Le but de ce projet est de mettre en place un template de vm arch linux avec le maximum de sécurité possible mise en place afin d'établir un environnement sécurisé pour mes services.

Pourquoi utiliser archlinux ?

- La distribution est ultra-personnalisable
- La quasi-totalité des services est à installer, on a donc le choix de ce qu'on installe sur la distribution

Point négatif

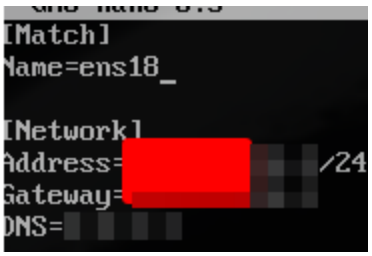
- La distribution est on-release donc il peut y avoir des conflits lors des mises à jours.
- Certains services peuvent être compliqués à mettre en place.

Installation

Disposition du clavier en français :

Mise en place d'une adresse ip statique :

J'applique pour l'instant le DNS de cloudflare tant que je n'ai pas mis en place mon propre DNS



Synchronisation du temps :

```
root@archiso ~ # timedatectl
               Local time: Wed 2025-02-19 10:51:32 UTC
           Universal time: Wed 2025-02-19 10:51:32 UTC
                 RTC time: Wed 2025-02-19 10:51:32
                Time zone: UTC (UTC, +0000)
System clock synchronized: yes
              NTP service: active
          RTC in local TZ: no
root@archiso ~ # _
```

Lister les disques :

```
root@archiso ~ # fdisk -l
Disk /dev/sda: 32 GiB, 34359738368 bytes, 67108864 sectors
sk model: QEMU HARDDISK
its: sectors of 1 * 512 = 512 bytes
ctor size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes


Disk /dev/loop0: 824.93 MiB, 864997376 bytes, 1689448 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
root@archiso ~ # _
```

Partition du disque :

- Création de la partition swap :

```
Device does not contain a recognized partition table.
Created a new DOS (MBR) disklabel with disk identifier 0xcaed195c.

Command (m for help): n
Partition type
   p   primary (0 primary, 0 extended, 4 free)
   e   extended (container for logical partitions)
Select (default p): p
Partition number (1-4, default 1):
First sector (2048-67108863, default 2048):
Last sector, +/-sectors or +/-size{K,M,G,T,P} (2048-67108863, default 67108863): +4GB

Created a new partition 1 of type 'Linux' and of size 3.7 GiB.

Command (m for help): _
```

- Création de la partition (comprenant le reste du disque)

```
Command (m for help): n
Partition type
   p   primary (1 primary, 0 extended, 3 free)
   e   extended (container for logical partitions)
lect (default p): p
rtition number (2-4, default 2): 2
First sector (7815168-67108863, default 7815168):
Last sector, +/-sectors or +/-size{K,M,G,T,P} (7815168-67108863, default 67108863):

Created a new partition 2 of type 'Linux' and of size 28.3 GiB.

Command (m for help): w
The partition table has been altered.
Calling ioctl() to re-read partition table.
Syncing disks.
```

- attribution du system de fichier :

```
root@archiso ~ # mkfs.ext4 /dev/sda2
mke2fs 1.47.2 (1-Jan-2025)
/dev/sda2 contains `DOS/MBR boot sector' data
Proceed anyway? (y,N) y
Discarding device blocks: done
Creating filesystem with 7411712 4k blocks and 1855952 inodes
Filesystem UUID: 95b8654c-bdcf-476d-9c01-74e6df491bec
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
        4096000

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

- Attribution du swap :

```
130 root@archiso ~ # mkswap /dev/sda1
mkswap: /dev/sda1: warning: wiping old swap signature.
Setting up swapspace version 1, size = 3.7 GiB (4000313344 bytes)
no label, UUID=3de921ae-626f-4a34-aa5b-4b8b6030f20d
root@archiso ~ #
```

Création d'un point de montage :

```
root@archiso ~ # mount /dev/sda2 /mnt
```

Démarrage de la partition swap :

```
root@archiso ~ # swapon /dev/sda1
root@archiso ~ #
```

Installation des packets de base et du kernel hardened linux :

```
root@archiso ~ # pacstrap /mnt base linux-hardened linux-hardened-headers linux-firmware
==> Creating install root at /mnt
==> Installing packages to /mnt
:: Synchronizing package databases...
 core                                                116.2 KiB   306 KiB/s 00:
 extra                                                 3.9 MiB   744 KiB/s 00:
```

Configuration du système

Génération du fstab :

```
root@archiso ~ # genfstab -U /mnt >> /mnt/etc/fstab
root@archiso ~ #
```

Nouveau système :

```
root@archiso ~ # arch-chroot /mnt
[root@archiso /]# _
```

configuration de la time zone :

```
[root@archiso /]# ln -sf /usr/share/zoneinfo/Europe/Paris /etc/localtime
[root@archiso /]#
```

génération de adjtime :

```
[root@archiso /]# hwclock --systohc
[root@archiso /]#
```

Retirer le commentaire dans locale.gen :

```
#fr_CH ISO-8859-1
fr_FR.UTF-8 UTF-8
#fr_FR ISO-8859-1
#fr_FR@euro ISO-8859-15
```

Création de /etc/locale.conf :

```
LANG=fr_FR.UTF-8
```

Création de /etc/vconsole.conf:

```
KEYMAP=fr
```

Installation de grub :

```
[root@archiso /]# grub-install --target=i386-pc /dev/sda
Installing for i386-pc platform.
Installation finished. No error reported.
[root@archiso /]#
```

Génération du grub.cfg:

```
[root@archiso /]# grub-mkconfig -o /boot/grub/grub.cfg
Generating grub configuration file ...
Found linux image: /boot/vmlinuz-linux-hardened
Found initrd image: /boot/initramfs-linux-hardened.img
Found fallback initrd image(s) in /boot:  initramfs-linux-hardened-fallback.img
Warning: os-prober will not be executed to detect other bootable partitions.
Systems on them will not be added to the GRUB boot configuration.
Check GRUB_DISABLE_OS_PROBER documentation entry.
Adding boot menu entry for UEFI Firmware Settings ...
done
```

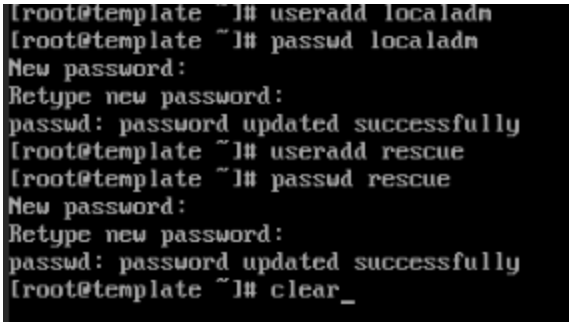
Configuration de initramfs :

On configure un mot de passe pour root avant de redémarrer la machine

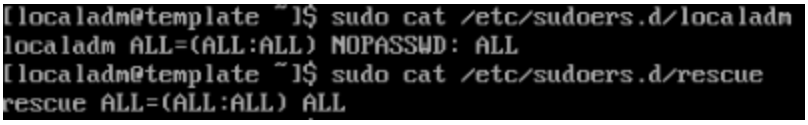
Authentification

Désactivation du compte root :

Ajout de deux utilisateurs :



Configuration sudo des nouveaux users :



Passage des fichiers en readonly :

Double authentification :

Installation d'un système d'authentification à double facteur via google-authentificator
On installe dans un premier temps, les paquets `libpam-google authenticator,ntp et qrencode`

Ces deux paquets sont utilisés pour la génération de token qr code :

par défaut google-authenticator va proposer des options anti man in the middle et anti-brutforce

```
Enter code from app (-1 to skip): 971328
Code confirmed
Your emergency scratch codes are:
   [redacted]

Do you want me to update your "/home/localadm/.google_authenticator" file? (y/n)

Do you want to disallow multiple uses of the same authentication
token? This restricts you to one login about every 30s, but it increases
your chances to notice or even prevent man-in-the-middle attacks (y/n) y

By default, a new token is generated every 30 seconds by the mobile app.
In order to compensate for possible time-skew between the client and the server,
we allow an extra token before and after the current time. This allows for a
time skew of up to 30 seconds between authentication server and client. If you
experience problems with poor time synchronization, you can increase the window
from its default size of 3 permitted codes (one previous code, the current
code, the next code) to 17 permitted codes (the 8 previous codes, the current
code, and the 8 next codes). This will permit for a time skew of up to 4 minutes
between client and server.
Do you want to do so? (y/n) y

If the computer that you are logging into isn't hardened against brute-force
login attempts, you can enable rate-limiting for the authentication module.
By default, this limits attackers to no more than 3 login attempts every 30s.
Do you want to enable rate-limiting? (y/n) y
```

Ajout de la double authentification avec SSH :

Retirer le commentaire de KbdInteractiveAuthentication dans ssh_config.d/99-archlinux.conf

```
# sshd_config defaults on Arch Linux
KbdInteractiveAuthentication yes
UsePAM yes
PrintMotd no
~
```

Modification du fichier de configuration pam.d/sshd :

```
#%PAM-1.0
auth       required   pam_google_authenticator.so
auth       include    system-remote-login
```

Refus de connexion ssh via l'utilisateur root ou rescue :

```
DenyUsers root,rescue
~
```