Luís José Machado de Sousa

Consolidação de Bases LDAP distintas em Ambiente Samba: Proposição para um Caso Real

Monografia de Pós-Graduação "*Lato Sensu*" apresentada ao Departamento de Ciência da Computação para obtenção do título de Especialista em "Administração em Redes Linux"

Orientador
Prof. M.Sc. Herlon Ayres Camargo

Lavras
Minas Gerais - Brasil
2010

Luís José Machado de Sousa

Consolidação de Bases LDAP distintas em Ambiente Samba: Proposição para um Caso Real

Monografia de Pós-Graduação "*Lato Sensu*" apresentada ao Departamento de Ciência da Computação para obtenção do título de Especialista em "Administração em Redes Linux"

Aprovada em *24 de Abril de 2010*

Prof. M.Sc. Denilvon V. Martins

Prof. D.Sc. Joaquim Quinteiro Uchôa

Prof. M.Sc. Herlon Ayres Camargo
(Orientador)

Lavras
Minas Gerais - Brasil
2010

Aos que de alguma forma constroem o Software Livre, sem o qual não seria possível a execução deste trabalho.

Agradecimentos

A Deus, sobretudo;
Às minhas amadas Rose e Maria Clara, pela paciência e carinho;
À minha família, pelo apoio incondicional;
Ao meu orientador Prof. Herlon Camargo, pelas valorosas considerações;
E aos amigos e professores do ARL, por todo afeto e conhecimento compartilhado.

Sumário

Lista de Figuras

Lista de Tabelas

Resumo

Este trabalho apresenta uma proposição para consolidação de bases LDAP distintas em um ambiente Samba. Baseia-se em um caso real da Justiça Federal de Primeira Instância do Ceará, onde vários servidores Samba/LDAP atuam como PDC de domínios distintos em sítios remotos. São discutidos os detalhes para a consolidação das bases de dados dos servidores OpenLDAP e as adequações necessárias nos servidores Samba para a implementação de servidor de réplica, com a utilização do programa Syncrepl, para sincronizar o conteúdo dos diretórios dos servidores BDC remotos. Também são discutidos os procedimentos para migração dos compartilhamentos de arquivos e diretórios com a utilização de quota de disco e POSIX ACL.

Palavras-Chave: LDAP; Samba; Smbldap; Consolidação de Bases; Replicação; Syncrepl.

Capítulo 1

Introdução

Algumas experiências institucionais bem sucedidas e, principalmente, um relatório do TCU do ano de 1993[1] impulsionaram a utilização do Software Livre no âmbito governamental. "*No Documento, o relator do processo, ministro Augusto Sherman Cavalcanti, determina a aquisição de software livres pelo setor público como uma alternativa que pode significar economia, segurança e flexibilidade.*"(LUZ; CAPARELLI, 2003).

Apoiada tecnicamente em experiências bem sucedidas e respaldada legalmente, a Justiça Federal de Primeiro Grau no Ceará iniciou em 2004 a sua primeira experiência de uso corporativo de Software Livre. Inicialmente, implantou o seu primeiro controlador de domínio baseado nessa tecnologia para atender à rede do edifício sede situado na cidade de Fortaleza.

A partir do ano seguinte, os mesmos serviços foram estendidos para as subsedes localizadas em pontos remotos, na mesma cidade da sede e em outras cidades do interior do estado. Em virtude da precariedade da infraestrutura da rede de dados utilizada para conexões remotas entre a sede e as subsedes, avaliou-se a inviabilidade da implantação de uma solução com uma única base utilizando o protocolo `Lightweight Directory Access Protocol` (`LDAP`), replicada por meio de uma rede `WAN`[2]. Em virtude dessa limitação, para cada sítio, foi instalado um servidor `Samba/LDAP` para gerenciar uma base de dados localmente.

[1] Disponível em http://www.tcu.gov.br/Consultas/Juris/Docs/judoc/Acord/20031016/TC%20003.789.doc

[2] Wide Area Network (WAN) é uma rede que abrange áreas de longa distância.

Solucionado o problema da infraestrutura da rede WAN e ampliada a demanda de sistemas na instituição, surgiu a necessidade de se fazer uso das facilidades que um sistema de diretório pode oferecer, tais como catálogo único de endereços e autenticação centralizada do tipo *Single Sign On*[3], integrando os mais diversos sistemas.

Embora as informações de contas e grupos de usuários já estejam armazenadas em diretórios LDAP, o fato de se encontrarem armazenadas de forma distribuída inviabiliza a implementação de uma autenticação única. Além disso essa abordagem cria dificuldades no gerenciamento de contas de usuários que se encontram em trânsito entre a sede e subsedes da instituição.

Este trabalho tem como objetivo ser uma proposição para a consolidação de bases LDAP em ambiente Samba no âmbito da Justiça Federal de Primeiro Grau no Ceará, com o intuito de promover uma utilização mais ampla e eficiente dos serviços de diretórios, engendrando facilidades de uso de sistemas computacionais para os usuários da instituição e melhorias na gerência de informações corporativas para a área de tecnologia da informação.

O caso real tomado como referência neste trabalho refere-se a seis bases LDAP a serem unificadas em uma única, perfazendo um total de aproximadamente 1200 contas de usuários de domínio e 1100 estações de trabalho. Entretanto, por questões didáticas, limitou-se o número de bases LDAP para apenas duas delas, pois todos os procedimentos aqui desenvolvidos podem ser aplicados para as demais bases em virtude da similaridade ambiental. Para preservar as informações da instituição, utilizou-se dados fictícios nas bases LDAP e nos nomes dos servidores, com a simulação do ambiente de rede o mais próximo possível do real. Para realizar a simulação do ambiente real foram utilizadas máquinas virtuais[4] implementadas com a aplicação Sun VirtualBox[5].

O Capítulo 1 apresenta os objetivos deste trabalho e um resumo da metodologia adotada. O Capítulo 2 apresenta a revisão de literatura. O Capítulo 3 expõe os procedimentos necessários para a unificação de bases LDAP distintas. O Capítulo 4 discute quais as adequações necessárias nos serviços Samba e LDAP para se implementar a replicação dos diretórios LDAP. O Capítulo 5 apresenta os procedimentos de migração de arquivos e diretórios compartilhados pelo servidor Samba. O Capí-

[3] Single Sign On (SSO) é um mecanismo que permite ao usuário realizar apenas uma única ação de autenticação e autorização para utilizar todos os sistemas e aplicações que lhe são disponibilizados.

[4] Máquina virtual é o nome dado a uma máquina simulada através de software.

[5] VirtualBox é uma ferramenta utilizada para emular máquinas virtuais em plataformas x86 e AMD64/Intel64. Disponível em http://www.virtualbox.org.

tulo 6 apresenta as considerações finais e aponta sugestões para trabalhos futuros. Por fim, o Apêndice A lista os arquivos de configuração do servidor `Samba/LDAP` principal utilizado neste trabalho.

Capítulo 2

Revisão de Literatura

2.1 Samba

"*O* Samba[1] *é um pacote de software tremendamente popular, disponível sob a licença pública* GNU*, que implementa o lado* CIFS[2] *em hosts* Linux."(NEMETH; SNYDER; HEIN, 2007). Possui um amplo conjunto de ferramentas bastante úteis para integrar redes onde convivem juntos sistemas GNU/Linux e Windows.

Mesmo em um ambiente de rede em que predominam clientes Windows, há bons motivos para se utilizar o servidor Samba. Por ser um sistema de alta confiabilidade executado em plataforma Unix, também bastante confiável, apresenta poucos problemas e um baixo custo de manutenção. De acordo com (TS; ECKSTEIN; COLLIER-BROWN, 2003) o Samba oferece um melhor desempenho sob fortes cargas de demandas, superando o servidor Windows 2000 na proporção de 2 para 1 em equipamentos idênticos.

Além de todas as vantagens relacionadas a desempenho, a utilização do Samba representa significativa redução de custos de instalação, pois além de ser distribuído livremente não requer licenças adicionais para seus clientes.

Por meio dos *daemons* smbd e nmbd , o servidor Samba oferece os seguintes serviços:

[1] Disponível em http://samba.org

[2] Common Internet File System (CIFS) é um protocolo de compartilhamento de arquivos, evolução posterior do protocolo Server Message Block (SMB) desenvolvido para sistemas Windows.

- autenticação e autorização em domínio Windows;
- compartilhamento de sistema de arquivo através do protocolo CIFS;
- impressão em rede;
- conversão de nomes;
- anúncio de serviços;
- resolução de nomes com Windows Internet Name Service (WINS).

Outro destaque desse servidor está no fato de toda a sua configuração ser definida apenas em um único arquivo em formato texto. As configurações do servidor Samba são armazenadas no arquivo smb.conf e podem ser modificadas por meio de um editor de texto simples. Através do uso de parâmetros definidos individualmente por linha, sua configuração pode ser muito simples ou extremamente complexa, a depender dos recursos habilitados e das possíveis integrações com outros sistemas.

Através do uso de seções são definidas, no arquivo smb.conf, as configurações globais e de compartilhamento de recursos do protocolo CIFS.

Na seção global, identificada pelo marcador [global], são especificados os parâmetros que afetam todo o servidor.

Dentre os principais parâmetros, destacam-se:

- netbios name = [nome do servidor] - especifica o nome NetBIOS do servidor;
- workgroup = [nome do grupo/domínio] - define o nome do grupo de trabalho ou domínio;
- server string = [identificação] - identificação do servidor enviada para o ambiente de rede;
- domain master = - define se o servidor tentará ou não se tornar Domain Master Browser (DMB) da rede;
- local master = [valor] - diz se o servidor tentará ou não se tornar Local Master Browser (LMB) da rede local.
- preferred master = [valor] - define se o servidor terá vantagem para ganhar a eleição para LMB;

- os level = [num] - define o nível do sistema operacional para eleições de controlador local ou de domínio;

Em um domínio controlado por um Samba sempre é realizada uma eleição para definir o LMB do segmento de rede. Sobre o papel da máquina vencedora desta eleição, Silva afirma:

> "*Logo que é declarada o local master browser, ela começa a receber via broadcasting a lista de recursos compartilhados por cada máquina para montar a lista principal que será retornada para outras máquinas do grupo de trabalho ou outras subredes que solicitem os recursos compartilhados por aquele grupo.*"(SILVA, 2007).

Uma outra eleição também é realizada para definir DMB da rede. Esse servidor é conhecido como Controlador Principal de Domínio ou Primary Domain Controller (PDC). Seu papel é manter uma lista completa dos nomes das máquinas e dos recursos disponibilizados na rede, enviados pelos LMB.

Como mostra (TS; ECKSTEIN; COLLIER-BROWN, 2003), um PDC também atua como LMB de seu segmento de rede.

Um outro recurso disponibilizado pelo Samba é a implementação de servidor para atuar como Controlador Secundário de Domínio ou Backup Domain Controller (BDC). Esse servidor aumenta a disponibilidade e provê maior grau de escalabilidade do servidor Samba.

O uso do Samba integrado com servidor LDAP, utilizando replicação de diretórios, é uma das formas recomendáveis de viabilizar a implementação de um servidor BDC.

Mais detalhes sobre implementação do Samba estão disponíveis em (TS; ECKSTEIN; COLLIER-BROWN, 2003) e (THE SAMBA TEAM, 2007).

2.2 OpenLDAP

O OpenLDAP[3] é um serviço de diretório baseado no protocolo LDAP, extensão do trabalho feito inicialmente na Universidade de Michigan e agora continuado como um projeto de código aberto.

[3]Disponível em http://openldap.org

"*LDAP ou Protocolo Leve de Acesso a Diretórios é um conjunto de regras que controla a comunicação entre serviços de diretórios e seus clientes.*"(TRIGO, 2007).

Esse serviço provê informações em forma de árvore com o objetivo de facilitar o acesso a cada item armazenado. Sob esta abordagem, diretório significa algo usado para indicar direções.

Assim, pode-se definir um diretório como um sistema que armazena dados de forma hierárquica e que contém mecanismo otimizados de pesquisa dessas informações.

Existem vários motivos para a utilização do `OpenLDAP`, de acordo com (CARTER, 2009). Dentre eles destacam-se:

- o código fonte está disponível para *download* sob a licença `OpenLDAP Public Licence`. Junto com o código são fornecidas diversas informações suplementares à documentação existente;
- é compatível com as especificações principais do `LDAPv3`;
- disponível para múltiplas plataformas, incluindo `GNU/Linux`, `Solaris`, `Mac OS` e `FreeBSD`;
- é possível integrá-lo com diversos outros sistemas, tais como `Samba`, `Postfix`, `QMail`, `Squid` e `Radius`;
- trabalha com servidor de réplica, o que viabiliza distribuição de carga entre múltiplos servidores e alta disponibilidade.

As configurações do servidor `OpenLDAP` são definidas pelos arquivos `slapd.conf` e `ldap.conf`.

O arquivo `slapd.conf` é a fonte central das informações de configuração para o servidor *standalone* `OpenLDAP` e é utilizado por ferramentas relacionadas à manipulação de *dump* do conteúdo do diretório, como `slapcat` e `slapadd`.

Dentre as principais informações, encontram-se:

- os arquivos de *schemas*, os quais definem a estrutura das entradas e dos atributos que podem ser inseridos na base `LDAP`;
- o tipo de banco de dados que será utilizado pelo `OpenLDAP`;

- o domínio utilizado, definido pelo parâmetro `suffix`;
- o usuário administrador do domínio e sua senha, por meio dos parâmetros `rootdn` e `rootpw`, respectivamente;
- definições de políticas de acesso à base de dados;
- índices mantidos para otimizar as consultas.

O arquivo `ldap.conf` contém o endereço do servidor onde se encontra a base `LDAP` e o `DN` base do diretório, que é o mesmo definido pelo parâmetro `suffix` no arquivo `slapd.conf`. É utilizado pelas ferramentas de cliente `OpenLDAP`, tais como `ldapmodify` e `ldapsearch`.

Dentre as principais ferramentas disponibilizadas pelo servidor `OpenLDAP`, destacam-se os seguintes comandos e suas opções mais usuais:

- `slapcat` - utilizado para gerar um *dump* da base de dados para um arquivo no formato `LDIF`[4].

  Opções:

  `-b sufixo` - usa o `sufixo` para determinar qual a base a ser gerada.

  `-f slapd.conf` - especifica um arquivo `slapd.conf` alternativo.

  `-l arquivo-ldif` - escreve no arquivo `arquivo-ldif` especificado.

  `-s árvore` - define qual a `árvore` que será pesquisada.

- `slapadd` - adiciona dados *off-line* em diretório `LDAP`.

  Opções:

  `-b sufixo` - usa o `sufixo` para determinar qual a base a ser modificada.

  `-f slapd.conf` - especifica um arquivo `slapd.conf` alternativo.

  `-l arquivo-ldif` - lê os dados do arquivo `arquivo-ldif` especificado.

- `ldapsearch` - realiza pesquisas na base.

  Opções:

[4]LDAP Data Interchange Format (LDIF) é arquivo em formato texto simples usado para representar entradas em diretórios LDAP.

`-b sufixo` - usa o `sufixo` para determinar qual a base a ser pesquisada.

`-L` - saída no formato `LDIF`.

`-x` - autenticação simples.

`filtros` - filtros de pesquisas aplicados à base.

`atributos` - especifica os atributos a serem retornados na pesquisa.

- `ldapmodify` - altera entradas da base `LDAP`.

  Opções:

  `-f arquivo-ldif` - lê as modificações do arquivo `arquivo-ldif` especificado.

  `-W` - solicita *prompt* para autenticação simples.

  `-x` - autenticação simples.

- `ldapdelete` - apaga entradas `LDAP`.

  Opções:

  `-f arquivo-ldif` - apaga as entradas do arquivo `arquivo-ldif` especificado.

  `-W` - solicita *prompt* para autenticação simples.

  `-x` - autenticação simples.

Mais detalhes sobre os comando do `OpenLDAP` estão disponíveis em (TRIGO, 2007).

2.3 `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 a usuários comuns quanto a 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 encontra-se 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.

Do Smbldap-tools, destacam-se os *scripts* e suas opções mais usuais:

- smbldap-useradd - adiciona um novo usuário em um diretório LDAP.

  Opções:

  -a - cria uma conta Windows.

  -c gecos - define o atributo gecos do usuário.

  -m - cria o home do usuário e copia o conteúdo do arquivo /etc/skel para esse diretório.

  -P - solicita o *prompt* para informar a senha.

- smbldap-userdel - remove usuário em um diretório LDAP.

  Opções:

  -r - remove diretório home do usuário.

  -R - remove diretório home do usuário interativamente.

- smbldap-groupadd - adiciona um novo grupo em um diretório LDAP.

  Opções:

`-g gidNumber` - define o `gidNumber` para o grupo.

`-p` - imprime o `gidNumber` do grupo.

- `smbldap-groupmod` - modifica uma conta de usuário em um diretório `LDAP`.

  Opções:

  `-m` - adiciona usuários em um grupo.

  `-x` - apaga usuários de um grupo.

- `smbldap-groupdel` - remove um grupo em um diretório `LDAP`.

  Opções:

  Não há opções disponíveis.

Mais informações sobre implementação do `Smbldap-tools` são encontradas em (TERPSTRA, 2006).

2.4 `Syncrepl`

O `Syncrepl`, disponível a partir da versão `2.2` do servidor `OpenLDAP`, é um programa que provê recursos para a replicação e sincronização de diretórios `LDAP`, viabilizando a implementação de serviços de alta disponibilidade, balanceamento de carga em procedimentos de consulta e a utilização de servidores de *backup*.

Antes disso era disponibilizado apenas o programa `Slurp`, que utilizava um *daemon* exclusivo (`Slurpd`) para realizar tarefas de replicação entre diretórios.

O `Syncrepl`, diferente de seu antecessor, é iniciado juntamente com o processo `LDAP` e possui as seguintes características, como mostra (TRIGO, 2007):

- é mais flexível e tolerante à falhas que o `Slurp`;
- a ação de replicar é baseada no estado da réplica, ou seja, o servidor de réplica envia arquivos que definem o estado de seu conteúdo (*cookies*) para o servidor provedor, dispensando o uso de arquivos de *log*;
- possui parâmetros que aumentam a segurança e o desempenho;
- a réplica é iniciada pelo cliente (consumidor);

- é possível replicar somente parte da base de dados;
- somente atualiza após a conclusão da última transmissão (incremental);
- réplica baseada em evento (refreshOnly) ou em tempo determinado (refreshAndPersist).

A partir da versão `2.4`, o `OpenLDAP` suporta novos métodos de replicação, dentre eles, o protocolo de sincronização multi-master, através do qual as mudanças no diretório podem ser aceitas em qualquer réplica. Nesse caso, a réplica propaga a mudança para todos os servidores que contenham copias da partição.

Detalhes sobre a replicação com o `Syncrepl` estão disponíveis em (TRIGO, 2007) e (THE OPENLDAP PROJECT, 2004).

Capítulo 3

Migração da Base LDAP

Neste trabalho foram utilizados três servidores: PDCJUST, PDCJUST-SS e BDCJUST.

O servidor PDCJUST simulou o servidor instalado no edifício sede da instituição, utilizado para controlar o domínio JUSTA. Esse foi o receptor da base migrada e, portanto, sofreu poucas alterações nas configurações de seus serviços.

Para atender à rede da subsede, foi utilizado o servidor PDCJUST-SS para controlar o domínio JUSTA-SS. A base LDAP desse servidor foi migrada para a unificação no servidor PDCJUST, definido como o Primary Domain Controller (PDC) do domínio JUSTA.

O servidor BDCJUST foi instalado na subsede para receber a base replicada e atuar como BDC do domínio JUSTA, substituindo o servidor PDCJUST-SS. A utilização simultânea desse servidor com o PDCJUST-SS proporcionou uma migração gradual das estações de trabalho do domínio JUSTA-SS para o domínio JUSTA, controlado localmente pelo BDC da subsede. Esse procedimento teve como objetivo minimizar o impacto do processo de mudanças para os usuários do domínio da subsede.

A Tabela 3.1 apresenta um resumo dos principais dados relacionados aos serviços e ambiente de rede relacionados aos servidores cujas bases foram unificadas.

A Figura 3.1 mostra o diagrama de rede do ambiente simulado para o desenvolvimento deste trabalho.

Para realizar a simulação do ambiente real foram utilizadas máquinas implementadas com a aplicação Sun VirtualBox Versão 3.1.2 r56127. Para ga-

Tabela 3.1: Dados dos servidores Samba/LDAP

Servidor	PDCJUST	PDCJUST-SS
Localização	sede	subsede
End. IP Local	172.16.0.6/16	172.20.0.6/16
Rede Local	172.16.0.0/16	172.20.0.0/16
End.IP WAN	192.168.3.10/24	192.168.3.11/24
Rede WAN	192.168.3.0/24	192.168.3.0/24
Nome de Host	pdcjust.jus.br	pdcjust-ss.jus.br
Nome NetBIOS	PDCJUST	PDCJUST-SS
Domínio Samba	JUSTA	JUSTA-SS
SAMBA SID	S-1-5-21-1175868153-3947730691-4236143472	S-1-5-21-1275883430-1708041124-1285709030
Sufixo Base LDAP	dc=justa,dc=jus,dc=br	dc=justa-ss,dc=jus,dc=br

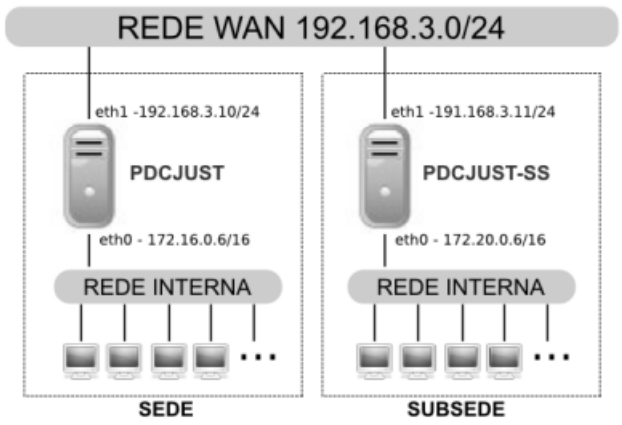

Figura 3.1: Diagrama do ambiente de rede simulado.

rantir a similaridade dos ambientes, os servidores Samba/LDAP utilizados neste trabalho foram instalados com o mesmo sistema operacional, bem como os mesmos pacotes dos serviços implementados no caso real. Utilizou-se o sistema operacional CentOS GNU/Linux i386 Versão 4.1 com os pacotes dos serviços apresentados na Tabela 3.2.

Vale salientar que este trabalho não tem como objetivo discutir a instalação de um servidor Samba/LDAP. Mais detalhes desses procedimentos são apresentados por (THE SAMBA TEAM, 2007).

Tabela 3.2: Pacotes utilizados nos servidores Samba/LDAP

Serviços	Pacotes
Samba	samba-3.0.10-1.4E
	samba-common-3.0.10-1.4E
	samba-client-3.0.10-1.4E
LDAP	openldap-2.2.13-2
	openldap-servers-2.2.13-2
	openldap-clients-2.2.13-2
Smbldap Tools	smbldap-tools-0.9.1-1.2.el4.rf
Quotas	quota-3.12-5

Este capítulo descreve os passos necessários para se efetuar a migração de uma base LDAP entre servidores distintos com o objetivo de unificação das informações em um diretório a ser replicado para um sítio remoto. O servidor denominado PDCJUST, instalado na sede, foi o receptor da migração oriunda do servidor PDCJUST-SS, localizado na subsede.

3.1 Migração de contas de usuários

Esta seção tem como objetivo apresentar os procedimentos necessários para a migração das contas de usuários observando-se detalhes fundamentais que evitaram inconsistências na base unificada.

Foram utilizadas ferramentas fornecidas nos pacotes do OpenLDAP e também alguns *scripts* desenvolvidos em Shell, exclusivamente para este processo, pelo autor deste trabalho. Informações detalhadas sobre programação em Shell estão disponíveis em (CAMARGO, 2005), (NEVES, 2008) e (JARGAS, 2008).

3.1.1 *Dump* da base de dados

Para extrair o *dump* da base de dados do servidor da subsede foi utilizado o programa Slapcat, fornecido junto com o pacote do Openldap-servers. Conforme orientação de (THE OPENLDAP PROJECT, 2004) o comando de um única linha, executado com privilégio de usuário root no console do servidor, foi o suficiente para gerar o *dump* da base desejada em formato LDIF:

```
    # slapcat -s ou=People,dc=justa-ss,dc=jus,dc=br \
-l usuarios_subsede.ldif
```

O arquivo `usuarios_subsede.ldif`, resultado da saída do comando acima, contém uma representação em formato textual simples de todas as entradas relacionadas aos usuários da base de dados `LDAP` do servidor da subsede `PDCJUST-SS`. Tais informações podem ser editadas *off-line* através de um editor de texto comum ou por meio de um *script*.

3.1.2 Tratando os atributos das contas de usuários

Dos dados obtidos no arquivo `usuarios_subsede.ldif`, apenas as entradas relacionadas às contas de usuários foram selecionadas para receberem o tratamento de seus atributos antes de se efetivar a migração para a base unificada. A Figura 3.2 exibe uma dessas entradas relativa a uma conta de usuário.

Como lembra (TRIGO, 2007), cada entrada é identificada por um atributo único denominado *Distinguished Name* - Nome distinto (`DN`). Para adequação dessa entrada à nova base, inicialmente foi necessário substituir o sufixo do domínio de `dc=justa-ss,dc=jus,dc=br` para `dc=justa,dc=jus,dc=br`.

Além do `DN`, também foi preciso ajustar os atributos `uidNumber`, `sambaSID` e `sambaPrimaryGroupSID`, implementado através do *script* escrito em `Shell` mostrado na Figura 3.3.

O atributo `uidNumber`, utilizado para identificar os usuários no sistema operacional `GNU/Linux`, deve ser único para cada conta. Para manter a integridade da base de dados, foi utilizado, no *script* da Figura 3.3, a variável `UID_NUMBER`, cujo valor foi definido com o próximo `uidNumber` a ser utilizado na base para onde estão sendo migradas as contas.

Para identificar o maior valor do atributo `uidNumber` na base do diretório do domínio `JUSTA` foi suficiente executar no servidor `PDCJUST` a seguinte linha de comando com privilégio de administrador do sistema:

```
    # ldapsearch -LLL -x -b ou=People,dc=justa,dc=jus,dc=br
uidNumber | grep uidNumber | cut -d":-f2 | tr -d " " |
sort -nr | head -n1
```

Para a base domínio `JUSTA`, utilizada neste trabalho, o valor retornado foi `1010`. Portanto, para evitar conflitos de dados, foi utilizado na variável `UID_NUMBER`

```
dn: uid=csabino,ou=People,dc=justa-ss,dc=jus,dc=br
objectClass: top
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
objectClass: sambaSamAccount
cn: Cesar Sabino
sn: csabino
uid: csabino
uidNumber: 1011
gidNumber: 513
homeDirectory: /home/csabino
loginShell: /bin/bash
gecos: Cesar Sabino
description: Cesar Sabino
structuralObjectClass: inetOrgPerson
entryUUID: 787ab2d6-aa1e-102e-8d76-b55582708a3b
creatorsName: uid=samba,ou=People,dc=justa-ss,dc=jus,dc=br
createTimestamp: 20100209232745Z
sambaLogonTime: 0
sambaLogoffTime: 2147483647
sambaKickoffTime: 2147483647
sambaPwdCanChange: 0
sambaPwdMustChange: 2147483647
displayName: Cesar Sabino
sambaAcctFlags: [UX]
sambaSID: S-1-5-21-1275883430-1708041124-1285709030-3022
sambaPrimaryGroupSID: S-1-5-21-1275883430-1708041124-1285709030-513
sambaHomeDrive: U:
sambaLMPassword: C7D36D999A7B2082AAD3B435B51404EE
sambaNTPassword: 2176503CCD06D05BBCE3E934465C555A
sambaPwdLastSet: 1265758069
userPassword:: e1NTSEF9czVRTVRCVG96QUpzcGQxbU5SNnhTLytFZlNWMk5VNUQ=
entryCSN: 20100209232749Z#000002#00#000000
modifiersName: uid=samba,ou=People,dc=justa-ss,dc=jus,dc=br
modifyTimestamp: 20100209232749Z
```

Figura 3.2: Conta de usuário da base `JUSTA-SS`

o valor imediatamente superior correspondente a 1011. Todos os uidNumber dos usuários migrados foram imputados com atributo a partir dessa numeração.

Os atributos sambaSID e sambaPrimaryGroupSID são relacionados ao conceito de domínio implementado pelo Samba. De acordo com (THE SAMBA TEAM, 2007), cada domínio provê um único Network Security Identifier (SID), o qual representa um contexto seguro. Todas as contas do domínio estão relacionadas ao SID do domínio. Para efetuar a migração dos usuários, também fez-se necessário a adequação desses atributos para o valor de SID (S-1-5-21-1175868153-3947730691-4236143472) relacionado ao domínio receptor da migração.

As contas de usuários e grupos são compostas pela combinação do SID e mais um identificador relativo (RID), o qual é único para cada conta de usuário do domínio. Para calcular o valor do identificador RID foi utilizada a função implementada pelo *script* Smbldap-useradd provido pelo pacote Smbldap-tools. Conforme consta no *script* mostrado na Figura 3.3, utilizou-se a seguinte função:

```
RID=uidNumber*2+1000
```

Calculado o RID correspondente, cada conta de usuário recebeu o valor de atributo sambaSID composto pela combinação SID-RID.

Para a conta de usuário apresentada na Figura 3.2, os atributos uidNumber e sambaSID receberam os valores 1014 e S-1-5-21-1175868153-3947730691-4236143472-3028, respectivamente.

O atributo sambaPrimaryGroupSID também é composto pela combinação SID-RID. Para adequá-lo para a migração, esse atributo recebeu o SID do domínio JUSTA combinado com o RID do grupo Domain Users, o qual possui o valor padrão igual a 513.

Portanto, todos os usuários receberam no atributo sambaPrimaryGroupSID o mesmo valor equivalente a S-1-5-21-1175868153-3947730691-4236143472-513.

Para implementar as adequações na base a ser migrada, executou-se o *script* da Figura 3.3 no servidor PDCJUST-SS, através da linha de comando no console, com privilégios de administrador do sistema:

```
# ./adiciona_grupos.sh usuarios_subsede.ldif > \
usuarios_subsede_migrados.ldif
```

O arquivo usuarios_subsede_migrados.ldif recebeu as contas dos usuários já com todas as adequações necessárias para serem inseridas na base unificada.

```
#!/bin/bash
# nome: ajusta_usuarios.sh
# descricao: ajusta contas de usuarios para migrar para novo domínio
# usage: ./ajusta_usuarios.sh <arquivo.ldif>

# Variaveis relacionadas as bases de dados
SUFIXO_ANTIGO="dc=justa-ss,dc=jus,dc=br"
SUFIXO_NOVO="dc=justa,dc=jus,dc=br"
SAMBA_SID="S-1-5-21-1175868153-3947730691-4236143472"
UID_NUMBER="1011"

# Seleciona os dn dos usuarios exceto os usuarios de sistema
grep 'dn: uid.*ou=People' $1 | grep -v 'uid=root,' |\
grep -v 'uid=nobody,' | grep -v 'uid=samba,' > ./dn_usuarios.ldif

while read DN_USUARIO
do
 # Calcula RID
 RID=$((($UID_NUMBER*2)+1000))

 # Seleciona atributos dos usuarios
 cat $1 |\
 sed -n "/$DN_USUARIO/,/modifyTimestamp:/p" |\

 # Troca SUFIXO
 sed -e "s/$SUFIXO_ANTIGO/$SUFIXO_NOVO/g

 # Troca UID Number
 s/^uidNumber:.*/uidNumber: $UID_NUMBER/g

 # Troca sambaSID
 s/^sambaSID:.*/sambaSID: ${SAMBA_SID}-${RID}/g

 # Troca sambaPrimaryGroupSID
 s/^sambaPrimaryGroupSID:.*/sambaPrimaryGroupSID: ${SAMBA_SID}-513/g"

 # Imprime linha em branco para separar usuarios
 echo ""

 # Incrementa UID NUMBER
 UID_NUMBER=$(($UID_NUMBER+1))
done < ./dn_usuarios.ldif

# Remove arquivo auxiliar
rm ./dn_usuarios.ldif
```

Figura 3.3: *Script* `ajusta_usuario.sh`

Por fim, para se efetivar a migração, foi copiado o arquivo de `usuarios_subsede_migrados.ldif` para o servidor `PDCJUST`, receptor da migração. Com o *daemon* `Ldapd` desligado, executou-se a seguinte linha de comando no console com privilégios de administrador:

```
# slapadd -l usuarios_subsede.ldif
```

Feito isso, iniciou-se o *daemon* `Ldapd` para que todas as contas de usuários estivessem disponíveis na base unificada:

```
# service ldap start
```

3.2 Migração de grupos de usuários

Esta seção descreve o processo de migração dos grupos de usuários do diretório `LDAP`, os quais são utilizados nas permissões de acesso ao servidor `Samba` citadas no Capítulo 4.

3.2.1 Copiando grupos e membros

Para migrar os grupos foi utilizado, no servidor da subsede `PDCJUST-SS`, o comando `ldapsearch`, que faz parte do conjunto de comandos do pacote `Openldap-clients`. As opções e os parâmetros de uso desse comando são detalhados por (TRIGO, 2007).

No console do servidor foi executado com privilégios administrativos a seguinte linha de comando:

```
# ldapsearch -LLL -x -b ou=Group,dc=justa-ss,dc=jus,dc=br \
'(&(!(ou=Group))(!(cn=Domain Admins))(!(cn=Domain Guests)) \
(!(cn=Domain Computers))(!(cn=Administrators)) \
(!(cn=Account Operators))(!(cn=Print Operators)) \
(!(cn=Backup Operators))(!(cn=Replicators)))' \
memberUid > grupos_subsede.ldif
```

A linha acima gerou o arquivo `grupos_subsede.ldif` contendo os grupos de usuários e seus respectivos membros.

É importante observar a utilização de filtros de busca para selecionar apenas os grupos que convenientemente deveriam ser migrados. Alguns desses grupos, criados automaticamente no processo de inicialização da base `LDAP` por meio da

execução do *script* `smbldap-populate`, disponível no pacote `smbldap-tools`, foram excluídos da seleção.

Apenas o grupo de sistema `Domain Users` e os grupos criados posteriormente foram selecionados, sendo excluídos os demais grupos de sistema, que já se encontravam na base receptora, com os mesmos membros da base em migração.

Como resultado, foi gerado um arquivo contendo os grupos `Domain Users`, `cartorio01` e `catorio02`, e seus respectivos membros, conforme apresentado na Figura 3.4.

```
dn: cn=Domain Users,ou=Group,dc=justa-ss,dc=jus,dc=br
memberUid: samba
memberUid: rbarros
memberUid: raraujo
memberUid: ralves
memberUid: csabino
memberUid: anascimento
memberUid: fpessoa

dn: cn=cartorio01,ou=Group,dc=justa-ss,dc=jus,dc=br
memberUid: rbarros
memberUid: ralves
memberUid: fpessoa

dn: cn=cartorio02,ou=Group,dc=justa-ss,dc=jus,dc=br
memberUid: csabino
memberUid: raraujo
memberUid: anascimento
```

Figura 3.4: Arquivo `grupos_subsede.ldif`

3.2.2 Adicionando grupos e membros

Para efetivar a migração dos grupos e seus respectivos membros, foi utilizado o *script* apresentado na Figura 3.5, desenvolvido em `Shell` pelo autor deste trabalho, junto com o arquivo `grupos_subsede.ldif`.

No servidor `PDCJUST`, com o *daemon* `Ldapd` desligado, executou-se a seguinte linha de comando no console do servidor com privilégios de administrador do sistema:

```
#./adiciona_grupos.sh grupos_subsede.ldif
```

Para finalizar a migração das contas de grupo de usuários, iniciou-se o *daemon* do serviço LDAP.

```
#!/bin/bash
# nome: adiciona_grupos.sh
# descricao: adiciona grupos e membros no novo domínio
# usage: ./adiciona_grupos.sh <arquivo.ldif>

while read LINHA
do
  ATRIBUTO=${LINHA%%:*}
  case $ATRIBUTO in
         "dn") GRUPO=$(echo ${LINHA##dn: } |\
                cut -d"," -f1 | cut -d"=" -f2);
               smbldap-groupadd "$GRUPO";;

  "memberUid") MEMBRO=$(echo ${LINHA##memberUid: })
               smbldap-groupmod -m "$MEMBRO" "$GRUPO";;
            *) shift;;
  esac
done < $1
```

Figura 3.5: *Script* adiciona_grupos.sh

3.3 Migração de estações de trabalho

Diferente das contas de usuários e grupos, a migração das contas das estações de trabalho não se realizou por meio da manipulação direta do conteúdo dos diretórios LDAP.

Ao adicionar as estações de trabalho no domínio JUSTA, o parâmetro add machine script, definido no arquivo smb.conf, foi suficiente para autorizar o servidor BDCJUST a incluir automaticamente as contas relativas a estas estações no diretório LDAP unificado. Os procedimentos para inclusão de clientes CIFS em domínio Samba são apresentados em detalhe por (TS; ECKSTEIN; COLLIER-BROWN, 2003).

Entretanto só foi possível realizar esse processo de migração das estações de trabalho após a instalação do servidor BDCJUST na subsede, já contendo a base replicada do domínio JUSTA. A instalação e configuração desse servidor é tratada no Capítulo 4.

Para reduzir o impacto desse processo foi necessária a convivência simultânea dos dois servidores Samba/LDAP na rede da subsede, o que viabilizou uma migração gradual das estações de trabalho.

Foi preciso então um ajuste para que apenas um dos servidores Samba desse suporte ao serviço WINS no segmento de rede da subsede. "*Nunca configure mais de um servidor WINS em uma mesma rede.*"(SILVA, 2007).

Durante o processo de migração foi desabilitado o serviço WINS no servidor BDCJUST, através da substituição do parâmetro `wins support = yes` por `wins server = 172.20.0.6`, endereço do servidor PDCJUST-SS.

Ao fim da migração de todas as estações de trabalho, foi desligado o antigo servidor PDCJUST-SS, restabelecido o serviço WINS no servidor BDCJUST e realizada as adequações nas estações de trabalho para utilização desse serviço.

3.4 Considerações Finais

Após os procedimentos apresentados neste Capítulo, o diretório LDAP do servidor PDCJUST passou a abrigar as contas dos usuários e grupos de rede da sede e subsede da instituição. A partir de então foi possível a replicação do diretório para um controlador de domínio secundário em uma subrede fora da sede.

O Capítulo 4 trata da preparação desse servidor Samba/LDAP secundário, denominado BDCJUST, configurado para atender ao domínio JUSTA na rede da subsede, implementando a replicação da base LDAP unificada no servidor PDCJUST, controlador principal do domínio.

Capítulo 4

Adequações nos Servidores Samba e LDAP

Este capítulo trata dos detalhes de configuração do servidor de réplica Samba/LDAP através da implementação do serviço Syncrepl, disponibilizado pelo pacote de programa Openldap-servers.

Para substituir o servidor PDCJUST-SS, foi implementado um servidor BDC do domínio JUSTA, denominado BDCJUST, responsável pelo controle do domínio com base única e replicada na subsede.

Para que houvesse uma migração gradual das estações de trabalho entre os domínios, o servidor BDCJUST foi colocado em produção em paralelo com o servidor PDCJUST-SS.

4.1 Adequações no servidor Samba

Esta seção apresenta as configurações necessárias para o servidor BDCJUST atuar como BDC na rede da subsede, migrando os compartilhamentos de recursos mantidos anteriormente pelo servidor PDCJUST-SS.

Foram ajustados o arquivo smb.conf e os *scripts* de *logon* de domínio e de grupos.

4.1.1 Ajustando o arquivo `smb.conf`

Para configurar o serviço `Samba` no `BDCJUST` foi utilizado como referência o arquivo `smb.conf` do servidor `PDCJUST` apresentado no Apêndice A.

O servidor `BDCJUST` foi configurado para atuar como `BDC` do domínio `JUSTA`, cujo servidor `PDC` encontra-se localizado no segmento de rede da sede. De acordo com (RED HAT, INC., 2005) só pode existir um único *Domain Master Browser* (`DMB`) por domínio, o qual recebe a lista dos recursos e compartilhamentos dos outros servidores `Local Master Browser` (`LMB`) presentes na rede.

O `PDCJUST`, instalado na sede, foi configurado para assumir o papel de `DMB` através da habilitação do parâmetro `domain master = yes`.

Para o servidor `BDCJUST`, o seu arquivo `smb.conf` foi configurado com o parâmetro `domain master = no`, entretanto foi utilizado o parâmetro `local master = yes`. Um trecho desse arquivo que define esse parâmetros globais é apresentado na Figura 4.1.

```
[global]
workgroup = JUSTA
server string = "Servidor BDCJUST"
netbios name = BDCJUST
domain master = no
local master = yes
preferred master = yes
domain logons = yes
os level = 65
wins server = 172.16.0.6
wins proxy = yes
```

Figura 4.1: Configurações globais do arquivo `smb.conf` no `BDCJUST`

Com esses parâmetros globais definidos, o servidor `BDCJUST` foi preparado para controlar o domínio `JUSTA` localmente (`LMB`), realizando a autenticação e autorização dos clientes no segmento de rede da subsede.

"*A máquina escolhida como Local Master Browser envia pacotes para a porta UDP 138 do Domain Master e este responde pedindo a lista de todos os nomes de máquinas que o Local Master conhece, e também o registra como Local Master para aquele segmento de rede.*"(SILVA, 2007).

Portanto, ao ser implementado um único domínio (JUSTA), o servidor PDCJUST passou a consolidar todas as informações relacionadas ao nomes de máquinas e recursos compartilhados através do protocolo CIFS em todos os segmentos da rede.

Também foram configurados dois parâmetros relativos ao serviço WINS.

O primeiro, wins server = 172.16.0.6, define exatamente o endereço do servidor PDCJUST, configurado como servidor WINS do domínio JUSTA.

Como lembra (THE SAMBA TEAM, 2007), o Samba não possui suporte nativo para replicação de serviço WINS. Como opção, utilizou-se o parâmetro wins proxy = yes que redireciona as solicitações de resoluções de nomes, feitas a partir dos clientes da rede local da subsede, para o serviço WINS prestado pelo servidor PDCJUST, localizado na sede.

Os outros parâmetros globais do servidor BDCJUST são exatamente iguais ao do servidor PDCJUST, apresentados no arquivo smb.conf do Apêndice A.

Além dos parâmetros globais utilizados pelo *daemon* smbd para definir os serviços de autenticação e autorização, também foram configurados no arquivo smb.conf as opções de compartilhamento de arquivos e diretórios utilizadas pelo protocolo CIFS.

Para que o novo servidor mantivesse os mesmos serviços de compartilhamento de recursos do PDCJUST-SS, foram migradas as definições de compartilhamentos apresentados na Figura 4.2.

Para os compartilhamentos [cartorio01] e [cartorio02], a opção valid users foi utilizada para delimitar o acesso apenas aos membros dos grupos correspondentes, migrados anteriormente para base LDAP unificada. Para cada compartilhamento de grupo foi utilizada a opção path que aponta para o diretório do sistema operacional onde se encontram os arquivos e diretórios compartilhados.

A migração de arquivos e diretórios disponibilizados por esse serviço é tratada no Capítulo 5.

Figura 4.2 apresenta ainda dois compartilhamentos especiais: [homes] e [net logon].

O primeiro refere-se ao compartilhamento do diretório inicial de cada usuário. Nos servidores tratados neste trabalho foi utilizado o padrão de diretório inicial do GNU/Linux, o qual é criado abaixo do diretório home, com o nome da conta do referido usuário de sistema e permissão de acesso restrita ao mesmo. Para a mon-

```
[homes]
  comment = Home Directories
  browseable = no
  writable = yes

[netlogon]
  comment = Netlogon
  path = /home/netlogon
  browseable = no
  public = yes
  read only = yes

[cartorio01]
  comment = 1o. Cartorio
  path = /home/compart/cartorio01
  browseable = yes
  writable = yes
  valid users = @cartorio01

[cartorio02]
  comment = 2o. Cartorio
  path = /home/compart/cartorio02
  browseable = yes
  writable = yes
  valid users = @cartorio02
```

Figura 4.2: Compartilhamento do arquivo `smb.conf` no `BDCJUST`

tagem automática desse diretório como uma unidade de rede remota, foi utilizado o parâmetro `logon drive` nas configurações globais do arquivo `smb.conf`.

O segundo compartilhamento refere-se ao diretório onde encontram-se os *scripts* de *logon* do domínio. Nesse diretório foi gravado o *script* `netlogon.bat`, definido no parâmetro global `logon script` do arquivo `smb.conf`, o qual deverá ser lido e executado por todas as máquinas clientes durante o *logon* no domínio. Em virtude da necessidade de apenas leitura desse *script* pelas máquinas clientes, o compartilhamento foi configurado com as opções `read only = yes` e `browseable = no`. Mais detalhes sobre o arquivo `netlogon.bat` são apresentados na Subseção 4.1.2.

4.1.2 Ajustando os *scripts* de *logon*

O arquivo `netlogon.bat`, disponibilizado por meio do compartilhamento de rede `[netlogon]` definido nas configurações globais do servidor `BDCJUST`, foi migrado do servidor `PDCJUST-SS` e sofreu alguns ajustes para se adequar ao novo domínio.

Esse arquivo, que contém comandos `MS-DOSNT` que são executados nos clientes `CIFS` no momento do *logon* das máquinas `Windows` no domínio, é apresentado na Figura 4.3.

```
echo off
@call net time \\bdcjust /YES

@REM Script especifico por usuario
@REM \\bdcjust\netlogon\%username%.bat

@echo Ativando unidades de rede...
@call \\bdcjust\cartorio01\netlogon.bat
@call \\bdcjust\cartorio02\netlogon.bat
```

Figura 4.3: *Script* de *logon* `netlogon.bat` do `BDCJUST`

Para adequar esse *script* ao novo servidor foi necessário modificar o nome `NetBIOS` em todas referências feitas ao servidor do domínio. Para isso, substituiu-se o nome `pdcjust-ss` por `bdcjust` nas referências aos compartilhamentos providos pelo servidor `BDCJUST`.

Também foram necessários os mesmos ajustes nos *scripts* `netlogon.bat` executados pelas duas últimas linhas da Figura 4.3, os quais foram configurados

com permissões de execução apenas para os membros dos grupos cartorio01 e cartorio02, respectivamente.

No caso do primeiro *script* netlogon.bat, foi concedida a permissão de execução apenas para os membros do grupo cartorio01. Durante o *logon* no domínio, este *script* solicita o mapeamento da uma unidade de rede para o compartilhamento [cartorio01], definido no servidor BDCJUST através da linha de comando MS-DOSNT a seguir:

```
net use T: \\bdcjust\cartorio01 /no
```

Efetuado o *logon* no domínio, os membros do grupo cartorio01 passaram a ter disponível, além da unidade (U:), relativa ao diretório inicial de usuário, a unidade de grupo (T:), equivalente ao compartilhamento correspondente no servidor BDCJUST.

Para o grupo catorio02 foi utilizado o mesmo *script* netlogon.bat, apenas com as adequações do nome do grupo e das permissões de execução.

4.2 Adequações nos arquivos do Smbldap-tools

Para configuração do novo servidor de domínio BDCJUST, necessitou-se realizar ajustes dos arquivos smbldap.conf e smbldap_bind.conf, gravados no diretório /etc/smbldap-tools, nos quais está baseado o uso destas ferramentas.

4.2.1 Ajustando o arquivo smbldap.conf

O arquivo smbldap.conf, utilizado para definir parâmetros globais a serem utilizados pelos *scripts* do Smbldap-tools, abriga as informações relacionadas ao domínio do servidor Samba.

Dessa forma, para ajustar o servidor BDCJUST ao domínio JUSTA, utilizou-se para esses três parâmetros, os mesmos definidos no PDC. Assim, foi suficiente copiar o arquivo smbldap.conf, sem nenhuma alteração, do servidor PDCJUST, listado no Apêndice A.

4.2.2 Ajustando o arquivo `smbldap_bind.conf`

O arquivo `smbldap_bind.conf` possui as credenciais de acesso do usuário administrador do diretório `LDAP`. Para manter uma padronização foi conveniente utilizar as mesmas credenciais em todos os servidores `LDAP`.

Portanto, para adequar esse arquivo do servidor `BDCJUST` ao novo domínio, foi suficiente ajustar o `DN` do usuário administrativo do diretório com o sufixo do domínio `JUSTA` e configurar a sua senha correspondente. Para todos servidores `Samba/LDAP` tratados neste trabalho foi utilizado o usuário `samba` com poderes administrativos, o qual possui permissão de leitura e escrita em todo conteúdo do diretório.

Foi suficiente copiar o arquivo `smbldap_bind.conf` do servidor `PDCJUST`, apresentado no Apêndice A.

4.3 Adequações no servidor `LDAP`

Esta seção detalha as configurações feitas nos arquivos do servidor `OpenLDAP` necessárias para garantir a sincronização das bases `LDAP` entre os servidores `PDCJUST` e `BDCJUST`.

4.3.1 Ajustando o arquivo `sldapd.conf`

Para prover as informações do domínio `JUSTA`, o servidor `BDCJUST` foi configurado com os mesmos parâmetros de domínio e *schemas*, exceto as definições de políticas de acesso, do servidor `PDCJUST`. As permissões de acesso para o `BDCJUST` são tratadas na Subseção 4.3.3.

Portanto, o servidor `BDCJUST` foi inicialmente configurado com o arquivo `slapd.conf` com o mesmo conteúdo, retiradando-se as permissões de acesso, do servidor `PDCJUST`, mostrado no Apêndice A.

4.3.2 Ajustando o arquivo `ldap.conf`

O arquivo `ldap.conf` contém apenas o endereço do servidor onde se encontra a base `LDAP` e o `DN` base do diretório.

Semelhante ao servidor PDCJUST, o servidor BDCJUST possui o serviço LDAP e o conteúdo de sua base instalados no mesmo equipamento. Também utiliza o mesmo DN base relativo ao domínio JUSTA.

Portanto, o servidor BDCJUST foi configurado com o conteúdo do arquivo ldap.conf idêntico ao do servidor PDCJUST, listado no Apêndice A.

4.3.3 Serviço de replicação de diretórios

Para garantir a unicidade e integridade da base LDAP entre os servidores, foi utilizado o programa Syncrepl, disponibilizado junto com o servidor OpenLDAP.

Pelo fato do mecanismo de sincronização do Syncrepl ser implementada do lado cliente, conforme ressalta (THE OPENLDAP PROJECT, 2004), é suficiente configurar o arquivo slapd.conf no servidor BDCJUST.

Para configurar a parte cliente do servidor de réplica, foram incluídos no arquivo slapd.conf, do servidor BDCJUST, os parâmetros apresentados na Figura 4.4.

```
syncrepl rid=123
                provider=ldap://172.16.0.6:389
                type=refreshOnly
                interval=00:00:05:00
                searchbase="dc=justa,dc=jus,dc=br"
                scope=sub
                schemachecking=off
                updatedn="cn=replica,dc=justa,dc=jus,dc=br"
                bindmethod=simple
                binddn="cn=Manager,dc=justa,dc=jus,dc=br"
                credentials=secret
updateref ldap://172.16.0.6
```

Figura 4.4: Configuração do Syncrepl no BDCJUST

O parâmetro provider indica o endereço do servidor provedor, de onde são consumidas as atualizações da base de dados, neste caso, o servidor PDCJUST.

As opções type=refreshOnly e interval=00:00:05:00 definem o modo de sincronização e a periodicidade de solicitação das atualizações ao servidor provedor das informações, respectivamente.

Para autenticação no servidor LDAP provedor foram utilizados os parâmetros binddn="cn=Manager,dc=justa,dc=jus,dc=br" e credentials=secret. Es-

tes indicam o DN e a senha do usuário que tem permissão de leitura e escrita no diretório LDAP do servidor PDCJUST.

Vale ainda ressaltar o parâmetro updateref, utilizado no lado consumidor da replicação. Esta opção indica que todas as solicitações de modificações enviadas para o servidor BDCJUST deverão ser redirecionadas para o servidor principal, indicado pelo endereço de rede fornecido. Portanto todas as modificações sempre ocorrerão no servidor PDCJUST e, posteriormente, replicadas para o servidor BDCJUST, quando este solicitar a sincronização do conteúdo de seu diretório.

Mais detalhes sobre esses e outros parâmetros do Syncrepl são encontradas em (TRIGO, 2007) e (THE OPENLDAP PROJECT, 2004).

Foi ainda necessário adequar as permissões de escrita no servidor consumidor das atualizações, de forma a assegurar que apenas o usuário definido pelo parâmetro updatedn pudesse fazer as modificações na base de dados, garantindo, assim, a consistência da replicação. Foi restringida, portanto, a permissão de escritas apenas ao DN equivalente ao usuário definido como responsável pela gravação da réplica no servidor BDCJUST: cn=replica,dc=justa,dc=jus,dc=br.

Para evitar ambiguidade, esse mesmo usuário também foi definido como o rootdn do diretório em substituição a cn=Manager,dc=justa,dc=jus,dc=br.

A Figura 4.5 apresenta as permissões de acesso com essas restrições definidas no arquivo slapd.conf do servidor BDCJUST.

Concluídas as configurações do Syncrepl, reiniciou-se os servidores LDAP, começando pelo provedor PDCJUST e, em seguida, o consumidor BDCJUST.

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

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

4.4 Considerações Finais

Após a conclusão dos procedimentos descritos neste Capítulo, o servidor BDCJUST ficou preparado para realizar o controle do domínio JUSTA na subsede, com a replicação do diretório LDAP unificado no servidor PDCJUST.

```
# Políticas de acesso para réplica
access to attrs=objectClass,entry,gecos,homeDirectory,
 uid,uidNumber,gidNumber,cn,memberUid,attrs=description,
 telephoneNumber
   by * read

access to attrs=cn,attrs=userPassword,sambaLMPassword,sambaNTPassword,
 sambaPwdLastSet, sambaLogonTime,sambaLogoffTime,sambaKickoffTime,
 sambaPwdCanChange, sambaPwdMustChange,sambaAcctFlags,displayName,
 sambaHomePath, sambaHomeDrive,sambaLogonScript,sambaProfilePath,
 description, sambaUserWorkstations,sambaPrimaryGroupSID,
 sambaDomainName,sambaSID,sambaGroupType,sambaNextRid,
 sambaNextGroupRid,sambaNextUserRid,sambaAlgorithmicRidBase
   by self read
   by * none

access to *
   by dn.base="cn=replica,dc=justa,dc=jus,dc=br" write
   by * none
```

Figura 4.5: Permissões de acesso no BDCJUST

Vale observar que no ambiente de rede real a comunicação entre os servidores Samba/LDAP em pontos remotos ocorre através de uma rede WAN, conetada por meio de alguns ativos, tais como roteadores e *firewalls*. É possível que haja a necessidade de ajustes nesses equipamentos para permitir a troca de pacotes através das portas de comunicação do protocolo TCP/IP utilizadas pelos serviços Samba e Syncrepl.

Para realizar a migração definitiva do domínio, com a transferência das estações de trabalho, ainda foi necessário migrar os arquivos e diretórios compartilhados pelo servidor PDCJUST-SS. O Capítulo 5 detalha esses procedimentos.

Capítulo 5

Migração de Dados Compartilhados no Servidor

Além de realizar tarefas de autenticação e autorização no domínio, os servidores Samba/LDAP tratados neste trabalho também implementam serviços de compartilhamento de arquivos.

Este Capítulo aborda os detalhes da migração dos arquivos e diretórios compartilhados pelo Samba no servidor PDCJUST-SS para o servidor BDCJUST, com a integração de outros recursos, como Posix ACL e serviço de quota.

5.1 Cópia de dados compartilhados e ACLs

5.1.1 Copiando os arquivos compartilhados

Conforme pode ser observado no arquivo smb.conf de configuração do servidor Samba da Figura 4.2, todos os compartilhamentos migrados são relativos a dados gravados no diretório /home do sistema de arquivos do GNU/Linux.

Considerando que foi atribuído o endereço de rede 172.20.0.7/16 para o servidor BDCJUST, para efetuar a transferência dos dados foi suficiente executar no console do servidor PDCJUST-SS a seguinte linha de comando com privilégios administrativos:

```
# rsync -a /home root@172.20.0.7:/home
```

A linha de comando acima realizou a cópia dos arquivos e diretórios do servidor PDCJUST-SS, no qual o comando foi executado, para o servidor BDCJUST, receptor da migração dos dados.

O Rsync[1], utilizado nesse procedimento, é um programa de código-aberto, disponível para sistemas Unix, que sincroniza remotamente dados entre servidores, com a vantagem de preservar as informações relacionadas ao controle de acesso nativo do sistema de arquivo.

A opção -a foi usada para ativar o archive mode, um conjunto de opções mais usuais para transferência de arquivos.

Para realizar a transferência dos arquivos entre os servidores Samba/LDAP, o Rsync utilizou o protocolo SSH[2]. Portanto, foi necessário disponibilizar esse serviço no servidor BDCJUST, receptor da transferência dos dados. Mais detalhes de utilização do Rsync e da implementação do servidor SSH estão disponíveis em (NEMETH; SNYDER; HEIN, 2007).

5.1.2 Copiando as permissões de acesso estendidas

A partir da versão do 2.4 do *kernel* do GNU/Linux foi disponibilizado uma extensão ao sistema de controle de acesso Unix tradicional, denominada POSIX ACL. Este recurso possibilitou a utilização de ACLs[3] com a especificações de permissão para múltiplos usuários ou grupos.

O Samba ao compartilhar arquivos e diretórios com sistemas Windows é compatível com a POSIX ACL e faz um bom esforço para traduzir ACLs entre este sistema operacional e o GNU/Linux.

Para habilitar esse recurso foi utilizada a opção acl no arquivo /etc/fstab, no qual são definidas todas as opções de montagem de sistema arquivos durante a inicialização do servidor.

O servidor BDCJUST foi instalado com uma partição separada para o diretório /home. Assim, para habilitar a POSIX ACL, foi incluída a cláusula acl, na linha relacionada a esta partição, dentro do arquivo /etc/fstab.

[1] Rsync é um utilitário que provê rápida transferência de arquivo de forma incremental. Disponível em http://samba.anu.edu.au/rsync/.

[2] Secury Shell ou SSH é um protocolo de rede que permite a conexão criptografada entre computadores que permite a execução remota de comandos.

[3] Access Control list (ACL) ou Lista de Controle de Acesso é uma lista que define as permissões de acesso a um determinado objeto de um sistema, como por exemplo, um sistema de arquivo.

Infelizmente ainda poucos utilitários de *backup* e transferência de arquivos dão suporte a POSIX ACL, como é o caso do Rsync, utilizado para migrar os dados compartilhados nos servidores. Para contornar essa limitação, fez-se uso de utilitários que manipulam POSIX ACL.

Para fazer o *dump* das ACLs no servidor PDCJUST-SS foi necessário executar a seguinte linha de comando com privilégio de administrador do sistema:

```
# getfacl -R /home > dir_home.acl
```

Para restaurar as ACLs, foi copiado o arquivo dir_home.acl para servidor BDCJUST, no qual executou-se a linha de comando, com privilégios de administrador do sistema:

```
# setfacl --restore=dir_home.acl
```

Os programas getfacl e setfacl estão disponíveis no pacote de programas acl, disponível no repositório oficial da distribuição GNU/Linux utilizada neste trabalho.

Mais informações sobre o uso de POSIX ACL são apresentadas em (TERPSTRA, 2006).

5.2 Configuração de quotas

De acordo com (RED HAT, INC., 2007), o sistema de quota de disco nativo do sistema GNU/Linux possibilita gerar restrições por partição para cada usuário do sistema ou mesmo para grupos de usuários. Uma boa gerência desse sistema promove o uso racional dos recursos de discos disponibilizados pelo servidor.

Para migrar as informações de quota de usuário para o servidor BDCJUST foram executados os seguintes passos:

- habilitação do sistema de quotas no arquivo /etc/fstab com a inclusão da opção usrquote para a partição do diretório /home. Para concluir esse passo foi ainda necessário remontar esta partição com a seguinte linha de comando executada com privilégio de administrador:

  ```
  # mount -o remount /home
  ```

- o uso do utilitário Rsync para migrar os dados do servidor PDCJUST-SS copiou também o arquivo aquota.user, no qual são guardadas as informações

de quota de disco para usuários. Portanto, foi apenas suficiente gerar a tabela de uso corrente de disco para o diretório `/home` com execução da seguinte linha de comando com privilégio de administrador no servidor `BDCJUST`:

```
# quotacheck -avu
```

Foram implementas apenas quotas de usuário no servidores tratados neste trabalho. (RED HAT, INC., 2007) apresenta os detalhes de implementação de quotas de grupo.

5.3 Considerações Finais

Os procedimentos abordados neste Capítulo prepararam o servidor `BDCJUST` para receber as estações de trabalho da rede da subsede no domínio `JUSTA`.

Ao final da migração das estações de trabalho do domínio `JUSTA-SS` para `JUSTA`, o servidor `PDCJUST-SS` pôde ser desativado, conforme descrito na Seção 3.3.

Capítulo 6

Considerações Finais

O serviço de diretório vem se tornando um padrão, com diversos programas dando suporte ao LDAP. Existem muitas formas de se disponibilizar um serviço de diretório, o que permite que diferentes tipos de informações sejam manipuladas com requerimentos diferentes sobre os objetos armazenados.

Devido a grande flexibilidade tanto do servidor Samba, quanto do servidor OpenLDAP, este trabalho abordou apenas uma das diversas possibilidades de utilização desses serviços, que podem ser configurados e integrados com muitas outras ferramentas de modo que melhor se adeque aos mais diversos cenários.

Para efeitos de simulação, foi alcançado o objetivo esperado. A solução apresentada neste trabalho, portanto, está apta para ser implementada, entretanto deve-se atentar para possíveis detalhes do ambiente real que não foram tratados na simulação. Deve ficar claro que não existe uma única forma de implementação de tais serviços e não foi pretensão desse trabalho delimitar essas possibilidades.

A utilização de réplica de diretório, tratada nessa proposição com o uso do Syncrepl, viabiliza a autenticação única no ambiente da Justiça Federal de Primeiro Grau no Ceará, o que pode resultar em grandes benefícios para a instituição. Dentre esses benefícios pode-se destacar: a diminuição do desgaste do usuário ao administrar apenas uma única credencial de acesso, redução do tempo gasto em vários processos de autenticação, redução do número de chamados técnicos para reinicialização de senhas e centralização de informações de acesso protegidas.

Em virtude de não haver restrição quanto ao número de réplicas, o uso de múltiplos servidores BDC, em cada segmento de rede, também possibilita o aumento do grau de escalabilidade e disponibilidade dos serviços de autenticação.

Além desses benefícios supra citados, a replicação também representa uma boa estratégia para a redução do tráfego na rede WAN da instituição, pois todas as requisições de leitura do diretório LDAP podem ocorre na própria rede local.

6.1 Trabalho Futuros

Este trabalho apresentou uma solução para autenticação única sem considerar os aspectos de segurança que envolvem um ambiente de rede. Uma proposta para trabalhos futuros é a implementação de uma solução *Single Sign On* com o uso do OpenLDAP integrado com Kerberos, visando aumentar o nível de segurança no processo de autenticação.

Outros trabalhos podem ser desenvolvidos utilizando os novos métodos de replicação disponibilizados a partir da versão 2.4 do OpenLDAP.

Referências Bibliográficas

CAMARGO, H. A. *Automação de Tarefas*. Lavras: UFLA/FAEPE, 2005. 152 p. Curso de Pós-Graduação "Lato Sensu"(Especialização) a Distância: Administração em Rede Linux.

CARTER, G. *LDAP Administração de Sistemas*. Rio de Janeiro: Starlin Alta Con. Com. Ltda, 2009.

JARGAS, A. M. *Shell Script Profissional*. São Paulo: Novatec Editora, 2008.

LUZ, C.; CAPARELLI, E. Governo x Microsoft. *Revista do TCU*, Tribunal de Contas da União, Brasília, v. 1, n. 98, dez. 2003.

NEMETH, E.; SNYDER, G.; HEIN, T. R. *Manual Completo do Linux*. São Paulo: Pearson Prentice Hall, 2007.

NEVES, J. C. *Programação Shell Linux*. 7. ed. Rio de Janeiro: Brasport, 2008.

RED HAT, INC. *Red Hat Enterprise Linux 4*: Reference guide. [S.l.], 2005. Acessado em: 02 de fevereiro de 2010. Disponível em: <http://www.redhat.com-/docs/manuals/enterprise/RHEL-4-Manual/ref-guide/index.html>.

RED HAT, INC. *Red Hat Enterprise Linux 4.5.0*: System administration guide. [S.l.], 2007. Acessado em: 02 de fevereiro de 2010. Disponível em: <http://www.redhat.com/docs/manuals/enterprise/RHEL-4-Manual/en-US-/System_Administration_Guide_/index.html>.

SILVA, G. M. d. *Guia Foca GNU/Linux*: Avançado. [S.l.], 27 nov. 2007. Acessado em: 10 de fevereiro de 2010. Disponível em: <http://focalinux.cipsga-.org.br/download/inic_interm/focalinux12-pdf.tar.gz>.

TERPSTRA, J. H. *Samba-3 by Example*: Practical exercises in successful samba deployment. [S.l.], jul. 2006. Acessado em: 31 de janeiro de 2010. Disponível em: <http://www.samba.org/samba/docs/man/Samba-Guide/>.

THE OPENLDAP PROJECT. *OpenLDAP Software 2.2 Administrator's Guide*. [S.l.], 25 fev. 2004. Acessado em: 02 de janeiro de 2010. Disponível em: <http://www.openldap.org/doc/admin22/>.

THE SAMBA TEAM. *The Official Samba 3.2.x HOWTO and Reference Guide*. [S.l.], 2007. Acessado em 31 de janeiro de 2010. Disponível em: <http://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/>.

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

TS, J.; ECKSTEIN, R.; COLLIER-BROWN, D. *Using Samba*. 2. ed. USA: O'Reilly & Associates, 2003.

Apêndice A

Arquivos de Configuração do Servidor PDCJUST

A.1 Arquivo smb.conf

```
[global]
  workgroup = JUSTA
  server string = "Servidor PDCJUST"
  netbios name = PDCJUST
  domain master = yes
  local master = yes
  preferred master = yes
  domain logons = yes
  os level = 100
  logon script = netlogon.bat
  logon path = \\%L\%U\Profiles
  logon home = \\%L\%U
  logon drive = U:
  wins support = yes
  name resolve order = wins lmhosts bcast
  admin users = samba
  log file = /var/log/samba/%m.log
  max log size = 50
  security = user
  encrypt passwords = yes
```

```
socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
read raw = yes
write raw = yes
max xmit = 65535
getwd cache = yes
oplocks = yes

# Integracao com LDAP
# scripts para adionar maquinas e usuarios automatico
add machine script = /usr/sbin/smbldap-useradd -w %u
add group script = /usr/sbin/smbldap-groupadd -p %g
add user to group script = /usr/sbin/smbldap-groupmod -m %u %g

# Base Ldap na qual deve realizar a autenticacao
passdb backend = ldapsam:ldap://127.0.0.1
# DN do administrador do LDAP
#ldap admin dn = "cn=Manager,dc=justa,dc=jus,dc=br"
ldap admin dn = "uid=samba,ou=People,dc=justa,dc=jus,dc=br"
# DN da base ldap
ldap suffix = dc=justa,dc=jus,dc=br
# Ramo de maquinas
ldap machine suffix = ou=Computers
# Ramo de Usuarios
ldap user suffix = ou=People
# Ramo de Grupos
ldap group suffix = ou=Group
# sicronizando senhas de todos os sistemas
ldap passwd sync = yes
# Utilizar ssl
ldap ssl = off
# Quando o usuario for removido do samba ser removido do ldap
ldap delete dn = yes

# ACLs Windows
map acl inherit = yes
inherit acls = yes
inherit permissions = yes

# Internacionalizacao
```

```
  ldap idmap suffix = ou=People
  dos charset = CP850
  unix charset = ISO8859-1

# Definicoes de compartilhamento

[homes]
  comment = Home Directories
  browseable = no
  writable = yes

[netlogon]
  comment = Netlogon
  path = /home/netlogon
  browseable = no
  public = yes
  read only = yes

[diretoria]
  comment = Diretoria Administrativa
  path = /home/compart/diretoria
  browseable = yes
  writable = yes
  valid users = @diretoria

[contadoria]
  comment = Secao de Contadoria
  path = /home/compart/contadoria
  browseable = yes
  writable = yes
  valid users = @contadoria
```

A.2 Arquivo `smbldap.conf`

```
# Security Identified do Dominio
SID="S-1-5-21-1175868153-3947730691-4236143472"

# Domínio do Samba
```

```
sambaDomain="JUSTA"

# Configurações LDAP
masterLDAP="127.0.0.1"
masterPort="389"
ldapTLS="0"
verify="none"
cafile="/etc/smbldap-tools/ca.pem"
clientcert="/etc/smbldap-tools/smbldap-tools.pem"
clientkey="/etc/smbldap-tools/smbldap-tools.key"
suffix="dc=justa,dc=jus,dc=br"
usersdn="ou=People,${suffix}"
computersdn="ou=Computers,${suffix}"
groupsdn="ou=Group,${suffix}"
idmapdn="ou=Idmap,${suffix}"
sambaUnixIdPooldn="sambaDomainName=JUSTA,${suffix}"
scope="sub"
hash_encrypt="SSHA"
crypt_salt_format="%s"

# Configurações GNU/Linux
userLoginShell="/bin/bash"
userHome="/home/%U"
userHomeDirectoryMode="700"
userGecos="System User"
defaultUserGid="513"
defaultComputerGid="515"
skeletonDir="/etc/skel"

# Configurações Samba
userSmbHome=""
userProfile=""
userHomeDrive="U:"
userScript=""
mailDomain="justa.jus.br"

# Configuracões SMBLDAP-TOOLS
with_smbpasswd="0"
smbpasswd="/usr/bin/smbpasswd"
```

```
with_slappasswd="0"
slappasswd="/usr/sbin/slappasswd"
```

A.3 Arquivo smbldap_bind.conf

```
# Usuário definido como "admin users" no arquivo smb.conf
masterDN="uid=samba,ou=People,dc=justa,dc=jus,dc=br"

# Senha do usuário samba
masterPw="secret"
```

A.4 Arquivo slapd.conf

```
# Arquivos de schemas para atributos
include /etc/openldap/schema/core.schema
include /etc/openldap/schema/cosine.schema
include /etc/openldap/schema/inetorgperson.schema
include /etc/openldap/schema/nis.schema
include /etc/openldap/schema/samba.schema

# Arquivo de processo
pidfile /var/run/slapd.pid

# Banco de dados utilizado pelo LDAP
database ldbm

# Estrutura da árvore
suffix          "dc=justa,dc=jus,dc=br"

# Administrador do domínio
rootdn          "cn=Manager,dc=justa,dc=jus,dc=br"

# Senha de acesso do administrador
rootpw secret

# Local onde serão armazenados os arquivos da base
directory /var/lib/ldap
```

```
# Políticas de acesso
access to attrs=userPassword,sambaLMPassword,sambaNTPassword,
 sambaPwdLastSet,sambaPwdMustChange
   by anonymous auth
   by dn.base="cn=Manager,dc=justa,dc=jus,dc=br" write
   by dn="uid=samba,ou=People,dc=justa,dc=jus,dc=br" write
   by self write
   by * none

access to attrs=objectClass,entry,gecos,homeDirectory,
 uid,uidNumber,gidNumber,cn,memberUid
   by dn="uid=samba,ou=People,dc=justa,dc=jus,dc=br" write
   by * read

access to attrs=description,telephoneNumber
   by dn="uid=samba,ou=People,dc=justa,dc=jus,dc=br" write
   by self write
   by * read

access to attrs=cn,sambaLMPassword,sambaNTPassword,sambaPwdLastSet,
 sambaLogonTime,sambaLogoffTime,sambaKickoffTime,sambaPwdCanChange,
 sambaPwdMustChange,sambaAcctFlags,displayName,sambaHomePath,
 sambaHomeDrive,sambaLogonScript,sambaProfilePath,description,
 sambaUserWorkstations,sambaPrimaryGroupSID,sambaDomainName,
 sambaSID,sambaGroupType,sambaNextRid,sambaNextGroupRid,
 sambaNextUserRid,sambaAlgorithmicRidBase
   by dn="uid=samba,ou=People,dc=justa,dc=jus,dc=br" write
   by self read
   by * none

access to dn="ou=People,dc=justa,dc=jus,dc=br"
   by dn="uid=samba,ou=People,dc=justa,dc=jus,dc=br" write
   by * none

access to dn="ou=Group,dc=justa,dc=jus,dc=br"
   by dn="uid=samba,ou=People,dc=justa,dc=jus,dc=br" write
   by * none
```

```
access to dn="ou=Computers,dc=justa,dc=jus,dc=br"
   by dn="uid=samba,ou=People,dc=justa,dc=jus,dc=br" write
   by * none

access to *
   by dn.base="cn=Manager,dc=justa,dc=jus,dc=br" write
   by dn="uid=samba,ou=People,dc=justa,dc=jus,dc=br" write
   by * none

# Índices
index objectClass                       eq,pres
index ou,cn,mail,surname,givenname      eq,pres,sub
index uidNumber,gidNumber,loginShell    eq,pres
index uid,memberUid                     eq,pres,sub
index nisMapName,nisMapEntry            eq,pres,sub
index sambaSID                          eq
index sambaDomainName eq
index sambaPrimaryGroupSid              eq
index default sub
```

A.5 Arquivo `ldap.conf`

```
# Endereço do servidor LDAP
HOST 127.0.0.1

# DN base
BASE dc=justa,dc=jus,dc=br
```