

**Implantação em ambiente de Software Livre**  
**Servidor de Backup de Controladores de Domínio**  
(Implementando um BDC em redes com soluções de Software Livre)

Autor:

Rodrigo Pinheiro Matias

Apoio:

Secretaria do Trabalho e Desenvolvimento Social – Governo do Estado do Tocantins

Palmas, 11 de Outubro de 2007

# Sumário

1. Apresentação do Problema.....	4
2. Sobre o artigo.....	4
3. Definindo prioridades.....	4
3.1. Configurando a replicação do OpenLDAP.....	5
3.1.1. Schema.....	5
3.1.2. Backend de armazenamento.....	6
3.1.3. Base de armazenamento.....	6
3.1.4. Replicação da base de dados.....	8
3.2. Configurando o nsswitch.conf.....	9
3.2.1. Arquivo de conexão com servidor de OpenLDAP (ldap.conf).....	10
3.2.2. Configurando o /etc/nsswitch.conf.....	11
3.3. Preparando o Samba.....	12
3.3.1. Escutando o Samba falar.....	12
3.3.2. Colocando a mão na massa smb.conf.....	13
3.3.2.1. Instalando os pacotes necessários.....	13
3.3.2.2. Detalhes da configuração.....	14
4. Conclusão.....	15

## 1. Apresentação do Problema

Inicialmente temos que na matriz existe um servidor de autenticação em pleno funcionamento que usa de uma base de dados localizada em um servidor LDAP para autenticar os usuários da rede da matriz. Com o passar do tempo observou-se que existia uma necessidade crescente das filiais terem autenticadores próximos, uma vez que as VPNs ou as antenas caem todos os serviços que dependem da rede ficam prejudicados.

Assim optou-se pela instalação de um servidor de domínio de backup para ficar dentro das redes das filiais, assim quando a estrutura de ligação entre as filiais cair o serviço de rede fica parcialmente prejudicado e não completamente.

## 2. Sobre o artigo

Primeiro iremos definir o que é prioridade para o funcionamento deste esquema e depois partiremos para configuração em si. Como todos sabem o Ubuntu conta com um sistema de gerenciamento de pacotes que oferece uma gama de vantagens, mas este mesmo procedimento pode ser aplicado em qualquer outra distribuição seja ela descendente do Debian ou não.

## 3. Definindo prioridades

A primeira situação que deve ser enfrentada é no que diz a respeito da replicação da base de dados, pois, na matriz existe a base de dados de usuário assim como a relação de grupos e equipamentos, isto deve ser replicado(slurp), depois temos que fazer o nosso servidor que ficar na filial reconhecer os usuários desta base (libnss-ldap), com este esquema funcionando temos que fazer com que as máquinas passem a autenticar no servidor Samba que esta na filial (Samba+SambaLdapTools). Fechando estas configurações teremos o nosso ambiente corporativo totalmente funcional.

Observação: Devida as grades dimensões dos textos iremos postar em partes este artigo, no final irei juntar tudo em um unico arquivo do tipo PDF que será disponibilizado neste blog.

### 3.1. Configurando a replicação do OpenLDAP

Primeiramente temos que instalar os pacotes necessários para o servidor de OpenLDAP funcionar, com o comando:

```
root@gw:~# apt-get install slapd ldap-utils db4.2-util libpam-ldap  
libnss-ldap nscd libpam-foreground
```

Com a instalação deste pacotes o Debconf deve fazer alguns questionamentos, caso esteja usando outra distribuição, algo equivalente deve ocorre ou deve ser gravado o arquivo de configuração default.

Então vamos começar com a edição do arquivo de configuração do nosso OpenLdap Server, no caso do Ubuntu ele usa um esquema de armazenamento de arquivos de configuração bem eficiente. (Os arquivos deste servidor se encontram em /etc/ldap/) familiarizando os serviços aos seus locais de configuração.

#### 3.1.1. Schema

Os esquemas serverem para dizer ao servidor de ldap como se dar com os tipos de dados, eles servem também para definir entidades e suas dependências, por exemplo para preparar o LDAP para receber o samba tempos que ter os seguintes esquemas: NIS, SAMBA e QMAIL.

O arquivo de configuração (/etc/ldap/slapd.conf) ficaria mais ou menos assim:

```
include /etc/ldap/schema/core.schema  
include /etc/ldap/schema/cosine.schema  
include /etc/ldap/schema/inetorgperson.schema  
include /etc/ldap/schema/nis.schema  
include /etc/ldap/schema/samba.schema  
include /etc/ldap/schema/qmail.schema
```

Agora que o LDAP sabe lhe dar com os tipos de dados podemos prosseguir com a configuração do arquivo slapd.conf.

### 3.1.2. Backend de armazenamento

Na sequência vamos dizer ao servidor que tipo de banco de dados ele deve usar, existem diversos tipos para saber mais entre no site do OpenLDAP, iremos usar o db4 como banco de dados então veja como deve ficar o arquivo de configuração:

```
modulepath /usr/lib/ldap
moduleload back_bdb
backend bdb
checkpoint 512 30
```

A primeira linha diz onde estão os módulos do OpenLDAP; a segunda linha diz para ele carregar o módulo back\_bdb, que é o backend para usar o db4; na terceira linha informamos o backend; por final colocamos as informações de checkpoint, que será usado pelo db4, no caso informamos que é para ele usar folhas de dados de 512 bytes e realizar checkpoints a cada 30 minutos.

Basicamente a infra estrutura do banco de dados está feita, agora vamos passar para o formato do banco de dados em sí.

### 3.1.3. Base de armazenamento

Primeiramente teremos que definir a raiz de armazenamento do nosso servidor de usuários, usualmente costuma-se usar o domínio da empresa como base, por exemplo vamos tomar que temos uma empresa que é dona do domínio matriz.com então esta definição ficaria assim:

```
suffix "dc=matriz,dc=com"
```

Com isto temos que definir a política de acesso root, ou seja um usuário com privilégios para administrar isto tudo, isto se faz da seguinte forma:

```
password-hash {MD5}
rootdn "cn=suporte,dc=matriz,dc=com"
rootpw {MD5}7gyEANJPvIWkc7KKFow3UQ==
```

Na primeira linha definimos que será usado o MD5 como hash da senha, na

segunda linha onde definimos o rootdn dizemos a nossa raiz que o cn=suporte é o nosso usuário. Logo na linha seguinte onde definimos o rootpw informamos ao servidor que senha usar para dizer que o usuário cn=suporte é realmente o usuário cn=suporte.

Aqui nos temos um detalhe muito importante, esta senha deve ser gerada com o auxílio do slappasswd, veja o exemplo:

```
slappasswd -h {MD5}
```

Será questionado qual é a senha e depois uma confirmação da mesma. Já configuramos a forma de entrar na base agora vamos configurar a forma como o OpenLDAP deve organizar a informação para um melhor desempenho de busca. Veja o nosso exemplo:

```
index objectClass,uidNumber,gidNumber eq
index cn,sn,uid,displayName pres,sub,eq
index
memberUid,mail,mailAlternateAddress,givenname,accountStatus,mailHost,d
eliveryMode eq
index sambaSID,sambaPrimaryGroupSID,sambaDomainName eq
index default sub
```

Agora já definimos como será a indexação que é simples; a ordem de indexação é de cima para baixo e da esquerda para a direita. Neste momento vamos ver como ficaria o acesso a estas informações, quem pode acessar, veja o exemplo abaixo:

```
access to attrs=userPassword,sambaLMPassword,sambaNTPassword
by self write
by anonymous auth
by * none
```

O acesso aos atributos userPassword,sambaLMPassword e sambaNTPassword é dado somente aos donos das contas, se um anonimo tentar acessar deverá ser autenticado e todos os outros não tem acesso. No exemplo abaixo ainda dizemos que o acesso aos demais campo para todos é de somente leitura, isto é bom para replicação.

```
access to *
```

by \* read

### 3.1.4. Replicação da base de dados

Bom já temos uma base funcionando faltando somente os dados. Para isto iremos parar o servidor na matriz para fazer um backup dos dados, este backup será usado para dar uma carga inicial no OpenLDAP da filial. No servidor da matriz execute o seguinte comando:

```
slapcat -b "dc=matriz,dc=com" -l backup.ldif
```

Feito isto será gerado um arquivo chamado backup.ldif no diretório corrente, então você deve copiar este arquivo para o servidor da filial e executar o seguinte comando:

```
slapadd -l backup.ldif
```

Com isto devemos ter uma réplica do banco de dados da matriz dentro do servidor da filial, ainda não devemos iniciar nenhum dos dois servidores. Agora temos que preparar o servidor da matriz para replicar os dados na filial. Para isto iremos inserir as seguintes linhas no arquivo /etc/ldap/slapd.conf da matriz.

```
replica host=<host>:389  
binddn="cn=suporte,dc=matriz,dc=com"  
bindmethod=simple  
credentials=senha  
tls=no
```

Você já deve ter se familiarizado com as informações a única novidade aí são as palavras `bindmethod` que diz que a autenticação será feita do modo simplificado usando apenas OpenLDAP, `credentials`, que é a senha que será usada para autenticar o usuário `cn=suporte,dc=matriz,dc=com` no servidor especificado como `<host>` o qual deve ser o servidor da matriz e a última linha que diz para não usar `tls` este último fica como projeto futuro, que seria colocar as transações para ocorrer sobre um socket criptografado.

Agora devemos informar ao servidor da filial quem é a base oficial, para que ele aceite as alterações e também para ele saber onde devem ser feitas as alterações solicitadas

pelos usuários da rede filial, veja o exemplo logo abaixo, /etc/ldap/slapd.conf da filial:

```
updatedn "cn=suporte,dc=matriz,dc=com"  
updateref ldap://<host matriz>:398
```

Na primeira linha estamos dizendo para ele usar o usuário master de acesso a base do servidor da matriz; na segunda linha estamos informando qual é o endereço para encontrar o servidor matriz, é importante colocar IP absoluto para evitar erro por falha de DNS. Veja que foi omitido a senha do usuário master na matriz isto se deve porque o slurp no servidor matriz faz uma conexão usando credenciais pre-aprovadas devido o fato do servidor matriz reconhecer o servidor filial como um nó de si mesmo. Não exponha isto desta forma na internet faça um controle do acesso antes.

Bem pessoal por hoje ficamos por aqui, no próximo artigo que irei escrever neste final de semana vou explicar como colocar o servidor da rede filial para reconhecer os usuários cadastrados no ldap como usuários do sistema linux, passo importante para que o samba possa autenticar no LDAP. Pretendo postar este próximo artigo neste final de semana.

### **3.2. Configurando o nsswitch.conf**

Boa tarde pessoal, hoje vamos fazer com que o nosso sistema operacional passe a reconhecer os usuários e os ID's do mesmos, para que possam criar arquivos, executar processos, entre outras tarefas que cabem permissões no Linux.

Como todos sabem o SAMBA usa as permissões de seus usuários para criar arquivos e conexões com o servidor de dominio, no caso os PDC's (Primary Domain Control) e os BDC's (Backup Domain Control), por este motivo temos que ter o nosso sistema operacional mãe autenticando com os mesmos usuários que o nosso samba autentica, e com uma particularidade os IDs dos grupos e usuários devem bater, para resolver isto podemos concentrar toda a autenticação no nosso OpenLDAP e hoje falaremos de como fazer isto no sistema operacional \*NIX.

### 3.2.1. Arquivo de conexão com servidor de OpenLDAP (ldap.conf)

Este arquivo de configuração fica localizado no caso do Ubuntu /etc/ldap/ldap.conf mas também pode ser localizado pelo comando `find / -name ldap.conf` neste arquivos temos definições de como o nsswitch-ldap fará pra localizar os usuários no servidor de ldap que pode ser local ou remoto. Veja as linha logo abaixo.

```
uri ldap://<host da filia>
base dc=matriz,dc=com
binddn cn=suporte,dc=matriz,dc=com
bindpw senhasecreta
```

Veja na primeira linha vamos especificar aquele servidor de ldap que criamos anteriormente, depois na linha seguinte adicionamo a informação onde esta esta a base de nomes e grupos do sistema, na terceira linha passamos o usuário master do servidor de ldap e por ultimo colocamos a senha do servidor.

Importante: Todos os arquivos que contiver informações secretas como password deve ser aplicada regras de acesso para que usuários mal intencionados tenham mais dificuldades para ler tais arquivos, para isto execute este comando:

```
chmod 600 <arquivo>
```

Tomando este cuidado você torna mais confiável o funcionamento de todo o conjunto.

### 3.2.2. Configurando o /etc/nsswitch.conf

Basicamente este arquivo é responsável por montar o esquema de reconhecimento de varias informações importantes para o sistema operacional, e duas delas nos importam muito hoje, são elas: password e group; estes dois são responsáveis pela a autenticação do nosso sistema operacional mãe.

No caso do ubuntu este arquivo se encontrara desta forma:

```
...
passwd: compat
```

```
group: compat
```

```
...
```

Veja desta forma ele está autenticando não somente nos arquivos locais, /etc/passwd e /etc/group com as modificações que serão feitas ele passará a autenticar tanto nestes arquivos quanto no ldap. Mas antes vamos executar um teste.

Pegue um usuário antigo que você sabe que tem no seu PDC e não tem no seu BDC, pelo menos não nos arquivos citados anteriormente, execute o seguinte comando:

```
id USUARIO
```

O sistema operacional não vai conseguir encontrar este usuário e retornará uma mensagem de erro, mas agora iremos modificar o /etc/nsswitch.conf para que isto não mais ocorra, veja as próximas linhas:

```
passwd: ldap compat
```

```
group: ldap compat
```

Agora execute o comando executado anteriormente só que no seu PDC veja o resultado, agora execute o mesmo comando no seu BDC e surpresa o mesmo resultado, isto diz que seu BDC está sincronizado com o seu PDC.

Bem pessoal por hoje é só, o próximo artigo será escrito na segunda-feira então fiquem atentos, uma boa para acompanhar é usar o feed do site, no caso de quem usa o Mozilla Firefox fica um ícone no final da barra de endereço.

### **3.3. Preparando o Samba**

Bem pessoal aqui neste ponto eu tive alguns problemas, mas tudo pode ser resolvido escutando o samba falando comigo, isto foi possível graças a uma ferramenta muito conhecida entre nós administradores de redes.

#### **3.3.1. Escutando o Samba falar**

No arquivo de configuração do samba /etc/samba/smb.conf possui um conjunto de parâmetros globais que é responsável por definir ao servidor de autenticação samba do que

ele deve relatar e onde ele deve relatar os acontecidos durante a execução dos processos, o principal destes parâmetro é o que define onde estes arquivos são gravados, (log file = /var/log/samba/log.%m).

Agora que sabemos onde fica os arquivos de log podemos escolher uma maquina qualquer e tentar acessar o nosso BDC, isto fará com que esta comunicação gere uma serie de linhas que agora podem ser acompanhados com a ajuda do comando tail, por exemplo digamos que escolhemos a maquina DOT01 logo será gerado log.DOT01, veja como poderíamos acompanhar a conexão entre este servidor e esta máquina.

```
tail -f /var/log/samba/log.DOT01
```

```
.  
.  
.
```

Todos os erros que ocorrerem durante a comunicação entre as duas máquinas será relatado na tela do console. Ainda temos o testparm que e uma ferramenta do samba que checa a syntax e a semantica do arquivo de configuração e gera um resumo da configuração.

### 3.3.2. Colocando a mão na massa smb.conf

Aconselho que todos mantem todos os processos do samba, para identificar se estes processos estão ativos então execute o seguinte comando:

```
ps aux | grep smbd
```

```
.  
.  
.
```

Se você verificar que existe algum processo sendo executado então execute o comando killall smbd, isto fará com que todos os processos sejam mortos, caso isto não ocorra o seu samba esta rodando como um processo inet.d veja como parar estes processos consultado o manual do seu sistema operacional.O mesmo procedimento deve ser feito para outros dois programas, nmbd e o winbind, este ultimo geralmente não é instalado por padrão.

### 3.3.2.1. Instalando os pacotes necessários

Bem pessoal primeiramente temos que ter os seguintes pacotes: samba, samba-common, samba-doc, swat e o openbsd-inet, além dos pacotes do samba podemos ver que temos o swat e o script de boot, o inet do openbsd, este pacote será responsável por inicializar o processo do swat já este ultimo é uma interface de manipulação do arquivo de configuração do samba. Então vamos por a mão na massa:

```
apt-get install samba samba-common samba-doc swat openbsd-inet
```

Após a instalação o processo de instalação o processo do samba será inicializado, repita o procedimento 3.3.2 mas se tiver com o ubuntu execute o comando `/etc/init.d/samba stop` isto deve bastar para parar os processo do servidor, mas agora temos um samba com as configurações de fábrica e ainda um frontend para manipular este arquivo. Para verificar se o seu swat este em execução tente acessar `http://localhost:901` será pedido a senha do root, entre com a mesma e terá acesso ao frontend de configuração.

### 3.3.2.2. Detalhes da configuração

Este artigo é destinado a leitores que já tem algum conhecimento sobre o samba uma vez que o mesmo deve conhecer como é o funcionamento deste conjunto de autenticação, logo deve ser de conhecimento do leito que é dever dele saber como colocar sua máquina para ficar com as características de seu domínio, aqui será relatado somente as configurações particulares de um BDC.

```
workgroup = MATRIZ_COM
passdb backend = ldapsam:ldap://localhost
domain master = no
domain logons = yes
ldap suffix = dc=matriz,dc=com
ldap user suffix = ou=usuario
ldap group suffix = ou=grupo
ldap machine suffix = ou=computador
ldap idmap suffix = ou=Idmap
ldap admin dn = cn=suporte,dc=matriz,dc=com
idmap backend = ldap:ldap://localhost
idmap uid = 10000-20000
```

```
idmap gid = 10000-20000
```

```
[netlogon]  
directory = /home/logons  
browsable = no  
read only = yes
```

Já definimos a configuração do nosso BDC, veja que você pode modificar outros detalhes, mas o que é importante é que estes parâmetros devem ficar desta forma claro que com os valores adequados a sua rede, mas veja que estamos usando o servidor de LDAP que foi replicado anteriormente isto é importante.

Antes de iniciarmos o processo do nosso samba vamos o informar qual a senha do usuário master do LDAP isto pode ser feito usando o seguinte comando:

```
smbpasswd -W
```

... a senha será solicitada no final do processo deve ser retornado com o valor da variável ldap admin dn isto indica que o samba já guardou a senha no banco de senhas, então já podemos iniciar o processo do samba. Execute o comando:

```
/etc/init.d/samba start
```

Bom lembra das máquinas windows, elas tinham que entrar no domínio, o mesmo tem que acontecer com o nosso BDC, no windows tem um procedimento gráfico simples, no caso do samba este processo também é muito simples, basta executar o seguinte comando:

```
net rpc join MATRIZ_COM -U administrador
```

A senha de administrador será solicitada caso não ocorra nenhum erro então teremos um BDC em pleno funcionamento. Caso exista algum script de logon para os usuários então deve ser feito uma sincronização dos arquivos de logon.

## 4. Conclusão

Bem pessoal como podemos ver o problema de distancia entre as filiais e a matriz

pode ser solucionado com a criação de autenticadores de backup, apesar do procedimento não ser tão simples de ser executado ele é eficaz e ajuda em momentos onde há problemas de comunicação entre as filiais e a matriz.