Fase 4 - Activitat 7: Directori. Servei de directori. LDAP. Servei NFS. Domini amb NFS+LDAP. VirtualBox amb NAT i Internal Network

1- Identificació del grup i activitat:

Curs: ASIX2
Projecte: PJ6 Administració de xarxes i sistemes operatius
Fase: 4
Activitat: 7
Grup/Individual: Individual

2- Objectius de l'activitat

Els objectius d'aquesta activitat són:

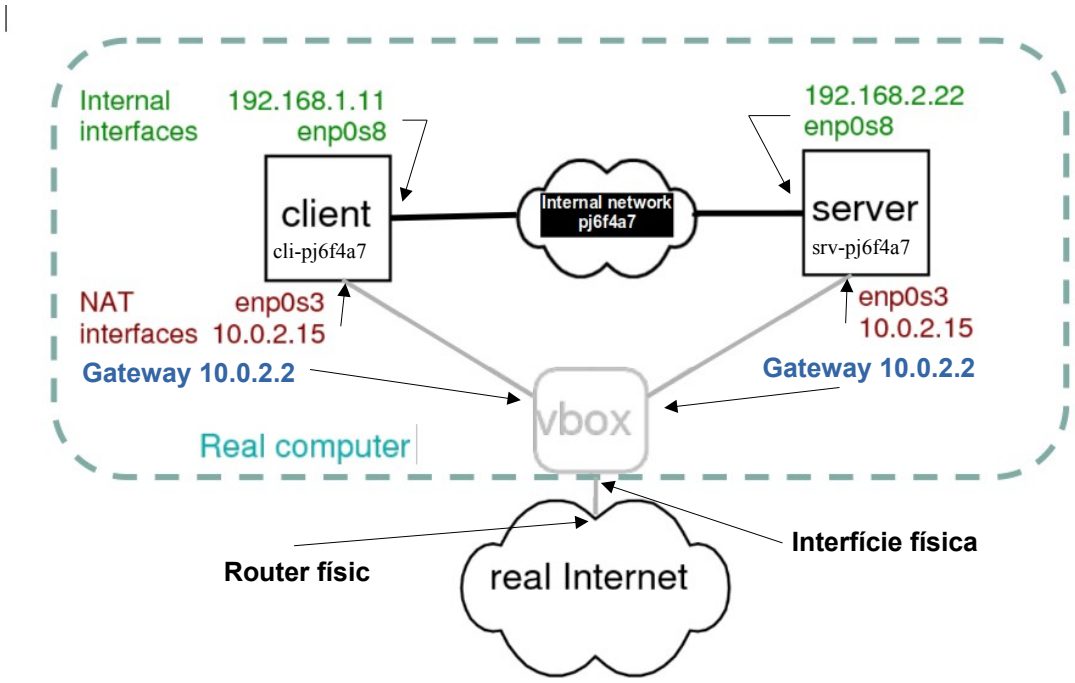
- Connexió d'equips utilitzant **VirtualBox + NAT + Internal Network** per muntar una xarxa de màquines virtuals interconnectades per mitjà de la xarxa interna i connectades a l'exterior per mitjà de NAT. Això ens permet crear una xarxa interna i aïllada a on els serveis que es posen en marxa només són visibles pels equips directament connectats i no interfereixen amb l'exterior i, al mateix temps, tots els equips tenen connexió a internet a través de NAT i poden descarregar programari fàcilment. Aquest esquema de xarxa ens obliga a crear i configurar dues 2 interfícies de xarxa dins de cadascuna de les màquines virtuals.
- Aprenentatge sobre:
  - Què és un directori i quina és la seva utilitat?
  - Exemples de directoris.
  - Com s'organitza un directori?
  - Que és un servei i un client de directori?
  - Què és el protocol LDAP?
  - Quines implementacions existeixen de serveis i clients de directori utilitzant LDAP?
  - Com es configura i administra un servei de directori?.
  - Com es configura un client de directori?
  - Com s'estableix una connexió a un servidor de directori des d'un client?
  - Quines operacions bàsqiues es poden realitzar dins d'un directori?
- Aprenentatge sobre:
  - Sobre el servei NFS i quina és la seva utilitat
  - Quines implementacions existeixen de serveis i clients NFS?
  - Com es configura i administra un servei NFS?.
  - Com es configura un client NFS?
  - Com s'estableix una connexió a un servidor NFS des d'un client?
  - Quines operacions bàsqiues es poden realitzar amb NFS?
- Creació d'un domini utilitzant:
  - Servei de directori
  - Servei de compartició de carpetes i fitxers en xarxa
  - Autenticació i autorització d'usuaris utiltzant el servei de directoris
  - Accés a la carpeta personal d'un usuari autenticat a través de NFS
  - Instal·lació i configuració de programari necessari per poder autenticar i permetre l'accés a la seva zona personal de qualsevol usuari des de qualsevol equip client.
- Configuració DHCP bàsica per poder assignar IPs als equips clients.
- Configuració DNS bàsica per poder resoldre el nom del servidor LDAP i NFS
- Documentació:
  - Introducció ràpida a LDAP a ldap1.pdf.
  - Conceptes de directori, servei de directori, protocol LDAP, clients, organització, configuració, administració, connexions i operacións bàsiques a ldap2.pdf.
  - Documentació de l'IOC a ldap3.pdf.
  - Introducció ràpida al servei NFS a nfs1.pdf.

3- Connexió d'equips utilitzant VirtualBox + NAT + Internal Network

a) Volem crear una xarxa de 2 màquines virtuals que estiguin:

- interconnectades per mitjà de la xarxa interna
- Connectades a l'exterior per mitjà de NAT.

L'esquema d'aquesta xarxa seria aquest:



Això ens permet crear una xarxa interna i aïllada de l'exterior a on els serveis:

- LDAP
- NFS
- DNS
- DHCP

només són visibles pels equips directament connectats i no interfereixen amb l'exterior i, al mateix temps, tots els equips tenen connexió a internet a través de NAT i poden descarregar programari fàcilment.

Aquest esquema de xarxa ens obliga a crear i configurar dues 2 interfícies de xarxa dins de cadascuna de les màquines virtuals.

b) En el següent *videoclip* podeu veure com es pot fer aquesta configuració i de quina manera s'han solucionat algunes dificultats que s'han trobat durant el procés de creació i configuració de les 2 interfícies de xarxa a l'equip client i l'equip servidor.

c) Si tot funciona correctament, els 2 equips han de poder:

- Fer pings entre ells a través de les interfícies **enp0s8** configurades amb les adreces IP **192.168.1.2** en el servidor **srv-pj6f4a7**, i **192.168.1.100** en el client **cli-pj6f4f7**.
- Fer pings a qualsevol adreça d'internet a través de les interfícies **enp0s3** configurades via **NAT** de **VirtualBox**.

4- Instal·lació de programari en el servidor i client

4.1- Instal·lació de programari en el servidor

a) Instal·lació del servidor LDAP

- Abans de començar executa:

```
sudo aptitude update
```

- Instal·la el servidor LDAP i les utilitat per gestionar-lo executant:

```
sudo aptitude install slapd ldap-utils
```

  NOTA: La contrasenya proposada per l'administrador d'OpenLDAP serà **fjeclot**.

- Executa l'assistent de configuració del servidor LDAP:

```
sudo dpkg-reconfigure -plow slapd
```

- Configura el servidor amb els següents paràmetres:
  - Voleu ometre la configuració del servidor openLDAP?: **No**
  - Nom del domini DNS: **clotfje.net**
  - Nom de l'organització: **clotfje.net**
  - Contrasenya de l'administrador: **fjeclot**
  - Tipus de Base de Dades (si ho demana): **MDB**
  - Eliminació de la base de dades en purgar slapd: **Sí**
  - Moure la base de dades anterior?: **Sí**

- Comprova amb l'ordre

  ```
  sudo slapcat
  ```

  que:
  - El nom distintiu (DN) complet del domini amb el qual treballa la base de dades LDAP és aquest: **dn: dc=clotfje,dc=net**
  - EL DN de l'administrador del servidor LDAP és aquest: **cn=admin,dc=clotfje,dc=net**.

b) Instal·lació de l'eina de gestió del servidor LDAP Apache Directory Studio

- Instal·la Java Development Kit versió 25. Executa: **sudo aptitude install openjdk-25-jdk**

- Instal·la Apache Directory Studio (amb les instruccions que hi ha a la web de descarrega) i realitza una connexió amb LDAP. Crea un enllaç a l'escriptori de l'aplicació i afegeix la icona **icon.pxm** a l'enllaç.

- Tanca la pàgina de benvinguda i a continuació configura **Apache Directory Studio** per establir connexió al servidor LDAP utilitzant els següents paràmetres de configuració:
  - Connection name: **pj6f4a7**
  - Hostname: **localhost**
  - Port: **389**
  - Encryption method: **No encryption**
  - Authentication method: **Simple Authentication**
  - Bind DN or user: **cn=admin,dc=clotfje,dc=net**
  - Bind password: **fjeclot**
  - Altres paràmetres: **opcions per defecte**

- Comprova que:
  - S'estableix una connexió
  - Pots veure el domini dc=clotfje,dc=net
  - Pots tancar la connexió un cop establerta
  - Pots tornar-la a establir la connexió tancada.

c) Instal·lació del servidor NFS

- Abans de començar executa:

```
sudo aptitude update
```

- El sistema Debian GNU/Linux utilitza **NFS** per poder exportar en el servidor i muntar en la part client sistemes d'arxius per mitjà de la xarxa. Per poder exportar arxius exportats per mitjà de la xarxa cal instal·lar dins de l'equip servidor **nfs-kernel-server**. Per tant, cal executar l'ordre:

```
sudo aptitude install nfs-kernel-server
```

- Comprova que el servei està en marxa i habilitat. Executa:

```
systemctl status  nfs-kernel-server
```

4.2- Instal·lació de programari en el client

a) Instal·lació i configuració del programari dins de l'equip client per autenticar-se en la xarxa per mitjà del servei LDAP

- Abans de començar executa:

```
sudo aptitude update
```

- El sistema Debian GNU/Linux:
  - Pot treballar amb usuaris locals o del domini. Els usuaris del domini es troben definits al servidor **LDAP** i els locals es troben dins **/etc/passwd**.
  - Utilitza el programari **NSS (Name Service Switch)** per saber en quin ordre ha de buscar un usuari per validar-lo d'acord amb la configuració que es troba a l'arxiu **/etc/nsswitch.conf**. Normalment primer intenta trobar l'usuari localment dins del fitxer **/etc/password** i si no el troba, després busca l'usuari dins de la base de dades **LDAP**.
  - Per poder buscar usuaris dins la base de dades LDAP cap instal·lar el paquet de programa **libnss-ldap**. Per tant, cal executar:

```
sudo aptitude install libnss-ldapd
```

  - Durant el procés d'instal·lació de **libnss-ldap** també es demana la seva configuració. Si volem utilitzar-lo per fer que *el client pugui validar usuaris utilitzant la informació dins de la base de dades LDAP*, la configuració ha de de ser la següent:
    - Multiple URIs can be separated by spaces: **Ok**
    - LDAP server URI: **ldap://192.168.1.2**
    - Distinguished name of the search base: **dc=clotfje,dc=net**
    - Respon **Ok** a la següent pantalla amb un missatge informatiu
    - Name services to configure → **passwd**, **group**, **shadow**

- Si calgués **reconfigurar libnss-ldap**, només cal executar:

```
sudo dpkg-reconfigure libnss-ldapd
```

- El sistema Debian GNU/Linux:
  - Delega la feina d'autenticació d'usuaris en un programari de nom PAM (Pluggable Authentication Module). Per poder autenticar usuaris utilitzant la informació dins la base de dades LDAP cap instal·lar el paquet de programa **libpam-ldap**. Per tant, cal executar:

    ```
    sudo aptitude install libpam-ldapd
    ```

  - Els arxius de configuració de **PAM** es troben a **/etc/pam.d**.

  - PAM permet autenticar usuaris utilitzant LDAP i a més a més, permet crear el directori home d'un usuari que s'identifica per primera vegada en el domini. Per poder activar aquesta opció, cal:
    - Obrir com a **root** el fitxer **/etc/pam.d/common-session**
    - Afegeix al final del fitxer la següent línia de configuració:
      session required pam_mkhomedir.so skel=/etc/skel umask=0022

  - Si calgués **reconfigurar libnss-ldap**, només cal executar:

    ```
    sudo dpkg-reconfigure libpam-ldapd
    ```

- El servei **nscd** controla la memòria cau de les autenticacions realitzades en domini. Aquesta memòria cau permet optimitzar el temps d'accés al domini posteriorment. Per instal·lar-lo cal executar l'ordre:

  ```
  sudo aptitude install nscd
  ```

  A vegades queden dades a la cau que no estan actualitzades. Després de configurar **NSS** i **PAM** per treballar amb **LDAP**, és una bona idea de reiniciar el servei **nscd** executant:

  ```
  systemctl restart nscd.
  ```

  Així estem segurs que la memòria cau està neta i no tindrem problemes amb dades obsoletes.

- Finalment, sempre és útil tenir les ordres per treballar amb LDAP des del terminal. Per instal·lar-les, executa:

  ```
  sudo aptitude install ldap-utils
  ```

b) Instal·lació del programari dins de l'equip client per muntar sistemes d'arxius exportats via NFS

- Abans de començar executa:

  ```
  sudo aptitude update
  ```

- El sistema Debian GNU/Linux utilitza **NFS** per poder exportar en el servidor i muntar en la part client sistemes d'arxius per mitjà de la xarxa. Per poder muntar sistemes d'arxius exportats per mitjà de la xarxa dins de l'equip client cal instal·lar el programari **nfs-client**. Per tant, cal executar l'ordre:

  ```
  sudo aptitude install nfs-client
  ```

5- Administrant el usuaris del domini amb Apache Directory Studio

Dins d'aquest apartat anem a crear els usuaris i grups del domini dins del servidor LDAP de manera que des de qualsevol equip client ens puguem autenticar. Per fer això, crearem les següents entrades dins de LDAP:

5.1- Creació de les entrades dins de la base de dades LDAP

a) Des d'**Apache Directory Studio**, crea una **unitat organitzativa** de nom **ouGrups**:
- Afegeix una nova entrada dins de **dc=clotfje,dc=net** → Fes clic amb el botó de la dreta sobre **dc=clotfje,dc=net** i selecciona: **New --> New Entry --> Create entry from scratch**
- Afegeix els **objectClass** de tipus **top** i **organitzationalUnit**
- Afegeix un **RDN** de tipus **ou** (unitat organitzativa) i de valor **ouGrups**, o sigui, **ou=ouGrups**. Això voldrà dir que el **nom distintiu (DN**) de la nova entrada serà el següent: **ou=ouGrups,dc=clotfje,dc=net**

b) Des d'**Apache Directory Studio**, crea una **unitat organitzativa** de nom **ouUsuaris**:
- Afegeix una nova entrada dins de **dc=clotfje,dc=net**
- Afegeix els **objectClass** de tipus **top** i **organitzationalUnit**
- Afegeix un **RDN** de tipus **ou** (unitat organitzativa) i de valor **ouUsuaris**, o sigui, **ou=ouUsuaris**. Això voldrà dir que el nom distintiu (DN) de la nova entrada serà el següent: **ou=ouUsuaris,dc=clotfje,dc=net**

c) Des d'**Apache Directory Studio**, crea una **unitat organitzativa** de nom **ouEquips**:
- Afegeix una nova entrada dins de **dc=clotfje,dc=net**
- Afegeix els **objectClass** de tipus **top** i **organitzationalUnit**
- Afegeix un **RDN** de tipus **ou** (unitat organitzativa) i de valor **ouEquips**, o sigui, **ou=ouEquips**. Això voldrà dir que el **nom distintiu (DN**) de la nova entrada serà el següent: **ou=ouEquips,dc=clotfje,dc=net**

d) Des d'**Apache Directory Studio** , crea un **grup** d'usuaris de nom **gUsuaris**:
- Afegeix una nova entrada dins d'**ouGrups**.
- Afegeix els **objectClass**: **top** i **posixGroup**
- Afegeix un **RDN** de tipus **cn** igual a **gUsuaris**. Per tant, el nom distintiu de la nova entrada serà: **cn=gUsuaris,ou=ouGrups,dc=clotfje,dc=net**
- Quan et demanin el **gidNumber** (per posar un GID al grup) escriu el valor **1001**, o sigui, **gidNumber=1001**.

e) Des d'**Apache Directory Studio** , crea un **grup** d'usuaris de nom **gAdmins**:
- Afegeix una nova entrada dins d'**ouGrups** .
- Afegeix els **objectClass**: **top** i **posixGroup**
- Afegeix un **RDN** de tipus **cn** igual a **gAdmins**. Per tant, el nom distintiu de la nova entrada serà: **cn=gAdmins,ou=ouGrups,dc=clotfje,dc=net**
- Quan et demanin el **gidNumber** (per posar un GID al grup) escriu el valor **1002**, o sigui, **gidNumber=1002**.

f) Des d'**Apache Directory Studio**,crea un **usuari** de nom **jgim:**
- Crea una nova entrada dins d'**ouUsuaris**.
- Afegeix els **objectClass**: **top**, **posixAccount**, **shadowAccount**, **person**.
- Afegeix un **RDN** de tipus **uid** igual a **jgim**. Per tant, el nom distintiu de la nova entrada serà: **uid=jgim,ou=ouUsuaris,dc=clotfje,dc=net**.
- Quant et demani:
  - Common name → escriu **cn: jordi**
  - Número de grup per defecte → **gidNumber: 2000**
  - Directori de l'usuari --> **homeDirectory: /home/jgim**
  - Surname → **sn: gimenez**
  - Número d'usuari → **uidNumber: 3000**
  - Afegeix l'atribut Shell de l'usuari → **loginShell: /bin/bash**
  - Afegeix l'atribut Contrasenya de l'usuari → **userPassword:: FjeClot25@**

g) Des d'**Apache Directory Studio**,crea un **usuari** de nom **alop:**

- Crea una nova entrada dins d'**ouUsuaris**.
- Afegeix els **objectClass**: **top**, **posixAccount**, **shadowAccount**, **person**.
- Afegeix un **RDN** de tipus **uid** igual a **alop**. Per tant, el nom distintiu de la nova entrada serà: **uid=alop,ou=ouUsuaris,dc=clotfje,dc=net**.
- Quant et demani:
  - Common name → escriu **cn: arnau**
  - Número de grup per defecte → **gidNumber: 200**
  - Directori de l'usuari --> **homeDirectory: /home/alop**
  - Surname → **sn: lopez**
  - Número d'usuari → **uidNumber: 3001**
  - Afegeix l'atribut Shell de l'usuari → **loginShell: /bin/bash**
  - Afegeix l'atribut Contrasenya de l'usuari → **userPassword:: FjeClot25#**

h) Des d'**Apache Directory Studio**,crea un **usuari** de nom **jpons:**

- Crea una nova entrada dins d'**ouUsuaris**.
- Afegeix els **objectClass**: **top**, **posixAccount**, **shadowAccount**, **person**.
- Afegeix un **RDN** de tipus **uid** igual a **jpons**. Per tant, el nom distintiu de la nova entrada serà: **uid=jpons,ou=ouUsuaris,dc=clotfje,dc=net**.
- Quant et demani:
  - Common name → escriu **cn: jaume**
  - Número de grup per defecte → **gidNumber: 2001**
  - Directori de l'usuari --> **homeDirectory: /home/jpons**
  - Surname → **sn: pons**
  - Número d'usuari → **uidNumber: 3002**
  - Afegeix l'atribut Shell de l'usuari → **loginShell: /bin/bash**
  - Afegeix l'atribut Contrasenya de l'usuari → **userPassword:: FjeClot25$**

5.2- Comprovació de funcionament de l'autenticació des del client

a) Verificació inicial:

- Executa: `getent passwd alop` i comprova que et mostra tota la informació sobre l'usuari.
- Prova-ho amb la resta d'usuaris.

b) Verificació final :

- Comprova que els usuari **alop, jpons i jgom** no tene una entrada dins de **/etc/passwd** i a **/etc/shadow**.
- Reinicia l'equip.
- Accedeix com usuari **alop** amb la seva contrasenya. Comprova que es crea un directori personal de l'usuari **alop** dins del client Debian i el seu entorn gràfic de treball.
- Comprova que pots autenticar-te també amb els usuaris **jgim** i **jpons**, i que també es creen els seus directoris personals i el seu entorns gràfics de treball.

6- Accés a la carpeta personal dels usuaris utilitzant NFS

Si volem que qualsevol usuari del domini, després d'autenticar-se, tingui accés a la seva carpeta personal haurem de:

- Exportar els continguts del directori **/home** del servidor i via NFS a la carpeta **/home** de tots els equips de la xarxa.
- Haurem de configurar els clients de manera que de format automàtica, durant l'arrancada **muntin** la carpeta **/home** exportada des del servidor via NFS dins de la seva carpeta **/home**, de manera que els usuaris tindran la sensació de tenir disponible la seva carpeta personal accedint des de qualsevol ordonador i des del principi de la sessió.

6.1- Configuració bàsica del servidor

a) Comenta qualsevol entrada existent del fitxer **/etc/exports** del servidor. Després, crea la següent entrada dins del fitxer **/etc/exports** del servidor:

```
/home *(rw,sync,no_subtree_check,no_root_squash)
```

Això permet:

- Exportar els directori **/home** (directori de tots dels usuaris).
- Amb ***** fem que exporti la carpeta a tots els equips de la xarxa.
- Dins de les opcions bàsiques, la més important és **rw** que permet a l'usuari **llegir/crear/modificar/esborrar** fitxers i carpetes dins del seu directoru personal.

b) Després executa:

```
sudo exportfs -a
```

i a conitnuació reinicia el servidor NFS amb:

```
sudo systemctl restart nfs-kernel-server
```

c) Assegura't que el servei NFS es posa en marxa durant l'arrancada de l'equip servidor. Executa:

```
sudo systemctl enable nfs-kernel-server
```

6.2- Configuració bàsica dels clients

a) Fes que el client munti durant l'arrancada el directori **/home** del servidor de la carpeta local de **/home** del client. Afegeix la següent línia al final de **/etc/fstab**:

```
# Muntatge del directori /home del servidor sobre el directori /home del client
xxyyzz-srv-pj6.clotfje.net:/home  /home  nfs  defaults  0  0
```

a on recorda que **xxyyzz** representa el nom del teu equip servidor.

b) Reinicia l'equip client. Accedeix com usuari **alop** i comprova que:

- L'usuari pot accedir a l'equip i té tot el seu entorn de treball.
- Es crea el directori personal **/home/alop** dins del servidor amb tot l'entorn de treball de l'usuari.
- Comprova que pots crear fitxers i carpetes dins del client que realment es creen dins del servidor.

c) Fes la mateixa comprovació amb els usuari **jpons** i **jgim**.

d) Comprova que **asix2** dins de l'ordinador client també pot accedir però que ara, la seva carpeta personal està en el servidor. Per què creus encara pot accedir aquest usuari?. AJUDA: Torna a llegir el **segon punt** de l'apartat **4.2.a**.

Lliurament de la pràctica

1- Data de lliurament: **13-11-2025** de **19.10** a **21.00**

2- Comprovacions:

a) Comprovació que les dues màquines virtuals es poden fer utilitzant les adreces indicades a l'apartat **3.c**.

b) Mostra les unitat organitzatives, grups i usuaris definits amb LDAP utilitzant **Apache Directory Studio**. Han de sortir les demanades a l'apartat **5.1** de l'activitat.

c) Mostra que **alop**, **jgim** i **jpons** no existeix a la màquina client, mostrant **/etc/passwd**. Mostra també que no tenen directori personal dins de la màquina client visualitzant el contingut de **/home**.

d) Comprova que pots accedir com un dels usuaris (el nom de l'usuari es diu en el moment de la validació) des de la màquina client utilitzant l'entorn gràfic **MATE** i que tens accés a la **carpeta personal**.

e) Mostra que l'usuari validat pot crear una carpeta (el nom de la qual es diu en el moment de la validació) dins del seu directori personal des de la màquina client.

f) Mostra que s'ha creat la carpeta demanada també dins de la màquina servidora.

g) Mostra en el servidor, el valors **UID** i **GID** de les carpetes i fitxers d'un usuari (el nom de l'usuari es diu en el moment de la validació) i comprova que coincideixen amb els emmagatzemats dins del directori **LDAP**.

h) L'usuari **asix2** pot validar-se tot i no estar definit al directori **LDAP**? Per què?