

Dossier projet d'entreprise

Refonte partielle de l'infrastructure réseau d'une école d'informatique : contrôle des accès, supervision et centralisation des identités

Objectifs du projet :

→L'installation d'un deuxième serveur ALCASAR sur une machine virtuelle séparée est envisagée pour garantir la continuité du service en cas de panne du serveur principal. Ce serveur de sauvegarde doit être équivalent sur le plan fonctionnel, utilisant non plus des comptes locaux MySQL pour l'authentification centralisée, mais un annuaire distant LDAP tel que Google Workspace, afin d'assurer une gestion des utilisateurs centralisée et simplifiée. De plus ça nous permettra de tester la nouvelle version d'ALCASAR sans toucher au serveur ALCASAR déjà en prod.

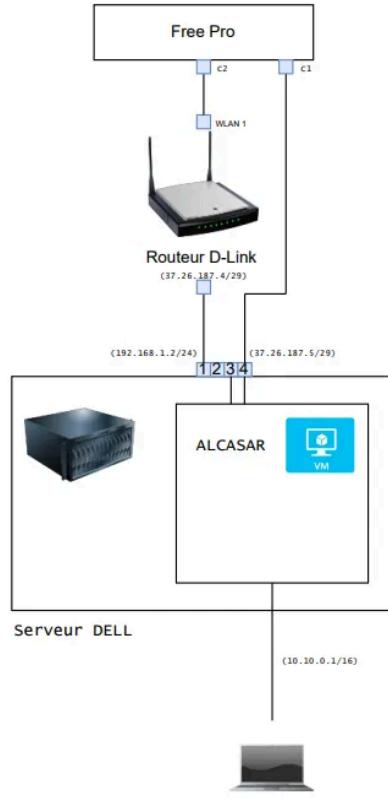
→Permettre une sauvegarde et une restauration plus aisées de l'infrastructure en utilisant la virtualisation. Le format VM au lieu de d'installer directement ALCASAR sur la machine hôte offre la possibilité d'effectuer des snapshot réguliers et instantanés et de rétablir rapidement l'environnement en cas de défaillance, ce qui participe à renforcer la résilience générale du système.

Étapes:

- 1) Installer et mettre en place KVM sur le serveur afin d'y héberger des VMs
- 2) Configurer une redirection de port du routeur vers le serveur
- 3) Créer une VM sous Mageia 9 (Et y installer Alcasar-3.7.1)
- 4) Configurer un PCI Passthrough pour que la VM Alcasar puisse directement accéder à certains périphériques (réseau) du serveur physique.
- 5) Configurer et Installer Mageia 9
- 6) Configurer et Installer Alcasar
- 7) Configurer l'annuaire LDAP Google afin de centraliser la gestion des utilisateurs et d'éviter l'usage de comptes locaux.
- 8) Trouver d'autres solutions à mettre en place à l'avenir

La Plateforme

Ce schéma représente l'architecture réseau mise en place dans le cadre de mon projet :



La connexion Internet passe par une box **Free Pro**, reliée à un routeur D-Link configuré avec une IP publique. Ce routeur distribue ensuite les connexions vers mon **serveur DELL**.

Sur ce serveur, j'ai créé une machine virtuelle qui héberge ALCASAR. Cette VM possède **deux interfaces réseau** :

- Une **IP publique** (37.26.187.5), pour communiquer avec l'extérieur
- Une en **LAN** (10.10.0.1/16), utilisée pour gérer les connexions des utilisateurs

ALCASAR joue ici le rôle de **portail captif** : il filtre les accès au réseau et oblige les utilisateurs à s'authentifier avant de pouvoir naviguer sur Internet. **Tous les clients passent donc par lui**.

La machine Debian qui héberge ALCASAR reste très peu exposée, car elle n'**émet presque aucune requête**. Même si elle possède une IP publique, elle reste discrète, et il est difficile de savoir si Alcasar s'agit d'une machine virtuelle, ce qui renforce sa sécurité.

La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) – 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

La Plateforme

La machine Debian reste intacte même si ALCASAR est compromis, car la virtualisation isole complètement les deux systèmes.

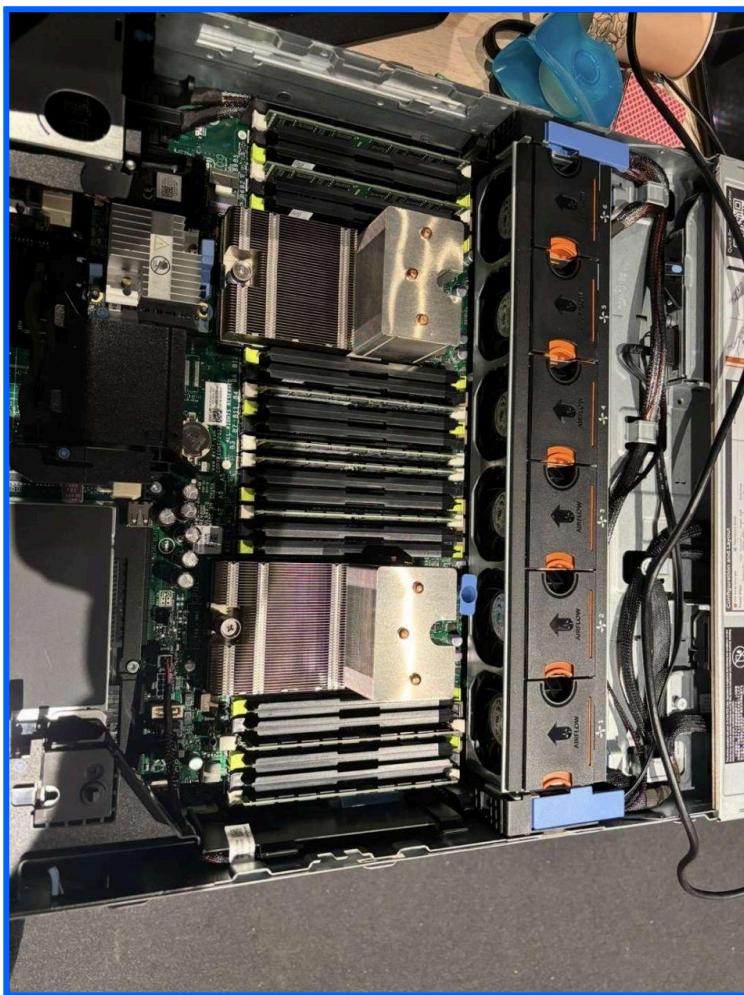
Il n'y a pas de connexion directe ni de services partagés, donc un attaquant dans ALCASAR reste enfermé dans la VM et ne peut pas facilement atteindre l'hôte Debian.
Cela fait partie des bonnes pratiques en cybersécurité : cloisonner les rôles pour limiter les risques de propagation en cas d'intrusion.

Déroulement du projet :

étape 1

- Préparation du serveur (mise en place des RAM, disque dur...)

j'ai connecté 128 Go de RAM au serveur pour garantir de bonnes performances, et j'ai branché les disques durs à la carte RAID afin d'assurer une meilleure gestion du stockage et de la tolérance aux pannes.



La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) – 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

La Plateforme

- Configurer un raid

J'ai configuré un RAID 1 directement depuis le BIOS, en démarrant sur la carte RAID. Pour cela, j'ai accédé à l'interface 3ware BIOS Manager en appuyant sur Alt + 3 au démarrage du serveur.

Mais d'abord, c'est quoi un raid ?

Un **raid** (ou Redundant Array of Independent Disks = Regroupement Redondant de Disques Indépendants) est **un type de stockage** consistant à écrire des données sur **plusieurs disques** d'un même système.

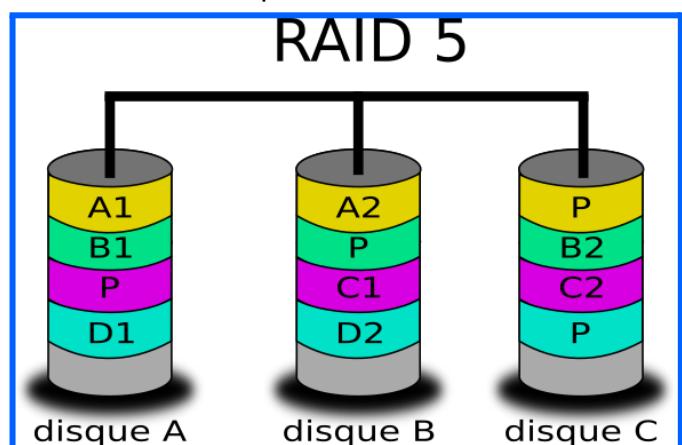
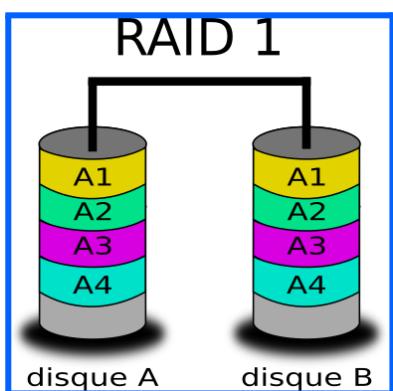
Différentes **configurations** sont exprimées sous la forme de chiffres, telles que **RAID 0**, **RAID 1** ou **RAID 5**. Chaque type de RAID **offre des bénéfices différents aux utilisateurs**, tels que des performances accrues, une meilleure tolérance aux pannes ou les deux, en fonction de sa manière d'écrire et de distribuer vos données.

Ici, nous allons utiliser un **Raid 1**.

La configuration **RAID 1** permet de sécuriser un système **en disposant de deux disques** avec exactement les mêmes données. Dans cette configuration, on ne recherche **pas la performance** mais plutôt **la sécurité**. Le disque 1 contenant exactement les mêmes données que le disque 2, la volumétrie utile sera divisée par 2.

Si un disque lâche, on ne perdra aucune donnée qui sera stockée **en miroir** sur l'autre disque.

Un raid 5 en comparaison :



La Plateforme

Raid 1 : données sont copiées à l'identique sur deux disques voir plus (miroir)

tolérance = perdre 1 disque si on en a 2 en tout, 2 disques si on en a 3 ainsi de suite.

point positif = lecture plus rapide (les informations sont les mêmes sur deux disques)

point négatif = vu que les données sont copiées à l'identique, on perd la moitié de l'espace de stockage disponible. 2 disques de 1To = 1To utilisable

Raid 5 : les données et la parité sont réparties sur au moins trois disques voir plus

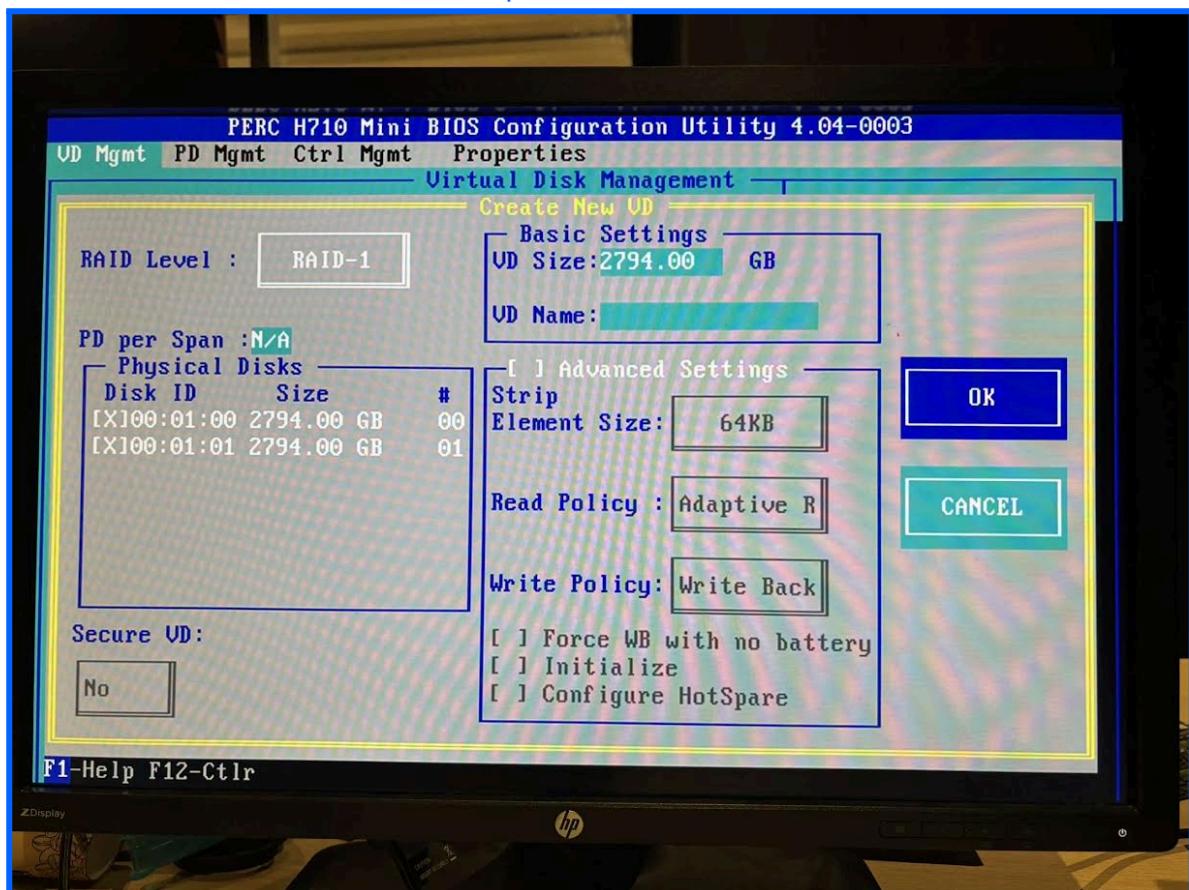
(La parité est une information de contrôle calculée à partir des données, qui permet de reconstruire les données perdues si un disque tombe en panne.)

tolérance = perdre 1 disque si on en a 3.

point positif = plus grande capacité grâce à la parité, si tu as 3 disques de 1To, tu as 2To utilisable

point négatif = Écriture plus lente (à cause du calcul de la parité) et également une reconstruction lente et risquée en cas de panne d'un disque

Donc, nous allons utiliser un RAID 1 pour une sécurité accrue.



La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) - 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

La Plateforme

Ceci est l'interface RAID de la carte PERC H710 (carte RAID Serveur Dell)

On voit bien ici que le [niveau de RAID sélectionné est de 1](#), et qu'il y a [2 disques de 2.7to](#) chacun qui seront en miroir entre eux.

Il ne nous reste plus qu'à valider et le RAID-1 sera mis en place.

Une fois le RAID 1 configuré, je [démarrer l'installation de Debian](#) en utilisant une [clé USB bootable](#).

Le volume RAID créé via la carte RAID est alors reconnu comme [étant un seul et unique disque au lieu de 2](#), sur lequel je vais installer le système d'exploitation.

Après l'installation, je configure l'ordre de démarrage du BIOS (avec le [boot order](#)) pour que le serveur boot directement sur la carte RAID.

C'est quoi le boot order : Le boot order, c'est [une liste de priorité](#) définie dans le BIOS ou l'UEFI d'une machine, qui indique dans [quel ordre les périphériques sont consultés pour démarrer le système](#).

- [Installation du système d'exploitation](#)

Afin d'installer le système d'exploitation qu'on veut, nous allons utiliser Rufus ([Reliable USB Formatting Utility with Source](#)) qui est un logiciel open-source qui permet de créer des supports bootable (live USB) et des clé bootable à partir d'un fichier ISO sur un périphérique externe comme une clé USB.

[Un fichier ISO c'est quoi](#) : un format de fichier numérique reproduisant un CD, un DVD ou un BD physique, contenant à l'intérieur tous les fichiers nécessaires à un OS rassemblé en 1 fichier.

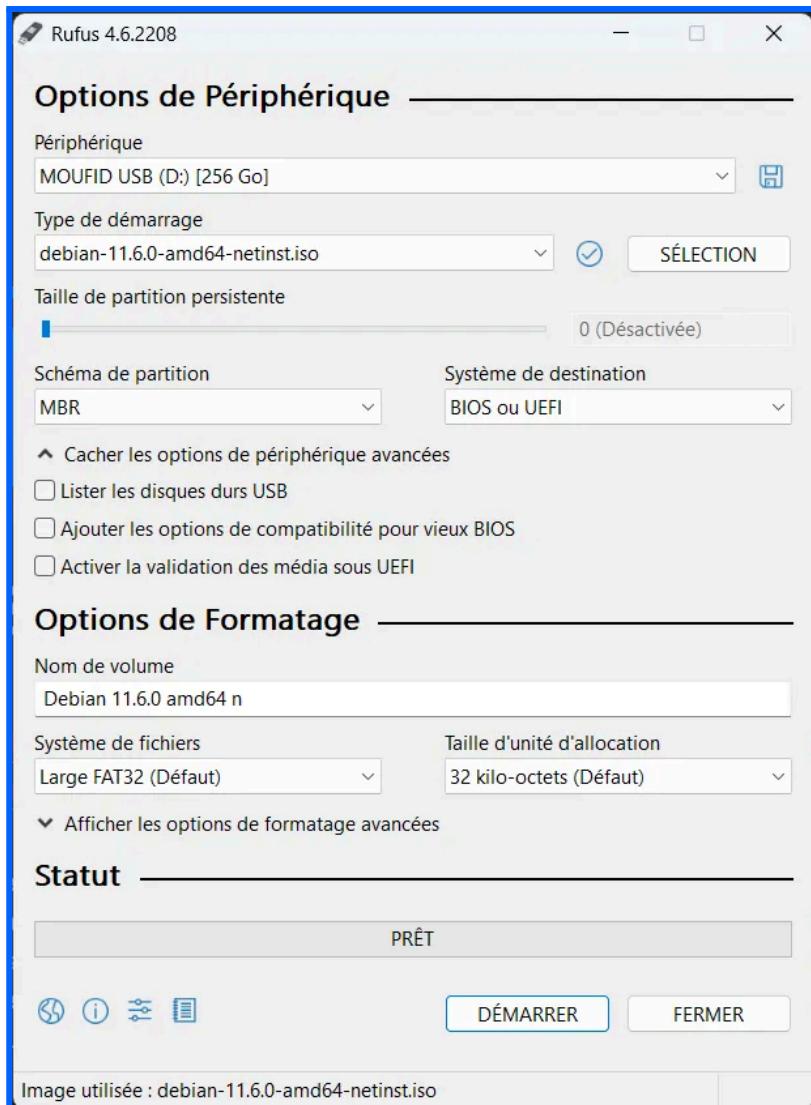
La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) – 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io



Une fois la clé USB bootable [contenant Debian 11](#) créée, je la branche sur le serveur et [modifie temporairement l'ordre de démarrage](#) (boot order) dans le BIOS afin de démarrer sur la clé. Cela permet de lancer l'installation de l'OS Debian 11 directement depuis le support USB.

Je vais maintenant montrer rapidement [les étapes d'installation](#), qui sont simples à suivre. Il suffit de renseigner quelques informations comme le nom d'utilisateur, les mots de passe, puis de choisir le disque d'installation. Dans notre cas, il faudra bien sûr sélectionner le volume RAID, reconnu comme un seul disque.

La Plateforme Formation

Société par actions simplifiée

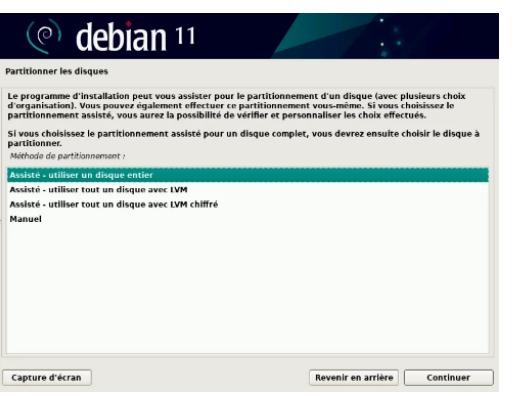
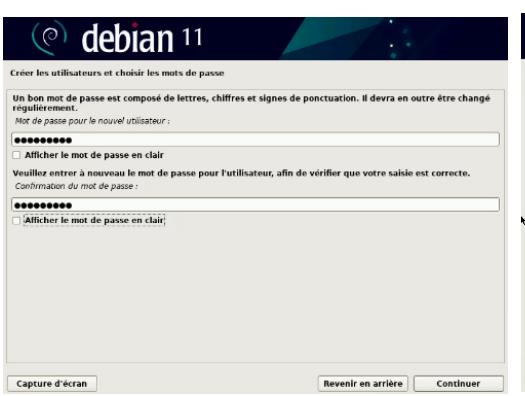
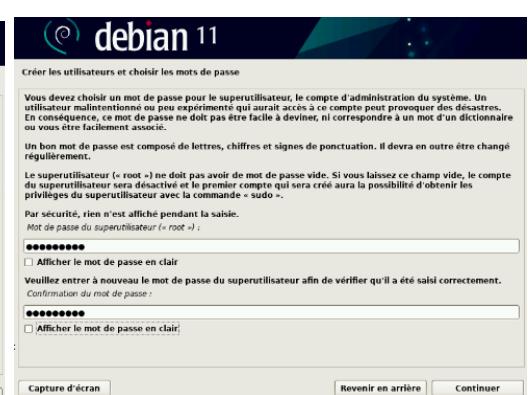
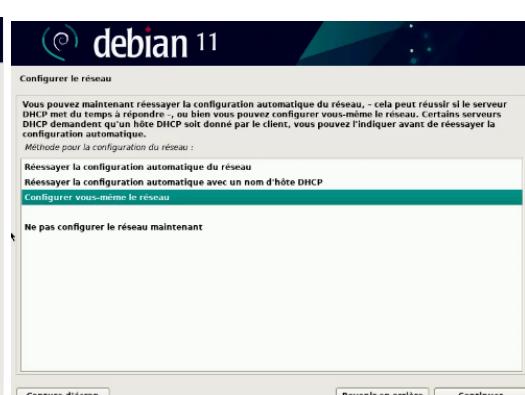
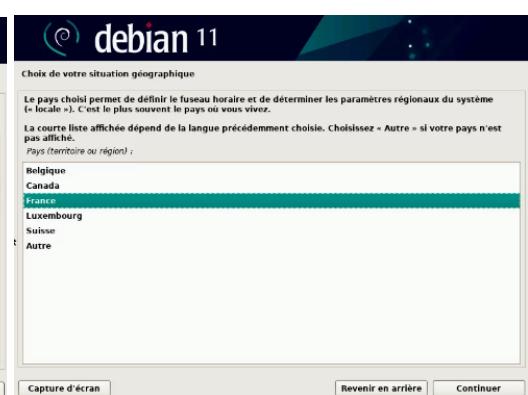
Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) - 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

La Plateforme

Installation de debian 11:



La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) - 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

La Plateforme

J'installe Debian [sans interface graphique](#), car il s'agit d'un serveur. [Une interface en ligne de commande suffit largement](#) pour l'administration et permet de garder le système plus léger et plus sécurisé.

Une machine sans interface graphique présente [plusieurs avantages](#) : elle consomme moins de ressources, évite d'installer des services inutiles ([Chacun de ces services est une porte d'entrée potentielle pour un attaquant.](#)), et réduit ainsi les risques de failles de sécurité. Moins il y a de logiciels installés, moins il y a de points d'entrée potentiels pour un attaquant. Ce choix permet donc d'avoir un système plus léger, plus stable et plus sécurisé.

- [Mise en place de KVM](#)

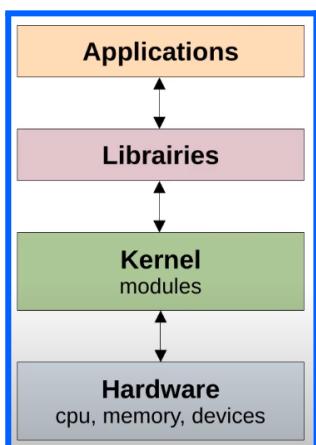
Une [machine virtuelle](#) permet de [simuler une machine à l'intérieur d'une autre](#). C'est une solution couramment utilisée pour tester ou faire [tourner plusieurs systèmes sur une seule machine physique](#).

Les solutions les plus connues du grand public sont [VirtualBox](#), qui est [gratuite](#), et [VMware](#), qui propose à la fois une version [gratuite et une version professionnelle payante](#).

Ces solutions sont [simples à utiliser](#), mais généralement [moins performantes que KVM](#), qui est une solution plus puissante, souvent utilisée dans un contexte [professionnel ou serveur](#).

Nous allons voir pourquoi nous allons utiliser KVM au lieu de VMWare par exemple.

L'image ci-dessous représente l'architecture d'un système Linux de manière simple



La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) - 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

La Plateforme

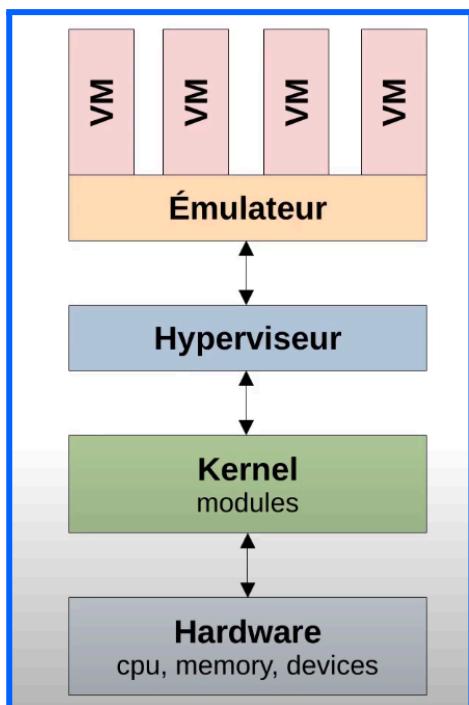
À la base, on trouve le **matériel** (le CPU, la RAM, les disques, etc.).

Ce matériel est directement géré par le **noyau** (**le Kernel**), qui fait le lien entre les composants physiques et le système d'exploitation.

Juste au-dessus, on a les **librairies**, qui servent d'intermédiaire entre le noyau et les programmes.

Enfin, tout en haut, on trouve les **applications**, celles que l'utilisateur lance ou installe.

A présent, voici comment les machines virtuelles habituelle fonctionnent :



Ce schéma montre **comment tournent les machines virtuelles sur un système Linux**.

D'abord, on installe un **hyperviseur** sur la machine physique. **Cet hyperviseur s'appuie sur le noyau Linux pour accéder aux composants matériels** (processeur, mémoire, etc.). Ensuite, grâce à cet hyperviseur, on peut **créer des émulateurs**, qui vont **simuler un vrai ordinateur**.

C'est sur **ces émulateurs qu'on vient installer les machines virtuelles**, comme si on lançait plusieurs petits ordinateurs dans un seul.

Quel est l'avantage de kvm ? et bien c'est ça :

La Plateforme Formation

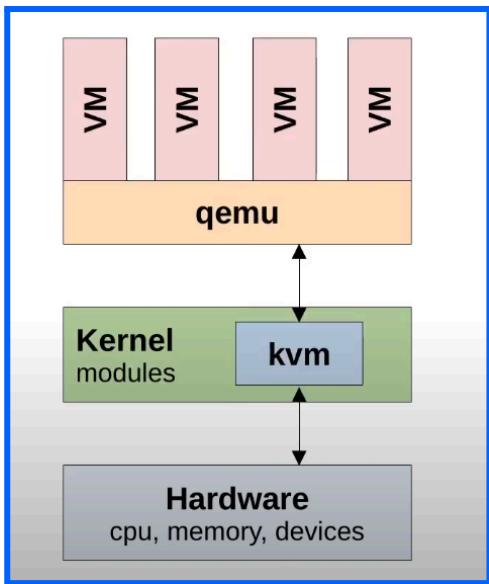
Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) – 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

La Plateforme



L'avantage de KVM, c'est qu'il (l'hyperviseur) est directement intégré au noyau Linux, sous forme de [module](#).

Cela signifie que l'hyperviseur fait partie du système lui-même, ce qui améliore énormément les performances. Résultat : une machine virtuelle avec KVM peut atteindre jusqu'à 95 % de l'efficacité du CPU réel, ce qui est très proche des performances d'un système physique.

Autre point fort : KVM est [open-source](#), tout comme QEMU, l'émulateur qui se place au-dessus pour faire tourner les machines virtuelles.

Kvm et qemu ne sont pas suffisant, pour gérer tout ça facilement, on a aussi [besoin de Libvirt](#), une bibliothèque qui fournit deux outils importants :

[virsh](#) : une interface en ligne de commande (pour créer, démarrer, arrêter, cloner, supprimer des VM, etc.)

[virt-manager](#) : une interface graphique qui permet de faire tout ce que virsh fait en terminal, mais de façon visuelle et plus intuitive

En résumé :

[KVM + QEMU + Libvirt](#) forment un ensemble complet pour faire de la virtualisation sous Linux, avec à la fois performance, contrôle et flexibilité.

La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) - 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

La Plateforme

On va maintenant pouvoir installer et configurer KVM sur notre serveur

Voici des commandes à exécuter sur notre debian pour installer KVM;

```
-sudo apt install virt-manager  
-sudo systemctl enable --now libvirtd  
-sudo apt-get install qemu-kvm libvirt-clients libvirt-daemon-system usermode  
ethtool  
-sudo systemctl status libvirtd
```

```
root@dellserver:/home/sysadmin# sudo systemctl enable --now libvirtd  
root@dellserver:/home/sysadmin# sudo systemctl status libvirtd  
● libvirtd.service - Virtualization daemon  
  Loaded: loaded (/lib/systemd/system/libvirtd.service; enabled; preset: enabled)  
  Active: active (running) since Tue 2025-07-15 16:21:44 CEST; 1s ago  
TriggeredBy: ● libvirtd-ro.socket  
              ● libvirtd-admin.socket  
              ● libvirtd.socket  
    Docs: man:libvirtd(8)  
          https://libvirt.org  
  Main PID: 72458 (Libvirtd)  
    Tasks: 22 (limit: 32768)  
   Memory: 52.7M  
     CPU: 602ms  
    CGroup: /system.slice/libvirtd.service  
            └─ 1104 /usr/sbin/dnsmasq --conf-file=/var/lib/libvirt/dnsmasq/default.conf --leasefile-ro --dhcp-script=/>  
            └─ 1105 /usr/sbin/dnsmasq --conf-file=/var/lib/libvirt/dnsmasq/default.conf --leasefile-ro --dhcp-script=/>  
            72458 /usr/sbin/libvirtd --timeout 120
```

Par défaut, seul l'utilisateur root peut gérer les machines virtuelles.

Pour permettre à un autre utilisateur (ici notre user sysadmin) de les contrôler, il faut l'ajouter [aux groupes libvirt et kvm](#) avec ces commandes :

```
-usermod -a -G libvirt sysadmin  
-usermod -a -G kvm sysadmin
```

```
sysadmin@dellserver:~$ id  
uid=1000(sysadmin) gid=1000(sysadmin) groupes=1000(sysadmin),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),100(users),104(kvm),106(netdev),111(libvirt)
```

Maintenant qu'on a ajouté sysadmin aux groupes, peut maintenant utiliser les commandes virsh directement

Dans l'exemple ci dessous, j'ai utilisé la commande 'list' qui permet de lister les machines virtuelles existantes.

La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) – 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

La Plateforme

```
sysadmin@dellserver:~$ virsh
Bienvenue dans virsh, le terminal de virtualisation interactif.

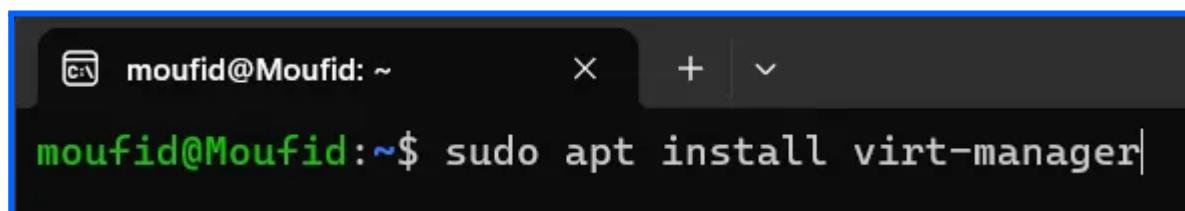
Taper : « help » pour l'aide ou « help » avec la commande
       « quit » pour quitter

virsh # list
  ID  Nom  État
-----
virsh # quit

sysadmin@dellserver:~$ |
```

Sur une machine tierce, on peut maintenant [créer des VMs](#) avec l'interface graphique [de virt-manager](#). (VMM, Virtual Machine Manager)

Sur un terminal, exécuter la commande ci dessous :



A screenshot of a terminal window titled "moufid@Moufid: ~". The window has standard Linux terminal icons at the top: a user icon, the title, a close button (X), a plus sign (+) for new tabs, and a dropdown arrow. The terminal content shows the command "moufid@moufid:~\$ sudo apt install virt-manager" in green text, which is the command to install the Virtual Machine Manager package.

Une fois dans [Virtual Machine Manager](#), on peut ajouter un nouveau serveur en cliquant sur [File](#) puis [Nouvelle connexion](#).

Cela permet de se connecter à notre serveur pour gérer les machines virtuelles.

La Plateforme Formation

Société par actions simplifiée

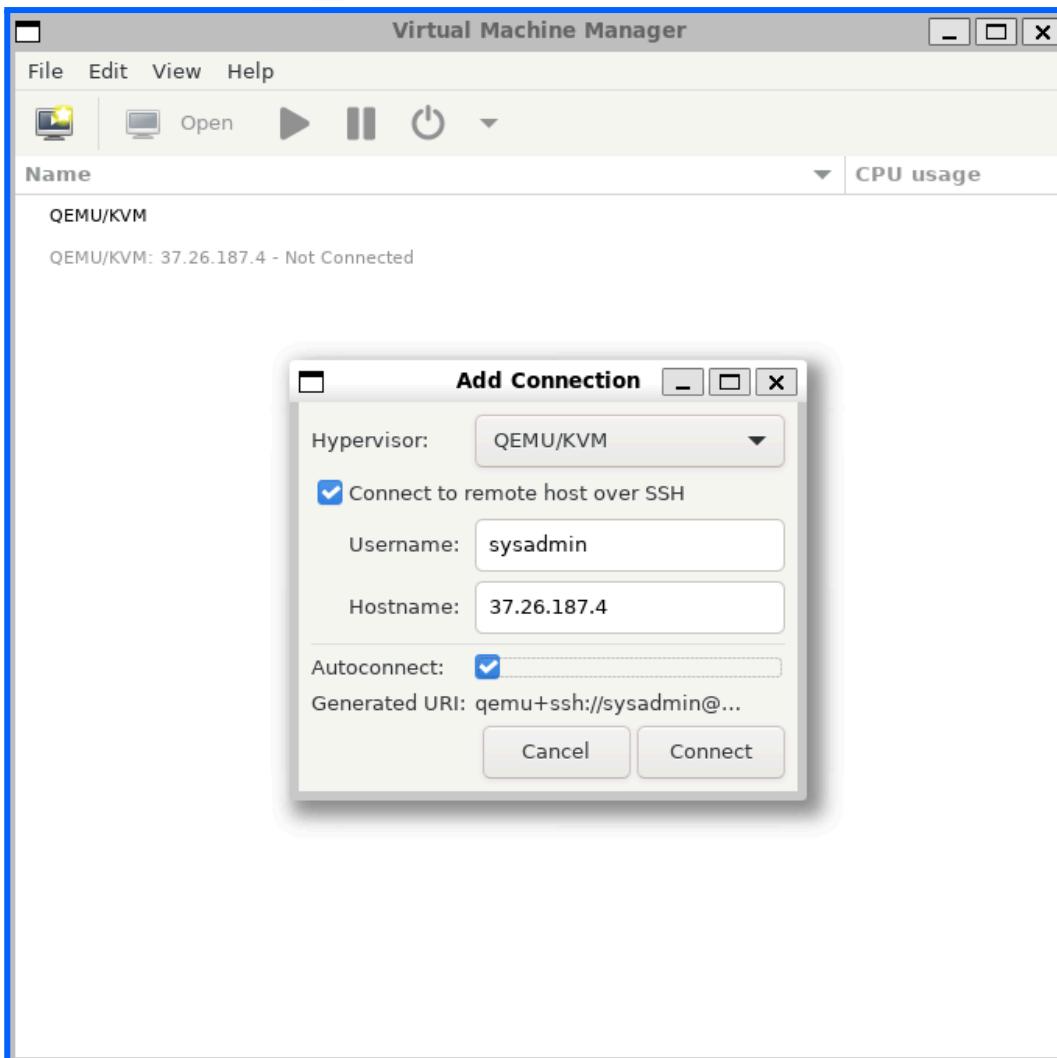
Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) – 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

La Plateforme

On sélectionne l'hyperviseur qui est QEMU/KVM,
Qu'on se connecte à distance au serveur via SSH,
Username = sysadmin (nom d'utilisateur du serveur)
Hostname = 37.26.187.4 (IP Publique de free pro donnée au serveur)
Autoconnect activée 



La Plateforme Formation

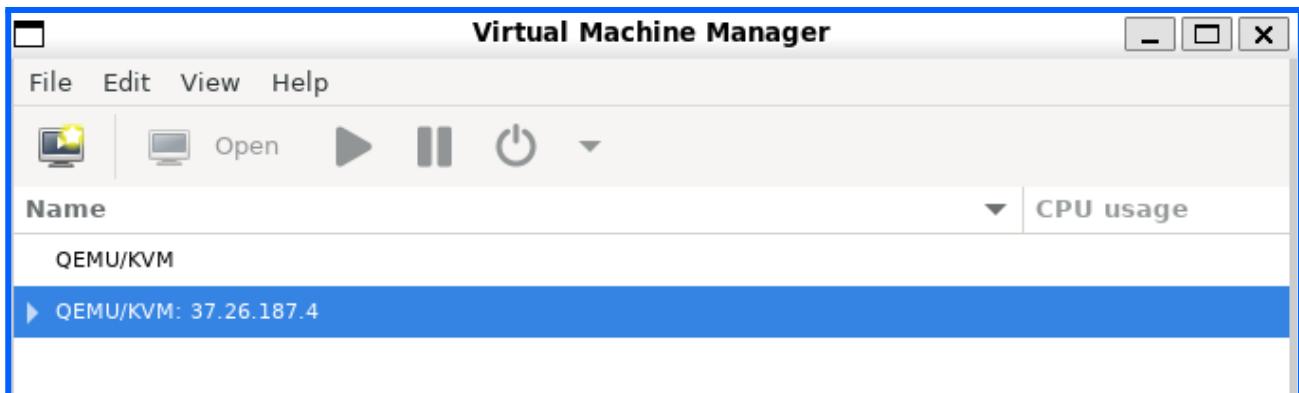
Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) – 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

La Plateforme



Ici nous pouvons voir que nous sommes bel et bien connecté au serveur

- Création de la VM Mageia 9 (qui va hébergé ALCASAR)

Nous allons maintenant [créer notre VM Alcasar](#) via [Virtual Machine Manager](#) qui sera [hébergé sur notre serveur](#).

Pourquoi faire [ALCASAR](#) sur une [machine virtuelle](#) et pas directement sur une machine ? Le fait que Alcasar soit une vm comporte [plusieurs avantages](#);

-Premièrement, avec une VM on va pouvoir [faire des snapshots](#) (captures de l'état du système à un instant T) facilement. Donc en cas de problème sur la machine on peut [revenir en arrière très facilement et rapidement](#), chose impossible sur une machine physique.

-Deuxièmement, avoir une [VM est moins risqué pour l'hôte](#) car si Alcasar est mal configuré, compromis ou comporte des failles de sécurité, [l'hôte reste intact car le système est isolé](#).

-Enfin, nous sommes [plus flexibles](#) avec une machine virtuelle, on peut allouer plus ou moins de RAM en fonction de notre nécessite, déplacer la vm ailleurs si besoin et surtout [faire tourner plusieurs VM sur la même machine hôte](#).

Pour ajouter une VM au serveur, il faut [cliquer-droit](#) sur le serveur précédemment connecté à Virtual Machine Manager, et appuyer sur [New](#).
(Comment montré dans l'exemple ci dessous)

La Plateforme Formation

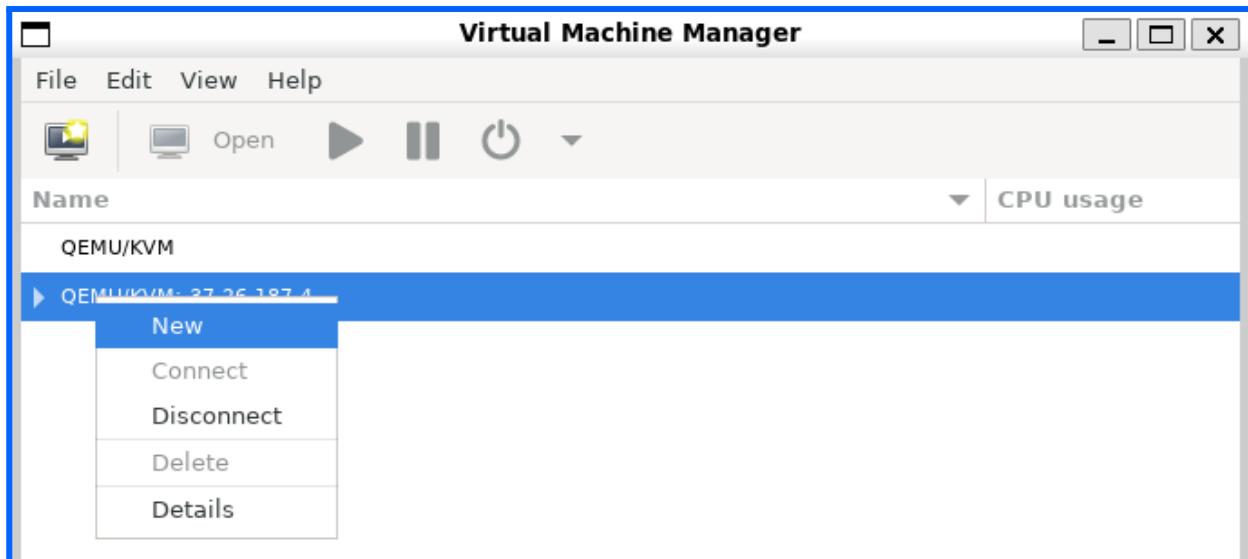
Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

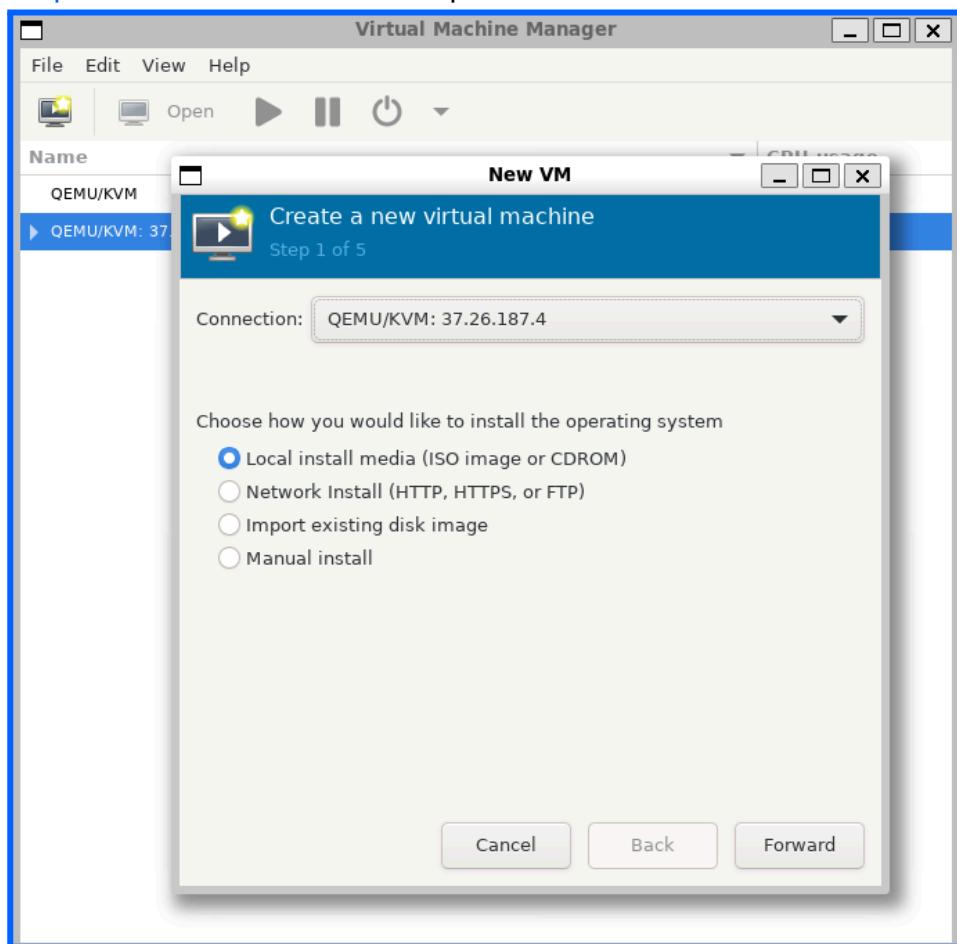
Dont le siège social est situé à Marseille (13007) - 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

La Plateforme



Cette fenêtre s'ouvre, il faudra sélectionner la [bonne connexion](#), ici notre serveur sous KVM, et sélectionner qu'on voudra installer le système d'exploitation [localement avec un fichier ISO de Mageia](#). Alcasar tourne sous [Mageia 8 ou 9](#), ici nous avons récupéré un ISO de Mageia depuis le site officiel de Alcasar qui contient [directement à l'intérieur le script d'installation d'ALCASAR](#) pour nous faciliter la tâche.



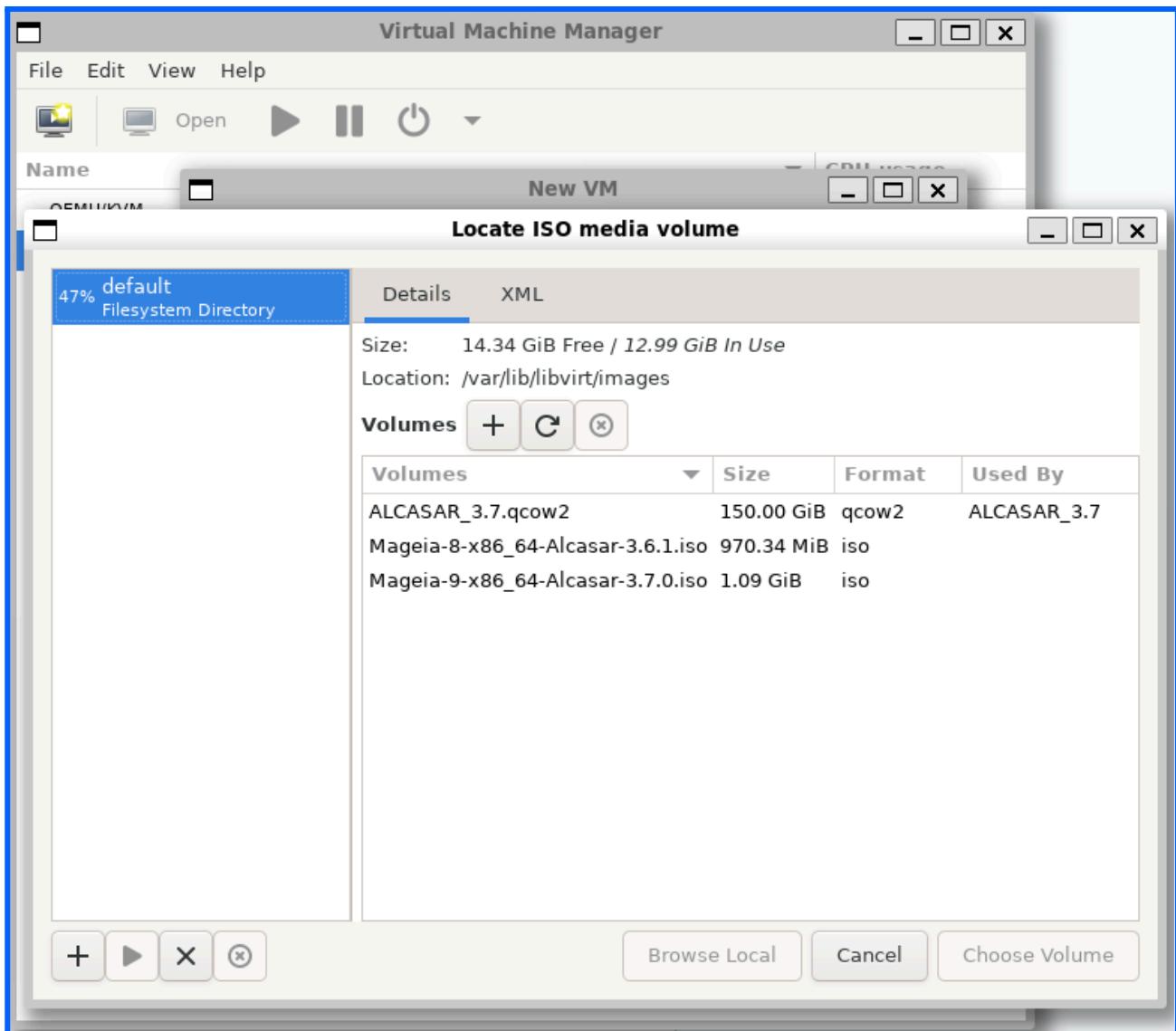
La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

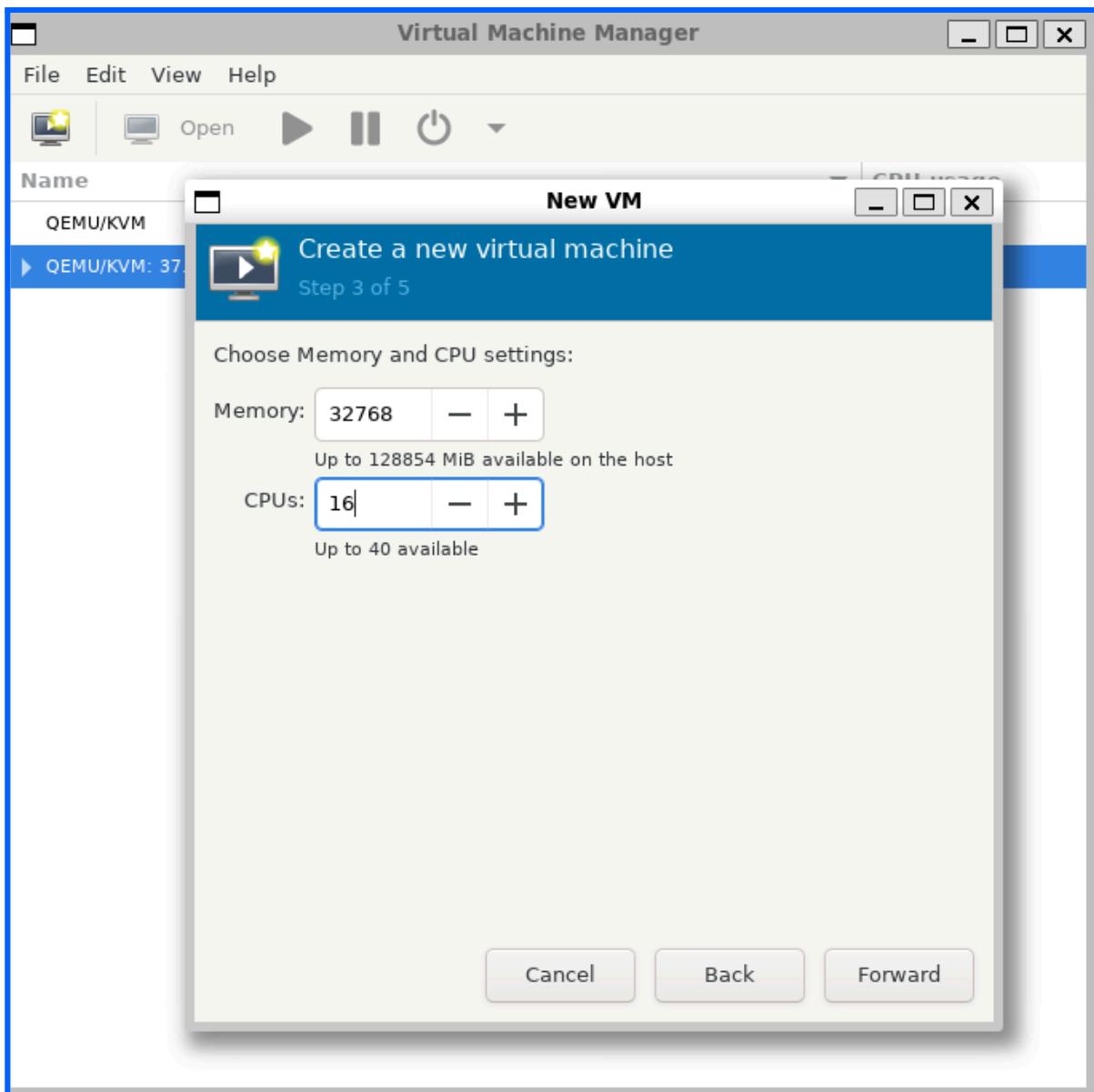
Dont le siège social est situé à Marseille (13007) - 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io



Pour pouvoir sélectionner une image ISO dans [Virtual Machine Manager](#), il faut d'abord copier le fichier ISO sur le serveur hôte dans le dossier [/var/lib/libvirt/images](#). Une fois placé dans ce répertoire, l'[ISO apparaît automatiquement dans la liste lors de la création d'une nouvelle machine virtuelle](#).

Comme précisé précédemment, on voit bien que c'est un fichier ISO de l'[OS Mageia 9](#), contenant à l'intérieur le script d'installation d'Alcasar.



Ensuite, il faut allouer des ressources à la machine virtuelle, notamment la mémoire RAM et le nombre de coeurs CPU.

Dans mon cas, j'ai choisi de lui attribuer **32 Go de RAM** et **16 coeurs**, afin d'assurer de bonnes performances et de la stabilité, même en cas de charge importante.

Avoir 32 Go de RAM et 16 coeurs assure une exécution fluide, sans ralentissements, même en cas de forte sollicitation, car il y aura plusieurs centaines de personnes connectées à Alcasar à la fois, donc pour l'analyse de paquets et des logs une bonne performance est utile.

La Plateforme Formation

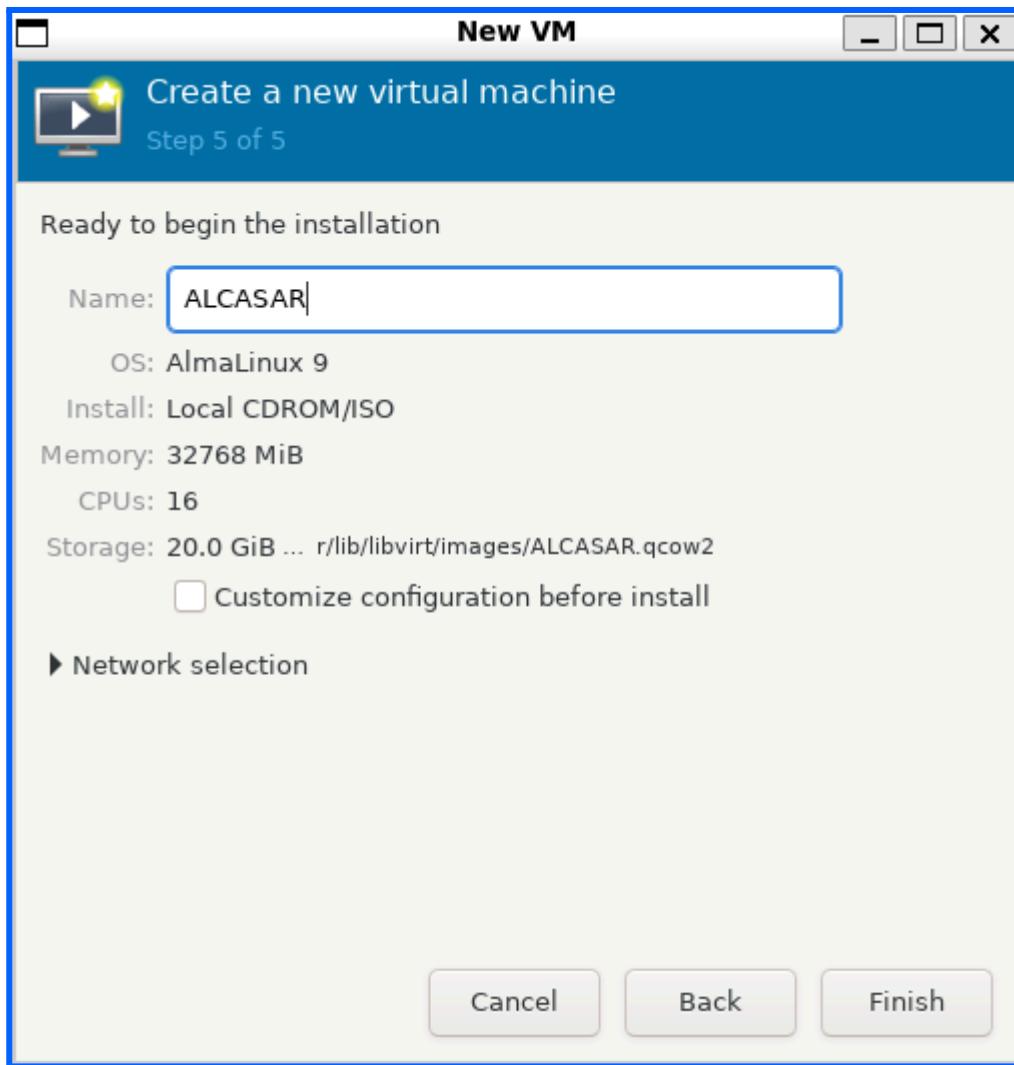
Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) - 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

La Plateforme



C'est déjà fini, il ne nous reste plus qu'à nommer notre machine virtuelle et finir le processus de création de machine virtuelle.

Avant de démarrer l'installation d'Alcasar dans la VM Mageia, j'ai configuré un [PCI passthrough](#) pour attribuer directement [deux interfaces réseau physiques du serveur à la machine virtuelle](#).

Cette méthode permet à ALCASAR d'avoir un accès direct au matériel, sans passer par la couche de virtualisation, ce qui [améliore les performances réseau](#), la [fiabilité](#) et la [compatibilité avec certaines fonctionnalités comme le portail captif](#).

Pourquoi attribuer deux interfaces réseau à Alcasar ?

ALCASAR agit comme un [pare-feu / proxy / portail captif](#) entre les utilisateurs et Internet, donc il lui faut une carte pour [gérer Internet \(WAN\)](#) et une pour [gérer les utilisateurs \(LAN\)](#).

La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) – 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

La Plateforme

- Configuration du PCI Passthrough sur KVM

Un [PCI Passthrough](#) c'est quoi ?

Le [PCI Passthrough](#) est une technique qui attribue un [périphérique PCI physique](#) à une [machine virtuelle](#) afin que la machine virtuelle puisse accéder directement au périphérique matériel avec [une implication minimale](#) (voire nulle) de VMM

PCI = Développée par Intel Corporation, la norme PCI (Peripheral Component Interconnect, Interconnexion de composants périphériques) est un bus haut débit standard qui se trouve sur presque tous les ordinateurs de bureau.

Un bus, c'est un "autoroute" qui permet à tous les composants de l'ordinateur de communiquer entre eux. Le bus PCI, lui, est une de ces autoroutes, utilisée pour brancher du matériel externe à la carte mère.

Il faut d'abord identifier les [deux interfaces réseau physiques](#) du serveur que l'on souhaite attribuer à ALCASAR.

La commande [lspci](#) est une commande Linux qui permet d'[afficher la liste des périphériques](#) connectés au bus PCI comme les cartes réseau, le GPU, les cartes raid...

En cherchant les périphériques réseau, on tombe sur ça :

```
sysadmin@dellserver:~$ lspci | grep Etherne
01:00.0 Ethernet controller: Broadcom Inc. and subsidiaries NetXtreme BCM5720 Gigabit Ethernet PCIe
01:00.1 Ethernet controller: Broadcom Inc. and subsidiaries NetXtreme BCM5720 Gigabit Ethernet PCIe
02:00.0 Ethernet controller: Broadcom Inc. and subsidiaries NetXtreme BCM5720 Gigabit Ethernet PCIe
02:00.1 Ethernet controller: Broadcom Inc. and subsidiaries NetXtreme BCM5720 Gigabit Ethernet PCIe
```

01:00.0, 01:00.1, 02:00.0 et 02:00.1 sont les adresses PCI des périphériques.

Pour activer le PCI Passthrough sur notre machine, il faut activer IOMMU sur le grub.

Il faut donc modifier /etc/default/grub et ajouter :

`intel_iommu=on` et `iommu=pt`

```
GNU nano 7.2                                     /etc/default/grub
# If you change this file, run 'update-grub' afterwards to update
# /boot/grub/grub.cfg.
# For full documentation of the options in this file, see:
#   info -f grub -n 'Simple configuration'

GRUB_DEFAULT=0
GRUB_TIMEOUT=5
GRUB_DISTRIBUTOR=`lsb_release -i -s 2> /dev/null || echo Debian`
GRUB_CMDLINE_LINUX_DEFAULT="intel_iommu=on iommu=pt pcie_acs_override=downstream,multifunction pci-stub.ids=14e4:165f quiet"
GRUB_CMDLINE_LINUX=""
```

Une fois fait, mettre à jour le grub via la commande : [sudo update-grub](#)

La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

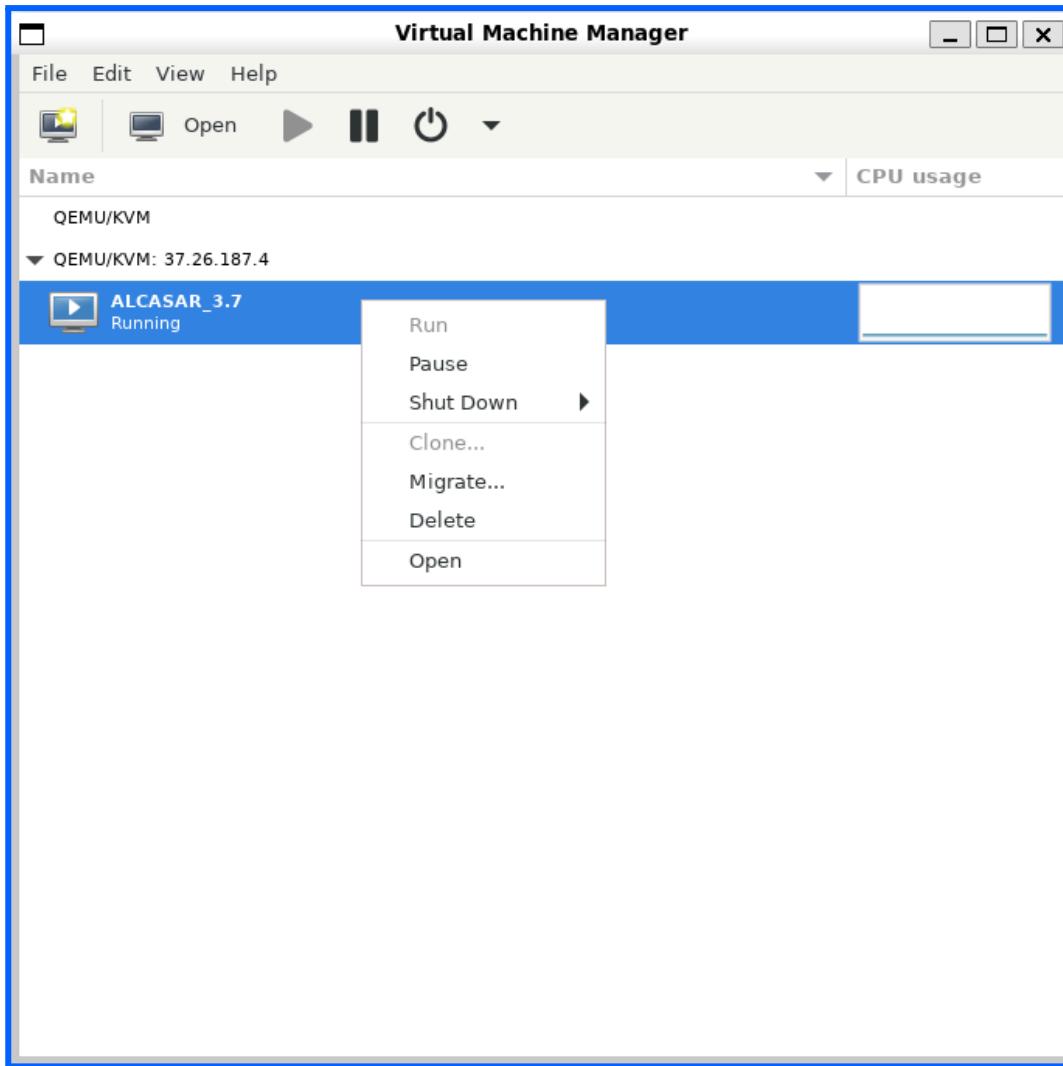
Dont le siège social est situé à Marseille (13007) – 14 Traverse Canoubier

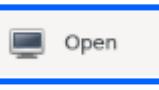
Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

La Plateforme

Maintenant que l'[IOMMU est activé](#), je peux sélectionner les [périphériques PCI](#) que je souhaite attribuer en passthrough directement depuis l'interface graphique de Virtual Machine Manager.

J'ai choisi KVM pour ce projet car il gère [nativement le PCI passthrough](#) via le noyau Linux, ce qui offre [meilleure performance](#), meilleure intégration et plus de flexibilité que des solutions comme VMware, qui nécessitent souvent des [versions payantes](#) ou des configurations [plus complexes](#) pour accéder aux mêmes fonctions.



Sur VMM, cliquer sur la machine virtuelle puis appuyer sur le bouton  Pour 'ouvrir' la machine virtuelle.

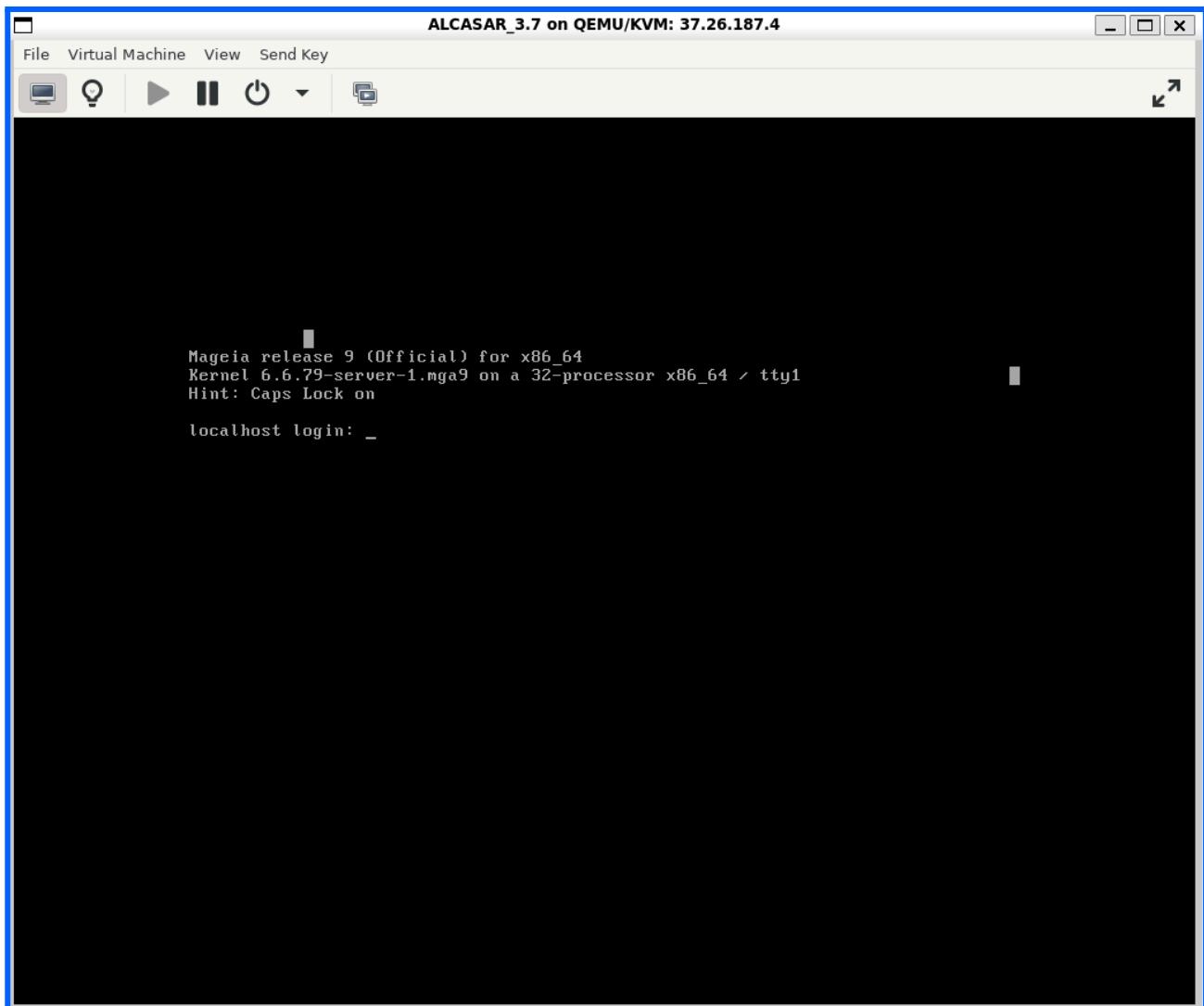
La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) - 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io



Le bouton "Open" permet d'[ouvrir la console graphique](#) d'une machine virtuelle pour interagir avec elle [comme si on était devant son écran](#).

Une fois la machine virtuelle ouverte on peut cliquer sur l'icône en forme d'ampoule pour accéder aux paramètres détaillés de la VM.

C'est ici qu'on va [configurer le PCI Passthrough](#), pour donner un accès direct à deux cartes réseaux physique.

La Plateforme Formation

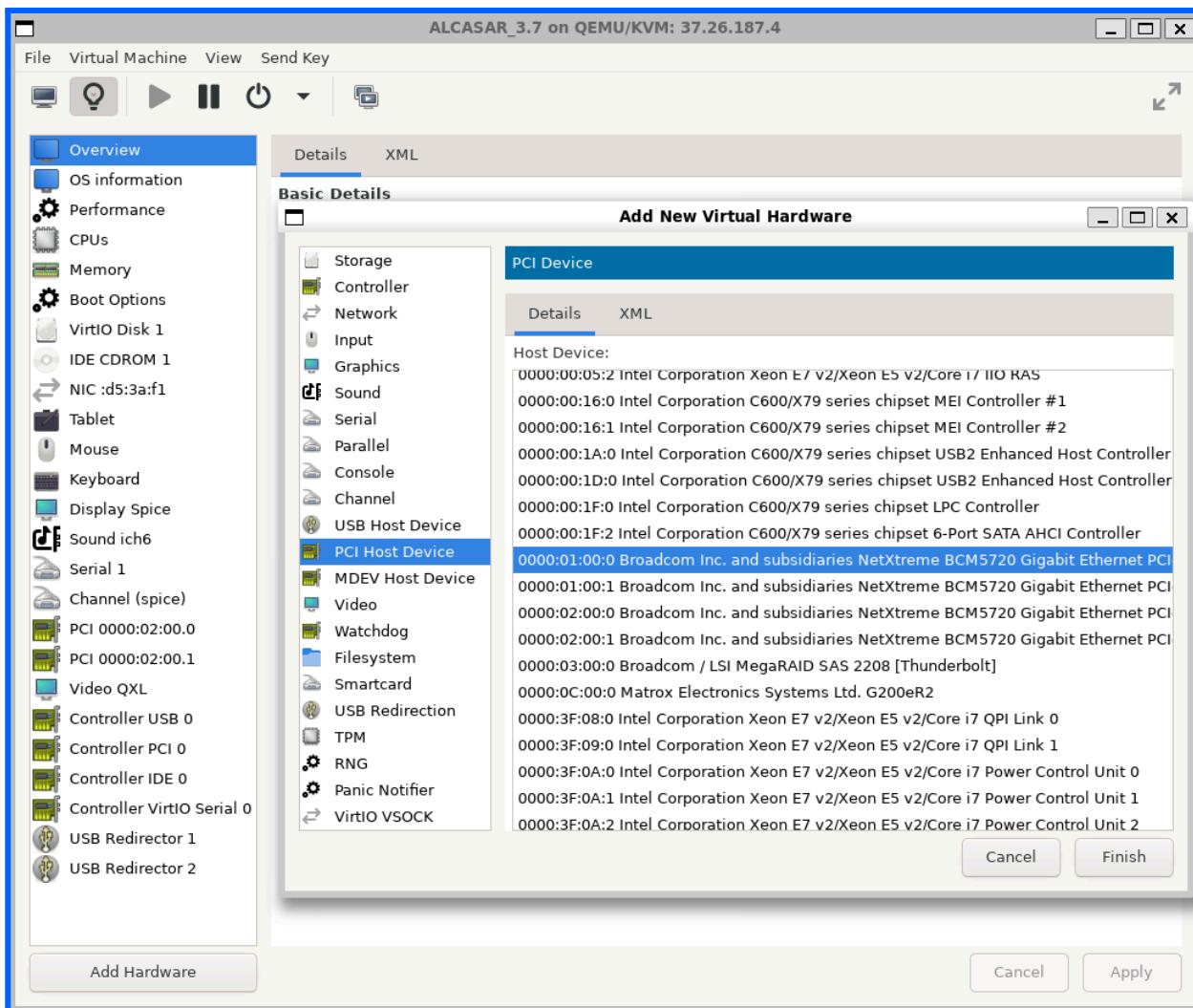
Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) – 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

La Plateforme



Après avoir cliqué sur l'[icône en forme d'ampoule](#) pour accéder aux paramètres de la VM, je clique sur "[Add Hardware](#)", puis je sélectionne "[PCI Host Device](#)". À cet endroit, je vois la liste de [tous les périphériques PCI disponibles](#) sur le serveur. Il me suffit alors de retrouver les deux cartes réseau que j'avais repérées précédemment [grâce à leur adresse PCI et leurs noms](#), ce qui me permet de les identifier facilement pour les ajouter à la VM.

J'ai choisis ces 2 interfaces réseaux:

```
02:00.0 Ethernet controller: Broadcom Inc. and subsidiaries NetXtreme BCM5720 Gigabit Ethernet PCIe  
02:00.1 Ethernet controller: Broadcom Inc. and subsidiaries NetXtreme BCM5720 Gigabit Ethernet PCIe
```

Sur VMM :



La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) - 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

La Plateforme

• Installation et configuration de Mageia

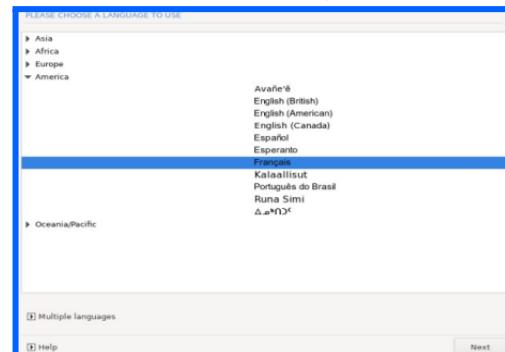
Je vais maintenant procéder à l'[installation du système d'exploitation Mageia 9](#). Pour cela, je récupère l'[ISO](#) directement depuis le site officiel d'ALCASAR, car il s'agit d'une [image préconfigurée de Mageia 9](#) qui contient déjà le [script d'installation d'ALCASAR](#) intégré, ce qui facilite grandement la mise en place d'ALCASAR.

Il faut maintenant [suivre les étapes suivantes](#) lors de l'installation de Mageia pour configurer correctement le système en vue d'accueillir ALCASAR :

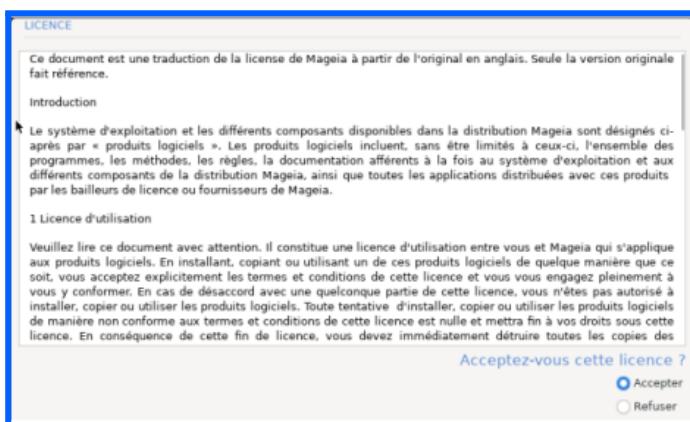
1) install Mageia



2) Choisir la langue



3) Accepter la licence



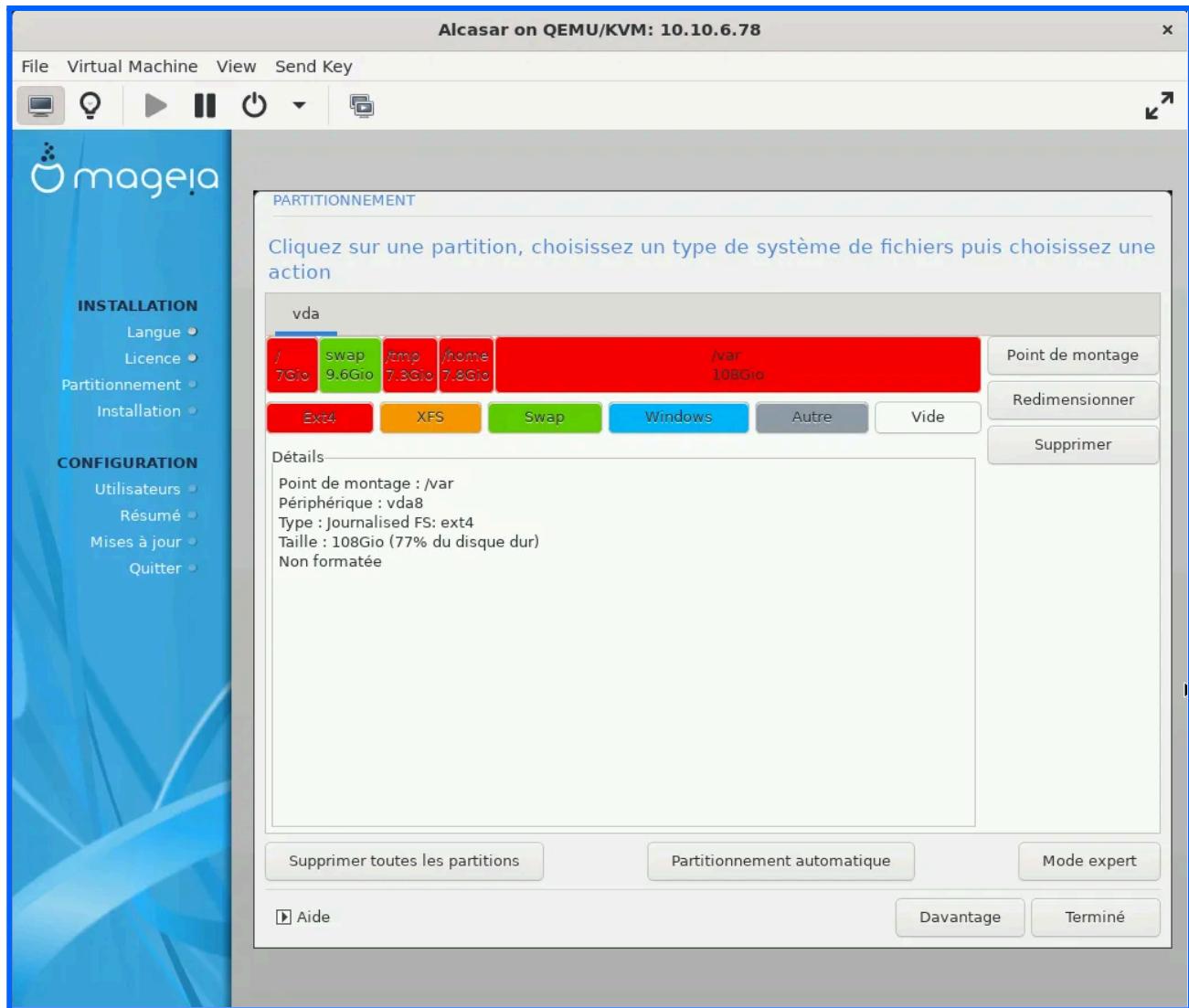
4) Disposition du clavier



5) Lors du partitionnement du disque, il faut faire le partitionnement de disque personnalisé et créer les partitions imposé par Alcasar



La Plateforme



Selon les besoins d'Alcasar, il faut au moins:

- / : 10 Go - type : Journalised FS: ext4
- swap : 5 Go - type : Linux swap
- /tmp : 5 Go - type : Journalised FS : ext4
- /home : 5 Go - type : Journalised FS : ext4
- /var : le reste du disque dur (10 Go mini) - type : Journalised FS :ext4

La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) – 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

La Plateforme

6) Création de l'user sysadmin et configuration du mot de passe root

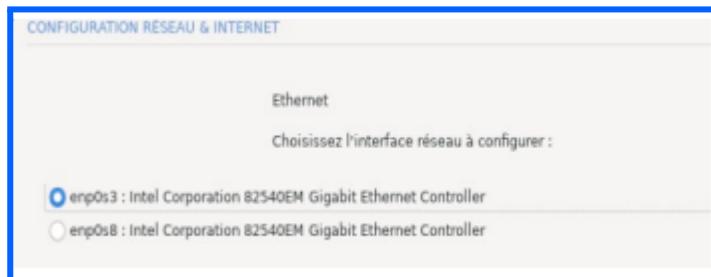


The screenshot shows the 'Gestion des utilisateurs' (User Management) interface. It displays two sets of fields for creating a new user:

- Definissez le mot de passe administrateur (root):**
 - Mot de passe: *********
 - Mot de passe (vérification): *********
- Tapez un nom d'utilisateur:**
 - Nom et prénom: **sysadmin**
 - Identifiant de connexion: **sysadmin**
 - Mot de passe: *********
 - Mot de passe (vérification): *********

7) Configuration de la première interface réseau, celle connectée à internet :

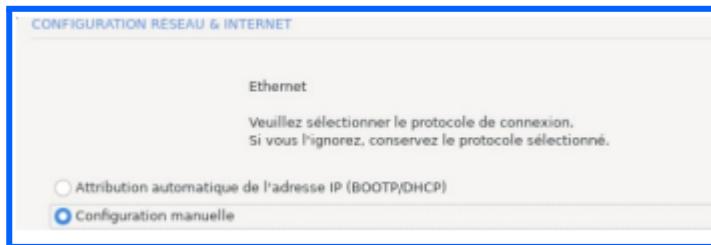
-Premièrement choisir l'interface qu'on veut utiliser comme réseau externe



The screenshot shows the 'CONFIGURATION RESEAU & INTERNET' (Network & Internet Configuration) interface. It lists two network interfaces:

- enp0s3 : Intel Corporation 82540EM Gigabit Ethernet Controller** (selected)
- enp0s8 : Intel Corporation 82540EM Gigabit Ethernet Controller** (not selected)

-Configuration manuelle



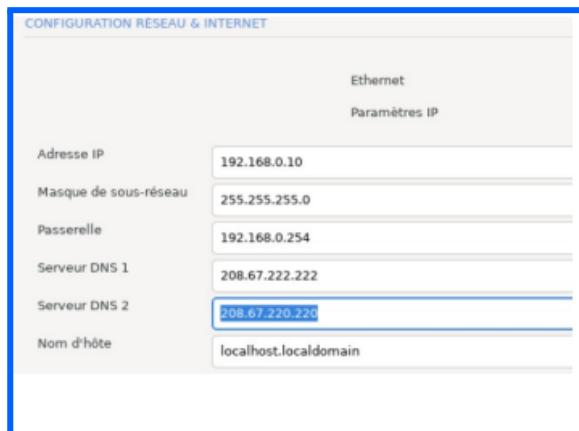
The screenshot shows the 'CONFIGURATION RESEAU & INTERNET' (Network & Internet Configuration) interface. It provides instructions for selecting a connection protocol:

Ethernet
Choisissez l'interface réseau à configurer :

enp0s3 : Intel Corporation 82540EM Gigabit Ethernet Controller
 enp0s8 : Intel Corporation 82540EM Gigabit Ethernet Controller

Attribution automatique de l'adresse IP (BOOTP/DHCP)
 Configuration manuelle

-Configuration du réseau : nous allons donner une des IP Publique de Free Pro



The screenshot shows the 'PARAMETRES IP' (IP Parameters) section of the network configuration. It includes the following fields:

	Paramètres IP
Adresse IP	192.168.0.10
Masque de sous-réseau	255.255.255.0
Passerelle	192.168.0.254
Serveur DNS 1	208.67.222.222
Serveur DNS 2	208.67.220.220
Nom d'hôte	localhost.localdomain

La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) - 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

La Plateforme

Adresse IP : 37.26.187.5

Masque de sous-réseau : 255.255.255.248

Passerelle : 37.26.187.1

Serveur DNS 1 : 8.8.8.8

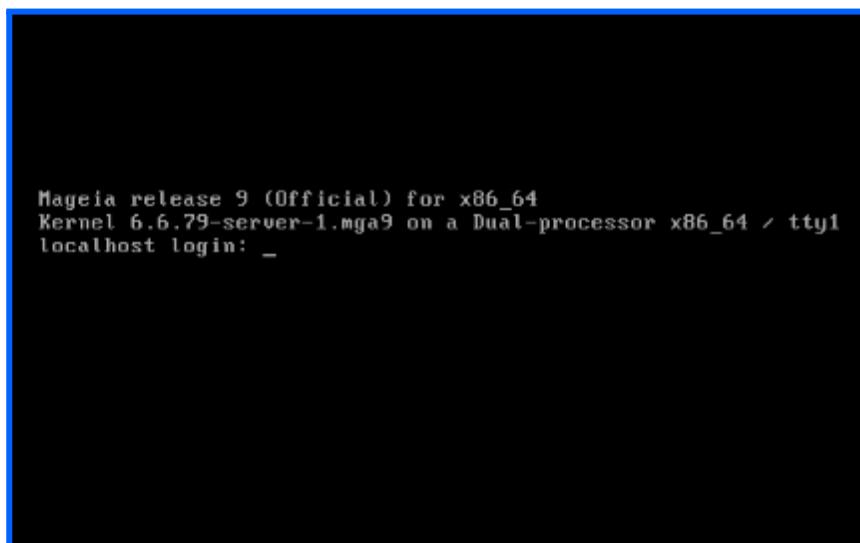
Serveur DNS 2 : 8.8.4.4

Nom d'hôte : localhost.localdomain (on laisse par défaut pour l'instant)

Tout a bien été configuré, il suffit d'appuyer sur 'Suivant' et finaliser



- Installation et configuration d'ALCASAR



La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) – 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

La Plateforme

Je vais maintenant lancer le script d'installation d'ALCASAR. Ce script va automatiquement configurer tous les éléments nécessaires au bon fonctionnement de la solution, y compris la deuxième interface réseau en mode interne.

Pour se faire, il faut aller dans le répertoire de l'user root (~)

```
[root@localhost var]# cd  
[root@localhost ~]# ls  
aif-mount/ alcasar-3.7.0/ drakx/ tmp/  
[root@localhost ~]# _
```

A l'intérieur du dossier `alcasar-3.7.0/`
il faut exécuter le script `alcasar.sh`

```
[root@localhost alcasar-3.7.0]# ls  
alcasar.sh* conf/ iso/ scripts/ VERSION  
blacklist/ gpl-3.0.fr.txt README.md SECURITY.md web/  
CHANGELOG.md gpl-3.0.txt rpms/ TODO.md  
[root@localhost alcasar-3.7.0]# sh alcasar.sh -i_
```

Accepter les termes de la licence ALCASAR, et l'installation se lancera.

```
ALCASAR V3.7.0 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) ? : _
```

La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) – 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

La Plateforme

Ecran de fin d'installation d'ALCASAR

```
s-nail: Warning: $LOGNAME (sysadmin) not identical to user (root)!  
s-nail: Warning: $USER (sysadmin) not identical to user (root)!  
Création du fichier de configuration GRUB®  
Thème trouvé : /boot/grub2/themes/maggy/theme.txt  
Image Linux trouvée : /boot/vmlinuz-6.6.79-server-1.mga9  
Image mémoire initiale trouvée : /boot/initrd-6.6.79-server-1.mga9.img  
Ajout de l'entrée du menu d'amorçage pour les paramètres du firmware UEFI à  
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.lan  
  
Appuyez sur 'Entrée' pour continuer  
-
```

ALCASAR a été configuré et installé avec succès.

```
db      88      ,ad8888ba,      db      ad88888ba      db      88888888ba  
d88b    88      d8''  ''8b      d88b    d8"    "8b      d88b    88      "8b  
d8''8b  88      d8'      d8'8b    88,      d8'8b    88      ,8P  
d8' '8b  88      88      d8' '8b    '8aaaaaa,      d8' '8b    88aaaaaa8P'  
d8YaaaaaY8b  88      88      d8YaaaaaY8b    "8b,      d8YaaaaaY8b    88"8b'  
d8"8b    88      88,      d8"8b    '8b      d8"8b    88      '8b  
d8'     '8b    88a.     .a8P  d8'      '8b  88a     a8P d8'      '8b  88      '8b  
d8'     '8b    888888888888  "Y8888Y"  d8'      '8b  "Y8888P"  d8'      '8b  88      '8b  
  
Bienvenue sur ALCASAR Version 3.6.0 (Mageia 8)  
Connectez-vous à l'URL 'https://alcasar.localdomain/acc'  
Kernel 5.15.82-server-1.mga8 on a Dual-processor x86_64 / tty1  
alcasar login: sysadmin  
Password:  
Last login: Mon May  5 11:54:01 from 192.168.182.5  
alcasar-formelaplate[~]$ su  
Mot de passe :  
alcasar-formelaplate[~$ ls
```

La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) - 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

La Plateforme

Courte démonstration des fonctionnalités de l'admin panel d'alcasar :

-se rendre sur *alcasar.localdomain/acc*

Il y plusieurs options disponible :

Home, System, Authentication, Filtering, Statistics, Backup

The screenshot shows the ALCASAR Control Center interface. At the top, there's a header with the ALCASAR logo and a 'Main' button. Below the header, the dashboard displays system status: Internet access (LAN, Router, DNS), installed version (3.6.0), available version (3.7.2), number of users (0), and system date (Wednesday, 16 July 2025, 22:09:29 CEST). On the left, a navigation menu lists: HOME, SYSTEM, AUTHENTICATION, FILTERING, STATISTICS, and BACKUPS. The AUTHENTICATION item is currently selected. At the bottom, a message says 'System information : alcasar (10.10.0.1)'.

System :

The screenshot shows the 'SYSTEM' section of the navigation menu. It includes sub-options: Network, Services, and LDAP/A.D.

Network

→ Permet de configurer les interfaces réseau, les adresses IP, les DNS, les passerelles, etc.

Services

→ Donne accès à la gestion des services actifs sur ALCASAR (comme le portail captif, le DHCP, le DNS, etc.). On peut y activer/désactiver ou redémarrer certains services critiques.

LDAP/A.D.

→ Sert à connecter ALCASAR à un annuaire LDAP ou Active Directory. On y configure l'URL du serveur, la base DN, les filtres d'authentification, etc.

Authentication :

The screenshot shows the 'AUTHENTICATION' section of the navigation menu. It includes sub-options: Activity, Create users, Manage users, Create a group, Manage groups, Import / Empty, Exceptions, SMS registration, E-mail registration, and a separator line for FILTERING, STATISTICS, and BACKUPS.

Activity

→ permet de visualiser les connexions en cours, leurs MAC etc.

Create users

→ pour créer manuellement un ou plusieurs utilisateurs.

Manage users

→ gérer les utilisateurs existants (modifier, désactiver, supprimer, etc.).

Create a group

→ pour créer des groupes d'utilisateurs.

Manage groups

→ gérer les groupes (attribution de droits, modification, suppression).

Import / Empty

→ pour importer une liste d'utilisateurs (via fichier CSV) ou vider la base.

La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) - 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

La Plateforme

Exceptions

→définir des sites web qui sont accessibles sans avoir besoin de se connecter au portail captif (exemple gmail etc..)

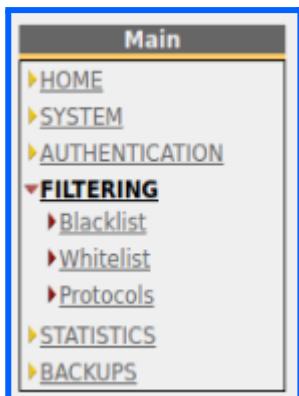
SMS registration

→permet de configurer l'inscription par SMS si activée.

E-mail registration

→permet de configurer une inscription par e-mail.

FILTERING :



Blacklist

→permet de bloquer l'accès à certains sites ou domaines indésirables (ex.: réseaux sociaux, sites pour adultes, etc.).

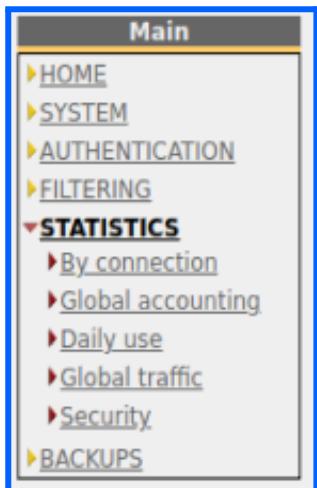
Whitelist

→permet d'autoriser certains sites à passer à travers le filtrage, même s'ils figurent dans une catégorie généralement bloquée.

Protocols

→permet de bloquer ou autoriser certains protocoles réseau (comme icmp SSH, etc.).

STATISTICS :



By connection

→visualiser les connexions actives ou passées des utilisateurs.

Global accounting

→affiche un résumé de l'activité réseau par utilisateur (temps de connexion, bande passante utilisée, etc.).

Daily use

→montre une vue journalière de l'utilisation d'Internet.

Global traffic

→donne une vue d'ensemble du trafic entrant et sortant sur le réseau.

Security

→affiche les événements de sécurité détectés (tentatives suspectes, attaques bloquées, etc.).

La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) - 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

La Plateforme

BACKUPS :

Main

- ▶ HOME
- ▶ SYSTEM
- ▶ AUTHENTICATION
- ▶ FILTERING
- ▶ STATISTICS
- ▶ BACKUPS
 - ▶ Archives
 - ▶ accountability logs

Archives

→ permet de télécharger ou restaurer des sauvegardes de la configuration ou des données d'ALCASAR (utilisateurs, filtres, etc.).

Accountability logs :

→ donne accès aux journaux de traçabilité, c'est-à-dire les logs de connexion qui permettent de savoir qui s'est connecté, quand et depuis quelle machine.

Création d'utilisateur :

Main

ALCASAR

Users management

Create a user

Login	<input type="text"/>
Password	<input type="password"/> generate <input type="button"/>
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"/>
Antivirus & domain Filtering	<input type="button"/>
Network protocols filtering	<input type="button"/>
Keeping sessions alive	<input type="button"/>
Voucher language	Français <input type="button"/>

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.

User Manager :

Main

ALCASAR

Users management

Search filter

Search criteria	Value (empty = all)
Login	<input type="text"/>

Start search

#	User	Actions	Member of group
1	moufid		

La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) - 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

La Plateforme

- Snapshot de la machine virtuelle

Une **snapshot** est une **sauvegarde de l'état d'un système** à un instant donné. Avant d'effectuer la moindre modification sur ma machine virtuelle, je réalise systématiquement une **snapshot** afin de pouvoir **revenir en arrière facilement** en cas de problème ou de mauvaise manipulation.

Pour créer une **snapshot** :

```
>virsh snapshot-create-as --domain ALCASAR_3.7 --name "avant_ldap_update"  
--description "Snapshot avant la mise en place de mon annuaire LDAP Google"
```

Pour lister les **snapshots actuelles** :

```
>virsh snapshot-list ALCASAR_3.7
```

Pour afficher les détails d'une **snapshot** :

```
>virsh snapshot-info --domain ALCASAR --current
```

Pour revenir à une **snapshot** (faire une restauration) :

```
>virsh shutdown --domain ALCASAR (éteindre la vm dans un premier temps)  
>virsh snapshot-revert --domain ALCASAR_3.7 --snapshotname "avant_ldap_update"  
--running
```

Pour supprimer une **snapshot** :

```
>virsh snapshot-delete --domain ALCASAR_3.7 --snapshotname "avant_ldap_update"
```

Scripter les snapshots de façon régulière :

```
GNU nano 7.2                                     snapshot_auto.sh *
```

```
#!/bin/bash

VM_NAME="ALCASAR_3.7"
DATE=$(date +'%Y-%m-%d_%H-%M')
SNAP_NAME="auto_snapshot_$DATE"
DESCRIPTION="Snapshot automatique créée le $DATE"

virsh snapshot-create-as --domain "$VM_NAME" --name "$SNAP_NAME" --description "$DESCRIPTION"
```

Rendre le script exécutable :

```
>sudo chmod +x /usr/local/bin/snapshot_auto.sh
```

Automatiser le script avec cron, de sorte à ce qu'il se lance chaque semaine :

```
>sudo crontab -e  
>0 3 * * 1 /usr/local/bin/snapshot_auto.sh >> /var/log/snapshot_kvm.log 2>&1
```

La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) – 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

La Plateforme

- Mise en place de l'annuaire Google LDAP sur Alcasar

Par défaut, ALCASAR utilise une base de données MySQL locale pour gérer les comptes utilisateurs. Mais dans une volonté de centralisation et de simplification de la gestion, j'ai voulu connecter ALCASAR à l'annuaire LDAP de l'entreprise, car nous utilisons beaucoup Google Workspace.

L'objectif est que lorsqu'on supprime un compte Google, le compte ALCASAR associé soit automatiquement désactivé également, afin de garder une cohérence globale, surtout que notre entreprise s'appuie fortement sur les outils de la suite Google.

PROBLEME

Les LDAP externe ne fonctionnent pas initialement sur Alcasar.

ALCASAR a été conçu à la base pour fonctionner avec un annuaire LDAP classique (OpenLDAP) hébergé en interne.

Les scripts ALCASAR sont très spécifiques. Ils s'attendent à un schéma LDAP classique, avec des champs bien définis (uid, cn, memberOf, etc.).

Or, chez Google, ces champs ne sont pas toujours nommés pareil ou sont même protégés

J'ai également contacté les développeurs de ALCASAR, car étant une solution open-source, il y a un forum très actif avec les développeurs de ALCASAR et des centaines d'utilisateurs qui aident à améliorer la solution.

Les développeurs eux-mêmes ont signalé que l'intégration LDAP externe (surtout avec Google) est soit :

- instable,
- obsolète,
- non testée,
- ou jamais vraiment terminée.

TROUVER LA SOLUTION

Afin de trouver une solution et réussir à connecter mon annuaire LDAP externe à ALCASAR (à la place du LDAP interne imposé par défaut) j'ai identifié deux pistes possibles que je vais explorer.

La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) - 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

MÉTHODE 1:

Dans cette [première méthode](#), j'ai configuré ALCASAR pour qu'il utilise notre annuaire [LDAP externe Google Workspace](#) à la place de [la base MySQL locale](#). Pour cela, j'ai récupéré [la clé et le certificat LDAP](#), que j'ai placés dans les répertoires système appropriés. J'ai ensuite [modifié le fichier alcasar.conf](#) pour y renseigner les informations de connexion LDAP ainsi que les chemins vers les fichiers TLS.

ALCASAR comporte de [nombreux scripts internes liés à ALCASAR](#), chacun ayant une [fonction précise](#) (gestion réseau, logs, utilisateurs, LDAP, mises à jour, etc.).

```
alcasar-formelaplate[~]# cd /usr/local/bin/
alcasar-formelaplate[~]# ls
alcasar-activity_report.sh    alcasar-dhcp.sh          alcasar-list-ip_gw.sh      alcasar-ticket-clean.sh
alcasar-archive.sh            alcasar-dns-local.sh    alcasar-logout.sh        alcasar-tot_stats
alcasar-bl-autoupdate.sh     alcasar-file-clean.sh   alcasar-macup.sh         alcasar-truncate_radacct
alcasar-bl.sh                 alcasar-flush_ipset_wl.sh alcasar-mail-install.sh  alcasar-uninstall.sh
alcasar-bypass.sh             alcasar-generate_log.sh  alcasar-monthly_tot_stats  alcasar-url_filter_bl.sh
alcasar-CA.sh                 alcasar-https.sh       alcasar-mysql.sh        alcasar-url_filter_wl.sh
alcasar-clean_radacct        alcasar-importcert.sh   alcasar-network.sh      alcasar-version.sh
alcasar-condown.sh           alcasar-iot_capture.sh  alcasar-profile.sh      alcasar-watchdog-hl.sh
alcasar-conf.sh               alcasar-iptables-bypass.sh alcasar-rpm-download.sh  alcasar-wifi4eu.sh
alcasar-conup.sh              alcasar-iptables.sh     alcasar-rpm.sh         alcasar-wifi4eu.sh
alcasar-daemon.sh            alcasar-ldap.sh        alcasar-sms.sh         alcasar-ssh.sh
alcasar-db-migrations        alcasar-letsencrypt.sh  alcasar-ssh.sh
```

J'ai repéré le [script dédié à la gestion du LDAP](#) dans ALCASAR, nommé `alcasar-ldap.sh`, situé dans le répertoire [Le script `alcasar-ldap.sh` a dû être \[modifié\]\(#\) afin de \[prendre en charge ces paramètres\]\(#\), notamment dans la section TLS du module FreeRADIUS. Enfin, j'ai \[remplacé la page `ldap.php`\]\(#\) de l'interface web d'administration pour pouvoir gérer cette configuration LDAP directement depuis le dashboard.](/usr/local/bin/. C'est ce script qui permet de configurer et d'activer la connexion à un annuaire LDAP.</p></div><div data-bbox=)

Cette méthode [m'a permis de faire fonctionner ALCASAR](#) avec notre annuaire Google, malgré les limitations initiales du système.

Processus de la méthode 1:

Méthode 1 : Intégration directe avec `alcasar-ldap.sh`

La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) - 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

La Plateforme

Principe : on modifie directement les scripts et la configuration LDAP d'ALCASAR (TLS, certificat, script alcasar-ldap.sh, FreeRADIUS, etc.).

•Récupérer sa clé et son certificat LDAP Google Workspace:

Renommer la clé en **ldap.key** et le certificat en **ldap.pem** puis les déplacer dans les dossiers suivant :

```
>cp ldap.pem /etc/pki/tls/certs/ldap.pem  
>cp ldap.key /etc/pki/tls/private/ldap.key
```

•On peut tester si on arrive à communiquer avec son serveur ldap grâce à la commande ldapsearch :

```
>LDAPTLS_CERT=/etc/pki/tls/certs/ldap.pem  
LDAPTLS_KEY=/etc/pki/tls/private/ldap.key ldapsearch -x -D CN=Utilisateur -w  
MotDePasse -H ldaps://ldap.google.com:636 -b DC=domain,DC=com -d1
```

•Configuration à faire dans le fichier /usr/local/etc/alcasar.conf :

LDAP_SERVER (server) : ldap.google.com (ou 216.239.32.58)
LDAP_USER (identity) = 'Utilisateur_qui_a_accès_a_la_base'
LDAP_PASSWORD (password) = 'mot_de_passe'
LDAP_BASE (base_dn) = 'dc=domain;dc=com'
LDAP_UID (uid) = uid

Ajouter les lignes suivante dans le fichier alcasar.conf :

```
LDAP_CERT= /etc/pki/tls/certs/ldap.pem  
LDAP_KEY= /etc/pki/tls/private/ldap.key
```

Exécuter le script alcasar-ldap.sh avec nos modifications :

```
>alcasar-ldap.sh --on
```

Modifications apportées au script :

- Modification de la définition de la syntaxe d'utilisation du script

```
usage="Usage: alcasar-ldap.sh {--on or -on } | {--off or -off} | --import-cert {certificatePath} | --import-ldap-cert {certificatePath}  
| --import-ldap-key {keyPath} | --delete-ldap-cert {certificatePath} | --delete-ldap-key {keyPath} | --test [-d]"
```

La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) – 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

La Plateforme

-Ajout de variables pour importer le certificat et la clé depuis les lignes qu'on a ajouté dans alcasar.conf

```
LDAP CERT LOC='/etc/raddb/certs/alcasar-ldaps.crt'
LDAP KEY LOC=$(grep '^LDAP KEY=' $CONF_FILE | cut -d"=" -f2)
LDAP CERT LOC=$(grep '^LDAP CERT=' $CONF_FILE | cut -d"=" -f2)
LDAP SERVER=$(grep '^LDAP SERVER=' $CONF_FILE | cut -d"=" -f2)
LDAP USER=$(grep '^LDAP USER=' $CONF_FILE | cut -d"=" -f2)
LDAP PASSWORD=$(grep '^LDAP PASSWORD=' $CONF_FILE | cut -d"=" -f2)
```

```
LDAP CERT LOC='/etc/raddb/certs/alcasar-ldaps.crt'
LDAP SERVER=$(grep '^LDAP SERVER=' $CONF_FILE | cut -d"=" -f2)
LDAP USER=$(grep '^LDAP USER=' $CONF_FILE | cut -d"=" -f2)
LDAP PASSWORD=$(grep '^LDAP PASSWORD=' $CONF_FILE | cut -d"=" -f2)
```

-Modification de la section TLS dans le module ldap alcasar en mettant le contenu de la variable LDAP_CERT_LOC et LDAP_KEY_LOC au bon endroit (dans /etc/raddb/mods-available/ldap-alcasar) :

```
# Modification de la section TLS

$SED '/^#\?s*certificate_file =/ s/^#/' $LDAP_MODULE
$SED "s@^#\?t\tcertificate_file =.*@t\tcertificate_file = $LDAP_CERT_LOC@g" $LDAP_MODULE

$SED '/^#\?s*private_key_file =/ s/^#/' $LDAP_MODULE
$SED "s@^#\?t\tpublic_key_file =.*@t\tpublic_key_file = $LDAP_KEY_LOC@g" $LDAP_MODULE
```

-Création de nouvelles options pour le script :

```
--import-ldap-cert) --delete-ldap-cert)
--import-ldap-key) --delete-ldap-key)
```

•Il faut également modifier la page ldap.php pour pouvoir modifier la configuration à partir du dashboard administrateur:

sur

>/var/www/html/acc/admin/ldap.php

2 champs :

LDAP_CERT → chemin vers le certificat (ex : /etc/pki/tls/certs/ldap.pem)

LDAP_KEY → chemin vers la clé privée (ex : /etc/pki/tls/private/ldap.key)

Ces deux nouvelles variable enregistre directement les valeurs dans le fichier /usr/local/etc/alcasar.conf

Méthode 1 terminée ;

On peut dès à présent se connecter sur ALCASAR avec les utilisateurs présent dans l'annuaire LDAP (Google par exemple)

La Plateforme

Processus de la méthode 2 :

Méthode 1 : via un proxy avec Stunnel

Principe : on utilise Stunnel comme proxy sécurisé local. Il intercepte les connexions LDAP classiques sur 127.0.0.1:1636 et les redirige vers ldap.google.com:636 (LDAPS).

•Récupérer sa clé et son certificat LDAP Google Workspace:

Renommer la clé en ldap.key et le certificat en ldap.pem puis les déplacer aux bon endroits :

```
>cp ldap.pem /etc/pki/tls/certs/ldap.pem  
>cp ldap.key /etc/pki/tls/private/ldap.key
```

•Utiliser stunnel en tant que proxy pour connecter notre serveur

ALCASAR à LDAP:

Télécharger le paquet stunnel :

```
>urpmi stunnel
```

Modifier le fichier de configuration stunnel.conf :

```
>nano /etc/stunnel/stunnel.conf
```

Insérer dans stunnel.conf :

[ldap]

client = yes

accept = 127.0.0.1:1636

connect = ldap.google.com:636

cert = /etc/pki/tls/certs/ldap.pem

key = /etc/pki/tls/private/ldap.key

Démarrer Stunnel avec la configuration qu'on a créer ci-dessus:

```
>sudo stunnel /etc/stunnel/stunnel.conf
```

```
>systemctl restart stunnel
```

(si erreur, kill le process)

La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) – 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

La Plateforme

•**Tester le bon fonctionnement de la configuration LDAP :**

Nous allons utiliser **la commande ldapsearch** qui est une commande utilisée pour **effectuer des recherches LDAP** pour tester si la connexion est bien établi entre notre serveur ALCASAR et l'annuaire LDAP:

```
>ldapsearch -H ldap://127.0.0.1:1636 -D CN=Utilisateur -w MotDePasse -b  
DC=domain,DC=com
```

•**Configurer L'Authentification LDAP :**

Configuration sur l'interface administrateur :

Se rendre sur <http://alcasar.localdomain/acc>

→SYSTEM

 └ LDAP/A.D.



(remplir les champs en dessous (jusqu'à DN minimum))

Secure connection = NO

Car en local, nous sommes en ldap:// et non en ldaps://



Dans cette méthode, j'utilise Stunnel comme **proxy sécurisé** pour permettre à ALCASAR de se **connecter à un annuaire LDAP externe**, en l'occurrence celui de Google Workspace.

Le principe est simple : ALCASAR envoie ses requêtes LDAP vers 127.0.0.1:1636, ce qui correspond à une connexion locale non sécurisée. Stunnel intercepte ces requêtes et les redirige en toute transparence vers le serveur LDAP de Google en LDAPS (port 636, sécurisé), en utilisant une clé et un certificat.

La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) – 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

La Plateforme

Du point de vue d'ALCASAR, il ne s'agit que d'[une connexion LDAP classique](#), donc je configure l'interface web en laissant l'option "Secure connection" sur NO, puisque la sécurisation est prise en charge par Stunnel.

Cette méthode permet [d'éviter les modifications internes d'ALCASAR](#) tout en bénéficiant d'une communication sécurisée avec un annuaire LDAP externe.

Méthode 1 (modification script alcasar) contre la méthode 2 (proxy) laquelle choisir ?

Méthode 1: via un proxy avec Stunnel

Avantages :

- › Plus simple à mettre en place
- › Aucune modification des scripts internes d'ALCASAR
- › Compatible avec l'interface graphique d'administration (SYSTEM > LDAP/A.D.)

Inconvénients :

- › Nécessite que Stunnel tourne en permanence
- › Moins intégré "nativement", on contourne la vraie gestion LDAP d'ALCASAR

Méthode 2 : Intégration directe avec alcasar-ldap.sh

Avantages :

- › Intégration plus propre et native avec ALCASAR

Inconvénients :

- › Beaucoup plus technique et compliqué
- › Nécessite de modifier plusieurs fichiers critiques
- › Moins maintenable si ALCASAR est mis à jour

La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) – 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

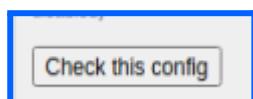
La Plateforme

Ce que j'ai fait :

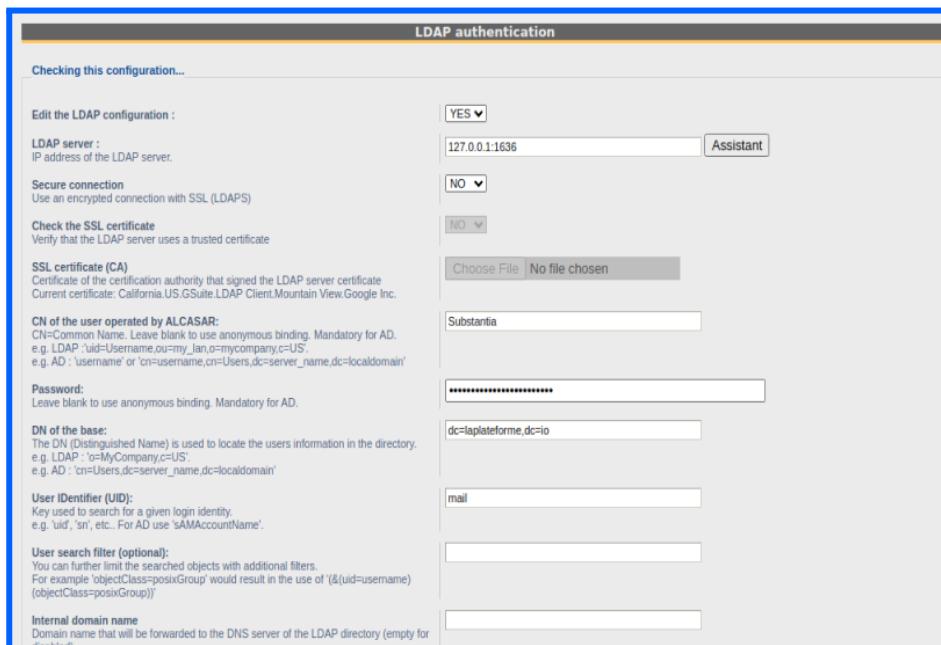
J'ai finalement [retenu la méthode utilisant Stunnel](#), car elle est plus [simple à mettre en place](#), ne nécessite pas de modifier les fichiers internes d'ALCASAR, et permet une [connexion sécurisée au LDAP externe tout en restant parfaitement compatible avec l'interface web d'administration](#).

Comme je l'ai déjà mentionné, [ALCASAR est une solution open source portée par une communauté active](#), notamment via leur [forum officiel](#) où les utilisateurs s'entraident régulièrement. En constatant que [je n'étais pas le seul à rencontrer ce problème de connexion à un LDAP externe](#), j'ai eu envie de contribuer à mon tour en partageant une solution accessible. La méthode via proxy Stunnel, beaucoup [plus simple à mettre en œuvre et surtout plus adaptée aux personnes moins à l'aise techniquement](#), m'a donc paru être la meilleure option à documenter et proposer.

Il y a le bouton 'Check this config' qui permet de vérifier si la connexion a bien pu être établie vers l'annuaire LDAP.



Après avoir vérifié que toutes les informations saisies dans cette interface étaient correctes (adresse du serveur LDAP, identifiants, base DN, attributs utilisateur, etc.), j'ai validé la configuration



The screenshot shows the 'LDAP authentication' configuration page. At the top, there's a progress bar indicating 'Checking this configuration...'. Below it, various configuration fields are displayed:

- LDAP server :** IP address of the LDAP server. Set to '127.0.0.1:1636'.
- Secure connection :** Use an encrypted connection with SSL (LDAPS). Set to 'NO'.
- SSL certificate (CA) :** Certificate of the certification authority that signed the LDAP server certificate. Current certificate: California.U.S.CSuite.LDAP Client.Mountain View.Google Inc.
- CN of the user operated by ALCASAR :** Leave blank to use anonymous binding. Mandatory for AD. Examples: e.g. LDAP : 'uid=Username,ou=my_lan,o=mycompany,c=US'; e.g. AD : 'cn=Username,dc=Users,dc=server_name,dc=localdomain'
- Password :** Leave blank to use anonymous binding. Mandatory for AD.
- DN of the base :** The DN (Distinguished Name) is used to locate the users information in the directory. Examples: e.g. LDAP : 'o=MyCompany,c=US'; e.g. AD : 'cn=Users,dc=server_name,dc=localdomain'
- User identifier (UID) :** Key used to search for a given login identity. Examples: e.g. 'uid', 'sn', etc.. For AD use 'sAMAccountName'.
- User search filter (optional) :** You can further limit the searched objects with additional filters. Example: 'objectClass=posixGroup' would result in the use of '(&(uid=username)(objectClass=posixGroup))'
- Internal domain name :** Domain name that will be forwarded to the DNS server of the LDAP directory (empty for local)

La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) - 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

La Plateforme

On peut voir ici que la connexion LDAP a bien été établie avec succès, et qu'ALCASAR parvient à accéder à l'annuaire distant, en reconnaissant les 1849 entrées présentes dans la base. Cela confirme que l'authentification fonctionne correctement via le proxy Stunnel.

LDAP authentication

A port 389 (636 with SSL) is open on this server
A LDAP connexion is established
Successful authentication
DN of the base seems to be ok (1849 entries in the base)

Edit the LDAP configuration :

LDAP server :

Secure connection

Check the SSL certificate

SSL certificate (CA)
Certificate of the certification authority that signed the LDAP server certificate
Current certificate: California.US.GSuite.LDAP Client.Mountain View.Google Inc.

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'

Password:

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'

User IDentifier (UID):
Key used to search for a given login identity.
e.g. 'uid', 'sn' etc.. For AD use 'sAMAccountName'.

La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) – 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

La Plateforme

Connexion avec un user classique MySQL local :

The screenshot shows a login form titled "Access Control". It features a logo of a penguin wearing a beret and a green camouflage jacket. The "User" field contains "moufid" and the "Password" field contains "...". A blue "Authentication" button is centered below the fields. Below the form, a link "Register by E-mail" is visible. To the right of the form, a circular seal with the text "ALCASAR" is displayed.

Information System Security

- That control was set up regulations to ensure traceability, accountability and non-repudiation of connections.
- The recorded data can be able to be operated by a judicial authority in the course of an investigation.
- Your activity on the network is registered in accordance with privacy.
- These data will be automatically deleted after one year.
- [Click here](#) to change your password or to integrate the security certificate in your browser

The screenshot shows a success message "Successful authentication." above a "Welcome moufid" greeting. It displays session statistics:

- Max Session Time: unlimited
- Max Idle Time: unlimited
- Start Time: 7/17/2025, 5:48:00 PM
- Session Time: 02s
- Idle Time: 01s
- Downloaded: 7.14 Kilobytes
- Uploaded: 104 Bytes

A warning at the bottom states: "(Warning: you will be disconnected if you close this window)". On the right side, a sidebar shows "Your last 3 connections" with two entries: "17 Jul 2025 - 19:01:57" and "17 Jul 2025 - 19:01:56".

La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) – 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

Connexion avec mon email gmail :

The screenshot shows the 'Access Control' login interface. At the top, the logo 'formelaplate' is displayed. Below it, the title 'Access Control' is centered. On the left, there is a small icon of a penguin wearing a beret and a camouflage jacket. To its right, there are two input fields: 'User' containing 'moufid.adoum.pro@laplateforme.io' and 'Password' containing '*****'. Below these fields is a blue button labeled 'Authentication'. At the bottom left, a link 'Register by E-mail' is visible. The background features a dark blue theme with binary code patterns and a circular seal on the right that reads 'ALCASAR'.

Information System Security

- That control was set up regulations to ensure traceability, accountability and non-repudiation of connections.
- The recorded data can be able to be operated by a judicial authority in the course of an investigation.
- Your activity on the network is registered in accordance with privacy.
- These data will be automatically deleted after one year.
- [Click here](#) to change your password or to integrate the security certificate in your browser

The screenshot shows the 'Successful authentication.' page. It features the same penguin icon and seal as the previous screen. The main message 'Successful authentication.' is prominently displayed. Below it, the user's welcome message 'Welcome moufid.adoum.pro@laplateforme.io' is shown. A table provides session details:

Max Session Time:	unlimited
Max Idle Time:	unlimited
Start Time:	7/17/2025, 5:47:21 PM
Session Time:	03s
Idle Time:	02s
Downloaded:	19.2 Kilobytes
Uploaded:	5.7 Kilobytes

(Warning: you will be disconnected if you close this window)

Your last 3 connections

- 17 Jul 2025 - 19:01:17
- 15 Jul 2025 - 16:26:01
- 22 May 2024 - 19:28:42

La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) – 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

La Plateforme

La problématique de la connexion à un annuaire LDAP externe a été résolue avec succès, grâce à la mise en place d'un proxy sécurisé via Stunnel qui permet à ALCASAR d'interagir correctement avec l'annuaire distant.

- Mise en place d'une règle de sécurité SSH

Afin de renforcer la sécurité du serveur ALCASAR, j'ai mis en place une règle iptables personnalisée visant à restreindre l'accès SSH uniquement à une adresse IP autorisée. Toute tentative non autorisée est automatiquement bloquée et journalisée, permettant une traçabilité complète des connexions rejetées.

Pour modifier du script de règles locales

il faut éditer le fichier suivant : </usr/local/etc/alcasar-iptables-local.sh>

iptables -A INPUT -p tcp --dport 2222 -s 88.187.64.209 -j ACCEPT

→Cette ligne permet d'autoriser les connexion SSH uniquement depuis mon adresse IP

iptables -A INPUT -p tcp --dport 2222 -j DROP

→Cette ligne permet de bloquer toute les autres connexions SSH

iptables -A INPUT -p tcp --dport 2222 -j LOG --log-prefix "Tentative de connexion SSH Bloqué "

→Cette ligne permet de journaliser toutes les tentatives de connexion refusée

Afin que les modifications soient appliquées:

exécuter : </usr/local/bin/alcasar-iptables.sh>

La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) – 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

La Plateforme

- Envoie d'un email d'alert à chaque connexion en SSH au serveur

Installation des outils nécessaire :

```
>sudo apt update  
>sudo apt install bsd-mailx msmt
```

Création d'un fichier de configuration personnel

```
>nano ~/.msmtprc
```

```
account default  
host smtp.gmail.com  
port 587  
auth on  
tls on  
tls_starttls on  
user adoummoufid0@gmail.com  
password ***** (mot de passe application généré spécialement pour msmt)  
from adoummoufid0@gmail.com
```

Sécuriser le fichier (car il contient des infos sensibles (mot de passe))

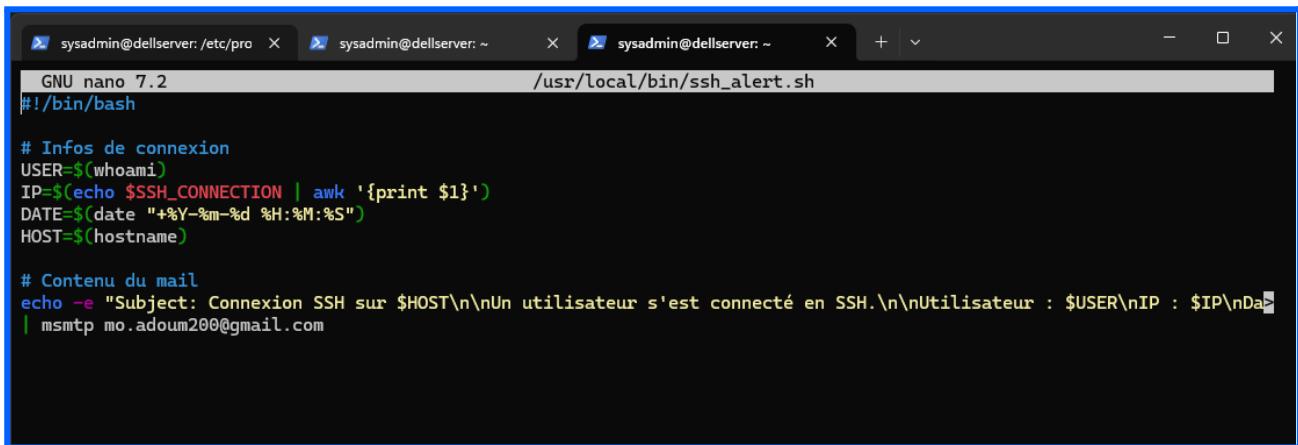
```
>chmod 600 ~/.msmtprc
```

Test d'email :

```
>echo -e "Hello" | msmt moufid.adoum.pro@laplateforme.io
```

Création d'un script qui envoie une notification à chaque connexion SSH

```
>sudo nano /usr/local/bin/ssh_alert.sh
```



```
sysadmin@dellserver: /etc/pro X sysadmin@dellserver: ~ X sysadmin@dellserver: ~ X + - □ ×  
GNU nano 7.2 /usr/local/bin/ssh_alert.sh  
#!/bin/bash  
  
# Infos de connexion  
USER=$(whoami)  
IP=$(echo $SSH_CONNECTION | awk '{print $1}')  
DATE=$(date "+%Y-%m-%d %H:%M:%S")  
HOST=$(hostname)  
  
# Contenu du mail  
echo -e "Subject: Connexion SSH sur $HOST\n\nUn utilisateur s'est connecté en SSH.\n\nUtilisateur : $USER\nIP : $IP\nDate : $DATE\nHOST : $HOST" | msmt mo.adoum200@gmail.com
```

```
>sudo chmod +x /usr/local/bin/ssh_alert.sh
```

La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

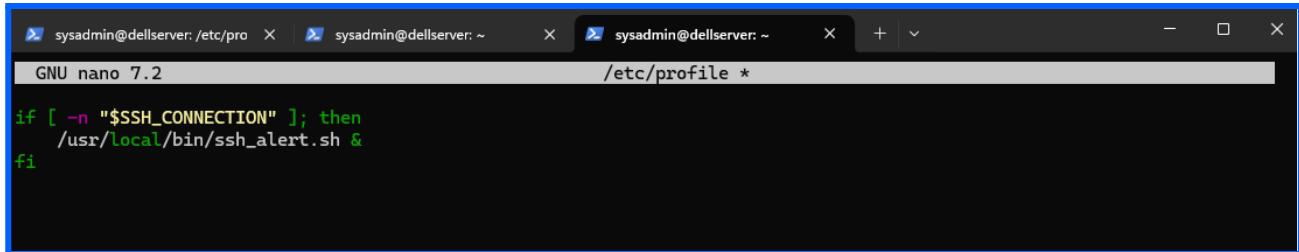
Dont le siège social est situé à Marseille (13007) – 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

La Plateforme

Modification du fichier /etc/profile pour qu'il s'exécute automatiquement

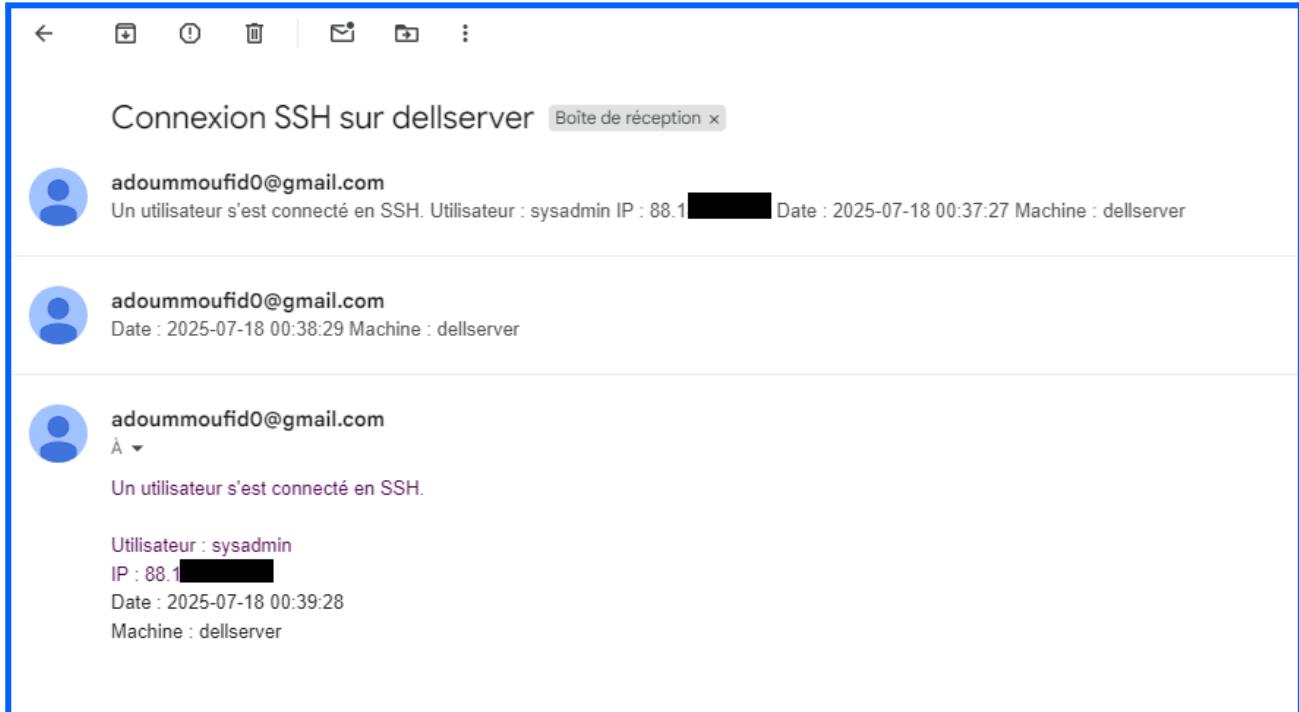
>sudo nano /etc/profile



```
GNU nano 7.2          /etc/profile *
```

```
if [ -n "$SSH_CONNECTION" ]; then
    /usr/local/bin/ssh_alert.sh &
fi
```

à présent, à chaque connexion SSH, je vais recevoir un email semblable à celui-ci :



Connexion SSH sur dellserver Boîte de réception x

adoummoufid0@gmail.com
Un utilisateur s'est connecté en SSH. Utilisateur : sysadmin IP : 88.1 [REDACTED] Date : 2025-07-18 00:37:27 Machine : dellserver

adoummoufid0@gmail.com
Date : 2025-07-18 00:38:29 Machine : dellserver

adoummoufid0@gmail.com
À ▾
Un utilisateur s'est connecté en SSH.
Utilisateur : sysadmin
IP : 88.1 [REDACTED]
Date : 2025-07-18 00:39:28
Machine : dellserver

La mise en place d'[une alerte mail à chaque connexion SSH](#) permet de [renforcer la sécurité du serveur](#) en assurant une [traçabilité en temps réel des accès](#). Elle permet de [déetecter immédiatement toute connexion non autorisée ou suspecte](#), ce qui facilite la réactivité face à une [tentative d'intrusion](#).

La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) – 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

La Plateforme

A FAIRE A L'AVENIR :

À l'avenir, il serait pertinent de mettre en place une supervision complète de ma VM (voir de mes VMs), avec d'une part Zabbix pour le monitoring en temps réel des ressources et des services, et d'autre part la stack ELK pour l'analyse centralisée des logs, la détection d'événements critiques et la génération de rapports avancés.

Zabbix et ELK sont deux solutions complémentaires :

Zabbix permet un monitoring en temps réel des performances système et réseau (CPU, RAM, services, etc.), tandis que la stack ELK se spécialise dans la centralisation et l'analyse des logs pour détecter des anomalies ou comportements suspects.

Mettre en place les deux permettrait donc d'avoir une visibilité complète sur l'état de ma VM : à la fois en temps réel avec Zabbix, et en profondeur grâce à ELK pour l'analyse post-événement et le reporting de sécurité.

- Mise en place de Zabbix

Le point positif est que la documentation officielle de Zabbix est particulièrement complète et bien structurée. Elle permet de sélectionner sa version, son système d'exploitation, ainsi que les composants souhaités, pour ensuite générer automatiquement les commandes adaptées à l'environnement cible, ce qui facilite grandement l'installation et la configuration.

1 Choisissez votre plateforme

VERSION DE ZABBIX	OS DISTRIBUTION	VERSION DU SYSTÈME D'EXPLOITATION	ZABBIX COMPONENT	BASE DE DONNÉES	SERVEUR WEB
7.4	Alma Linux	12 Bookworm (amd64, arm64)	Server, Frontend, Agent	MySQL	Apache
7.2	Amazon Linux	11 Bullseye (amd64)	Server, Frontend, Agent 2	PostgreSQL	Nginx
7.0 LTS	CentOS	10 Buster (amd64, i386)	Proxy		
6.0 LTS	Debian		Agent		
	OpenSUSE Leap		Agent 2		
	Oracle Linux		Java Gateway		
	Raspberry Pi OS		Web Service		
	Red Hat Enterprise Linux				
	Rocky Linux				
	SUSE Linux Enterprise Server				
	Ubuntu				

Notes de publication 7.4

La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) - 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

La Plateforme

→ Installation du dépôt de zabbix

```
client@client-virtual-machine:~$ wget https://repo.zabbix.com/zabbix/7.4/release/debian/pool/main/z/zabbix-release/zabbix-release_latest_7.4+debian12_all.deb
--2025-07-22 12:08:27-- https://repo.zabbix.com/zabbix/7.4/release/debian/pool/main/z/zabbix-release/zabbix-release_latest_7.4+debian12_all.deb
Resolving repo.zabbix.com (repo.zabbix.com)... 178.128.6.101, 2604:a880:2:d0::2062:d001
Connecting to repo.zabbix.com (repo.zabbix.com)|178.128.6.101|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7132 (7,0K) [application/octet-stream]
Saving to: 'zabbix-release_latest_7.4+debian12_all.deb'

zabbix-release_latest_7.4+deb 100%[=====] 6,96K --.-KB/s in 0s

2025-07-22 12:08:28 (3,73 GB/s) - 'zabbix-release_latest_7.4+debian12_all.deb' saved [7132/7132]
```

```
client@client-virtual-machine:~$ sudo dpkg -i zabbix-release_latest_7.4+debian12_all.deb
Selecting previously unselected package zabbix-release.
(Reading database ... 208894 files and directories currently installed.)
Preparing to unpack zabbix-release_latest_7.4+debian12_all.deb ...
Unpacking zabbix-release (1:7.4-1+debian12) ...
Setting up zabbix-release (1:7.4-1+debian12) ...
```

→ Installation des composants nécessaires à Zabbix

```
client@virtualmachine:~$ sudo apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
```

→ Création de la base de donnée

> mysql -uroot -p

```
MariaDB [(none)]> create database zabbix character set utf8mb4 collate utf8mb4_bin;
Query OK, 1 row affected (0,000 sec)

MariaDB [(none)]> create user admin@localhost identified by 'root';
Query OK, 0 rows affected (0,001 sec)

MariaDB [(none)]> grant all privileges on zabbix.* to admin@localhost;
Query OK, 0 rows affected (0,001 sec)

MariaDB [(none)]> set global log_bin_trust_function_creators = 1;
Query OK, 0 rows affected (0,000 sec)

MariaDB [(none)]> quit;
Bye
client@virtualmachine:~$ |
```

→ Configuration de la base de donnée Zabbix

```
client@virtualmachine:~$ sudo nano /etc/zabbix/zabbix_server.conf
```

DBPassword='mdp'

→ Démarrer les processus du serveur et de l'agent Zabbix

```
client@virtualmachine:~$ sudo systemctl restart zabbix-server zabbix-agent apache2
client@virtualmachine:~$ sudo systemctl enable zabbix-server zabbix-agent apache2
```

La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) – 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

La Plateforme

→ Se connecter à l'UI Web de Zabbix pour finaliser la configuration :
<http://host/zabbix>

ZABBIX

Bienvenue
Vérification des prérequis
Configurer la connexion à la base de données
Paramètres
Résumé pré-installation
Installer

Bienvenue dans Zabbix 7.4

Langage par défaut: Français (fr_FR)

Retour Prochaine étape

ZABBIX

Vérification des prérequis

	Valeur actuelle	Requis
Version de PHP	8.2.28	8.0.0 OK
Option PHP "memory_limit"	128M	128M OK
Option PHP "post_max_size"	16M	16M OK
Option PHP "upload_max_filesize"	2M	2M OK
Option PHP "max_execution_time"	300	300 OK
Option PHP "max_input_time"	300	300 OK
support de bases de données par PHP	MySQL	OK
bcmath pour PHP	actif	OK
mbstring pour PHP	actif	OK
Option PHP "mbstring.func_overload"	inatif	inatif OK

Retour Prochaine étape

ZABBIX

Configurer la connexion à la base de données

Veuillez créer la base de données manuellement et configurer les paramètres de connexion. Appuyez sur le bouton "Prochaine étape" quand c'est fait.

Type de base de données: MySQL
Hôte base de données: localhost
Port de la base de données: 0
Nom de la base de données: zabbix
Stocker les informations d'identification dans: Texte brut (selected), Coffre HashiCorp, Coffre CyberArk
Utilisateur: zabbix
Mot de passe: ****

Chiffrement TLS de la base de données: La connexion ne sera pas chiffrée car elle utilise un fichier socket (sous Unix) ou de la mémoire partagée (Windows).

Retour Prochaine étape

ZABBIX

Paramètres

Nom du serveur Zabbix: DELL Server
Fuseau horaire par défaut: Système: (UTC+00:00) UTC
Thème par défaut: Bleu
Encrypt connections from Web interface:

Bienvenue
Vérification des prérequis
Configurer la connexion à la base de données
Paramètres
Résumé pré-installation
Installer

Retour Prochaine étape

ZABBIX

Global view

Top hosts by CPU utilization

Host name	Utilisation	1m avg	5m avg	15m avg	Processus
Zabbix server	0.37 %	0.08	0.02	0.00	345

Information système

Paramètre	Valeur	Détails
Le serveur Zabbix est en cours d'exécution	Oui	localhost:10051
Version du serveur Zabbix	7.4.0	À jour
Version du frontend Zabbix	7.4.0	À jour
Nombre d'hôtes (activé/désactivé)	1	1 / 0
Nombre de modèles	347	
Nombre d'éléments (activé/désactivé/non supporté)	125	114 / 0 / 11
Nombre de déclencheurs (activé/désactivé/monITORé/ok)	73	73 / 0 [0 / 73]

Disponibilité de l'hôte

Statut	Nombre	Total
Disponible	1	1
Non disponible	0	
Mixte	0	
Inconnu	0	

Problems by severity

Sévérité	Nombre
Désastre	0
Haut	0
Moyen	0
Avertisse...	0
Information	0
Non classé	0

Current problems

Temps	Info	Hôte	Problème	Sévérité	Durée	Actualiser	Actions	Tags
Aucune donnée disponible								

Memory utilization

Values per second

2025-07-22 13:16 (UTC+02:00) Europe/Paris

Memory utilization: 38.45 %

Available memory: 3.25 GB

CPU utilization: 1.71

Map of Riga, Latvia showing monitoring points P1-P4.

Zabbix est maintenant configuré avec succès, je vais ajouter un nouvel hôte afin de le monitorer et explorer les possibilités de Zabbix.

La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) – 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

La Plateforme

L'agent étant déjà installé sur la machine hôte, je procède à sa configuration :

```
client@virtualmachine:~$ sudo nano /etc/zabbix/zabbix_agentd.conf |
```

Dans le fichier conf de l'agent, mettre l'ip du serveur Zabbix

```
GNU nano 7.2                                     /etc/zabbix/zabbix_agentd.conf *
# Mandatory: yes, if StartAgents is not explicitly set to 0
# Default:
# Server=
Server=192.168.163.129
```

```
GNU nano 7.2                                     /etc/zabbix/zabbix_agentd.conf
# Mandatory: no
# Default:
# ServerActive=
ServerActive=192.168.163.129
```

>sudo systemctl enable --now zabbix-agent

>sudo systemctl status zabbix-agent

Maintenant, je vais ouvrir le port TCP 10050 dans mon pare-feu.

Ce port est utilisé par l'[agent Zabbix](#) pour communiquer avec le serveur.

```
client@virtualmachine:~$ sudo ufw allow 10050/tcp|
```

ou

>[sudo iptables -A INPUT -p tcp --dport 10050 -j ACCEPT](#)

De retour sur l'UI Web de Zabbix

The screenshot shows the 'Hôte' (Host) configuration dialog in the Zabbix UI. The 'Nom de l'hôte' field contains 'ZServer'. The 'Nom visible' field contains 'Debian 12 VM'. Under 'Modèles', 'Linux by Zabbix agent' is selected. In the 'Groupes d'hôtes' section, 'Linux servers' is selected. The 'Interfaces' section shows an interface with 'Agent' as the type, '192.168.163.129' as the IP, and '10050' as the port. The 'Surveillé par' section has 'Serveur' selected. At the bottom, there are buttons for 'Actualiser', 'Clone', 'Supprimer', and 'Annuler'.

La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

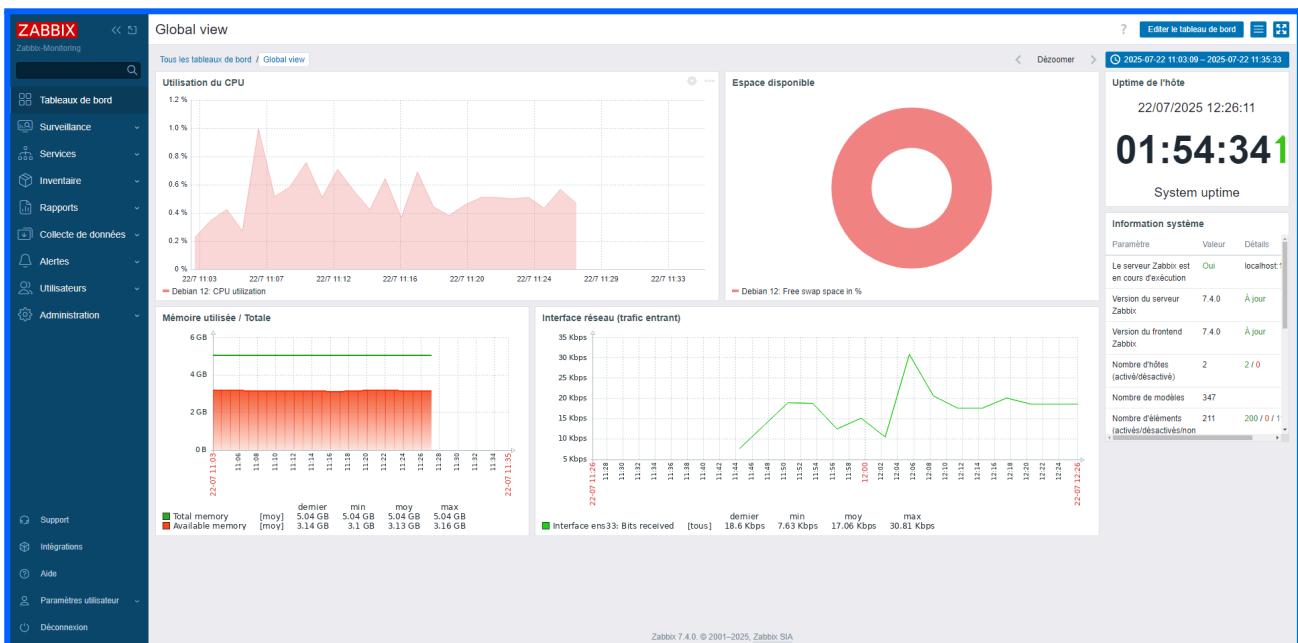
Dont le siège social est situé à Marseille (13007) – 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

La Plateforme



On voit maintenant que cet hôte est activé et disponible, donc que la connexion a bien été établie.



Grâce aux [templates intégrés](#) de Zabbix, je suis en mesure de [superviser facilement](#) des indicateurs clés tels que [l'utilisation de la mémoire](#), du [CPU](#), [l'espace disque disponible](#), [le trafic réseau entrant](#) sur une interface spécifique, ainsi que [le temps de fonctionnement \(uptime\)](#) de ma machine. Zabbix offre de nombreuses [autres possibilités de surveillance](#), et son interface graphique à la fois [claire et intuitive](#) permet un suivi [efficace et agréable](#) des [composants essentiels](#) d'un système.

Comment ajouter un graphique à l'aide d'une template :

[Editer le tableau de bord](#)

This screenshot shows the 'Ajouter un widget' (Add a widget) dialog box. It allows you to create a new graph. The form includes fields for 'Type' (set to 'Graph (classique)'), 'Nom' (Name, set to 'Exemple graph'), 'Intervalle de rafraîchissement' (Refresh interval, set to '10 secondes'), 'Source' (set to 'Graphique simple'), 'Élément' (Element, set to 'Debian 12: CPU idle time'), 'Période de temps' (Time period, set to 'Tableau de bord'), 'Afficher la légende' (Show legend, checked), and 'Remplacer l'hôte' (Replace host, set to 'taper ici pour rechercher'). At the bottom are 'Ajouter' (Add) and 'Annuler' (Cancel) buttons.

La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) - 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

La Plateforme

Lorsqu'on appuie sur le bouton Sélectionner un élément, nous avons une multitude de choix sur ce qu'on veut moniterer :

Nom	Clé	Type	Type d'information	État
Available memory	vm.memory.size[available]	agent Zabbix	Numérique (non signé)	Activé
Available memory in %	vm.memory.size[available]	agent Zabbix	Numérique (flottant)	Activé
Configuration cache, % used	zabbix[cache,buffer,pused]	Zabbix interne	Numérique (flottant)	Activé
Connector queue	zabbix[connector_queue]	Zabbix interne	Numérique (non signé)	Non supporté
Context switches per second	system.cpu.switches	agent Zabbix	Numérique (flottant)	Activé
CPU guest nice time	system.cpu.util[guest_nice]	agent Zabbix	Numérique (flottant)	Activé
CPU guest time	system.cpu.util[guest]	agent Zabbix	Numérique (flottant)	Activé
CPU idle time	system.cpu.util[idle]	agent Zabbix	Numérique (flottant)	Activé
CPU interrupt time	system.cpu.util[interrupt]	agent Zabbix	Numérique (flottant)	Activé
CPU iowait time	system.cpu.util[iowait]	agent Zabbix	Numérique (flottant)	Activé
CPU nice time	system.cpu.util[nice]	agent Zabbix	Numérique (flottant)	Activé
CPU softirq time	system.cpu.util[softirq]	agent Zabbix	Numérique (flottant)	Activé
CPU steal time	system.cpu.util[steal]	agent Zabbix	Numérique (flottant)	Activé
CPU system time	system.cpu.util[system]	agent Zabbix	Numérique (flottant)	Activé
CPU user time	system.cpu.util[user]	agent Zabbix	Numérique (flottant)	Activé
CPU utilization	system.cpu.util	Élément dépendant	Numérique (flottant)	Activé
Discovery queue	zabbix[discovery_queue]	Zabbix interne	Numérique (non signé)	Activé
Free swap space	system.swap.size[free]	agent Zabbix	Numérique (non signé)	Activé
Free swap space in %	system.swap.size[pfree]	agent Zabbix	Numérique (flottant)	Activé
FS [/]: Inodes: Free, in %	vfs.fs.dependent.inode[/,pfree]	Élément dépendant	Numérique (flottant)	Activé
FS [/]: Option: Read-only	vfs.fs.dependent[/,readonly]	Élément dépendant	Numérique (non signé)	Activé
FS [/]: Space: Available	vfs.fs.dependent.size[/,free]	Élément dépendant	Numérique (non signé)	Activé

On peut également mettre en place des [alertes](#) qui nous notifient à chaque incident. On va ici configurer un [alerting par email](#) sur Zabbix.

On se rend sur [Actions](#) puis Actions de déclencheur.

La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) - 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

La Plateforme

On peut ici activer l'option qui permet d'envoyer à l'administrateur zabbix des notifications à chaque alertes :

The screenshot shows a list of users with one item selected. The header bar includes 'Nom', 'Conditions', 'Opérations', 'État' (Active), and 'Info'. A yellow bar at the top says 'Envoyer le message aux groupes d'utilisateurs: Zabbix administrators via tous les médias'. The status for the selected user is 'Désactivé' (Disabled). A footer note says 'Affichage de 1 sur 1 trouvés'.

Mais on peut également mettre en place des alertes plus spécifiques, par exemple à chaque fois que la Mémoire est insuffisante un mail est envoyé. Ici on va choisir d'envoyer un mail à chaque incident.

Ensuite nous allons créer quel type de média sera cette alerte. Une alerte peut être un SMS, un webhook, un e-mail...

Dans Alertes -> Types de média, on va appuyer sur le bouton de création d'un média.

The screenshot shows a list of media types. The left sidebar has 'Alertes' selected under 'Types de média'. The main area has a search bar and filters for 'Nom', 'État' (Active), and 'Désactivé'. A button 'Appliquer' is at the top right. The list includes: 'Brevis.one' (Webhook, Désactivé), 'Discord' (Webhook, Désactivé), 'Email' (Courriel, Désactivé), 'Email (HTML)' (Courriel, Désactivé), 'Event-Driven Ansible' (Webhook, Désactivé), and 'Express.ms' (Webhook, Désactivé). Some entries have notes about SMTP servers: 'serveur SMTP: "mail.ex..."' and 'serveur SMTP: "mail.ex..."'.

Sur le mail qu'on veut utiliser pour envoyer les alertes :

Activer les accès IMAP :

(IMAP = Protocole d'accès à la messagerie Internet)

The screenshot shows the 'Transfert et POP/IMAP' tab in Gmail settings. It includes sections for 'Transfert', 'Téléchargement POP', and 'Accès IMAP'. Under 'Accès IMAP', it says 'Lorsque je marque un message comme supprimé dans IMAP : Active l'effacement automatique, mise à jour immédiate du serveur (par défaut)'. There are also sections for 'Lorsqu'un message est marqué comme supprimé ou effacé du dossier IMAP visible' and 'Instructions de configuration'.

Et également créer un mot de passe d'application pour qu'on puisse envoyer des mail depuis l'adresse email qu'on désiré :

The screenshot shows a page titled 'Mots de passe des applications'. It explains that application passwords are less secure than regular ones. A note says 'Les mots de passe d'application vous permettent de vous connecter à votre compte Google sur des applis et des services plus anciens, non compatibles avec les normes de sécurité les plus récentes.' Below is a section for creating a new password for 'Nom de l'appli: Zabbix'. A 'Créer' button is at the bottom right.

La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) - 14 Traverse Co

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www

La Plateforme

On peut maintenant finaliser la création de l'envoie de mail :

On va utiliser **SMTP** (protocole de communication utilisé pour envoyer et recevoir des messages électroniques sur Internet).

Pour Gmail, le nom de domaine complet du service SMTP est smtp.gmail.com

Nouveau type de média

Type de média **Modèles de messages** Options

* Nom ZabbixMail

Type Courriel

Fournisseur de messagerie Generic SMTP

* serveur SMTP smtp.gmail.com

Port du serveur SMTP 465

* Courriel moufid.adoum@laplateforme.io

SMTP helo gmail.com

Sécurité de la connexion Aucun STARTTLS SSL/TLS

Vérifier le pair SSL

Vérifier l'hôte SSL

Authentification Aucun Nom d'utilisateur et mot de passe OAuth

Nom d'utilisateur moufid.adoum@laplatefor

Mot de passe *****

Format du message HTML Texte brut

Description Zabbix Alert

Activé

Ajouter Annuler

On peut **tester l'envoie de mail** grâce au bouton "Test" à droite du type de média d'alerte qu'on vient de créer

ZabbixMail Courriel Activé Report not supported items, Report not supported low level discovery rules, Report problems to Zabbix administrators, Report unknown triggers serveur SMTP: "smtp.gmail.com", SMTP helo: "gmail.com", courriel: "moufid.adoum@laplateforme.io" Test

Tester le type de média "ZabbixMail"

* Envoyer à mo.adoum200@gmail.com

Sujet TEST EMAIL ZABBIX

* Message Ceci est un message de test de Zabbix pour vérifier que les email fonctionnent bel et bien

Test Annuler

La Plateforme Formation

Société par actions simplifiée

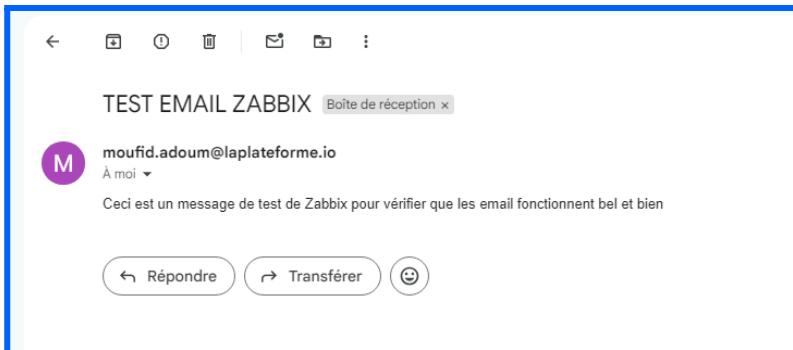
Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) - 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

La Plateforme

Et on peut voir qu'on a bien reçu l'alerte :



A présent, dans Utilisateur -> Utilisateurs -> Admin -> Media, on attribue à l'utilisateur Admin le type de média "email" que j'ai préalablement configuré, afin de lui permettre de recevoir des notifications en cas d'alerte.

A screenshot of the Zabbix 'Utilisateurs' configuration page. On the left is a sidebar with various monitoring sections like Tableaux de bord, Surveillance, Services, Inventaire, Rapports, etc. The main panel shows a form for editing a user named 'Admin'. Fields include Nom d'utilisateur (Admin), Prénom (Zabbix), Nom de famille (Administrateur), Groupes (Internal, Zabbix administrators), Mot de passe (password field), Langue (Valeur système par défaut), Fuseau horaire (Valeur système par défaut (UTC+00:00 UTC)), Thème (Valeur système par défaut), Connexion automatique (checked), Auto-déconnexion (15m), Raffraîchir (30s), Lignes par page (50), and URL (empty). Buttons at the bottom are 'Actualiser', 'Supprimer', and 'Annuler'.

A screenshot of the 'Nouveau média' dialog. It shows a 'Type' dropdown set to 'ZabbixMail'. Under 'Envoyer à', there is an input field with the value 'mo.adoum200@gmail.com' with a 'Supprimer' button. Below it is an 'Ajouter' button. A 'Lorsque actif' field contains the value '1-7,00:00-24:00'. Under 'Utiliser si sévérité', several checkboxes are checked: Non classé, Information, Avertissement, Moyen, Haut, and Désastre. An 'Activé' checkbox is also checked. At the bottom are 'Ajouter' and 'Annuler' buttons.

Dorénavant, à chaque fois qu'une alerte sera détectée sur n'importe lequel de mes hôtes, un mail sera envoyé à cet email.

La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) – 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

La Plateforme

- Mise en place d'ELK

ELK est un ensemble d'outils [open source](#) composé de [Elasticsearch](#), [Logstash](#) et [Kibana](#), utilisé pour [collecter](#), [centraliser](#), [analyser](#) et [visualiser](#) des logs en temps réel. Il est largement utilisé pour le [monitoring](#), le [dépannage](#) et la [cybersécurité](#).

On peut surveiller le CPU ou la mémoire avec ELK en ajoutant des outils comme [Metricbeat](#), mais [Zabbix](#) reste plus pratique et efficace pour le monitoring en temps réel. De son côté, ELK est plus adapté à l'[analyse de logs](#), à la [visualisation de données](#) et à tout ce qui touche à la [détection d'événements](#).

Stack ELK – Elasticsearch

ELK est une suite d'outils composée de :

→ **E = Elasticsearch**

Serveur de recherche et d'indexation hautement scalable, utilisé pour stocker et interroger les données.

→ **L = Logstash**

Outil permettant de collecter, filtrer, transformer et transférer des données (par exemple : des fichiers de logs).

→ **K = Kibana**

Interface web pour explorer, visualiser et gérer les données indexées dans Elasticsearch.

Mise en place d'Elasticsearch :

→ Elasticsearch a besoin de Java pour fonctionner car il est développé en java

```
client@virtualmachine:~$ sudo apt install openjdk-17-jdk
```

```
>java --version
```

→ On définit JAVA_HOME pour que le système et Elasticsearch sachent où Java est installé.

```
GNU nano 7.2                                     /etc/environment
JAVA_HOME="/usr/lib/jvm/java-17-openjdk-amd64"
```

La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) - 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

La Plateforme

→ On charge le nouvel environnement qu'on a défini

```
client@virtualmachine:~$ source /etc/environment
```

→ Ajouter le dépôt officiel d'Elasticsearch

```
> wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor  
-o /usr/share/keyrings/elasticsearch-keyring.gpg
```

```
> echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg]  
https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee  
/etc/apt/sources.list.d/elasticsearch-8.x.list
```

On peut maintenant installer Elasticsearch

```
> sudo apt-get update  
> sudo apt-get install elasticsearch  
> sudo systemctl start elasticsearch  
> sudo systemctl enable elasticsearch  
> sudo systemctl status elasticsearch
```

Configuration d'Elasticsearch :

On modifie le fichier de configuration Yaml d'elasticsearch

Un fichier YML (ou YAML, pour YAML Ain't Markup Language) est un fichier de configuration lisible par l'humain, utilisé pour structurer des données de manière claire et simple. Il est très utilisé dans les outils modernes (comme Docker, Kubernetes, Ansible, GitHub Actions...) car il est facile à lire, léger, et supporte la hiérarchie avec indentation (=le fait de décaler une ligne vers la droite à l'aide d'espaces, pour montrer que cette ligne dépend d'une autre, ou fait partie d'un groupe.) .

```
> sudo nano /etc/elasticsearch/elasticsearch.yml
```

```
GNU nano 7.2          /etc/elasticsearch/elasticsearch.yml
# ----- Network -----
#
# By default Elasticsearch is only accessible on localhost. Set a different
# address here to expose this node on the network:
#
#network.host: 0.0.0.0
#
# By default Elasticsearch listens for HTTP traffic on the first free port it
# finds starting at 9200. Set a specific HTTP port here:
#
#http.port: 9200
#
# For more information, consult the network module documentation.
#
# ----- Discovery -----
#
# Pass an initial list of hosts to perform discovery when this node is started:
# The default list of hosts is ["127.0.0.1", "[::1]"]
#
discovery.seed_hosts: []
#
# Bootstrap the cluster using an initial set of master-eligible nodes:
#
#cluster.initial_master_nodes: ["node-1", "node-2"]
#
# For more information, consult the discovery and cluster formation module documentation.
#
```

La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) – 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

La Plateforme

On décommente network.host et le modifie

Par défaut, Elasticsearch écoute uniquement sur localhost, donc il n'est accessible que depuis la machine locale.

En mettant 0.0.0.0, on dit à Elasticsearch d'écouter toutes les interfaces réseau disponibles (LAN, Wi-Fi, etc.).

Vérifier qu'Elasticsearch fonctionne :

Pour s'assurer qu'il est bien installé et répond aux requêtes, on fait
curl -X GET "localhost:9200" OU <http://192.168.163.129:9200>

```
← → C ⚠ Non sécurisé http://192.168.163.129:9200

Impression élégante □

{
  "name" : "virtualmachine",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "se-ZexQwQT2b83dYb3ZRiA",
  "version" : {
    "number" : "8.18.4",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "43b24f613cf25fd3f3369df174e9535a99512aec",
    "build_date" : "2025-07-16T22:07:56.651816195Z",
    "build_snapshot" : false,
    "lucene_version" : "9.12.1",
    "minimum_wire_compatibility_version" : "7.17.0",
    "minimum_index_compatibility_version" : "7.0.0"
  },
  "tagline" : "You Know, for Search"
}
```

Mise en place de Kibana :

```
>sudo apt-get install kibana  
>sudo systemctl start kibana  
>sudo systemctl enable kibana  
>sudo systemctl status kibana
```

```
client@virtualmachine:~$ sudo systemctl status kibana
● kibana.service - Kibana
   Loaded: loaded (/lib/systemd/system/kibana.service; enabled; preset: enabled)
   Active: active (running) since Tue 2025-07-22 19:58:03 CEST; 6s ago
     Docs: https://www.elastic.co
Main PID: 7576 [kibana]
  Tasks: 11 (limit: 6111)
    Memory: 11.7M
      CPU: 5.528%
       CGroup: /system.slice/kibana.service
               └─ 7576 /usr/share/kibana/bin/_node/glibc-217/bin/node /usr/share/kibana/bin/_node/cld

jul 22 19:58:03 virtualmachine systemd[1]: Started Kibana service - Kibana.
jul 22 19:58:03 virtualmachine kibana[7576]: Kibana is currently running with legacy OpenSSL provider
jul 22 19:58:04 virtualmachine kibana[7576]: {}{"log.level": "INFO", "timestamp": "2025-07-22T19:58:04"
jul 22 19:58:04 virtualmachine kibana[7576]: Native global console methods have been overridden in
jul 22 19:58:05 virtualmachine kibana[7576]: {"log.level": "INFO", "timestamp": "2025-07-22T19:58:05.639400+00:00"}[root] Kibana is
jul 22 19:58:05 virtualmachine kibana[7576]: {"log.level": "INFO", "timestamp": "2025-07-22T19:58:05.657400+00:00"}[INFO][node] Kibana pr
https://www.elastic.co
```

Configurer Kibana :

```
>sudo nano /etc/kibana/kibana.yml  
    server.port: 5601  
    server.host: "0.0.0.0"  
    elasticsearch.hosts: ["http://localhost:9200"]  
>sudo systemctl restart kibana
```

```
server.port: 5601

# Specifies the address to which
# The default is 'localhost', i.e.
# To allow connections from remote
server.host: "0.0.0.0"
```

La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) - 14 Traverse Canoubier

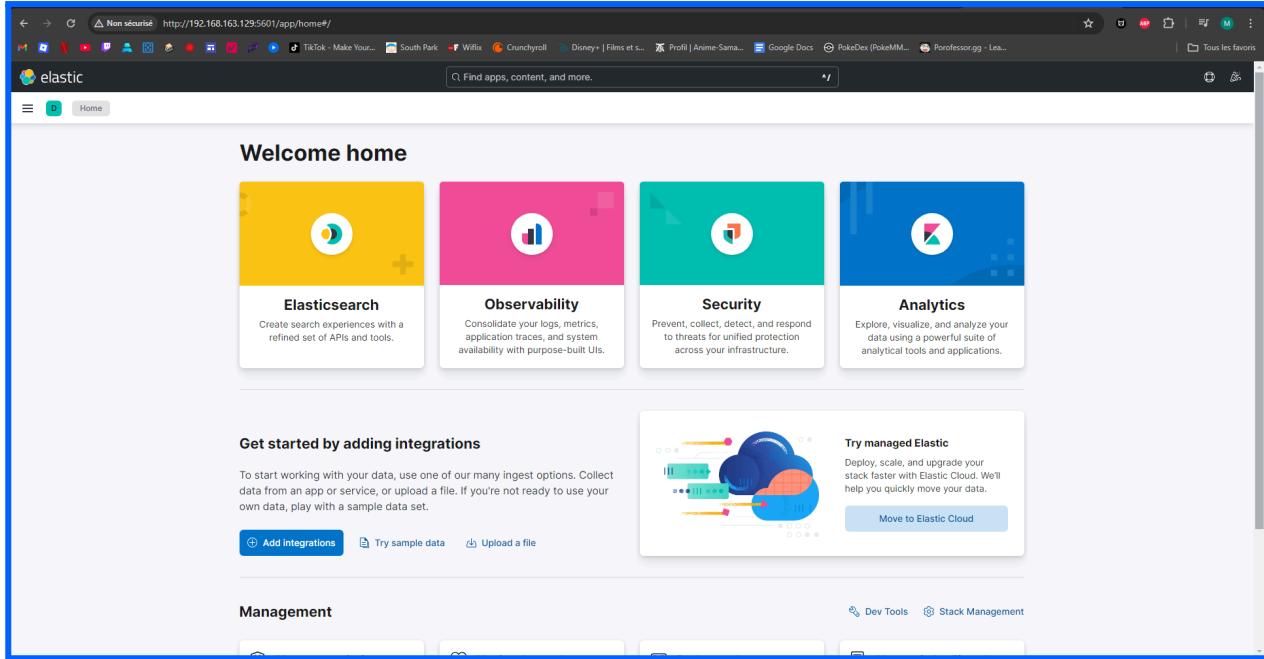
Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

La Plateforme

Vérifier que Kibana fonctionne :

On va vérifier que Kibana fonctionne en entrant dans un navigateur l'ip de ma machine et le port que kibana utilise

<http://192.168.163.129:5601/>



Mise en place de Logstash :

Pour collecter et analyser les logs, nous devons installer [Logstash](#). Les logs collectés et filtrés seront ensuite [stockés dans la base de données Elasticsearch](#).

```
>sudo apt-get install logstash  
>sudo systemctl start logstash  
>sudo systemctl enable logstash  
>sudo systemctl status logstash
```

Mise en place de Filebeat :

Filebeat [collecte et envoie les logs](#) du système ou d'autres applications à [Logstash](#) ou [Elasticsearch](#).

Filebeat → Logstash → Elasticsearch → Kibana

Filebeat lit les fichiers de conf, il les envoie vers Logstash et Logstash applique des filtres complexes et les renvoie ensuite vers Elasticsearch

La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) - 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

La Plateforme

```
>sudo apt-get install filebeat  
>sudo systemctl start filebeat  
>sudo systemctl enable filebeat  
>sudo systemctl status filebeat
```

Configuration de Filebeat :

```
>sudo nano /etc/filebeat/filebeat.yml  
on commente ça
```

```
# ----- Elasticsearch Output -----  
#output.elasticsearch:  
# Array of hosts to connect to.  
# hosts: ["localhost:9200"]
```

On commente cette partie, car [on ne veut pas que Filebeat envoie directement les logs à Elasticsearch](#), mais plutôt à [Logstash](#), qui se chargera de les parser.

parser des logs = Parser des logs, c'est analyser et décomposer automatiquement une ligne de log pour en extraire des informations structurées (lisibles, filtrables, exploitables).

et on décommente ça

```
# ----- Logstash Output -----  
output.logstash:  
# The Logstash hosts  
hosts: ["localhost:5044"]
```

Nous allons activer les modules qu'on veut utiliser.

En activant un module, Filebeat sait automatiquement où trouver les bons fichiers, comment les lire et comment parser les lignes de log, sans qu'on ait à tout faire manuellement.

```
client@virtualmachine:~$ sudo filebeat modules enable system  
Enabled system
```

Le [module system](#) de Filebeat est super utile car il permet de [surveiller automatiquement les connexions SSH](#), les [tentatives sudo](#) et [les messages système](#), sans avoir à tout configurer manuellement.

On peut aussi activer d'autres modules comme apache pour [surveiller les accès à un site web](#), ou mysql pour [détecter des événements importants](#) comme la création de comptes, les erreurs de connexion, ou les requêtes lentes, le tout automatiquement parsé et prêt à être analysé dans Kibana.

La Plateforme Formation

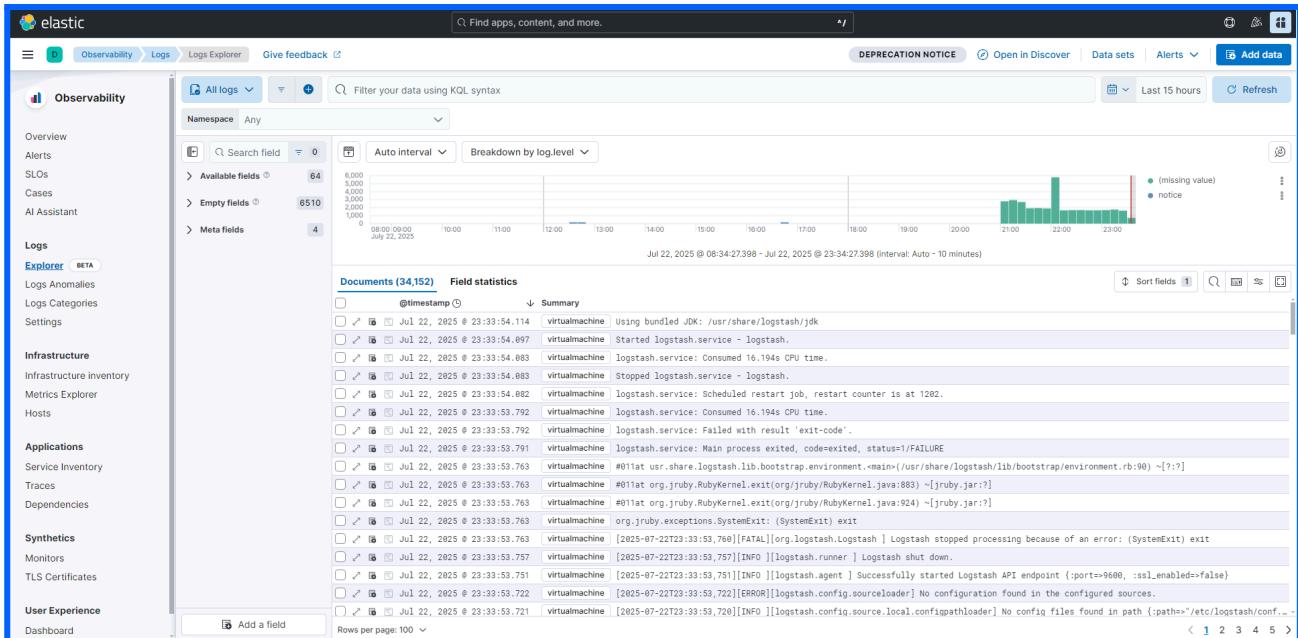
Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) - 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io

La Plateforme



La Plateforme Formation

Société par actions simplifiée

Immatriculée au RCS de Marseille sous le numéro 883 780 496

Dont le siège social est situé à Marseille (13007) – 14 Traverse Canoubier

Tél : 04 84 89 43 69 • email : contact@laplateforme.io • www.laplateforme.io