

Alcasar

Il faut deux cartes réseau pour cette VM

Une pour relier à internet une en NAT l'autre en host only avec IP fixe :

Ajouter un réseau par exemple numéro 10 et utiliser ce réseau(par exemple) sur la 2eme carte locale

Sur la deuxième VM avec interface graphique il faut utiliser une carte réseau locale et utiliser le réseau numéro 10 pour la connecter a la VM Alcasar

Gestion des utilisateurs

Root : mot de passe Tmoche3

User Anne2Cannes id de connexion anne2cannes

Mdp Tmoche3

Télécharger https://adullact.net/frs/download.php/file/8873/Mageia-8-x86_64-Alcasar-3.6.0.iso

Suivre le tuto <https://adullact.net/frs/download.php/file/8859/alcasar-3.6.0-installation-fr.pdf>

Pour installer puis aller dans le .conf et autoriser HTTPS, mettre les IP correctes

ATTENTION

Pour utiliser nano il faut l'installer :

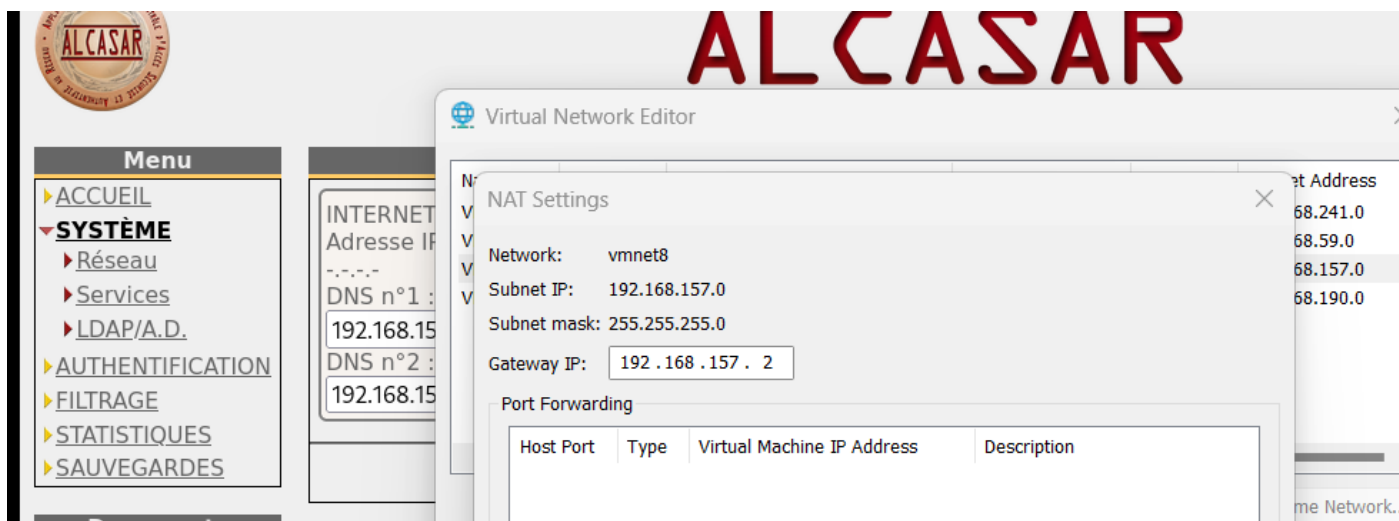
dnf in nano

car le fourbi Mageia ne l'a pas

de plus le fichier .conf est situé :

/usr/local/etc

```
GNU nano 5.4 /usr/local/etc/alca
#####
##                                ##
##          ALCASAR Parameters    ##
##                                ##
#####
INSTALL_DATE=25 septembre 2023 - 11h38
VERSION=3.6.0
ORGANISM=Anne2Cannes
HOSTNAME=alcasar
DOMAIN=localdomain
EXTIF=ens33
INTIF=ens36
LANIF=lo
PUBLIC_IP=dhcp
GW=dhcp
DNS1=192.168.157.2
DNS2=192.168.157.2
PROXY=off
PROXY_IP="192.168.0.100:80"
PUBLIC_WEIGHT=1
PUBLIC_MTU=1500
PRIVATE_IP=192.168.182.1/24
DHCP=on
EXT_DHCP_IP=
RELAY_DHCP_IP=192.168.182.1
RELAY_DHCP_PORT=67
INT_DNS_DOMAIN=
INT_DNS_IP=
INT_DNS_ACTIVE=off
HTTPS_LOGIN=on
HTTPS_CHILLI=on
SSH_LAN=22
SSH_WAN=0
SSH_ADMIN_FROM=0.0.0.0/0.0.0
INTERLAN=off
LDAP=on
LDAP_SERVER=192.168.182.5
LDAP_BASE=ou=People,dc=alcasar;dc=localdomain
LDAP_UID=uid
LDAP_FILTER=
LDAP_USER=
LDAP_PASSWORD=
LDAP_SSL=off
LDAP_CERT_REQUIRED=
[ Lecture de 60 liq
```

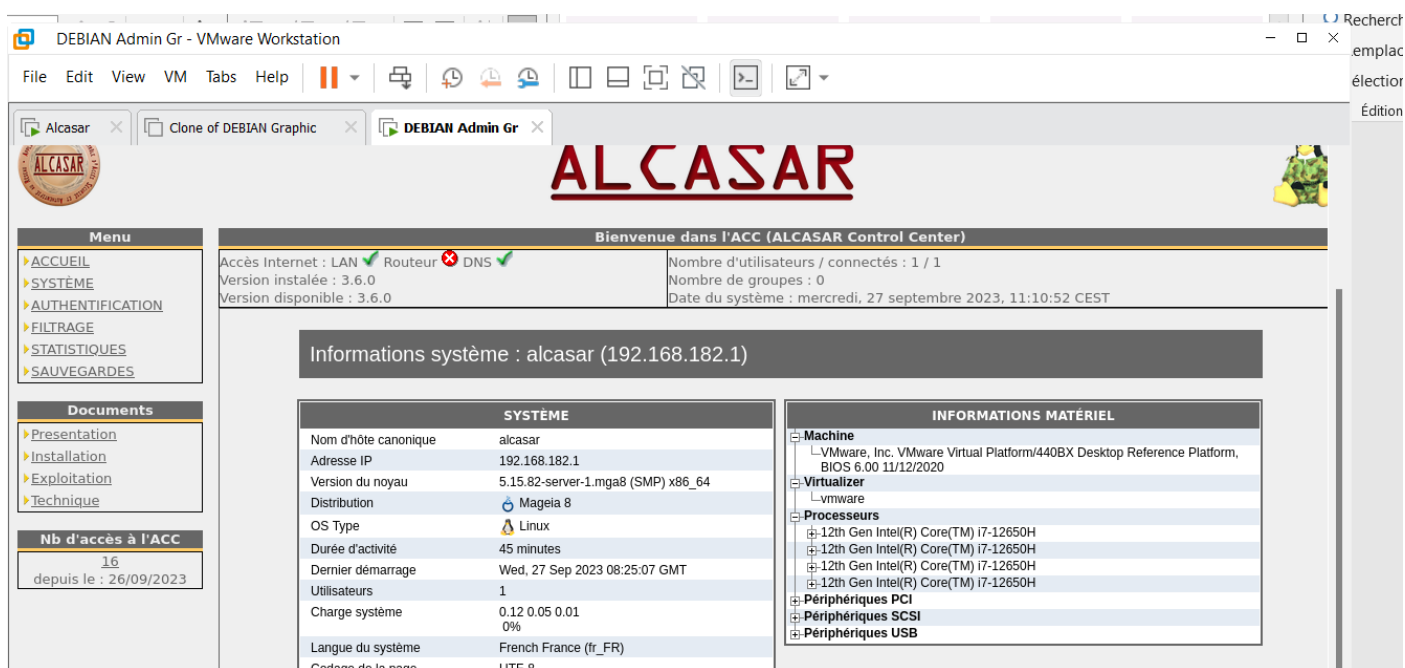
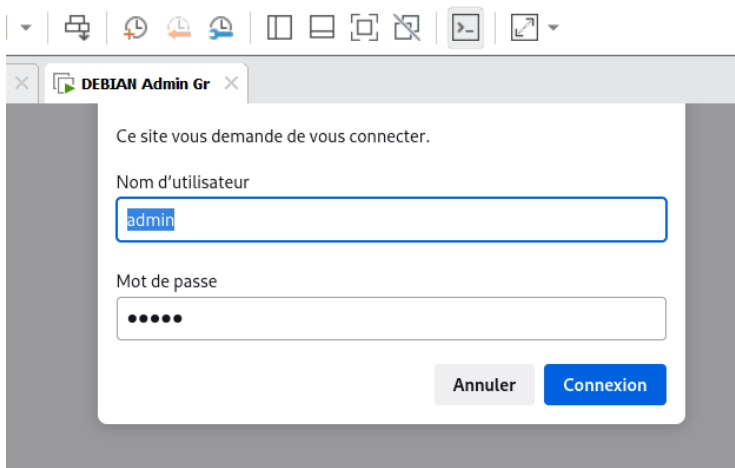
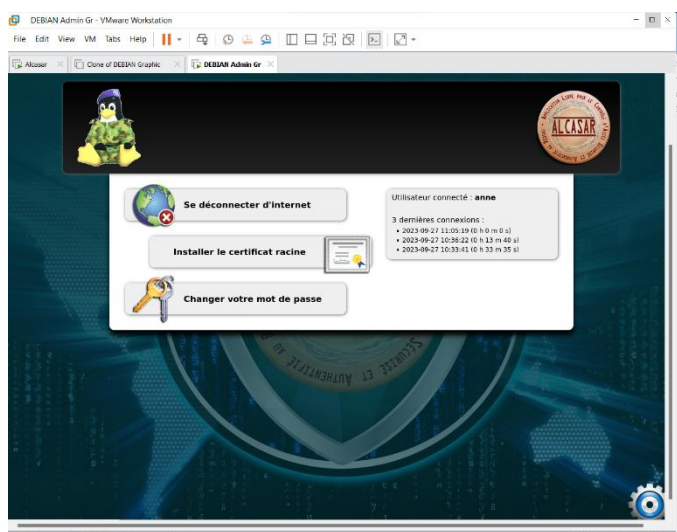


Sur la deuxième VM aller sur internet à <https://alcasar.localdomain>

ATTENTION

Aller sur la roue crantée en bas à droite pour rentrer en admin

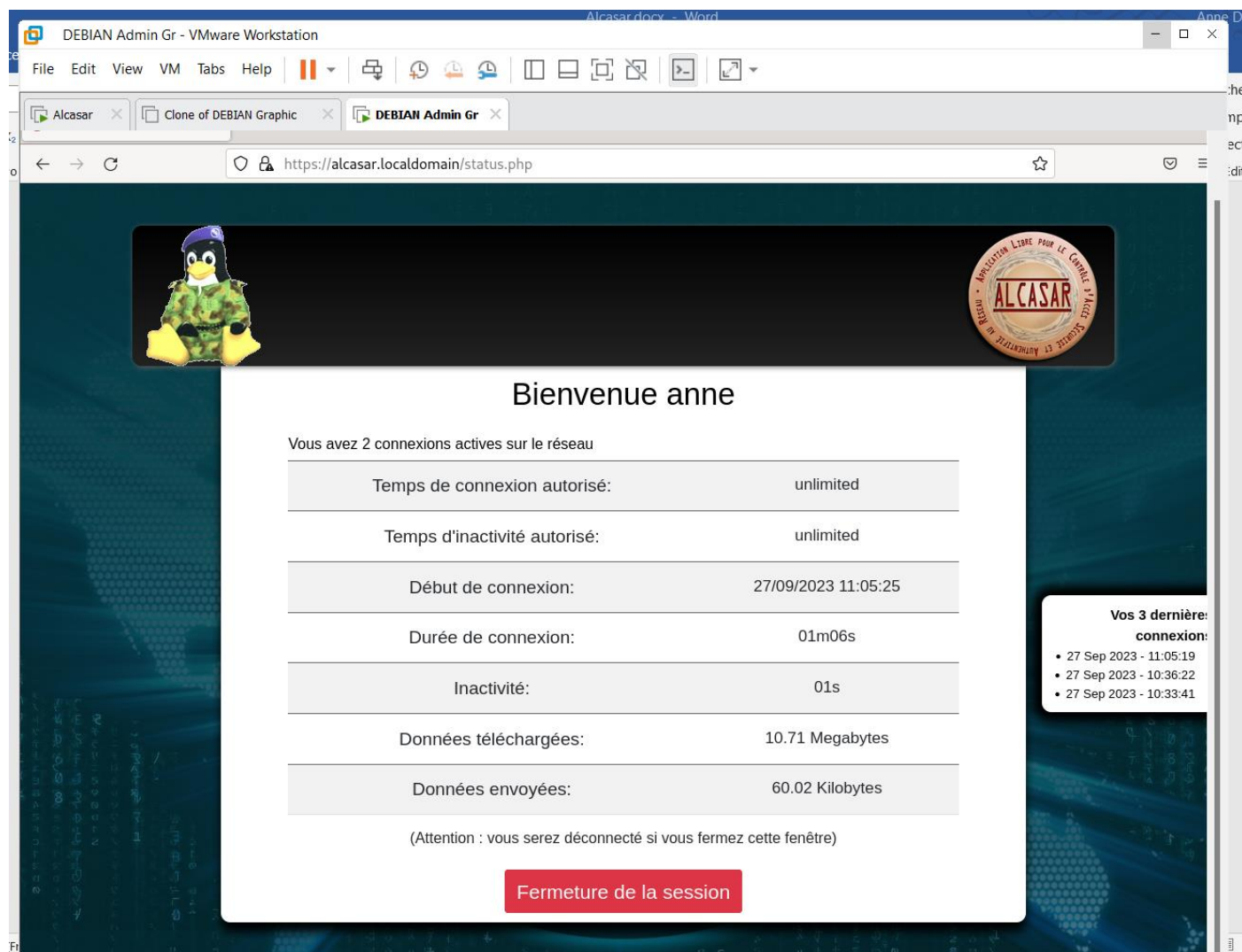
Attention il faut accepter le risque d'aller sur la page



Créer un user -bon c'est pas compliqué il faut aller dans AUTHENTIFICATION – créer un user

Ensuite pour être bien dans sa tête on peut cloner la VM (ce qui gardera les paramètres)

Et aller sur internet pour se loguer avec le user



The screenshot shows a web browser window with the address `https://alcasar.localdomain/status.php`. The page has a dark blue background with a penguin mascot on the left and the Alcasar logo on the right. The main content area is white and displays the following information:

Bienvenue anne

Vous avez 2 connexions actives sur le réseau

Temps de connexion autorisé:	unlimited
Temps d'inactivité autorisé:	unlimited
Début de connexion:	27/09/2023 11:05:25
Durée de connexion:	01m06s
Inactivité:	01s
Données téléchargées:	10.71 Megabytes
Données envoyées:	60.02 Kilobytes

(Attention : vous serez déconnecté si vous fermez cette fenêtre)

Fermeture de la session

On the right side, there is a box titled "Vos 3 dernière: connexion:" with the following list:

- 27 Sep 2023 - 11:05:19
- 27 Sep 2023 - 10:36:22
- 27 Sep 2023 - 10:33:41

Installer ldap

Sur une des deux autres VM car compliqué avec Mageia

Il faudra aller config l'interface control center de alcasar pour mettre l'ip et les paramètres de la VM qui contient le LDAP

<https://www.howtoforge.com/how-to-install-openldap-server-on-debian-12/>

Installation de LDAP :

```
root@debian:~# nano /etc/hosts
root@debian:~# hostnamectl set-hostname ldap.alcasar.localdomain
root@debian:~# hostname -f
ldap.alcasar.localdomain
root@debian:~# ping -c3 ldap.alcasar.localdomain
PING ldap.alcasar.localdomain (192.168.182.5) 56(84) bytes of data.
64 bytes from ldap.alcasar.localdomain (192.168.182.5): icmp_seq=1 ttl=64 time=0.020 ms
64 bytes from ldap.alcasar.localdomain (192.168.182.5): icmp_seq=2 ttl=64 time=0.027 ms
64 bytes from ldap.alcasar.localdomain (192.168.182.5): icmp_seq=3 ttl=64 time=0.028 ms

--- ldap.alcasar.localdomain ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2025ms
rtt min/avg/max/mdev = 0.020/0.025/0.028/0.003 ms
root@debian:~#
```

```
apt install slapd ldap-utils
```

Configuration de slapd

Veuillez indiquer le mot de passe de l'administrateur de l'annuaire LDAP.

Mot de passe de l'administrateur :

<Ok>

```
dpkg-reconfigure slapd
```

Configuration de slapd

Si vous choisissez cette option, aucune configuration par défaut et aucune base de données ne seront créées.

Voulez-vous omettre la configuration d'OpenLDAP ?

<Oui> <Non>

Configuration de slapd

Le nom de domaine DNS est utilisé pour établir le nom distinctif de base (« base DN » ou « Distinguished Name ») de l'annuaire LDAP. Par exemple, si vous indiquez « toto.example.org » ici, le nom distinctif de base sera « dc=toto, dc=example, dc=org ».

Nom de domaine :

alcasar.localdomain

<Ok>

```
systemctl restart slapd
systemctl status slapd
```

```
root@debian:~# dpkg-reconfigure slapd
Backing up /etc/ldap/slapd.d in /var/backups/slapd-2.5.13+dfsg-5... done.
Moving old database directory to /var/backups:
- directory unknown... done.
Creating initial configuration... done.
Creating LDAP directory... done.
root@debian:~# systemctl restart slapd
root@debian:~# systemctl status slapd
● slapd.service - LSB: OpenLDAP standalone server (Lightweight Directory Access Protocol)
   Loaded: loaded (/etc/init.d/slapd; generated)
   Drop-In: /usr/lib/systemd/system/slapd.service.d
            └─slapd-remain-after-exit.conf
   Active: active (running) since Mon 2023-10-02 11:33:10 CEST; 8s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 4805 ExecStart=/etc/init.d/slapd start (code=exited, status=0/SUCCESS)
    Tasks: 3 (limit: 2244)
   Memory: 5.3M
      CPU: 33ms
   CGroup: /system.slice/slapd.service
            └─4813 /usr/sbin/slapd -h "ldap:/// ldapi:///" -g openldap -u openldap -F /etc/ldap/slapd.d

oct. 02 11:33:10 ldap.alcasar.localdomain systemd[1]: Starting slapd.service - LSB: OpenLDAP standalone server (Lightweight Directory Access Protocol)
oct. 02 11:33:10 ldap.alcasar.localdomain slapd[4812]: @(#) $OpenLDAP: slapd 2.5.13+dfsg-5 (Feb  8 2023 01:56:12) $
                        Debian OpenLDAP Maintainers <pkg-openldap-devel@lists.aliases.debian.org>
oct. 02 11:33:10 ldap.alcasar.localdomain slapd[4813]: slapd starting
oct. 02 11:33:10 ldap.alcasar.localdomain slapd[4805]: Starting OpenLDAP: slapd.
oct. 02 11:33:10 ldap.alcasar.localdomain systemd[1]: Started slapd.service - LSB: OpenLDAP standalone server (Lightweight Directory Access Protocol)
lines 1-19/19 (END)
```

```
slapcat
```

```
root@debian:~# slapcat
dn: dc=alcasar,dc=localdomain
objectClass: top
objectClass: dcObject
objectClass: organization
o: alcasar.localdomain
dc: alcasar
structuralObjectClass: organization
entryUUID: 4d657098-f552-103d-8fdf-3b48573dc26e
creatorsName: cn=admin,dc=alcasar,dc=localdomain
createTimestamp: 20231002093208Z
entryCSN: 20231002093208.896645Z#000000#000#000000
modifiersName: cn=admin,dc=alcasar,dc=localdomain
modifyTimestamp: 20231002093208Z
```

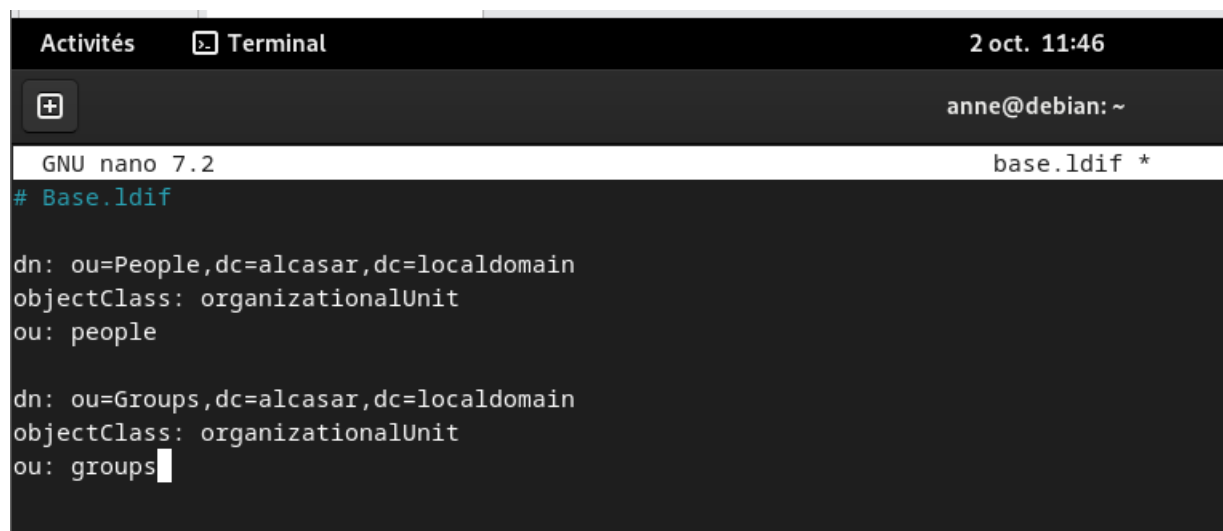
Sécuriser le ldap :

```
apt install ufw
```

```
ufw allow ssh
ufw enable
```

ajouter une base groupe :

```
nano base.ldif
```



```
Activités Terminal 2 oct. 11:46
anne@debian: ~
GNU nano 7.2 base.ldif *
# Base.ldif

dn: ou=People,dc=alcasar,dc=localdomain
objectClass: organizationalUnit
ou: people

dn: ou=Groups,dc=alcasar,dc=localdomain
objectClass: organizationalUnit
ou: groups
```

```
root@debian:~# ldapadd -x -D cn=admin,dc=alcasar,dc=localdomain -W -f base.ldif
Enter LDAP Password:
adding new entry "ou=People,dc=alcasar,dc=localdomain"

adding new entry "ou=Groups,dc=alcasar,dc=localdomain"
```

Vérifier les groupes :

```
root@debian:~# ldapsearch -x -b "dc=alcasar,dc=localdomain" ou
# extended LDIF
#
# LDAPv3
# base <dc=alcasar,dc=localdomain> with scope subtree
# filter: (objectclass=*)
# requesting: ou
#
# alcasar.localdomain
dn: dc=alcasar,dc=localdomain

# People, alcasar.localdomain
dn: ou=People,dc=alcasar,dc=localdomain
ou: people

# Groups, alcasar.localdomain
dn: ou=Groups,dc=alcasar,dc=localdomain
ou: groups

# search result
search: 2
result: 0 Success

# numResponses: 4
# numEntries: 3
root@debian:~#
```

Ajouter un user

```
slappasswd
```

copier la clé du passwd

```
nano user.ldif
```

```
anne@debian: ~  
GNU nano 7.2 user.ldif  
## user.ldif  
  
dn: uid=debian,ou=People,dc=alcasar,dc=localdomain  
objectClass: inetOrgPerson  
objectClass: posixAccount  
objectClass: shadowAccount  
cn: debian  
sn: bookworm  
userPassword: {SSHA}Smql7IceBw0IYmFrtsZEmyDjwUbojyJ9  
loginShell: /bin/bash  
uidNumber: 2000  
gidNumber: 2000  
homeDirectory: /home/debian  
shadowLastChange: 0  
shadowMax: 0  
shadowWarning: 0  
  
dn: cn=debian,ou=Groups,dc=alcasar,dc=localdomain  
objectClass: posixGroup  
cn: debian  
gidNumber: 2000  
memberUid: debian
```

La ligne de commande pour ajouter un user :

```
root@debian:~# ldapadd -x -D cn=admin,dc=alcasar,dc=localdomain -W -f user.ldif  
Enter LDAP Password:  
adding new entry "uid=debian,ou=People,dc=alcasar,dc=localdomain"  
  
adding new entry "cn=debian,ou=Groups,dc=alcasar,dc=localdomain"
```

Puis vérifier la liste des users :


```
root@debian:~# ldapsearch -x -b "ou=People,dc=alcasar,dc=localdomain"
# extended LDIF
#
# LDAPv3
# base <ou=People,dc=alcasar,dc=localdomain> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# People, alcasar.localdomain
dn: ou=People,dc=alcasar,dc=localdomain
objectClass: organizationalUnit
ou: people

# debian, People, alcasar.localdomain
dn: uid=debian,ou=People,dc=alcasar,dc=localdomain
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: debian
sn: bookworm
loginShell: /bin/bash
uidNumber: 2000
gidNumber: 2000
homeDirectory: /home/debian
shadowLastChange: 0
shadowMax: 0
shadowWarning: 0
uid: debian

# search result
search: 2
result: 0 Success

# numResponses: 3
# numEntries: 2
```

```
apt install ldap-account-manager
```

```
nano /etc/php/8.2/apache2/php.ini
```

```
; Maximum amount of memory a script may consume
; https://php.net/memory-limit
memory_limit = 256M
```

```
nano /etc/apache2/conf-enabled/ldap-account-manager.conf
```

```
# HSTS header to enforce https:// connections (requires active mod_h
# Header always set Strict-Transport-Security "max-age=31536000"

<Directory /usr/share/ldap-account-manager>
  Options +FollowSymLinks
  AllowOverride None
  Require ip 127.0.0.1 192.168.182.5
  DirectoryIndex index.html
</Directory>
```

Le 1er IP c'est pour autoriser l'accès en local et le deuxième c'est celui de la machine ldap

```
systemctl restart apache2
```

puis aller sur le web de la VM et taper <http://192.168.182.5/lam>

aller à droite dans configuration puis sur edit server profiles

le user est lam, le passwd par défaut est lam

ceci donne accès à la page de config du LAM

il faut créer les groupes et les users comme dans un AD puis l'exporter dans le ldap

The screenshot shows the LDAP Account Manager (LAM) web interface in a browser. The address bar shows the URL 192.168.182.5/lam/templates/account/edit.php?editKey=editContainer1696412544tXbl9QB0BQtySsvkZWTm. The page title is "LDAP Account Manager - 8.3" and the user is logged in as "admin".

At the top, there are buttons: "Save", "Set password", "Delete", "Reset changes", and "Back to user list". On the right, there are links for "Accounts", "Tools", "Help", and "Logout", along with a "default" profile selector and a "Load profile" button.

The main content area is titled "Seb Guarnera" and shows the configuration for a user. The "Suffix" is "People > alcasar > localdomain" and the "RDN identifier" is "cn".

On the left, there are tabs for "Personal", "Unix", and "Shadow". The "Personal" tab is selected.

The configuration fields include:

- User name: seb
- Common name: Seb Guarnera
- UID number: 10002
- Gecos: (empty)
- Primary group: LES JEUNES
- Additional groups: (empty)
- Home directory: /home/seb
- Login shell: /bin/bash
- Password: (empty)

At the bottom right, there are buttons for "Lock password" and "Remove password".

ALCASAR - Anne2Cannes × ALCASAR Control Center × LDAP Account Manager (l × +

















192.168.182.5/lam/templates/lists/list.php?type=user

LDAP Account Manager - 8.3 admin Accounts Tools Help Logout

Users

New user File upload Delete selected users

User count: 4

Actions	User name	First name	Last name	UID number	GID number
Sort sequence	▼ ▲	▼ ▲	▼ ▲	▼ ▲	▼ ▲
<input type="checkbox"/> Filter ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>    	admin	Thierry	Rami	2000	10001
<input type="checkbox"/>    	lawrie	Lawrie	Falcao	10001	10002
<input type="checkbox"/>    	leo	Leo	Herr	10000	10001
<input type="checkbox"/>    	seb	Seb	Guarnera	10002	10002

ALCASAR - Anne2Cannes × ALCASAR Control Center × LDAP Account Manager (l × +

192.168.182.5/lam/templates/tools/importexport.php

LDAP Account Manager - 8.3 admin Accounts Tools Help Logout

Import Export

Export

Base DN * ?

Search scope

Search filter ?

Attributes ?

Include system attributes ☐ ?

Save as file ☐

Export format


End of line

Submit

Configurer le LDAP de Alcasar comme suit : l'adresse correspond à celle dans laquelle on fait l'export



ALCASAR



Menu

> ACCUEIL
 > **SYSTÈME**
 > Réseau
 > Services
 > LDAP/A.D.
 > AUTHENTIFICATION
 > FILTRAGE
 > STATISTIQUES
 > SAUVEGARDES

Documents

> Présentation
 > Installation
 > Exploitation
 > Technique

Nb d'accès à l'ACC

10
 depuis le :
 02/10/2023

Éditer la configuration LDAP:

OUI

Serveur LDAP:

192.168.182.5
 Assistant

Connexion chiffrée

NON

Vérifier le certificat SSL

NON

Certificat SSL (CA)

Parcourir...
 Aucun fichier sélectionné.

CN de l'utilisateur exploité par ALCASAR:

Mot de passe:

DN de la base:

ou=People,dc=alcasar,dc=localdomain

Identifiant d'utilisateur (UID):

uid

Filtre de recherche des utilisateurs (optionnel):

Nom de domaine interne

Nota : on ne peut voir les users et groupes que dans l'interface du LDAP, pas dans ALCASAR

ALCASAR gère tout sauf les users et groupes, il faut considérer la question comme ça

Se dé-loguer et re-renter avec un user créé dans le LDAP pour vérifier :



 Cofinancé par
l'Union européenne





Bienvenue leo

Temps de connexion autorisé:	unlimited
Temps d'inactivité autorisé:	unlimited