Manual do Usuário
do Smbldap-tools

Tradução para o Português Brasileiro (pt-br) por

Clovis Sena (csena2k2@fisepe.pe.gov.br)

revisão 0.795

Apoio:

www.ldap.org.br

Introdução

Smbldap-tools é um conjunto de scripts desenhados para ajudar a integrar o Samba e um diretório LDAP. Eles visam tanto usuários quanto administradores de sistemas Linux. Usuários podem mudar suas senhas de um modo semelhante ao comando padrão "passwd'' . Os administradores podem realizar o gerenciamento de usuários e grupos via linha de comando e sincronizar contas do Samba consistentemente. Este documenta apresenta:

- uma visão detalhada dos scripts smbldap-tools
- uma explicação passo a passo de como configurar um controlador de domínio Samba3

1.1Requisitos de Software

O smbldap-tools foi desenvolvido e testado com a seguinte configuração:

- Linux RedHat 9 (deveria funcionar em qualquer distribuição Linux)
- Samba release 3.0.2pre1,
- OpenLDAP release 2.1.22
- Microsoft Windows NT 4.0, Windows 2000 and Windows XP Workstations e Servers,

Este guia se aplica para smbldap-tools Release: 0.8.5 .

1.2Atualizações deste documento

A versão mais atualizada deste documento pode ser encontrada na página do projeto smbldap-tools, disponível em http://samba.IDEALX.org/. Se você achar algum erro neste documento, ou se você quiser integrar informações adicionais a este documento, por favor mande-nos um email com seu reletório de erros ou solicitação de alterações para samba@IDEALX.org.

1.3Disponibilidade deste documento

Este documento é propriedade da **IDEALX** (http://www.IDEALX.com/). É dada permissão para distribuir este documento nos termos da GNU Free Documentation License (Veja em http://www.gnu.org/copyleft/fdl.html).

2Instalação

2.1Requisitos

Os principais requisitos para usar smbldap-tools são dois módulos perl: Net::LDAP e Crypt::SmbHash. Na maioria dos casos, você também irá precisar do módulo perl IO-Socket-SSL para usar as funcionalidades TLS. Se você quiser que o samba chame os scripts de modo que você possa usar o Gerenciador de Usuários (User Manager ou qualquer outro) no MS-Windows (para adicionar, deletar, modificar usuários e grupos), Samba deve ser instalado no mesmo computador. Finalmente, o OpenLDAP pode ser instalado em qualquer computador. Por favor, verifique que ele possa ser contactado por um software cliente padrão LDAP. A instalação do Samba e do OpenLDAP não será discutida aqui. Você pode consultar o howto também disponível na página do projeto (http://samba.IDEALX.org). Embora ele tenha sido escrito para o Samba2, a maioria do conteúdo também se aplica ao Samba3. A principal diferença reside nas definições do schema LDAP.

2.2Instalação

Um arquivo dos scripts smbldap-tools pode ser baixadoi de nossa página do projeto http://samba.IDEALX.org/. Arquivos e pacotes RedHat estão disponíveis. Se você está fazendo upgrade, veja no arquivo INSTALL ou leia o link 6.13.

2.2.1Instalando do rpm

Para instalar os scripts em um sistema RedHat, baixe os pacotes RPM e execute o seguinte comando:

```
rpm -Uvh smbldap-tools-0.8.5-1.i386.rpm
```

2.2.2 Instalando a partir dos fontes

Em sistemas não RedHat, baixe o arquivo fonte dos scripts. O arquivo atual é smbldap-tools-0.8.5.tar.gz. Descompacte ele e copie todos os scripts Perl para o direrório /usr/local/sbin, e os dois arquivos de configuração para o diretório /etc/smbldap-tools/:

```
mkdir /etc/smbldap-tools/
cp *.conf /etc/smbldap-tools/
cp smbldap-* /usr/local/sbin/
```

A configuração agora é baseada em dois arquivos diferentes:

- smbldap.conf: define parâmetros globais
- smbldap_bind.conf: define uma conta administrativa para acessar ao diretório

O segundo arquivo deve ser lido **apenas** pelo 'root', pois ele contém as credenciais que permitem modificações em todo o diretório. Tenha certeza de que os arquivos estão protegidos, rodando o seguinte comando:

```
chmod 644 /etc/smbldap-tools/smbldap.conf
chmod 600 /etc/smbldap-tools/smbldap_bind.conf
```

3 Configurando o smbldap-tools

Como mencionado na seção anterior, você terá que atualizar dois arquivos de configuração. O primeiro (smbldap.conf) permite que você defina parâmetros globais que serão legíveis por todo mundo, e o segundo (smbldap_bind.conf) define duas contas administrativas para acessar os servidores ldap mestre e escrevo: este arquivo deve então ser lido apenas pelo root. Um script chamado configure.pl pode ajudar você a definir os seus conteúdos. Ele está localizado no tarball baixado ou no diretórios da documentação se você pegou o arquivo RPM (veja em /usr/share/doc/smbldap-tools/). Basta chamá-lo assim:

```
/usr/share/doc/smbldap-tools/configure.pl
```

Ele irá perguntar por valores padrão definidos em seu arquivo smb.conf, e irá atualizar os dois arquivos de configuração usados pelos scripts. Observe que você pode parar o script a qualquer momento usando as teclas Crtl-c. Antes de usar este script :

- os dois arquivo de configuração devem estar presentes no diretório /etc/smbldap-tools/
- verifique se o samba está configurado e rodando, pois o script irá tentar obter seu domain secure id (SID) para o seu grupo de trabalho (workgroup).

Nestes arquivos existem parametros que são definidos como este:

```
key="value"
```

Exemplos completos dos arquivos de configuração podem ser encontrados em 8.1.

3.1 O arquivo smbldap.conf

Este arquivo é usado para definir parâmetros que podem ser lidos por todo mundo. Um exemplo completo deste arquivo está disponível na seção 8.1.1.
Vamos dar uma olhada em todos os parâmetros disponíveis.

- UID_START e GID_START : estes parâmetros estão desaprovados.

Os uid e gid disponíveis são agora definidos na nova entrada padrão cn=NextFreeUnixId,dc=idealx,dc=org.

- SID : Secure Identifier Domain
  - Exemplo: SID="S-1-5-21-3703471949-3718591838-2324585696"
  - Observação: você pode obter o SID para seu domínio usando o comando **net getlocalsid**. O Samba deve estar rodando para isto funcionar (pode demorar **vários** minutos para um servidor Samba corretamente negociar seu status com outros servidores da rede).
- slaveLDAP : servidor LDAP escravo
  - Exemplo: slaveLDAP="127.0.0.1"
  - Observação: deve ser um nome válido de DNS ou seu endereço IP
- slavePort : a porta onde contactar no servidor escravo
  - Exemplo: slavePort="389"
- masterLDAP : servidor LDAP mestre
  - Exemplo: masterLDAP="127.0.0.1"
- masterPort : a porta onde contactar no servidor mestre
  - Exemplo: masterPort="389"
- ldapTLS : devemos usar uma conexão TLS para contactar os servidores ldap ?
  - Exemplo: ldapTLS="1"
  - Observação: os servidores LDAP devem estar configurados para aceitar conexões TLS. Veja na seção Samba-LDAP Howto (http://samba.idealx.org/smbldap-howto.fr.html) para maiores detalhes. Se você estiver usando suporte TLS, selecione a porta 389 para conectar aos diretórios mestre e escravo.
- verify : Como verificar o certificado do servidor (none, optional or require). Veja "man Net::LDAP" na seção start_tls para maiores detalhes
  - Exemplo: verify="require"
- cafile : o arquivo de formato PEM contendo certificados para o CA que slapd irá confiar
  - Exemplo: cafile="/etc/smbldap-tools/ca.pem"
- clientcert : o arquivo que contém o certificado do cliente
  - Exemplo: clientcert="/etc/smbldap-tools/smbldap-tools.iallanis.com.pem"
- clientkey : o arquivo que contém a chave privada que combina o certificado armazenado no arquivo clientcert
  - Exemplo: clientkey="/etc/smbldap-tools/smbldap-tools.iallanis.com.key"
- suffix : O nome distinto da base de pesquisas
  - Exemplo: suffix="dc=idealx,dc=com"
- usersdn : ramo em que as contas dos usuários podem ser encontradas ou devem ser adicionadas
  - Exemplo: usersdn="ou=Users,${suffix}"
  - Observação: este ramo **não é** relativo ao valor do sufixo
- computersdn : ramo em que as contas de computadores podem ser

encontradas ou devem ser adicionadas
    - Exemplo: computersdn"ou=Computers,${suffix}"
    - Observação: este ramo **não é** relativo ao valor do sufixo
- groupsdn : ramo em que as contas de grupos podem ser encontradas ou devem ser adicionadas
    - Exemplo: groupsdn="ou=Groups,${suffix}"
    - Observações: este ramo **não é** relativo ao valor do sufixo
- idmapdn : onde são armazenadas entradas Idmap (usadas se o samba é um servidor membro do domínio)
    - Exemplo: idmapdn="ou=Idmap,${suffix}"
    - Observações: este ramo **não é** relativo ao valor do sufixo
- sambaUnixIdPooldn : objeto em que os próximos uidNumber e gidNumber disponíveis são armazenados
    - Exemplo: sambaUnixIdPooldn="cn=NextFreeUnixId,${suffix}"
    - Observações: este ramo **não é** relativo ao valor do sufixo
- scope : o escopo de pesquisa.
    - Exemplo: scope="sub"
- hash_encrypt : hash para ser utilizado quando gerando uma nova senha.
    - Exemplo: hash_encrypt="SSHA"
    - Observação: Isto é usado para a senha unix armazenada no atributo userPassword.
- crypt_salt_format="%s" : se hash_encrypt for definido como CRYPT, você pode definir um formato salt. O padrão é "%s", porém muitos sistemas irão gerar senhas MD5 hashed se você usar "1%.8s". Este parâmetro é opicional.
- userLoginShell : shell padrão dado aos usuários.
    - Exemplo: userLoginShell="/bin/bash"
    - Observação: Isto é armazenado no atributo loginShell .
- userHome : diretório padrão onde os diretórios home dos usuários ficam localizados.
    - Exemplo: userHome="/home/%U"
    - Observação: Isto é armazenado no atributohomeDirectory.
- userGecos : gecos usado para os usuários
    - Exemplo: userGecos="System User"
- defaultUserGid : grupo primário padrão definido para as contas de usuários
    - Exemplo: defaultUserGid="513"
    - Observação: isto é armazenado no atributo gidNumber.
- defaultComputerGid : grupo primário padrão definido para as contas de computadores
    - Exemplo: defaultComputerGid="550"
    - Observação: isto é armazenado no atributo gidNumber.
- skeletonDir : diretório skeleton (modelo) usado para a conta dos usuários
    - Exemplo: skeletonDir="/etc/skel"
    - Observação: esta opção é usada apenas se você pedir pela criação do diretório home quando adicionar um novo usuário.

- defaultMaxPasswordAge : tempo padrão de validação para uma senha (em dias)
    - Exemplo: defaultMaxPassword="55"
- userSmbHome : compartilhamento samba usado para armazenar os diretórios home dos usuários
    - Exemplo: userSmbHome="\\PDC-SMB3\ home\%U"
    - Observação: isto é usado no atributo sambaHomePath.
- userProfile : compartilhamento samba usado para armazenar os perfis dos usuários
    - Exemplo: userProfile="\\PDC-SMB3\ profiles\%U"
    - Observação: isto é armazenado no atributo sambaProfilePath.
- userScript : nome do script de netlogon padrão do usuário. Se não for usado, será automaticamente username.cmd
    - Exemplo: userScript="%U"
    - Observação: isto é armazenado no atributo sambaProfilePath.
- userHomeDrive : letra usada em sistemas windows para mapear o diretório home
    - Exemplo: userHomeDrive="K:"
- with_smbpasswd : should we use the smbpasswd command to set the user's password (instead of the mkntpwd utility) ?
    - Exemplo: with_smbpasswd="0"
    - Observação: deve ser um valor booleano (0 ou 1).
- smbpasswd : caminho para o binário smbpasswd
    - Exemplo: smbpasswd="/usr/bin/smbpasswd"
- mk_ntpasswd : caminho para o binário mkntpwd
    - Exemplo: mk_ntpasswd="/usr/local/sbin/mkntpwd"
    - Observação: o pacote rpm do smbldap-tools irá instalar este utilitário. Se você está usando os arquivos do tarball (instalou dos fontes), você tem que instalá-lo você mesmo (os fontes também estão no arquivo smbldap-tools).
- mailDomain : Domínio anexado ao atributo "mail" dos usuários.
    - Exemplo: mailDomain="idealx.org"

3.2 O arquivo smbldap_bind.conf

Este arquivo é apenas usado pelo root para modificar o conteúdo do diretório. Ele contém nomes distintos (DN=distinguished names) e credenciais para conectar para ambos os diretórios mestre e escravo. Um exemplo completo deste arquivo está disponível na seção 8.1.2. Vamos dar uma olhada em todos os parâmetros disponíveis.

- slaveDN : nome distinto usado para acessar ao servidor escravo
    - Exemplo 1: slaveDN="cn=Manager,dc=idealx,dc=com"
    - Exemplo 2: slaveDN=""
    - Observação: esta pode ser a conta manager do diretório ou qualquer conta LDAP que tenha permissões suficientes para ler todo o diretório (Diretório escravo é apenas para leitura). Conexões anônimas usam a segunda forma do exemplo.
- slavePw : as credenciais usadas para acessar ao servidor escravo
    - Exemplo 1: slavePw="secret"

    - Exemplo 2: slavePw=""
    - Observação: a senha deve ser armazenada aqui de forma clara. Este arquivo deve então ser legível apenas pelo root! Todas as conexões anônimas usam a segunda forma mostrada em nosso exemplo.
- masterDN : o nome distinto usado para acessar o servidor mestre
    - Exemplo: masterDN="cn=Manager,dc=idealx,dc=com"
    - Observação: esta pode ser a conta manager do diretório ou qualquer conta LDAP que tenha permissoes suficientes para modificar o conteúdo do diretório. Acessos anônimos não fazem sentido aqui.
- masterPw : as credenciais para acessar ao servidor mestre
    - Exemplo: masterPw="secret"
    - Observação: a senha deve ser em texto puro. Tenha certeza de proteger este arquivo contra leitores não autorizados!

4 Usando os scripts

4.1 Preenchimento inicial do diretório

Você pode inicializar o diretório LDAP usando o script smbldap-populate. Para fazer isto, a conta definida no arquivo /etc/smbldap-tools/smbldap_bind.conf para acessar o diretório mestre **deve** ser a conta manager, definida na configuração do diretório. Em sistemas RedHat, este arquivo é /etc/openldap/slapd.conf e a conta é definida com

```
rootdn          "cn=Manager,dc=idealx,dc=com"
rootpw          secret
```

O arquivo smbldap_bind.conf deve então ser configurado de modo que os parâmetros para conectar ao servidor LDAP master batam com os anteriores:

```
masterDN="cn=Manager,dc=idealx,dc=com"
masterPw="secret"
```

As opções disponíveis para este script estão resumidas na tabela 1:

opção	definição	valor padrão
-u uidNumber	primeiro uidNumber para alocar	1000
-g gidNumber	primeiro gidNumber para alocar	1000
-a user	nome de login do administrador	Administrator
-b user	nome de login do convidado (guest)	nobody
-e file	exportar um arquivo init	
-i file	importar um arquivo init	

Table 1: Opções disponíveis para o script smbldap-populate

Na maioria dos casos, para definir seu diretório, simplesmente use o

seguinte comando:

```
[root@etoile root]# smbldap-populate
Using builtin directory structure
adding new entry: dc=idealx,dc=com
adding new entry: ou=Users,dc=idealx,dc=com
adding new entry: ou=Groups,dc=idealx,dc=com
adding new entry: ou=Computers,dc=idealx,dc=com
adding new entry: ou=Idmap,dc=idealx,dc=org
adding new entry: cn=NextFreeUnixId,dc=idealx,dc=org
adding new entry: uid=Administrator,ou=Users,dc=idealx,dc=com
adding new entry: uid=nobody,ou=Users,dc=idealx,dc=com
adding new entry: cn=Domain Admins,ou=Groups,dc=idealx,dc=com
adding new entry: cn=Domain Users,ou=Groups,dc=idealx,dc=com
adding new entry: cn=Domain Guests,ou=Groups,dc=idealx,dc=com
adding new entry: cn=Print Operators,ou=Groups,dc=idealx,dc=com
adding new entry: cn=Backup Operators,ou=Groups,dc=idealx,dc=com
adding new entry: cn=Replicator,ou=Groups,dc=idealx,dc=com
adding new entry: cn=Domain Computers,ou=Groups,dc=idealx,dc=com
```

Após este passo, se você não quiser mais usar a conta cn=Manager,dc=idealx,dc=com, você pode criar uma conta dedicada para o Samba e o smbldap-tools. Veja a seção 8.2 para maiores detalhes. A entrada cn=NextFreeUnixId,dc=idealx,dc=org á apenas usada para definir os próximos uidNumber e gidNumber disponíveis para criar novos usuários e grupos. O valor padrão para estes números é 1000. Você pode mudar isto com a opção -u e -g. Por exemplo, se você quiser que o primeiro valor disponível para uidNumber e gidNumber seja definido como 1500, você pode usar o seguinte comando :

```
smbldap-populate -u 1550 -g 1500
```

4.2 Gerencimaneto de Usuários

4.2.1 Adicionando um usuário

Para adicionar um usuário, use o script smbldap-useradd. As opções disponiveis estão resumidas na tabela 2. Quando aplicável, valores padrão são mencionados na terceira coluna. Qualquer string começado com um sinal de $ refere-se a um parâmetro definido no arquivo de configuração /etc/smbldap-tools/smbldap.conf.

opção	definição	Exemplo	valor padrão
-a	cria uma conta de Windows. De outro modo, apenas uma conta Posix é criada		
-w	cria uma conta de estação de trabalho Windows		
-i	cria uma conta de confiança interdomain. Veja a seção 4.4 para mais detalhes		

-u	define um valor uid	-u 1003	primeiro uid disponível
-g	define um valor gid	-g 1003	primeiro gid disponível
-G	adiciona a nova conta para um ou vários grupos suplementares (separados por vírgula)	-G 512,550	
-d	define o diretório home	-d /var/user	$userHomePrefix/user
-s	define o login shell	-s /bin/ksh	$userLoginShell
-c	define o gecos do usuário	-c "admin user"	$userGecos
-m	cria o diretório home do usuário e copia /etc/skel para ele		
-k	define o diretório esqueleto (com -m)	-k /etc/skel2	$skeletonDir
-P	termina por invocar smbldap-passwd para definir a senha do usuário		
-A	o usuário pode mudar a senha ? 0 se não, 1 se sim	-A 1	
-B	o usuário deve mudar a senha na primeira seção ? 0 se não, 1 se sim	-B 1	
-C	define o compartilhamento home do samba	-C \\PDC\homes	$userSmbHome
-D	define uma letra associada com o compartilhamento home	-D H:	$userHomeDrive
-E	define o script DOS para executar no login	-E common.bat	$userScript
-F	define o deretório dos pérfis	-F \\PDC\profiles\user	$userProfile
-H	define os bits de controle da conta samba como '[NDHTUMWSLKI]'	-H [X]	
-N	define o nome canônico do usuário		
-S	define o sobrenome do usuário		
-M	mailAddress local (separado por vírgula)	-M testuser,aliasuser	

-T	endereços para repasse de email (separado por vírgula)	-T testuser@domain.org

Table 2: Opções disponíveis para o script smbldap-useradd

Por exemplo, se você quiser adicionar um usuário chamado user_admin e que :

- é um usuário windows
- deve pertencer ao grupo de gid=512 (grupo 'Domain Admins')
- tem um diretório em home
- não tem um login shell
- tem um homeDirectory difinido para /dev/null
- não tem um roaming profile
- e para quem nós queremos definir uma senha para o primeiro login

Você deve executar assim:

```
smbldap-useradd -a -G 512 -m -s /bin/false -d /dev/null -F "" -P user_admin
```

4.2.2 Removendo um usuário

Para remover uma conta de usuário, use o script smbldap-userdel. As opções disponíveis são

opção	definição
-r	remover o diretório home
-R	remover o diretório home interativamente

Table 3: Opções disponíveis para o script smbldap-userdel

Por exemplo, se você quiser remover a conta user1 do diretório LDAP, e se também quiser deletar seu diretório home, use o seguinte comando :

```
smbldap-userdel -r user1
```

OBS: '-r' é perigoso visto que ele pode deletar dados preciosos e não backupeados, por favor seja cauteloso.

4.2.3 Modificando um usuário

Para modificar uma conta de usuário, use o script smbldap-usermod. As opções disponíveis estão listadas na tabela 4.

opção	definição	Exemplo
-c	define o gecos do usuário	-c "admin user"
-d	define o diretório home	-d /var/user
-u	define um valor uid	-u 1003
-g	define um valor gid	-g 1003

-G	adiciona a nova conta para um ou vários grupos suplementares (separados por vírgula)	-G 512,550
		-G -512,550
		-G +512,550
-s	define o login shell	-s /bin/ksh
-N	define o nome canônico do usuário	
-S	define o sobrenome do usuário	
-P	termina por invocar smbldap-passwd para definir a senha dos usuários	
-a	adiciona sambaSAMAccount objectclass	
-e	define uma data de expiração para a senha (formato: YYYY-MM-DD HH:MM:SS)	
-A	o usuário pode mudar a senha ? 0 se não, 1 se sim	-A 1
-B	o usuário deve mudar a senha na primeira seção ? 0 se não, 1 se sim	-B 1
-C	define o compartilhamento home do samba	-C \\PDC\homes
		-C ""
-D	define uma letra associada com o compartilhamento home	-D H:
		-D ""
-E	define o script DOS para executar no login	-E common.bat
		-E ""
-F	define o diretório dos perfís	-F \\PDC\profiles\user
		-F ""
-H	define os bits de controle da conta samba como '[NDHTUMWSLKI]'	-H [X]
-I	disabilita uma conta de usuário	-I 1
-J	habilita um usuário	-J 1
-M	endereços de email local (separado por vírgula)	-M testuser,aliasuser
-T	endereços para repasse de email (separado por vírgula)	-T testuser@domain.org

Table 4: Opções disponíveis para o script smbldap-usermod

4.3 Gerenciamento de Grupos

4.3.1 Adicionando um grupo

Para adicionar um novo grupo no diretório LDAP, use o script smbldap-groupadd. As opções disponíveis são listadas na tabela 5.

opção	definição	Exemplo
-a	adiciona entrada de mapeamento automático de grupo	
-g gid	define o gidNumer para este grupo como gid	-g 1002
-o	gidNumber não é único	
-r group-rid	define o rid do grupo como group-rid	-r 1002
-s group-sid	define o sid do grupo como group-sid	-s S-1-5-21-3703471949-3718591838-2324585696-1002
-t group-type	define o sambaGroupType como group-type	-t 2
-p	imprimir o gidNumber para a saída padrão	

Table 5: Opções disponíveis para o script smbldap-groupadd

4.3.2 Removendo um grupo

Para remover o grupo chamado group1, use o seguinte comando :

```
smbldap-userdel group1
```

4.4 Adicionando uma conta de confiança interdomain

Para adicionar uma conta de confiança interdomain para o controlador primário trust-pdc, use a opção -i do smbldap-useradd como segue :

```
[root@etoile root]# smbldap-useradd -i trust-pdc
New password : *******
Retype new password : *******
```

O script irá terminar pedindo por uma senha para esta conta de confiança. A conta será criada no ramo do diretório onde todas as contas de computadores são armazenadas (por padrão ou=Computers). As duas únicas particularidades desta conta são que você está definindo uma senha para a conta, e as opções desta conta é apenas [I].

5 Samba e os scripts smbldap-tools

5.1 Configuração geral

O Samba pode ser configurado para usar os scripts smbldap-tools. Isto permite aos administradores adicionar, deletar ou modificar contas de usuários e grupos para sistemas operacionais Microsoft Windows usando, por exemplo, o utilitário Gerenciador de Usuários sob MS-Windows. Para

habilitar o uso deste utilitário, o Samba precisa ser configurado corretamente. O arquivo de configuração smb.conf deve conter as seguintes diretivas:

```
ldap delete dn = Yes
add user script = /usr/local/sbin/smbldap-useradd -m "%u"
add machine script = /usr/local/sbin/smbldap-useradd -w "%u"
add group script = /usr/local/sbin/smbldap-groupadd -p "%g"
add user to group script = /usr/local/sbin/smbldap-groupmod -m "%u" "%g"
delete user from group script = /usr/local/sbin/smbldap-groupmod -x "%u" "%
g"
set primary group script = /usr/local/sbin/smbldap-usermod -g "%g" "%u"
```

Observação: as duas diretivas **delete user script** e **delete group script** também podem ser usadas. Todavia, uma mensagem de erro pode aparecer no Gerenciador de Usuários mesmo se a operação for bem sucedida. Se você quiser habilitar este comportamento, você precisa adicionar

```
delete user script = /usr/local/sbin/smbldap-userdel "%u"
delete group script = /usr/local/sbin/smbldap-groupdel "%g"
```

5.2 Migrado um NT4 PDC para o Samba3

O procedimento de migração de contas torna-se realmente mais simples quando o samba for configurado para usar o smbldap-tools. A configuração do samba (arquivo smb.conf) deve conter as diretivas definidas acima para adequadamente chamar os scripts para gerenciar as contas de usuários, grupos e computadores. O processo de migração é esboçado no capítulo 30 do samba howto: http://sambafr.idealx.org/samba/docs/man/Samba-HOWTO-Collection/NT4Migration.html.

6 Perguntas Frequentes

6.1 Como eu posso usar uidNumber e gidNumber já liberados?

Há duas maneiras de fazer isto :

- modifique o cn=NextFreeUnixId,dc=idealx,dc=org e mude os valores uidNumber e/ou gidNumber. Isto deve ser feito manualmente. Por exemplo, se você quiser usar todos os uidNumber e gidNumber disponíveis maiores que 1500, você precisa criar um arquivo update-NextFreeUnixId.ldif contendo :

  ```
  dn: cn=NextFreeUnixId,dc=idealx,dc=org
  changetype: modify
  uidNumber: 1500
  gidNumber: 1500
  ```

e então atualizar o diretório:

```
ldapmodify -x -D "cn=Manager,dc=idealx,dc=org" -w secret -f update-NextFreeUnixId.ldif
```

- usar a opção -u ou -g com o script que você precisa para definir o valor que você quer usar

6.2 Eu sempre tenho este erro: "Can't locate IO/Socket/SSL.pm"

Isto acontece quando você quer usar um certificado. Neste caso, você precisa instalar o módulo Perl IO-Socket-SSL.

6.3 Eu não consgigo inicializar o diretório com smbldap-populate

Quando eu quero inicializar o diretório usando o script smbldap-populate, eu obtenho

```
[root@slave sbin]# smbldap-populate.pl
  Using builtin directory structure
  adding new entry: dc=IDEALX,dc=COM
  Can't call method "code" without a package or object reference at
  /usr/local/sbin/smbldap-populate.pl line 270, <GEN1> line 2.
```

Resposta: verifique a configuração TLS

- se você não quiser usar o suporte TLS, defina no arquivo /etc/smbldap-tools/smbldap.conf com

  ```
  ldapSSL="0"
  ```

- se você quiser o suporte TLS, defina no arquivo /etc/smbldap-tools/smbldap.conf com

  ```
  ldapSSL="1"
  ```

  e verifique que o servidor de diretórios está configurado para aceitar conexões TLS.

6.4 Eu não consigo juntar ao domínio com a conta do root

- verifique que a conta do root tem o sambaSamAccount objectclass
- verifique que a diretiva add machine script está presente e configurada

6.5 Eu tenho a sambaSamAccount mas não consigo logar

Verifique se o atributo sambaPwdLastSet não é nulo (igual a 0)

6.6 Eu quero criar contas de máquina 'on the fly', porém isto não funciona ou eu devo fazer duas vezes

- O script definido com o add machine script não deve adicionar o sambaSAMAccount objectclass da conta de máquina. O script deve apenas adicionar a conta de máquina Posix. O Samba irá adicionar o sambaSAMAccount quando juntando ao domínio.
- Verifique que o **add machine script** está presente no arquivo de configuração do samba.

6.7 Eu nãoconsigo gerenciar a Oracle Internet Database

Se você tiver uma mensagem de erro como:

```
Function Not Implemented at /usr/local/sbin/smbldap_tools.pm line 187.
Function Not Implemented at /usr/local/sbin/smbldap_tools.pm line 627.
```

Para a Oracle Database, todos os atributos que serão solicitados ao diretório devem ser indexados. Adicione um novo index para os atributos do samba e certifique-se que os seguintes atributos também sejam indexados: uidNumber, gidNumber, memberUid, homedirectory, description, userPassword ...

6.8 A diretiva passwd program = /usr/local/sbin/smbldap-passwd -u %u não é chamada, ou eu recebo uma mensagem de erro quando mudando a senha pelo windows

A diretiva é chamada se você também definiu unix password sync = Yes.
Observações:

- se você usa OpenLDAP, nenhuma destas duas opções são necessárias. Você precisa apenas de ldap passwd sync = Yes.
- o script chamado aqui deve apenas atualizar o atributo userPassword. Esta é a razão para a opção -u. As senhas do samba serão atualizadas pelo próprio samba.
- a diretiva passwd chat deve combinar o que é digitado quando usando o comando smbldap-passwd

6.9 A conta de novos computadores não pode ser definida em ou=computers

Isto é um bug conhecido do samba. Há uma solução de contorno (workaround): veja em http://marc.theaimsgroup.com/?l=samba&m=108439612826440&w=2

6.10 Eu consigo juntar ao domínio, mas não consigo logar

veja a seção 6.9

6.11 Eu não consigo criar um usuário com smbldap-useradd

Quando criando uma nova conta de usuário, eu recebo a seguinte mensagem de erro:

```
/usr/local/sbin/smbldap-useradd.pl: unknown group SID not set for unix group 513
```

Resposta:

- o nss_ldap está corretamente configurado ?
- o grupo padrão dos usuários está mapeado para o grupo 'Domain Users' do NT ?

  ```
  net groupmap add rid=513 unixgroup="Domain Users" ntgroup="Domain Users"
  ```

6.12 smbldap-useradd: Não posso chamar o método "get_value" em um valor não definido em /usr/local/sbin/smbldap-useradd, linha 154

- o grupo padrão definido em smbldap.conf existe (defaultUserGid="513") ?
- o grupo NT "Domain Users" está mapeado para um grupo unix de rid 513 (veja opção -r do smbldap-groupadd e smbldap-groupmod para definir um rid) ?

6.13 Eu obtive erros criando um novo usuário ou novo grupo

- eu obtive o seguinte erro:

  ```
  Could not find base dn, to get next uidNumber at /usr/local/sbin//smbldap_tools.pm line 909
  ```

  Você atualizou o smbldap-tools para versão 0.8.5 ou mais recente, mas você não criou o objeto para definir o next uidNumber e gidNumber disponível. Você tem de fazer isto manualmente. Crie um arquivo chamado add.ldif contendo o seguinte:

  ```
  dn: cn=NextFreeUnixId,dc=idealx,dc=org
  objectClass: inetOrgPerson
  objectClass: sambaUnixIdPool
  uidNumber: 1000
  gidNumber: 1000
  cn: NextFreeUnixId
  sn: NextFreeUnixId
  ```

e então adicione o objeto com o utilitário ldapadd:

```
$ ldapadd -x -D "cn=Manager,dc=idealx,dc=org" -w secret -f add.ldif
```

Aqui, 1000 é o primeiro valor disponível para uidNumber e gidNumber (naturalmente, se este valor já for usado por um usuário ou grupo, o próximo valor disponível depois de 1000 será utilizado).

- eu recebi o seguinte erro:

```
Use of uninitialized value in string at
/usr/local/sbin//smbldap\_tools.pm line 914.
Error: No DN specified at /usr/local/sbin//smbldap\_tools.pm line 919
```

Você não atualizou o arquivo de configuração para definir os objetos onde são armazenados os próximos uidNumber e gidNumber disponíveis. Em nosso exemplo, você tem de adicionar uma entrada em /etc/smbldap-tools/smbldap.conf contendo:

```
# Where to store next uidNumber and gidNumber available
sambaUnixIdPooldn="cn=NextFreeUnixId,${suffix}"
```

a propósito, agora uma nova opção também está disponível: o domínio para juntar aos usuários. Você pode adicionar ao arquivo de configuração as seguintes linhas:

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

- eu tive o seguinte erro:

```
Use of uninitialized value in concatenation (.) or string at /
usr/local/sbin/smbldap-useradd line 183.
Use of uninitialized value in substitution (s///) at /
usr/local/sbin/smbldap-useradd line 185.
Use of uninitialized value in string at /usr/local/sbin/smbldap-
useradd line 264.
failed to add entry: homedirectory: value #0 invalid per syntax at /
usr/local/sbin/smbldap-useradd line 280.
userHomeDirectory=User "jto" already member of the group "513".
failed to add entry: No such object at /usr/local/sbin/smbldap-useradd
line 382.
```

você tem que mudar o nome da variável userHomePrefix para userHome em /etc/smbldap-tools/smbldap.conf

-
- eu tive o seguinte erro:

```
failed to add entry: referral missing at /usr/local/sbin/smbldap-
useradd line 279, <DATA> line 283.
```

você tem que atualizar o arquivo de configuração que definiu o dn dos usuários, grupos e computadores. Aqueles parâmetros não devem ser relativos ao parâmetro sufixo. Uma configuração típica parece com isto:

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

```
computersdn="ou=Computers,${suffix}"
groupsdn="ou=Groups,${suffix}"
```

7 Agradecimentos

Pessoas que trabalharam neste documento:

- Jérôme Tournier <jerome.tournier@IDEALX.com>
- David Barth <david.barth@IDEALX.com>
- Nat Makarevitch <nat@IDEALX.com>

Os autores gostariam de agradecer as seguintes pessoas por fornecerem ajuda com alguns dos assuntos mais complicados, por esclarecerem alguns dos funcionamentos internos do Samba ou OpanLDAP, por indicarem erros os enganos em versões anteriores deste documento, ou geralmente por fazerem sugestões:

- equipe IDEALX :
  - Roméo Adekambi <romeo.adekambi@IDEALX.com>
  - Aurelien Degremont <adegremont@IDEALX.com>
  - Renaud Renard <rrenard@IDEALX.com>
- John H Terpstra <jht@samba.org>

8 Anexos

8.1 Arquivos de configuração completos

8.1.1 O arquivo /etc/smbldap-tools/smbldap.conf

```
# $Source: /opt/cvs/samba/smbldap-tools/smbldap.conf,v $
# $Id: smbldap.conf,v 1.14 2004/06/25 20:57:51 jtournier Exp $
#
# smbldap-tools.conf : Q & D configuration file for smbldap-tools
#  This code was developped by IDEALX (http://IDEALX.org/) and
#  contributors (their names can be found in the CONTRIBUTORS file).
#
#                 Copyright (C) 2001-2002 IDEALX
#
#  This program is free software; you can redistribute it and/or
#  modify it under the terms of the GNU General Public License
#  as published by the Free Software Foundation; either version 2
#  of the License, or (at your option) any later version.
#
#  This program is distributed in the hope that it will be useful,
#  but WITHOUT ANY WARRANTY; without even the implied warranty of
#  MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
#  GNU General Public License for more details.
#
#  You should have received a copy of the GNU General Public License
#  along with this program; if not, write to the Free Software
#  Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307,
#  USA.
#  Purpose :
#       . be the configuration file for all smbldap-tools scripts
```

```
##############################################################################
##
#
# General Configuration
#
##############################################################################
##
# Put your own SID
# to obtain this number do: net getlocalsid
SID="S-1-5-21-1911238739-97561441-2706018148"
##############################################################################
##
#
# 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)
# Ex: slaveLDAP=127.0.0.1
slaveLDAP="127.0.0.1"
slavePort="389"
# Master LDAP : needed for write operations
# Ex: masterLDAP=127.0.0.1
masterLDAP="127.0.0.1"
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)
ldapTLS="1"
# 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.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.key"
# LDAP Suffix
# Ex: suffix=dc=IDEALX,dc=ORG
suffix="dc=idealx,dc=org"
# Where are stored Users
# Ex: usersdn="ou=Users,dc=IDEALX,dc=ORG"
usersdn="ou=Users,${suffix}"
# Where are stored Computers
# Ex: computersdn="ou=Computers,dc=IDEALX,dc=ORG"
computersdn="ou=Computers,${suffix}"
# Where are stored Groups
# Ex groupsdn="ou=Groups,dc=IDEALX,dc=ORG"
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"
idmapdn="ou=Idmap,${suffix}"
# Where to store next uidNumber and gidNumber available
sambaUnixIdPooldn="cn=NextFreeUnixId,${suffix}"
# Default scope Used
scope="sub"
# Unix password encryption (CRYPT, MD5, SMD5, SSHA, SHA)
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"
# 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="99"
##############################################################################
##
#
# SAMBA Configuration
#
##############################################################################
##
# The UNC path to home drives location (%U username substitution)
# Ex: \\My-PDC-netbios-name\homes\%U
# Just set it to a null string if you want to use the smb.conf 'logon home'
# directive and/or disable roaming profiles
userSmbHome="\\PDC-SMB3\homes\%U"
# The UNC path to profiles locations (%U username substitution)
# Ex: \\My-PDC-netbios-name\profiles\%U
# Just set it to a null string if you want to use the smb.conf 'logon path'
# directive and/or disable roaming profiles
userProfile="\\PDC-SMB3\profiles\%U"
# The default Home Drive Letter mapping
# (will be automatically mapped at logon time if home directory exist)
# Ex: H: for H:
```

```
userHomeDrive="H:"
# 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: %U.cmd
# 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
mailDomain="idealx.com"
##############################################################################
##
#
# 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"
```

8.1.2 O arquivo /etc/smbldap-tools/smbldap_bind.conf

```
############################
# Credential Configuration #
############################
# Notes: you can specify two differents configuration if you use a
# master ldap for writing access and a slave ldap server for reading access
# By default, we will use the same DN (so it will work for standard Samba
# release)
slaveDN="cn=Manager,dc=idealx,dc=org"
slavePw="secret"
masterDN="cn=Manager,dc=idealx,dc=org"
masterPw="secret"
```

8.1.3 O arquivo de configuração do samba: /etc/samba/smb.conf

```
# Global parameters
[global]
        workgroup = SMB3
        netbios name = PDC-SMB3
        interfaces = 192.168.5.11
        username map = /etc/samba/smbusers
        #admin users= @"Domain Admins"
        server string = Samba Server %v
        security = user
        encrypt passwords = Yes
        min passwd length = 3
        obey pam restrictions = No
        ldap passwd sync = Yes
        #unix password sync = Yes
        #passwd program = /usr/local/sbin/smbldap-passwd -u %u
        #passwd chat = "Changing password for*\nNew password*" %n\n "*Retype
new password*" %n\n"
        ldap passwd sync = Yes
        log level = 0
        syslog = 0
        log file = /var/log/samba/log.%m
```

```
        max log size = 100000
        time server = Yes
        socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
        mangling method = hash2
        Dos charset = 850
        Unix charset = ISO8859-1
        logon script = logon.bat
        logon drive = H:
        logon home =
        logon path =
        domain logons = Yes
        os level = 65
        preferred master = Yes
        domain master = Yes
        wins support = Yes
        passdb backend = ldapsam:ldap://127.0.0.1/
                        #   passdb   backend   =   ldapsam:"ldap://127.0.0.1/
ldap://slave.idealx.com"
 # ldap filter = (&(objectclass=sambaSamAccount)(uid=%u))
        ldap admin dn = uid=samba,ou=Users,dc=idealx,dc=com
        ldap suffix = dc=idealx,dc=com
        ldap group suffix = ou=Groups
        ldap user suffix = ou=Users
        ldap machine suffix = ou=Computers
        ldap idmap suffix = ou=Users
        ldap ssl = start tls
        add user script = /usr/local/sbin/smbldap-useradd -m "%u"
        ldap delete dn = Yes
        #delete user script = /usr/local/sbin/smbldap-userdel "%u"
        add machine script = /usr/local/sbin/smbldap-useradd -w "%u"
        add group script = /usr/local/sbin/smbldap-groupadd -p "%g"
        #delete group script = /usr/local/sbin/smbldap-groupdel "%g"
         add user to group script = /usr/local/sbin/smbldap-groupmod -m "%u"
"%g"
         delete user from group script = /usr/local/sbin/smbldap-groupmod -x
"%u" "%g"
          set primary group script = /usr/local/sbin/smbldap-usermod -g "%g"
"%u"
        # printers configuration
        printer admin = @"Print Operators"
        load printers = Yes
        create mask = 0640
        directory mask = 0750
        nt acl support = No
        printing = cups
        printcap name = cups
        deadtime = 10
        guest account = nobody
        map to guest = Bad User
        dont descend = /proc,/dev,/etc,/lib,/lost+found,/initrd
        show add printer wizard = yes
          ; to maintain capital letters in shortcuts in any of the profile
folders:
        preserve case = yes
        short preserve case = yes
        case sensitive = no
[homes]
        comment = repertoire de %U, %u
        read only = No
```

```
        create mask = 0644
        directory mask = 0775
        browseable = No
[netlogon]
        path = /home/netlogon/
 browseable = No
        read only = yes
[profiles]
        path = /home/profiles
        read only = no
        create mask = 0600
        directory mask = 0700
        browseable = No
        guest ok = Yes
        profile acls = yes
        csc policy = disable
        # next line is a great way to secure the profiles
        force user = %U
        # next line allows administrator to access all profiles
        valid users = %U "Domain Admins"
[printers]
        comment = Network Printers
        printer admin = @"Print Operators"
        guest ok = yes
        printable = yes
        path = /home/spool/
        browseable = No
        read only  = Yes
        printable = Yes
        print command = /usr/bin/lpr -P%p -r %s
        lpq command = /usr/bin/lpq -P%p
        lprm command = /usr/bin/lprm -P%p %j
[print$]
        path = /home/printers
        guest ok = No
        browseable = Yes
        read only = Yes
        valid users = @"Print Operators"
        write list = @"Print Operators"
        create mask = 0664
        directory mask = 0775
[public]
        comment = Repertoire public
        path = /home/public
 browseable = Yes
        guest ok = Yes
        read only = No
        directory mask = 0775
        create mask = 0664
```

8.1.4 O arquivo de configuração do OpenLDAP : /etc/openldap/slapd.conf

```
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
schemacheck on
lastmod  on
```

```
TLSCertificateFile /etc/openldap/ldap.idealx.com.pem
TLSCertificateKeyFile /etc/openldap/ldap.idealx.com.key
TLSCACertificateFile /etc/openldap/ca.pem
TLSCipherSuite :SSLv3
#TLSVerifyClient demand
#######################################################################
# ldbm database definitions
#######################################################################
database ldbm
suffix  dc=idealx,dc=com
rootdn  "cn=Manager,dc=idealx,dc=com"
rootpw  secret
directory /var/lib/ldap
index    sambaSID    eq
index    sambaPrimaryGroupSID    eq
index    sambaDomainName    eq
index objectClass,uid,uidNumber,gidNumber,memberUid eq
index cn,mail,surname,givenname   eq,subinitial
# users can authenticate and change their password
access to attrs=userPassword,sambaNTPassword,sambaLMPassword
      by dn="cn=Manager,dc=idealx,dc=com" write
      by self write
      by anonymous auth
      by * none
# all others attributes are readable to everybody
access to *
      by * read
```

8.2 Mudando a conta administrativa (ldap admin dn no arquivo smb.conf)

Se você não quiser mais usar a conta cn=Manager,dc=idealx,dc=com, você pode criar uma conta dedicada para o Samba e os scripts smbldap-tools. Para fazer isto, crie uma conta chamada samba como segue (veja a seção 4.2.1 para uma sintaxe mais detalhada) :

```
smbldap-useradd -s /bin/false -d /dev/null -P samba
```

Este comando irá pedir a você que defina uma senha para esta conta. Vamos definí-la como samba para este exemplo. Você então precisa modificar os arquivos de configuração:

- arquivo /etc/smbldap-tools/smbldap_bind.conf

  ```
  slaveDN="uid=samba,ou=Users,dc=idealx,dc=com"
  slavePw="samba"
  masterDN="uid=samba,ou=Users,dc=idealx,dc=com"
  masterPw="samba"
  ```

- arquivo /etc/samba/smb.conf

  ```
  ldap admin dn = uid=samba,ou=Users,dc=idealx,dc=com
  ```

  não esqueça de também definir a senha da conta samba no arquivo secrets.tdb:

```
smbpasswd -w samba
```

- arquivo /etc/openldap/slapd.conf: dê ao usuário samba permissão de modificar alguns atributos: este usuário precisa ser capaz de modificar todos os atributos do samba e alguns outros (uidNumber, gidNumber ...) :

```
# users can authenticate and change their password
access                                                                  to
attrs=userPassword,sambaNTPassword,sambaLMPassword,sambaPwdLastSet,sam
baPwdMustChange
      by dn="uid=samba,ou=Users,dc=idealx,dc=com" write
      by self write
      by anonymous auth
      by * none
# some attributes need to be readable anonymously so that 'id user'
can answer correctly
access                                                                  to
attrs=objectClass,entry,gecos,homeDirectory,uid,uidNumber,gidNumber,cn
,memberUid
      by dn="uid=samba,ou=Users,dc=idealx,dc=com" write
      by * read
# somme attributes can be writable by users themselves
access to attrs=description,telephoneNumber
      by dn="uid=samba,ou=Users,dc=idealx,dc=com" write
      by self write
      by * read
# some attributes need to be writable for samba
access                                                                  to
attrs=cn,sambaLMPassword,sambaNTPassword,sambaPwdLastSet,sambaLogonTim
e,sambaLogoffTime,sambaKickoffTime,sambaPwdCanChange,sambaPwdMustChang
e,sambaAcctFlags,displayName,sambaHomePath,sambaHomeDrive,sambaLogonSc
ript,sambaProfilePath,description,sambaUserWorkstations,sambaPrimaryGr
oupSID,sambaDomainName,sambaSID,sambaGroupType,sambaNextRid,sambaNextG
roupRid,sambaNextUserRid,sambaAlgorithmicRidBase
      by dn="uid=samba,ou=Users,dc=idealx,dc=com" write
      by self read
      by * none
# samba need to be able to create the samba domain account
access to dn.base="dc=idealx,dc=com"
      by dn="uid=samba,ou=Users,dc=idealx,dc=com" write
      by * none
# samba need to be able to create new users account
access to dn="ou=Users,dc=idealx,dc=com"
      by dn="uid=samba,ou=Users,dc=idealx,dc=com" write
      by * none
# samba need to be able to create new groups account
access to dn="ou=Groups,dc=idealx,dc=com"
      by dn="uid=samba,ou=Users,dc=idealx,dc=com" write
      by * none
# samba need to be able to create new computers account
access to dn="ou=Computers,dc=idealx,dc=com"
      by dn="uid=samba,ou=Users,dc=idealx,dc=com" write
      by * none
# this can be omitted but we leave it: there could be other branch
# in the directory
access to *
      by self read
      by * none
```

8.3 Erros conhecidos

- Opção -B (usuário deve mudar a senha) do smbldap-useradd não tem efeito: quando o script smbldap-passwd é chamado, o atributo sambaPwdMustChange é re-escrito.