

ALCASAR



Laurent FAUVEAU

24 juin 2024

[lien utile :](#)

Introduction

Portail captif c ‘est quoi ?

Un **portail captif** est une page web que les utilisateurs voient avant d'accéder au réseau Internet lorsqu'ils se connectent à un réseau Wi-Fi public ou semi-public. Ce mécanisme est couramment utilisé dans divers lieux comme les hôtels, les cafés, les aéroports, et les établissements scolaires.

			
Protection Installé sur un réseau public, il protège le responsable du réseau en journalisant et en attribuant (imputation) toutes les connexions afin de répondre aux exigences légales et réglementaires*.	Pédagogie ALCASAR est utilisé comme outil pédagogique dans le cadre de diverses formations : "sécurité des réseaux", "contrôles et éthique", "respect de la vie privée", etc. La documentation complète de ce projet est disponible dans la section "Téléchargement" de ce site Web.	Projet libre ALCASAR est un projet indépendant, libre (licence GPLv3) et gratuit. L'équipe de suivi de projet (ALCASAR team) est conduite par Richard Rey "rexy" et Franck Boujoux "3abtux". Elle est constituée de développeurs "seniors", de développeurs «juniors», de "padawan", de rédacteurs/traducteurs, de graphistes et de testeurs identifiables sur le forum .	Contribution Si vous souhaitez contribuer ou simplement remercier l'équipe de ce projet : rendez-vous dans la rubrique contribution .

ALCASAR peut être installé sur un ordinateur standard équipé de deux cartes réseau Ethernet.

La première est connectée à l'équipement du Fournisseur d'Accès Internet (FAI).

La deuxième est connectée au commutateur utilisé pour desservir le réseau des équipements de consultation.

Par défaut, l'adresse **IP** de cette deuxième carte réseau est : **192.168.182.1/24**

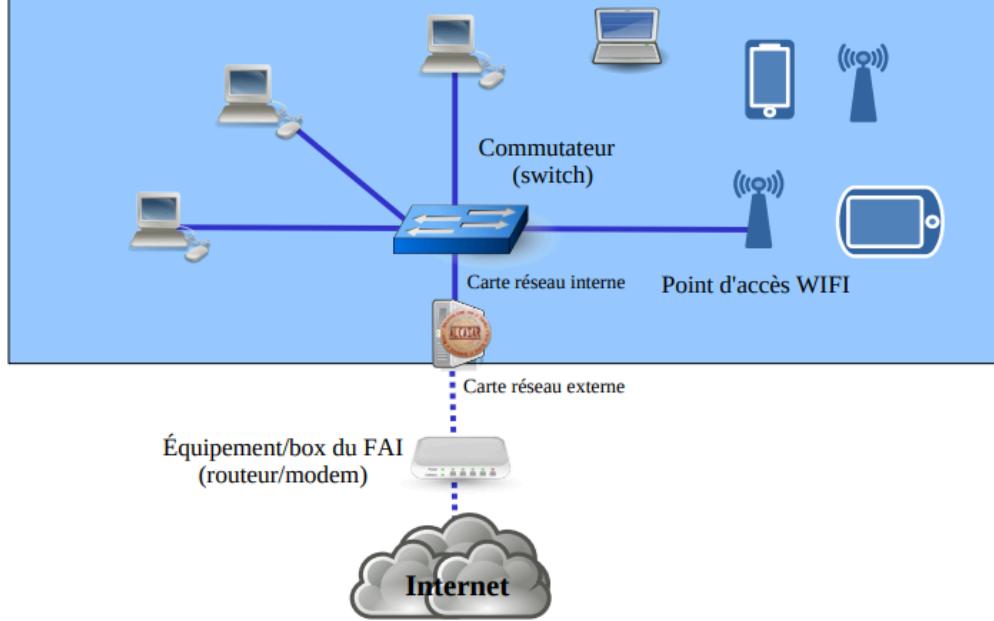
Cela permet de disposer d'un plan d'adressage de classe C (254 équipements).

Ce plan d'adressage est modifiable lors de l'installation.

Pour tous les équipements situés sur le réseau de consultation, ALCASAR est le serveur DHCP, le serveur DNS, le serveur de temps et le routeur par défaut (« default gateway »).

Ainsi, sur ce réseau, il ne doit y avoir aucun autre routeur ou serveur DHCP (vérifiez bien vos points d'accès WIFI).

Réseau de consultation



<ul style="list-style-type: none"> ✓ Authentifie et contrôle les accès à Internet ✓ Trace et impute les connexions conformément aux lois françaises et européennes ✓ Respecte la vie privée ✓ Protège et filtre les flux par utilisateur ou groupe d'utilisateurs (antivirus HTTP, filtrage de protocoles réseau, de noms de domaine, d'URLs et d'adresses IP) ✓ Filtrage par liste rouge (sites interdits) ou par liste verte (sites autorisés) 	<ul style="list-style-type: none"> ✓ Contrôle d'accès et contrôle parental par utilisateur ou groupe d'utilisateurs (temps de connexion, périodes autorisées, volume maximum téléchargé, bande passante autorisée) ✓ Fonctionne sous forme de machine virtuelle ou sur mini-PC possédant deux cartes réseaux ✓ Libre et gratuit ✓ Compatible avec l'initiative "WiFi4EU" de la Commission Européenne
---	--

Pour Info !

Conservation des Données de Connexion

En France, la **loi n° 2006-64 du 23 janvier 2006** et le **Décret n° 2011-219 du 25 février 2011** imposent aux fournisseurs d'accès Internet et aux opérateurs de communications électroniques la conservation des données de connexion pour une durée d'un an. Cela concerne aussi les gestionnaires de points d'accès Wi-Fi.



WiFi4EU est une initiative de l'Union européenne visant à fournir une connexion Wi-Fi gratuite dans les espaces publics des municipalités à travers l'Europe.

224 villes en France

PLAN d'ADRESSAGE :

Paramètres sésses du réseaux	@IP du réseau	Nombre d'équipements de consultation	masque du réseau	@IP d'ALCASAR (cette adresse est l'adresse IP DNS et du routeur par défaut du réseau)	Suffixe DNS
en d'adressage posé par défaut asse “ ”)					

Bien que cela soit possible, **il est déconseillé de définir un réseau de consultation en classe A**

(ex : 15.x.y.z/8). En effet, le serveur **DHCP** interne d'ALCASAR devra alors réservé et gérer plus de 16 millions d'adresses IP.

La gestion d'un tel volume d'adresses est très gourmande en ressource système et mémoire.

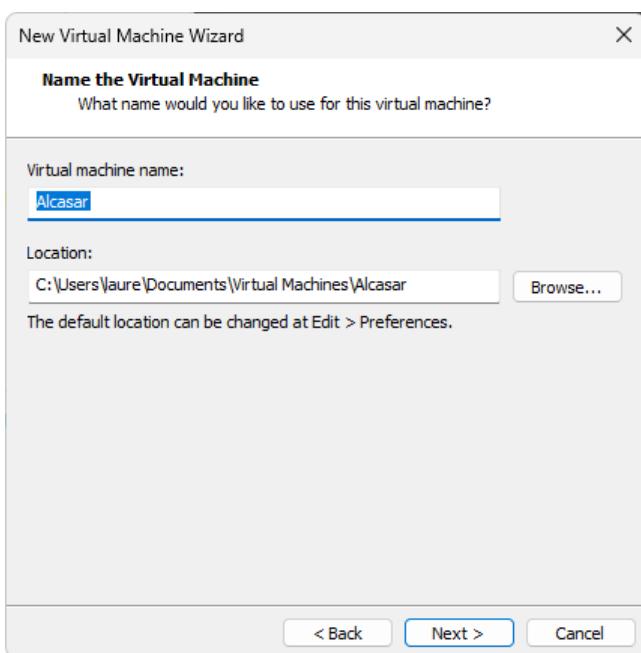
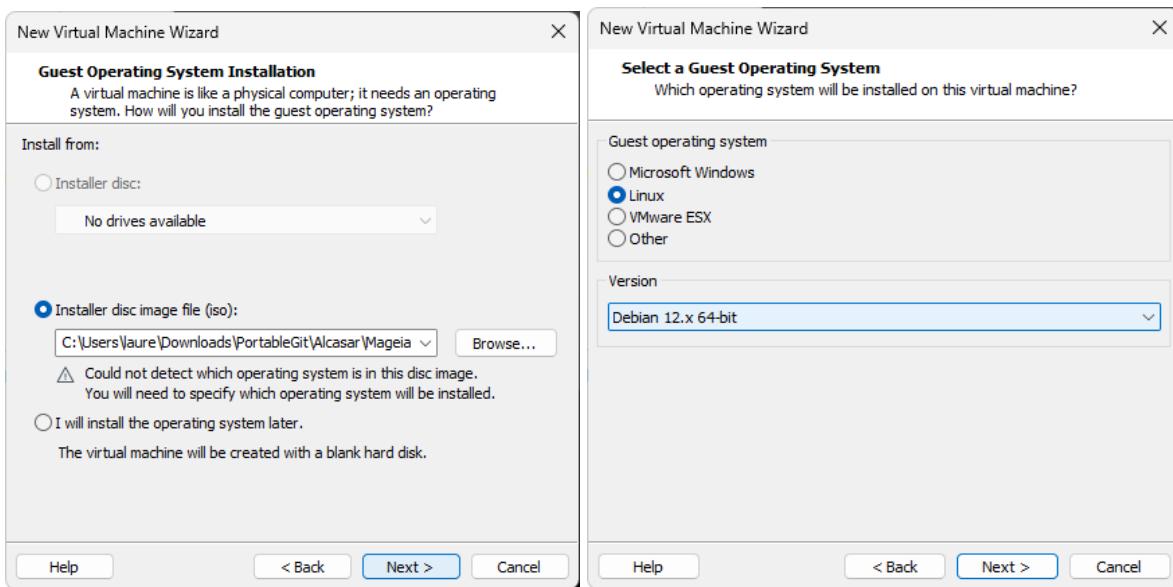
Faire deux VM une serveur ALCAZAR et une VM client DEBIAN

INSTALLATION :

doc : <https://adullact.net/frs/download.php/file/8927/alcasar-3.6.1-installation-fr.pdf>

1 - Configurer l'accès à l'iso d'installation d'alcasar sous VMWARE

lien iso => https://adullact.net/frs/download.php/file/8934/Mageia-8-x86_64-Alcasar-3.6.1.iso



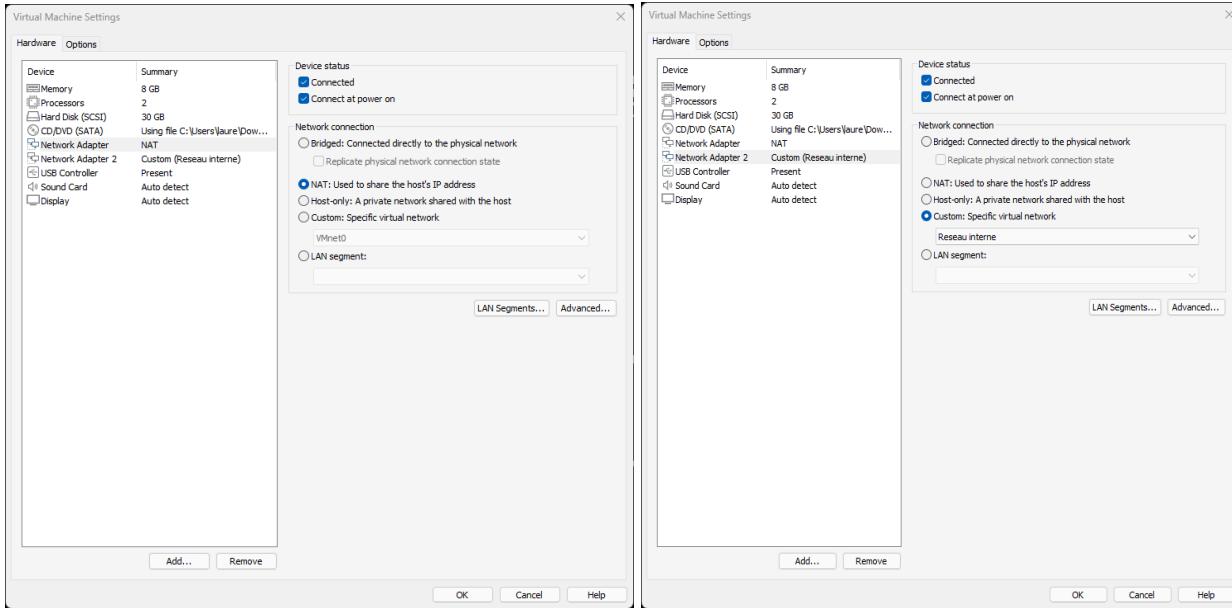
2 - configurer les deux cartes reseaux Sous VMWARE

ENS 33 Nat

ENS 34 Custom => adresse 192.168.128.0 masque sous reseau 255.255.255.0



VMnet8	NAT	NAT	Connected	Enabled	192.168.126.0
Réseau ...	Custom	-	-	-	192.168.182.0



3 - configurer la mémoire et la capacité du disque dur sous VMWARE

30 GB

8GB de mémoire

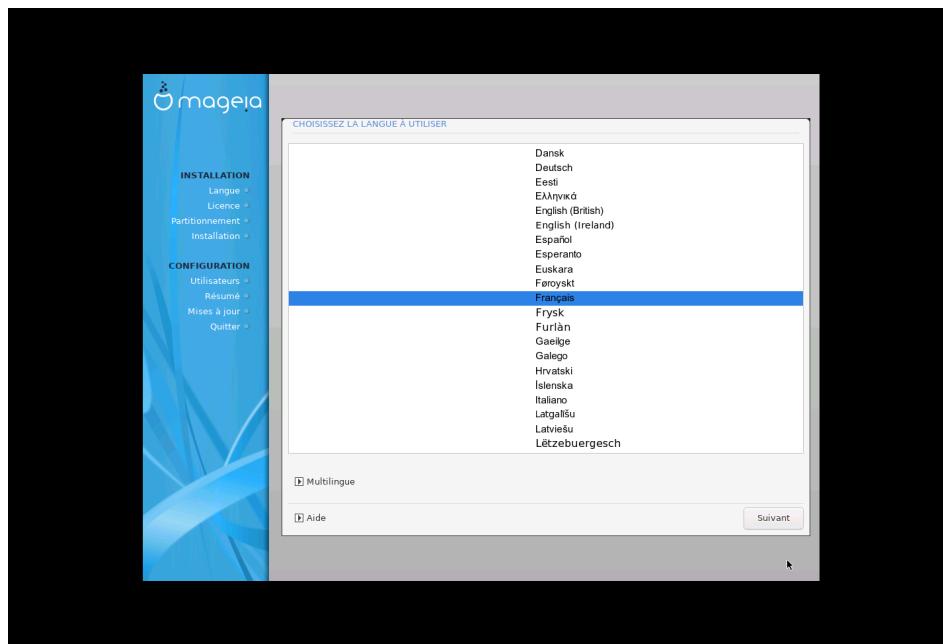
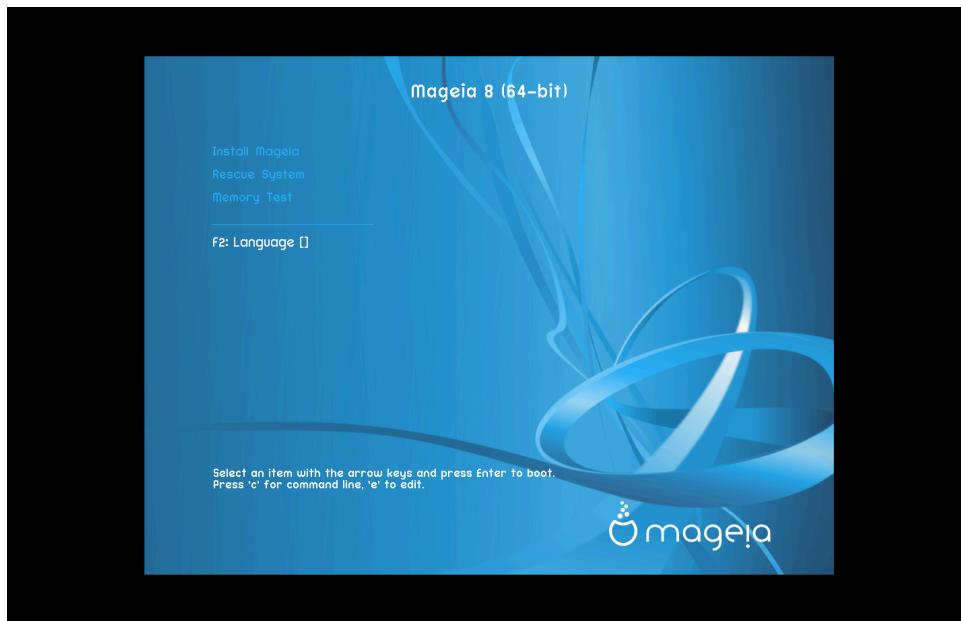
▼ Devices		
	Memory	8 GB
	Processors	2
	Hard Disk (SCSI)	30 GB

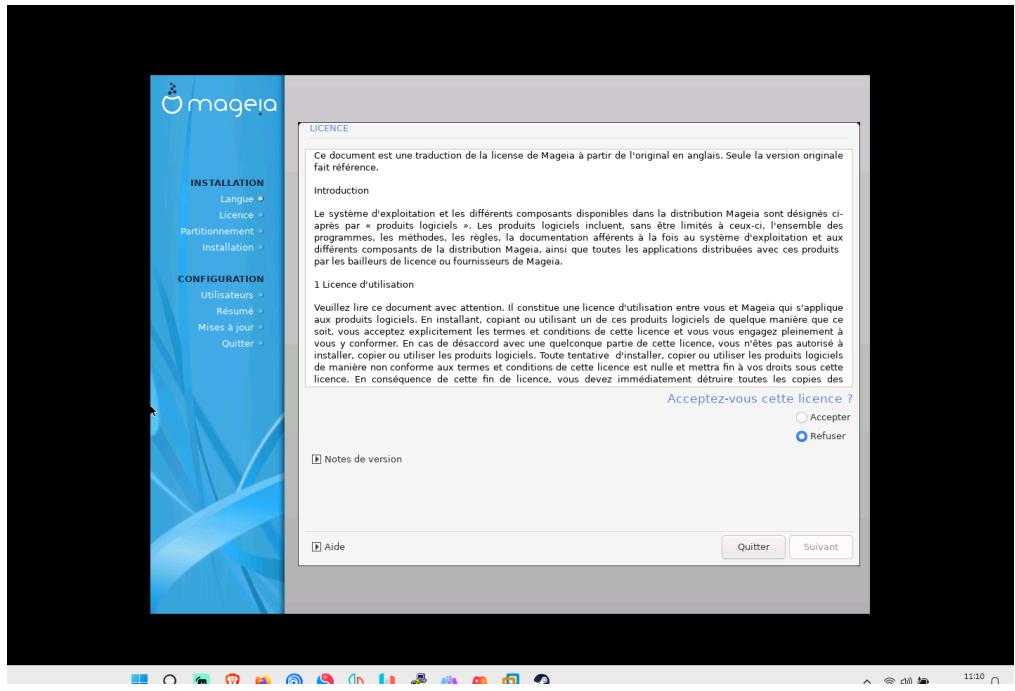
A ce moment la on peut lancer l'installation du serveur ALCASAR

INSTALLATION de MAGEIA

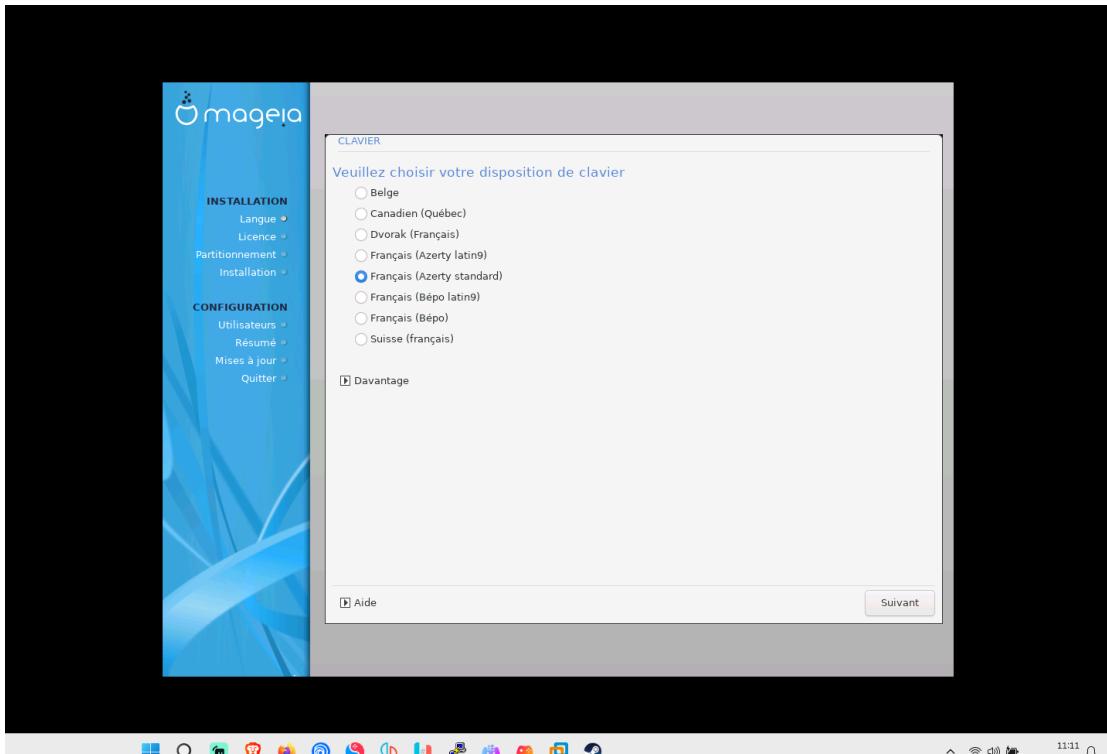
1 - lancer la VM sous VMWare pour installer Mageia qui est l'OS qui permet l'installation d'alcasar car Alcasar à été développé pour qu'il fonctionne seulement sous Mageia !!

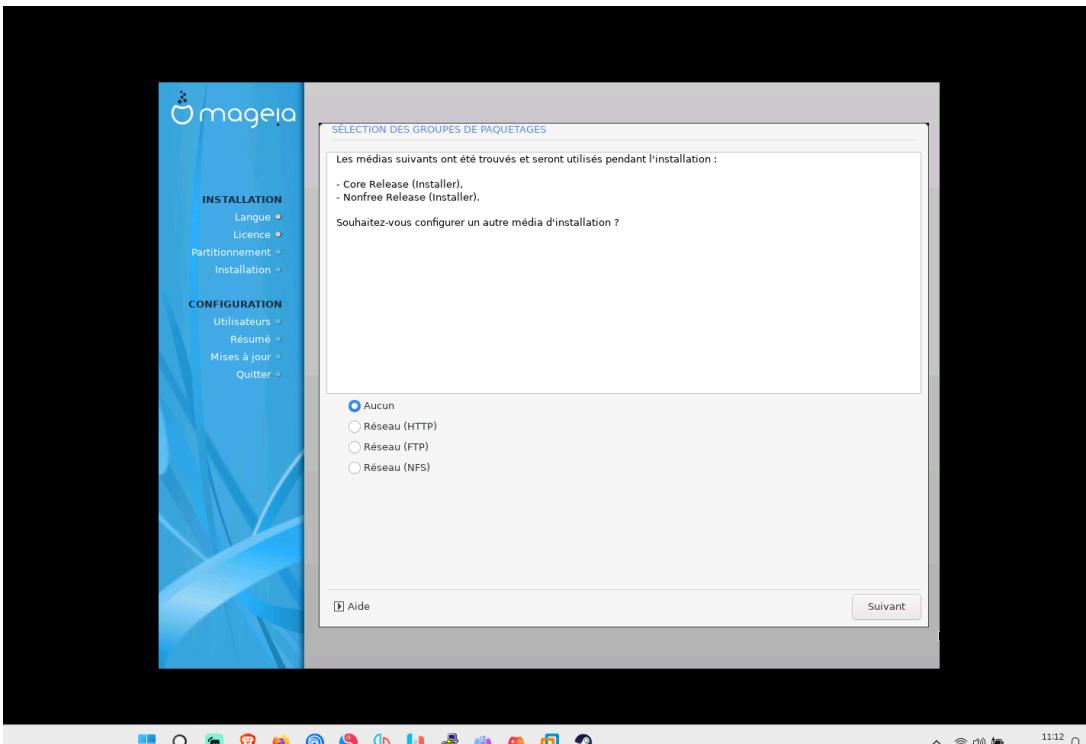
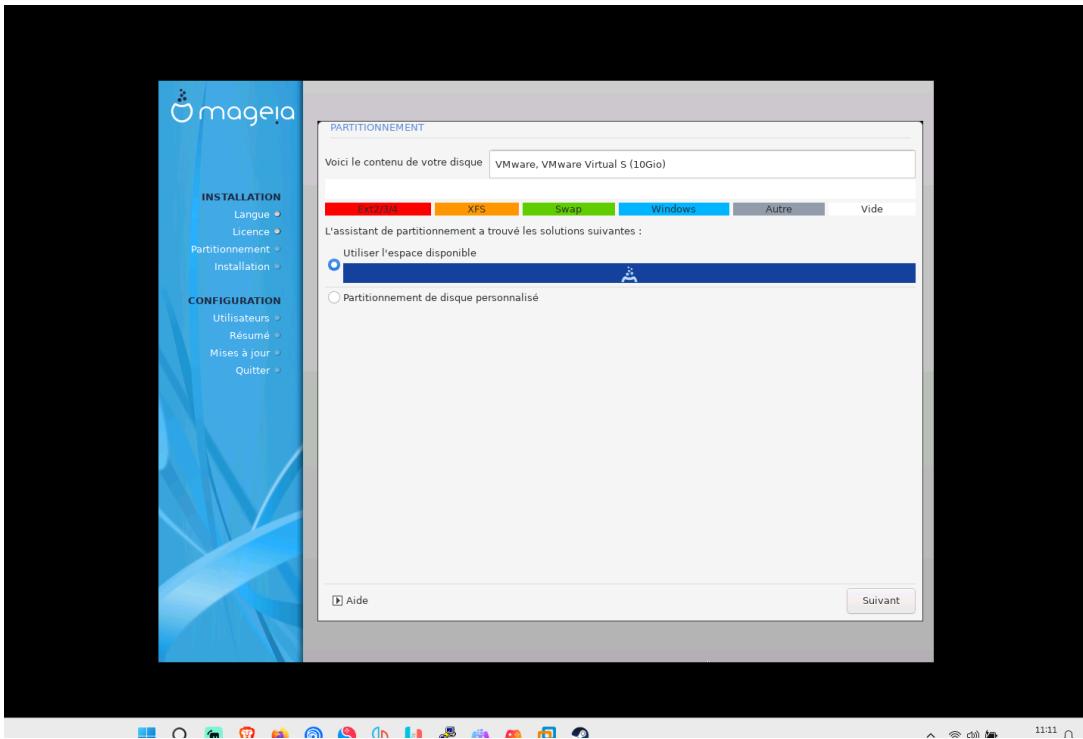
Choisissez le langage



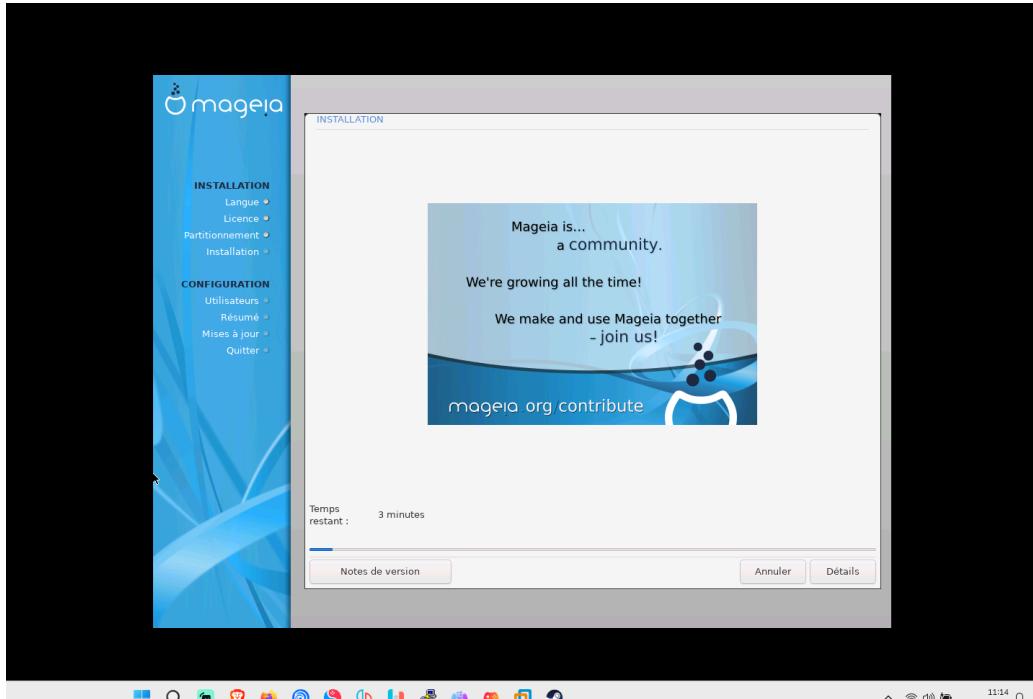


Choisissez le type de clavier

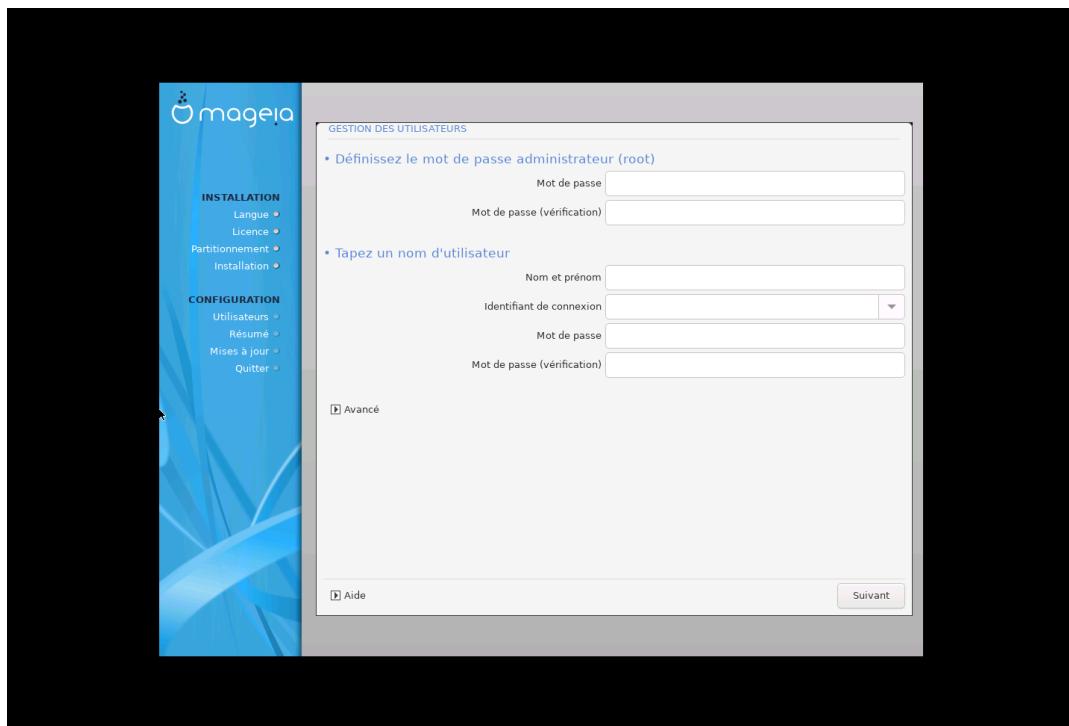


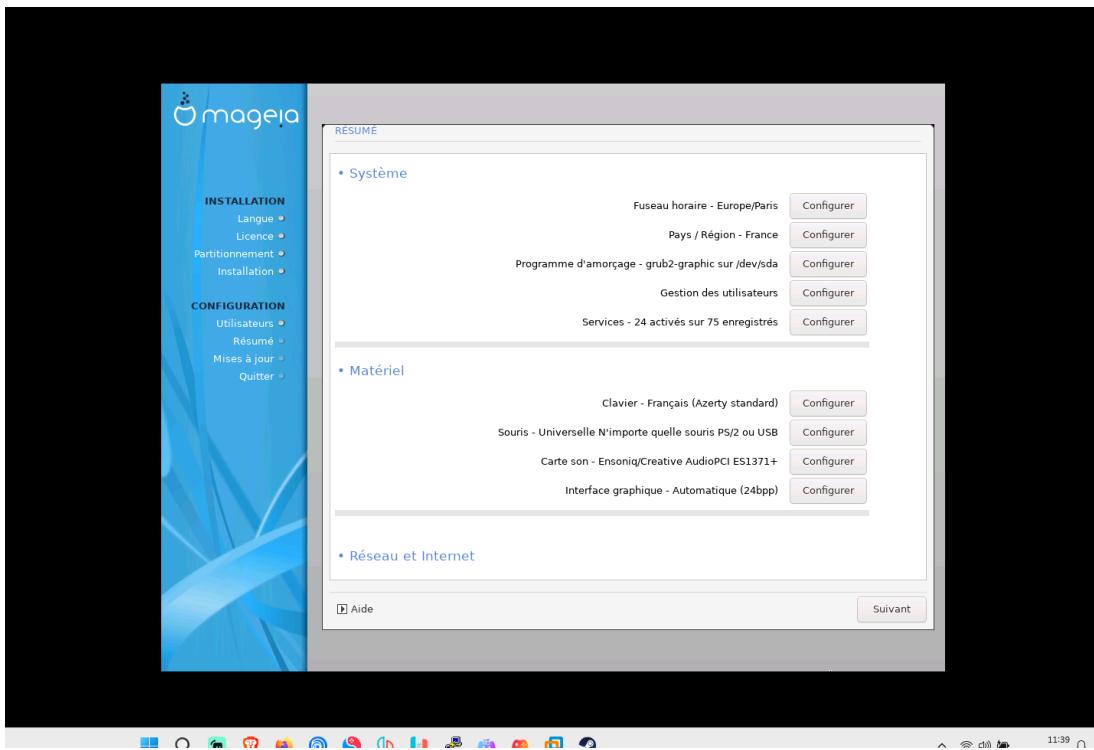


l'installation de Mageia commence

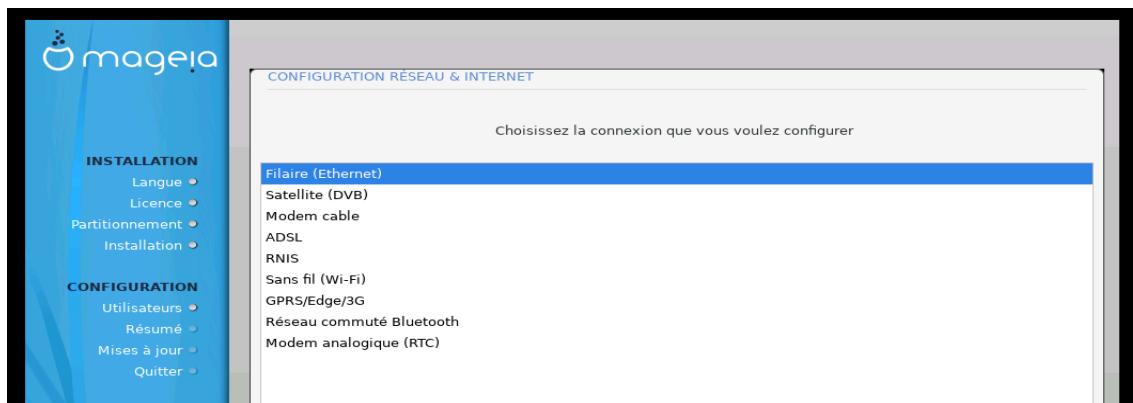


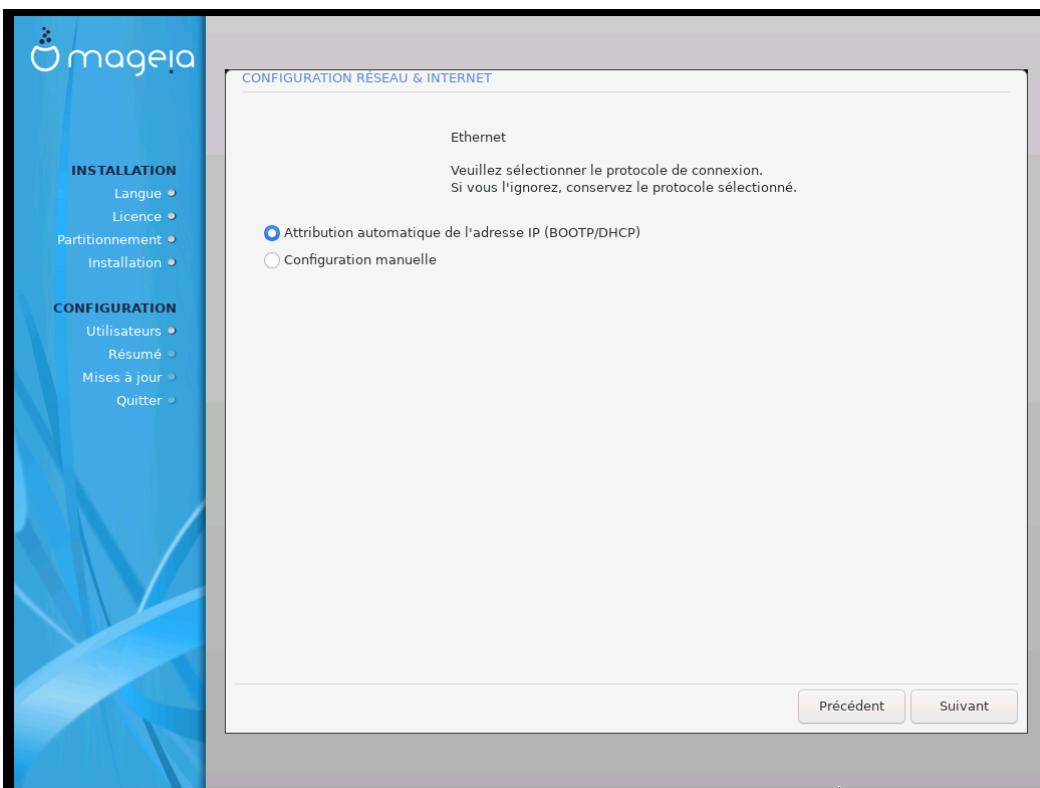
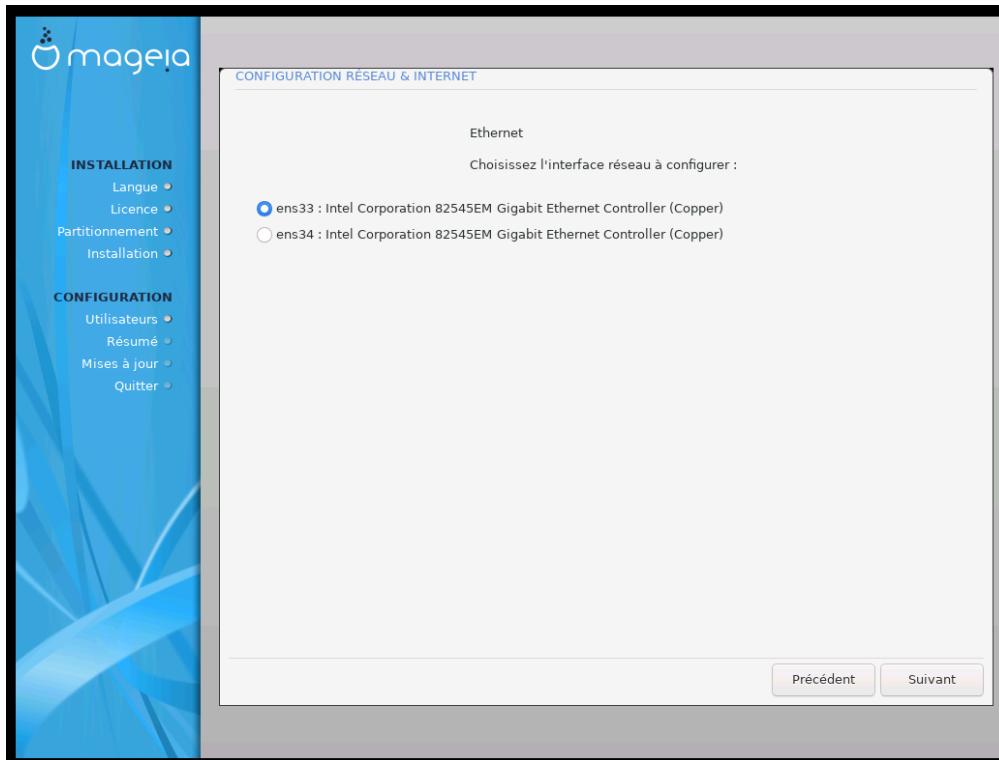
définir le mot de passe ROOT et UTILISATEUR

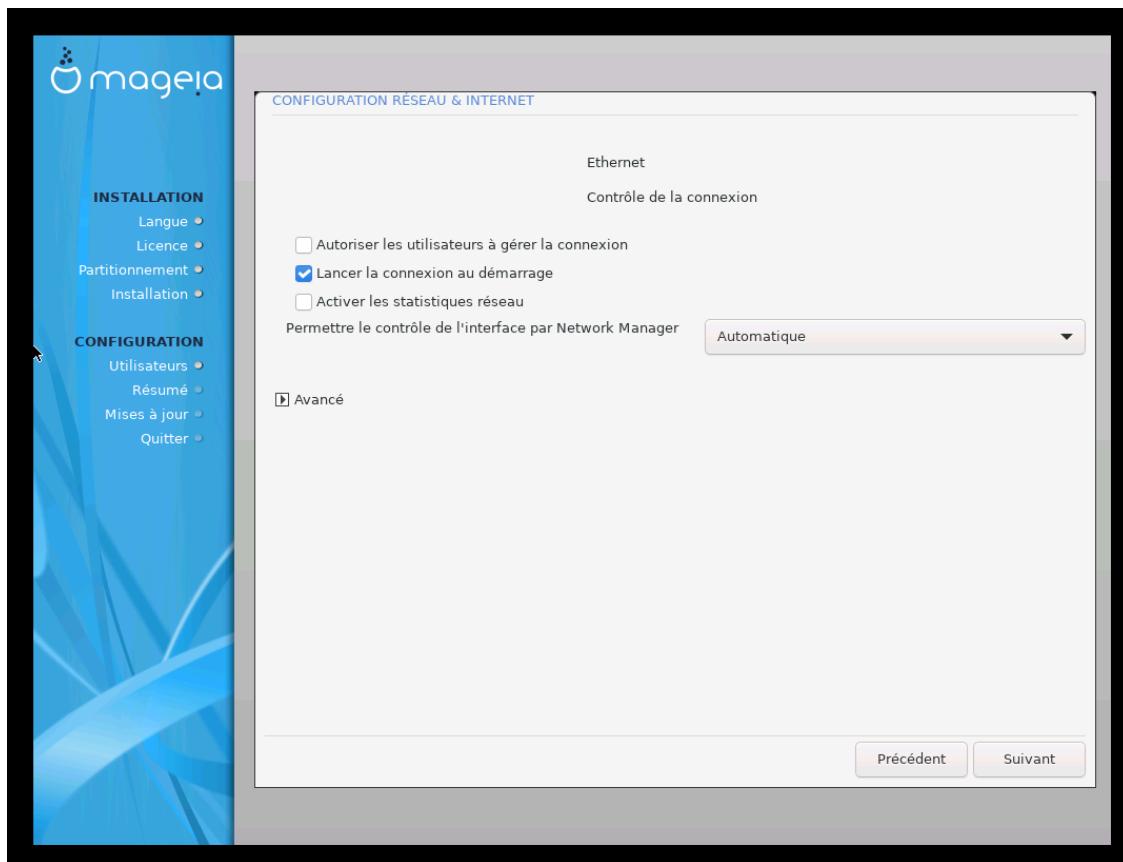
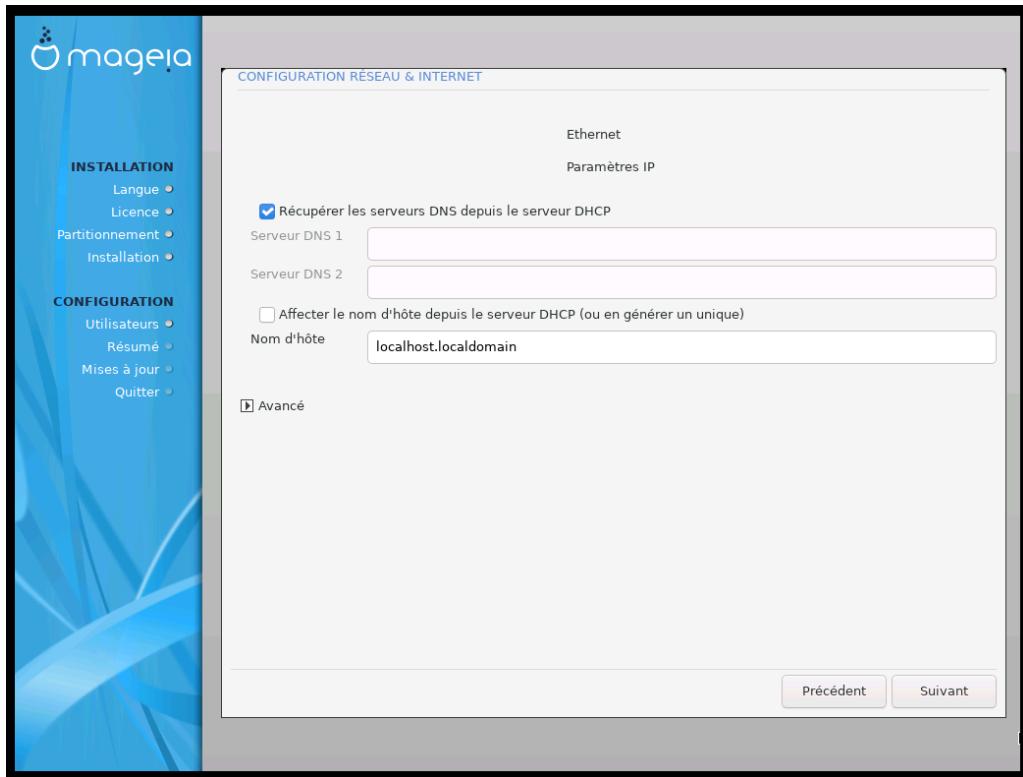




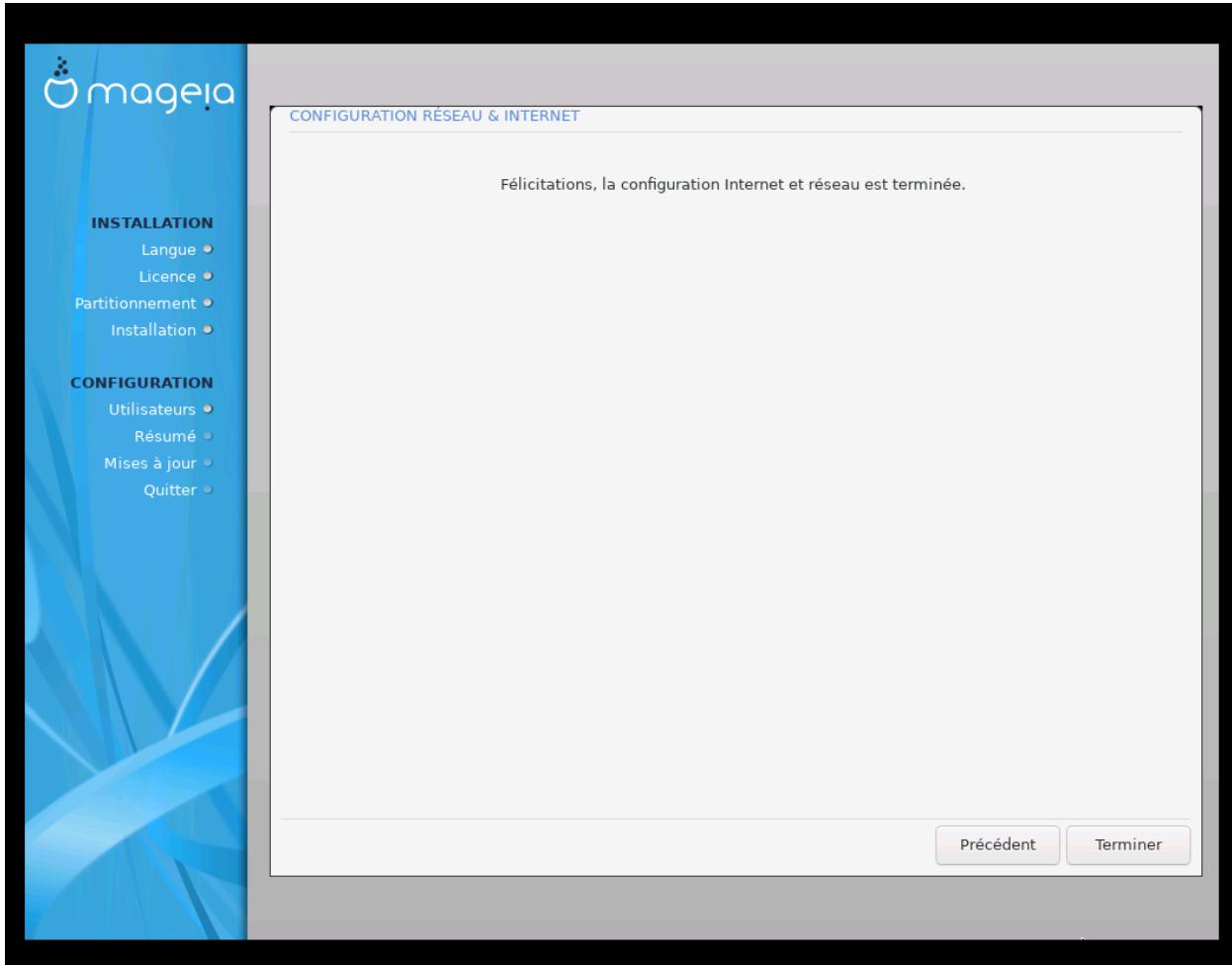
Sélectionné Filaire car la VM simule le lien réseau entre la carte wifi et la carte virtualisée ENS 33







Fin de l'installation de Mageia



A présent on va démarrer Mageia qui va permettre d'installer le serveur ALCASAR

On arrive sans interface graphique sur cette interface se connecter en ROOT et pour afficher de manière continue l'état de vos cartes réseau => **watch ip link**

a ce niveau faut que les deux carte soit => **state UP**

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT
    group default qlen 1000
        link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode
    group default qlen 1000
        link/ether 00:0c:29:16:62:b8 brd ff:ff:ff:ff:ff:ff
        altname enp2s1
3: ens34: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode
    group default qlen 1000
        link/ether 00:0c:29:16:62:c2 brd ff:ff:ff:ff:ff:ff
        altname enp2s2
```

savoir si on est bien connecté on lance une commande => **ping -c3 google.fr**

```
[root@localhost ~]# ping -c3 google.fr
PING google.fr (172.217.18.35) 56(84) octets de données.
64 octets de ham02s12-in-f35.1e100.net (172.217.18.35) : icmp_seq=1 ttl=128 temp
s=10.5 ms
64 octets de ham02s12-in-f35.1e100.net (172.217.18.35) : icmp_seq=2 ttl=128 temp
s=35.0 ms
64 octets de mrs00s01-in-f3.1e100.net (172.217.18.35) : icmp_seq=3 ttl=128 temps
=15.7 ms

--- statistiques ping google.fr ---
3 paquets transmis, 3 reçus, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 10.403/20.385/35.022/10.562 ms
[root@localhost ~]#
```

INSTALLATION D'ALCASAR

faire **ls** et

se dirigé vers => **cd alcasar-3.6.1**

```
[root@localhost ~]# ls
aif-mount/  alcasar-3.6.1/  drakx/  tmp/
[root@localhost ~]# cd a
aif-mount/  alcasar-3.6.1/
[root@localhost ~]# cd alcasar-3.6.1/
[root@localhost alcasar-3.6.1]# _
```

lancer la commande d'installation => **sh alcasar.sh -i**

```
[root@localhost alcasar-3.6.1]# sh alcasar.sh -i
```

[accepter la licence](#)

```
-----  
          ALCASAR V3.6.1 Installation  
          Application Libre pour le Contrôle d'Accès Sécurisé et Authentifié au Réseau  
-----
```

```
*****  
**** Licence d'utilisation ****  
*****
```

ALCASAR est un logiciel libre

Avant de l'installer, vous devez accepter les termes de sa licence 'GPL-V3'.
Le descriptif de cette licence est disponible dans le fichier 'GPL-3.0.txt'.
Une traduction française est disponible dans le fichier 'GPL-3.0.fr.txt'.

Les objectifs de cette licence sont de garantir à l'utilisateur :

- La liberté d'exécuter le logiciel, pour n'importe quel usage ;
- La liberté d'étudier et d'adapter le logiciel à ses besoins ;
- La liberté de redistribuer des copies ;
- L'obligation de faire bénéficier à la communauté les versions modifiées.

Acceptez-vous les termes de cette licence (O/n) ? :

```
-----  
          ALCASAR V3.6.1 Installation  
          Application Libre pour le Contrôle d'Accès Sécurisé et Authentifié au Réseau  
-----
```

Interface externe (Internet) utilisée : ens33
Interface interne utilisée : ens34

Tests des paramètres réseau : : ok

Le paquetage wget-1.21.3-1.mga8.x86_64 est déjà installé

http://ftp.free.fr/mirrors/mageia.org/distrib/8/x86_64

ajout du média « core »

http://ftp.free.fr/mirrors/mageia.org/distrib/8/x86_64/media/core/release/me

dia_info/20210224-165404-synthesis.hdlist.cz

ajout du média « core-updates »

http://ftp.free.fr/mirrors/mageia.org/distrib/8/x86_64/media/core/updates/me

dia_info/20231219-182251-synthesis.hdlist.cz

ajout du média « nonfree »

http://ftp.free.fr/mirrors/mageia.org/distrib/8/x86_64/media/nonfree/release

/media_info/20210224-171907-synthesis.hdlist.cz

ajout du média « nonfree-updates »

http://ftp.free.fr/mirrors/mageia.org/distrib/8/x86_64/media/nonfree/updates

/media_info/20230911-130142-synthesis.hdlist.cz

entrez le nom de l'organisme => **laplateforme**

```
-----  
          ALCASAR V3.6.1 Installation  
          Application Libre pour le Contrôle d'Accès Sécurisé et Authentifié au Réseau  
-----
```

Entrez le nom de votre organisme : laplateforme_

on insère l'IP de la carte réseau **ENS 34** qui sert au protocole **DHCP** du serveur **ALCASAR**

```
ALCASAR V3.6.1 Installation
Application Libre pour le Contrôle d'Accès Sécurisé et Authentifié au Réseau
-----
Par défaut, l'adresse IP d'ALCASAR sur le réseau de consultation est : 192.168.1
82.1/24
Voulez-vous utiliser cette adresse et ce plan d'adressage (recommandé) (O/n) ? :
n
Entrez l'adresse IP d'ALCASAR au format CIDR (a.b.c.d/xx) : 192.168.182.254/24_
```

on insère le nom du compte **admin**

ALCASAR V3.6.1 Installation
Application Libre pour le Contrôle d'Accès Sécurisé et Authentifié au Réseau

Création du premier compte administrateur :
Entrez le nom du compte à créer (profil 'admin') :

```
/etc/ssh/sshd_config /etc/security /etc/cron.allow /etc/at.allow /etc/systemd/journald.conf /etc/pam.d/system-auth /etc/security/shell  
Création du fichier de configuration GRUB®  
Thème trouvé : /boot/grub2/themes/maggy/theme.txt  
Image Linux trouvée : /boot/vmlinuz-5.15.126-server-1.mga8  
Image mémoire initiale trouvée : /boot/initrd-5.15.126-server-1.mga8.img  
fait

#####
#          Fin d'installation d'ALCASAR
#
#      Application Libre pour le Contrôle Authentifié et Sécurisé
#          des Accès au Réseau ( ALCASAR )
#
#####

- ALCASAR sera fonctionnel après redémarrage du système
- Lisez attentivement la documentation d'exploitation
- Le centre de contrôle d'ALCASAR (ACC) est à l'adresse http://alcasar.localdomain
```

Démarrage du serveur ALCASAR

```

db      88      ,ad8888ba,      db      ad88888ba      db      88888888ba
d88b    88      d8''    "8b      d88b    d8"    "8b      d88b    88      "8b
d8' '8b  88      d8'    '8b      d8' '8b     8,      d8' '8b    88      ,8P
d8' '8b  88      88      d8' '8b     '8aaaaaa,   d8' '8b    88aaaaaa8P'
d8YaaaaY8b 88      88      d8YaaaaY8b     '8b,      d8YaaaaY8b  88""""8b'
d8""""8b  88      88      d8""""8b     '8b      d8""""8b  88      '8b
d8'      '8b  88      88a.    .a8P d8'      '8b  88a.    a8P d8'      '8b  88      '8b
d8'      '8b  88      88     "88888Y" d8'      '8b  "88888P" d8'      '8b  88      '8b
d8'      '8b  888888888888  "88888Y" d8'      '8b  "88888P" d8'      '8b  88      '8b

Bienvenue sur ALCASAR Version 3.6.1 (Mageia 8)
Connectez-vous à l'URL 'https://alcasar.localdomain/acc'
Kernel 5.15.126-server-1.mga8 on a Dual-processor x86_64 / tty1
alcasar login: root
Password:
Last login: Wed Jun 26 10:14:15 on tty1
alcasar-laplateforme[~]#

```

Vous pouvez vérifier que tous les composants d'ALCASAR sont bien lancés en tapant la commande alcasar-daemon.sh

```

db      88      ,ad8888ba,      db      ad88888ba      db      88888888ba
d88b    88      d8''    "8b      d88b    d8"    "8b      d88b    88      "8b
d8' '8b  88      d8'    '8b      d8' '8b     8,      d8' '8b    88      ,8P
d8' '8b  88      88      d8' '8b     '8aaaaaa,   d8' '8b    88aaaaaa8P'
d8YaaaaY8b 88      88      d8YaaaaY8b     '8b,      d8YaaaaY8b  88""""8b'
d8""""8b  88      88      d8""""8b     '8b      d8""""8b  88      '8b
d8'      '8b  88      88a.    .a8P d8'      '8b  88a.    a8P d8'      '8b  88      '8b
d8'      '8b  88      88     "88888Y" d8'      '8b  "88888P" d8'      '8b  88      '8b
d8'      '8b  888888888888  "88888Y" d8'      '8b  "88888P" d8'      '8b  88      '8b

Bienvenue sur ALCASAR Version 3.6.1 (Mageia 8)
Connectez-vous à l'URL 'https://alcasar.localdomain/acc'
Kernel 5.15.126-server-1.mga8 on a Dual-processor x86_64 / tty1
alcasar login: root
Password:
Last login: Wed Jun 26 10:14:15 on tty1
alcasar-laplateforme[~]# alcasar-daemon.sh_

```

Last login: Wed Jun 26 10:14:15 on tty1
alcasar-laplateforme[~]# alcasar-daemon.sh
18 services needed by ALCASAR are started.
The Log system is active
alcasar-laplateforme[~]#

Vérifions les cartes réseaux :

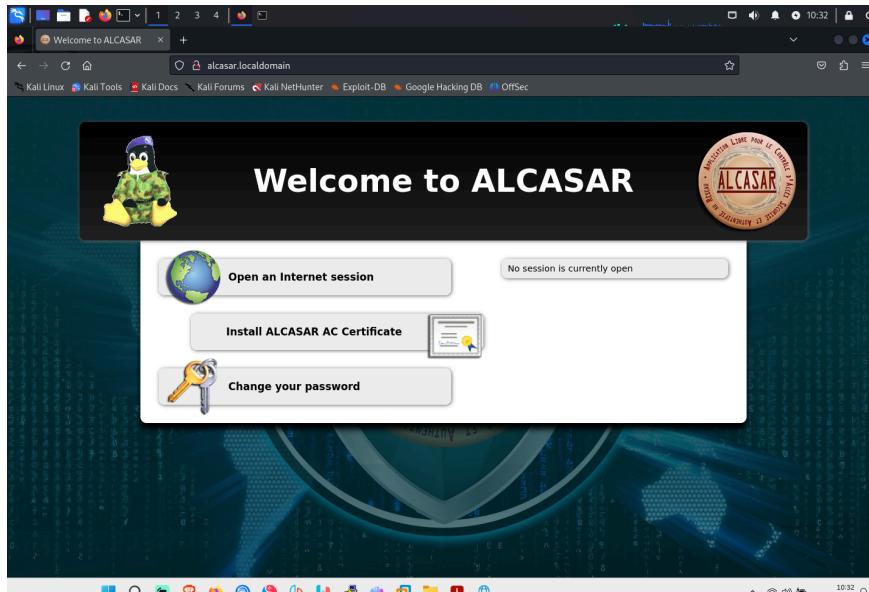
```

alcasar-laplateforme[~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
  link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
  inet 127.0.0.1/8 scope host lo
    valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
  link/ether 00:0c:29:16:62:b8 brd ff:ff:ff:ff:ff:ff
  altname emp2s1
  inet 192.168.126.131/24 brd 192.168.126.255 scope global ens33
    valid_lft forever preferred_lft forever
3: ens34: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
  link/ether 00:0c:29:16:62:c2 brd ff:ff:ff:ff:ff:ff
  altname emp2s2
4: tun0: <POINTPOINT,UP,LOWER_UP> mtu 1500 qdisc mq state UNKNOWN group default qlen 100
  link/none
  inet 192.168.182.254/24 scope global tun0
    valid_lft forever preferred_lft forever

```

Configuration d'un portail captif par défaut :

Démarrer la VM client puis tapez l'ip serveur alcasar sa affiche la page de connexion



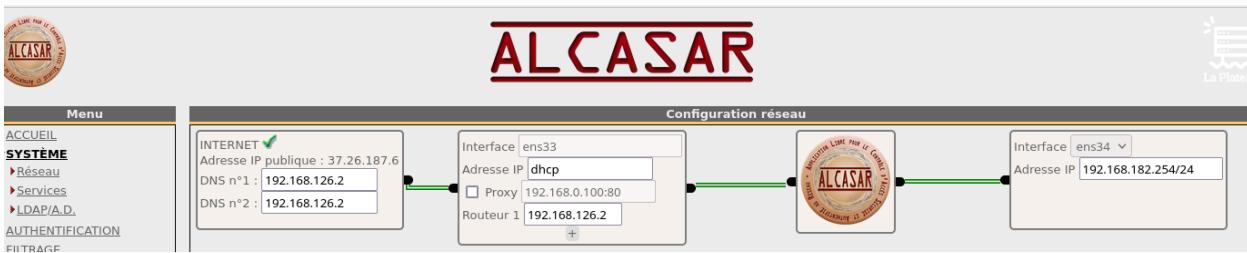
Pour accéder à la page de configuration faut rentrer son Utilisateur et son mot de passe

admin et x

on remarque un défaut routeur

A screenshot of the ALCASAR Control Center (ACC) web interface. At the top right is the ALCASAR logo. The left sidebar has a 'Menu' section with 'ACCUEIL' (selected), 'SYSTÈME' (expanded), and 'Réseau'. The main content area displays system status: 'Accès Internet : LAN ✓ Routeur ✗ DNS ✓', 'Version instalée : 3.6.1', and 'Version disponible : 3.6.1'. On the right side, there are links for 'Nombre d'utilisateurs', 'Nombre de groupes', and 'Date du système : v'.

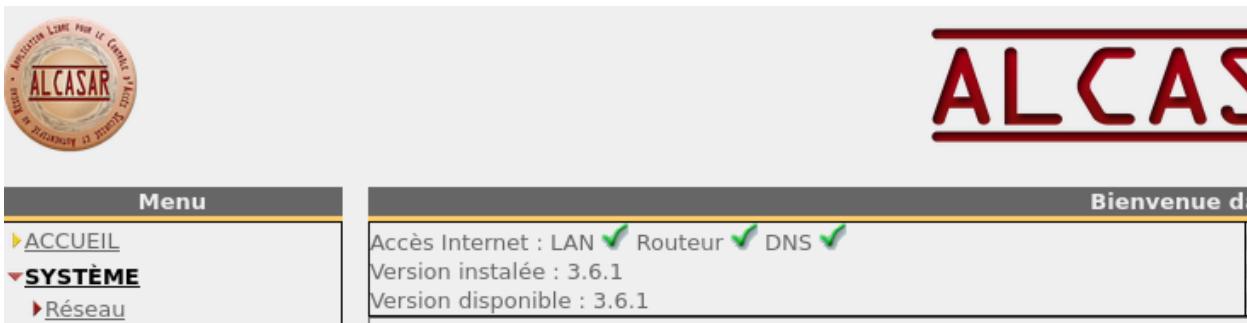
dans **Réseau** faut activer la **passerelle** faut y mettre l'adresse **DNS** dans **Routeur 1**



Ne pas oublier d'**appliquer les changements**

Appliquer les changements

on à **résolu** le pb de la **passerelle**



Informations système : localhost (192.168.182.254)

SYSTÈME		INFORMATIONS MATÉRIEL	
Nom d'hôte canonique	localhost	Machine	VMware, Inc. VMware Virtual Platform/440BX Desktop Reference Platform, BIOS 6.00 11/12/2020
Adresse IP	192.168.182.254	Virtualizer	vmware
Version du noyau	5.15.126-server-1.mga8 (SMP) x86_64	Processeurs	Intel(R) Core(TM) i7-10750H CPU @ 2.60GHz, Intel(R) Core(TM) i7-10750H CPU @ 2.60GHz
Distribution	Mageia 8	Pérophériques PCI	
OS Type	Linux	Pérophériques SCSI	
Durée d'activité	47 minutes	Pérophériques USB	
Dernier démarrage	Fri, 28 Jun 2024 07:08:52 GMT		
Utilisateurs	0		
Charge système	0.13 0.07 0.01 0%		
Langue du système	French France (fr_FR)		
Codage de la page	UTF-8		
Processus	216 (3 running, 137 sleeping, 76 autre)		

UTILISATION MÉMOIRE				
Type	Utilisation	Libre	Occupé	Taille
Mémoire physique	50%	3.84 Gio	3.90 Gio	7.74 Gio
Swap disque	0%	4.00 Gio	0 B	4.00 Gio

SYSTÈMES DE FICHIERS MONTÉS						
Point de montage	Type	Partition	Utilisation	Libre	Occupé	Taille
/	ext4	/dev/sda1 (rw, noatime)	21% (4%)	20.13 Gio	3.97 Gio	25.42 Gio
		Totaux	20.81%	20.13 Gio	3.97 Gio	25.42 Gio

RÉSEAU			
Périphérique	Réception	Envoi	Err/Drop
+ens33	33.75 Mio (223.30 B/s)	2.23 Mio (120.33 B/s)	0/0
+ens34	3.33 Mio (447.52 B/s)	39.67 Mio (1.00 Kio/s)	0/0

Les services :

Services principaux						
Status	chilli	Rôle du service			Actions	
✓	radiusd	Passerelle d'interception et serveur DHCP			---	Redémarrer
✓	mysqld	Serveur d'authentification et d'autorisation			---	Arrêter Redémarrer
✓	lighttpd	Serveur WEB (Alcasar Control Center)			---	Arrêter Redémarrer
✓	unbound	Serveur DNS principal			---	Arrêter Redémarrer
✓	nfcapd	Collecteur de flux NetFlow			---	Arrêter Redémarrer
✓	ulogd_ssh	journalisation des accès par SSH			---	Arrêter Redémarrer
✓	ulogd_ext_access	journalisation des tentatives d'accès externes			---	Arrêter Redémarrer
✓	ulogd_traceability	journalisation des connexions WEB filtrés			---	Arrêter Redémarrer
✓	sshd	Accès sécurisée distant			---	Arrêter Redémarrer
✓	ntp	Service de mise à l'heure réseau			---	Arrêter Redémarrer
✓	fail2ban	Détecteur d'intrusion			---	Arrêter Redémarrer
✓	vnstat	Grapher de flux réseau			---	Arrêter Redémarrer
✓	postfix	Service de messagerie			---	Arrêter Redémarrer
Services de filtrage						
Status	unbound_blacklist	Rôle du service			Actions	
✓	unbound_whitelist	Serveur DNS pour la Blacklist			---	Arrêter Redémarrer
✓	unbound_blackhole	Serveur DNS pour la Whitelist			---	Arrêter Redémarrer
✓	e2guardian	Serveur DNS 'trou noir'			---	Arrêter Redémarrer
		Filtre d'URL et de contenu WEB			---	Arrêter Redémarrer
Services optionnels						
Status	WIFI4EU Entrez votre identifiant réseau : <input type="text" value="123e4567-e89b-12d3-a456-426655440000"/>			Démarrer	---	---
Arrêt et redémarrage du système						
Relancer le système	Exécuter					

Créez un utilisateur sous interface ALCASAR :

▼ AUTHENTICATION

- ▶ [Activity](#)
- ▶ [Create users](#)

remplir:

Login, password au minimum => cliquez sur

[Create](#)

Create a user

Login	<input type="text"/>
Password	<input type="password"/> generate <input type="text"/>
Group	The group list is empty
Surname and name	<input type="text"/>
Email Address	<input type="text"/>
Expiration date	<input type="text"/>
Number of simultaneous sessions	<input type="text"/>
Domain name Filtering	<input type="text"/>
Network protocols filtering	<input type="text"/>
Keeping sessions alive	<input type="text"/>
Voucher language	<input type="text"/> Français

[Create](#) [Advanced menu](#)

Or :

[Create several tickets](#)

Note: when creating multiple tickets simultaneously :
- username and password are randomly generated,
- fields "Surname and name" and "Email Address" are not used.

Utilisateur Créez :

Users management

Create a user

User 'aurore' has been correctly created

[Create a ticket \(voucher\)](#)

[Show profile](#)

clique sur **show profile**

Status	Attributes	Personal Informations
Connections	Remove	Open Sessions
User : aurore (-)		
This user has never logged in	-	
Remain connection time	The user can log in during unlimited time	

Check Password

Password

Analyse

	total	monthly	weekly	daily	by session
limit	none	none	none	none	none
Used time	0 seconds	-	0 seconds	0 seconds	-
Day	daily limit			Used time	
sunday	none			0 seconds	
monday	none			0 seconds	
tuesday	none			0 seconds	
wednesday	none			0 seconds	
thursday	none			0 seconds	
friday	none			0 seconds	
saturday	none			0 seconds	

Last 7 days status

On peut voir les logs des utilisateurs qui sont soit d'**ALCASAR** ou bien ceux inscrits sous **LDAP**:

Connections log							
Client IP Address	Upload	Group Name	Login Time	Logout Time	Session Time	Download	User Name
192.168.182.2	284.95 Kbs	-	2024-07-03 10:33:04	2024-07-03 15:09:55	02:10:07	328.64 Kbs	amandine
192.168.182.2	2.66 Kbs	-	2024-07-03 10:32:23	2024-07-03 10:32:55	00:00:32	9.86 Kbs	amandine
192.168.182.2	8.58 Kbs	-	2024-07-03 10:28:05	2024-07-03 10:32:02	00:03:57	14.09 Kbs	thierry
192.168.182.2	16.19 Kbs	-	2024-07-03 10:22:40	2024-07-03 10:27:52	00:05:12	23.69 Kbs	amandine
192.168.182.2	26.34 Kbs	-	2024-07-03 10:16:43	2024-07-03 10:22:17	00:05:34	65.70 Kbs	aurore
192.168.182.2	118.83 Kbs	-	2024-07-03 09:40:50	2024-07-03 10:00:03	00:19:13	507.50 Kbs	thierry
192.168.182.2	1.55 Kbs	-	2024-07-03 09:40:02	2024-07-03 09:40:02	00:00:00	2.10 Kbs	thierry
192.168.182.2	160.40 Kbs	-	2024-07-02 09:06:26	2024-07-02 09:23:25	00:16:59	1.26 MBs	amandine
192.168.182.2	0.57 MBs	-	2024-07-02 09:02:07	2024-07-02 09:03:55	00:01:48	37.03 MBs	laurent
192.168.182.2	425.21 Kbs	-	2024-07-02 08:55:48	2024-07-02 09:00:43	00:04:55	10.22 MBs	thierry
192.168.182.3	68.01 Kbs	-	2024-06-28 10:53:39	2024-06-28 11:08:38	00:15:00	355.82 Kbs	amandine
192.168.182.2	7.41 MBs	-	2024-06-28 10:11:42	2024-07-01 07:57:09	04:55:13	290.48 MBs	amandine
192.168.182.2	2.08 MBs	-	2024-06-28 09:20:53	2024-06-28 09:42:19	00:21:26	33.76 MBs	amandine

LDAP

Le protocole **LDAP** est très souvent utilisé pour centraliser l'accès aux services d'annuaires et leur gestion.

Il permet aux entreprises de stocker, gérer et sécuriser leurs informations et celles de leurs utilisateurs ainsi que d'autres ressources telles que les noms d'utilisateurs .



Authentification LDAP

Éditer la configuration LDAP:

Serveur LDAP: Adresse IP du serveur	<input type="text" value="127.0.0.1"/> NON <input type="button" value="Assistant"/>
Connexion chiffrée: Utiliser une connexion chiffré avec SSL (LDAPS)	<input type="button" value="OUI"/>
Vérifier le certificat SSL: Vérifier que le serveur LDAP utilise un certificat connu	<input type="button" value="NON"/>
Certificat SSL (CA): Certificat de l'autorité de certification signant celui du serveur LDAP Aucun certificat installé	<input type="button" value="Parcourir..."/> Aucun fichier sélectionné.
CN de l'utilisateur exploité par ALCASAR: CN=Common Name. Laissez vide pour utiliser un accès invité (ou anonyme). Obligatoire sur un AD. - Exemple LDAP : 'uid=username,ou=my_lan,o=mycompany,c=FR'. - Exemple AD : 'username' ou 'cn=username,cn=Users,dc=server_name,dc=localdomain'	<input type="text" value="alcasar"/>
Mot de passe: Laissez vide pour un accès invité (ou anonyme). Obligatoire sur un AD.	<input type="password"/>
DN de la base: Le DN (Distinguished Name) définit où se situent les informations des utilisateurs dans l'annuaire. - Exemple LDAP: 'o=mycompany, c=FR'. - Exemple AD 'cn=Users,dc=server_name,dc=localdomain'	<input type="text" value="cn=Users;dc=serverad;dc=localdomain"/>
Identifiant d'utilisateur (UID): Clé utilisée pour rechercher un identifiant de connexion. - Exemple LDAP: 'uid', 'sn', etc. - Pour A.D. mettre 'sAMAccountName'.	<input type="text" value="sAMAccountName"/>
Filtre de recherche des utilisateurs (optionnel): Vous pouvez limiter les objets recherchés avec des filtres additionnels. Exemple 'objectClass=posixGroup' ajouterait le filtre '(&(uid=username)(objectClass=posixGroup))'	<input type="text"/>
Nom de domaine interne: Nom de domaine qui sera redirigé vers le serveur DNS de l'annuaire LDAP (vide pour désactivé)	<input type="text"/>

Pour configurer le serveur **LDAP** on a **Open LDAP** faut installer :

apt-get install slapd ldap-utils

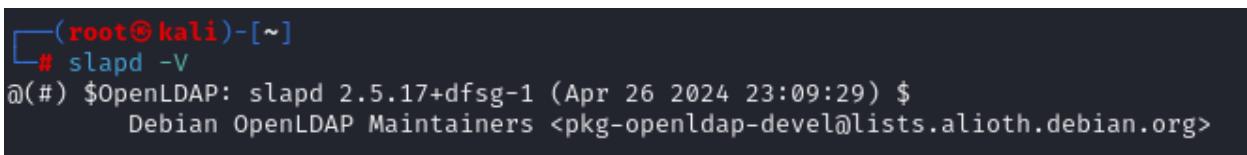
```
(root㉿kali)-[~] # apt-get install slapd ldap-utils
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
ldap-utils is already the newest version (2.5.17+dfsg-1).
ldap-utils set to manually installed.
The following packages were automatically installed and are no longer required:
  appstream-adaptor apt-config-icons-hidpi apt-config-icons-large apt-config-large hidpi fwupd jq kde-config-updates libabsl20220623 libbadwaita-1-0 libbaio1
  libbatik-adaptor libboost-dev libboost1.83-dev libdabxctl1 libfwupd2 libgphoto2-l10n libjcat1 libmarkdown2 libndctl16 libpns1-dev libopenblas-dev libopenblas-pthread-dev
  libopenblas1 libmemomi libpthread-stubs0-dev libpython3-all-dev libpython3.12-dev libpython3.12 libqt5webview5 libtirpc-dev libunibreak5 libxsimd-dev
  linux-image-6.6.9-amd64 plasma-discover-common python3-all-dev python3-anyjson python3-beniget python3-editables python3-gast python3-httplib2 python3-lzr.restfulclient
  python3-lazr.uri python3-mistune0 python3-oauthlib python3-pyatspi python3-pypdf2 python3-pypeteer python3-persistent python3-pytrhan python3-software-properties
  python3-wadllib python3.12-dev vlc-110m xtl-dev zenity zenity-common
Use 'apt autoremove' to remove them.
The following additional packages will be installed:
  libdb5.3 libgdbm-compat4 libgdbm6 libpam-modules libpam-modules-bin libperl5.38t64 perl perl-base
Suggested packages:
  gdm-1l0n perl-doc libterm-readline-gnu-perl | libterm-readline-perl-perl libtap-harness-archive-perl libsasl2-modules-gssapi-mit | libsasl2-modules-gssapi-heimdal
The following packages will be REMOVED:
  libdb5.3 libgdbm-compat4 libgdbm6 libperl5.38t64
The following NEW packages will be installed:
  libdb5.3t64 libgdbm-compat4 libgdbm6 libperl5.38t64 slapd
The following packages will be upgraded:
  libpam-modules libpam-modules-bin perl perl-base
4 upgraded, 5 newly installed, 4 to remove and 71 not upgraded.
Need to get 8736 kB of archives.
After this operation, 4764 kB of additional disk space will be used.
```

Pour continuer l'installation faut mettre en place le password admin = **X**

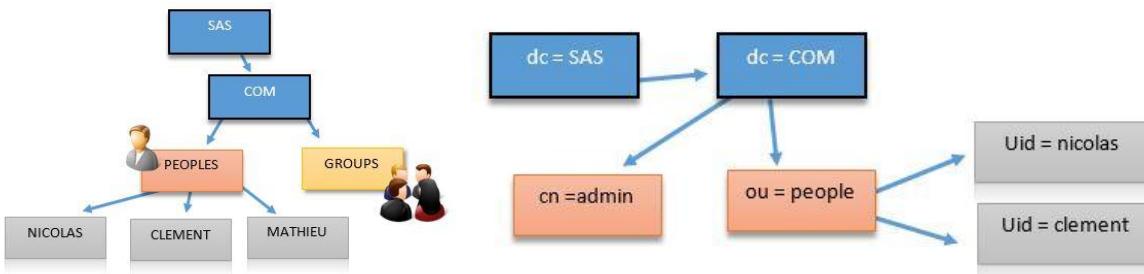


puis laissez finir l'installation tapez => **slapd -V**

permet de voir si l'installation c'est bien passé !!

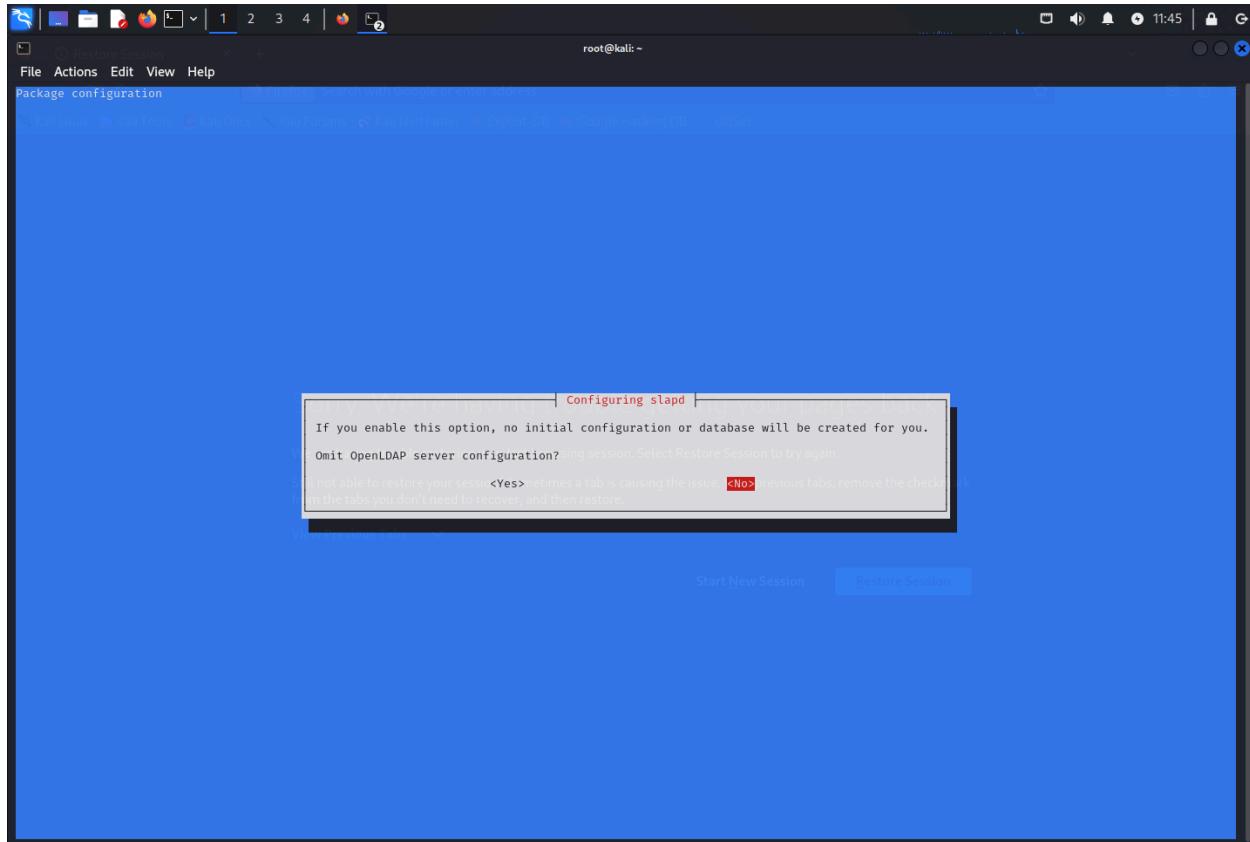


Configurer l'annuaire :



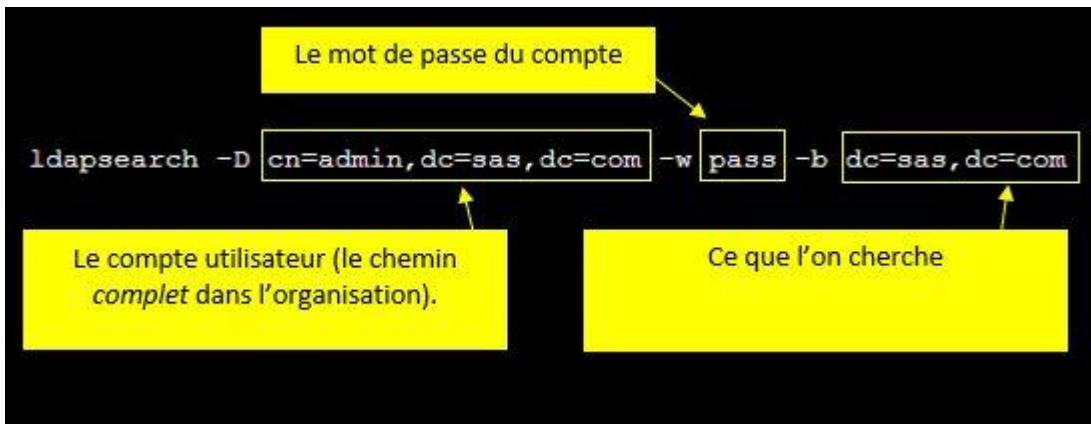
utiliser l'outil dpkg-reconfigure

```
(root㉿kali)-[~]
# dpkg-reconfigure slapd
```



une fois avoir rempli le nom du domaine = **alca.local** et le mot de passe = **x**

```
(root㉿kali)-[~]
# dpkg-reconfigure slapd
Backing up /etc/ldap/slapd.d in /var/backups/slapd-2.5.17+dfsg-1 ... done.
Moving old database directory to /var/backups:
- directory unknown ... done.
Creating initial configuration ... done.
Creating LDAP directory ... done.
```



Démarrez le serveur **LDAP** =>

```
(root@kali)-[~]
# systemctl enable slapd
```

Important : [systemctl enable slapd] ça démarre le serveur automatique à chaque session en revanche si on démarre le serveur avec [systemctl start slapd] à chaque démarrage du serveur il sera éteint faudra l'activer manuellement.

vérifier le status du serveur=[**systemctl status slapd**]

```
(root@kali)-[/etc/ldap]
# 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 Fri 2024-06-28 14:39:44 CEST; 14s ago
   Invocation: 9cb5cd6b821d4f50832bd4b25183fe25
     Docs: man:systemd-sysv-generator(8)
   Process: 189233 ExecStart=/etc/init.d/slapd start (code=exited, status=0/SUCCESS)
   Tasks: 3 (limit: 4907)
   Memory: 7.2M (peak: 7.7M)
     CPU: 28ms
   CGroup: /system.slice/slapd.service
           └─189256 /usr/sbin/slapd -h "ldap:/// -g openldap -u openldap -F /etc/ldap/slapd.d
```

*pour vérifier que votre LDAP est bien configuré tapez = **SLAPCAT**

```
└─(root㉿kali)-[~/etc/ldap]
└─# slapcat
dn: dc=alca,dc=local
objectClass: top
objectClass: dcObject
objectClass: organization
o: alca.local
dc: alca
structuralObjectClass: organization
entryUUID: df09a560-c981-103e-8112-1942b5ea696b
creatorsName: cn=admin,dc=alca,dc=local
createTimestamp: 20240628100646Z
entryCSN: 20240628100646.097579Z#000000#000#000000
modifiersName: cn=admin,dc=alca,dc=local
modifyTimestamp: 20240628100646Z
```

sécurisez le serveur avec [UFW](#)

```
└─(root㉿kali)-[~/etc/ldap]
└─# ufw allow openSSH
Rules updated
Rules updated (v6)
```

activer le [firewall](#)

```
└─(root㉿kali)-[~/etc/ldap]
└─# ufw enable
Firewall is active and enabled on system startup
```

pour éviter les doutes lors de l'install “[desactiver le Firewall](#)”

```
└─(root㉿kali)-[~/etc/ldap]
└─# ufw disable
Firewall stopped and disabled on system startup
```

Exemple d'Organigramme:

The screenshot shows the VC LDAP Server interface. At the top, there are several icons: schema, search, refresh, info, import, export, and disconnect. Below the icons, the text "schéma rechercher rafraîchir info importer exporter se déconnecter" is displayed. Underneath that, it says "Connecté en tant que :: cn=admin,dc=maison,dc=chezrami,dc=fr". The main pane displays the LDAP tree structure:

- dc=maison, dc=chezrami, dc=fr (2)**
 - ou=dhcp (2)**
 - ou=dns (5)**
 - dc=localhost
 - dc=maison
 - dc=mirror.deb
 - ou=OVH (3)**
 - dc=srv4.ovh
 - dc=srv6.ovh
 - dc=srv7.ovh
 - ★ Créez une nouvelle entrée ici
 - ou=pve (4)**
 - dc=pve1_10
 - dc=pve1_2.5
 - dc=pve2_10
 - dc=pve2_2.5
 - ★ Créez une nouvelle entrée ici
 - ★ Créez une nouvelle entrée ici
 - ★ Créez une nouvelle entrée ici

Configurer le Group “people”

faut d'abord créer le fichier “people”

nano people.ldif

```
File Actions Edit View Help
GNU nano 8.0
dn: ou=People,dc=alca,dc=local
objectClass: organizationalUnit
ou: People
```

Ligne de commande pour ajouter le Groups “people”

```
[root@kali]~[/etc/ldap]
# ldapadd -x -D "cn=admin,dc=alca,dc=local" -w -f people.ldif
Enter LDAP Password:
adding new entry "ou=People,dc=alca,dc=local"
```

avec **slapcat** on peut vérifier le fichier configurer **people.ldif**

```
[root@kali]~[/etc/ldap]
# slapcat
dn: dc=alca,dc=local
objectClass: top
objectClass: dcObject
objectClass: organization
o: alca.local
dc: alca
structuralObjectClass: organization      We are having trouble
entryUUID: df09a560-c981-103e-8112-1942b5ea696b
creatorsName: cn=admin,dc=alca,dc=local Still not able to read from the tabs you
createTimestamp: 20240628100646Z          from the tabs you
entryCSN: 20240628100646.097579Z#000000#000#000000
modifiersName: cn=admin,dc=alca,dc=local
modifyTimestamp: 20240628100646Z          View Previous Tab

dn: ou=People,dc=alca,dc=local
objectClass: organizationalUnit
ou: People
structuralObjectClass: organizationalUnit
entryUUID: 52e9ec44-c999-103e-8ac9-973c6a381620
creatorsName: cn=admin,dc=alca,dc=local
createTimestamp: 20240628125438Z
entryCSN: 20240628125438.930196Z#000000#000#000000
modifiersName: cn=admin,dc=alca,dc=local
modifyTimestamp: 20240628125438Z
```

Ajouter les utilisateurs

Créer le fichier `nouvelle_utilisateur.ldif`

```
└─(root㉿kali)-[~/etc/ldap]
└─# nano nouvelle_utilisateur.ldif

FILE ACTIONS Edit View Help
GNU nano 8.0
dn: uid=laurent,ou=people,dc=alca,dc=local
objectClass: inetOrgPerson
uid: laurent
sn: Laurent
givenName: Voulzy
cn: Laurent Voulzy
displayName: Laurent Voulzy
userPassword:x
```

insérez les utilisateurs dans la base du serveur **LDAP** :

```
└─(root㉿kali)-[~/etc/ldap]
└─# ldapadd -x -D "cn=admin,dc=alca,dc=local" -W -f nouvelle_utilisateur.ldif
Enter LDAP Password:
adding new entry "uid=laurent,ou=people,dc=alca,dc=local"
```

en cas de détresse faire appel à : **man ldapadd**

```
└─(root㉿kali)-[~/etc/ldap]
└─# man ldapadd
```

IMPORTANT:

Pour inscrire un autre utilisateur sous ldap alors que le fichier utilisateur a été déjà lu il faut taper cette commande en y rajoutant **-c** :

```
└─(root㉿kali)-[~/etc/ldap]
└─# ldapadd -x -D cn=admin,dc=alca,dc=local -W -c -f nouvelle_utilisateur.ldif
Enter LDAP Password:
```

et si les utilisateurs sont déjà lus ils seront pris en compte sinon sans cette commande **-c** ils ne seront pas lus pour être rajoutés dans la base de données de LDAP.

Pour avoir un password en **SSHA** faut taper:

SLAPPASSWD

```
[# slappasswd  
New password: ]
```

on obtient la **clef SSHA** que l'on doit rajouter dans le script **nouvelle_utilisateur.ldif**

```
[# slappasswd  
New password: [REDACTED] Kali Tools Kali Docs Kali  
Re-enter new password: [REDACTED]  
{SSHA}LauIOY0yfNtrw/09uqG8IgBbVI7lsFrL
```

on doit ajouter la clé **SSHA**:

```
dn: uid=thierry,ou=People,dc=alca,dc=local  
objectClass: inetOrgPerson  
objectClass: posixAccount  
objectClass: shadowAccount  
cn: thierry  
sn: Ramion  
userPassword: {SSHA}e5n5Jy5z6SCmXMxTlY3yIgrzmSQc8m35  
loginShell: /bin/false  
uidNumber: 2001  
gidNumber: 2001  
homeDirectory: /home/thierry  
shadowLastChange: 0  
shadowMax: 0  
shadowWarning: 0  
  
dn: cn=thierry,ou=Groups,dc=alca,dc=local  
objectClass: posixGroup  
cn: thierry  
gidNumber: 2001  
memberUid: thierry
```

Pour vérifier les utilisateurs ajouter faire : **SLAPCAT**

```
[root@kali]~[/etc/ldap]
# slapcat
dn: dc=alca,dc=local
objectClass: top
objectClass: dcObject
objectClass: organization
o: alca.local
dc: alca
structuralObjectClass: organization
entryUUID: df09a560-c981-103e-8112-1942b5ea696b
creatorsName: cn=admin,dc=alca,dc=local
createTimestamp: 20240628100646Z
entryCSN: 20240628100646.097579Z#000000#000#000000
modifiersName: cn=admin,dc=alca,dc=local
modifyTimestamp: 20240628100646Z

dn: ou=People,dc=alca,dc=local
objectClass: organizationalUnit
ou: People
structuralObjectClass: organizationalUnit
entryUUID: 52e9ec44-c999-103e-8ac9-973c6a381620
creatorsName: cn=admin,dc=alca,dc=local
createTimestamp: 20240628125438Z
entryCSN: 20240628125438.930196Z#000000#000#000000
modifiersName: cn=admin,dc=alca,dc=local
modifyTimestamp: 20240628125438Z

dn: uid=laurent,ou=People,dc=alca,dc=local
objectClass: inetOrgPerson
uid: laurent
sn: Laurent
givenName: Voulzy
cn: Laurent Voulzy
displayName: Laurent Voulzy
userPassword:: eA==
structuralObjectClass: inetOrgPerson
entryUUID: 93322ff0-c999-103e-8aca-973c6a381620
creatorsName: cn=admin,dc=alca,dc=local
createTimestamp: 20240628125626Z
entryCSN: 20240628125626.777950Z#000000#000#000000
modifiersName: cn=admin,dc=alca,dc=local
modifyTimestamp: 20240628125626Z

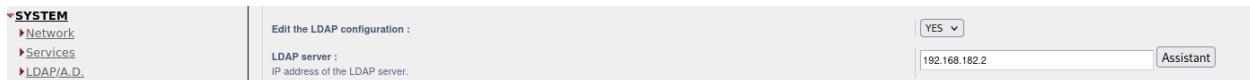
dn: uid=thierry,ou=People,dc=alca,dc=local
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: thierry
sn:: UmFtaQkJ
userPassword:: e1NTSEF9ZTVuNUp5NXo2U0NtWE14VGxZM3lJZ3J6bVNRYzhtMzU=
```

Configurer le DNS et la liaison entre le serveur ALCASAR et la base de données LDAP:

Dans **SYSTEM** on accède au réglage pour configurer l'accès au **base de données LDAP**

Cliquez sur : **YES**

Mettre l'adresse IP du serveur LDAP : **192.168.182.2**



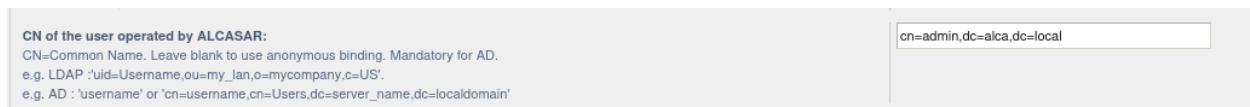
YES

LDAP server : 192.168.182.2

Assistant

et remplir le

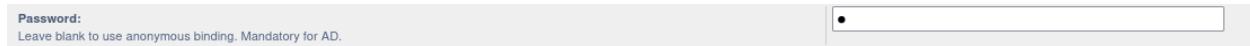
CN : cn=admin,dc=alca,dc=local



cn=admin,dc=alca,dc=local

CN of the user operated by ALCASAR:
CN=Common Name. Leave blank to use anonymous binding. Mandatory for AD.
e.g. LDAP : 'uid=Username,ou=my_lan,o=mycompany,c=US'.
e.g. AD : 'username' or 'cn=username,cn=Users,dc=server_name,dc=localdomain'

Mot de passe : X



>Password:
Leave blank to use anonymous binding. Mandatory for AD.

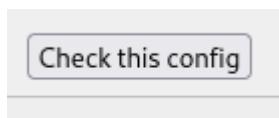
DN of the base : ou=People,dc=alca,dc=local



ou=People,dc=alca,dc=local

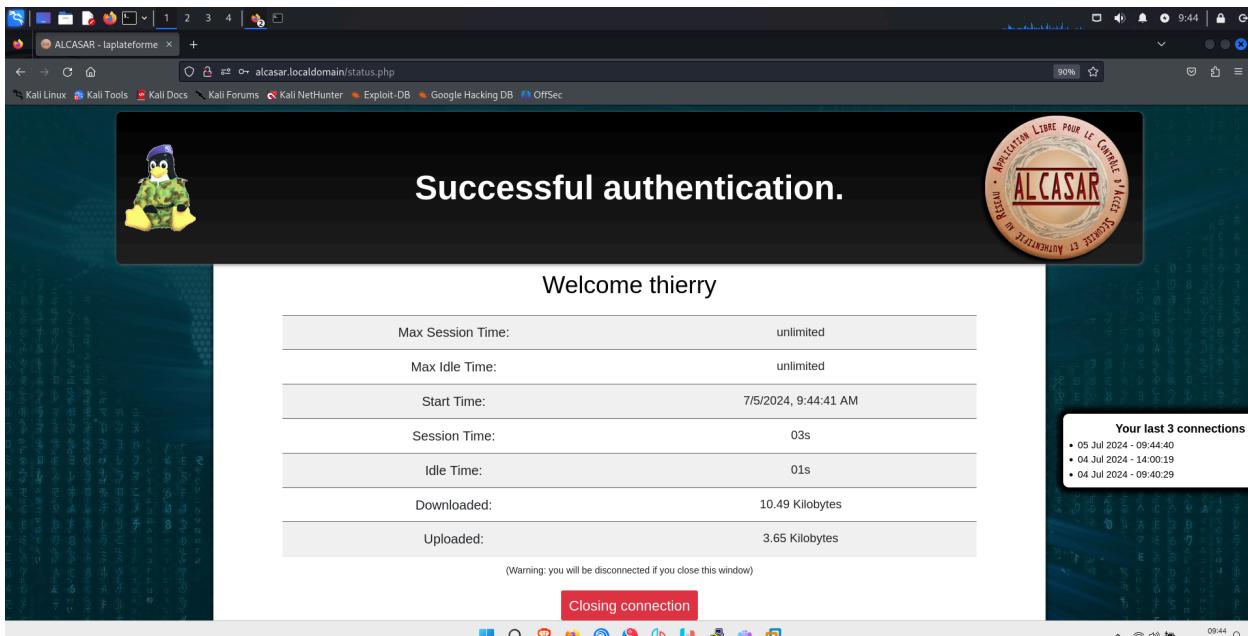
DN of the base:
The DN (Distinguished Name) is used to locate the users information in the directory.
e.g. LDAP : 'o=MyCompany,c=US'.
e.g. AD : 'cn=Users,dc=server_name,dc=localdomain'

confirmez:



Check this config

Une fois que l'on à créeé l'utilisateur sous **LDAP** et que l'on a connecter à **ALCASAR** on vérifie que l'utilisateur **enregistré est opérationnel** en se **connectant** :



Configurer la surveillance du trafic réseau:

pour détecter toute activité suspecte ou malveillante par les log

Main

- HOME
- SYSTEM
- AUTHENTICATION
- FILTERING
- STATISTICS
 - By connection
 - Connection
 - Daily use
 - Global traffic
 - Security

Connections log

Client IP Address	Upload	Group Name	Login Time	Logout Time	Session Time	Download	User Name
192.168.182.2	302.80 Kbs	-	2024-07-05 09:44:40	2024-07-04 14:23:07	02:15:07	365.10 Kbs	thierry
192.168.182.2	244.41 Kbs	-	2024-07-04 14:23:07	2024-07-04 15:00:02	00:36:55	1.41 MBs	laurent
192.168.182.2	0.91 MBs	-	2024-07-04 14:00:19	2024-07-04 14:21:34	00:21:15	9.10 MBs	thierry
192.168.182.2	93.76 Kbs	-	2024-07-04 09:40:29	2024-07-04 09:42:11	00:01:42	3.34 MBs	thierry

AUTHENTICATION

Activity	192.168.182.2	00-0C-29-4E-FD-43 (vMware) - LDAP	thierry	Disconnect
Create users	192.168.182.1	00-0C-29-16-62-C2 (vMware)	ALCASAR system	
Manage users				

Filtrage de ALCASAR:

FILTRAGE:

Liste Noire:

Main

Download the last version | (Estimated time : one minute)

Main BlackList

4960177 Domain names : 20180 URL: 78473 IP :

Select the categories to filter

adult	associations_religieuses	astrology	audio-video	bank	bitcoin	blog	celebrity	chat	child
<input type="checkbox"/>									
cleaning	cooking	dating	dialer	download	educational_games	examen_pix	exceptions_liste_bu	filehosting	financial
<input type="checkbox"/>									
forums	games	jobsresearch	gambling	late_bu	manga	mobile-phone	news	publicite	radio
<input type="checkbox"/>									
radio	infected	sexual_education	shopping	shortener	social_networks	special	sports	stalkerware	translation
<input type="checkbox"/>									
update	von	webmail	adult	agressif	cryptojacking	dangerous_material	malware	noob	ougue
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
gambling	hacking	malware	marketingware	mixed_adult	phishing	redirector	remote-control	sext	strict_redirector
<input checked="" type="checkbox"/>									
strong_redirector	tricheur	warez							
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>							

[Save changes]

Domain names to rehabilitated

Enter here domain names that are blocked by the blacklist
and you want to rehabilitate.
Enter one DNS per row (example : www.domain.com)

IP addresses to rehabilitated

Enter here IP that are blocked by the blacklist
and you want to rehabilitate.
Enter one IP per row (example : 123.123.123.123)

Domain names or IP addresses to add to the blacklist

Enter one domain name or one IP address or one network address per row
example (domain): domain.org. - example (ip): 61.54.56.52 - example (network) : 172.16.0.0/16

Save changes |

Liste Blanche :

Main WhiteList

Actualmente están autorizados los siguientes : 29522 domain names, 0 URL, 0 IP@

Select the allowed categories

adult	agressif	ariel	associations_religieuses	astrology	audio-video	bitcoin	blog	celebrity	chat
<input type="checkbox"/>									
cooking	cryptojacking	dangerous_material	dating	ddos	dialer	doh	drogue	examen_pix	exceptions_liste_bu
<input type="checkbox"/>									
fakenews	filehosting	financial	forums	gambling	games	hacking	lingerie	malware	manga
<input type="checkbox"/>									
marketingware	mixed_adult	mobile-phone	phishing	publicite	radio	reaffected	redirector	remote-control	residential-proxies
<input type="checkbox"/>									
sext	shopping	social_networks	special	sports	stalkerware	strict_redirector	strong_redirector	tricheur	tricheur_pix
<input type="checkbox"/>									
von	warez	webmail	bank	child	cleaning	download	educational_games	jobssearch	liste_blanche
<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
late_bu	press	sexual_education	shortener	translation	update				
<input checked="" type="checkbox"/>									

Domain names or IP addresses to add to the whitelist

Enter one domain name or one IP address or one network address per row
example (domain): domain.org. - example (ip): 61.54.56.52 - example (network) : 172.16.0.0/16

Protocoles:

Custom network protocols filter

You can define here the custom network protocols filtering. Then, You can assign it to a user (see)

Port number	protocol name	Authorized	Remove from list
-	icmp	<input type="checkbox"/>	<input type="checkbox"/>
22	ssh	<input type="checkbox"/>	<input type="checkbox"/>
25	smtp	<input type="checkbox"/>	<input type="checkbox"/>
80	http	<input type="checkbox"/>	<input type="checkbox"/>
110	pop	<input type="checkbox"/>	<input type="checkbox"/>
143	imap2	<input type="checkbox"/>	<input type="checkbox"/>
220	imap3	<input type="checkbox"/>	<input type="checkbox"/>
443	https	<input type="checkbox"/>	<input type="checkbox"/>
631	ipp	<input type="checkbox"/>	<input type="checkbox"/>
993	imaps	<input type="checkbox"/>	<input type="checkbox"/>
995	pop3s	<input type="checkbox"/>	<input type="checkbox"/>

[Save changes]

Génération de Rapports:

sous nano on fait n' importe quoi !!!

et on s' en fiche ! 😊

```
root@alcasar:~/alcasar-3.6.1
GNU nano 5.4
#Configuration
LDAP SERVER="ldap://192.168.182.2"
BASE DN="ou=People,dc=alca,dc=local"
ADMIN DN="cn=admin,dc=alca,dc=local"
ADMIN PASSWORD="x"
ALCASAR URL="https://alcasar.localdomain/"
LOG FILE="/var/log/alcasar_test.log"

#Fonctions d'assistance
log() {
    echo "$(date +'%Y-%m-%d %H:%M:%S') - $1" | tee -a $LOG_FILE
}

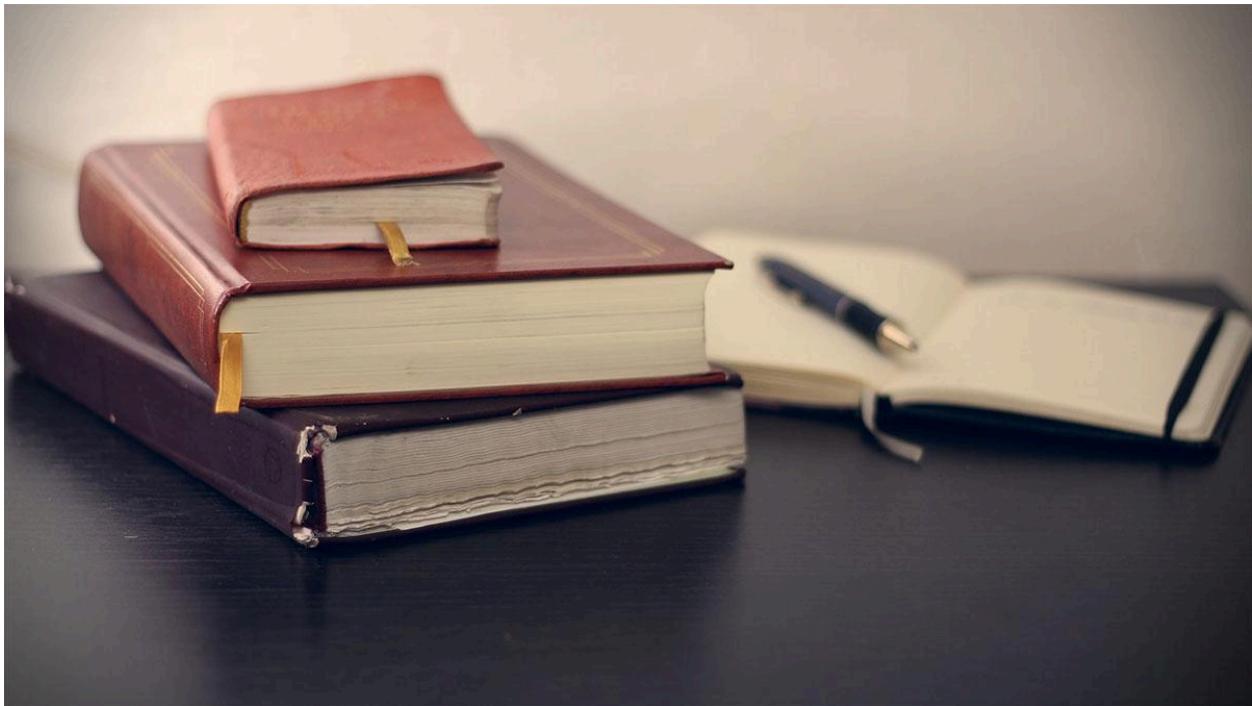
test_ldap_authentication() {
    log "Testing LDAP authentication..."
    ldapsearch -x -H $LDAP_SERVER -D "$ADMIN_DN" -w $ADMIN_PASSWORD -b "$BASE_DN" "(uid=$TEST_USER)" > /dev/null 2>&1
    if [ $? -eq 0 ]; then
        log "LDAP authentication for user $TEST_USER succeeded."
    else
        log "LDAP authentication for user $TEST_USER failed."
        exit 1
    fi
}

test_network_traffic() {
    log "Testing network traffic monitoring..."
    #Simulate some network traffic
    curl -I $ALCASAR_URL > /dev/null 2>&1
    # Check if the traffic is logged
    if grep -q "curl" /var/log/alcasar/traffic.log; then
        log "Network traffic monitoring succeeded."
    else
        log "Network traffic monitoring failed."
        exit 1
    fi
}

test_log_management() {
    log "Testing log management..."
    #Check if log files are being created and rotated
    ^G Aide      ^O Écrire      ^W Chercher      ^K Couper      [ Lecture de 102 lignes ]
    ^X Quitter   ^R Lire fich.  ^\ Remplacer   ^U Coller      ^T Exécuter      ^C Emplacement  M-U Annuler      M-A Placer la mar
    ^Q Retrouver          ^J Justifier   ^A Aller ligne   M-E Refaire      M-B Copier       M-L Crotchet
    ^L           ^P             ^S             ^V             ^B             ^D             ^I             ^N             ^O             ^R             ^U             ^X             ^Y             ^Z
```


Le cadre

Astuce : Demande-toi QUAND et OÙ l'action se déroule, et COMBIEN DE TEMPS s'écoule entre le début et la fin de l'histoire. Décris le cadre de telle manière que tes camarades aient l'impression de VIVRE l'histoire.



Astuce : Trouve sur Internet une image qui ressemble au cadre de cette histoire, puis insère-la à la place de l'image ci-dessus.

Les personnages

Astuce : Qui est le personnage principal ? A-t-il des amis ou des personnes qui l'aident ? Y a-t-il quelqu'un qui s'oppose au personnage principal ? Plutôt que de nommer simplement les personnages, explique ce qui caractérise chacun d'eux.



Astuce : Trouve sur Internet une image du personnage principal, ou une image qui lui ressemble, puis insère-la à la place de l'image ci-dessus.

L'intrigue

1. Début : que se passe-t-il au début du livre ?
2. Milieu : généralement le point culminant de l'action dans l'histoire.
3. Fin : comment tout cela se termine-t-il ?

Astuce : Identifie les événements les plus importants de l'histoire. Ne raconte pas toute l'intrigue, mais donne suffisamment de détails pour que des personnes n'ayant pas lu le livre puissent en comprendre l'intrigue.



Conclusion

Astuce : Il est important de donner ton avis ! Conseillerais-tu ce livre à d'autres personnes ?

