```
# Desliga SElinux
sestatus
cd /etc
cd sysconfig
vi selinux

# Desliga Firewall
chkconfig iptables off

# Desliga Network Manager
chkconfig NetworkManager off
chkconfig network on

# Configura Interface de rede e IP estatico para o Servidor
system-config-network-tui
cd /etc
cd sysconfig
cd network-scripts
vi ifcfg-eth0
service network restart

vi /etc/hosts
192.168.1.34 pdc.mtask pdc

# Coloca em runlevel 3 (Inicializacao em modo texto)
vi /etc/inittab

# Verifica se o IP esta correto
ifconfig

# Atualiza todo o sistema
yum update

# Instala os pacotes necessarios para SAMBA+LDAP
yum install openldap-servers
yum install smbldap-tools
yum install samba
yum install phpldapadmin

# Gera Backup da configuracao original
cp slapd.conf slapd.conf.original
cp smb.conf smb.original

# Refazer configuracoes modificando o template
vi slapd.conf

# Gera novo password do rootdn
slappasswd

# Configura a database
cp /usr/share/doc/openldap-servers-2.4.15/DB_CONFIG.example
/var/lib/ldap/DB_CONFIG
chown ldap:ldap /var/lib/ldap/DB_CONFIG
chmod 600 /var/lib/ldap/DB_CONFIG
```

```
# Refazer configuracoes modificando o template
vi smb.conf

mkdir /etc/skel/profiles
mkdir /home/samba/netlogon
mkdir /home/publico

service ldap start
service smb start
/usr/share/doc/smbldap-tools-0.9.5/configure.pl
smbldap-populate
smbpasswd -w mtask123

#Sincroniza senha do root no UNIX com root do samba (mtask123)
passwd

# Phpldapadmin
# Incluir Allow from <client ip>
vi /etc/httpd/conf.d/phpldapadmin.conf
service httpd start

# Acessar via browser de 127.0.0.1 para http://127.0.0.1/phpldapadmin
cn=root,dc=mtask
mtask123

# Configura startup das daemons no boot
chkconfig ldap on
chkconfig smb on
chkconfig httpd on
# Incluir em /etc/rc.d/rc.local
/usr/sbin/nmbd -D

# Configurando os grupos no unix
groupadd geral -g 600
groupadd financeiro -g 601
groupadd vendas -g 602

# Configurando os grupos no samba
smbldap-groupadd geral
smbldap-groupadd financeiro
smbldap-groupadd vendas

# Faz o mapeamento dos grupos do unix para os grupos do samba
net groupmap add rid=601 unixgroup=financeiro type=local ntgroup=financeiro
net groupmap add rid=602 unixgroup=vendas type=local ntgroup=vendas
net groupmap add rid=600 unixgroup=geral type=local ntgroup=geral

net groupmap list

# Criando usuarios usuarios no samba e no unix
useradd paulo
passwd paulo
smbldap-useradd -a -G geral -m -P paulo
```

```
# Configura autenticacao LDAP para o sistema
startx
system-config-authentication
# Configurar User Information e Authentication para LDAP
ou=Usuarios,dc=ldap
# editar arquivo /etc/ldap.conf conforme o modelo

# Servico LDAP precisa iniciar antes (Bug do fedora) (workaround by Juliano)
cd /etc/rc.d/rc3.d/
cp S27ldap S11ldap

# Teste de conexao no samba
smbclient -L 192.168.1.34 -U paulo

# Testa mapeamento e autenticaçao LDAP
ls -la /home
getent passwd

--------------------------------------------------------------------------------
# Backup e Manutenções no LDAP Server

# Dump inteiro da base LDAP (Primeiro pare o LDAP service ldap stop)
# Ou coloque em read-only, isso para garantir que nao estao sendo feitas
escritas na base

slapcat -l base.ldif

# Importar a base
# Primeiro apague tudo que ja existe
service ldap stop
cd /var/lib/ldap
rm -rf *

# Importando
cp /usr/share/doc/openldap-servers-2.4.15/DB_CONFIG.example
/var/lib/ldap/DB_CONFIG
slapadd -l base.ldif (slapadd -q -l base.ldif)
cd /var/lib/ldap
chown ldap:ldap *
chmod g+r *
chmod o+r *
service ldap start

--------------------------------------------------------------------------------

[global]
      hosts allow = 127. 192. 10.
      unix charset = UTF-8
      dos charset = UTF-8
      display charset = LOCALE
      workgroup = mtask
      netbios name = PDC
      netbios aliases = PDC
      server string = PDC Server
      security = user
```

```
      encrypt passwords = Yes
      passwd chat debug = Yes
      load printers = Yes
      log level = 2
        syslog = 0
      log file = /var/log/samba/%m.log
      max log size = 1000
      os level = 250
      #debug level = 10
      username level = 2
      local master = yes
      domain master = yes
      preferred master = yes
      domain logons = yes
      admin users = root Administrador @"Domain Admins"
      logon script = logon.vbs
      logon path = \\PDC\%U\profiles
      logon home = \\PDC\%U
      auto services = %U
      logon drive = U:
      wins support = yes
      ldap ssl = off
        ldap passwd sync = yes
      ldap admin dn = cn=root,dc=mtask
      ldap suffix = dc=mtask
      ldap group suffix = ou=Grupos
      ldap user suffix = ou=Usuarios
      ldap idmap suffix = ou=Idmap
      ldap machine suffix = ou=Computadores
      passdb backend = ldapsam:ldap://127.0.0.1/
      ldap delete dn = yes
      idmap uid = 1000-1500
      idmap gid = 1000-1500
      inherit acls = Yes
      nt acl support = Yes
      map acl inherit = Yes
      create mask = 600
      directory mask = 0700
      force directory mode = 0700
      passwd chat = *new*password* %n\n *Retype*new*password*
%n\n*passwd:*all*authentication*tokens*updated*successfully* *Nova*senha* %n\n
*Redigite*nova*senha*
%n\n*senha:*todos*autentica√ß√µes*tokens*atualizados*sucesso*
      socket options = TCP_NODELAY IPTOS_LOWDELAY SO_RCVBUF=8192 SO_SNDBUF=8192
      add machine script = /usr/sbin/smbldap-useradd -W "%u"
      add user script = /usr/sbin/smbldap-useradd -m "%u"
      delete user script = /usr/sbin/smbldap-userdel "%u"
      add group script = /usr/sbin/smbldap-groupadd -p "%g"
      delete group script = /usr/sbin/smbldap-groupdel "%g"
      add user to group script = /usr/sbin/smbldap-groupmod -m "%u" "%g"
      delete user from group script = /usr/sbin/smbldap-groupmod -x "%u"
      set primary group script = /usr/sbin/smbldap-usermod -g "%g" "%u"
      getwd cache = No
      stat cache = No
      dns proxy = No
```

```
      guest ok = No
      restrict anonymous = 1
      #vfs objects = full_audit
      #full_audit:success = open, opendir, write, unlink, rename, mkdir, rmdir,
chmod, chown
      #full_audit:prefix = %u|%I|%S
      name resolve order = wins bcast
      hide dot files = yes


[homes]
      comment = Pastas pessoais
      read only = No
      inherit acls = Yes
      browseable = No
      fake oplocks = yes

[profiles]
      comment = Network Profiles Service
      path = /home/%U/profiles
      read only = No
      create mask = 0600
      directory mask = 0700
      store dos attributes = Yes
      browseable = no
      guest ok = yes
      profile acls = yes
      csc policy = disable
      force user = %u

[users]
      comment = All users
      path = /home
      valid users = @geral
      read only = No
      inherit acls = Yes
      #veto files = /aquota.user/groups/shares/
      browseable = yes

[fiscal]
      comment = Usuarios do Grupo Financeiro
      path = /home/fiscal
      valid users = @financeiro
      read only = no
      browseable = yes
      write list = @financeiro

[printers]
      comment = All Printers
      path = /var/spool/samba
      create mask = 0600
      guest ok = Yes
      printable = Yes
      browseable = No
```

```
[print$]
      comment = Printer Drivers
      path = /var/lib/samba/drivers
      write list = @ggTI
      force group = ntadmin
      read only = No
      acl check permissions = No
      acl map full control = No
      create mask = 0664
      directory mask = 0775
      force unknown acl user = Yes
      inherit permissions = Yes
      inherit acls = Yes
      inherit owner = Yes
      guest ok = Yes
      map acl inherit = Yes

[netlogon]
      path = /home/samba/netlogon
      read only = No
      public = no
      writeable = Yes
      browsable = Yes
      write list = @ggTI
      force directory mode = 0777
      force create mode = 0777
      force directory security mode = 0777

[Publico]
      comment = Publico
      public = yes
      path = /home/publico
      #force group = ggPublico
      writeable = Yes
      read only = No
      browseable = Yes
      force directory mode = 0770
      force create mode = 0770
      force directory security mode = 0770

----------------------

#
# See slapd.conf(5) for details on configuration options.
# This file should NOT be world readable.
#

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/misc.schema
include          /etc/openldap/schema/samba.schema

# Allow LDAPv2 client connections.  This is NOT the default.
```

```
allow bind_v2

# Do not enable referrals until AFTER you have a working directory
# service AND an understanding of referrals.
#referral   ldap://root.openldap.org

pidfile          /var/run/openldap/slapd.pid
argsfile    /var/run/openldap/slapd.args

# Load dynamic backend modules:
# modulepath     /usr/lib/openldap # or /usr/lib64/openldap
# moduleload accesslog.la
# moduleload auditlog.la
# moduleload back_sql.la
# moduleload denyop.la
# moduleload dyngroup.la
# moduleload dynlist.la
# moduleload lastmod.la
# moduleload pcache.la
# moduleload ppolicy.la
# moduleload refint.la
# moduleload retcode.la
# moduleload rwm.la
# moduleload syncprov.la
# moduleload translucent.la
# moduleload unique.la
# moduleload valsort.la

# The next three lines allow use of TLS for encrypting connections using a
# dummy test certificate which you can generate by changing to
# /etc/pki/tls/certs, running "make slapd.pem", and fixing permissions on
# slapd.pem so that the ldap user or group can read it.  Your client software
# may balk at self-signed certificates, however.
# TLSCACertificateFile /etc/pki/tls/certs/ca-bundle.crt
# TLSCertificateFile /etc/pki/tls/certs/slapd.pem
# TLSCertificateKeyFile /etc/pki/tls/certs/slapd.pem

# Sample security restrictions
#     Require integrity protection (prevent hijacking)
#     Require 112-bit (3DES or better) encryption for updates
#     Require 63-bit encryption for simple bind
# security ssf=1 update_ssf=112 simple_bind=64

# Sample access control policy:
#     Root DSE: allow anyone to read it
#     Subschema (sub)entry DSE: allow anyone to read it
#     Other DSEs:
#           Allow self write access
#           Allow authenticated users read access
#           Allow anonymous users to authenticate
#     Directives needed to implement policy:
# access to dn.base="" by * read
# access to dn.base="cn=Subschema" by * read
# access to *
#     by self write
```

```
#     by users read
#     by anonymous auth
#
# if no access controls are present, the default policy
# allows anyone and everyone to read anything but restricts
# updates to rootdn.  (e.g., "access to * by * read")
#
# rootdn can always read and write EVERYTHING!

#######################################################################
# ldbm and/or bdb database definitions
#######################################################################

database    bdb
suffix          "dc=mtask"
checkpoint  1024 15
rootdn          "cn=root,dc=mtask"
rootpw          {SSHA}A5iYm+jfXNSKWeuHl8ytmazuKBbyMMaE
#rootpw mtask123

# Cleartext passwords, especially for the rootdn, should
# be avoided.  See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
# rootpw        secret
# rootpw        {crypt}ijFYNcSNctBYg

# The database directory MUST exist prior to running slapd AND
# should only be accessible by the slapd and slap tools.
# Mode 700 recommended.
directory   /var/lib/ldap

# Indices to maintain for this database
#index objectClass                      eq,pres
#index ou,cn,mail,surname,givenname     eq,pres,sub
#index uidNumber,gidNumber,loginShell   eq,pres
#index uid,memberUid                    eq,pres,sub
#index nisMapName,nisMapEntry           eq,pres,sub

index objectClass,uidNumber,gidNumber   eq
index cn,sn,uid,displayName       pres,sub,eq
index memberUid,mail,givenname          eq
index sambaSID,sambaPrimaryGroupSID,sambaDomainName eq
index default    sub


# Replicas of this database
#replogfile /var/lib/ldap/openldap-master-replog
#replica host=ldap-1.example.com:389 starttls=critical
#     bindmethod=sasl saslmech=GSSAPI
#     authcId=host/ldap-master.example.com@EXAMPLE.COM


# enable monitoring
database monitor
```

```
# allow only rootdn to read the monitor
#access to *
#        by dn.exact="cn=Manager,dc=my-domain,dc=com" read
#        by * none

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

access to *
      by * read

----------------------------------------------------------------------

# @(#)$Id: ldap.conf,v 1.38 2006/05/15 08:13:31 lukeh Exp $
#
# This is the configuration file for the LDAP nameservice
# switch library and the LDAP PAM module.
#
# The man pages for this file are nss_ldap(5) and pam_ldap(5)
#
# PADL Software
# http://www.padl.com
#

# Your LDAP server. Must be resolvable without using LDAP.
# Multiple hosts may be specified, each separated by a
# space. How long nss_ldap takes to failover depends on
# whether your LDAP client library supports configurable
# network or connect timeouts (see bind_timelimit).
#host 127.0.0.1

# The distinguished name of the search base.
base ou=Usuarios,dc=mtask

# Another way to specify your LDAP server is to provide an
# uri with the server name. This allows to use
# Unix Domain Sockets to connect to a local LDAP Server.
#uri ldap://127.0.0.1/
#uri ldaps://127.0.0.1/
#uri ldapi://%2fvar%2frun%2fldapi_sock/
# Note: %2f encodes the '/' used as directory separator

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

# The distinguished name to bind to the server with.
# Optional: default is to bind anonymously.
binddn cn=root,dc=mtask

# The credentials to bind with.
# Optional: default is no credential.
bindpw mtask123
```

```
# The distinguished name to bind to the server with
# if the effective user ID is root. Password is
# stored in /etc/ldap.secret (mode 600)
#rootbinddn cn=root,dc=matsk

# The port.
# Optional: default is 389.
#port 389

# The search scope.
#scope sub
#scope one
#scope base

# Search timelimit
#timelimit 30
timelimit 120

# Bind/connect timelimit
#bind_timelimit 30
bind_timelimit 120

# Reconnect policy: hard (default) will retry connecting to
# the software with exponential backoff, soft will fail
# immediately.
#bind_policy hard

# Idle timelimit; client will close connections
# (nss_ldap only) if the server has not been contacted
# for the number of seconds specified below.
#idle_timelimit 3600
idle_timelimit 3600

# Filter to AND with uid=%s
#pam_filter objectclass=account

# The user ID attribute (defaults to uid)
#pam_login_attribute uid

# Search the root DSE for the password policy (works
# with Netscape Directory Server)
#pam_lookup_policy yes

# Check the 'host' attribute for access control
# Default is no; if set to yes, and user has no
# value for the host attribute, and pam_ldap is
# configured for account management (authorization)
# then the user will not be allowed to login.
#pam_check_host_attr yes

# Check the 'authorizedService' attribute for access
# control
# Default is no; if set to yes, and the user has no
# value for the authorizedService attribute, and
```

```
# pam_ldap is configured for account management
# (authorization) then the user will not be allowed
# to login.
#pam_check_service_attr yes

# Group to enforce membership of
#pam_groupdn cn=PAM,ou=Groups,dc=example,dc=com

# Group member attribute
#pam_member_attribute uniquemember

# Specify a minium or maximum UID number allowed
#pam_min_uid 0
#pam_max_uid 0

# Template login attribute, default template user
# (can be overriden by value of former attribute
# in user's entry)
#pam_login_attribute userPrincipalName
#pam_template_login_attribute uid
#pam_template_login nobody

# HEADS UP: the pam_crypt, pam_nds_passwd,
# and pam_ad_passwd options are no
# longer supported.
#
# Do not hash the password at all; presume
# the directory server will do it, if
# necessary. This is the default.
#pam_password clear

# Hash password locally; required for University of
# Michigan LDAP server, and works with Netscape
# Directory Server if you're using the UNIX-Crypt
# hash mechanism and not using the NT Synchronization
# service.
#pam_password crypt

# Remove old password first, then update in
# cleartext. Necessary for use with Novell
# Directory Services (NDS)
#pam_password clear_remove_old
#pam_password nds

# RACF is an alias for the above. For use with
# IBM RACF
#pam_password racf

# Update Active Directory password, by
# creating Unicode password and updating
# unicodePwd attribute.
#pam_password ad

# Use the OpenLDAP password change
# extended operation to update the password.
```

```
#pam_password exop

# Redirect users to a URL or somesuch on password
# changes.
#pam_password_prohibit_message Please visit http://internal to change your
password.

# RFC2307bis naming contexts
# Syntax:
# nss_base_XXX         base?scope?filter
# where scope is {base,one,sub}
# and filter is a filter to be &'d with the
# default filter.
# You can omit the suffix eg:
# nss_base_passwdou=People,
# to append the default base DN but this
# may incur a small performance impact.
#nss_base_passwd ou=People,dc=example,dc=com?one
#nss_base_shadow ou=People,dc=example,dc=com?one
#nss_base_group        ou=Group,dc=example,dc=com?one
#nss_base_hosts        ou=Hosts,dc=example,dc=com?one
#nss_base_services     ou=Services,dc=example,dc=com?one
#nss_base_networks     ou=Networks,dc=example,dc=com?one
#nss_base_protocols    ou=Protocols,dc=example,dc=com?one
#nss_base_rpc          ou=Rpc,dc=example,dc=com?one
#nss_base_ethers ou=Ethers,dc=example,dc=com?one
#nss_base_netmasks     ou=Networks,dc=example,dc=com?ne
#nss_base_bootparams   ou=Ethers,dc=example,dc=com?one
#nss_base_aliasesou=Aliases,dc=example,dc=com?one
#nss_base_netgroup     ou=Netgroup,dc=example,dc=com?one

# Just assume that there are no supplemental groups for these named users
nss_initgroups_ignoreusers
root,ldap,named,avahi,haldaemon,dbus,radvd,tomcat,radiusd,news,mailman,nscd,gdm,
polkituser

# attribute/objectclass mapping
# Syntax:
#nss_map_attribute     rfc2307attribute mapped_attribute
#nss_map_objectclass   rfc2307objectclass     mapped_objectclass

# configure --enable-nds is no longer supported.
# NDS mappings
#nss_map_attribute uniqueMember member

# Services for UNIX 3.5 mappings
#nss_map_objectclass posixAccount User
#nss_map_objectclass shadowAccount User
#nss_map_attribute uid msSFU30Name
#nss_map_attribute uniqueMember msSFU30PosixMember
#nss_map_attribute userPassword msSFU30Password
#nss_map_attribute homeDirectory msSFU30HomeDirectory
#nss_map_attribute homeDirectory msSFUHomeDirectory
#nss_map_objectclass posixGroup Group
#pam_login_attribute msSFU30Name
```

```
#pam_filter objectclass=User
#pam_password ad

# configure --enable-mssfu-schema is no longer supported.
# Services for UNIX 2.0 mappings
#nss_map_objectclass posixAccount User
#nss_map_objectclass shadowAccount user
#nss_map_attribute uid msSFUName
#nss_map_attribute uniqueMember posixMember
#nss_map_attribute userPassword msSFUPassword
#nss_map_attribute homeDirectory msSFUHomeDirectory
#nss_map_attribute shadowLastChange pwdLastSet
#nss_map_objectclass posixGroup Group
#nss_map_attribute cn msSFUName
#pam_login_attribute msSFUName
#pam_filter objectclass=User
#pam_password ad

# RFC 2307 (AD) mappings
#nss_map_objectclass posixAccount user
#nss_map_objectclass shadowAccount user
#nss_map_attribute uid sAMAccountName
#nss_map_attribute homeDirectory unixHomeDirectory
#nss_map_attribute shadowLastChange pwdLastSet
#nss_map_objectclass posixGroup group
#nss_map_attribute uniqueMember member
#pam_login_attribute sAMAccountName
#pam_filter objectclass=User
#pam_password ad

# configure --enable-authpassword is no longer supported
# AuthPassword mappings
#nss_map_attribute userPassword authPassword

# AIX SecureWay mappings
#nss_map_objectclass posixAccount aixAccount
#nss_base_passwd ou=aixaccount,?one
#nss_map_attribute uid userName
#nss_map_attribute gidNumber gid
#nss_map_attribute uidNumber uid
#nss_map_attribute userPassword passwordChar
#nss_map_objectclass posixGroup aixAccessGroup
#nss_base_group ou=aixgroup,?one
#nss_map_attribute cn groupName
#nss_map_attribute uniqueMember member
#pam_login_attribute userName
#pam_filter objectclass=aixAccount
#pam_password clear

# Netscape SDK LDAPS
#ssl on

# Netscape SDK SSL options
#sslpath /etc/ssl/certs
```

```
# OpenLDAP SSL mechanism
# start_tls mechanism uses the normal LDAP port, LDAPS typically 636
#ssl start_tls
#ssl on

# OpenLDAP SSL options
# Require and verify server certificate (yes/no)
# Default is to use libldap's default behavior, which can be configured in
# /etc/openldap/ldap.conf using the TLS_REQCERT setting.  The default for
# OpenLDAP 2.0 and earlier is "no", for 2.1 and later is "yes".
#tls_checkpeer yes

# CA certificates for server certificate verification
# At least one of these are required if tls_checkpeer is "yes"
#tls_cacertfile /etc/ssl/ca.cert
#tls_cacertdir /etc/ssl/certs

# Seed the PRNG if /dev/urandom is not provided
#tls_randfile /var/run/egd-pool

# SSL cipher suite
# See man ciphers for syntax
#tls_ciphers TLSv1

# Client certificate and key
# Use these, if your server requires client authentication.
#tls_cert
#tls_key

# Disable SASL security layers. This is needed for AD.
#sasl_secprops maxssf=0

# Override the default Kerberos ticket cache location.
#krb5_ccname FILE:/etc/.ldapcache

# SASL mechanism for PAM authentication - use is experimental
# at present and does not support password policy control
#pam_sasl_mech DIGEST-MD5
uri ldap://127.0.0.1/
ssl no
tls_cacertdir /etc/openldap/cacerts
pam_password md5
```