemplo, o grupo de trabalho, nome do servidor, página de código, restrições de acesso por nome, etc.

[homes]

Especifica opções de acesso a diretórios homes de usuários. O diretório *home* é disponibilizado somente para seu dono, após se autenticar no sistema.

[printers]

Define opções gerais para controle das impressoras do sistema. Este compartilhamento mapeia os nomes de todas as impressoras encontradas no `/etc/printcap`. Configurações especiais podem ser feitas separadamente.

[profile]

Define um perfil quando o servidor samba é usado como PDC de domínio.

Qualquer outro nome de [seção] no arquivo `smb.conf` que não sejam as acima, são tratadas como um compartilhamento ou impressora.

O servidor Samba é um software poderoso e bastante eficiente. Alguns especialistas no assunto até o consideram mais seguro e confiável que as soluções baseadas no Windows. Sua compreensão não é difícil, mas requer um certo tempo de aprendizado, pois sua configuração é bastante abrangente para atender os mais diversos tipos de necessidade.

2.3 OPENLDAP

O OpenLDAP é um *software* livre que implementa o protocolo LDAP². Ele é um *serviço de diretório*³ baseado no padrão X.500⁴.

O OpenLDAP é independente de sistema operacional. Funcionando tanto em Linux como também BSD, AIX, HP-UX, Mac OS X, Solaris, Microsoft Windows (2000, XP, 2003,

² *Lightweight Directory Access Protocol*, ou *LDAP*, é um protocolo para atualizar e pesquisar diretórios rodando sobre TCP/IP.

³ Um *serviço de diretório* é um serviço que armazena e organiza informações sobre os recursos e os utilizadores de uma rede de computadores, e que permite os administradores de rede gerenciar o acesso de utilizador e sistemas a esses recursos. Além disso, os serviços de diretório atuam como uma camada de abstração entre os utilizador e esses recursos. Em geral esta tecnologia é usada no modelo cliente-servidor, no qual um servidor oferece serviços a um cliente.

⁴ X.500 é uma série de padrões para redes de computador abordando serviço de diretório.

2008 e Vista) e z/OS.

O OpenLDAP foi desenvolvido inicialmente pela Universidade de Michigan com as seguintes características principais:

- suporte a IPv4 e IPv6;
- autenticação (Cyrus Sasl-Kerberos V, GSSAPI, Digest-MD5);
- segurança no transporte – SSL e TLS;
- controle de acessos;
- escolha entre banco de dados;
- capacidade de atender a múltiplos bancos de dados simultaneamente;
- alta performance em múltiplas chamadas;
- replicação de base.

O OpenLDAP armazena as informações de modo semelhante a uma árvore (ou DNS), como raízes, troncos, galhos e folhas. Cada item armazenado pertence ao contexto (galho, folha, tronco) onde foi criado e é tratado como um objeto, podendo ter diferentes propriedades, atributos, diretivas, finalidades e valores.

O OpenLDAP possui basicamente 2 arquivos de configuração, que são, respectivamente:

- slapd.conf - configuração do *daemon*;
- ldap.conf - configuração para acesso dos clientes à base.

2.4 SMBLDAP-TOOLS

Smbldap-tools é um conjunto de scripts escritos em linguagem Perl que integram o servidor de domínio Samba com o serviço de diretório OpenLDAP. Esses scripts estão disponíveis nos repositórios da maioria das distribuições GNU/Linux.

As ferramentas Smbldap-tools visam tanto aos usuários comuns quanto aos administradores de sistemas GNU/Linux e utilizam dois arquivos de configuração que devem estar configurados de acordo com o ambiente: smbldap.conf e smbldap_bind.conf.

No arquivo smbldap.conf são definidos os parâmetros globais a serem utilizados pelos scripts do Smbldap-tools que manipulam objetos da base do diretório LDAP. Dentre as principais informações definidas nesse arquivo destacam-se o SID do domínio, o sufixo do diretório LDAP, representado pelo parâmetro suffix, e o nome do domínio Samba. Esses três parâmetros definem as informações primordiais para a integração de um determinado domínio

Samba com um diretório LDAP, correspondente e adequado para abrigar os objetos que integram o ambiente: usuários, grupos e computadores.

O arquivo `smbldap_bind.conf` abriga as credenciais de acesso do usuário com permissão de modificar o conteúdo do diretório LDAP. Em virtude disso, deve ter permissão de acesso apenas ao usuário *root* do sistema, pois a senha encontrasse em formato de texto puro e não criptografado.

É condição fundamental para o uso do Smbldap-tools que os servidores Samba e OpenLDAP estejam configurados através dos arquivos `smb.conf` e `slapd.conf`, respectivamente, de forma coerente com todo o ambiente.

2.5 REPLICAÇÃO DE BASE LDAP

Replicação é a manutenção de uma cópia, seja parcial ou total, dos dados em outros servidores.

A replicação da base de dados LDAP se torna um fator preponderante quando trabalhasse em um ambiente corporativo, devido a vários fatores, entre eles:

- Economia de banda;
- Distribuição de carga;
- Garantia de serviço;
- Alta disponibilidade;
- Backup.

No OpenLDAP existem duas técnicas distintas de replicação: 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 a replicação parcial de uma base e a Utilização de mais de um servidor Master.

Quando se trabalha 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, encarregado de replicar as alterações para seus servidores slaves.

2.5.1 Replicação Master x Slave

Nesse método de replicação temos um único servidor Master o qual tem seu conteúdo replicado em todos os seus servidores slaves. 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.

2.5.2 Replicação Master x Master (multimaster)

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.

2.5.3 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 uma sede e várias filiais, 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.

Com o crescimento da utilização do OpenLDAP, temos que ter a segurança que o serviço nunca pare, pois outros serviços da rede dependem dele.

A replicação da base LDAP é uma ótima escolha para se distribuir as bases em diversos servidores e garantir o funcionamento do OpenLDAP em casos de falha.

3 DESENVOLVIMENTO DA SOLUÇÃO

Para desenvolvimento do trabalho fez-se a instalação de dois servidores Linux/CentOS (*release 5.5*), sendo um configurado como servidor PDC⁵ da nossa rede de testes e outro como BDC⁶, servindo como uma máquina de backup. Nas duas máquinas foram instalados o Samba versão 3.3.8 e o OpenLDAP 2.4. Configurou-se, também, o aplicativo Rsync⁷ para sincronizar os dados entre os dois servidores. Com isso haverá um ambiente seguro, onde caso haja falha no servidor Primário, o servidor Secundário assume sem prejuízo para os usuários.

Neste trabalho não é mostrado o processo de instalação de um servidor Linux, nem dos aplicativos envolvidos: Samba, OpenLDAP, smbldap-tools e Webmin⁸. Será levado em consideração o fato de os servidores já estarem com todos os aplicativos instalados e funcionando.

Os pacotes utilizados no ambiente proposto foram os vistos na Figura 3.1.

Serviço	Pacote
Samba	Samba3x-client.i386
	Samba3x.i386
	Samba3x-doc.i386
	Samba3x-common.i386
	Samba3x-domainjoin-gui.i386
	Samba3x-winbind.i386
OpenLDAP	Openldap2.4.i386
	Openldap2.4-clients.i386
	Openldap2.4-debuginfo.i386
	Openldap2.4-extra-schemas.noarch
	Openldap2.4-servers.i386
SmbLDAP-tools	Smbldap-tools-0.9.5-1.noarch.rpm
Webmin	Webmin-1.510-1.noarch.rpm

Figura 3.1: Pacotes necessários

Lembrando que o suporte ao Windows 7 por um controlador de domínio Samba foi

⁵ PDC – Primary Domain Controller

⁶ BDC – Backup Domain Controller

⁷ Rsync, como o nome sugere, é um programa que sincroniza remotamente os dados entre duas máquinas. Por ser baseado no antigo rcp (remote copy), o software herdou as propriedades de criptografia do protocolo SSH, o que torna sua transmissão de dados mais segura que o FTP. Além das propriedades de segurança, o rsync utiliza o protocolo remote-update, o que aumenta assustadoramente sua velocidade e diminui a quantidade de dados transferidos, pois são trocados entre os servidores somente as diferenças entre dois grupos de arquivos.

⁸ Utilitário responsável por gerenciar os serviços instalados no servidor Linux.

incluído a partir da versão 3.3.12 do Samba, portanto, recomenda-se utilizar sempre as versões mais novas e estáveis dos pacotes.

Os servidores serão configurados com os seguintes parâmetros, vistos na Figura 3.2.

Serviço	Servidor PDC	Servidor BDC
End. IP Local	10.21.0.5/19	10.21.0.11/19
Nome do host	pipa.prt21.mpt.gov.br	pontanegra.prt21.mpt.gov.br
Nome NetBIOS	pipa	pontanegra
Domínio Samba	prt21	prt21
Sufixo base LDAP	dc=prt21,dc=lan	dc=prt21,dc=lan

Figura 3.2: Parâmetros dos servidores

3.1 AJUSTES NO SERVIDOR PDC SAMBA

Esta seção apresenta as configurações necessárias para que o servidor PIPA atue como PDC da nossa rede.

Serão necessárias fazer algumas alterações no arquivo de configurações globais do samba (/etc/samba/smb.conf) para que o servidor funcione como um Controlador de Domínio Primário. Na Figura 3.3, os parâmetros necessários para que o Samba assuma tais funções.

```
##### Arquivo smb.conf #####
[global]

# Configurar como Controlador de Dominio Primário (PDC)

# Nome de domínio do servidor Samba
workgroup = PRT21

#Define o nome ou a descrição que aparecerá ao lado do nome do servidor na
#visualização da lista de compartilhamentos no ambiente de rede. (%L é o nome
#NetBIOS do servidor Samba).
server string = Servidor PDC %L

#Define o nome NetBIOS pelo qual o servidor Samba será conhecido na rede.
netbios name = pipa

#Define a política de acesso, autenticação e segurança mediante senhas. Pode
#assumir os seguintes valores: share, user, server e domain. No nosso caso
#(security=user) os usuários terão contas Unix e respectivas senhas.
security = user

#Define um caminho relativo [netlogin] para o recurso compartilhado de um
#script DOS(.bat) a ser executado para o cliente no momento de acesso. (%G
#corresponde ao grupo do usuário e %U é o nome de usuário.
```

```

logon script = %G.bat %U.bat

#Unidade onde será mapeado o diretório /HOME do usuário.
logon drive = H:

#Permite clientes Windows acessarem um domínio como se fossem um domínio
#Windows.
domain logons = Yes

#Define a candidatura do servidor na eleição de um servidor de lista de recursos
#principal (master browser). Utilizado com as opções domain master ou local
#master para determinar se o Samba tornará um master browser na rede local.
#Deve ser definido um valor mais alto que o de um sistema operacional
#competidor se quiser que o Samba vença a eleição.
os level = 99

#Escolha o Samba para tornar-se o servidor de lista de recursos principal.
preferred master = Yes

#Especifica se o Samba deve se tornar um receptor de lista de recursos disponíveis
#principal do domínio e se possível para todo o grupo ou domínio.
domain master = Yes

#Especifica que o Samba deve tentar tornar-se o servidor de lista de recursos
#local principal (local master browser) na sub-rede durante a inicialização.
local master = Yes

#Ativa o serviço Wins9
wins support = Yes

# Configuração LDAP
#Informa que a base de autenticação dos usuários é o LDAP e mostra em qual
#servidor esta base está localizada. No nosso caso, no mesmo servidor PDC.
passdb backend = ldapsam:ldap://127.0.0.1

#Scripts responsáveis por administrar os usuários, grupos e máquinas da base
#LDAP.
add user script = /usr/sbin/smbldap-useradd -m "%u"
delete user script = /usr/sbin/smbldap-userdel "%u"
add group script = /usr/sbin/smbldap-groupadd -p "%g"
delete group script = /usr/sbin/smbldap-groupdel "%g"
add user to group script = /usr/sbin/smbldap-groupmod -m "%u" "%g"
delete user from group script = /usr/sbin/smbldap-groupmod -x "%u" "%g"
set primary group script = /usr/sbin/smbldap-usermod -g "%g" "%u"
add machine script = /usr/sbin/smbldap-useradd -w "%u"

#Configurações para integração com o OpenLDAP. Aqui utilizaremos os mesmos

```

⁹ Windows Internet Name Service (WINS) ou NetBIOS Name Service (NBNS) é um serviço do protocolo TCP/IP, muito semelhante ao DNS server. O WINS fornece endereços TCP/IP em função de nomes NetBIOS e garante a manutenção e a replicação da base de dados de nomes existentes na rede.

```
#valores definidos para a nossa base LDAP.
ldap suffix = dc=prt21,dc=lan
ldap machine suffix = ou=Computers
ldap user suffix = ou=Users
ldap group suffix = ou=Groups
ldap idmap suffix = ou=Idmap
ldap admin dn = cn=admin,dc=prt21,dc=lan
ldap ssl = No

#Mapeamento de identidade (idMap) de identificadores de segurança do Windows
#(SIDs) para UNIX UIDs e GIDs.
idmap backend = ldap:ldap://127.0.0.1
idmap uid = 10000-20000
idmap gid = 10000-20000
idmap cache time = 900

#Sincronizar a base LDAP com o arquivo de senhas passwd do Linux.
ldap passwd sync = Yes
```

Figura 3.3: Parâmetros principais do arquivo smb.conf do servidor PIPA.

Com esses parâmetros globais definidos, o servidor PIPA foi preparado para controlar o domínio PRT21 localmente, realizando a autenticação e autorização dos clientes no segmento de rede.

Além desses parâmetros pode-se incluir outros, cuja finalidade é fazer com que nosso servidor PIPA crie compartilhamentos de arquivos na rede, bem como parâmetros para criação de lixeira e auditoria, assuntos esses que fogem ao escopo deste trabalho.

Com relação aos compartilhamentos vale ressaltar que todos eles possuem a diretiva *valid users* habilitada. Ela é responsável por delimitar o acesso aos dados apenas para os usuários e grupos autorizados.

Os usuários e grupos são definidos na base LDAP.

Um exemplo de compartilhamento com a diretiva *valid users* habilitada está mostrado na figura 3.4.

```
[Pericia]
comment = Pasta Pericia
path = /dados/setores/pericia
browseable = yes
writeable = yes
create mask = 0666
directory mask = 2777
valid users = @"PRT21\diretores" @"PRT21\pericia"
```

```
public = no
vfs objects = recycle full_audit
veto files = /*.exe/*.*pif/*.*bat/*.*mp3/*.*avi/*.*vob/*.*iso/*.*mpeg/*.*wav/*.*mpg
```

Figura 3.4: Exemplo de compartilhamento criado no servidor PIPA.

Há dois compartilhamentos especiais que vale a pena tecermos um comentário. São eles o *homes* e *netlogon*.

O primeiro refere-se ao diretório particular do usuário na rede. É o diretório definido no *logon drive*, na seção [global] do *smb.conf*.

E o segundo é o responsável por executar os *scripts* DOS (.bat) no momento em que o usuário conecta no servidor. Definimos na nossa rede os scripts baseados nos usuários (%U) e grupos (%G) do LDAP. Abaixo temos um exemplo de script definido para o grupo Informática.

```
##### Arquivo informatica.bat #####
@echo off
echo mudar unidade
c:
echo Desconectar todos os mapeamentos
net use * /del /yes
echo Mapeando home
net use h: /home
echo Mapeando Sistemas
net use s: \\pipa\sistemas /yes
echo Mapeando Informatica
net use i: \\pipa\informatica /yes
```

Figura 3.5: Script de logon para o grupo Informática.

3.2 AJUSTES NOS ARQUIVOS DO SMBLDAP-TOOLS

Para configuração do servidor de domínio PIPA, faz-se necessário realizar ajustes nos arquivos *smbldap.conf* e *smbldap_bind.conf*, gravados no diretório */etc/smbldap-tools*, nos quais está baseado o uso destas ferramentas.

3.2.1 Arquivo smbldap.conf

Os parâmetros principais desse arquivo que precisam ser alterados são:

- **SID (Secure Identifier Domain):** você pode obter o SID para seu domínio usando o comando `net getlocalsid`. O Samba deve estar rodando para isto funcionar (pode demorar vários minutos para um servidor Samba corretamente negociar seu status com outros servidores da rede).

SID: S-1-5-21-240481417-1895177459-1423778804

- **SambaDomain:** Nome do domínio do servidor Samba.

SambaDomain: PRT21

- **Suffix LDAP:** O nome distinto da base de pesquisas.

suffix="dc=prt21,dc=lan"

- **UsersDN :** ramo em que as contas dos usuários podem ser encontradas ou devem ser adicionadas

usersdn="ou=Users,\${suffix}"

- **ComputersDN :** ramo em que as contas de computadores podem ser encontradas ou devem ser adicionadas.

computersdn="ou=Computers,\${suffix}"

- **GroupsDN :** ramo em que as contas de grupos podem ser encontradas ou devem ser adicionadas.

groupsdn="ou=Groups,\${suffix}"

- **idmapDN :** onde são armazenadas entradas Idmap (usadas se o samba é um servidor membro do domínio).

idmapdn="ou=Idmap,\${suffix}"

- **sambaUnixIdPool:** objeto em que os próximos uidNumber e gidNumber disponíveis são armazenados.

sambaUnixIdPool="sambaDomainName=PRT21,\${suffix}"

- **mailDomain :** Domínio anexado ao atributo "mail" dos usuários.

mailDomain="prt21.mpt.gov.br"

3.2.2 Arquivo smbldap_bind.conf

Este arquivo é apenas usado pelo `root` para modificar o conteúdo do diretório. Ele contém nomes distintos (DN=*distinguished names*) e credenciais para conectar para ambos os

diretórios mestre e escravo. Abaixo, os principais parâmetros que precisam ser alterados.

- slaveDN : nome distinto usado para acessar ao servidor escravo.
`slaveDN="cn=admin,dc=prt21,dc=lan"`
- slavePw : as credenciais usadas para acessar ao servidor escravo.
`slavePw="chave"`
- masterDN : o nome distinto usado para acessar o servidor mestre.
`masterDN="cn=admin,dc=prt21,dc=lan"`
- masterPw : as credenciais para acessar ao servidor mestre.
`masterPw="chave"`

Observação: a senha deve ser armazenada aqui em texto puro. Este arquivo deve então ser legível apenas pelo *root*!

3.3 AJUSTES NO SERVIDOR LDAP DO PDC

Esta seção detalha as configurações necessárias feitas na base LDAP do servidor PDC. Utilizar-se-á para isso os dois arquivos de configuração do LDAP, já mencionados anteriormente na seção 2.3.

3.3.1 Arquivo *slapd.conf*

Este arquivo é responsável pelas configurações do serviço de diretório OpenLDAP. A seguir, os principais parâmetros habilitados no arquivo *slapd.conf* do nosso servidor PDC para que haja uma integração entre o Samba e o LDAP. Nesse arquivo as linhas começadas com o caracter # são apenas comentários.

```
##### /etc/openldap2.4/slapd.conf #####
# Schema para habilitar o samba no ldap
include /etc/openldap2.4/schema/samba.schema

#Nessa linha estamos permitindo que clientes LDAP conectem ao nosso
#diretório utilizando a versão 2 do protocolo. Atualmente a suíte
#OpenLDAP utiliza a versão 3, mas mantém o suporte à versão 2 pois
#muitos aplicativos, principalmente clientes de e-mail, ainda a utilizam.
allow bind_v2
```

```

#A base do diretório LDAP
suffix      "dc=prt21,dc=lan"

# Administrador do domínio e senha para o mesmo.
rootdn      "cn=admin,dc=prt21,dc=lan"
rootpw      "chave"

# Índices para otimizar as operações de busca. Existem quatro tipos de
#índices (approx,eq,pres,sub), e o suporte de um tipo de índice por parte de
#um atributo é determinado pelo arquivo de schema ao qual o atributo
#pertence .
index objectClass      eq
index cn                pres,sub,eq
index sn                pres,sub,eq
index uid               pres,sub,eq
index displayName      pres,sub,eq
index uidNumber         eq
index gidNumber         eq
index memberUID         eq
index sambaSID          eq
index sambaPrimaryGroupSID eq
index sambaDomainName   eq
index sambaGroupType    eq
index sambaSIDList              eq
index UniqueMember        eq
index default              sub
index entryCSN,entryUUID    eq

```

Figura 3.6: Parâmetros principais para integração Samba e LDAP

3.3.2 Arquivo `ldap.conf`

Neste arquivo serão indicadas as configurações gerais para os clientes LDAP.

```
##### /etc/openldap2.4/ldap.conf #####
# Endereço do servidor. No nosso caso é local.
host 127.0.0.1

# Base do LDAP
base dc=prt,dc=lan

# Usuário e senha padrão para as pesquisas
binddn cn=admin,dc=prt21,dc=lan
bindpw chave
```

Figura 3.7: Parâmetros do arquivo ldap.conf

Com isso termina-se as configurações necessárias para a integração entre o Samba e o OpenLDAP.

O próximo passo é informar ao sistema que use a base LDAP para pesquisa aos usuários. Isso é feito alterando o arquivo `/etc/nsswitch.conf` para que ele fique da seguinte forma.

```
##### /etc/nsswitch.conf #####
passwd:    files  ldap
shadow:    files  ldap
group:     files  ldap
```

Figura 3.8: Arquivo nsswitch.conf

Para testar se a configuração do servidor PDC com Samba e OpenLDAP está funcionando, e se está sendo feita consulta a base LDAP, pode-se utilizar o comando `id <usuário>`¹⁰ do Linux.

Id edson, por exemplo, vai retornar os seguintes dados de consulta:

¹⁰ O comando *id* mostra a identificação atual do usuário, grupo primário e outros grupos que pertence.

```

root@pipa:/etc/openldap2.4# id edson
uid=1236(Edson) gid=1018(Mat-Almox) grupos=1018(Mat-Almox)
root@pipa:/etc/openldap2.4#

```

Figura 3.9: Saída comando id.

Analizando o log do Serviço de Diretório vê-se que foi feita uma consulta a base do LDAP.

```

Dec 9 16:18:42 pipa slapd2.4[28141]: conn=1004 fd=22 ACCEPT from IP=127.0.0.1:48979 (IP=0.0.0.0:389)
Dec 9 16:18:42 pipa slapd2.4[28141]: conn=1004 op=0 BIND dn="" method=128
Dec 9 16:18:42 pipa slapd2.4[28141]: conn=1004 op=0 RESULT tag=97 err=0 text=
Dec 9 16:18:42 pipa slapd2.4[28141]: conn=1004 op=1 SRCH base="dc=prt21,dc=lan" scope=2 deref=0
filter="(&(objectClass=posixAccount)(uid=edson))"
Dec 9 16:18:42 pipa slapd2.4[28141]: conn=1004 op=1 SRCH attr=uid userPassword uidNumber gidNumber cn homeDirectory
loginShell gecos description objectClass
Dec 9 16:18:42 pipa slapd2.4[28141]: conn=1004 op=1 SEARCH RESULT tag=101 err=0 nentries=1 text=
Dec 9 16:18:42 pipa slapd2.4[28141]: conn=1004 op=2 SRCH base="dc=prt21,dc=lan" scope=2 deref=0
filter="(&(objectClass=posixAccount)(uidNumber=1236))"
Dec 9 16:18:42 pipa slapd2.4[28141]: conn=1004 op=2 SRCH attr=uid userPassword uidNumber gidNumber cn homeDirectory
loginShell gecos description objectClass
Dec 9 16:18:42 pipa slapd2.4[28141]: conn=1004 op=2 SEARCH RESULT tag=101 err=0 nentries=1 text=
Dec 9 16:18:42 pipa slapd2.4[28141]: conn=1004 op=3 SRCH base="dc=prt21,dc=lan" scope=2 deref=0
filter="(&(objectClass=posixGroup)(gidNumber=1018))"
Dec 9 16:18:42 pipa slapd2.4[28141]: conn=1004 op=3 SRCH attr=cn userPassword memberUid uniqueMember gidNumber
Dec 9 16:18:42 pipa slapd2.4[28141]: conn=1004 op=3 SEARCH RESULT tag=101 err=0 nentries=1 text=
Dec 9 16:18:42 pipa slapd2.4[28141]: conn=1004 op=4 SRCH base="dc=prt21,dc=lan" scope=2 deref=0
filter="(&(objectClass=posixAccount)(uid=edson))"
Dec 9 16:18:42 pipa slapd2.4[28141]: conn=1004 op=4 SEARCH RESULT tag=101 err=0 nentries=1 text=
Dec 9 16:18:42 pipa slapd2.4[28141]: conn=1004 op=5 SRCH base="dc=prt21,dc=lan" scope=2 deref=0
filter="(&(objectClass=posixGroup)((memberUid=edson)(uniqueMember=uid=edson,ou=users,dc=prt21,dc=lan)))"
Dec 9 16:18:42 pipa slapd2.4[28141]: conn=1004 op=5 SRCH attr=gidNumber
Dec 9 16:18:42 pipa slapd2.4[28141]: conn=1004 op=5 SEARCH RESULT tag=101 err=0 nentries=0 text=
Dec 9 16:18:42 pipa slapd2.4[28141]: conn=1004 op=6 SRCH base="dc=prt21,dc=lan" scope=2 deref=0
filter="(&(objectClass=posixAccount)(uid=edson))"
Dec 9 16:18:42 pipa slapd2.4[28141]: conn=1004 op=6 SEARCH RESULT tag=101 err=0 nentries=1 text=
Dec 9 16:18:42 pipa slapd2.4[28141]: conn=1004 op=7 SRCH base="dc=prt21,dc=lan" scope=2 deref=0
filter="(&(objectClass=posixGroup)((memberUid=edson)(uniqueMember=uid=edson,ou=users,dc=prt21,dc=lan)))"
Dec 9 16:18:42 pipa slapd2.4[28141]: conn=1004 op=7 SRCH attr=gidNumber
Dec 9 16:18:42 pipa slapd2.4[28141]: conn=1004 op=7 SEARCH RESULT tag=101 err=0 nentries=0 text=
Dec 9 16:18:42 pipa slapd2.4[28141]: conn=1004 op=8 SRCH base="dc=prt,dc=lan" scope=2 deref=0
filter="(&(objectClass=posixGroup)(gidNumber=1018))"
Dec 9 16:18:42 pipa slapd2.4[28141]: conn=1004 op=8 SRCH attr=cn userPassword memberUid uniqueMember gidNumber
Dec 9 16:18:42 pipa slapd2.4[28141]: conn=1004 op=8 SEARCH RESULT tag=101 err=0 nentries=1 text=
Dec 9 16:18:42 pipa slapd2.4[28141]: conn=1004 fd=22 closed (connection lost)

```

Figura 3.10: Dados do arquivo de log do LDAP

3.4 AJUSTES NO SERVIDOR BDC SAMBA

No caso do servidor secundário (BDC) tem-se alguns parâmetros configurados de

forma diferente dos utilizados no servidor PDC. São eles:

```
##### Arquivo smb.conf #####
[global]

# Configurar como Controlador de Dominio Secundário (BDC)

server string = Servidor BDC %L
netbios name = pontanegra

os level = 33

preferred master = No
domain master = No
local master = No
wins support = No
wins server = 10.21.0.5
```

Figura 3.11: Parâmetros do smb.conf do BDC PONTANEGRA

3.4.1 Ajustes no aplicativo smbldap-tools do BDC

Para os arquivos de configuração smbldap_bind.conf e smbldap.conf do BDC PONTANEGRA faz-se-á as mesmas configurações utilizadas no servidor PDC PIPA.

3.4.2 Ajustes no servidor LDAP do BDC

O arquivo de configurações do servidor (slapd.conf) terá a mesma estrutura do servidor PDC PIPA. Mudará somente a linha referente a identificação do servidor no arranjo de replicação da base LDAP.

```
##### /etc/openldap2.4/slapd.conf #####
#Parâmetro que identifica o servidor no arranjo de replicação mirrormode
#(master vs. master)
serverID 002
```

Figura 3.12: Alteração no servidor BDC PONTANEGRA

Também será feita uma modificação no arquivo nsswitch.conf do servidor BDC para que ele fique igual ao mostrado na Figura 3.8, e com isso busque os usuários na base LDAP.

3.5 SERVIÇO DE REPLICAÇÃO DE DIRETÓRIOS

Para garantir alta disponibilidade da rede institucional será utilizada a replicação das bases LDAP, através do método Syncrepl, tendo com isso um backup para o caso de falha no servidor Primário. Será adotado o modo de replicação multimaster, pois ele mostrou estar melhor adaptado a estratégia de trabalho da instituição, onde procura-se manter a independência das sub-redes.

Será acrescentado no arquivo de configuração do OpenLDAP do servidor PDC PIPA:

```
##### /etc/openldap2.4/slapd.conf #####
#Parâmetro que identifica o servidor no arranjo de replicação mirrormode
#(master vs. master)
serverID 001

# Habilitar o módulo de sincronização syncrepl
moduleload syncprov.la

# Carrega o módulo protocolo de sincronização
moduleload syncprov

# Cria o overlay para o syncprov
overlay syncprov

# Outras configurações
syncprov-checkpoint 100 10
syncprov-sessionlog 100

# Habilita o modo de replicação master - master
mirrormode on
```

Figura 3.13: Parâmetros do servidor Master PIPA que habilitam a replicação da base LDAP.

No servidor de backup (BDC) PONTANEGRA será modificado o arquivo de configuração do OpenLDAP para que ele replique a base do servidor PDC PIPA.

```
##### /etc/openldap2.4/slapd.conf #####
#Parâmetro que identifica o servidor no arranjo de replicação mirrormode
#(master vs. Master)
#Parâmetro alterado, conforme mencionado na seção 3.6
```

```
serverID 002

# Habilitar o módulo de sincronização syncrepl
moduleload syncprov.la

# Carrega o módulo protocolo de sincronização
moduleload syncprov

# Cria o overlay para o syncprov
overlay syncprov

# Outras configurações
syncprov-checkpoint 100 10
syncprov-sessionlog 100

# Habilita o modo de replicação master - master
mirrormode on

# Replicação do ldap
# Replicação para servidor PIPA
# rid: ID do syncrepl atual. Não pode ser negativo e deve ter 3 dígitos.
syncrepl rid=001
# provider: Servidor de onde será feita a réplica
provider=ldap://10.21.0.5
# bindmethod: Define o método de autenticação: tradicional, com simple,
#ou sasl.
bindmethod=simple
# binddn: Usuário que acessará a base original para buscar os dados que
#serão utilizados na sincronização.
binddn="cn=admin,dc=prt21,dc=lan"
# credentials: Senha do usuário descrito acima
credentials=chave
# searchbase: Como num servidor ldap é possível ter-se mais que uma base,
#aqui especificamos qual delas desejamos replicar.
searchbase="dc=prt21,dc=lan"
schemachecking=on
```

```
# Existem dois modos de operação do syncrepl, que determinarão como a
#réplica será realizada: refreshOnly: determina um intervalo de tempo no
#qual a base será replicada; e refreshAndPersist: sincroniza com uma
#conexão persistente.
type=refreshAndPersist
retry="60 +"
```

Figura 3.14: Parâmetros do servidor Master PONTANEGRA que habilitam a replicação da base LDAP.

Com o Syncrepl não foi necessário ter uma base inicial no servidor PONTANEGRA, adicionada manualmente antes de iniciar a réplica. Ao solicitar a primeira atualização da base toda a estrutura foi replicada do servidor PIPA.

Após essa primeira atualização completa, apenas as alterações da base passaram a ser propagadas por meio da replicação entre os servidores.

3.6 SINCRONIZAÇÃO DOS SERVIDORES PDC E BDC

A sincronização dos arquivos dos servidores é muito importante para que haja um ambiente seguro de backup dos dados. Caso haja necessidade do servidor secundário assumir o domínio não haverá perda de informação. Para esse processo decidiu-se por utilizar o programa Rsync¹¹, que acompanha a distribuição Linux utilizada.

Criou-se um script que faz a replicação dos dados e programou-se para que ele fosse executado num intervalo de tempo predeterminado. Para isso utiliza-se o Rsync em conjunto com o agendador de tarefas (cron). Abaixo a instrução que foi adicionada ao crontab¹², bem como o script de backup utilizado.

```
* /10 * * * * root /usr/local/sbin/replicapastas.sh
```

Figura 3.15: Instrução do cron

```
##### replicapastas.sh #####
#!/bin/bash
# Replicar dados para PONTANEGRA
```

11 Rsync é um programa de computador, utilizado em sistemas Unix, para sincronização de arquivos e diretórios (pastas) entre duas localidades diferentes enquanto minimiza a transferência de dados.

12 Crontab é um programa do Unix que edita o arquivo onde são especificados os comandos a serem executados e a hora e dia de execução pelo cron, um programa que executa comandos agendados nos sistemas operacionais do tipo Unix.

```
/usr/bin/rsync --delete -avzp --numeric-ids --rsh='ssh -p5555' /dados* root@10.21.0.11:/dados  
# Replica homedirectory  
/usr/bin/rsync --delete --exclude lixeira -avzp --numeric-ids --rsh='ssh -p5555' /home/* root@10.21.0.11:/home  
# Replicar netlogon  
/usr/bin/rsync --delete -avzp --numeric-ids --rsh='ssh -p5555' /etc/samba/netlogon/* root@10.21.0.11:/etc/samba/netlogon/
```

Figura 3.16: Script de backup

4 CONCLUSÕES E RECOMENDAÇÕES

Este trabalho teve o objetivo de mostrar como implantar um ambiente de rede com ferramentas de Software Livre capazes de executar tarefas de gerenciamento de arquivos e usuários de forma segura e com total transparência para o usuário. Com esses programas vimos que não é mais preciso que uma empresa invista quantias assustadoras de dinheiro para ter uma plataforma confiável e que esteja sempre em evolução, acompanhando o desenvolvimento dos equipamentos e tirando o máximo proveito deles.

A utilização do Samba com o serviço de diretório OpenLDAP na Procuradoria Regional do Trabalho da 21ª Região tornou o ambiente computacional da instituição mais seguro, ágil e ainda aberto para novas tecnologias, o que é de fundamental importância para o Ministério Público do Trabalho, devido ao seu crescimento dia após dia.

Com a implantação dessa estrutura (Samba com OpenLDAP) na sede da Procuradoria, estaremos futuramente criando duas novas sub-redes, em municípios distintos, e utilizando a mesma base de dados LDAP. Dessa forma o usuário terá acesso aos seus dados não importando se ele está acessando as informações da sede ou de uma sub-sede.

As possibilidades de utilização de um serviço de diretório centralizado leva-nos a pensar em novos serviços a serem oferecidos, sem que tenhamos a necessidade de termos diversos cadastros de usuários. O acesso a nossa Intranet e um comunicador instantâneo integrados a base LDAP são duas das diversas possibilidades que temos pela frente.

5 REFERÊNCIAS BIBLIOGRÁFICAS

CAMPOS, Augusto. O que é software livre. BR-Linux. Florianópolis, março de 2006. Disponível em (<http://br-linux.org/linux/faq-softwarelivre>). Consultado em 07/12/2010.

Guia Foca GNU/Linux (<http://focalinux.cipsga.org.br/guia/avancado/ch-s-samba.htm>)
Versão 6.42 - domingo, 18 de novembro de 2007, Gleydson Mazioli da Silva

MENEGUITE, Ronaldo. Replicação com Open LDAP

Enciclopédia Livre, Wikipédia (<http://pt.wikipedia.org/>).

THE SAMBA TEAM. The Official Samba-3 HOWTO and Reference Guide. Disponível em (<http://www.samba.org/samba/docs>). Consultado em 03/12/2010.

Comunidade de desenvolvedores do OpenLDAP (<http://openldap.org>).