Instalação

Vamos atualizar os repositórios e vamos fazer um upgrade do sistema

```
yum check-update && yum update -y
```

Agora vamos instalar as dependências para podemos compilar o samba

```
yum install -y findutils readline glibc-devel findutils-locate gcc flex compat-readline5 ctdb-devel libldb-devel gcc-c++ make python libacl-devel libblkid-devel gnutls-devel readline-devel python-devel gdb pkgconfig krb5-devel cups-devel pam-devel nss-pam-ldapd openldap openldap-devel openldap-clients python-ldap

yum install -y openldap-devel pam-devel git gcc make wget  libacl-devel libblkid-devel gnutls-devel readline-devel python-devel cups-devel libaio-devel quota-devel ctdb-devel krb5-devel krb5-workstation acl setroubleshoot-server setroubleshoot-plugins policycoreutils-python libsemanage-python setools-libs-python setools-libs popt-devel libpcap-devel libidn-devel libxml2-devel libacl-devel libsepol-devel libattr-devel keyutils-libs-devel cyrus-sasl-devel cups-devel avahi-devel mingw32-iconv gamin libcap-devel rpc2-devel glusterfs-devel python-dns
```

Atenção para os programas já instalados pelo yum referente ao SAMBA. Desistale todos os que listarem.

```
rpm -qa | grep smb
rpm -qa | grep samba

Exemplo:
yum remove samba-winbind-clients samba-winbind samba-client samba-common
```

Agora vamos ajustar o fstab para que ele de suporte a acl,user_xattr e barrier eu vou habilitar isso na partição / se você tiver várias partições é bom habilitar em todas que você queira habilitar os compartilhamentos.

```
vim /etc/fstab
[...]
/dev/mapper/VolGroup-lv_root   /                                                 ext4
defaults,acl,user_xattr,barrier=1         1 1


Exemplo:

UUID=02e71e2a-9e29-4199-80e8-a7f2d2aa45b6 / ext4       defaults,acl,user xattr,barrier=1         1 1
UUID=efb1edd8-4317-4b75-ad0e-60eacdb8c764 /boot  ext4     defaults                               1 2
UUID=39d30164-34fb-43aa-b47b-ef85f0c055af /share ext4     defaults,acl,user xattr,barrier=1   1 2
UUID=2cee0f7b-d665-41f6-9c3a-2703933ff4b4 /users ext4     defaults,acl,user xattr,barrier=1   1 2
UUID=9cee9aee-9703-4cd1-ba2a-08544d1c23ca /usr   ext4     defaults,acl,user_xattr,barrier=1   1 2
UUID=f694aad6-72e9-48f2-acbc-17f443560a21 /usr/local ext4 defaults,acl,user_xattr,barrier=1   1 2
UUID=023c4c12-0b48-4049-97d6-58bbac20e71f swap            swap    defaults                    0 0
tmpfs                   /dev/shm                tmpfs   defaults        0 0
devpts                  /dev/pts                devpts  gid=5,mode=620  0 0
sysfs                   /sys                    sysfs   defaults        0 0
proc                    /proc                   proc    defaults        0 0
```

Agora vamos remontar a raiz

```
mount -o remount /

E as demais:

mount -o remount /share
mount -o remount /users
Etc…
```

Agora vamos listar os atributos da raiz

```
mount | egrep acl

/dev/sda2 on / type ext4 (rw,acl,user_xattr,barrier=1)
/dev/sdb1 on /share type ext4 (rw,acl,user_xattr,barrier=1)
/dev/sdc1 on /users type ext4 (rw,acl,user_xattr,barrier=1)
```

Agora os atributos já estão carregados.

Agora vamos testar o sistema de arquivos precisamos criar um arquivo e setar as flags de attr

```
touch test.txt

setfattr -n user.test -v test test.txt

setfattr -n security.test -v test2 test.txt
```

Agora testar o atributo user

```
getfattr -d test.txt

# file: test.txt

user.test="test"
```

Agora vamos testar o atributo security

```
getfattr -n security.test -d test.txt

# file: test.txt

security.test="test2"
```

Agora vamos obter o samba vamos acessar o diretório que vai armazenar os fontes

```
cd /usr/src
```

Agora vamos obter os fontes

```
Verificar a versão mais atual.
```

```
wget -c http://ftp.samba.org/pub/samba/stable/samba-4.1.6.tar.gz
```

Agora vamos desempacotar o samba

```
tar -xzvf samba-4.1.6.tar.gz
```

Agora vamos acessar o diretório dos fontes

```
cd samba-4.1.6
```

Agora vamos criar a configuração para o samba

```
./configure --enable-debug --enable-selftest
```

Agora vamos mandar compilar o samba este processo demora um pouco

```
make
```

Agora vamos mandar instalar o samba

```
make install
```

Agora vamos acertar a PATH do usuário root no caso dele estar utilizando o shell Bash

```
echo -e "export PATH=$PATH:/usr/local/samba/bin:/usr/local/samba/sbin"
>> /etc/profile
```

Agora precisamos importar a nova PATH

```
source /etc/profile
```

Criar o diretório de log:

```
mkdir /var/log/samba
touch /var/log/samba/smbd.log
```

Essas conf acimas só serão validadas na próximo login para que o path seja exportado nessa sessão atual execute o comando abaixo

```
export PATH=$PATH:/usr/local/samba/bin:/usr/local/samba/sbin
```

Agora vamos acertar a PATH do usuário root no caso dele estar utilizando o shell zsh

```
echo "export
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr
/bin/X11:/usr/local/samba/sbin:/usr/local/samba/bin" >> /root/.zshrc
```

Agora precisamos importar a nova PATH

```
source /root/.zshrc
```

Agora vamos ajustar o resolv.conf ele vai utilizar o nome do nosso domínio e o ip do pdc.

```
vim /etc/resolv.conf
domain empresa.net
search empresa.net
nameserver 192.168.0.190
```

Agora vamos ajustar a interface de rede para utilizar o nosso novo DNS

```
vim /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE="eth0"
BOOTPROTO="static"
BROADCAST="192.168.218.255"
DNS1="192.168.218.190"
GATEWAY="192.168.218.190"
IPADDR="192.168.0.25"
NETMASK="255.255.255.0"
NM_CONTROLLED="yes"
ONBOOT="yes"
TYPE="Ethernet"
```

Agora vamos provisionar o nosso domínio

Para saber quais opções podem ser utilizadas podemos listar da seguinte forma

```
samba-tool domain provision -h
```

Agora vamos provisionar o nosso domínio

```
/usr/local/samba/bin/samba-tool domain provision
```

Adicionar seu domínio como no exemplo abaixo. Deverá escolher uma senha com caracteres especiais, algumas letras maiúsculas e números.

```
Realm [LOCALDOMAIN]: DOMINIOEMPRESA.NET
Domain [DOMINIOEMPRESA]:
Server Role (dc, member, standalone) [dc]: dc
DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE)
[SAMBA_INTERNAL]:
DNS forwarder IP address (write 'none' to disable forwarding)
[192.168.218.120]:
Administrator password:
Retype password:
Looking up IPv4 addresses
Looking up IPv6 addresses
No IPv6 address will be assigned
Setting up share.ldb
Setting up secrets.ldb
Setting up the registry
Setting up the privileges database
Setting up idmap db
Setting up SAM db
Setting up sam.ldb partitions and settings
Setting up sam.ldb rootDSE
```

```
Pre-loading the Samba 4 and AD schema
Adding DomainDN: DC=dominioempresa,DC=net
Adding configuration container
Setting up sam.ldb schema
Setting up sam.ldb configuration data
Setting up display specifiers
Modifying display specifiers
Adding users container
Modifying users container
Adding com  puters container
Modifying computers container
Setting up sam.ldb data
Setting up well known security principals
Setting up sam.ldb users and groups
Setting up self join
Adding DNS accounts
Creating CN=MicrosoftDNS,CN=System,DC=dominioempresa,DC=net
Creating DomainDnsZones and ForestDnsZones partitions
Populating DomainDnsZones and ForestDnsZones partitions
Setting up sam.ldb rootDSE marking as synchronized
Fixing provision GUIDs
A Kerberos configuration suitable for Samba 4 has been generated at
/usr/local/samba/private/krb5.conf
Once the above files are installed, your Samba4 server will be ready
to use
Server Role:           active directory domain controller
Hostname:              dominio
NetBIOS Domain:        DOMINIOEMPRESA
DNS Domain:            dominioempresa.net
DOMAIN SID:            S-1-5-21-3424873523-2946863768-2191613857
```

Alterar o resolv.conf (DNS) uma vez que o novo ACTIVE será o servidor DNS backend adicionando o search para o domínio e o nameserver para o próprio ip do servidor. Lembrar de remover da configuração da placa de rede (/etc/sysconfig/network-scripts/ifcfg-eth**X**) o parâmetro de DNS para que ao restart do serviço network ele não reescreva o resolv.conf.

Após restart da placa de rede sem o parâmetro de DNS aplicar no resolv.conf

O servidor irá resolver o DNS por ele mesmo.

```
cat /etc/resolv.conf
search dominioempresa.net
nameserver 192.168.218.190
```

Após start do samba, podemos testar com o comando host com a chave _ldap._tcp trazendo o sucesso da resolução do registro de DNS (dns resolvendo corretamente).

```
/usr/local/samba/sbin/samba

host -t SRV _ldap._tcp.dominioempresa.net
_ldap._tcp.dominioempresa.net    has    SRV    record    0    100    389
dominio.dominioempresa.net.
```

Verificação das configurações do Kerberos verificando a configuração se esta correta:

```
vim /usr/local/samba/private/krb5.conf
[libdefaults]
        default_realm = DOMINIOEMPRESA.NET
        dns_lookup_realm = false
        dns_lookup_kdc = true
```

Vamos criar um link para o sistema reconhecer o arquivo de configuração do samba como default

```
rm /etc/krb5.conf
ln -sf /usr/local/samba/private/krb5.conf /etc/krb5.conf
```

Checando os compartilhamentos com o comando smbclient no server local (netlogon e sysvol devem estar criados para o funcionamento).

```
/usr/local/samba/bin/smbclient -L localhost -U%
Domain=[DOMINIOEMPRESA] OS=[Unix] Server=[Samba 4.1.6]

        Sharename       Type      Comment
        ---------       ----      -------
        netlogon        Disk
        sysvol          Disk
        IPC$            IPC       IPC Service (Samba 4.1.6)
Domain=[DOMINIOEMPRESA] OS=[Unix] Server=[Samba 4.1.6]

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
```

Agora vamos criar o script de inicialização

```
vim /etc/init.d/samba4

#!/bin/bash
. /etc/init.d/functions


# Source networking configuration.
. /etc/sysconfig/network


prog=samba
prog_dir=/usr/local/samba/sbin/
lockfile=/var/lock/subsys/$prog

start() {
        [ "$NETWORKING" = "no" ] && exit 1
#       [ -x /usr/sbin/ntpd ] || exit 5

                # Start daemons.
                echo -n $"Starting samba4: "
                daemon $prog_dir/$prog -D
        RETVAL=$?
                echo
        [ $RETVAL -eq 0 ] && touch $lockfile
```

```
        return $RETVAL
}


stop() {
        [ "$EUID" != "0" ] && exit 4
                echo -n $"Shutting down samba4: "
        killproc $prog_dir/$prog
        RETVAL=$?
                echo
        [ $RETVAL -eq 0 ] && rm -f $lockfile
        return $RETVAL
        kill `ps aux | grep samba | grep -v "grep" | awk '{print $2}'`
}

# See how we were called.
case "$1" in
start)
        start
        ;;
stop)
        stop
        ;;
status)
        status $prog
        ;;
restart)
        stop
        sleep 2
        start
        ;;
reload)
        /usr/local/samba/bin/smbcontrol all reload-config
        echo       -e       "Reload       do       servico       samba4""
"'\033[37;0m[\033[m''\033[32;3m  OK  \033[m''\033[37;0m]\033[m'
        exit 3
        ;;
*)
        echo $"Usage: $0 {start|stop|status|restart|reload}"
        exit 2
esac
```

Agora vamos dar permissão para o nosso script e vamos inserir ele na incialização

```
chmod +x /etc/init.d/samba4
cd /etc/init.d

chkconfig --add samba4
chkconfig samba4 on
chkconfig --list | grep samba4
        samba4      0:off  1:off  2:on   3:on   4:on   5:on   6:off
```

Vamos realizar um reboot do servidor para verificar se o daemon start automaticamente:

```
reboot
```

Agora vamos consultar o daemon do samba

```
ps aux | egrep samba
root      4184  6.2  8.2 528976 41260 ?        Ss   12:08   0:00 /usr/local/samba/sbin/samba
root      4187  0.0  5.7 528976 28648 ?        S    12:08   0:00 /usr/local/samba/sbin/samba
root      4188  0.0  5.8 528976 29500 ?        S    12:08   0:00 /usr/local/samba/sbin/samba
root      4189  0.1  6.1 533128 31100 ?        S    12:08   0:00 /usr/local/samba/sbin/samba
root      4190  0.0  5.6 528976 28608 ?        S    12:08   0:00 /usr/local/samba/sbin/samba
root       4191  6.6  8.6 579936 43304 ?          Ss    12:08    0:00 /usr/local/samba/sbin/smbd --
option=server role check:inhibit=yes --foreground
root      4192 11.3  6.1 528976 30768 ?        S    12:08   0:00 /usr/local/samba/sbin/samba
root      4193  0.0  5.8 528976 29204 ?        S    12:08   0:00 /usr/local/samba/sbin/samba
root      4194  0.0  6.1 528976 30716 ?        S    12:08   0:00 /usr/local/samba/sbin/samba
root      4195  0.3  5.9 528976 30096 ?        S    12:08   0:00 /usr/local/samba/sbin/samba
root      4196  0.1  6.0 532436 30568 ?        S    12:08   0:00 /usr/local/samba/sbin/samba
root      4197  0.0  5.7 528976 28748 ?        S    12:08   0:00 /usr/local/samba/sbin/samba
root      4198  0.0  5.9 528976 29712 ?        S    12:08   0:00 /usr/local/samba/sbin/samba
root      4199  0.1  5.8 528976 29632 ?        S    12:08   0:00 /usr/local/samba/sbin/samba
root       4203  0.0  5.7 579420 29052 ?          S     12:08    0:00 /usr/local/samba/sbin/smbd --
option=server role check:inhibit=yes --foreground
```

Como pode ser visto ele está rodando ok.

Agora vamos listar a versão do nosso samba

```
smbclient --version
Version 4.1.6

smbd -V
Version 4.1.6
```

Agora vamos mandar listar o netlogon com o usuário administrator para verificar se esta autenticando corretamente.

```
smbclient //localhost/netlogon -UAdministrator%'SENHA' -c 'ls'

Domain=[DOMINIOEMPRESA] OS=[Unix] Server=[Samba 4.1.6]
  .    D        0  Mon Mar 17 11:39:56 2014
  ..   D        0  Mon Mar 17 11:40:11 2014

                49214 blocks of size 1048576. 46378 blocks available
```

Agora vamos mandar listar a configuração do nosso samba

```
testparm

Load smb config files from /etc/samba/smb.conf
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit
(16384)
Processing section "[homes]"
Processing section "[printers]"
Loaded services file OK.
Server role: ROLE_STANDALONE
Press enter to see a dump of your service definitions

[global]
        workgroup = MYGROUP
        server string = Samba Server Version %v
        log file = /var/log/samba/log.%m
        max log size = 50
        idmap config * : backend = tdb
        cups options = raw

[homes]
        comment = Home Directories
        read only = No
```

```
        browseable = No

[printers]
        comment = All Printers
        path = /var/spool/samba
        printable = Yes
        print ok = Yes
        browseable = No
```

Agora vamos ajustar o limits.conf para não aparecer os avisos no samba

```
vim /etc/security/limits.conf
#colocar no final do arquivo
root hard nofile 131072
root soft nofile 65536
mioutente hard nofile 32768
mioutente soft nofile 16384
```

Agora vamos testar a resolução de nome

```
nslookup dominioempresa.net
Server:         192.168.218.190
Address:        192.168.218.190#53

Name:   dominioempresa.net
Address: 192.168.218.190
```

Agora vamos ajustar a configuração do samba para que ele consiga mapear via winbind

```
vim /usr/local/samba/etc/smb.conf
[global]
        workgroup = DOUGLAS
        realm = douglas.lan
         netbios name = NODO1
        server role = active directory domain controller
        passdb backend = samba_dsdb
        server services = s3fs, rpc, nbt, wrepl, ldap, cldap, kdc,
drepl, winbind, ntp_signd, kcc, dnsupdate
        rpc_server:tcpip = no
        rpc_daemon:spoolssd = embedded
        rpc_server:spoolss = embedded
        rpc_server:winreg = embedded
        rpc_server:ntsvcs = embedded
        rpc_server:eventlog = embedded
        rpc_server:srvsvc = embedded
        rpc_server:svcctl = embedded
        rpc_server:default = external
        #IDMAP
        idmap_ldb:use rfc2307 = yes
        idmap config * : backend = tdb
         idmap config *:range = 70001-80000
         idmap config DOUGLAS:backend = ad
         idmap config DOUGLAS:schema_mode = rfc2307
         idmap config DOUGLAS:range = 500-40000
        #WINBIND
         winbind nss info = rfc2307
         winbind trusted domains only = no
         winbind use default domain = yes
         winbind enum users  = yes
```

```
        winbind enum groups = yes
        map archive = No
        map readonly = no
        store dos attributes = Yes
        vfs objects = dfs_samba4, acl_xattr
        #o template shell é necessário para logar com a autenticação
via winbind
        template shell = /bin/bash
        #DESABILITANDO AS IMPRESSORAS
        printcap name = /dev/null
        load printers = no
        disable spoolss = yes
        printing = bsd
        ### LOGS
        log file = /var/log/samba/smbd.log
        max log size = 50
        log level = 2
        vfs objects = recycle full_audit
        ### LIXEIRA
        recycle:repository = Lixeira
        recycle:exclude = *.tmp *.TMP *.temp *.TEMP ~*
        recycle:keeptree = yes
        full_audit:success = rmdir mkdir open write rename unlink
        full_audit:failure = rmdir mkdir open write rename unlink
        full_audit:prefix = %U|%I|%m|%S
        full_audit:failure = none
        full_audit:facility = local5
        full_audit:priority = notice
        veto files = /*.mp3/*.wav/*.exe/*.cmd/*.adm/*.inf/*.ini/*.pif
        delete veto files = yes
        dos filemode = yes


[netlogon]
        path = /usr/local/samba/var/locks/sysvol/douglas.lan/scripts
        read only = No

[sysvol]
        path = /usr/local/samba/var/locks/sysvol
        read only = No
```

Agora vamos criar o diretório para armazenar os logs

```
mkdir -p /var/log/samba
```

Agora precisamos ajustar as bibliotecas do winbind para os sistemas de 32bits precisamos fazer da seguinte forma (se for 32 bits proceda):

```
ln -s /usr/local/samba/lib/libnss_winbind.so.2 /lib/libnss_winbind.so
ln -s /lib/libnss_winbind.so /lib/libnss_winbind.so.2
ldconfig
```

Para os sistemas de 64bits precisamos fazer da seguinte forma (se for 64 bits proceda):

```
ln -s /usr/local/samba/lib/libnss_winbind.so.2 /lib64/libnss_winbind.so
ln -s /lib64/libnss_winbind.so /lib64/libnss_winbind.so.2
ldconfig
```

Agora vamos ajustar o nsswitch.conf adicionando na frente dos parâmetros

```
vim /etc/nsswitch.conf
[...]
passwd: files winbind
[...]
group:  files winbind
```

Agora vamos inicializar um ticket para o administrator

```
kinit administrator@DOMINIOEMMAIUSCULO.LAN

Password for administrator@DOUGLAS.LAN:
Warning: Your password will expire in 41 days on Mon Oct  7 12:02:11
2013
```

Agora vamos listar o nosso ticket

```
klist

Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@DOUGLAS.LAN

Valid starting     Expires            Service principal
08/26/13 12:22:19  08/26/13 22:22:19  krbtgt/DOUGLAS.LAN@DOUGLAS.LAN
        renew until 08/27/13 12:22:16
```

O nosso kerberos está ok.

Vamos instalar o ntp

```
yum install ntp -y
```

Agora vamos fazer um backup do arquivo de configuração default do ntp.conf

```
cp /etc/ntp.conf /etc/ntp.conf.old
```

Agora vamos configurar o ntp

```
vim /etc/ntp.conf
server 127.127.1.0
fudge  127.127.1.0 stratum 10
server a.ntp.br iburst prefer
server 0.pool.ntp.org  iburst prefer
server 1.pool.ntp.org  iburst prefer
driftfile /var/lib/ntp/ntp.drift
logfile /var/log/ntp
ntpsigndsocket /usr/local/samba/var/lib/ntp_signd/
restrict default kod nomodify notrap nopeer mssntp
restrict 127.0.0.1
restrict a.ntp.br mask 255.255.255.255 nomodify notrap nopeer noquery
restrict  0.pool.ntp.org  mask  255.255.255.255  nomodify  notrap  nopeer
noquery
restrict  1.pool.ntp.org  mask  255.255.255.255  nomodify  notrap  nopeer
noquery
```

Agora vamos iniciar ele

```
/etc/init.d/ntpd start
```

Agora vamos consultar o seu sincronismo

```
ntpq -p 127.0.0.1
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 LOCAL(0)        .LOCL.          10 l    -   64    1    0.000    0.000   0.000
 a.ntp.br        .INIT.          16 u    -   64    0    0.000    0.000   0.000
 a.st1.ntp.br    .INIT.          16 u    -   64    0    0.000    0.000   0.000
 roma.coe.ufrj.b .INIT.          16 u    -   64    0    0.000    0.000   0.000
```

Agora vamos inserir o ntp na incialização

```
chkconfig --add ntpd
chkconfig ntpd on
```

Agora vamos atualizar o nosso ntp

```
ntpdate -u a.ntp.br
```

Agora vamos ajustar o grupo do arquivo ntp_signd

```
chgrp ntp /usr/local/samba/var/lib/ntp_signd
```

O nosso samba já está ok.

Agora podemos obter os RSAT(Admin pack) para administrar o active diretory pelo Windows:

- http://www.microsoft.com/download/details.aspx?id=28972 (Windows 8)
- http://www.microsoft.com/downloads/details.aspx?FamilyId=9FF6E897-23CE-4A36-B7FC-D52065DE9960&displaylang=en (Vista)
- http://www.microsoft.com/downloads/details.aspx?FamilyID=7D2F6AD7-656B-4313-A005-4E344E43997D&displaylang=en (Windows 7)
- http://www.microsoft.com/en-us/download/details.aspx?id=6315 (Windows XP/Server 2003)
- Para instalar o RSAT no Windows 7: http://social.technet.microsoft.com/wiki/contents/articles/2593.instalando-o-remote-server-administration-tools-rsat-no-windows-7-sp1-pt-br.aspx
- Para instalar o RSAT no Windows 8: http://www.canaldainfo.com.br/index.php/windows-8rsat/

Agora vamos testar o winbind

```
wbinfo -t
checking the trust secret for domain DOUGLAS via RPC calls succeeded
```

Agora vamos listar os grupos

```
wbinfo -g
Enterprise Read-Only Domain Controllers
Domain Admins
```

```
Domain Users
Domain Guests
Domain Computers
Domain Controllers
Schema Admins
Enterprise Admins
Group Policy Creator Owners
Read-Only Domain Controllers
DnsUpdateProxy
```

Agora vamos listar os usuários

```
wbinfo -u
Administrator
Guest
krbtgt
dns-nodo1
```

Agora vamos testar o update de dns no samba

```
samba_dnsupdate --verbose
IPs: ['192.168.0.25']
Looking for DNS entry A douglas.lan 192.168.0.25 as douglas.lan.
Looking for DNS entry A nodo1.douglas.lan 192.168.0.25 as
nodo1.douglas.lan.
Looking for DNS entry A gc._msdcs.douglas.lan 192.168.0.25 as
gc._msdcs.douglas.lan.
Looking for DNS entry CNAME eae04ba1-3ca2-4ec6-b08c-
4962ca4f04b4._msdcs.douglas.lan nodo1.douglas.lan as eae04ba1-3ca2-
4ec6-b08c-4962ca4f04b4._msdcs.douglas.lan.
Looking for DNS entry SRV _kpasswd._tcp.douglas.lan nodo1.douglas.lan
464 as _kpasswd._tcp.douglas.lan.
Checking 0 100 464 nodo1.douglas.lan. against SRV
_kpasswd._tcp.douglas.lan nodo1.douglas.lan 464
Looking for DNS entry SRV _kpasswd._udp.douglas.lan nodo1.douglas.lan
464 as _kpasswd._udp.douglas.lan.
Checking 0 100 464 nodo1.douglas.lan. against SRV
_kpasswd._udp.douglas.lan nodo1.douglas.lan 464
Looking for DNS entry SRV _kerberos._tcp.douglas.lan nodo1.douglas.lan
88 as _kerberos._tcp.douglas.lan.
Checking 0 100 88 nodo1.douglas.lan. against SRV
_kerberos._tcp.douglas.lan nodo1.douglas.lan 88
Looking for DNS entry SRV _kerberos._tcp.dc._msdcs.douglas.lan
nodo1.douglas.lan 88 as _kerberos._tcp.dc._msdcs.douglas.lan.
Checking 0 100 88 nodo1.douglas.lan. against SRV
_kerberos._tcp.dc._msdcs.douglas.lan nodo1.douglas.lan 88
Looking for DNS entry SRV _kerberos._tcp.default-first-site-
name._sites.douglas.lan nodo1.douglas.lan 88 as
_kerberos._tcp.default-first-site-name._sites.douglas.lan.
Checking 0 100 88 nodo1.douglas.lan. against SRV
_kerberos._tcp.default-first-site-name._sites.douglas.lan
nodo1.douglas.lan 88
Looking for DNS entry SRV _kerberos._tcp.default-first-site-
name._sites.dc._msdcs.douglas.lan nodo1.douglas.lan 88 as
_kerberos._tcp.default-first-site-name._sites.dc._msdcs.douglas.lan.
Checking 0 100 88 nodo1.douglas.lan. against SRV
_kerberos._tcp.default-first-site-name._sites.dc._msdcs.douglas.lan
nodo1.douglas.lan 88
Looking for DNS entry SRV _kerberos._udp.douglas.lan nodo1.douglas.lan
88 as _kerberos._udp.douglas.lan.
```

```
Checking 0 100 88 nodo1.douglas.lan. against SRV
_kerberos._udp.douglas.lan nodo1.douglas.lan 88
Looking for DNS entry SRV _ldap._tcp.douglas.lan nodo1.douglas.lan 389
as _ldap._tcp.douglas.lan.
Checking 0 100 389 nodo1.douglas.lan. against SRV
_ldap._tcp.douglas.lan nodo1.douglas.lan 389
Looking for DNS entry SRV _ldap._tcp.dc._msdcs.douglas.lan
nodo1.douglas.lan 389 as _ldap._tcp.dc._msdcs.douglas.lan.
Checking 0 100 389 nodo1.douglas.lan. against SRV
_ldap._tcp.dc._msdcs.douglas.lan nodo1.douglas.lan 389
Looking for DNS entry SRV _ldap._tcp.gc._msdcs.douglas.lan
nodo1.douglas.lan 3268 as _ldap._tcp.gc._msdcs.douglas.lan.
Checking 0 100 3268 nodo1.douglas.lan. against SRV
_ldap._tcp.gc._msdcs.douglas.lan nodo1.douglas.lan 3268
Looking for DNS entry SRV _ldap._tcp.pdc._msdcs.douglas.lan
nodo1.douglas.lan 389 as _ldap._tcp.pdc._msdcs.douglas.lan.
Checking 0 100 389 nodo1.douglas.lan. against SRV
_ldap._tcp.pdc._msdcs.douglas.lan nodo1.douglas.lan 389
Looking for DNS entry SRV _ldap._tcp.default-first-site-
name._sites.douglas.lan nodo1.douglas.lan 389 as _ldap._tcp.default-
first-site-name._sites.douglas.lan.
Checking 0 100 389 nodo1.douglas.lan. against SRV _ldap._tcp.default-
first-site-name._sites.douglas.lan nodo1.douglas.lan 389
Looking for DNS entry SRV _ldap._tcp.default-first-site-
name._sites.dc._msdcs.douglas.lan nodo1.douglas.lan 389 as
_ldap._tcp.default-first-site-name._sites.dc._msdcs.douglas.lan.
Checking 0 100 389 nodo1.douglas.lan. against SRV _ldap._tcp.default-
first-site-name._sites.dc._msdcs.douglas.lan nodo1.douglas.lan 389
Looking for DNS entry SRV _ldap._tcp.default-first-site-
name._sites.gc._msdcs.douglas.lan nodo1.douglas.lan 3268 as
_ldap._tcp.default-first-site-name._sites.gc._msdcs.douglas.lan.
Checking 0 100 3268 nodo1.douglas.lan. against SRV _ldap._tcp.default-
first-site-name._sites.gc._msdcs.douglas.lan nodo1.douglas.lan 3268
Looking for DNS entry SRV _ldap._tcp.15cf6198-7655-4ba1-9563-
2682bf9b6483.domains._msdcs.douglas.lan nodo1.douglas.lan 389 as
_ldap._tcp.15cf6198-7655-4ba1-9563-
2682bf9b6483.domains._msdcs.douglas.lan.
Checking 0 100 389 nodo1.douglas.lan. against SRV _ldap._tcp.15cf6198-
7655-4ba1-9563-2682bf9b6483.domains._msdcs.douglas.lan
nodo1.douglas.lan 389
Looking for DNS entry SRV _gc._tcp.douglas.lan nodo1.douglas.lan 3268
as _gc._tcp.douglas.lan.
Checking 0 100 3268 nodo1.douglas.lan. against SRV
_gc._tcp.douglas.lan nodo1.douglas.lan 3268
Looking for DNS entry SRV _gc._tcp.default-first-site-
name._sites.douglas.lan nodo1.douglas.lan 3268 as _gc._tcp.default-
first-site-name._sites.douglas.lan.
Checking 0 100 3268 nodo1.douglas.lan. against SRV _gc._tcp.default-
first-site-name._sites.douglas.lan nodo1.douglas.lan 3268
No DNS updates needed
```

Agora vamos mandar atualizar todos os registros

```
samba_dnsupdate --verbose --all-names
IPs: ['192.168.0.25']
Calling nsupdate for A douglas.lan 192.168.0.25
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id:      0
;; flags:; ZONE: 0, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; UPDATE SECTION:
```

```
douglas.lan.            900     IN      A       192.168.0.25

Calling nsupdate for A nodo1.douglas.lan 192.168.0.25
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id:      0
;; flags:; ZONE: 0, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; UPDATE SECTION:
nodo1.douglas.lan.      900     IN      A       192.168.0.25

Calling nsupdate for A gc._msdcs.douglas.lan 192.168.0.25
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id:      0
;; flags:; ZONE: 0, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; UPDATE SECTION:
gc._msdcs.douglas.lan. 900      IN      A       192.168.0.25

Calling      nsupdate      for      CNAME      eae04ba1-3ca2-4ec6-b08c-
4962ca4f04b4._msdcs.douglas.lan nodo1.douglas.lan
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id:      0
;; flags:; ZONE: 0, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; UPDATE SECTION:
eae04ba1-3ca2-4ec6-b08c-4962ca4f04b4._msdcs.douglas.lan.     900     IN
        CNAME nodo1.douglas.lan.

Calling nsupdate for SRV _kpasswd._tcp.douglas.lan nodo1.douglas.lan
464
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id:      0
;; flags:; ZONE: 0, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; UPDATE SECTION:
_kpasswd._tcp.douglas.lan. 900 IN      SRV     0       100         464
nodo1.douglas.lan.

Calling nsupdate for SRV _kpasswd._udp.douglas.lan nodo1.douglas.lan
464
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id:      0
;; flags:; ZONE: 0, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; UPDATE SECTION:
_kpasswd._udp.douglas.lan. 900 IN      SRV     0       100         464
nodo1.douglas.lan.

Calling nsupdate for SRV _kerberos._tcp.douglas.lan nodo1.douglas.lan
88
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id:      0
;; flags:; ZONE: 0, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; UPDATE SECTION:
_kerberos._tcp.douglas.lan. 900        IN      SRV     0       100     88
nodo1.douglas.lan.

Calling   nsupdate   for   SRV   _kerberos._tcp.dc._msdcs.douglas.lan
nodo1.douglas.lan 88
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id:      0
;; flags:; ZONE: 0, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; UPDATE SECTION:
_kerberos._tcp.dc._msdcs.douglas.lan.   900   IN   SRV   0   100   88
nodo1.douglas.lan.
```

```
Calling nsupdate for SRV _kerberos._tcp.default-first-site-name._sites.douglas.lan nodo1.douglas.lan 88
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id:      0
;; flags:; ZONE: 0, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; UPDATE SECTION:
_kerberos._tcp.default-first-site-name._sites.douglas.lan.  900  IN  SRV  0  100  88  nodo1.douglas.lan.

Calling nsupdate for SRV _kerberos._tcp.default-first-site-name._sites.dc._msdcs.douglas.lan nodo1.douglas.lan 88
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id:      0
;; flags:; ZONE: 0, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; UPDATE SECTION:
_kerberos._tcp.default-first-site-name._sites.dc._msdcs.douglas.lan.
900 IN SRV0 100 88 nodo1.douglas.lan.

Calling nsupdate for SRV _kerberos._udp.douglas.lan nodo1.douglas.lan
88
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id:      0
;; flags:; ZONE: 0, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; UPDATE SECTION:
_kerberos._udp.douglas.lan. 900       IN      SRV     0       100     88
nodo1.douglas.lan.

Calling nsupdate for SRV _ldap._tcp.douglas.lan nodo1.douglas.lan 389
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id:      0
;; flags:; ZONE: 0, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; UPDATE SECTION:
_ldap._tcp.douglas.lan.       900     IN      SRV     0       100     389
nodo1.douglas.lan.

Calling nsupdate for SRV _ldap._tcp.dc._msdcs.douglas.lan
nodo1.douglas.lan 389
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id:      0
;; flags:; ZONE: 0, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; UPDATE SECTION:
_ldap._tcp.dc._msdcs.douglas.lan. 900 IN SRV  0         100         389
nodo1.douglas.lan.

Calling nsupdate for SRV _ldap._tcp.gc._msdcs.douglas.lan
nodo1.douglas.lan 3268
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id:      0
;; flags:; ZONE: 0, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; UPDATE SECTION:
_ldap._tcp.gc._msdcs.douglas.lan. 900 IN SRV  0         100         3268
nodo1.douglas.lan.

Calling nsupdate for SRV _ldap._tcp.pdc._msdcs.douglas.lan
nodo1.douglas.lan 389
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id:      0
;; flags:; ZONE: 0, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; UPDATE SECTION:
_ldap._tcp.pdc._msdcs.douglas.lan. 900 IN SRV 0         100         389
nodo1.douglas.lan.
```

```
Calling nsupdate for SRV _ldap._tcp.default-first-site-name._sites.douglas.lan nodo1.douglas.lan 389
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id:      0
;; flags:; ZONE: 0, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; UPDATE SECTION:
_ldap._tcp.default-first-site-name._sites.douglas.lan.  900  IN  SRV  0 100 389 nodo1.douglas.lan.

Calling nsupdate for SRV _ldap._tcp.default-first-site-name._sites.dc._msdcs.douglas.lan nodo1.douglas.lan 389
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id:      0
;; flags:; ZONE: 0, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; UPDATE SECTION:
_ldap._tcp.default-first-site-name._sites.dc._msdcs.douglas.lan.    900 IN      SRV 0 100 389 nodo1.douglas.lan.

Calling nsupdate for SRV _ldap._tcp.default-first-site-name._sites.gc._msdcs.douglas.lan nodo1.douglas.lan 3268
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id:      0
;; flags:; ZONE: 0, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; UPDATE SECTION:
_ldap._tcp.default-first-site-name._sites.gc._msdcs.douglas.lan.    900 IN      SRV 0 100 3268 nodo1.douglas.lan.

Calling nsupdate for SRV _ldap._tcp.15cf6198-7655-4ba1-9563-2682bf9b6483.domains._msdcs.douglas.lan nodo1.douglas.lan 389
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id:      0
;; flags:; ZONE: 0, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; UPDATE SECTION:
_ldap._tcp.15cf6198-7655-4ba1-9563-2682bf9b6483.domains._msdcs.douglas.lan.   900IN   SRV   0   100   389 nodo1.douglas.lan.

Calling nsupdate for SRV _gc._tcp.douglas.lan nodo1.douglas.lan 3268
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id:      0
;; flags:; ZONE: 0, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; UPDATE SECTION:
_gc._tcp.douglas.lan.  900     IN      SRV     0         100         3268 nodo1.douglas.lan.

Calling nsupdate for SRV _gc._tcp.default-first-site-name._sites.douglas.lan nodo1.douglas.lan 3268
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id:      0
;; flags:; ZONE: 0, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; UPDATE SECTION:
_gc._tcp.default-first-site-name._sites.douglas.lan. 900 IN SRV      0 100 3268 nodo1.douglas.lan.
```

Agora vamos efetuar uma consulta de dns para registros de serviços

Vamos consultar o serviço do ldap

```
host -t SRV _ldap._tcp.douglas.lan.
```

```
_ldap._tcp.douglas.lan has SRV record 0 100 389 nodo1.douglas.lan.
```

Vamos consultar o serviço do kerberos

```
host -t SRV _kerberos._udp.douglas.lan.
_kerberos._udp.douglas.lan has SRV record 0 100 88 nodo1.douglas.lan.
```

Agora vamos consultar o registro do tipo A do nosso server

```
host -t A dominioempresa.lan
nodo1.douglas.lan has address 192.168.0.25
```

Agora vamos listar a keytab do kerberos

```
klist -k
Keytab name: FILE:/etc/krb5.keytab
KVNO Principal
---- --------------------------------------------------------------------
---------
   1 DNS/nodo1.douglas.lan@DOUGLAS.LAN
   1 dns-nodo1@DOUGLAS.LAN
   1 DNS/nodo1.douglas.lan@DOUGLAS.LAN
   1 dns-nodo1@DOUGLAS.LAN
   1 DNS/nodo1.douglas.lan@DOUGLAS.LAN
   1 dns-nodo1@DOUGLAS.LAN
   1 DNS/nodo1.douglas.lan@DOUGLAS.LAN
   1 dns-nodo1@DOUGLAS.LAN
   1 DNS/nodo1.douglas.lan@DOUGLAS.LAN
   1 dns-nodo1@DOUGLAS.LAN
```

Agora vamos consultar os tickets ativos

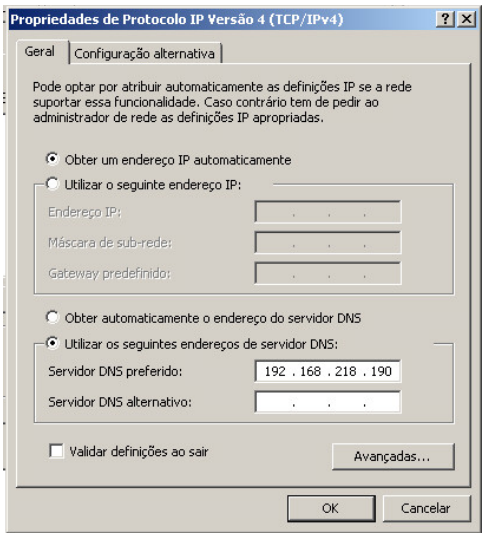
```
klist -e
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@DOUGLAS.LAN

Valid starting     Expires            Service principal
08/26/13 12:22:19  08/26/13 22:22:19  krbtgt/DOUGLAS.LAN@DOUGLAS.LAN
        renew until 08/27/13 12:22:16, Etype (skey, tkt): aes256-cts-
hmac-sha1-96, aes256-cts-hmac-sha1-96
```

Administrando o samba pelo WINDOWS

Tem uma pequena diferença entre windows xp e seven, vou fazer separadamente.

Colocando a Maquina WINDOWS XP no domínio
1º - Coloque como DNS primário o ip do servidor samba.



2º - Clique com o botão direito no "Meu Computador" -> Propriedades -> Alterar Nome do Computador -> coloque o nome do dominio: dominioempresa , será solicitado o nome de usuário e senha do admin, é "Administrator" e a senha cadastrada anteriormente.

Gerenciador de Usuário.

Instale a ferramenta da microsoft de Gerênciamento de Usuários e Grupos. São 2 arquivos disponibilizados:

http://www.microsoft.com/downloads/en/details.aspx?FamilyID=86b71a4f-4122-44af-be79-3f101e533d95

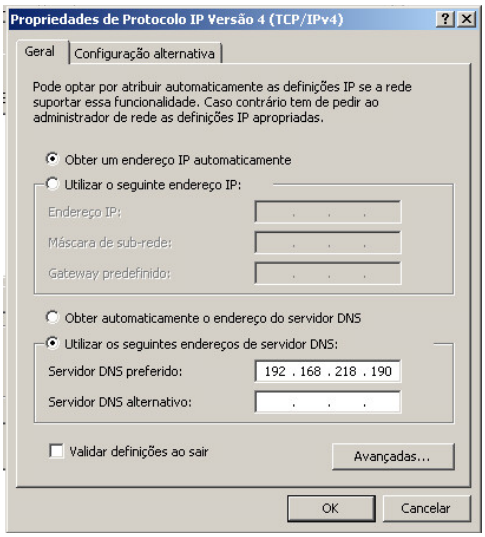
http://download.microsoft.com/download/3/e/4/3e438f5e-24ef-4637-abd1-981341d349c7/WindowsServer2003-KB892777-SupportTools-x86-ENU.exe

Gerenciador de GPOs

http://www.microsoft.com/en-us/download/details.aspx?id=21895

3º Com tudo instalado , deslogue e logue como Administrator dentro do domínio , vá no painel de controle -> ferramentas administrativas e você vai ver os 2 lá gerenciador de politicas de grupos e usuário e computadores do active directory , basta abrir e administrar o samba como administra um servidor Windows server.

Colocando no domínio (Windows 7)
1º - altere o DNS para para ser o samba

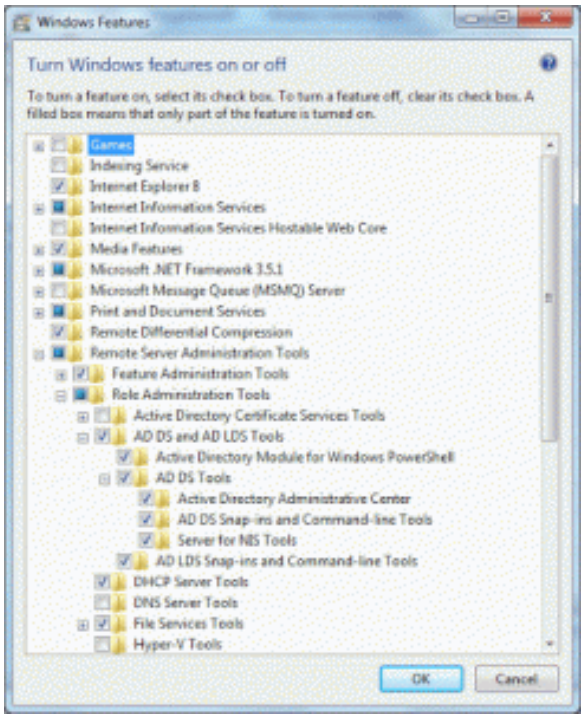


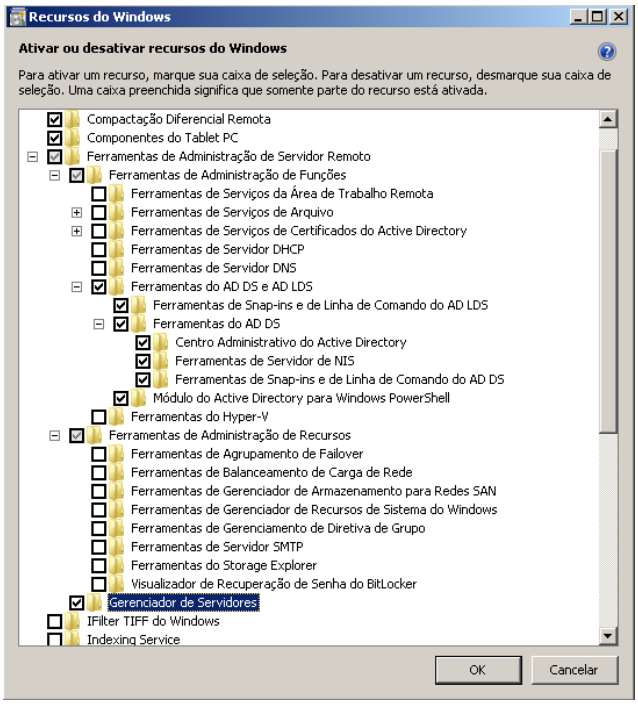
2º - Clique com o botão direito no "Meu computador" -> Propriedades -> Alterar configurações -> Altere o nome do dominio para linuxextreme
Diferente do windows xp , o windows 7 só precisa de um arquivo para download.

http://www.microsoft.com/en-us/download/details.aspx?id=7887

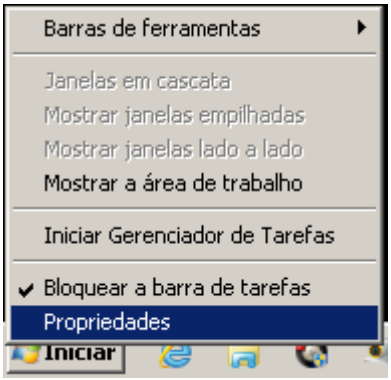
Após a instalação

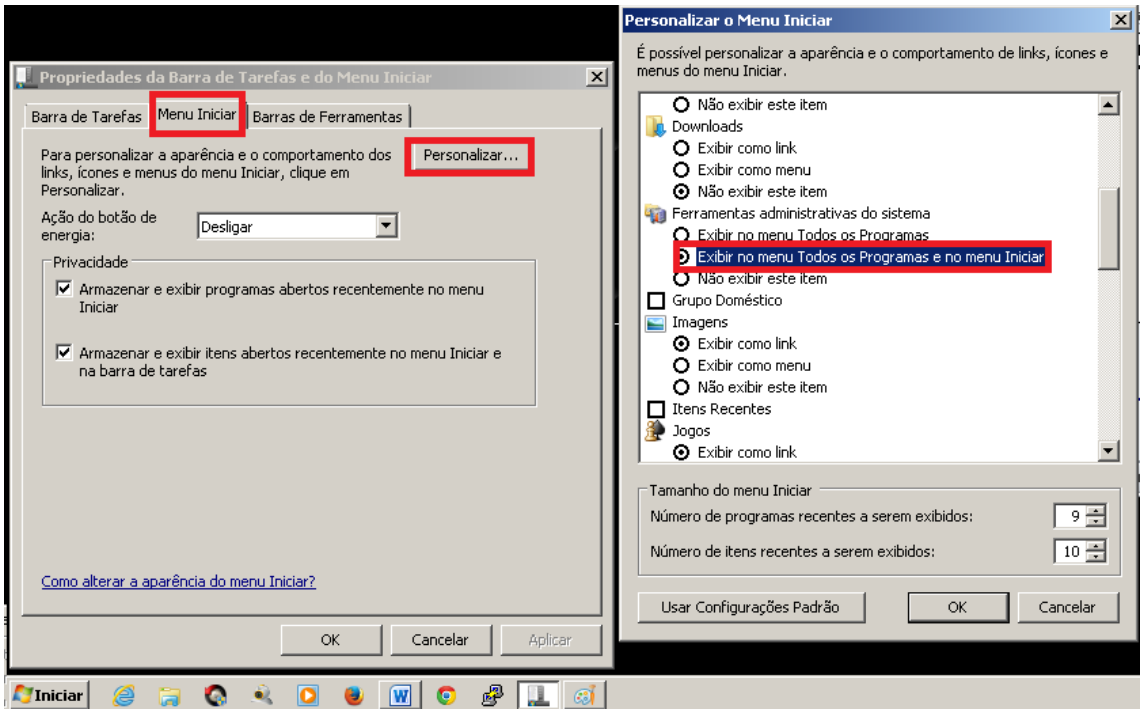
No painel de controle -> Programas e Recursos -> Ativar e Desativar recursos do windows e adicione as opções do Remote administration tools como na imagem abaixo.





Habilita-lo no MENU INICIAR





Administrando o SAMBA 4

Para alterar a complexidade de senha do SAMBA4 utilize o poderoso comando samba-tool.

Recuperar Senha do usuario Administrator

```
samba-tool user setpassword administrator
```

Para testar se a autenticação está funcionando, você deve tentar se conectar ao compartimento netlogon usando a senha do "administrator" que você definiu anteriormente:

```
$ smbclient //localhost/netlogon -UAdministrator%'p4$$word' -c 'ls'
```

Se você desejar executar o SAMBA em modo de desenvolvedor para debugar mensagens use:

```
# /usr/local/samba/sbin/samba -i -M single
```

O comando para listar as regras de política de senha:

```
# samba-tool domain passwordsettings show
```

Lista de outras variáveis do Samba para referência smb.conf:

%a : A versão do Windows usada, onde o "%a" é substituído pelas strings "Win95" (Windows 95/98), "WinNT" (Windows NT 3.x ou 4.x), "Win2K" (Windows 2000 ou XP) ou "Samba" (máquinas Linux rodando o Samba)
%I : Endereço IP da máquina cliente (ex: 192.168.1.2)
%m : Nome da máquina cliente (ex: cliente1)
%L : Nome do servidor (ex: athenas)
%u : Nome do usuário, como cadastrado no servidor Linux (ex: joao)
%U : Nome do usuário, como enviado pelo cliente Windows (pode ser diferente do login cadastrado no servidor em algumas situações)
%H : Diretório home do usuário (ex: /home/maria)
%g : Grupo primário do usuário (ex: users)
%S : Nome do compartilhamento atual (o valor informado entre colchetes, ex: arquivos)
%P : Pasta compartilhada (o valor informado na opção "path", ex: /mnt/arquivos)
%v : Versão do Samba (ex: 3.2.24)
%T : Data e horário atual

Já para desativar ou fazer alterações:

samba-tool domain passwordsettings set --complexity=off --history-length=0 --min-pwd-length=0 --min-pwd-age=0
Desativar a verificação de complexidade de senha (por padrão a senha de qualquer usuário deve ter pelo menos três dos quatro ítens: Maiúsculas, Minusculas, Números, Simbolos):
samba-tool domain passwordsettings set --complexity=off
Alterar o tamanho mínimo da senha, por exemplo para 6:
samba-tool domain passwordsettings set --min-pwd-length=6
Alterar o prazo mínimo em que o usuário pode mudar a senha (usuário só vai poder mudar a senha após 4 dias da última mudança)
samba-tool domain passwordsettings set --min-pwd-age=4
Mudar o tempo de vida máximo da senha do usuário (usuário terá que mudar a senha após 30 dias da última mudança)
samba-tool domain passwordsettings set --max-pwd-age=30

Mudar o histórico de senhas que impede que o usuário utilize uma senha repetida (usuário não vai poder repetir nenhuma das últimas 5 senhas)
samba-tool domain passwordsettings set --history-length=5
Para mudar a senha de um usuário do domínio dentro do windows xp basta logar com o usuário, pressionar ctrl+alt+del e clicar em alterar senha.

Verificando entradas do DNS

samba-tool dns query 127.0.0.1 dominio.intra @ ALL -U administrator

NOTAS:
1 – Configuração do usuário terá efeito depois de sair e fazer o login.
2 – Configuração do computador terá efeito quando você reiniciar o computador.
3 – Políticas GPO de senha não são lidos pelo Samba ao atribuir senhas, para mudar a política que o Samba usa, você deve usar **samba-tool domain passwordsettings**

SAMBA4 – Backup e Restore

Este material tem o intuito de ensinar a como fazer backup e restore da base do Samb4 (Objetos do AD, DNS, Domínio).

Cenário:

Sistema Operacional: Ubuntu 12.10 Server x64

Versão do Samba: 4.0.5

Local de instalação: /usr/local/samba

Arquivos de instalação: /usr/src/samba-4.0.5

Local de backup: /usr/local/samba/backups

Módulo DNS: Samba Internal

Backup:

- Durante a instalação do Samba4 (./configure, make e make install) alguns scripts não são instalados, entre eles o samba_backup e o tdbbackup, que são essências para o backup. Por isso teremos que adicionar esses arquivos manualmente.

Para isso será necessário possuir os arquivos de instalação do Samba4, aqueles que normalmente baixamos em /usr/src.

Configuração:

- "Instalar" arquivos faltantes durante a instalação do Samba4. (samba_backup e tdbbackup):

cp /usr/src/samba-4.0.5/source4/scripting/bin/samba_backup /usr/sbin

cp /usr/src/samba-4.0.5/bin/tdbbackup /usr/sbin

chown root:root /usr/sbin/samba_backup

chown root:root /usr/sbin/tdbbackup

chmod 750 /usr/sbin/samba_backup

chmod 750 /usr/sbin/tdbbackup

*Dependências instaladas.

- Configurar o script de backup:

vi /usr/sbin/samba_backup

Edite as linhas abaixo, conforme suas necessidades:

FROMWHERE=/usr/local/samba (Local da instalação do Samba, de onde será extraído o backup)

WHERE=/usr/local/samba/backups (Local de destino do backup)

DAYS=90 (Dias de backup, até 90 dias atrás)

- Crie o local de destino de backup:

mkdir /usr/local/samba/backups

chmod 750 /usr/local/samba/backups

*Está então, criado e configurado o script de backup e criada a pasta de destino do backup.

- Executar o script de backup.

/usr/sbin/samba_backup

O script irá rodar silenciosamente (sem exibir nada na tela) durante alguns segundos.

Se não houver nenhum erro, acesse a pasta de destino do backup /usr/local/samba/backups e verifique se estão criados os seguintes arquivos.

- etc.{Timestamp}.tar.bz2
- samba4_private.{Timestamp}.tar.bz2
- sysvol.{Timestamp}.tar.bz

Se o backup rodou sem erros e os arquivos acima foram gerados com sucesso, crie um agendamento de backup no cron.

crontab –e

Adicione a linha abaixo para efetuar o backup diário as 02:00:

0 2 * * * /usr/sbin/samba_backup

Restore:

- Neste cenário, vamos simular que o Domain Controller sofreu um dano irreversível, sendo necessário subir um novo servidor em um novo hardware. O procedimento que eu segui deu certo e funcionou perfeitamente, seguindo o conceito que o novo servidor irá substituir por completo o antigo hardware. E que os arquivos de backup estão salvos em um local seguro (Fita, CD, Pendrive, etc.)

Antes de prosseguir, configure a nova maquina com as configurações abaixo:

- Instalação do Samba4:

- Instale a mesma versão do SAMBA da versão anterior. (no meu caso versão 4.0.5).
- Apenas instale o samba, e configure o script de inicialização do serviço não é necessário executar o Provision nem iniciar o serviço do samba.
- Esteja certo de que as seguintes pastas estejam vazias: /usr/local/samba/etc | /usr/local/samba/private | /usr/local/samba/var/locks/sysvol

- Configurações de rede:

- Para evitar problemas de DNS, o novo servidor, deve ter as mesmas configurações de rede do servidor anterior. IP e DNS (Importante que o DNS deve apontar para si mesmo, ou seja, 127.0.0.1)

- Arquivos de Backup:

- Copie os arquivos de backup que devem estar salvos em lugar seguro para /usr/local/samba/backups

Obs: executei essas configurações e consegui restaurar as configurações PERFEITAMENTE.

- Executar o Restore no novo servidor:

cd /usr/local/samba/backups

Descompacte os arquivos de backup em seus respectivos locais:

tar -jxf etc.{Timestamp}.tar.bz2 -C /usr/local/samba/

tar -jxf samba4_private.{Timestamp}.tar.bz2 -C /usr/local/samba/

tar -jxf sysvol.{Timestamp}.tar.bz2 -C /usr/local/samba/

Renomeie os arquivos *.ldb.bak que estão em /usr/local/samba/private para *.ldb. Com o comando abaixo:

find /usr/local/samba/private/ -type f -name '*.ldb.bak' -print0 | while read -d $'{TEXTO}' f ; do mv "$f" "${f%.bak}" ; done

Se o backup não conter ACLs estendidas, execute o comando abaixo:

samba-tool ntacl sysvolreset

Neste ponto o backup já está recuperado. Inicie o samba e faça alguns testes:

/etc/init.d/samba start

*IMPORTANTE: Neste cenário o módulo DNS é o SAMBA Internal, sendo assim, não é necessário efetuar mais nenhuma configuração pois o novo PDC já estará funcionando perfeitamente.

Porém, se o módulo DNS for o BIND9, será necessário além de executar o passos acima, executar os procedimentos do LINK: https://wiki.samba.org/index.php/DNS#A_note_on_DNS_problems_with_BIND9_DLZ

Regra importante para validar e permitir um DOMAIN ADMIN para trabalhar com a ferramenta do windows.

Para configurar os compartilhamentos voce precisa ter uma conta com privilegios “SeDiskOperatorPrivilege“. Vamos garantir esse privilégio ao grupo “Domain Admin“

```
# net rpc rights grant 'SEUDOMINIO\Domain Admins'
SeDiskOperatorPrivilege -Uadministrator
```

Podemos listar os privilégios:

```
# net rpc rights list accounts -Uadministrator
```

OBS: SOMENTE IRÁ CONSEGUIR MANIPULAR PELAS FERRAMENTAS DO WINDOWS CASO TENHA EM SEU DNS PRIMÁRIO O IP DO SERVIDOR DE DOMINIO.

Compartilhamento do diretório HOME para cada usuário privadamente.

Introduction

In a professional environment, you setup the permissions on the share, containing the user homes, in a way that allows the automatic creation for new accounts, without setting ACLs manually.

Adding the share

- Add the new share to your smb.conf

```
[home]
        path = /srv/samba/home/
        read only = No
```

Don't name the share „[homes]", as this is a special section (see the smb.conf manpage)! The „[homes] section can't handle the automatic folder creation, we'll setup below!

- Create the folder that will contain the home directories later. The permissions will be set later.

```
# mkdir /srv/samba/home/
```

- Reload Samba, to take the changes effect

```
# smbcontrol all reload-config
```

No servidor samba em smb.conf criar:

vim /etc/samba/smb.conf

```
[home]
        path = /share/homes
        read only = no
```

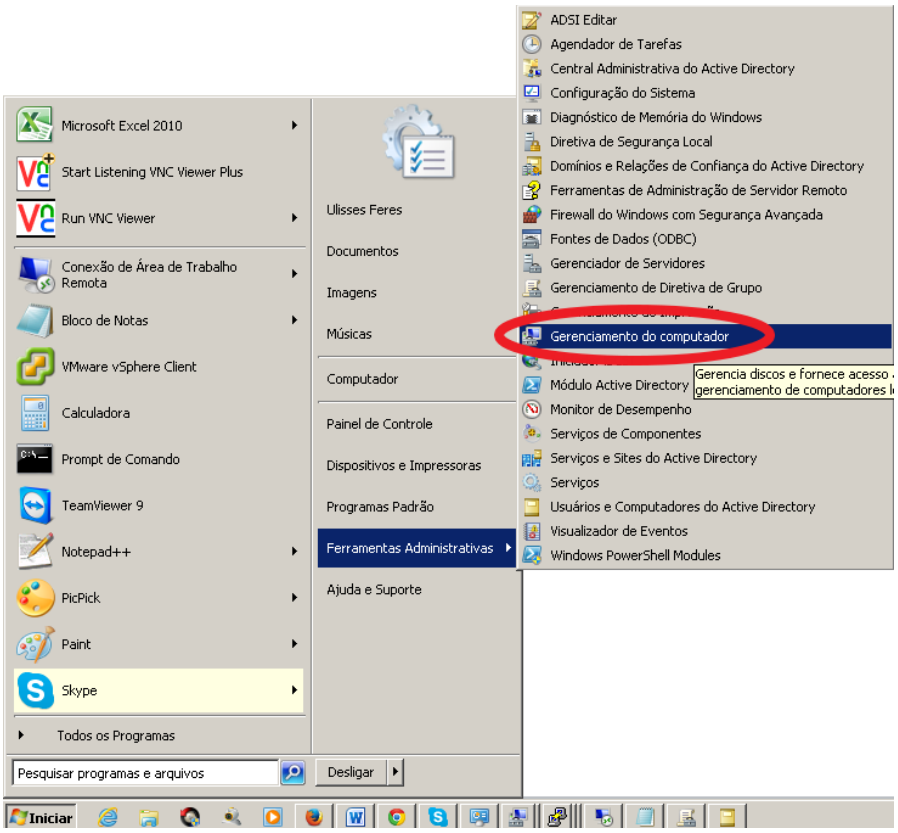
Após realizer um reload do samba4
/etc/init.d/samba4 reload

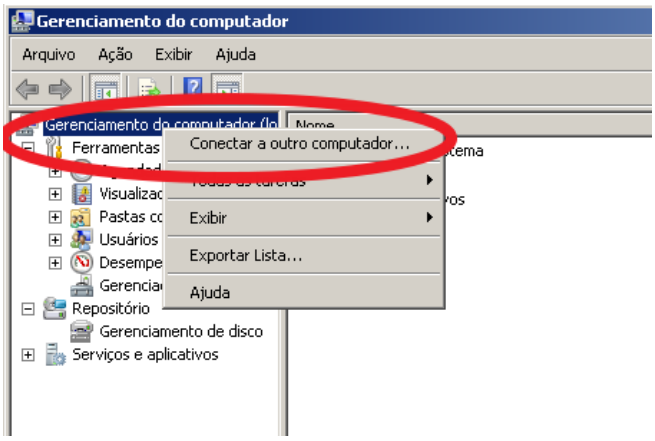
Obs: Diretório /share/homes deve existir.

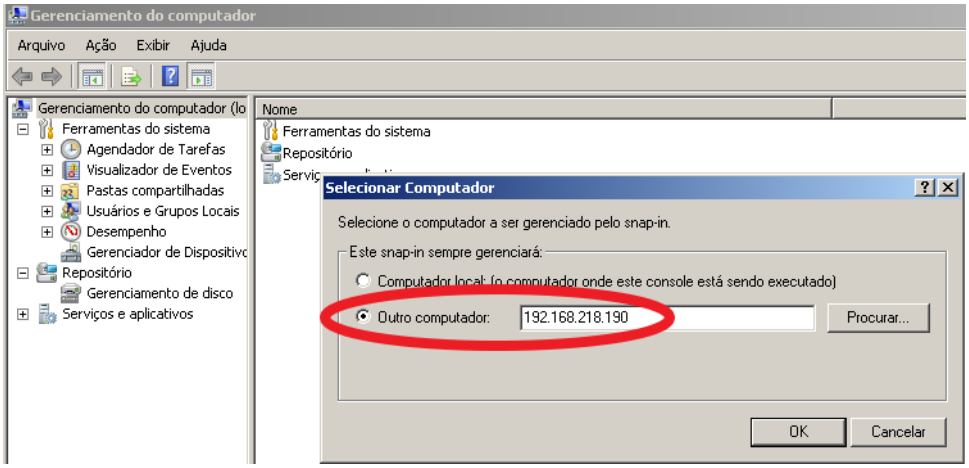
Note: Se você tem a exigência, que seus usuários precisam acessar sua pasta pessoal localmente no servidor, também, você tem que adicionar um grupo que contenha essas contas de usuário. Adicionar este grupo em todas as etapas a seguir e definir as permissões para exatamente a mesma do que para "usuários autenticados". É claro que este grupo tem de estar disponível localmente através winbindd, sssd, nslcd, ou outros. Isso é necessário, porque se o usuário efetuar login localmente no servidor, não existe um "Usuário Autenticado"!

- Realizar o login em uma estação como administrator do dominio em questão, nesta estação é necessário ter instalado as Ferramentas Administrativas.

- Abra o menu INICIAR, vá até Ferramentas Administrativas e clique sobre Gerenciamento do Computador".


Microsoft Excel 2010
Start Listening VNC Viewer Plus
Run VNC Viewer
Conexão de Área de Trabalho Remota
Bloco de Notas
VMware vSphere Client
Calculadora
Prompt de Comando
TeamViewer 9
Notepad++
PicPick
Paint
Skype
Todos os Programas
Pesquisar programas e arquivos
Desligar
Iniciar
Ulisses Feres
Documentos
Imagens
Músicas
Computador
Painel de Controle
Dispositivos e Impressoras
Programas Padrão
Ferramentas Administrativas
Ajuda e Suporte
ADSI Editar
Agendador de Tarefas
Central Administrativa do Active Directory
Configuração do Sistema
Diagnóstico de Memória do Windows
Diretiva de Segurança Local
Domínios e Relações de Confiança do Active Directory
Ferramentas de Administração de Servidor Remoto
Firewall do Windows com Segurança Avançada
Fontes de Dados (ODBC)
Gerenciador de Servidores
Gerenciamento de Diretiva de Grupo
Gerenciamento do computador
Módulo Active Directory
Monitor de Desempenho
Serviços de Componentes
Serviços e Sites do Active Directory
Serviços
Usuários e Computadores do Active Directory
Visualizador de Eventos
Windows PowerShell Modules

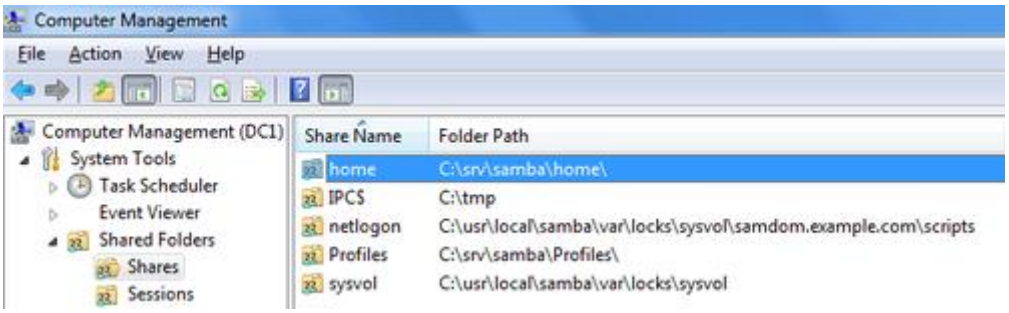

Gerenciamento do computador
Arquivo Ação Exibir Ajuda
Conectar a outro computador...
Exibir
Exportar Lista...
Ajuda
Repositório
Gerenciamento de disco
Serviços e aplicativos


Gerenciamento do computador
Arquivo Ação Exibir Ajuda
Ferramentas do sistema
Agendador de Tarefas
Visualizador de Eventos
Pastas compartilhadas
Usuários e Grupos Locais
Desempenho
Repositório
Gerenciamento de disco
Serviços e aplicativos
Nome
Selecionar Computador
Selecione o computador a ser gerenciado pelo snap-in.
Este snap-in sempre gerenciará:
Computador local: (o computador onde este console está sendo executado)
Outro computador:
192.168.218.190
Procurar...
OK
Cancelar

- Sobre o item Gerenciamento do computador (local) clique com o botão direito e escolha "Conectar a outro computador..."

- Entre com o ip do servidor SAMBA4 no qual deseja gerenciar.

- Navegue até Ferramentas do Sistema → Pastas Compartilhadas → COMPARTILHAMENTOS.

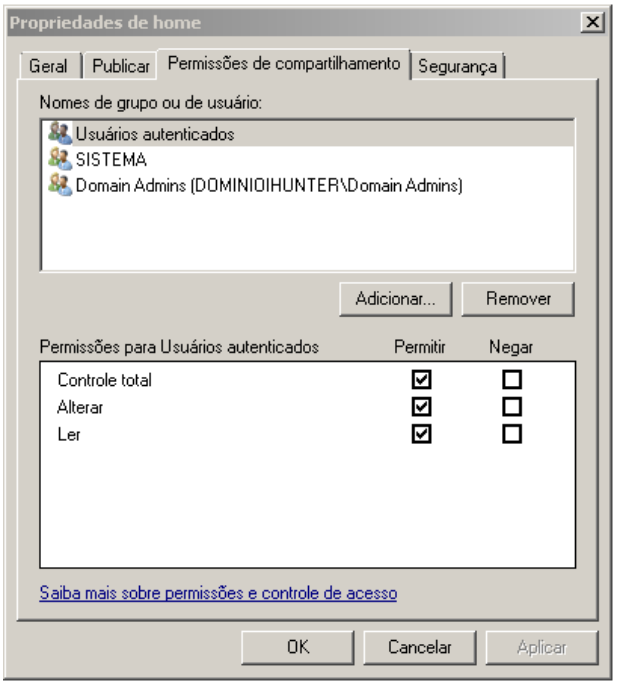


  - Clique o botão direito sobre o compartilhamento home e vá em PROPRIEDADES.

  - Vá até a aba PERMISSÕES DE COMPARTILHAMENTO.

  - Remova todos os usuários existentes e adicione de acordo com as permissões:

Authenticated Users: Full Control
Domain Admins: Full Control
System: Full Control



Se você tem a exigência, que seus usuários precisam acessar sua pasta pessoal localmente no servidor, também, adicionalmente, ou adicionar um grupo que contém essas contas de usuário. Porque, se o usuário efetuar login localmente no servidor, não existe um "Usuário Autenticado"! As permissões para esse grupo addional tem que ser o mesmo do que para "usuários autenticados"

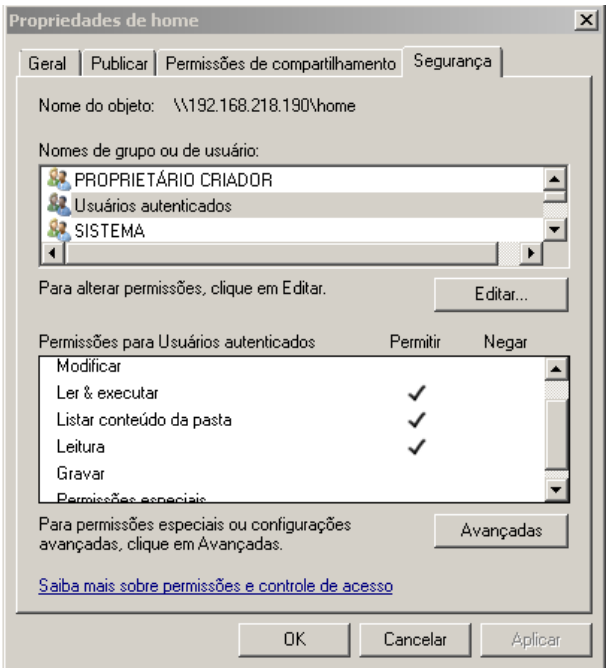
- Vá até a a aba SEGURANÇA
- Clique, no botão "Avançado" e, na janela que aparece no botão "Alterar permissões". Na próxima janela, desmarque a opção "Incluir permissões de obketos filhos por permissão herdadas deste objeto."

- Feche as janelas com "OK" até voltar na aba "Segurança".

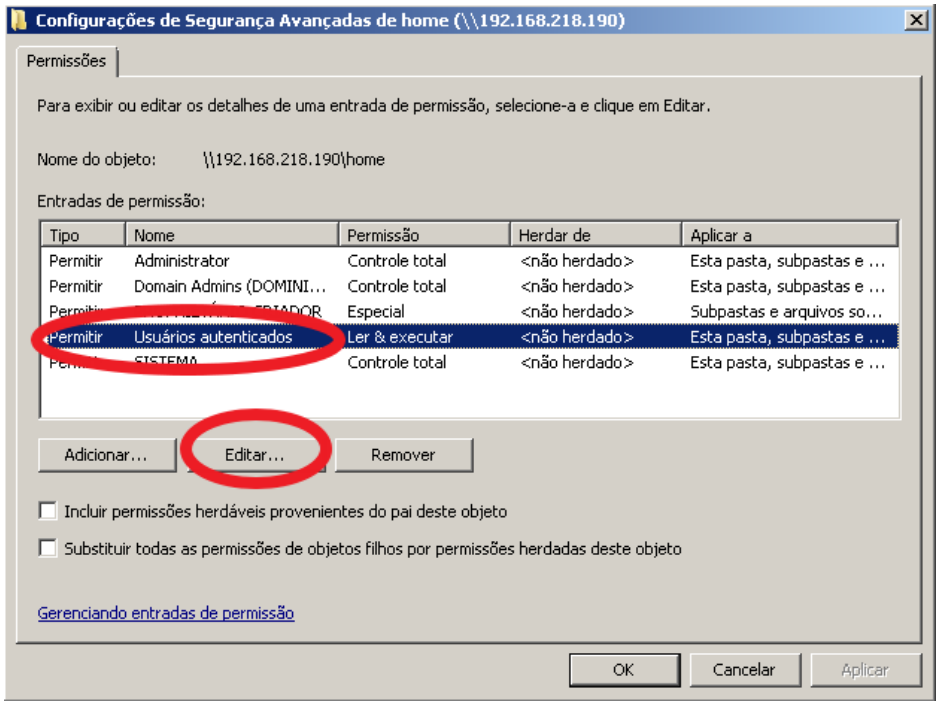
- Clique em EDITAR para realizer de acordo com as permissões abaixo.

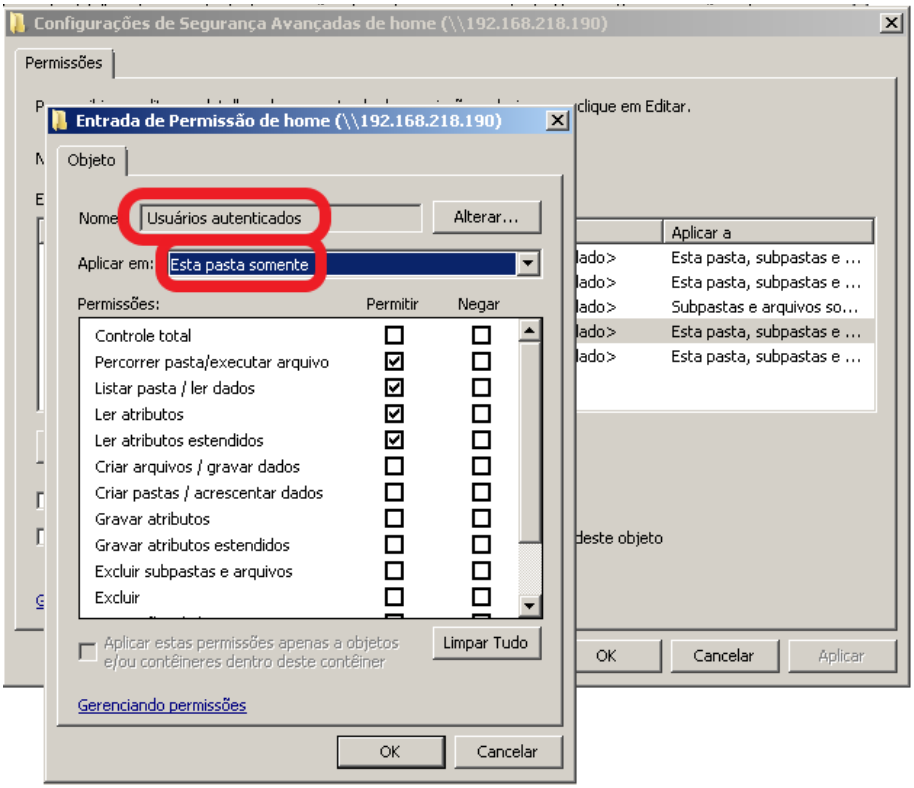
- Administrator: Full Control
- Authenticated Users: Read & Execute, List Folder Contents, Read
- Creator Owner: Full Control
- Domain Admins: Full Control
- System: Full Control

As permissões de " proprietário Criador " são automaticamente limitados a "subpasta e apenas os arquivos". Isso é correto.



- Para evitar "Usuários autenticados" acessar a outra pasta home de outros usuários, clique novamente no botão "Avançado" e na sub-janela que aparece no botão "Alterar permissões". Selecione "Usuários autenticados" da lista, clique em "Editar" e mudar o "Aplicar a" valor para "Isso só pasta".





- Feche todas as janelas com OK.

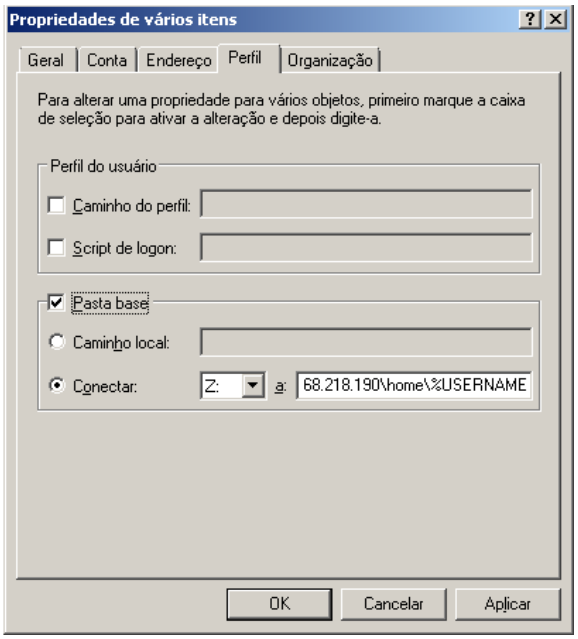
Defina a pasta pessoal do utilizador nas configurações da conta

Utilizando das ferramentas administrativas Microsoft RSAT (Remote Server Administration Tools) instalada.

- INICIAR → FERRAMENTAS ADMINISTRATIVAS → Usuários e Computadores do AD.

- Selecione com CTRL + A todas as contas dos usuários e em Propriedades altere a aba PERFIL

- Utilize a variável %USERNAME% para configuração.



- Clique em OK e terá a confirmação de criação.
- Logue com a conta e verifique se foi criado o mapeamento Z.

https://wiki.samba.org/index.php/Setup_and_configure_file_shares

Comando para verificação das ACLs no Linux:

```
[root@intranet instantclient_11_1]# getfacl -p /share/home/mrocha/
# file: /share/home/mrocha/
# owner: EMPRESA\134mrocha
# group: EMPRESA\134Domain\040Admins
user::rwx
user:root:rwx
user:3000005:rwx
user:3000018:rwx
group::rwx
group:EMPRESA\134Domain\040Admins:rwx
group:3000018:rwx
group:3000029:rwx
mask::rwx
other::---
default:user::rwx
default:user:root:rwx
default:user:3000005:rwx
default:user:3000018:rwx
default:user:EMPRESA\134mrocha:rwx
default:group::---
default:group:EMPRESA\134Domain\040Admins:rwx
default:group:3000018:rwx
```

As some of the xIDs are may not be resolved, you can search for them in the local ID mapping database of Samba for them. Example:

```
# ldbsearch -H /usr/local/samba/private/idmap.ldb xidNumber=3000000 dn
# record 1
dn: CN=S-1-5-32-544

# returned 1 records
# 1 entries
# 0 referrals
```

default:mask::rwx
default:other::---

Autenticando o Proxy Squid + DansGuardian no AD (samba4)

A autenticação do usuário e senha e feita sempre pelo squid, mesmo que trabalhe em conjundo com o DansGuardiam e sua porta do browser esteja `virada` para o dans, toda a autenticação eh feita no squid.

Há três maneiras de serem feitas as autenticações do squid no samba4 sendo que duas há necessidade de ingressar anteriormente esse servidor squid no domínio existente do samba4.

Descrição

- Permitir que o squid autentique usuários do windows active directory ou samba.
- Isso proporcina uma maior integração e utilização de uma única base de senhas.
- Também facilita o controle da navegação e relatórios por usuários.
- Existem 2 autenticadores no squid para isso:
    - NTLM: Pega automaticamente ou não o login do usuário logado no dominio. Caso o usuário não esteja logado, solicita a senha.
    - MSNT: Solicita que o usuário digite o usuário e senha. O NTLM é bem melhor, sugiro usar ele.
    - SMB_AUTH: Faz autenticação através do samba. Bem simples e fácil de configurar.
- Se estiver utilizando o squid do SuSE, ele vem com todos os autenticadores. Caso contrário terá que compilar no squid.

Uma forma fácil e rápida eh pelo executável distribuído no squid chamada smb_auth (no freebsd localizado em /usr/local/libexec/squid/smb_auth). Usando deste executável não há necessidade de ingressar o servidor ao domínio.

1 – No servidor samba4 sera necessário criar um compartilhamento chamado netlogon contendo um arquivo dentro do diretório de nome proxyauth escrito em seu conteúdo o nome allow.

[root@dominio ~]# vim /etc/samba/smb.conf

```
[netlogon]
      comment = The domain logon service
      path = /share/netlogon
 #   valid users = @"Domain Users"
      valid users = %U
      browseable = no
      guest ok = yes
      writeable = no
      read only = yes
```

[root@dominio ~]# cat /share/netlogon/proxyauth
allow

[root@dominio ~]# chmod 777 /share/netlogon/proxyauth

```
[root@dominio ~]# ls -lah /share/netlogon/
total 12K
drwxr-xr-x. 2 root root 4.0K Mar 20 19:35 .
drwxr-xr-x. 6 root root 4.0K Mar 20 19:35 ..
-rwxrwxrwx. 1 root root    6 Mar 20 19:35 proxyauth
```

Abaixo iremos realizer um teste do usuario e senha. Onde escrevo USUARIO SENHA substitui por dados reais. Após dar um enter no comando escreva com um espaço o Usuario e senha e posterior de enter e espere.

Quando eu escrevo um usuário e senha corretos tenho a mensagem de OK ao final.
Observação para o domínio no qual omite o .net, .com, etc..

```
(root@proxy)~# /usr/local/libexec/squid/smb_auth -W DOMINIOEMPRESA -d
USUARIO SENHA
Domain name: DOMINIOEMPRESA
Pass-through authentication: no
Query address options:
Domain controller IP address: 192.168.218.190
Domain controller NETBIOS name: DOMINIO
Contents of //DOMINIO/NETLOGON/proxyauth: allow
OK
```

Quando introduzo um usuario e senha incorretos tenho a mensagem de ERR ao final.

(root@proxy)~# /usr/local/libexec/squid/smb_auth -W DOMINIOEMPRESA -d
uferes 123
Domain name: DOMINIOEMPRESA
Pass-through authentication: no
Query address options:
Domain controller IP address: 192.168.218.190
Domain controller NETBIOS name: DOMINIO
Contents of //DOMINIO/NETLOGON/proxyauth:
ERR

Para finalizar iremos aplicar no arquivo squid.conf a autenticação (não irei abortar o arquivo todo e muito menos a configuração do squid):

auth_param basic program /usr/local/libexec/squid/smb_auth -W DOMINIOEMPRESA -U 192.168.218.190

Mas abaixo temos a clausula de requerimento.
acl auth proxy_auth REQUIRED

Reinicie o squid e teste a autenticação.

Alguns artigos mandam alterar o conteúdo com um patch ou manualmente do arquivo abaixo: /usr/local/libexec/squid/smb_auth.sh
Trocando
USER="$SMBUSER%$SMBPASS"
por
USER="$SMBUSER"
PASSWD="$SMBPASS"

Porem isso não foi necessário. Quando realizei essa modificação parou de funcionar.

Outras formas de integrar o squid com o samba4

Descrição

- Permitir que o squid autentique usuários do windows active directory ou samba.
- Isso proporcina uma maior integração e utilização de uma única base de senhas.
- Também facilita o controle da navegação e relatórios por usuários.
- Existem 2 autenticadores no squid para isso:
    - NTLM: Pega automaticamente ou não o login do usuário logado no dominio. Caso o usuário não esteja logado, solicita a senha.
    - MSNT: Solicita que o usuário digite o usuário e senha. O NTLM é bem melhor, sugiro usar ele.
    - SMB_AUTH: Faz autenticação através do samba. Bem simples e fácil de configurar.
- Se estiver utilizando o squid do SuSE, ele vem com todos os autenticadores. Caso contrário terá que compilar no squid.

Softwares e Versões

- Squid 2.5.X
- Samba client 3.x

Configuração para MSNT e NTLM

Configurar samba e winbind para entrar no domínio

- Editar o smb.conf

```
workgroup = mydomain
password server = myPDC
security = ads
winbind uid = 10000-20000
winbind gid = 10000-20000
winbind use default domain = yes
# tirar outras opcoes de dominio master
```

- Editar o /etc/hosts e adicionar uma entrada para o nome do servidor AD.

- Entrar no dominio.

```
$ net join -S NOMESERVIDORDOMINIOWINDOWS -
Uuserdowindows%senhadowindows
```

- **OBS:** È necessário um usuário no windows com permissão no grupo Administradores.

- Verificar se o nscd está rodando e parar

```
$ ps auxwww | grep [n]scd
root      3036  0.0  0.2 141416  1080 ?        Ssl  10:04   0:00
/usr/sbin/nscd
$ /etc/init.d/nscd stop
$ chkconfig nscd off
```

- **OBS:** Esse procedimento acima é muito importante, pois dependendo da versão do samba, se o nscd estiver rodando o winbind não funciona!

- Startar nmb e winbind

```
$ /etc/init.d/nmb start; /etc/init.d/winbind start;
```

- Setar diretorio do winbind para mesmo grupo do squid:

```
chown root.GRUPOSQUID /var/lib/samba/winbindd_privileged
```

- Rodar diariamente no crontab

```
$ net rpc changetrustpw
```

- Testar se logou com sucesso no domínio:

```
$ wbinfo -t
Secret is good
```

- Testar autenticação do winbind:

```
$ wbinfo -a mydomain\\myuser%mypasswd
plaintext password authentication succeeded
error code was NT_STATUS_OK (0x0)
challenge/response password authentication succeeded
error code was NT_STATUS_OK (0x0)
```

MSNT

- Editar o /etc/squid/msntauth.conf

```
server PDCNAME PDCNAME WORKGROUP
```

- Editar o squid.conf:

```
auth_param basic program /usr/local/squid/libexec/msnt_auth
auth_param basic children 5
auth_param basic realm Usuário e Senha
auth_param basic credentialsttl 5 minutes

acl password proxy_auth REQUIRED
http_access allow LAN password
```

NTLM

- Particularidade do squid RPM do SuSE:
  - No SUSE tem 2 ntlm_auth, um em /usr/bin outro em /usr/sbin. TEM QUE USAR O DO /usr/bin:

```
 $ /usr/bin/ntlm_auth --helper-protocol=squid-2.5-basic
myuser mypasswd
OK
```

- Testar o autenticador na linha de comando:

```
$ /usr/local/bin/ntlm_auth --helper-protocol=squid-2.5-basic
mydomain+myuser mypasswd
OK
```

- Para debugar a autenticação, rodar o winbind com o parametro -d 6

- Inserir no squid.conf:

```
#Auth AD
auth_param ntlm program /usr/bin/ntlm_auth --helper-protocol=squid-
2.5-ntlmssp
auth_param ntlm children 30
auth_param basic program /usr/bin/ntlm_auth --helper-protocol=squid-
2.5-basic
auth_param basic children 5
auth_param basic realm Linux Proxy Server
auth_param basic credentialsttl 2 hours
```

- **OBS IMPORTANTE:** Perceba que no arquivo squid.conf existem 2 chamadas ao ntlm_auth. A primeira é referente a autenticação automática, pegando o usuário do windows já logado e a segunda é para pedir senha, para usuários não logados. Caso deseje que ele sempre solicite senha, mesmo para usuários logados, comente a primeira opção (ntlmssp) e deixe somente a segunda opção (basic).

Ingressar OpenSuse 10 no domínio.

Primeiramente é necessário instalar a última versão do samba3 ou do samba4. Nesse site ainda mantem o repositório para o samba. Caso não tenha mais acesso baixar os softwares abaixo para instalação.

libsmbclient-devel-3.6.23-45.suse102.i586.rpm
libsmbclient0-3.6.23-45.suse102.i586.rpm
libwbclient-devel-3.6.23-45.suse102.i586.rpm
libwbclient0-3.6.23-45.suse102.i586.rpm
samba3-3.6.23-45.suse102.i586.rpm
samba3-client-3.6.23-45.suse102.i586.rpm
samba3-debuginfo-3.6.23-45.suse102.i586.rpm

Caso o repositório ainda esteja online iremos utiliza-lo adicionando em YaST2 → Software → Installation Source → Add (ftp):

Protocol: FTP
Server Name: ftp.sernet.de
Directory on Server :pub/samba/3.6/suse/10.2 (pois a nossa versão é 10.2)

Após selecione os arquivos fazendo uma busca pelo nome samba em YaST2 → Software → Software Management
Todos arquivos que forem desta versão seleciona-los. Nota que ao selecionar irá excluir automaticamente o samba da versão anterior (a-).
Instalamos para o necessário:

ldapsmb	1.34b
libsmbclient-devel	3.6.23
libsmbclient0	3.6.23
libwbclient0	3.6.23
samba3	3.6.23
samba3-client	3.6.23

```
samba3-utils          |3.6.23
samba3-winbind        |3.6.23
samba3-winbind-32bit  |3.6.23
yast2-samba-client    |2.14.4
yast2-samba-server    |2.14.3
```

cat /etc/krb5.conf

```
[libdefaults]
        default_realm = DOMINIOEMPRESA.NET
        clockskew = 300

[realms]
DOMINIOEMPRESA.NET = {
        kdc = dominio.dominioempresa.net
        default_domain = dominioempresa.net
        admin_server = DOMINIO.DOMINIOEMPRESA.NET
}
EXAMPLE.COM = {
        kdc = dominio.dominioempresa.net
        admin_server = dominio.dominioempresa.net
}

[logging]
        kdc = FILE:/var/log/krb5/krb5kdc.log
        admin_server = FILE:/var/log/krb5/kadmind.log
        default = SYSLOG:NOTICE:DAEMON
[appdefaults]
pam = {
        ticket_lifetime = 1d
        renew_lifetime = 1d
        forwardable = true
        proxiable = false
        retain_after_close = false
        minimum_uid = 1
        use_shmem = sshd
}
[domain_realm]
        .DOMINIOEMPRESA.NET = DOMINIOEMPRESA.NET
        .DOMINIOEMPRESA = DOMINIOEMPRESA.NET
        .dominioempresa.net = DOMINIOEMPRESA.NET
```

```
[global]
        security = ADS
        realm = DOMINIOEMPRESA.NET
        workgroup = DOMINIOEMPRESA
        idmap uid = 500-40000
```

```
        idmap gid = 500-40000

        winbind enum users = yes
        winbind enum groups = yes
        template homedir = /home/%D/%U
        client use spnego = yes
        winbind use default domain = yes
        winbind cache time = 300
        restrict anonymous = 2
        usershare allow guests = No
        winbind refresh tickets = yes
        template shell = /bin/bash
        winbind offline logon = yes
        #winbind refresh tickets = yes



[htdocs]
        comment = Aplicacoes
        path = /opt/apache/htdocs
        read only = No
        writable = yes
        create mask = 0777
        directory mask = 0777


[www]
        comment = Aplicacoes
        path = /opt/apache/htdocs
        read only = No
        writable = yes
        create mask = 0777
        directory mask = 0777
```

```
cat /etc/nsswitch.conf

passwd: files winbind
group:  files winbind

#passwd: compat winbind
#group:  compat winbind

hosts:  files dns
networks:       files dns

services:       files
protocols:      files
rpc:    files
```

```
ethers: files
netmasks:       files
netgroup:       files nis
publickey:      files

bootparams:     files
automount:      files nis
aliases:        files
```

```
cat /etc/hosts

127.0.0.1       localhost
# fqdn do servidor de dominio
192.168.218.190 DOMINIO.DOMINIOEMPRESA.NET DOMINIO
# fqdn do próprio server suse
192.168.218.204 hmgcasp.dominioempresa.net hmgcasp
```

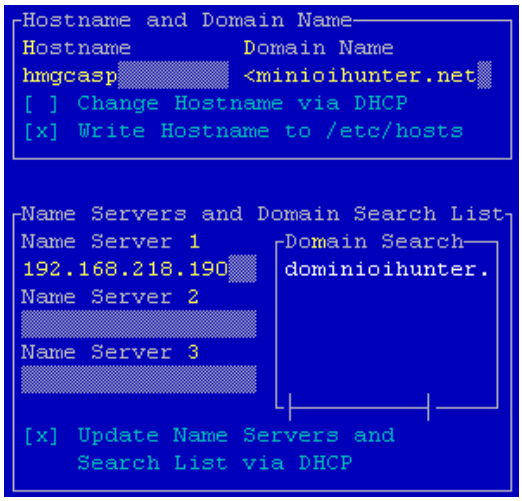
```
hostname -f
hmgcasp.dominioempresa.net
```

```
cat /etc/resolv.conf
nameserver 192.168.218.190
search dominioempresa.net
```

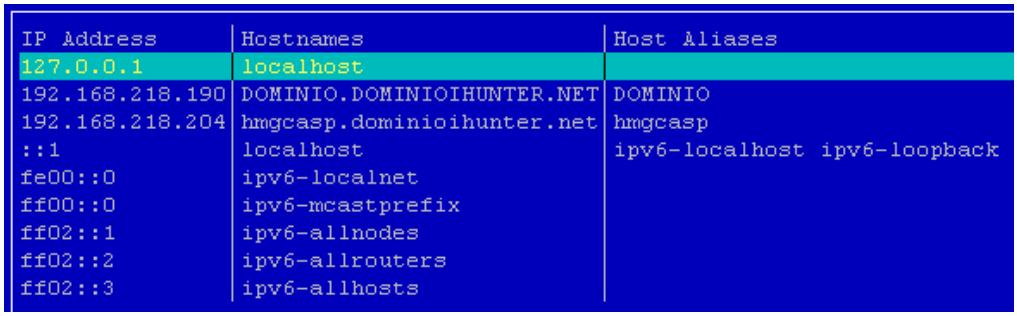
```
smbclient  -V
Version 3.6.23

smbd  -V
Version 3.6.23
```

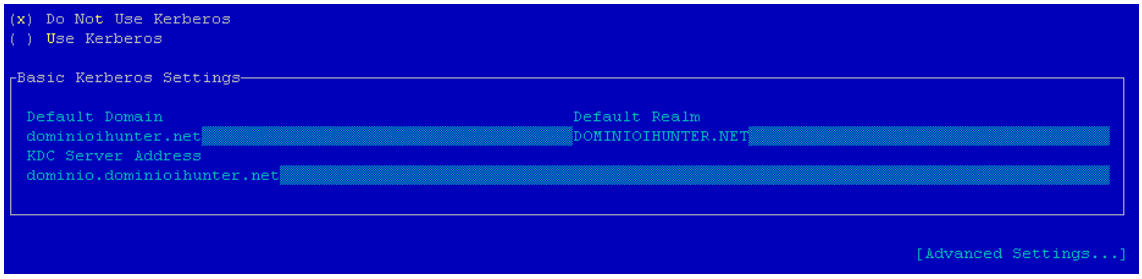
Network Services → DNS and Hostname



Network Services → Hostnames

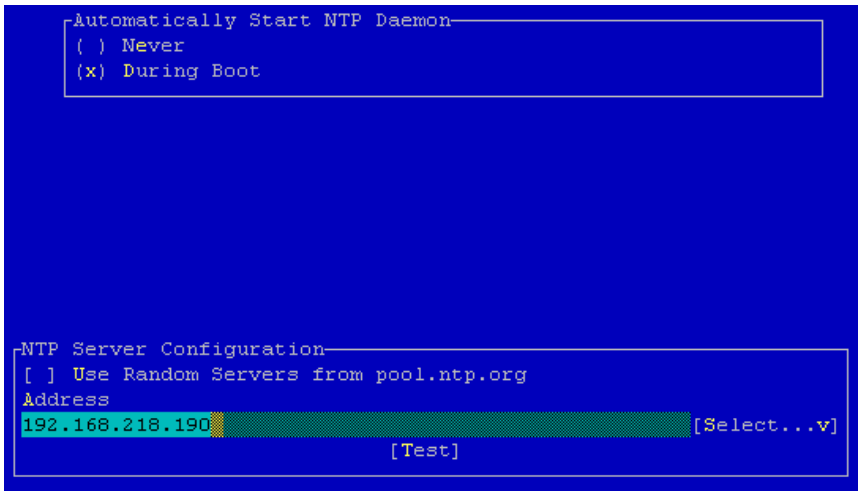


Network Services → Kerberos Client

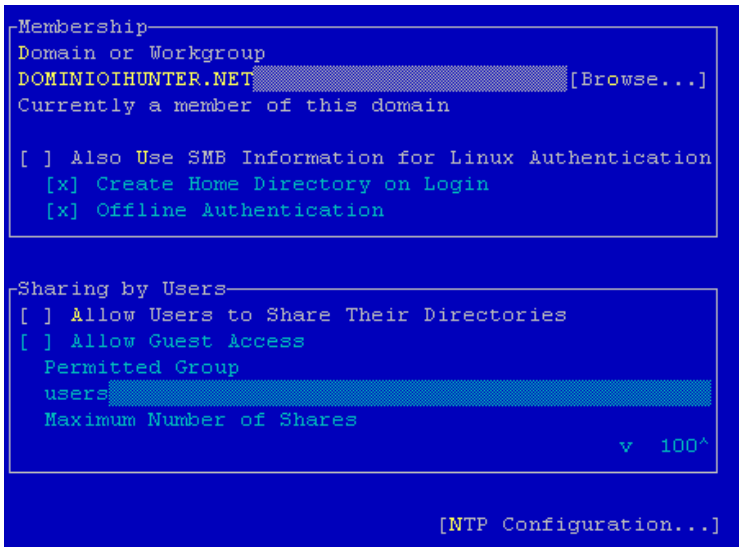


Network Services → Windows Domain Membership

Network Services → NTP Configuration →



Se tudo deu certo sera solicitado o nome de user e senha admin do dominio.




```
wbinfo -u
asantos
anascimento
rbarreiro
…

wbinfo -g
allowed rodc password replication group
enterprise read-only domain controllers
denied rodc password replication group
read-only domain controllers
group policy creator owners
ras and ias servers
domain controllers
```

Colocar os programas para subir no boot

YaST2 → System → System Services (Runlevel)
Nmb, smb, smbfs, winbind

Ingressar CentOS 6 no domínio

```
yum install samba samba-winbind samba-winbind-devel samba-client
samba-common \
 pam_krb5 cifs-utils samba-winbind-krb5-locator samba-doc krb5-
workstation -y
```

```
cat /etc/resolv.conf
nameserver 192.168.218.190
search dominioempresa.net
```

```
smbd -V
Version 3.6.9-167.el6_5

smbclient -V
Version 3.6.9-167.el6_5
```

```
cat /etc/samba/smb.conf
[global]
   security = ads
   realm= DOMINIOEMPRESA.NET
   workgroup = DOMINIOEMPRESA
   idmap uid =  500-40000

   idmap gid =  500-40000

   winbind enum users = yes
   winbind enum groups = yes
   template homedir = /home/%D/%U
   template shell = /bin/sh
   client use spnego = yes
   client ntlmv2 auth = yes
   winbind use default domain = yes
   winbind cache time = 300
   restrict anonymous = 2
```

```
   winbind refresh tickets = yes
```

```
cat /etc/krb5.conf
[libdefaults]
default_realm = DOMINIOEMPRESA.NET
[realms]
   DOMINIOEMPRESA.NET  =  {
      kdc  =  dominio.dominioempresa.net
      default_domain  =  DOMINIOEMPRESA.NET
      admin_server  =  dominio.mistoli.net
   }

[domain_realm]
.dominioempresa.net = DOMINIOEMPRESA.NET
```

```
(alterar esses dois parâmetros)
cat /etc/nsswitch.conf

passwd:     files winbind
shadow:     files
group:      files winbind
```

```
chkconfig --add nmb
chkconfig --add smb
chkconfig --add winbind
chkconfig nmb on

chkconfig smb on

chkconfig winbind on
```

```
/etc/init.d/nmb restart
/etc/init.d/smb restart
/etc/init.d/winbind restart
```

```
net ads join dominioempresa.net -U administrator
```

```
wbinfo -u
douglas.santos
```

```
administrator
dns-nodo1
krbtgt
guest
```

Vamos listar os grupos

```
wbinfo -g
allowed rodc password replication group
enterprise read-only domain controllers
denied rodc password replication group
ti-admin
read-only domain controllers
group policy creator owners
ras and ias servers
domain controllers
enterprise admins
domain computers
cert publishers
dnsupdateproxy
domain admins
domain guests
schema admins
domain users
dnsadmins
```

Comandos

Para logar no domínio:

 # kinit

Para ver os tickets emitidos:

 # klist

Para destruir a lista de tickets:

 # kdestroy

Testar configurações do Samba:

 # testparm

Adicionar máquina ao domínio:

 # net ads join -UNomeUsuario

Verificar se foi adicionado com sucesso:

```
# net ads testjoin
```