# ############ ####

#### ####### <kurin@causa-sui.net>
#######: 52213

######### © 2007, 2008 ####### ## ############ ## #######

####### ## # ########## ######### ## ### ####### ##########.

#### ## ### ############ #### ## ############ ### ####### ## ########## ##### ######## ### ####### ## ##########. ##### ##### ############ ###### ## #### ########, ### ### ####### ####### ### ##### ## ### ######### #####, ### ############ #### #### ######## ## ### ### ## ### ### ######.

2018#09#06 00:20:03 ### #######.

## ######

#### ######### ######## ### ## #### #### # ############ ## ## ######## #### (############## ## ######## ########) #### ############ ## #######. #### # #### #### ######### ## ### ###### ########## ######## ### ###### ###### ## #######, ### #######, #### ########## ## ###.

## ######

1. ######## ..... 1
2. ############ # #### ..... 1
3. ############ ## ####### ..... 5
4. ############# ## ######### ..... 9
#. ###### ##### ..... 11
#. ############ ## ####### #### #### ..... 12

## 1. ########

#### ######### ########## # ######## ## ###### ### ########### ########## ## #### #### ########## ## ######## ####. #### ######### ######## ######## ### ########## ## ###/###_#### # ########/###_#### #### ### ### ######## ## ######## ######## #### ### ### # ######## ####.

###### ########, # ###### #### ### ##### ## ########## # ######### ## ######## ####### ### ##### ######## ## ######### #### # ########## # ######### ## ######## ####### ### ##### ########## ## ## ######### ####.

#### ###### ### ######## ### ## ###### ######### ## #########, ######## ## ############# ##### ######## ############ #### ########## # #### ## ## ###### ######## ########## ####. ###### # ##### ##### # ####### ## ##### #### ############, ### ### ###### ######### ## ######### #### ## ###### #####. #### ###### #### ### ########### #### ########### ## ##### ######## ########, # ######## ############## #### #### ### ########### ### ### ######## ######### ### ##########.

## 2. ############ # ####

#### ######### ############ ######### ###### ######### # # ## ########### ## #.500 ######### ###### ########. #### ############## #### ######## ##### ## ###4510 # ########## #########. ##############, # ## ##### ## ##### ### ###### ### #### ### #### ########## ## ### # ########.

# ######## #### ######## #### ##### ### ######## ##### #########; ###### ## ########## #### ##### ### ########## ########## # ###### ########## ##########, # ##### ##### ## ############## ######## # ################ #### ########. ######## ###### ######## ## ######## ### #####, ### ######## ###/########24########. ## ########## ######## ########## ### ########### ###/########24######## ###############.

######## (############) #### ##### ## ######## #### ### ######## ## ############. # ######## # # ############ ## ## ######## #### ######## ## ######## ############, # # ######## # ######### ######## ## ######### ## ######## #### ### ## ########## ## ######## ###### #### ######### ### ###.

## 2.1. ############ # ######## #### ########

### ####

#### ##### # ########## ## ########. ## #### ######## ###### ##### ########, ######### ######### # ############ ##### ########.

### 2.1.1. ########## # ########

########, ######## # ########:

#### 1. ########## # ########

```
# cd /usr/ports/net/openldap24-server
# make install clean
```

#### ######## ## ######## slapd # slurpd, ########## ### ## ########### ######## ##########.

### 2.1.2. ############ # ########

## ########, ######## ########## # ########.

#### ######## ###### ############ ## #### ######## ### # ######## ####; #### #########, ## ###### ## #### ######## ##### ############ ## ##### ########, # ### # ########### ########. ## ########### ### ######## ######## #### ##### ##### ########### ## ############, ### # ###.

### ######### ########## ## ###### ## ###########. ######## ### ######## ### ###### # ## ######## ### *mesmas* ###### ### ## ###### ######## ### ###; #####, ## ######## #### ### ######## # ### ######## ## ######## ## ##### 25 # ## ######## #### ######## ## 389.

### ######### ######## ######## ######, # ######## ### ########### ### *não* ######## ### ###### ###### ### #### ############ ########. #####, # ##### ###### ## ##### 465 (### 25), ##### ###### ## 443 # ##### ## 636.

# ##### #### #### # ### ### ### ##### ######### ## ### # ###### ### ######## ### ###### #### ##### ######## # ######## #### # ######## ############## #### # ######## STARTTLS. ## ######## ### ### ############### ##### # ######. #### #####, ### ## ########## ############ ##### ## ####.

### ####

########## # ######## #### #### # ###, ## ### # ### # ########## ########.

### ### ### # ######## ###### ######### ### #####, ## ######### ########## ## ############ ## /usr/local/etc/openldap/slapd.conf #### ###### # ###:

```
security ssf=128

TLSCertificateFile /caminho/para/seu/cert.crt
TLSCertificateKeyFile /caminho/para/sua/cert.key
TLSCACertificateFile /caminho/para/seu/cacert.crt
```

####, ssf=128 ### ## ######## #### ###### ############ ## 128 #### #### ##### ## ########, ##### ## ######## ###### ## ############. #### ######### #### ### ########### ### #### ### ############ ## ######### ## ### ####, ### ######### # ########## ############, #### # ####### ### ########### ## ######## #### ####### ####### # ############ #####.

## ######## cert.crt, cert.key # cacert.crt ### ########### #### ### ## ######## ########### *você* #### # ######## #### ######. ## #### ############ ###### ## ######## ### #### #########, ###### ##### ## ########### ############ ### # #######:

### 2. ####### ### ##### ###

```
% openssl genrsa -out cert.key 1024
Generating RSA private key, 1024 bit long modulus
.....++++++
...++++++
e is 65537 (0x10001)
% openssl req -new -key cert.key -out cert.csr
```

##### #####, #### #### ### ########## #### ####### ###### #######. #### #### ####### ## ####### ### ######; ## #######, # ########## ### # ##### ####### ##### #### # #### ## ####### ########## ########## ## ######## ########. ## ##### ####, # ## ######## ####, # ######## # *server.example.org*. ######## ############## #### ##### #### ### ### ## ######## ###### ## ##### ########. #### #### ###### ### ###### ##########, ########, ############# ## ###### ########### ##### ######.

### ###, # ########## ## ########## ## ########### ####### ### ########:

### 3. ############## # ###########

```
% openssl x509 -req -in cert.csr -days 365 -signkey cert.key -out cert.crt
Signature ok
subject=/C=AU/ST=Some-State/O=Internet Widgits Pty Ltd
Getting Private key
```

#### ###### ## ########### ############# ### #### ### ##### #### ## ######### ## slapd.conf, #### cert.crt # cacert.crt ### # ##### #######. ## #### ### #### ###### ########## ######## (#### ########## ### slurpd),

#### ### ###### ### ######## #, *Certificados do OpenSSL para LDAP* #### ##### ### ##### ## # ###### #### ####### ############ ## ######## ###########.

##### ####, ####### # ######## ## /etc/rc.conf:

```
slapd_enable="YES"
```

## #######, ####### **/usr/local/etc/rc.d/slapd start**. #### #### ####### # ########. ######## ### #### ######### ## 389 ###

```
% sockstat -4 -p 389
ldap     slapd      3261  7  tcp4   *:389                 *:*
```

### 2.1.3. ############ # #######

####### # #### ###/########24######## #### ## ########### ## ########. ## ######## ####### ###### ##### ########### ########, ## ### # #### # ####### # ########/###_#### # ###/###_####, #### ##### ### ########.

# ####### ## ############ #### ## ########### ######## # /usr/local/etc/openldap/ldap.conf. ##### #### ####### #### ###### ## ######### #######:

```
base dc=example,dc=org
uri ldap://server.example.org/
ssl start_tls
tls_cacert /path/to/your/cacert.crt
```

#### 

# ########## ### #### ######## ###### ###### ## cacert.crt, #### #########, #### ### ####### ## ########.

#### 

####### #### ######## ######## ldap.conf. # ######## # #### #######, ### # #### ## ########### ######## # ###### #### ##### ### # ########. # ####### # /usr/local/etc/ldap.conf # # #### ###_####.

##### #####, #### #### ######### ######## **ldapsearch -Z** ## ####### #######; -Z ######### ##### # ####. ## #### ######### ## ####, ##### #### #### ########### ######; ##### ############# ### #### ############. ### ## ######## s_client # s_server ## #######(1) #### ######### ### #### ## ##### ########### # ######## ############.

## 2.2. ######## ## ##### ## #####

# ############ ## ## ######### #### ########## # ######### #### ######### ## ######## ## ######### #### # ####### ## #######. #### # ##### ############# ## ####### ######### ## ######### ### # #### ## ####### #########. ## ###### ### ####### ### # uid ##### ## #### ## ####### # # ######## userPassword ## ####### ############ # ##### #########, # ######## #### ############.

# ######## ##### ### ##### ### ##### # ######### #### ## ######### ## ###### ######## #### #####.

# ####### ## #### #### ##### ##### ## ##### # dc=example,dc=org. # ##### ###### #### ######## ### # ####### ### ######## ###### ####### # #### #### ou=people, *base* , ##### # #### ### #### ##### ####. ## #######, ##### ## ##### ### #### # ############.

#####, # ####### #### #### # ####### ############## people #### ########## #:

```
dn: ou=people,dc=example,dc=org
objectClass: top
objectClass: organizationalUnit
ou: people
```

##### ## ######## ##### ####### #### ########## ##### ####### ##############.

###### ############ #### ### #### # ###### ## ###### # ### #### ######## ###########. # ####### ### ###########, ### ######, ##### people, # ### # ### ## #### ###### ############ ######## ######## #### ##########. ## #######, ## #### ### ######### ########## ## ####### ## ##### ## ##### ####, ############ ##### inetOrgPerson, ### ###### ###### ######### #####. ## ##### ## #####, ## ######## ########## ######## ### ########## ## slapd.conf.

#### #### #######, ######## # ###### ## ###### person. ## #### ####### ###### inetOrgPerson, ## ###### ### ########## #########, ###### ### # ######## sn # ##########.

#### ######### ## ####### testuser, # #### #####:

```
dn: uid=tuser,ou=people,dc=example,dc=org
objectClass: person
objectClass: posixAccount
objectClass: shadowAccount
objectClass: top
uidNumber: 10000
gidNumber: 10000
homeDirectory: /home/tuser
loginShell: /bin/csh
uid: tuser
cn: tuser
```

## ###### ## #### ### #### ######## #### ## 10000 #### ###### ######## ### ###### ## #######; #### #### ########## # ###### ### ######## ####, ##### ### #### ##### ### 65536.

###### ########## ## ######## ## #####. #### ### ############# #### ######## ## #######, ### ######## ## ####### ######:

```
dn: ou=groups,dc=example,dc=org
objectClass: top
objectClass: organizationalUnit
ou: groups

dn: cn=tuser,ou=groups,dc=example,dc=org
objectClass: posixGroup
objectClass: top
gidNumber: 10000
cn: tuser
```

#### ########## ## ### ##### ## #####, #### #### #### slapadd ## ldapadd ## ## ####### ######## ##### ########. ################, #### #### #### # ########/######.

# ########## ldapsearch ## ######## ######## #### ##### ######## ##### ########. ## #### ##########, # ##### ## ##### #### ########### ############ #### ### ##### #### ## ######## ## ############ ####.

## 3. ############ ## #######

# ####### ## #### ### ########## ## ######## ## ##### 2.1.3, ############ # ########, ### ## #### ####### ########## ###### ######## ########, ######### ######## # ###/########24######## ## #### ## #####.

# ####### ###### ### #### ##### ##### ########## #### ############ ## ## ######## ####, ########/###_#### # ###/###_####.

## 3.1. ############

# ########/###_#### # ############ ####### ## /usr/local/etc/ldap.conf.

### ####

#### # ## *arquivo diferente* ### # ####### ## ############ ### ####### ## ########## ########, /usr/local/etc/openldap/ldap.conf; ## #######, ### ############ ###### ### ###### ######; ## #######, # ## ############## ##### #######. #### # ##### ##### #####, ########### # ldap.conf #### ########## # ######## /usr/local/etc/ldap.conf.

#####, ##### ###### ###### ##### ## ###### ########## ## ############ ######### ## openldap/ldap.conf #### # #### ldap.conf. ##### ####, ######## ######## ## ########/###_#### # ### ######## ## ######## ## #########.

####### ############# ###### ######## ### # ######## uid. #### ########## #### (###### #### # ######), ###### # ######## pam_login_attribute ## ldap.conf:

### ####### 4. ######### pam_login_attribute

```
pam_login_attribute uid
```

### #### #########, # ########/###_#### ########## #### # ######### #### ## base #### # ##### uid=*username*. ## ######### ### # ###### ### #######, ### ######## ## ######## #### ###### ######## ### # ##### ### ### #########. ## ######## ############, ##### ######### # ######. #### #########, ########.

## ######## #### ##### ### #### ## /etc/shells ### ######## ######## #####. #### # ############### ########## ###### # #### # ######## #### # ##### ## ######## ## ######## ####. # #### ### #### ######## ## ### ########## ###### ## ########. ###### ######### # ###### ## ## ###### ## ####, ### #### ########## ## /usr/local/bin/bash. ######### ## # ######## #### # ##### ## ######## #### ######## ############:

```
% getent passwd username
```

######## #### ###### ###### # ##### ###### /bin/bash ## ###### ######. # ######## # ######## # ######## ## ######## ## ######## #### #### /usr/local/bin/bash. # ######## ##### # ##### ## #### ######### ## ########## ######## #### #### ### # #### #### ########## ## ##### ########:

```
# ln -s /usr/local/bin/bash /bin/bash
```

############## ## ### /etc/shells ######## ######## #### ##### /usr/local/bin/bash # /bin/bash. # ######## ###### ##### ######## ##### ## ######## ### #### #### ### #####.

### 3.1.1. ###

###, ### ######### ########## ############### ########, # # ###### #### #### # ######## ######### # ######## ## #### ########. #### ##### ## ######## ### ######### #### ## ######## ####, ######## ### ######### ### ##### ## ######## ### ##########.

## ######## ### ##### # ######## ### ########## # /etc/pam.d/sshd, ## #### ###### #### ### (######### ## ######## ## ###### ########## ## /etc/ssh/sshd_config, #### ######### # ### ### ##### # ###).

#### #### # ### #### ############, ######## # #####

```
auth suficiente /usr/local/lib/pam_ldap.so no_warn
```

########## #### #### ##### ####### ## ####### # ##### ###### ######## ## ###### ######, ######### # ############# ##### ## ######### ## ############; #### ###.#(5)

### #### ############, #### #### ######### ########## ## ####### ## ## ######### ####. # ### ######### ### ####### ### #### ########### #, ## ### ############, ######### ## ### #### ######## # ######.

## #######, ### # ### ### ##### ######## ### *todo* ####### ## ######### ###### ## *todo* ########## #######. ### # ############ #####, #### # ### ## ####### ####### #### ####### ##### ## ### ####### # ### ####### ####. ##########, ####### ####### ######## ## ########## # ###### ## #######.

# ldap.conf ####### ### ######## pam_groupdn; #### ##### ### ## ####### # #### ####### ####### ### ###### ## ##### ############ ####. ### #######, ## #### ###

```
pam_groupdn cn=servername,ou=accessgroups,dc=example,dc=org
```

## ldap.conf, ####### ## ####### ##### ##### ####### ####### #####. ##########, ## ####### ###### # ##### #########.

## ####### ##### ##### ### ############# ## ## ## #### ######### memberUid # #### ######## #### ### # #### ######## ######## ## ######. ##### memberUid:someuser ### ##########; #### ###:

```
memberUid: uid=algum usuário, ou=pessoas, dc=exemplo, dc=org
```

#### #####, #### ######## ### # ########## ## ### ####### # ############, ### # ########## ####### # ############# ## ######, ########, #### ######### ## ### ####### ##### ## #### ######## ### ### account. #### #######, ### ### ###, ### *todo* ####### #### ####### ## #####, # ### ### # ################ # ### ########. #### ###### # ######## ## ######## ### ### ##### ## ####, #### #### ###### # ######## ignore_unknown_user. ##########, #### #### ####### # ##### ignore_authinfo_unavail #### ### #### ### ##### ######### ## ##### ## ############ ###### # ######## #### ####### ############.

### pam.d/sshd #### ###### ####### #####:

### ####### 5. ####### **pam.d/sshd**

```
auth        required      pam_nologin.so          no_warn
auth        sufficient    pam_opie.so             no_warn no_fake_prompts
auth        requisite     pam_opieaccess.so       no_warn allow_local
auth        sufficient    /usr/local/lib/pam_ldap.so      no_warn
auth        required      pam_unix.so             no_warn try_first_pass

account     required      pam_login_access.so
account     required      /usr/local/lib/pam_ldap.so      no_warn ignore_authinfo_unavail ignore_unknown_user
```

### ####

#### ####### ########### ##### ###### ############### #### pam.d/sshd, #### ## #### ## ###### ### ######## ###. ## ######## #### ### ####### ####### ##### ## #######. #### ##### #### ##############, ######## ## ###### ######## ## /etc/pam.d # ########## ## ## ######.

## 3.2. ###### ## ####### ## ####

### # # ####### ### ###### ######### #### #####. #####, ### #######, ## ## ####### # ## ########## ## ####### 1001, ## ########## ########## # ### #### # #### ## 1001, # ### #### ##### bob ## ted ## ######## ### #### # #### ## #######.

##### ### ###### ########## ##### # ####### ### ######## ## ####, ########## ##### ## ### #### ######## ## ###### ##########.

# #### ###/###_#### ### ####. ### ### # ##### ####### ## ############ #### ########/###_#### # ### #### ######## ## ###### ######### ##### ###### ## #########. ## ### #####, # ### ##### # ############ ###### # /etc/nsswitch.conf #### ########## # #########. ############ ######### ## ######### ######:

```
group: compat
passwd: compat
```

###

```
group: files ldap
passwd: files ldap
```

#### ######### ### #### ###### ##### ## ######## #### #### # #### #### ##### ## ########.

########! ##### #### #### ### ############ #### ## #############.

## 3.3. #########

############, # ###### ## ####### ## ### #### ### #######, # ####### ### ######### # ####### ## ###### ## ####### ### ######(1). ### ##### #####, # ####### ### ############### ##### ######## #### ########### ### ####### ### ##### #######. ## ####### ###### ######## ####. ####### ###, ## #### ######## ### ####### ###### ## ######### ## #####, ## ###### ######### ## ######### ### ##### #### #### ##### ######; #### ##### 4.3, ############## ## ######

## ####### 6. ###### ## ##### #### ######### ## ######

```
#!/bin/sh

stty -echo
read -p "Old Password: " oldp; echo
read -p "New Password: " np1; echo
read -p "Retype New Password: " np2; echo
stty echo

if [ "$np1" != "$np2" -]; then
  echo "Passwords do not match."
  exit 1
fi

ldappasswd -D uid="$USER",ou=people,dc=example,dc=org \
  -w "$oldp" \
  -a "$oldp" \
  -s "$np1"
```

### #######

#### ###### ############ ### ######## ########## ## #####, ###, # #### ##########, # ##### ########## ##### #### ### ######## #### ######. ## #### ##### #### #####, ###### #### ##### # ##### ## ###### security.bsd.see_other_uids:

```
# sysctl security.bsd.see_other_uids=0
```

### ######### #### ######## (# ############# #### ######) #### ### ##### ########## ## ######## #############, ## ### ##### ### ######### ###. # ######, ##### ## ### ########## #### ### #### ####### ###### ####. ### ## # ### ## ##### ## ####### # ## ###.

### ####### 7. ###### #### #### ####### ######

```
require 'ldap'
require 'base64'
require 'digest'
require 'password' # ruby-password

ldap_server = "ldap.example.org"
luser = "uid=#{ENV['USER']},ou=people,dc=example,dc=org"

# get the new password, check it, and create a salted hash from it
def get_password
  pwd1 = Password.get("New Password: ")
  pwd2 = Password.get("Retype New Password: ")

  raise if pwd1 != pwd2
  pwd1.check # check password strength

  salt = rand.to_s.gsub(/0\./, '')
  pass = pwd1.to_s
  hash = "{SSHA}"+Base64.encode64(Digest::SHA1.digest("#{pass}#{salt}")+salt).chomp!
  return hash
end

oldp = Password.get("Old Password: ")
newp = get_password

# We'll just replace it.  That we can bind proves that we either know
# the old password or are an admin.

replace = LDAP::Mod.new(LDAP::LDAP_MOD_REPLACE | LDAP::LDAP_MOD_BVALUES,
                        "userPassword",
                        [newp])

conn = LDAP::SSLConn.new(ldap_server, 389, true)
conn.set_option(LDAP::LDAP_OPT_PROTOCOL_VERSION, 3)
conn.bind(luser, oldp)
conn.modify(luser, [replace])
```

###### ## ### ### # ######## ## ##### ##### ## ###### ## ######### (# ##### # ####### ## #######, ### #######), #### # #### ##### # #### ######## ## ### ## ####### ###### sh.

## 4. ############ ## #########

##### ### #### ######## (# ############ ###### ########) ##### ############ ## ### ######## ####, #### ######## ####### ### ######### #### ##### ### ### ###### /etc/master.passwd ##### ## ## ######## #######, # ############ #### #####, ### ### ### ## ######## #### ########## ######### ##### ## ######## ## #######.

#########, #### ##### ### # #########. #### #### ####### ############# ### ############ # ############# #### #########.

## 4.1. ######### ######### ####### #######

###### ######### ## #### ##### ### ####### #######. ## ####### ######## #### #######, ### #######, ## ####### ####### ####### ### ######## uidNumber #### 0 # ##### ###### ## root!

#### #######, # ######## userPassword ### #### ### ####### ### #####. ### ######, ######## ###### ### ##### ## ######## ## ######## #### #### ### #### ########. #### ########### ####, ####### # ######## ## slapd.conf:

### 8. ####### ######

```
access to dn.subtree="ou=people,dc=example,dc=org"
  attrs=userPassword
  by self write
  by anonymous auth
  by * none

access to *
  by self write
  by * read
```

#### ### ######### # ####### ## ######## userPassword, ######## ##### ####### ### ## ######## ####### #### ######## ######.

#### #####, #### ######## ####### ### ## ######## ####### ###### ## #### ######## #########. ### ######, ## ######## ##### ####### ######## ######## (###### ####### ### ## ######## ######## #### ##### ##########), #### uidNumber. #### ###### #### ######, ######### # ##### ####

### 9. ######### ####### #######

```
access to dn.subtree="ou=people,dc=example,dc=org"
  attrs=userPassword
  by self write
  by anonymous auth
  by * none

access to attrs=homeDirectory,uidNumber,gidNumber
  by * read

access to *
  by self write
  by * read
```

#### ######## ### ## ######## ## ######### #### ###### ########.

## 4.2. ######### ## ##### **root**

##########, # #####  root  ## # ##### ## ############# #### # ####### #### #### ######## ## ####### ## ############. # ######## ####### ####, ### #######, # ########, ### #### ###### ######### ## # slapd.conf ####### #############. #### ### ###### #### #### ###### #### ## ############### ## ####, # ##### ####### ### #####  root .

###### ##### # ####### ###### ### ########## ######### # ###### ########## ### ##### root. ### #######, ## ######## ### ##### ######### ## ####### ###### ## ####### ### ########### # ## #####, ### ### ##### ####### # ############ ##### #####. #### ######## ## ######### ######## # ####### ## ####### ## ### ##### #######.

### 4.2.1. ####### ## ##### ## ##############

####### ### #### ###### ### ### ############ ## ## ##### ####### ## ########## ######## ### ########, ### ### ###### ### ##### #### ###### ######### ## ####### ########. # ####### ## ##### #### # ######### ## ##### #### ##### ###############:

**####### 10. ####### ## ##### ## ##############**

```
dn: cn=homemanagement,dc=example,dc=org
objectClass: top
objectClass: posixGroup
cn: homemanagement
gidNumber: 121 # required for posixGroup
memberUid: uid=tuser,ou=people,dc=example,dc=org
memberUid: uid=user2,ou=people,dc=example,dc=org
```

# ##### #### ## ######### ## ########## ## slapd.conf:

**####### 11. #### #### ## ##### ## ############ ## ######### #######**

```
access to dn.subtree="ou=people,dc=example,dc=org"
  attr=homeDirectory
  by dn="cn=homemanagement,dc=example,dc=org"
  dnattr=memberUid write
```

##### tuser # user2 ##### ####### ## ########## #### ## ###### ########.

##### #######, ##### ## ########### ## ##### ############## # ###### ######## ### ### # #### ##### ## ###### ########. # ##### # ### ## ##### ####### ##### ## ####### ##### # ##### ## ### ##### root, ### #### ##### ### #### ### #### #### ### #### ##### ## #######. # ##### root ######## ############# # #### ### ########.

### 4.3. ############## ## #####

### ######, ######## ########## # ##### ## ######## userPassword ######## ### ######## ######### ###### #####: #### #####. ## ####### ### #####, ### # ########## ## #### 64, # ### ####### ######## ########## #### ####### ### ## ############## ####### ####### ### #####, ### ##### #####.

# ### ### #####, #####, ######### ###### ## ## ####### #### ######, #### # #### (###### ###). #### # ##### ### ######## ######## ### #### ### #### ####### ## ###### ### ########.

## #. ###### #####

####### ###### ###### ######### ### ##### ### #####, ############## ## #### ##### ###### ######## # ### ###### ########## #### ###########.

# ########/###_######### # ## ###### ### ### ###### # ############; ### ########## # ##### ########## ######## #### ######## ### ### ## #######. ## #### ##### ####### ## ########## ######## # ######## ## ########, # ##### #### ##### #### #### # ########## ########## ########## ## ### ######## #### ######### #######.

# ########/### # ## ########## ## #### ##(8) ### #### ### ##### #### ######### ######## ## ######### ####. #### #### ######## ########## ## ########## ## ####### ## ##### ####. ### #### ######### ##### # ### (### # ########## -x) ###### # ### (##########).

# ########/###### # ## ##### ########## #### ###### ####### #### ## ### ####### ########## # ####. # ######### (## ######## ## #########) # ########## ## ###### ######### #### ######## ## ######## EDITOR. #### ######## # ######## ## ########## ## ###### ###### ## ######### ### # ########## ## ######## ### ########## ##############.

# ########/################## ### # ########## ## ######## ## ######## #### #### ######### ## ###### ###. #### # ############ ### ## #### ##### ###### ########## # ### ###### ###### #### ###### ######## ## ##### ####.

## #. ############ ## ####### #### ####

## #### ####### ########## #### ## #### ########## ####, ############ ### ######## #### ############ ############, ## ### #### ####### ######### ### ########## #### ######### ### #### ##########. ###### #### #### ########, ### # ### ####### ###### ##### ### ####### ########## ## ########## # ####### ## ############ ## #### ########## ### ####.

## ###### #### ### ############ #### #### ###, ### ##### ##### ######### ## ######## # ### #### ########## # #### ########## ##### ### ########## ## #######(1) # ########## ######.

#### ##### ### ########## ## ############, ############ ########## ## ## ########## # ##### #############. ## ###### #### #### ######### ###

### ####### #.1. ####### ## ###########

```
% openssl genrsa -out root.key 1024
% openssl req -new -key root.key -out root.csr
% openssl x509 -req -days 1024 -in root.csr -signkey root.key -out root.crt
```

##### ##### ### ##### # ########## ## ## ####. #### ############ ######## ############ # ##### # ########## ## ## ##### ######; ######## ###### ### ###### # ### #### ## ###### ### ## ### #### ########## ####.

## #######, ###### ## #### ######### ###### #####, #### ### ##### ldap-server-one.key # # ########## ## ########## ## ########## ldap-server-one.csr. ###### ## ######## # ###### ## ########## ### root.key, #### ###### #### # ldap-server-one.* ### ########## ####.

### ## ####### ## #### # #### ## ####### ########## ########## #### # ######## ####### ##### ## ##### # ########## ## ########## ## ##########; #### #########, ## ######## ########## ### ####### ### #### # ###### ### ##### ########## ############.

#### ####### # #####, ### -CA # -CAkey ## ### ## -signkey:

### ####### #.2. ######### #### ### ########## ## ############

```
%  openssl x509 -req -dias 1024 \
-em servidor ldap-one.csr -CA root.crt -CAkey root.key \
-out ldap-server-one.crt
```

# ####### ########## #### # ########### ### #### #### #### ## #### ########## ####.

##########, #### ## ######## ######### ## ##### ## #### ##########, ######### root.crt (# *certificado* , ### # #####!) #### #### #######, # ############## ## ######### TLSCACertificateFile ## ldap.conf.