Integrando o Samba ao LDAP usando modelo config=cn

By admin on 19 de novembro de 2012 in LDAP, Linux
18 Flares Twitter 2 Facebook 7 Google+ 4 LinkedIn 5 Email -- Filament.io **18** Flares ×

Vimos em dois Posts anteriores à configuração do Servidor LDAP e como configurar o cliente LDAP que são pré-requisitos para esse novo Post.

Neste artigo iremos configurar o samba para autenticar na Base LDAP atuando como PDC numa rede Microsoft.

Como a configuração do Servidor já está pronto, partindo que os Posts anteriores foram seguidos, neste iremos popular a base e configurar o nosso servidor Samba. E todo esse trabalho será feito usando o padrão novo do LDAP o cn=config e não mais o arquivo de configuração.

Então vamos ao trabalho.

O primeiro passo é instalar o samba e o que for necessário para configuração de ambos.

Em seguida iremos converter o schema do samba para o novo formato do LDAP, trabalhando diretamente com arquivos do tipo LDIF.

root@local:~# apt-get install samba-doc root@local:~# cp /usr/share/doc/samba-doc/examples/LDAP/samba.schema.gz /etc/ldap/schema/

root@local:~#gzip –d /etc/ldap/schema/samba.schema.gz

root@local:~#vim schema_convert.conf

#Criando novos schemas, adicione todos os schemas que serão migrados

include /etc/ldap/schema/core.schema include /etc/ldap/schema/collective.schema include /etc/ldap/schema/corba.schema include /etc/ldap/schema/cosine.schema include /etc/ldap/schema/duaconf.schema include /etc/ldap/schema/dyngroup.schema include

/etc/ldap/schema/inetorgperson.schema include /etc/ldap/schema/java.schema include /etc/ldap/schema/misc.schema include /etc/ldap/schema/nis.schema include /etc/ldap/schema/openldap.schema include /etc/ldap/schema/ppolicy.schema include /etc/ldap/schema/samba.schema

root@local:~# mkdir -p ./tmp/ldif_output

root@local:~# slapcat -f schema_convert.conf -F ./tmp/ldif_output -n0 -s "cn={12}samba,cn=schema,cn=config" > ./tmp/cn=samba.ldif

root@local:~# vi ./tmp/cn=samba.ldif

Neste passo acima já convertemos o schema para o novo padrão do LDAP, iremos alterar alguns itens para não termos problemas, futuros. Devemos editar o arquivo novo criado cn=samba.ldif

root@local:~# vim ./tmp/cn=samba.ldif

#Linha 1 até 3: altere o valor removendo o "{12}"

dn: cn=samba,cn=schema,cn=config

objectClass: olcSchemaConfig

cn: samba

#Remova as linhas abaixo (Estão na parte de baixo do arquivo de configuração)

structuralObjectClass: olcSchemaConfig entryUUID: bd8a7a82-3cb8-102f-8d5f-070b4e5d16f8 creatorsName: cn=config createTimestamp: 20100815125953Z entryCSN: 20100815125953.198505Z#000000#000#000000 modifiersName: cn=config modifyTimestamp: 20100815125953Z

Agora que já editamos os valores do arquivo LDIF iremos importar para a Base LDAP. O esquema de importação também está um pouco diferente, vejamos.

```
root@local:~# ldapadd -Y EXTERNAL -H ldapi:/// -f ./tmp/cn=samba.ldif

SASL/EXTERNAL authentication started

SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth

SASL SSF: 0

adding new entry “cn=samba,cn=schema,cn=config”



root@local:~# /etc/init.d/slapd restart
```

Agora iremos popular nossa base, mas para tanto iremos instalar o samba propriamente dito. E as ferramentas de samba ldap.

```
root@local:~#  apt-get install samba smbldap-tools
```

Neste Post iremos usar um arquivo de configuração de exemplo que já vem com o Samba, e após copia-lo iremos alterar conforme nossa necessidade.

Lembrando que seguindo os Posts anteriores, estarei usando o dominiolinux.net, e serão necessários alterar alguns itens conforme mencionado abaixo:

```
root@local:~#mv /etc/samba/smb.conf /etc/samba/smb.conf.bak

root@local:~#cp /usr/share/doc/smbldap-tools/smb.conf /etc/samba/smb.conf

root@local:~#vim /etc/samba/smb.conf
```

#Linha 3 alterar grupo de trabalho/Dominio

workgroup = DOMINIOLINUX

#Comentar Linha 12

#min passwd length = 3

#Linha 22 alterar para o valor abaixo

ldap passwd sync = yes

#Linha 48 alterar para o usuário correto

ldap admin dn = cn=admin,dc=dominiolinux,dc=net

#Linha 50 alterar para seus respectivos valores

ldap suffix = dc=dominiolinux,dc=net

ldap group suffix = ou=groups

ldap user suffix = ou=people

#Linha 60 Descomente

delete group script = /usr/sbin/smbldap-groupdel “%g”

#Linha 64 especifique o administrador e remova o uso de SSL

admin users = domainadm

ldap ssl = no

Neste arquivo alterar os valores conforme necessários, tais como : Dominio, sincronização de senhas, administrador do LDAP, Domínio LDAP, prefixo para usuários e grupos, e no final quem é o administrador , seguido da linha que remove ssl para ldap.

Para usuários de domínio é comum o uso de script logon entre outros para isso é necessário à criação do diretório **netlogon,** que já está configurado no nosso smb.conf.

Aqui deixo uma cópia do smb.conf usando neste post, para baixar clique aqui.

```
root@local:~# mkdir /home/netlogon
```

Agora já podemos reiniciar nosso servidor samba.

```
/etc/init.d/samba restart
```

Acredito que até agora não tenhamos nenhum problema. Se erros ocorrerem verifique novamente os arquivos de configuração do samba, e os procedimentos de adicionar o schema do samba ao ldap.

O próximo passo será adicionar a senha do Ldap para o samba e enfim , popularmos nossa base LDAP. No procedimento abaixo iremos adicionar a senha do LDAP no samba e iremos criar o arquivo de base para podermos popular a base LDAP.

O script "**configure.pl"** , é um script em perl que nos auxiliar a criar as entradas necessárias no samba, para podermos popular, de outra forma , se torna bastante trabalhoso e a chance de erramos na digitação é bem grande.

```
root@local:~# smbpasswd -W

Setting stored password for "cn=admin,dc=dominiolinux,dc=net" in secrets.tdb

New SMB password:

Retype new SMB password:
```

```
root@local:~# gzip -d /usr/share/doc/smbldap-tools/configure.pl.gz

root@local:~# perl /usr/share/doc/smbldap-tools/configure.pl


$# is no longer supported at /usr/share/doc/smbldap-tools/configure.pl line 314.

-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-

       smbldap-tools script configuration

       -=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

Before starting, check

 . if your samba controller is up and running.

 . if the domain SID is defined (you can get it with the ‘net getlocalsid’)


 . you can leave the configuration using the Crtl-c key combination

 . empty value can be set with the “.” character

-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-

Looking for configuration files…


Samba Configuration File Path [/etc/samba/smb.conf] >


The default directory in which the smbldap configuration files are stored is
shown.

If you need to change this, enter the full directory path, then press enter to
continue.

Smbldap-tools Configuration Directory Path [/etc/smbldap-tools/] >

-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

Let’s start configuring the smbldap-tools scripts …
```

. workgroup name: name of the domain Samba act as a PDC

workgroup name [DOMINIOLINUX] > **#ENTER**

. netbios name: netbios name of the samba controler

netbios name [PDC-SRV] > **#ENTER**

. logon drive: local path to which the home directory will be connected (for NT Workstations). Ex: 'H:' **#ENTER**

logon drive [H:] > **#ENTER**

. logon home: home directory location (for Win95/98 or NT Workstation).

(use %U as username) Ex:'\PDC-SRV%U'

logon home (press the "." character if you don't want homeDirectory) [\PDC-SR V%U] > **#ENTER**

. logon path: directory where roaming profiles are stored. Ex:'\PDC-SRVprofile s%U' logon path (press the "." character if you don't want roaming profile) [\PDC-SRVprofiles%U] > . **#PONTO**

. home directory prefix (use %U as username) [/home/%U] >**#ENTER**

. default users' homeDirectory mode [700] >**#ENTER**

. default user netlogon script (use %U as username) [logon.bat] >**#ENTER**

default password validation time (time in days) [45] >**#ENTER**

. ldap suffix [dc=dominiolinux,dc=net] >**#ENTER**

. ldap group suffix [ou=groups] >**#ENTER**

. ldap user suffix [ou=people] >**#ENTER**

. ldap machine suffix [ou=Computers] >**#ENTER**

. Idmap suffix [ou=Idmap] >**#ENTER**

. sambaUnixIdPooldn: object where you want to store the next uidNumber

and gidNumber available for new users and groups

sambaUnixIdPooldn object (relative to ${suffix})

[sambaDomainName=DOMINIOLINUX
] >**#ENTER**

. ldap master server: IP adress or DNS name of the master (writable) ldap server

ldap master server [127.0.0.1] >**#ENTER**

. ldap master port [389] >**#ENTER**

. ldap master bind dn [cn=admin,dc=dominiolinux,dc=net] >**#ENTER**

. ldap master bind password [] > **#SENHA LDAP DO ADMIN**

. ldap slave server: IP adress or DNS name of the slave ldap server: can also be the master one

ldap slave server [127.0.0.1] >**#ENTER**

. ldap slave port [389] >**#ENTER**

. ldap slave bind dn [cn=admin,dc=dominiolinux,dc=net] >**#ENTER**

. ldap slave bind password [] > **#SENHA LDAP DO ADMIN**

. ldap tls support (1/0) [0] > **#ENTER**

. SID for domain DOMINIOLINUX: SID of the domain (can be obtained with 'net getlocalsid PDC-SRV')

SID for domain DOMINIOLINUX [S-1-5-21-182168821-137747198-1560271109] >**#ENTER**

. unix password encryption: encryption used for unix passwords

unix password encryption (CRYPT, MD5, SMD5, SSHA, SHA) [SSHA] > **MD5**

. default user gidNumber [513] >**#ENTER**

. default computer gidNumber [515] >**#ENTER**

. default login shell [/bin/bash] >**#ENTER**

. default skeleton directory [/etc/skel] >**#ENTER**

. default domain name to append to mail adress [] >**#ENTER**

-=

Use of uninitialized value $# in concatenation (.) or string at /usr/share/doc/smbldap-

tools/configure.pl line 314, <STDIN> line 33.

backup old configuration files:

/etc/smbldap-tools/smbldap.conf->/etc/smbldap-tools/smbldap.conf.old

/etc/smbldap-tools/smbldap_bind.conf->/etc/smbldap-tools/smbldap_bind.conf.old

writing new configuration file:

/etc/smbldap-tools/smbldap.conf done.

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

Nos valores acima, usei quase tudo como padrão, alterando somente o tipo de criptografia para MD5,que é o padrão do Linux, e lógico colocamos a senha correta do servidor LDAP. Mas outros valores podem ser alterados conforme necessidade, por exemplo o logon script por padrão irá usar /home/netlogon/logon.bat, para alterar por exemplo para /home/netlogon/usuario.bat, devemos alterar os valores de "**default user netlogon script".** E no meu caso preferi não ter roaming profile, por isso ao final adicionei um ponto.

O próximo passo é o ato de popular o samba com LDAP, vejamos abaixo:

root@local:~# smbldap-populate Populating LDAP directory for domain DOMINIOLINUX (S-1-5-21-182168821-137747198-1560271109)

(using builtin directory structure)

entry dc=dominiolinux,dc=net already exist.

entry ou=people,dc=dominiolinux,dc=net already exist.

entry ou=groups,dc=dominiolinux,dc=net already exist.

adding new entry: ou=Computers,dc=dominiolinux,dc=net

adding new entry: ou=Idmap,dc=dominiolinux,dc=net

adding new entry: uid=root,ou=people,dc=dominiolinux,dc=net

adding new entry: uid=nobody,ou=people,dc=dominiolinux,dc=net

adding new entry: cn=Domain Admins,ou=groups,dc=dominiolinux,dc=net

adding new entry: cn=Domain Users,ou=groups,dc=dominiolinux,dc=net

adding new entry: cn=Domain Guests,ou=groups,dc=dominiolinux,dc=net

adding new entry: cn=Domain Computers,ou=groups,dc=dominiolinux,dc=net

adding new entry: cn=Administrators,ou=groups,dc=dominiolinux,dc=net

adding new entry: cn=Account Operators,ou=groups,dc=dominiolinux,dc=net

adding new entry: cn=Print Operators,ou=groups,dc=dominiolinux,dc=net

adding new entry: cn=Backup Operators,ou=groups,dc=dominiolinux,dc=net

adding new entry: cn=Replicators,ou=groups,dc=dominiolinux,dc=net

entry sambaDomainName=DOMINIOLINUX,dc=dominiolinux,dc=net already exist. Updating it…

Please provide a password for the domain root:

Changing UNIX and samba passwords for root

New password: **#senha do admin**

Retype new password: **#senha do admin**

Neste momento já está pronto o nosso servidor LDAP samba. Podemos verificar usando o **slapcat,** que nos trará grupos como: Replicators, Backup Operators, Print Operators, entre outros.

Agora precisamos criar a conta do administrador, que definimos no smb.conf, no caso domainadm, e criarmos contas de usuários.

root@local:~# smbldap-groupadd -a domainadm

root@local:~# smbldap-useradd -am -g domainadm domainadm

root@local:~# smbldap-passwd domainadm

#Criando usuário comum

root@local:~# smbldap-useradd –a ivan

root@local:~# smbldap-passwd ivan

Agora sim finalizado, com esses passos já podemos ingressar uma máquina Windows, no domínio, usando como conta de administrador a domainadm.

O processo de ingressar no domínio, não muda em nada de um PDC padrão Microsoft, será solicitado a conta de administrador, em nosso caso domainadm, e posteriormente será criado uma conta de máquina, dentro do Servidor LDAP.

Em meus teste , ingressei um Windows XP, sem nenhum problema, já atuando no Dominio.

Os compartilhamentos são comuns ao samba.

Logando Windows 7

Para ingressar uma máquina windows 7, alguns procedimentos em relação ao registro devem ser tomados. Alterações que farão , ou melhor , permitirão que o windows ingresse e logo no Dominio samba.

Peguei essa dica de http://www.vivaolinux.com.br/etc/prepara_win7_logar_samba.reg.

Abaixo o conteudo do arquivo de registro.

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINESYSTEMControlSet001servicesLanmanWorkstationParamet
ers]
"ServiceDll"=hex(2):25,00,53,00,79,00,73,00,74,00,65,00,6d,00,52,00,6f
,00,6f,
  00,74,00,25,00,5c,00,53,00,79,00,73,00,74,00,65,00,6d,00,33,00,32,00
,5c,00,
  77,00,6b,00,73,00,73,00,76,00,63,00,2e,00,64,00,6c,00,6c,00,00,00
"ServiceDllUnloadOnStop"=dword:00000001
"EnablePlainTextPassword"=dword:00000000
"EnableSecuritySignature"=dword:00000001
"RequireSecuritySignature"=dword:00000000
"OtherDomains"=hex(7):00,00
"DNSNameResolutionRequired"=dword:00000000
"DomainCompatibilityMode"=dword:00000001
[HKEY_LOCAL_MACHINESYSTEMControlSet001servicesNetlogonParameters]
"Update"="no"
```

```
"DisablePasswordChange"=dword:00000000
"MaximumPasswordAge"=dword:0000001e
"RequireSignOrSeal"=dword:00000001
"RequireStrongKey"=dword:00000001
"SealSecureChannel"=dword:00000001
"SignSecureChannel"=dword:00000001
[HKEY_LOCAL_MACHINESYSTEMCurrentControlSetControlLsa]
"auditbaseobjects"=dword:00000000
"auditbasedirectories"=dword:00000000
"crashonauditfail"=dword:00000000
"fullprivilegeauditing"=hex:00
"LimitBlankPasswordUse"=dword:00000001
"NoLmHash"=dword:00000001
"Notification
Packages"=hex(7):73,00,63,00,65,00,63,00,6c,00,69,00,00,00,00,00
"Security
Packages"=hex(7):6b,00,65,00,72,00,62,00,65,00,72,00,6f,00,73,00,00,
  00,6d,00,73,00,76,00,31,00,5f,00,30,00,00,00,73,00,63,00,68,00,61,00
,6e,00,
  6e,00,65,00,6c,00,00,00,77,00,64,00,69,00,67,00,65,00,73,00,74,00,00
,00,74,
  00,73,00,70,00,6b,00,67,00,00,00,70,00,6b,00,75,00,32,00,75,00,00,00
,00,00
"Authentication
Packages"=hex(7):6d,00,73,00,76,00,31,00,5f,00,30,00,00,00,00,
  00
"LsaPid"=dword:000001dc
"SecureBoot"=dword:00000001
"ProductType"=dword:00000001
"disabledomaincreds"=dword:00000000
"everyoneincludesanonymous"=dword:00000000
"forceguest"=dword:00000000
"restrictanonymous"=dword:00000000
"restrictanonymoussam"=dword:00000001
"LmCompatibilityLevel"=dword:00000001
```

Deixei o arquivo feito por Vitorio, disponivel para downlaod, para clicar aqui para baixar o arquivo prepara_win7_logar_samba.reg.

Com isso não terá problemas para ingressar e logar num dominio Samba. Baixe o arquivo e importe via regedit, ou ainda execute como administrador.

Abaixo uma video aula, exibindo todo o procedimento da 3 partes

1 – Configuranrando Servidor LDAP – http://stato.blog.br/wordpress/novo-modelo-ldap-server-configurando-servidor/

2 – Configurando Cliente LDAP -http://stato.blog.br/wordpress/configurando-ldap-cliente/

3 – Integrando LDAP e Samba – http://stato.blog.br/wordpress/integrando-samba-ldap/

Espero que aproveitem.

[youtube]http://www.youtube.com/watch?v=La_6QeUf0So[/youtube]