Autenticação centralizada usando OpenLDAP e exemplos com Samba e Linux

Mario Luiz Bernardinelli
mariolb@gmail.com

22 de outubro de 2012

v1.6

A autenticação centralizada evita vários problemas enfrentados por usuários e administradores: memorização de várias contas (e senhas) e o gerenciamento de contas, respectivamente.
No GNU/Linux, é possível implementar a autenticação centralizada usando o OpenLDAP. Este documento foi escrito usando um ambiente com GNU/Linux e Samba (operando como PDC), ambos autenticando diretamente no serviço OpenLDAP.
Como o intuito é fornecer o caminho das pedras para uma configuração básica, questões como *backup*, replicação de dados e suporte ao SSL/TLS, todas suportadas pelo OpenLDAP, não são abordadas neste documento.

1. Introdução

A diversidade de tipos de serviços disponíveis numa rede, seja ela de qualquer tamanho, tende a crescer com tempo. Novas necessidades surgem a todo momento e novos serviços são disponibilizados nas redes.

Muitos destes serviços requerem a autenticação de usuários, por exemplo, o que obriga num primeiro momento, que sejam criadas contas para cada indivíduo em cada um destes serviços. Duplicidade de dados duplicadas surgem em decorrência disso. O trabalho e a complexidade na administração destes ambientes cresce quase que exponencialmente.

A integração de diversos ambientes, de diferentes fabricantes e tecnologias nem sempre é fácil ou mesmo possível. O LDAP é um protocolo de acesso à diretórios que permite a centralização de dados, permitindo que diversos sistemas consultem bases de dados centralizadas, eliminando problemas de duplicidade de dados.

O *software* discutido aqui é o OpenLDAP, que é uma implementação *open source* do LDAP que pode ser executada em ambientes GNU/Linux.

O OpenLDAP possui diversas características muito interessantes, tais como replicação de dados, suporte SSL/TLS. Neste documento serão apresentadas as configurações básicas do serviço LDAP para integrá-lo com o GNU/Linux e Samba. Questões como replicação de dados e uso de SSL/TLS, que é imprescindível para a segurança do sistema, não serão discutidas aqui. Estes assuntos serão deixados para uma versão futura deste artigo, ou até mesmo, um artigo específico para isso.

Como este documento é mais um *how to* (como fazer) do que um artigo propriamente dito, muitas das configurações aqui apresentadas seguiram sugestões apresentadas por (SUNGAILA, 2008) e (OPENLDAP, 2011).

Notas:

- Windows, MS-Windows e Microsoft Windows são marcas registradas da Microsoft Corporation.

2. LDAP: configuração tradicional versus configuração online

A forma tradicional de configuração do OpenLDAP consiste em adicionar os parâmetros de configuração num único arquivo, normalmente o `slapd.conf`. Esta forma de configuração tem seus prós e contras. Um dos prós é que torna a configuração mais fácil de entender. Por outro lado, o contra é que toda vez que a configuração é alterada, o serviço deve ser reiniciado para que as alterações sejam carregadas.

Uma nova forma de configuração foi criada para resolver este problema, conhecida como *runtime configuration* ou simplesmente `cn=config`. Esta forma permite que o administrador altere os parâmetros em tempo de execução, ou seja, as alterações são carregadas sem que o serviço tenha que ser totalmente reiniciado.

Na configuração baseada no `cn=config`, os parâmetros são carregados em memória seguindo o formato DIT (*Directory Information Tree*), que é uma árvore. A grande vantagem disso é que esta árvore de parâmetros é similar à qualquer outra árvore da base de dados do LDAP, permitindo que os parâmetros sejam alterados utilizando-se a mesma interface de utilizada para acesso às bases de dados. Isto permite que as configurações sejam alteradas utilizando arquivos no formato LDIF e que as mesmas sejam assumidas imediatamente após a carga e/ou alteração, sem a necessidade de reinicialização do serviço LDAP.

Segundo a documentação, esta nova forma de configuração tornou-se disponível à partir da versão 2.3 do OpenLDAP. na versão 2.4 do OpenLDAP, esta configuração ainda é opcional, mas a tendência é que ela passe a ser padrão nas próximas versões, inclusive, podendo substituir completamente a configuração tradicional (`slapd.conf`).

Alguns cuidados devem ser tomados no uso do novo formato de configuração:

- Como trata-se de um formato novo, o suporte ainda está incompleto. Por exemplo, a remoção de configurações ainda exige a reinicialização do serviço.
- As alterações têm efeito imediato, então, é preciso muito cuidado ao alterar as ACLs (*Access Control List*).
- Uma vez gerada a configuração no formato `cn=config` (o pacote OpenLDAP trás uma ferramenta capaz de fazer isto), não há nenhuma ferramenta que converta o formato `cn=config` novamente para o formato `slapd.conf`.

2.1. cn=config: estrutura

Vejamos a estrutura de um diretório de configuração no formato `cn=config` armazenado em `/etc/ldap/slapd.d`:

```
/etc/ldap/slapd.d/
+-- cn=config
|   +-- cn=module0.ldif
|   +-- cn=schema
|   |   +-- cn=0core.ldif
|   |   +-- cn=1cosine.ldif
|   |   +-- cn=2nis.ldif
|   |   +-- cn=3inetorgperson.ldif
|   |   +-- cn=4samba.ldif
|   |   +-- cn=5autofs.ldif
|   +-- cn=schema.ldif
|   +-- olcDatabase=0config.ldif
|   +-- olcDatabase=1bdb.ldif
|   +-- olcDatabase=-1frontend.ldif
+-- cn=config.ldif
```

Observe que todos os arquivos de configuração agora estão no formato LDIF, que é um formato texto no qual os parâmetros (ou atributos) são separados de seus valores pelo caractere dois pontos.

O arquivo `cn=config.ldif` contém as configurações globais que antes eram armazenadas no arquivo slapd.conf. Todos os atributos usados pelo OpenLDAP possuem o prefixo "olc"(*OpenLDAP Configuration*).

Alguns arquivos e/ou diretórios possuem também números, como por exemplo, `cn=0core.ldif`, que é uma forma de indicar a ordem de carregamento do arquivo.

O conteúdo básico do diretório de configuração é o seguinte:

- **cn=config.ldif:** Contém os parâmetros globais de configuração.
- **cn=config:** Contém os arquivos e/ou diretórios com as demais configurações.
- **cn=module{NUMERO}:** Armazena a configuração de um módulo, o que equivale ao parâmetro `moduleload` do arquivo slapd.conf. Observe que, para cada módulo adicionado, deve ser criado um

novo arquivo com um número diferente dos demais. Este número irá indicar a ordem de carregamento do módulo.

- **cn=schema:** Neste diretório ficam armazenados os *schemas* utilizados.
- **olcDatabase={-1}frontend.ldif:** é uma base de dados especial que contém as configurações que serão aplicadas à todas as demais bases de dados. Se uma diretiva deste arquivo for repetida na configuração da base de dados específica, valerá o valor especificado na configuração específica da base. Portanto, os parâmetros aqui especificados podem ser considerados valores padrões que, se não forem reconfigurados nas configurações específicas, serão utilizados como definidos aqui.
- **olcDatabase={NÚMERO}[backend].ldif:** Definição da base de dados específica. Os valores aqui definidos podem sobrescrever os valores definidos globalmente. O `olcDatabase` de número zero (0) é o próprio `cn=config`.

3. Instalando os pacotes

Vamos fazer a instalação dos pacotes necessários em quatro etapas, a saber:

- Pacotes para o serviço LDAP
- Pacotes para a autenticação do Linux (contas POSIX)
- Servidor Samba
- Pacotes para a manipulação de base de dados LDAP para autenticação de estações Windows©(Samba) e POSIX (Linux)

Este documento é baseado em sistemas Debian, porém, o ambiente de teste utilizado foi um Ubuntu. Se você estiver usando o Ubuntu, instale primeiro o `aptitude`:

```
apt-get install aptitude
```

Ou, se preferir, utilize o `apt-get` para instalar os *softwares* apresentados a seguir.

Vamos partir para a instalação dos softwares.

3.1. Pacotes para o serviço LDAP

Estes pacotes só devem ser instalados no servidor de autenticação. Durante a instalação dos pacotes a seguir, serão solicitadas algumas informações como senha do administrador e nome do domínio da empresa. Preencha com qualquer valor, ou assuma os valores padrões (se apresentados), pois iremos reconfigurar todo o sistema manualmente, para entendermos o funcionamento com detalhes.

```
aptitude install slapd ldap-utils
```

3.2. Pacotes para autenticação de clientes Linux no LDAP

```
aptitude install libpam-ldap libnss-ldap ldap-utils nscd
```

Nota: o pacote `nscd` só tem utilidade para máquinas Linux clientes.

3.3. Pacotes para o serviço Samba

```
aptitude install samba samba-client
```

3.4. Pacotes de ferramentas

O `smblda-tools` contém ferramentas para manipular contas Windows©e POSIX e suporte à criação de base de dados LDAP para contas Windows©(Samba) e POSIX (Linux).

```
aptitude install smbldap-tools
```

4. Configuração do LDAP

Nesta etapa iremos configurar o LDAP com as configurações necessárias para a criação das bases de dados de autenticação POSIX e Windows©(Samba).

Antes de iniciarmos o processo, devemos ter em mãos algumas informações: precisamos do nome do domínio da empresa e de uma senha para o administrador do serviço LDAP. Vamos utilizar os seguintes valores:

- Domínio da empresa: EMPRESA
- Senha do administrador: (invente uma senha que seja forte)

As versões mais atuais do OpenLDAP utilizam um mecanismo de configuração baseado em inúmeros arquivos e diretórios armazenados normalmente em */etc/ldap/slapd.d*. Utilizaremos, porém, a forma convencional de configurar o OpenLDAP, que utiliza apenas um arquivo de configuração. Depois de criado o arquivo de configuração, utilizaremos uma ferramenta do próprio OpenLDAP que faz as conversões necessárias.

Precisaremos criar uma senha para o administrador da base LDAP e adicionar o seu *hash* no arquivo de configuração (onde indicado pelo parâmetro `rootpw`). Para criar o *hash* da senha, utilize o comando `slappasswd` a seguinte forma:

```
slappasswd
New password:
Re-enter new password:
SSHAolrVkiKDx4P/omI55IatjsVQMfFUSZln
```

Adicione a linha contendo o *hash* no parâmetro `rootpw` do arquivo de configuração.

A configuração do OpenLDAP deve ser realizada através do arquivo `/etc/ldap/slapd.conf`. O exemplo a seguir apresenta as configurações básicas para a autenticação Windows©(Samba) e POSIX. Observe, no entanto, que o nome da empresa (domínio) deve ser alterado em função das suas necessidades (veja o parâmetro `rootdn` no arquivo de configuração). O exemplo apresentado já contempla as configurações necessárias para autenticação de contas POSIX e Samba.

```
# ----------- /etc/ldap/slapd.conf
# slapd.conf
#
# EMPRESA
#

# Protocol version
allow bind_v2


# Schemas
include /etc/ldap/schema/core.schema
include /etc/ldap/schema/cosine.schema
```

```
include /etc/ldap/schema/nis.schema
include /etc/ldap/schema/inetorgperson.schema
include /etc/ldap/schema/samba.schema

# X.509 certificate
#TLSCipherSuite HIGH:MEDIUM:+SSLv2:RSA
#TLSCipherSuite       HIGH:MEDIUM:-SSL2:+RSA
#TLSCipherSuite       +AES-256-CBC:+AES-128-CBC:+SHA256:+RSA
#TLSCertificateFile    /etc/ldap/ssl/certs/ldap.pem
#TLSCertificateKeyFile /etc/ldap/ssl/certs/ldap.key

# Process control files
pidfile  /var/run/slapd/slapd.pid
argsfile /var/run/slapd/slapd.args

# Modules
modulepath /usr/lib/ldap
moduleload back_bdb

# Backend type
backend bdb

# Database type
database bdb

# No limit for retrieving records
sizelimit unlimited

# Directory structure and management
suffix "dc=EMPRESA"
rootdn "cn=admin,dc=EMPRESA"
rootpw SSHAolrVkiKDx4P/omI55IatjsVQMfFUSZln

# Database directory (storage)
directory /var/lib/ldap

# Search indexes
index objectClass                                 eq
index cn,sn,givenName                             eq,sub,approx
index mail                                        eq,sub
index uid,uidNumber,gidNumber,memberUid,loginShell eq
index default                                     eq,sub
index sambaSID                                    eq
index sambaPrimaryGroupSID                        eq
index SambaDomainName                             eq

# ACLs

# Root dir access
access to dn.exact=""
  by * read

# Password access control (TLS)
#access to attrs=userPassword,sambaLMPassword,sambaNTPassword
#  by anonymous ssf=56 auth
#  by self ssf=56 write
#  by * none

# Password access control (without TLS)
```

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

# Password changes date and time
access to attrs=shadowLastChange
  by self write
  by * none

# Global access
access to *
  by * read
```

Como este arquivo já contempla as configurações necessárias para o Samba, precisamos adicionar ao diretório `/etc/ldap/schema` o esquema da base de dados do Samba. Este esquema acompanha o pacote do Samba e devemos copiá-lo manualmente. Execute os seguintes comando para fazer isso:

```
cd /etc/ldap/schema/
cp /usr/share/doc/samba/examples/LDAP/samba.schema.gz .
gunzip samba.schema.gz
```

Agora, vamos parar o serviço LDAP:

```
root@server # invoke-rc.d slapd stop
Stopping OpenLDAP: slapd.
```

Como estamos configurando o LDAP do zero, vamos remover a base de dados atual:

```
rm -f /var/lib/ldap/*
```

Agora vamos criar o arquivo `/var/lib/ldap/DB\_CONFIG`, que contém configurações específicas para base dados e que deve sempre ser mantido no diretório da base de dados LDAP (`/var/lib/ldap`):

```
#-----/var/lib/ldap/DB_CONFIG
set_cachesize 0 2097152 0
set_lk_max_objects 1500
set_lk_max_locks 1500
set_lk_max_lockers 1500
```

Agora vamos alterar as permissões do arquivo, já que o LDAP deve poder lê-lo:

```
chown openldap:openldap /var/lib/ldap/*
```

Agora vamos converter a configuração do OpenLDAP para o novo formato. Devemos criar o diretório de configuração. Antes disso, porém, vamos remover o diretório existente, se existir:

```
rm -rf /etc/ldap/slapd.d
mkdir /etc/ldap/slapd.d
```

Para evitar confusões futuras, vamos renomear o arquivo de configuração do OpenLDAP para ficar claro que o sistema não utiliza este arquivo, mas sim as configurações especificadas no diretório `/etc/slapd.d`:

```
mv slapd.conf slapd.conf.old
```

Para converter o arquivo de configuração `slapd.conf.old` para o novo formato, vamos utilizar o aplicativo `slaptest`, que é parte do OpenLDAP:

```
slaptest -f slapd.conf.old -F /etc/ldap/slapd.d
bdb_db_open: database "dc=EMPRESA": db_open(/var/lib/ldap/id2entry.bdb) failed:
No such file or directory (2).
backend_startup_one (type=bdb, suffix="dc=EMPRESA"): bi_db_open failed! (2)
slap_startup failed (test would succeed using the -u switch)
```

Observe que ocorreram alguns erros, que são esperados, porque a base de dados ainda não existe.

Como executamos os comandos como `root` e o OpenLDAP é executado por um usuário de privilégios reduzidos (`openldap`, no caso do Debian), devemos alterar as permissões dos arquivos da base de dados e de configuração:

```
chown openldap:openldap /var/lib/ldap/*
chown -R openldap:openldap /etc/ldap/slapd.d
```

Edite o arquivo `/etc/default/slapd` e procure pelo parâmetro `SLAPD_CONF` e deixe-o em branco (se já não estiver):

```
#---- trecho do arquivo /etc/default/slapd
...
SLAPD_CONF=
...
```

Isto irá garantir que o `slapd` utilizará o novo formato de configuração que está em `/etc/slapd`.

Vamos iniciar o serviço LDAP:

```
invoke-rc.d slapd start
 * Starting OpenLDAP slapd                                                    [ OK ]
```

Verifique se o serviço está em execução:

```
netstat -ntpul | grep slap
tcp     0  0 0.0.0.0:389    0.0.0.0:*   LISTEN   3415/slapd
tcp6    0  0 :::389         :::*        LISTEN   3415/slapd
```

Atenção:

- Sempre que remover uma base da dados LDAP, **antes** de iniciar o `slapd` o arquivo `DB_CONFIG` deve ser criado no diretório `/var/lib/ldap`.
- Sempre que a base de dados LDAP for removida, inicie o serviço `slapd` **antes** de tentar reindexá-la, para que a base, mesmo que vazia, seja efetivamente criada.
- Sempre que a base de dados for reindexada, devemos alterar o proprietário dos arquivos, pois a indexação é realizada como `root`, mas o serviço LDAP no Debian é sempre executado como um usuário sem privilégios administrativos (usuário `openldap` e grupo `openldap`). A base de dados pode ser reindexada através do comando `slapindex`.

Como nossa base de dados está vazia, não há necessidade de reindexá-la.

4.1. Restaurar a base de dados

Se você estiver substituindo ou instalando um servidor de *backup*, é bem provável que você tenha uma cópia da base de dados LDAP do servidor outro servidor.

Se o outro servidor estiver em operação, você pode fazer uma cópia de segurança da base de dados e restaurá-la agora.

Basicamente, há várias formas de fazer o *backup* da base de dados LDAP:

- Copiar os arquivos do diretório `/var/lib/ldap`, incluindo os arquivos de *log* contidos neste mesmo diretório, pois estes arquivos contém as informações de transações realizadas.
- Realizar um *dump* da base de dados em arquivo texto para posterior recuperação. neste caso, apenas o *dump* será necessário para a recuperação.

O ideal é fazer o *backup* pelos dois métodos (o seguro morreu de velho :)).

O *dump* da base pode ser realizado pelo comando `ldapsearch`, mas há alguns problemas:

- Como a base é acessada em tempo de execução (*online*), as restrições de consulta e acesso serão aplicadas e, portanto, será necessário o uso da conta de administrador da base para a execução do *backup*.
- O número de linhas retornado pelo comando `ldapsearch` é limitado, por padrão, e isto pode inviabilizar o seu uso em bases grandes. Para contornar este problema, deve ser inserido o seguinte parâmetro nos arquivos `/etc/ldap/ldap.conf` e `/etc/ldap.conf`:

```
SIZELIMIT 0
```

Além disso, o seguinte parâmetro deve ser configurado no arquivo `/etc/ldap/slapd.conf`:

```
sizelimit unlimited
```

Uma segunda forma de realizar o *dump* da base LDAP é usar o comando `slapcat`. Este utilitário acessa diretamente os arquivos da base de dados, não tendo nenhuma interferência das ACLs definidas. Ele pode ser usado com o *slapd* em execução, mas o prórpio manual sugere que é melhor que o *slapd* não esteja em execução no momento do *backup*, a fim de evitar inconsistências caso ocorram operações de escrita na base durante a execução da cópia de segurança.

Em linhas gerais, o *backup* com o `slapcat` pode ser executado da seguinte forma:

```
invoke-rc.d slapd stop
slapcat -l ARQUIVO_DE_BACKUP.ldif
invoke-rc.d slapd start
```

Em linhas gerais, o *dump* gerado pelo `slapcat` não pode ser utilizado como entrada para o comando `ldapadd`, pois o *dump* é realizado na ordem dos registros na base, e não na ordem da estrutura de diretórios. A base de dados pode ser reconstruída (restaurada) usando o comando `slapadd` (observe que não é o `ldapadd`).

Para restaurar a base de dados no servidor novo, execute os seguintes comandos (observe que o serviço deve ser encerrado antes da restauração):

```
invoke-rc.d slapd stop
slapadd -g -F /etc/ldap/slapd.d -q -b dc=EMPRESA -l ARQUIVO_DE_BACKUP.ldif
```

Antes de iniciar o serviço, altere as permissões dos arquivos de configuração e base de dados:

```
chown openldap:openldap /var/lib/ldap/*
chown -R openldap:openldap /etc/ldap/slapd.d
```

Agora o serviço *slapd* pode ser iniciado:

```
invoke-rc.d slapd start
```

Para testar se a base de dados foi restaurada, podemos usar o comando `ldpapsearch`. Este utilitário possui inúmeras opções, mas para nosso objetivo, o comando a seguir é suficiente:

```
ldapsearch -x -b "dc=EMPRESA" "(objectclass=*)"
```

Substitua EMPRESA pelo DC da empresa, lembrando que ele deve ser completo, conforme configurado no OpenLDAP. Por exemplo: "dc=empresa,dc=com,dc=br".

O comando apresentado irá mostrar **todos** os registros da base de dados LDAP.

Também podemos procurar por um determinado usuário na base de dados, como apresentado no exemplo a seguir:

```
ldapsearch -x -b "dc=EMPRESA" "(uid=antonio)"
```

Neste exemplo, como a base de dados continha dados das contas POSIX (Linux) e Samba, o resultado foi o seguinte:

```
# extended LDIF
#
# LDAPv3
# base <dc=EMPRESA> with scope subtree
# filter: (uid=antonio)
# requesting: ALL
#

# antonio, Users, EMPRESA
dn: uid=antonio,ou=Users,dc=EMPRESA
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
objectClass: sambaSamAccount
cn: antonio
sn: antonio
givenName: antonio
uid: antonio
uidNumber: 1053
gidNumber: 513
homeDirectory: /home/antonio
gecos: System User
sambaLogonTime: 0
sambaLogoffTime: 2147483647
sambaKickoffTime: 2147483647
sambaPwdCanChange: 0
displayName: mario
sambaPrimaryGroupSID: S-1-5-21-1011439938-2526806255-774746513-513
sambaLogonScript: antonio.cmd
sambaSID: S-1-5-21-1011439938-2526806255-774746513-3092
loginShell: /bin/bash
sambaAcctFlags: [U]
sambaPwdLastSet: 1305544325
```

```
sambaPwdMustChange: 1313320325
shadowLastChange: 15110
shadowMax: 10000000

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

4.2. Configuração das ferramentas básicas do OpenLDAP

Configure o arquivo `/etc/libnss-ldap.conf` (substitua EMPRESA pelo nome do domínio):

```
host 127.0.0.1

# The distinguished name of the search base.
base dc=EMPRESA

# The LDAP version to use (defaults to 3
# if supported by client library)
ldap_version 3

# The distinguished name to bind to the server with
# if the effective user ID is root. Password is
# stored in /etc/libnss-ldap.secret (mode 600)
# Use 'echo -n "mypassword" > /etc/libnss-ldap.secret' instead
# of an editor to create the file.
rootbinddn cn=admin,dc=EMPRESA
```

Crie/altere o arquivo `/etc/libnss-ldap.secret` para que tenha apenas uma linha com a senha do administrador do LDAP (`admin`, em nosso exemplo). Exemplo:

```
senha_do_admin_ldap
```

Por questões de segurança, altere as permissões do arquivo `/etc/libnss-ldap.secret`:

```
chmod 600 /etc/libnss-ldap.secret
chown roo:root /etc/libnss-ldap.secret
```

Para facilitar o uso dos comandos e integrar o NSS com o LDAP, crie um *link* simbólico para o arquivo de configuração no diretório `/etc/ldap`:

```
cd /etc/ldap
mv ldap.conf ldap.conf.old
ln -s ../libnss-ldap.conf ldap.conf
```

Esta alteração se faz necessária porque os utilitários do OpenLDAP procuram as configurações em `/etc/ldap/ldap.conf`, porém, outras ferramentas, como as de sistema, procuram as configurações do LDAP em `/etc/libnss-ldap.conf`. Como os dois arquivos devem possuir o mesmo conteúdo, ao criarmos um *link* simbólico, evitamos problemas com a sincronização dos arquivos (isto é, mantê-los sempre com o mesmo conteúdo).

No caso do Ubuntu, verifiquei que ele também utiliza os arquivos `/etc/ldap.conf` e `/etc/ldap.secret`. Para evitar problemas, vamos criar também os *links* para estes arquivos apontando para os arquivos `libnss-ldap.conf` e `libnss-ldap.secret`:

```
cd /etc
ln -sf libnss-ldap.secret /etc/ldap.secret
ln -sf libnss-ldap.conf /etc/ldap.conf
```

5. Configuração básica do Samba

Antes de configurarmos o Linux para autenticar no LDAP, vamos configurar um PDC básico com Samba. A razão disso é que vamos utilizar o `smbldap-tools` para criar e popular a base de dados LDAP e esta ferramenta cria as bases tanto para contas POSIX (Linux), como Windows©(Samba).

O Samba é configurado através do arquivo `/etc/samba/smb.conf`. Os detalhes de configuração não serão explorados aqui, mas o arquivo de configuração de um PDC básico é apresentado a seguir. Note que este arquivo já contempla as configurações necessárias para acesso à base de dados LDAP, que criaremos mais tarde.

```
#---- /etc/samba/smb.conf
[global]
#----------------------------------------
# Domain information
#----------------------------------------
workgroup = EMPRESA
server string = EMPRESA's Domain Controller
netbios name = vmubuntu

#----------------------------------------
# Log
#----------------------------------------
log file = /var/log/samba/%m.log
max log size = 500
log level = 1

#----------------------------------------
# Name resolution
#----------------------------------------
name resolve order = lmhosts wins bcast
dos charset = CP850
unix charset = UTF-8
display charset = UTF-8
wins support = Yes

#----------------------------------------
# Security and authentication
#----------------------------------------
security = user
encrypt passwords = true
passdb backend = ldapsam:ldap://127.0.0.1/
username map = /etc/samba/smbusers

#----------------------------------------
# Printing
#----------------------------------------
load printers = No
# printing = cups
# printcap name = cups

#----------------------------------------
# PDC options
```

```
#----------------------------------------
domain logons = Yes
logon script = %U.cmd

#----------------------------------------
# Disable remote profiles
#----------------------------------------
logon path =
logon home =
logon drive =

#----------------------------------------
# Domain browser options
#----------------------------------------
#preferred master = auto
#domain master = auto
preferred master = Yes
domain master = Yes
local master = yes
os level = 100
time server = Yes
remote announce = 10.1.255.255

#----------------------------------------
# LDAP parameters.
#----------------------------------------
ldap admin dn = cn=admin,dc=EMPRESA
ldap ssl = off
ldap delete dn = no
ldap user suffix = ou=Users
ldap group suffix = ou=Groups
ldap machine suffix = ou=Computers
ldap suffix = dc=EMPRESA
# Allow mambers of "Domain Admins" to add computers into the domain
enable privileges = yes


#----------------------------------------
# Allow the automatic creation of machine accounts
# on domain joins.
#----------------------------------------
add user script = /usr/sbin/smbldap-useradd -m "%u"
delete user script = /usr/sbin/smbldap-userdel "%u"

add machine script = /usr/sbin/smbldap-useradd -t 0 -w "%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"

# Password synchronization
passwd program = /usr/sbin/smbldap-passwd -u "%u"
passwd chat = "Changing*\nNew*password*" %n\n "*Retype*new*password*" %n\n
ldap password sync = yes
unix password sync = yes
```

```
#----------------------------------------
# ACL control through Windows Explorer
# To this options run, it is necessary to add the following options
# to the file fstab: "acl,user_xattr" for all shared partitions
#----------------------------------------
map acl inherit = Yes
inherit acls = Yes
inherit permissions = Yes
nt acl support = Yes

#----------------------------------------
# Client access
#----------------------------------------
hosts allow = 10.0., 127.


#----------------------------------------
# Network options
#----------------------------------------
socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192

#obey pam restrictions = Yes
#smb passwd file = /etc/samba/smbpasswd
#pam password change = Yes
#passwd program = /usr/bin/passwd %u
#passwd chat = *New*password* %n\n *Retype*new*password* %n\n \
#              *passwd:*all*authentication*tokens*updated*successfully*
#unix password sync = Yes
#add machine script = /usr/sbin/useradd -g machines -c Workstation -d /dev/null \
#                     -s /sbin/false %u
#dns proxy = No


#----------------------------------------
# Domain administrator's group
#----------------------------------------
admin users = @"Domain Admins"

#----------------------------------------
# Allow the user authentication through smb_auth (Squid)
#----------------------------------------
lanman auth = yes

[netlogon]
comment = Network Logon Service
path = /var/lib/samba/netlogon
write list = root
browseable = yes

[infra]
comment = Infra estrutura
path = /EMPRESA/infra
valid users = "@Domain Users"
read list = "@Domain Users"
write list = "@Domain Users"
read only = No
create mask = 0775
```

```
directory mask = 02775
browseable = No
```

Este arquivo de configuração assume o seguinte:

- Já possui as configurações para acesso ao LDAP (`smbldap-tools`, que ainda não configuramos).
- É um controlador de domínio (`security=user`).
- O nome NetBIOS do servidor é vmubuntu (`netbiosname=vmubuntu`).
- Assume que o nome do domínio é EMPRESA (`workgroup=EMPRESA`).
- Está configurado para aceso através da rede 10.0.0.0/16 (`hosts allow = 10.0., 127.`).
- Assume que o servidor LDAP está instalado no próprio servidor (`passdbbackend=ldapsam:ldap://127.0.0.1/`).
- Possui dois compartilhamentos: um de sistema (`netlogon`) e outro de dados (`infra`).

Observando a configuração do Samba apresentada no exemplo, devemos criar o diretório de armazenamento dos *scripts* de *logon* dos usuários:

```
mkdir /var/lib/samba/netlogon
```

Além disso, também devemos criar o diretório especificado para os compartilhamentos. No caso do exemplo, deveríamos criar o diretório `/EMPRESA/infra`:

```
mkdir -p /EMPRESA/infra
```

Também pode ser necessário alterar as permissões do diretório, mas vamos deixar isso por conta das necessidades da aplicação real.

Antes de iniciarmos o samba, devemos armazenar a senha do administrador do LDAP no arquivo de controle do samba, o `secrets.tdb` (`/var/lib/samba/secrets.tdb`):

```
smbpasswd -w senhaDoManager
Setting stored password for "cn=admin,dc=EMPRESA" in secrets.tdb
```

Além disso, vamos obter o SID do domínio para adicioná-lo na configuração do `smbldap-tools`, que realizaremos posteriormente:

```
net getlocalsid EMPRESA
SID for domain empresa is: S-1-5-21-2860471069-3029604567-4147374860
```

Anote o SID obtido, pois ele será necessário na configuração do `smbldap-tools`.

Vamos parar o serviço Samba. Se estivermos usando o Debian (considerando a versão 6.x - Squeeze), o comando é o seguinte:

```
invoke-rc.d samba stop
```

Já se for o Ubuntu, é provável que o sistema já esteja utilizando o `upstart`, que é uma variação do `init`. Neste caso, os comandos devem ser os seguintes:

```
stop nmbd
nmbd stop/waiting
stop smbd
smbd stop/waiting
```

Agora, vamos reiniciar o Samba:

Para os sistemas que utilizam o `init` (Debian 6.x, por exemplo):

```
invoke-rc.d samba stop
```

Para os sistemas que utilizam o `upstart` (como o Ubuntu 11.10, por exemplo):

```
start smbd
smbd start/running, process 3555
start nmbd
nmbd start/running, process 3563
```

Agora precisamos criar a base de dados e populá-la com os usuários e grupos básicos necessários para o domínio Windows©.

6. Configuração do smbldap-tools

As configurações do `smbldap-tools` são armazenadas no diretório `/etc/smbldap-tools`, porém, este diretório pode não ser criado automaticamente na instalação, portanto, mãos a obra:

```
mkdir /etc/smbldap-tools
cd /etc/smbldap-tools
cp /usr/share/doc/smbldap-tools/examples/smbldap_bind.conf .
cp /usr/share/doc/smbldap-tools/examples/smbldap.conf.gz .
gunzip smbldap.conf
```

Altere o arquivo `smbldap_bind.conf` conforme a seguir (nos parâmetros de senha, coloque a senha do manager que você configurou):

```
#----- /etc/smbldap-tools/smbldap_bind.conf
slaveDN="cn=admin,dc=EMPRESA"
slavePw="senha_do_manager"
masterDN="cn=admin,dc=EMPRESA"
masterPw="senha_do_manager"
```

Por questões de segurança, permita acesso a este arquivo apenas ao `root`:

```
chown root:root /etc/smbldap-tools/smbldap_bind.conf
chmod 600 /etc/smbldap-tools/smbldap_bind.conf
```

Agora, precisamos configurar alguns parâmetros do domínio armazenado na base do LDAP, através do arquivo `/etc/smbldap-tools/smbldap.conf`, apresentado a seguir (a maioria dos comentários foram removidos do exemplo a seguir). Os comentários originais foram mantidos, por serem uma boa referência de documentação. É de extrema importância que os parâmetros sejam verificados um a um e adequados às necessidades da aplicação. Segue o arquivo `/etc/smbldap-tools/smbldap.conf`:

```
#----- /etc/smbldap-tools/smbldap.conf
##############################################################################
#
# General Configuration
#
```

```
##############################################################################

# Put your own SID. To obtain this number do: "net getlocalsid".
# If not defined, parameter is taking from "net getlocalsid" return
SID="S-1-5-21-2860471069-3029604567-4147374860"

# Domain name the Samba server is in charged.
# If not defined, parameter is taking from smb.conf configuration file
# Ex: sambaDomain="IDEALX-NT"
sambaDomain="EMPRESA"

##############################################################################
#
# LDAP Configuration
#
##############################################################################

# Notes: to use to dual ldap servers backend for Samba, you must patch
# Samba with the dual-head patch from IDEALX. If not using this patch
# just use the same server for slaveLDAP and masterLDAP.
# Those two servers declarations can also be used when you have
# . one master LDAP server where all writing operations must be done
# . one slave LDAP server where all reading operations must be done
#   (typically a replication directory)

# Slave LDAP server
# Ex: slaveLDAP=127.0.0.1
# If not defined, parameter is set to "127.0.0.1"
slaveLDAP="127.0.0.1"

# Slave LDAP port
# If not defined, parameter is set to "389"
slavePort="389"

# Master LDAP server: needed for write operations
# Ex: masterLDAP=127.0.0.1
# If not defined, parameter is set to "127.0.0.1"
masterLDAP="127.0.0.1"

# Master LDAP port
# If not defined, parameter is set to "389"
#masterPort="389"
masterPort="389"

# Use TLS for LDAP
# If set to 1, this option will use start_tls for connection
# (you should also used the port 389)
# If not defined, parameter is set to "0"
ldapTLS="0"

# Use SSL for LDAP
# If set to 1, this option will use SSL for connection
# (standard port for ldaps is 636)
# If not defined, parameter is set to "0"
ldapSSL="0"

# How to verify the server's certificate (none, optional or require)
# see "man Net::LDAP" in start_tls section for more details
verify="require"
```

```

# CA certificate
# see "man Net::LDAP" in start_tls section for more details
cafile="/etc/smbldap-tools/ca.pem"

# certificate to use to connect to the ldap server
# see "man Net::LDAP" in start_tls section for more details
clientcert="/etc/smbldap-tools/smbldap-tools.EMPRESA.pem"

# key certificate to use to connect to the ldap server
# see "man Net::LDAP" in start_tls section for more details
clientkey="/etc/smbldap-tools/smbldap-tools.EMPRESA.key"

# LDAP Suffix
# Ex: suffix=dc=IDEALX,dc=ORG
suffix="dc=EMPRESA"

# Where are stored Users
# Ex: usersdn="ou=Users,dc=IDEALX,dc=ORG"
# Warning: if 'suffix' is not set here, you must set the full dn for usersdn
usersdn="ou=Users,${suffix}"

# Where are stored Computers
# Ex: computersdn="ou=Computers,dc=IDEALX,dc=ORG"
# Warning: if 'suffix' is not set here, you must set the full dn for computersdn
computersdn="ou=Computers,${suffix}"

# Where are stored Groups
# Ex: groupsdn="ou=Groups,dc=IDEALX,dc=ORG"
# Warning: if 'suffix' is not set here, you must set the full dn for groupsdn
groupsdn="ou=Groups,${suffix}"

# Where are stored Idmap entries (used if samba is a domain member server)
# Ex: groupsdn="ou=Idmap,dc=IDEALX,dc=ORG"
# Warning: if 'suffix' is not set here, you must set the full dn for idmapdn
idmapdn="ou=Idmap,${suffix}"

# Where to store next uidNumber and gidNumber available for new users and groups
# If not defined, entries are stored in sambaDomainName object.
# Ex: sambaUnixIdPooldn="sambaDomainName=$sambaDomain,${suffix}"
# Ex: sambaUnixIdPooldn="cn=NextFreeUnixId,${suffix}"
sambaUnixIdPooldn="sambaDomainName=$sambaDomain,${suffix}"

# Default scope Used
scope="sub"

# Unix password encryption (CRYPT, MD5, SMD5, SSHA, SHA, CLEARTEXT)
hash_encrypt="SSHA"

# if hash_encrypt is set to CRYPT, you may set a salt format.
# default is "%s", but many systems will generate MD5 hashed
# passwords if you use "$1$%.8s". This parameter is optional!
crypt_salt_format="%s"

##############################################################################
#
# Unix Accounts Configuration
#
##############################################################################
```

```
# Login defs
# Default Login Shell
# Ex: userLoginShell="/bin/bash"
userLoginShell="/bin/bash"

# Home directory
# Ex: userHome="/home/%U"
userHome="/home/%U"

# Default mode used for user homeDirectory
userHomeDirectoryMode="700"

# Gecos
userGecos="System User"

# Default User (POSIX and Samba) GID
defaultUserGid="513"

# Default Computer (Samba) GID
defaultComputerGid="515"

# Skel dir
skeletonDir="/etc/skel"

# Default password validation time (time in days) Comment the next line if
# you don't want password to be enable for defaultMaxPasswordAge days (be
# careful to the sambaPwdMustChange attribute's value)
defaultMaxPasswordAge="180"

##############################################################################
#
# SAMBA Configuration
#
##############################################################################

# The UNC path to home drives location (%U username substitution)
# Just set it to a null string if you want to use the smb.conf 'logon home'
# directive and/or disable roaming profiles
# Ex: userSmbHome="\\PDC-SMB3\%U"
userSmbHome=""

# The UNC path to profiles locations (%U username substitution)
# Just set it to a null string if you want to use the smb.conf 'logon path'
# directive and/or disable roaming profiles
# Ex: userProfile="\\PDC-SMB3\profiles\%U"
userProfile=""

# The default Home Drive Letter mapping
# (will be automatically mapped at logon time if home directory exist)
# Ex: userHomeDrive="H:"
userHomeDrive=""

# The default user netlogon script name (%U username substitution)
# if not used, will be automatically username.cmd
# make sure script file is edited under dos
# Ex: userScript="startup.cmd" # make sure script file is edited under dos
userScript="%U.cmd"
```

```
# Domain appended to the users "mail"-attribute
# when smbldap-useradd -M is used
# Ex: mailDomain="idealx.com"
mailDomain="EMPRESA"

##############################################################################
#
# SMBLDAP-TOOLS Configuration (default are ok for a RedHat)
#
##############################################################################

# Allows not to use smbpasswd (if with_smbpasswd == 0 in smbldap_conf.pm) but
# prefer Crypt::SmbHash library
with_smbpasswd="0"
smbpasswd="/usr/bin/smbpasswd"

# Allows not to use slappasswd (if with_slappasswd == 0 in smbldap_conf.pm)
# but prefer Crypt:: libraries
with_slappasswd="0"
slappasswd="/usr/sbin/slappasswd"

# comment out the following line to get rid of the default banner
# no_banner="1"
```

ATENÇÃO: Os parâmetros apresentados servem para instalações novas. Se já existir um servidor OpenLDAP no ambiente, as configurações do pacote `smbldap-tool` precisarão ser idênticas às do servidor original.

Os principais parâmetros que precisam ser editados são os seguintes:

Parâmetro	Comentários
`SID`	ID do domínio.
`sambaDomain`	Nome do domínio.
`slaveLDAP`	Servidor LDAP escravo (se houver um segundo servidor, para disponibilidade). Se não houver use o mesmo *host* do servidor mestre.
`slavePort`	Porta de acesso no servidor escravo.
`masterLDAP`	Servidor LDAP mestre.
`masterPort`	Porta de acesso ao servidor mestre.
`ldapTLS`	Ajustar para zero significa não ter segurança na comunicação, e habilitar este parâmetro implica em configurações específicas de criptografia, não cobertas neste documento.
`caFile`, `clientcert` e `clientkey`	Somente para casos em que SSL/TLS forem utilizados.
`suffix`	Sufixo do domínio, com as partes precedidas pelos sufixos do LDAP.
`hash_encrypt`	Função de *hash* a ser utilizada para o armazenamento das senhas dos usuários. Normalmente, pode ser uma das seguintes opções: `CRYPT`, `MD5`, `SMD5`, `SSHA`, `SHA`, `CLEARTEXT`. Não é preciso dizer que, por questões de segurança, a última opção (`CLEARTEXT`) **não** deve ser utilizada.
`userLoginShell`	Interpretador de comandos (*shell*) padrão para usuários GNU/Linux.
`userHome`	Diretório *home* do usuário.
`defaultUserGid`	Grupo padrão dos usuários.
`defaultComputerGid`	Grupo padrão para as contas de máquinas.
`userSmbHome`	Deixe branco para desabilitar diretório *home* para usuários Windows©.
`userProfile`	Deixe em branco para desabilitar a gravação do perfil (*desktop* do usuário).
`userHomeDrive`	Deixe em brando para desabilitar a unidade a ser mapeada como *home* do usuário.
`userScript`	Define o nome do *script* de *logon* do usuário Windows©.

Há alguns grupos necessários para o domínio Samba que ainda não foram criados. Podemos fazer isso através do utilitário `smbldap-populate` (digite a senha do `root` quando solicitado, no final da execução):

ATENÇÃO: Só é necesário popular base de dados se você estiver criando uma nova base de dados. Se você restaurou uma cópia de segurança da base de dados, não é necessário populá-la, pois ela já contém os registros necessários.

```
smbldap-populate
Populating LDAP directory for domain EMPRESA (S-1-5-21-2860471069-3029604567-4147374860)
(using builtin directory structure)

adding new entry: dc=EMPRESA
adding new entry: ou=Users,dc=EMPRESA
adding new entry: ou=Groups,dc=EMPRESA
adding new entry: ou=Computers,dc=EMPRESA
adding new entry: ou=Idmap,dc=EMPRESA
adding new entry: uid=root,ou=Users,dc=EMPRESA
adding new entry: uid=nobody,ou=Users,dc=EMPRESA
adding new entry: cn=Domain Admins,ou=Groups,dc=EMPRESA
adding new entry: cn=Domain Users,ou=Groups,dc=EMPRESA
```

```
adding new entry: cn=Domain Guests,ou=Groups,dc=EMPRESA
adding new entry: cn=Domain Computers,ou=Groups,dc=EMPRESA
adding new entry: cn=Administrators,ou=Groups,dc=EMPRESA
adding new entry: cn=Account Operators,ou=Groups,dc=EMPRESA
adding new entry: cn=Print Operators,ou=Groups,dc=EMPRESA
adding new entry: cn=Backup Operators,ou=Groups,dc=EMPRESA
adding new entry: cn=Replicators,ou=Groups,dc=EMPRESA
adding new entry: sambaDomainName=EMPRESA,dc=EMPRESA

Please provide a password for the domain root:
Changing UNIX and samba passwords for root
New password:
Retype new password:
```

Agora, se desejado, podemos remover o usuário `root` da base LDAP e adicionar o usuário *administrator*:

```
smbldap-userdel root

smbldap-useradd -a administrator

smbldap-groupmod -m administrator "Domain Admins"
```

Agora podemos verificar se o SID do domínio foi corretamente inserido na base de dados LDAP:

```
ldapsearch -x -LLL | grep -i sid
sambaPrimaryGroupSID: S-1-5-21-2860471069-3029604567-4147374860-512
sambaSID: S-1-5-21-2860471069-3029604567-4147374860-500
sambaPrimaryGroupSID: S-1-5-21-2860471069-3029604567-4147374860-514
sambaSID: S-1-5-21-2860471069-3029604567-4147374860-2998
sambaSID: S-1-5-21-2860471069-3029604567-4147374860-512
sambaSID: S-1-5-21-2860471069-3029604567-4147374860-513
sambaSID: S-1-5-21-2860471069-3029604567-4147374860-514
sambaSID: S-1-5-21-2860471069-3029604567-4147374860-515
sambaSID: S-1-5-32-544
sambaSID: S-1-5-32-548
sambaSID: S-1-5-32-550
sambaSID: S-1-5-32-551
sambaSID: S-1-5-32-552
sambaSID: S-1-5-21-2860471069-3029604567-4147374860
```

Agora já poderíamos até inserir usuários do domínio Windows©, usando as ferramentas `smbldap-tools`, porém, como nosso objetivo é também usar a autenticação centralizada para clientes Linux, vamos configurá-la antes de fazer os testes.

7. Configuração do Linux para autenticação na base LDAP

Nosso objetivo iniciar era autenticar os usuários Linux numa base de dados centralizada LDAP. Como nosso servidor LDAP também poderia autenticar usuários do domínio Windows©, partimos para a configuração do Samba, já que uma das ferramentas de manipulação de contas de usuário em bases LDAP que suporta contas de domínio Windos, também é capaz manipular as contas POSIX (Linux).

Uma vez que configuramos esta ferramenta (smbldap-tools), vamos agora configurar o Linux para autenticar no LDAP. Observe que esta configuração serve também para as estações de trabalho Linux.

Observe que nas estações de trabalho não deve ser instalado o slapd, mas apenas os pacotes específicos de clientes, conforme descrito no capítulo de instalação dos softwares.

7.1. Configuração do libnss-ldap

Como parte da configuração do cliente, que também deve ser efetuada no servidor, vamos descrever a configuração do libnss-ldap. observe que nós já fizemos esta configuração durante o proceso de configuração do servidor OpenLDAP, mas a repetimos aqui para que fique claro a configuração dos clientes Linux.

Configure o arquivo `/etc/libnss-ldap.conf` (substitua EMPRESA pelo nome do domínio):

```
host 127.0.0.1

# The distinguished name of the search base.
base dc=EMPRESA

# The LDAP version to use (defaults to 3
# if supported by client library)
ldap_version 3

# The distinguished name to bind to the server with
# if the effective user ID is root. Password is
# stored in /etc/libnss-ldap.secret (mode 600)
# Use 'echo -n "mypassword" > /etc/libnss-ldap.secret' instead
# of an editor to create the file.
rootbinddn cn=admin,dc=EMPRESA
```

Crie (ou altere, se existir) o arquivo `/etc/libnss-ldap.secret` para que tenha apenas uma linha com a senha do administrador do LDAP (admin, em nosso exemplo). Exemplo:

```
senha_do_admin_ldap
```

Por questões de segurança, altere as permissões do arquivo `/etc/libnss-ldap.secret`:

```
chmod 600 /etc/libnss-ldap.secret
chown roo:root /etc/libnss-ldap.secret
```

Para facilitar o uso dos comandos e integrar o NSS com o LDAP, crie um link simbólico para o arquivo de configuração no diretório */etc/ldap*:

```
cd /etc/ldap
mv ldap.conf ldap.conf.old
ln -s ../libnss-ldap.conf ldap.conf
```

Esta alteração se faz necessária porque os utilitários do OpenLDAP procuram as configurações em `/etc/ldap/ldap.conf`, porém, outras ferramentas, como as de sistema, procuram as configurações do LDAP em `/etc/libnss-ldap.conf` e, em suma, os dois arquivos são similares e devem ter o mesmo conteúdo. Assim, ao criarmos um *link* simbólico, evitamos problemas com a sincronização dos arquivos (isto é, mantê-los sempre com o mesmo conteúdo).

No caso do Ubuntu, verifiquei que ele também utiliza os arquivos `/etc/ldap.conf` e `/etc/ldap.secret`. Para evitar problemas, vamos criar também os *links* para estes arquivos apontando para os arquivos `libnss-ldap.conf` e `libnss-ldap.secret`:

```
cd /etc
ln -sf libnss-ldap.secret /etc/ldap.secret
ln -sf libnss-ldap.conf /etc/ldap.conf
```

Reinicie o serviço ldap:

```
invoke-rc.d slapd restart
```

7.2. Configuração do PAM

Precisamos configurar adequadamente o PAM para que o sistema operacional consulte a base LDAP para a autenticação dos usuários. uma vez configurado corretamente o PAM, todas as aplicações que autenticarem usuários usando o PAM já estarão automaticamente fazendo a autenticação na base LDAP. Este é o caso, por exemplo, dos serviços SSH, Telnet e FTP.

Antes de fazermos as alterações, convém que sejam efetuadas cópias de segurança dos arquivos originais.

Edite o arquivo `/etc/nsswitch.conf` conforme a seguir:

```
# /etc/nsswitch.conf
#
# (MLB): changed authentication to the LDAP
#
passwd:         files ldap
group:          files ldap
shadow:         files ldap

hosts:          files dns
networks:       files

protocols:      db files
services:       db files
ethers:         db files
rpc:            db files

netgroup:       ldap
```

Edite (ou crie, se não existir) crie o arquivo `/etc/pam_ldap.conf` conforme a seguir:

```
host 127.0.0.1
base dc=EMPRESA
ldap_version 3
rootbinddn cn=admin,dc=EMPRESA
pam_password SSHA
```

Crie, ou altere, o arquivo `/etc/pam_ldap.secret` para que tenha apenas uma linha com a senha do administrador do LDAP (`admin`, em nosso exemplo). Exemplo:

```
senha_do_admin_ldap
```

Altere as permissões do arquivo `/etc/pam_ldap.secret`:

```
chmod 600 /etc/pam_ldap.secret
chown roo:root /etc/pam_ldap.secret
```

Reinicie o ldap e o nscd:

```
invoke-rc.d slapd restart
invoke-rc.d nscd restart
```

Edite o arquivo `/etc/pam.d/commom-account` e deixe-o assim:

```
#----- /etc/pam.d/common-account
# MLB
# PAM+LDAP
#
#account  required   pam_unix.so try_first_pass
#account  sufficient pam_succeed_if.so uid > 1000 quiet
#account  [default=bad success=ok user_unknown=ignore] pam_ldap.so
#account  required   pam_permit.so

#account sufficient pam_ldap.so
#account required   pam_unix.so try_first_pass

account  required   pam_unix.so try_first_pass
account  sufficient pam_succeed_if.so uid < 500 quiet
account  [default=bad success=ok user_unknown=ignore] pam_ldap.so
account  required   pam_permit.so
```

Edite o arquivo `/etc/pam.d/commom-auth` e deixe-o assim:

```
#----- /etc/pam.d/common-auth
auth sufficient  pam_unix.so nullok_secure
auth requisite   pam_succeed_if.so uid >= 1000 quiet
auth sufficient  pam_ldap.so use_first_pass
auth required    pam_deny.so
```

Edite o arquivo `/etc/pam.d/commom-session` e deixe-o assim:

```
#----- /etc/pam.d/common-session
session required   pam_mkhomedir.so skel=/etc/skel umask=0022 silent
session sufficient pam_unix.so
```

Edite o arquivo `/etc/pam.d/commom-password` e deixe-o assim:

```
#----- /etc/pam.d/common-password
# password sufficient pam_unix.so md5 obscure min=8 nullok try_first_pass
password sufficient pam_unix.so md5 obscure min=4 max=8 nullok try_first_pass
password sufficient pam_ldap.so
password required   pam_deny.so
```

Reinicie o serviço `nscd`:

```
invoke-rc.d nscd restart
```

8. Conclusão

Apesar de ser um tanto quanto complicada a configuração OpenLDAP e das ferramentas necessárias implementar a autenticação centralizada, ela é de suma importância para os ambientes corporativos, mesmo pequenas empresas. Veja só um exemplo: imagine que uma pequena empresa tenha um servidor com Samba autenticando máquinas Windows©, um servidor *proxy* para o acesso à Internet e, digamos, um servidor FTP, todos em equipamentos (servidores) separados.

Do ponto de vista dos usuários, na falta de autenticação centralizada, provavelmente os usuários teriam que memorizar duas contas (e senhas) de acesso, uma para o acesso ao domínio (Windows©+ Samba), e outra para o servidor FTP. E nem consideramos o *proxy*, que poderia necessitar autenticação...

Do ponto de vista da administração, sempre seria necessária a criação das contas nos dois servidores e, quando um colaborador deixa a empresa, é necessária a remoção destas contas. O gerenciamento torna-se mais trabalhoso com o aumento do número de serviços e servidores.

Com a autenticação centralizada, este problema desaparece, porque todos os serviços podem usar o LDAP para autenticação dos usuários.

Até mesmo sistemas desenvolvidos internamente podem se utilizar do LDAP. Imagine que a empresa tenha desenvolvido um sistema interno para controle de documentos, ou até mesmo um ERP. Estes sistemas poderiam ser desenvolvidos para usar o LDAP como meio de autenticação.

O roteiro apresentado neste documento foi bastante superficial no que diz respeito aos recursos disponíveis no OpenLDAP. Temas como *backup*, replicação e SSL/TLS não foram cobertos. Talvez estes temas sejam cobertos numa versão futura deste documento. Quem sabe...

A. Dicas rápidas

Seguem algumas dicas de sintaxe de comandos para consulta rápida.

A.1. Grupos e usuários

Para adicionar um usuário Samba e POSIX:

```
smbldap-useradd -a USUÁRIO
```

Para definir ou alterar a senha de um usuário (Samba e POSIX):

```
smbldap-passwd USUÀRIO
```

Para adicionar o usuário USUÁRIO no grupo GRUPO:

```
smbldap-groupmod -m "USUÁRIO" "GRUPO"
```

Para remover o usuário USUÁRIO do grupo GRUPO:

```
smbldap-groupmod -x "USUÁRIO" "GRUPO"
```

Para desabilitar a conta do usuário (sem removê-la):

```
smbldap-usermod -I USUÁRIO   (Windows)
smbldap-usermod -L USUÁRIO   (Linux)
```

Neste caso, o parâmetro `sambaAcctFlags` passa a ter o bit `D` habilitado (para contas Samba/Windows©).

Para habilitar a conta do usuário:

```
smbldap-usermod -J USUÁRIO  (Windows)
smbldap-usermod -U USUÁRIO  (Linux)
```

A.2. Senhas

Para forçar o usuário (Windows©) a trocar a senha no próximo *logon*:

```
net sam set pwdmustchangenow <username> yes
```

Para alterar a data de validade da senha:

Somente POSIX:

```
smbldap-usermod --shadowExpire YYYY-MM-DD
```

ou

```
smbldap-usermod --shadowExpire n usuário
```

Onde **n** corresponde ao número de dias desde 1-jan-1970 (*Unix Epoch*).

Somente Samba:

```
smbldap-usermod --sambaExpire YYYY-MM-DD(HH:MM:SS) usuário
```

ou

```
smbldap-usermod --sambaExpire n usuário
```

Para POSIX e Samba:

```
smbldap-usermod --expire YYYY-MM-DD(HH:MM:SS) usuário
```

ou

```
smbldap-usermod --expire n usuário
```

Mesmo alterando a data de expiração, se a senha estiver vencida, ela ainda deverá ser trocada.

É possível ajustar as datas de expiração das senhas POSIX e Samba, conforme os exeplos a seguir:

```
smbldap-usermod --expire       YYYY-MM-DD USUÁRIO
smbldap-usermod --shadowExpire YYYY-MM-DD USUÁRIO
smbldap-usermod --sambaExpire  YYYY-MM-DD USUÁRIO
smbldap-usermod --shadowmax    3650       USUARIO
```

Onde:

- **–sambaExpire** Ajusta a data de expiração da senha do Samba.
- **–shadowExpire** Ajusta a data de expiração da senha POSIX (Linux)
- **–expire Ajusta** a data de expiração das senhas Samba e POSIX (logo, os dois parâmetros anteriores são desnecessários)
- **–shadowMax** Ajusta quantos dias, no máximo, uma senha pode ficar sem ser alterada.

Além disso, para destravar a conta, precisei executar os seguintes comandos (Samba e Linux):

```
smbldap-usermod -J USUÁRIO
smbldap-usermod -U USUÁRIO
```

A.3. Renomear conta de usuário

Em meu trabalho tenho precisado renomear contas de usuário quando, por exemplo, um colaborador passa a exercer as funções de outro usuário. Neste caso, é importante que SSID da conta não seja alterado.

Fiz um teste com um usuário que deixou a empresa e o usuário que o substituiu precisava manter o perfil do usuário antigo no Windows©. Então, renomeei a conta diretamente no LDAP, juntamente com o *script* de *logon* usando o seguinte comando (observe que é possível alterar mais de um atributo de uma conta num mesmo comando):

```
smbldap-usermod -r novo.usuario -E novo.usuario.cmd -d novo_home_dir usuario.antigo
```

O comando `smbldap-usermod` sempre executa alguma operação sobre uma conta de usuário, que deve ser o último parâmetro. No exemplo apresentado, usamos o comando `smbldap-usermod` para alterar a conta `usuario.antigo`, que é o último parâmetro, alterando os seguintes atributos da conta:

- O nome da conta, alterado para `novo.usuario` através da opção **-r**.
- O nome do *script* de *logon*, alterado para `novo.usuario.cmd`, através da opção **-E**
- O nome do novo diretório *home* do usuário, através da opção **-d**

Referências

OPENLDAP, T. P. Openldap software 2.4 administrator's guide. 2011. Disponível em: <http://www.openldap.org/doc/admin24/>. Acesso em: 20 jan. 2012.

SUNGAILA, M. *Autenticação Centralizada com OpenLDAP*. Primeira edição. [S.l.]: Novatec, 2008. ISBN 978-8575221426.