System Administration - CC4069 - Project Report

Authors

```
 Joaquim Oliveira
up201908075@edu.fc.up.pt
Department of Computer Science
University of Porto

Luís Leite
up201906750@edu.fc.up.pt
Department of Computer Science
University of Porto
```

Abstract

In this paper we describe the necessary steps needed to implement an LDAP-based system directory for authentication and NFS for user directory exportation. If all steps are correctly followed the result should be something similar to the image shown below.

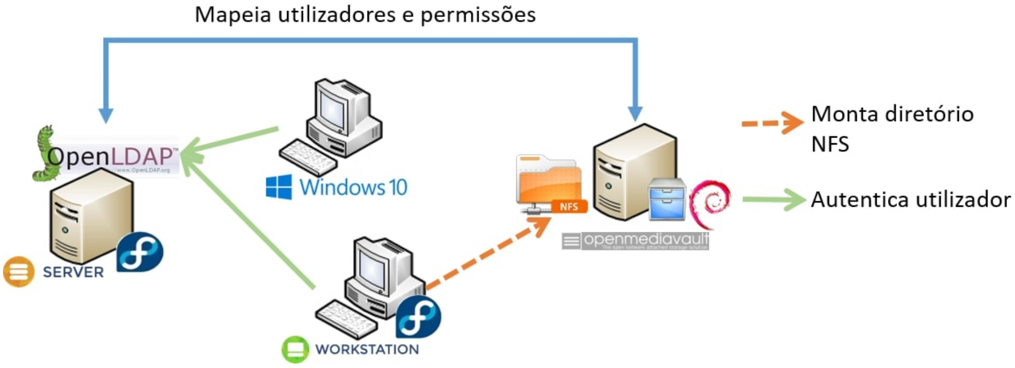

Table of Contents

Virtual machines specs

Fedora - Workstation

```
 Type: e2-micro
Location: europe-west1-d
OS: Fedora-36
```

Server - Openmediavault

```
 Type: e2-micro
Location: europe-west1-b
OS: Debian-11
```

Server - Openldap

```
 Type: e2-micro
Location: europe-west1-b
OS: CentOS-7
```

SSH commands

Generate ssh key:

```
ssh-keygen -b 2048 -t rsa
```

Connect to any VM using:

```
ssh -i private-key user@external-ip
```

Default location of ssh key: */home/user/.ssh*

Installation commands

## Workstation - Fedora

IMPORTANT NOTE: - To turn on the virtual display device, select the **Enable display device** checkbox from the **Machine configuration > Display device** settings

---

Installing desktop environment

```
 dnf group install "LXDE Desktop"

systemctl set-default graphical.target
```

## Creating new user for the remote desktop

```
 useradd admin-gui

passwd admin-gui

usermod -a -G google-sudoers admin-gui
usermod -a -G adm admin-gui
usermod -a -G video admin-gui
usermod -aG wheel admin-gui
```

Installing Xrdp Server (Remote Desktop)

```
 dnf -y install xrdp

firewall-cmd --add-port=3389/tcp
firewall-cmd --runtime-to-permanent

systemctl enable --now xrdp
```

Xrdp client on linux: Remmina (optional package required: *freerdp*)

OpenLDAP access

```
 dnf -y install openldap-clients sssd sssd-ldap oddjob-mkhomedir

vi /etc/openldap/ldap.conf
    TLS_REQCERT     allow

ldapsearch  -x -L -W -H ldaps://ip_servidor/ -D "cn=Manager,dc=ads,dc=dcc" -b "dc=ads,dc=dcc"

firewall-cmd --add-service=ldap --permanent

firewall-cmd --reload
```

Setup autentication

```
 # in root home dir - using root shell
authselect --trace select --force sssd  with-mkhomedir > change-authselect-with-sssd.log  2>&1

nano /etc/sssd/sssd.conf
    [domain/default]
    id_provider = ldap
    auth_provider = ldap
    chpass_provider = ldap
    ldap_uri = ldaps://ip_servidor/
    ldap_search_base = dc=ads,dc=dcc
    ldap_id_use_start_tls = True
    ldap_tls_cacertdir = /etc/openldap/certs
    cache_credentials = True
    ldap_tls_reqcert = allow

    [sssd]
    services = nss, pam
    domains = default

    [nss]
    homedir_substring = /home

chmod 600 /etc/sssd/sssd.conf

systemctl restart sssd
systemctl enable oddjobd
systemctl start oddjobd

# change adsevil password
ldappasswd  -S -x -W -H ldaps://ip_servidor -D "uid=adsDevil,ou=Developers,dc=ads,dc=dcc" "uid=adsdevi

# create dir of authenticated user
su - adsdevil
```

Setup auto mount

```
 yum install autofs
```

To mount a NFS share for file_server on /srv/shared_dir at location /mnt/foo, add a new configuration, e.g. file_server.autofs:

```
 vi /etc/autofs/auto.master.d/file_server.autofs
    /mnt   /etc/autofs/auto.file_server --timeout 60

vi /etc/autofs/auto.file_server
    foo  -rw,soft,rsize=8192,wsize=8192 file_server:/srv/shared_dir
```

## Server - Openmediavault

Install basic software

```
 apt-get install --yes gnupg
apt-get install --yes wget

wget -O "/etc/apt/trusted.gpg.d/openmediavault-archive-keyring.asc" https://packages.openmediavault.or

apt-key add "/etc/apt/trusted.gpg.d/openmediavault-archive-keyring.asc"

cat <<EOF >> /etc/apt/sources.list.d/openmediavault.list deb https://packages.openmediavault.org/publi

export LANG=C.UTF-8
export DEBIAN_FRONTEND=noninteractive
export APT_LISTCHANGES_FRONTEND=none

apt-get update

apt-get --yes --auto-remove --show-upgraded \
--allow-downgrades --allow-change-held-packages \
--no-install-recommends \
--option DPkg::Options::="--force-confdef" \
--option DPkg::Options::="--force-confold" \
install openmediavault-keyring openmediavault

omv-confdbadm populate
```

RAID setup

```
 # Create 4 disk with 1GB
for i in disk{1..4}-1GB; do dd if=/dev/zero of=$i bs=1024 count=1048576; done

# loop to create and associate devices to the files
for i in disk{1..4}-1GB; do sudo losetup --find --show $i; done

# Create 2 disk with 500M
for i in disk{5..6}-500M; do dd if=/dev/zero of=$i bs=1024 count=524288; done

# loop to create and associate devices to the files
for i in disk{5..6}-500M; do sudo losetup --find --show $i; done
```

IMPORTANT: Create systemd script to mapp loop devices

Restore RAID after reboot

```
 for i in disk{1..4}-1GB; do sudo losetup --find --show $i; done

for i in disk{5..6}-500M; do sudo losetup --find --show $i; done
```

Creating 1 disk with 10G and partitions

```
# partition disk
fdisk

# create raid 10
sudo mdadm --create --verbose /dev/md0 --level=10 --raid-devices=4 /dev/sda5 /dev/sda6 /dev/sda7 /dev/

# Create PV
pvcreate /dev/sda9
pvcreate /dev/sda10
```

Create LDAP user

```
# create users from webui

# change UID and GID as LDAP server
vipw # user
vigr # group
```

Automount home directory

```
vi /etc/auto.home
    * -rw,nfs4 NFS-IP:/radi-sh/&

vi /etc/auto.master
    /home /etc/auto.home
```

## Server - Openldap

OpenLDAP : Install

```
yum -y install openldap-servers openldap-clients nano

cp /usr/share/openldap-servers/DB_CONFIG.example /var/lib/ldap/DB_CONFIG

chown ldap. /var/lib/ldap/DB_CONFIG

systemctl start slapd
systemctl enable slapd

nano /etc/hosts
    EXTERNAL_IP server.ads.dcc server
    EXTERNAL_IP client.ads.dcc client

# create ssha of password for ldap
slappasswd

vi chrootpw.ldif
    # specify the password generated above for "olcRootPW" section
    dn: olcDatabase={0}config,cn=config
    changetype: modify
    add: olcRootPW
    olcRootPW: {SSHA}LVtjdrLgXyb3PrZNOxWe1Q8zQk+zIvtz
    # pass: ads2020

ldapadd -Y EXTERNAL -H ldapi:/// -f chrootpw.ldif
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/cosine.ldif
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/nis.ldif
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/inetorgperson.ldif

vi chdomain.ldif
    # replace to your own domain name for "dc=***,dc=***" section
    # specify the password generated above for "olcRootPW" section

    dn: olcDatabase={1}monitor,cn=config
    changetype: modify
    replace: olcAccess
    olcAccess: {0}to * by dn.base="gidNumber=0+uidNumber=0 cn=peercred,cn=external,cn=auth" read by dn

    dn: olcDatabase={2}hdb,cn=config
    changetype: modify
    replace: olcSuffix
    olcSuffix: dc=ads,dc=dcc

    dn: olcDatabase={2}hdb,cn=config
    changetype: modify
    replace: olcRootDN
    olcRootDN: cn=Manager,dc=ads,dc=dcc

    dn: olcDatabase={2}hdb,cn=config
    changetype: modify
    add: olcRootPW
    olcRootPW: {SSHA}LVtjdrLgXyb3PrZNOxWe1Q8zQk+zIvtz

    dn: olcDatabase={2}hdb,cn=config
    changetype: modify
    add: olcAccess
    olcAccess: {0}to attrs=userPassword,shadowLastChange by dn="cn=Manager,dc=ads,dc=dcc" write by anon
    olcAccess: {1}to dn.base="" by * read
    olcAccess: {2}to * by dn="cn=Manager,dc=ads,dc=dcc" write by * read

ldapmodify -Y EXTERNAL -H ldapi:/// -f chdomain.ldif

vi basedomain.ldif
    # replace to your own domain name for "dc=***,dc=***" section

    dn: dc=ads,dc=dcc
    objectClass: top
    objectClass: dcObject
    objectclass: organization
    o: Server World
    dc: ads

    dn: cn=Manager,dc=ads,dc=dcc
    objectClass: organizationalRole
    cn: Manager
    description: Directory Manager

    dn: ou=People,dc=ads,dc=dcc
    objectClass: organizationalUnit
    ou: People

    dn: ou=Group,dc=ads,dc=dcc
    objectClass: organizationalUnit
    ou: Group

ldapadd -x -D cn=Manager,dc=ads,dc=dcc -W -f basedomain.ldif

firewall-cmd --add-service=ldap --permanent

firewall-cmd --reload
```

External link: https://www.server-world.info/en/note?os=CentOS_7&p=openldap&f=1

Add user and group

```
 vi adduser-adsdevil.ldif
    dn: uid=adsdevil,ou=People,dc=ads,dc=dcc
    uid: adsdevil
    cn: adsdevil
    objectClass: account
    objectClass: posixAccount
    objectClass: top
    objectClass: shadowAccount
    shadowLastChange: 17838
    shadowMax: 99999
    shadowWarning: 7
    loginShell: /bin/bash
    uidNumber: 2002
    gidNumber: 2002
    homeDirectory: /rhome/adsdevil

ldapadd -x -D cn=Manager,dc=ads,dc=dcc -W -f adduser-adsdevil.ldif

# change user password
ldappasswd  -S -x -W -D "cn=Manager,dc=ads,dc=dcc" "uid=adsdevil,ou=People,dc=ads,dc=dcc"



vi adduser-group.ldif
    dn: cn=adsdevil,ou=People,dc=ads,dc=dcc
    gidNumber: 5001
    objectClass: top
    objectClass: posixGroup
    cn: adsdevil

ldapadd -x -D cn=Manager,dc=ads,dc=dcc -W -f adduser-group.ldif
```

Delete user from DB:

```
 vi delete-user.ldif
    dn: uid=aauser,ou=Developers,dc=ads,dc=dcc
    changetype: delete

ldapmodify -Z -x -W -D "cn=Manager,dc=ads,dc=dcc" -f delete-user.ldif
```

Opensl setup

```
sudo yum install openssl

cd /etc/openldap/certs

openssl req -new -newkey rsa:4096 -x509 -sha256 -days 365 -nodes -out server.crt -keyout server.key

sudo chown ldap. server.crt
sudo chown ldap. server.key

sudo ln /etc/pki/tls/certs/ca-bundle.crt ca-bundle.crt

vi openssl.ldif
    dn: cn=config
    changetype: modify
    add: olcTLSCACertificateFile
    olcTLSCACertificateFile: /etc/openldap/certs/ca-bundle.crt

    add: olcTLSCertificateFile
    olcTLSCertificateFile: /etc/openldap/certs/server.crt

    add: olcTLSCertificateKeyFile
    olcTLSCertificateKeyFile: /etc/openldap/certs/server.key

ldapmodify -Y EXTERNAL -H ldapi:/// -f openssl.ldif

vi /etc/sysconfig/slapd
    # line 9: add
    SLAPD_URLS="ldapi:/// ldap:/// ldaps:///"

systemctl restart slapd
```

phpLDAPadmin : Install / optional

```
yum --enablerepo=epel -y install phpldapadmin

vi /etc/phpldapadmin/config.php
    # line 397: uncomment, line 398: comment out

    $servers->setValue('login','attr','dn');
    //
    $servers->setValue('login','attr','uid');

vi /etc/httpd/conf.d/phpldapadmin.conf
    # line 12: add access permission
    Require all granted

systemctl restart httpd
```

External link: https://www.server-world.info/en/note?os=CentOS_7&p=openldap&f=7

Dasboard

Openmediavault : (only available after Installation commands / Server - Openmediavault)

```
http://external-ip-of-openmediavault-vm/#/dashboard
```

Credentials:

```
 user: admin
password: openmediavault
```

Openldap : (only available after Installation commands / Server - Openldap)

```
http://external-ip-of-openldap/ldapadmin/
```

Credentials:

```
 user: cn=Manager,dc=ads,dc=dcc
password: ads2020
```