

**Principes et pratiques de l'administration des
systèmes**

Module 3I015

Semaine 6

1. Déploiement automatique de machines Debian

L'objectif est de déployer via FAI (*Fully Automatic Installation*) une nouvelle machine Linux (installation du client par PXE), comme nous l'avons vu en cours. La machine « serveur » FAI considérée est ssLDAP. Une seule machine (cliente) nommée c2LDAP sera déployée automatiquement. Afin de télécharger les packages nécessaires à l'installation, vous aurez besoin d'un accès à un dépôt Debian et le poste n°2 de la salle de TME est justement un miroir Debian (il simule le serveur ftp du LIP6).

Étape 1 – Installation des packages manquants sur ssLDAP

Comme nous l'avons vu en cours, afin d'installer de nouvelles machines automatiquement, il faut posséder un serveur TFTP ainsi qu'un serveur DHCP. Enfin, votre client (la nouvelle machine installée) bootant par le réseau (par PXE), il faut installer le *boot loader* correspondant. Pour tout cela, installez donc sur ssLDAP via la commande `apt install` les packages suivants :

- tftpd-hpa
- isc-dhcp-server
- syslinux-common
- pxelinux

Étape 2 – Installation des packages manquants sur ssLDAP (bis)

Afin de déployer vos nouvelles machines via FAI, il faut également avoir à disposition les packages contenant FAI. Installez les packages ci-dessous.

- fai-quickstart
- fai-server
- fai-client
- fai-doc
- fai-setup-storage

Étape 3 – Vérification de `/etc/exports` de ssLDAP

Vérifiez que la dernière ligne du fichier `/etc/exports` de ssLDAP contient bien un retour chariot. En effet, FAI va rajouter de nouvelles lignes dans ce fichier. Si la dernière ligne du fichier ne contient pas de retour chariot, ces ajouts produiront une erreur lors de l'installation du serveur FAI.

Étape 4 – Extinction de c1LDAP

Vous pouvez éteindre c1LDAP, qui est inutile pour ce TME et consomme de la RAM inutilement.

Étape 5 – Création du serveur DHCP sur ssLDAP

Sur ssLDAP, configurez un serveur d'adresses DHCP, comme nous l'avons vu en cours (fichiers `/etc/default/isc-dhcp-server` et `/etc/dhcp/dhcpd.conf`) : vous pouvez utiliser la configuration ci-dessous, en remplaçant le *X* des adresses IP par le numéro de votre poste dans la salle de TME.

Notez l'option `routers` qui indiquera à votre client la passerelle à utiliser afin de télécharger les packages se trouvant sur le miroir Debian du poste n°2 (sans cette option, vous ne pourriez rien télécharger et, par conséquent, votre installation échouerait). Notez également l'option `domain-name-servers` qui indiquera à votre client l'adresse IP d'un serveur DNS, qui permettra de communiquer aisément avec le dépôt Debian sur internet si vous travaillez sur votre ordinateur personnel. L'instruction « `range` » indique, quant à elle, la plage d'adresses IP que votre serveur DHCP fournira.

```
option domain-name "3i015_dhcp";
authoritative; # serveur DHCP officiel du réseau

subnet 192.168.X.0 netmask 255.255.255.0 {
    option routers 192.168.X.2;           # la passerelle
    option broadcast-address 192.168.X.255; # le broadcast
    option domain-name-servers 8.8.8.8;   # serveur DNS de google
    default-lease-time 3000;
    max-lease-time 7200;

    pool {
        next-server 192.168.X.2;         # permet tftp/bootp
        filename="fai/pxelinux.0";      # boot loader
        range 192.168.X.100 192.168.X.200; # plage d'adresses
        allow unknown-clients;         # allouees dynamiquement
    }
}
```

N'oubliez pas de redémarrer le service `isc-dhcp-server` via la commande `systemctl` afin que votre configuration soit prise en compte. Vérifiez que le serveur est bien démarré. Si ce n'est pas le cas, arrêtez le serveur via la commande `systemctl`, vérifiez bien avec la commande `ps` qu'aucun process `dhcpd` ne s'exécute et qu'il n'y a pas de fichier `dhcpd.pid` dans `/var/run`. Puis, redémarrez votre serveur DHCP via `systemctl` et assurez-vous qu'il fonctionne bien.

Enfin, n'oubliez pas non plus de pérenniser le démarrage de ce service via un `systemctl enable` lorsque tout fonctionne correctement.

Étape 6 – Mise en place du serveur TFTP sur sSLDAP

Assurez-vous via la commande `systemctl status` que votre serveur `tftpd-hpa` est bien démarré. Si ce n'est pas le cas, démarrez-le.

Étape 7 – Configuration du fichier `/etc/fai/fai.conf`

Il est maintenant temps d'installer votre serveur FAI. La première étape consiste à créer le `nfsroot`. Comme précisé en cours, `nfsroot` est un mini-système Linux qui permettra à votre client de démarrer.

Pour sa création, il faut éditer 3 fichiers :

- /etc/fai/fai.conf
- /etc/fai/nfsroot.conf
- /etc/fai/apt/sources.list

Éditez donc le fichier /etc/fai/fai.conf comme indiqué ci-dessous (vous donnerez comme adresse de serveur FAI celle de la première carte réseau de ssLDAP).

```
SERVER=192.168.X.2
```

```
# URL to access the fai config space
FAI_CONFIG_SRC=nfs://$SERVER/srv/fai/config
```

```
LOGUSER=fai
LOGSERVER=$SERVER
FAI_LOGPROTO=ssh
```

Étape 8 – Configuration des autres fichiers de /etc/fai

Le deuxième fichier à configurer pour installer votre serveur FAI est /etc/fai/nfsroot.conf. Dans ce fichier, on précise le dépôt Debian à utiliser afin de créer le mini-système nfsroot. C'est le rôle des deux lignes suivantes :

```
FAI_DEBOOTSTRAP="buster http://ftp.lip6.fr/pub/linux/distributions/debian"
FAI_DEBOOTSTRAP_OPTS="--exclude=info --include=aptitude --no-check-gpg"
```

 Notez que l'on indique que l'on va utiliser une debian 10 (buster) pour les installations. Par FAI, on peut donc installer d'autres versions de Linux que celle utilisée par le serveur de déploiement.

Enfin, il faut indiquer quel sera le dépôt à utiliser par le client lors de son installation. On spécifie cela dans le fichier /etc/fai/apt/sources.list. Commentez toutes les lignes de ce fichier et rajoutez :

```
deb http://ftp.lip6.fr/pub/linux/distributions/debian buster main contrib non-free
```

Étape 9 – Installation du nfsroot sur ssLDAP

Exécutez la commande `fai-setup -v`. Celle-ci installera votre nfsroot. Si vous affichez le contenu de votre /etc/exports après exécution de cette commande, vous pourrez observer 2 nouvelles lignes, l'une correspondant à /srv/fai/config et l'autre à /srv/fai/nfsroot.

 Si `fai-setup -v` n'a produit aucune erreur, nous vous suggérons de faire un instantané de votre machine virtuelle. En effet, comme vous avez pu le constater, le processus de création du nfsroot est assez long. Si vous faites des erreurs par la suite, vous pourrez revenir à votre instantané et, ainsi, vous dispensez de perdre du temps à recréer votre nfsroot.

Étape 10 – Création du *config space* sur ssLDAP

Le *config space*, l'espace où l'on précise comment les clients doivent être installés, se situe par défaut dans le répertoire `/srv/fai/config`. Créez donc ce dernier.

Un exemple de config space est proposé dans le répertoire `/usr/share/doc/fai-doc/examples/simple`. Copiez donc les fichiers de celui-ci afin d'avoir une première base de travail pour votre *config space* :

```
cp -a /usr/share/doc/fai-doc/examples/simple/* /srv/fai/config
```

Enfin, faites en sorte que le répertoire `/srv/fai/config` et tous les sous-répertoires et fichiers qu'il contient appartiennent à l'utilisateur `fai`.

Étape 11 – Classe X3I015

Dans le répertoire `/srv/fai/config/class` se trouvent les fichiers permettant de sélectionner les classes d'installation ainsi que leurs variables associées (comme nous l'avons vu en cours). Notamment, éditez le fichier `50-host-classes` afin d'indiquer dans le dernier cas du `case` (règle « `*` ») que les machines dont le hostname est non identifié (celles qui sont donc non installées) appartiennent aux classes :

```
FAIBASE DEBIAN X3I015 XORG XFCE
```

FAIBASE et DEBIAN proposent en effet des configurations spécifiques au système Debian. XORG et XFCE contiennent les instructions pour booter en mode graphique avec l'environnement graphique xfce (celui que vous utilisez sur vos machines virtuelles). À ces classes, nous avons rajouté X3I015 qui vous permettra de spécifier les instructions dédiées à votre installation personnalisée (utilisation de LDAP, *etc.*).

Vous pouvez maintenant éditer à votre convenance les fichiers d'extension `.var` de ces classes qui se trouvent dans le même répertoire (`/srv/fai/config/class`). Notamment, n'hésitez pas à indiquer dans le fichier `FAIBASE.var` que votre `TIMEZONE` correspond à celle de Paris et, dans le fichier `DEBIAN.var`, que votre `KEYMAP` est de type `fr-latin1` (clavier azerty).

Étape 12 – Instructions de partitionnement des disques durs des clients

Les instructions de partitionnement des disques durs des machines clientes se situent dans le répertoire `/srv/fai/config/disk_config`. Éditez dans ce répertoire le fichier `FAIBASE` :

```
disk_config disk1 disklabel:msdos bootable:1 fstabkey:uuid
```

```
primary /      20G  ext4  rw,noatime,errors=remount-ro
logical swap   1G   swap  sw
```

Cela permettra de créer un `/` de 20 gigaoctets et un `swap` d'1 gigaoctet.

Étape 13 – Sélection des packages

Dans le répertoire `/srv/fai/config/package_config`, vous devez spécifier les packages que vous souhaitez installer. Pour cela, créez dans ce répertoire un fichier X3I015 et précisez les packages en question. Vous pouvez observer la syntaxe à utiliser dans les autres fichiers du répertoire. Nous vous suggérons d'installer au moins :

- gcc, make et linux-headers-amd64 car ces packages seront nécessaires si vous souhaitez installer par la suite les VirtualBox guest additions sur vos clients (qui vous permettront de faire des copier/coller entre machines virtuelles et de redimensionner vos fenêtres).
- gedit, emacs ou tout autre éditeur de texte que vous utilisez.
- ldap-utils, libnss-ldap et libpam-ldap, pour que vos utilisateurs créés dans LDAP puissent se connecter.
- nfs-common pour pouvoir réaliser les montages NFS.
- dbus-x11 et lightdm-gtk-greeter, qui permettent d'obtenir l'écran de login que vous avez actuellement sur vos machines virtuelles.
- gvfs, exfat-fuse, fuse, exfat-utils et thunar-volman, qui vous permettent de lire/écrire aisément à partir de vos clefs USB dans vos nouvelles machines virtuelles.
- policykit-1 qui permet d'avoir accès aux boutons « éteindre », « redémarrer » et « hiberner » du popup de déconnexion.

Étape 14 – Configuration des packages (1/2)

Éditez le fichier `/srv/fai/config/debconf/DEBIAN` et précisez que votre « locale » est « `fr_FR.UTF-8` ». Indiquez également que votre clavier est français :

```
keyboard-configuration keyboard-configuration/xkb-keymap      select fr
keyboard-configuration keyboard-configuration/variant select French(alternative)
keyboard-configuration keyboard-configuration/model    select Generic 101-key PC
keyboard-configuration keyboard-configuration/layoutcode string fr
```

Étape 15 – Configuration des packages (2/2)

Étant donné que vos utilisateurs sont authentifiés via un annuaire LDAP, vous avez spécifié à l'étape 13 que vous souhaitiez l'installation des packages `libnss-ldap` et `libpam-ldap`. Or, ceux-ci nécessitent une configuration (cf. les `dpkg-reconfigure libnss-ldap` et `dpkg-reconfigure libpam-ldap` que vous avez effectués lors du TME des semaines 3 et 4). Il faut donc également configurer ces packages sur votre machine cliente. L'idée consiste donc à expliciter ces configurations dans un fichier du répertoire `/srv/fai/config/debconf`, par exemple dans un fichier nommé `/srv/fai/config/debconf/X3I015` (du nom de la classe X3I015). Quel contenu mettre dans ce fichier ? Eh bien une configuration identique à celle de `ssLDAP`. Pour l'obtenir, il suffit simplement d'exécuter la commande :

```
debconf-get-selections | grep ldap
```

Si vous copiez l'affichage résultant de cette commande dans le fichier `/srv/fai/config/debconf/X3I015`, lorsque le client s'installera, la tâche « `debconf` » exploitera votre fichier pour configurer automatiquement les packages liés à LDAP.

Étape 16 – Miroir du mk-basefile

Éditez le fichier `/srv/fai/config/basefiles/mk-basefile` et faites en sorte que les variables d'environnement du shell `MIRROR_DEBIAN` et `EXCLUDE_BUSTER` soient respectivement égales à :

- `http://ftp.lip6.fr/pub/linux/distributions/debian/` et
- `info,tasksel,tasksel-data`

Étape 17 – Les fichiers de /etc

Lorsque vous avez installé vos machines mSLDAP, sSLDAP et c1LDAP, vous avez été amené à éditer des fichiers de configuration situés dans le répertoire /etc (ou l'un de ses sous-répertoires). Le répertoire /srv/fai/config/files sert précisément à cet effet lors de l'installation de votre client : en principe, on y reproduit l'arborescence de /etc. Par exemple, pour spécifier la configuration d'un client LDAP (qui se trouve normalement dans le fichier /etc/ldap/ldap.conf), il suffit de créer un fichier /srv/fai/config/files/etc/ldap/ldap.conf/X3I015 dont le contenu est précisément celui du ldap.conf. Notez qu'ici ldap.conf est un répertoire, le fichier contenant la configuration étant X3I015, autrement dit le nom de votre classe d'installation.

Afin de paramétrer correctement l'authentification via LDAP de votre client, placez dans le répertoire /srv/fai/config/files les fichiers de configuration correspondant à :

- /etc/ldap/ldap.conf
- /etc/nsswitch.conf
- /etc/libnss-ldap.secret
- /etc/pam_ldap.secret
- /etc/hosts

Pour ldap.conf, vous pouvez par exemple exécuter les commandes :

```
mkdir -p /srv/fai/config/files/etc/ldap/ldap.conf
cp /etc/ldap/ldap.conf /srv/fai/config/files/etc/ldap/ldap.conf/X3I015
```

puis modifier à votre convenance le fichier /srv/fai/config/files/etc/ldap/ldap.conf/X3I015.



Il faut que l'ensemble des fichiers que vous créez soient accessibles en lecture et les répertoires doivent être accessibles en lecture et exécution.

Étape 18 – Lightdm et les fichiers de /etc

Étant donné que votre client c2LDAP utilisera lightdm en tant que « *display manager* », il faut le paramétrer. Pour cela, recopiez tous les fichiers du répertoire /etc/lightdm dans /srv/fai/config/files :

```
cd /etc/lightdm
for i in * ; do mkdir -p /srv/fai/config/files/etc/lightdm/$i; done
for i in * ; do cp $i /srv/fai/config/files/etc/lightdm/$i/X3I015; done
```

Étape 19 – Vos scripts de postinstallation (1/2)

]

Le répertoire /srv/fai/config/scripts contient des scripts exécutés à la fin de l'installation.

Créez vos propres scripts de postinstallation dans le répertoire /srv/fai/config/scripts/X3I015 (à créer). Par exemple, dans un fichier /srv/fai/config/scripts/X3I015/10-etc, vous pouvez recopier les fichiers que vous avez sauvegardés dans le répertoire /srv/fai/config/files. Pour cela, FAI propose une commande fcopy adaptée. Vous pouvez également rajouter des lignes dans des fichiers déjà existants via la commande FAI ainsl (acronyme de « add if no such line ») :

```

#! /bin/bash

error=0; trap 'error=$(( $?>$error?${?}:$error))' ERR # save maximum error code

fcopy -iM /etc/ldap/ldap.conf
fcopy -iM /etc/nsswitch.conf
fcopy -iM /etc/libnss-ldap.secret
fcopy -iM /etc/pam_ldap.secret
fcopy -iM /etc/hosts
fcopy -iMr /etc/lightdm

ainsl /etc/fstab "msLDAP:/users /users ....."

exit $error

```

Si vous recopiez les lignes ci-dessus, modifiez la dernière de manière à ce que ce soit une ligne syntaxiquement valide pour l'/etc/fstab.



n'oubliez pas de donner les droits en lecture et exécution à tout le monde sur le fichier /srv/fai/config/scripts/X3I015/10-etc

Étape 20 – Vos scripts de postinstallation (2/2)

Par défaut, le service `lightdm` n'est pas exécuté au démarrage. Pour l'exécuter, il faut donc effectuer un `systemctl enable lightdm`. Dans la syntaxe des scripts FAI, cela se traduit par :

```
$ROOTCMD systemctl enable lightdm
```

Créez donc un fichier `/srv/fai/config/scripts/X3I015/20-services`

Dans lequel vous exécuterez cette commande. Utilisez le même en-tête avec la gestion des erreurs que dans la question précédente. N'oubliez pas de donner les droits en exécution à votre fichier.

Pour que vos utilisateurs puissent se connecter à leur compte, il faut créer un répertoire `/users` sur votre client. Créez un fichier `/srv/fai/config/scripts/X3I015/30-users` permettant cela :

```

#! /bin/bash

error=0; trap 'error=$(( $?>$error?${?}:$error))' ERR # save maximum error code

mkdir $target/users

exit $error

```

Notez que, lorsque vous utilisez de commandes non FAI (comme `mkdir`, `chown`, *etc.*), les noms des répertoires et fichiers de votre machine cliente sont préfixés par `$target`. Le répertoire `$target` contient la racine du système de fichiers contenant le système d'exploitation que vous installez (autrement dit le répertoire `/` de la machine que vous installez). Là encore, n'oubliez pas de donner les droits en exécution au fichier `/srv/fai/config/scripts/X3I015/30-users`.

Certaines commandes comme `passwd` modifient des fichiers système prédéfinis comme `/etc/shadow`. Or, comme nous l'avons vu plus haut, les fichiers système de la machine que vous installez se trouvent dans un sous-répertoire de `$target`, par exemple `$target/etc/shadow`. Afin de résoudre ce problème, on utiliserait en principe la commande `chroot` (voir le man de `chroot`). Dans FAI, cette commande est remplacée par `$ROOTCMD` : par exemple, pour supprimer le password de l'utilisateur `toto`, on exécuterait le code suivant :

```
$ROOTCMD passwd -d toto
```

Étape 21 – Configuration du boot loader

Voilà, votre config `space` est configuré. Il reste maintenant à configurer le boot loader que votre machine cliente va utiliser. Pour cela, il suffit d'exécuter la commande :

```
fai-chboot -B -I -u nfs://192.168.X.2/srv/fai/config default
```

en remplaçant le `X` par le numéro adéquat pour obtenir l'adresse IP de SSLDAP. Cela générera en particulier un fichier `/srv/tftp/fai/pxelinux.cfg/default` qui contiendra les instructions « à la grub » pour démarrer votre client.

Voilà, votre serveur de déploiement est maintenant terminé. La suite de ce TME consiste maintenant à créer une nouvelle machine virtuelle et à la démarrer. Elle s'installera alors automatiquement.

Étape 22 – Création d'une nouvelle machine

Créez maintenant une nouvelle machine virtuelle : dans la fenêtre de la VirtualBox, cliquez sur l'icône "Nouvelle" (en haut à gauche de la fenêtre). Vous verrez apparaître une fenêtre similaire à celle de la figure 1. Choisissez le nom de votre machine (`c2LDAP`) et indiquez qu'il s'agit d'une distribution Linux Debian (64-bit).

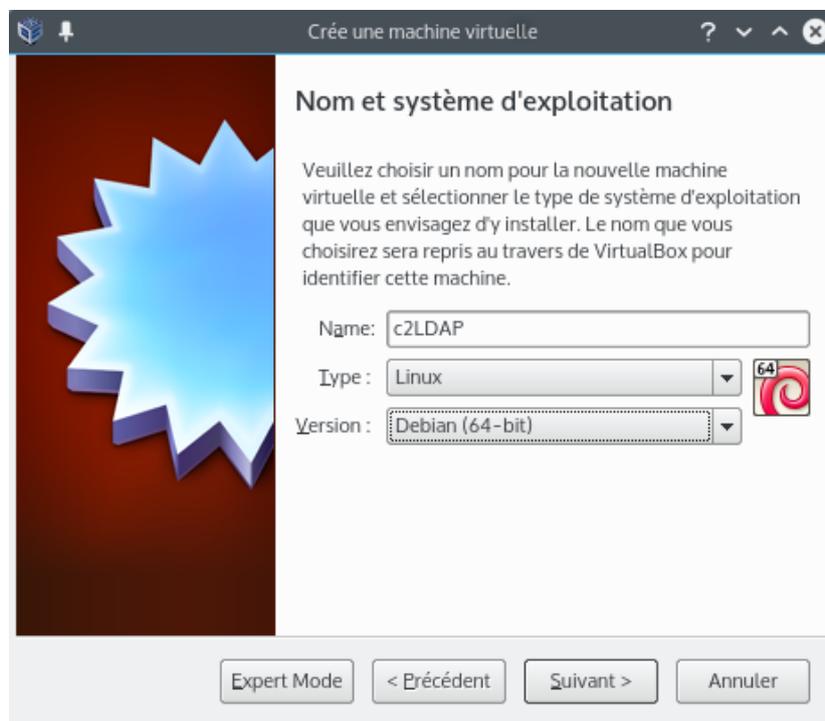


FIGURE 1 – Déclaration du nom et du système de la nouvelle machine

Cliquez sur "Suivant". Cela vous ouvrira une nouvelle fenêtre, comme celle de la figure 2, vous permettant de saisir la taille de la mémoire consommée par votre machine. *A priori*, 2,5Go devraient suffire mais si vous avez la possibilité de mettre 4Go, ce sera sans doute plus confortable.



FIGURE 2 – Déclaration de la taille de la RAM de la machine virtuelle

Après avoir sélectionné votre taille mémoire, cliquez sur “Suivant”, puis sur “Créer un disque dur virtuel maintenant” (cf. la figure 3).

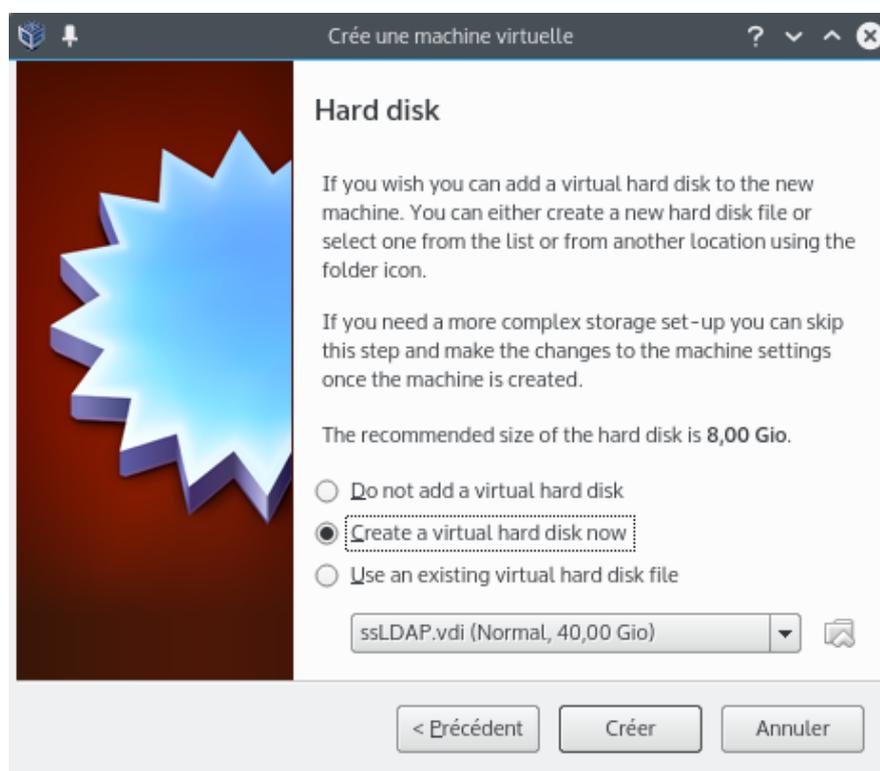


FIGURE 3 – Création du disque dur

Cliquez sur “Créer” puis sur “VDI”, sur “Suivant”, sur “Dynamiquement alloué”, “suivant” et sélec-

tionnez une taille de 25Go (cf. la figure 4).

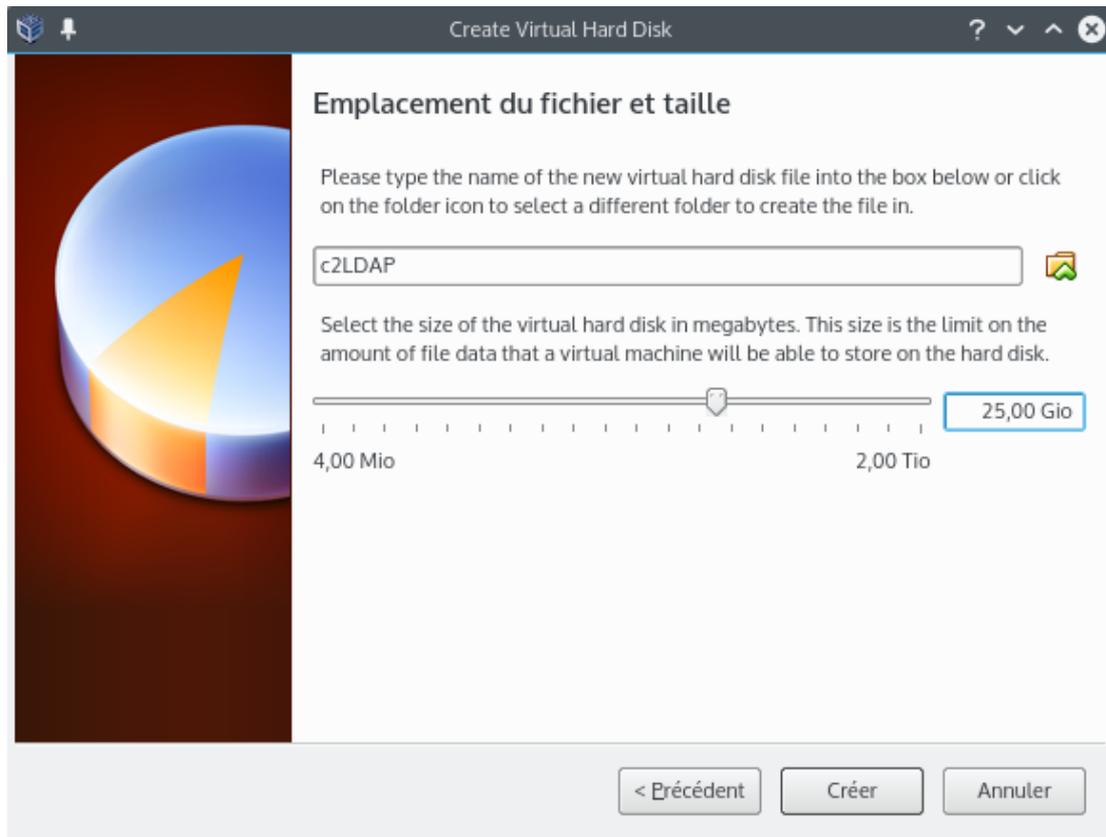


FIGURE 4 – Création du disque dur

Enfin, cliquez sur “Créer”. Voilà, vous avez une nouvelle machine virtuelle complètement vierge.

Étape 23 – Configuration de la nouvelle machine (1/2)

Dans la fenêtre VirtualBox, sélectionnez votre nouvelle machine virtuelle en cliquant dessus une fois avec le bouton gauche de votre souris, puis en cliquant sur le bouton “configuration”.

Dans la rubrique “système/carte mère”, décochez dans l’ordre d’amorçage “Disquette” et “Optical”, et cochez “Réseau” (cf. figure 5).

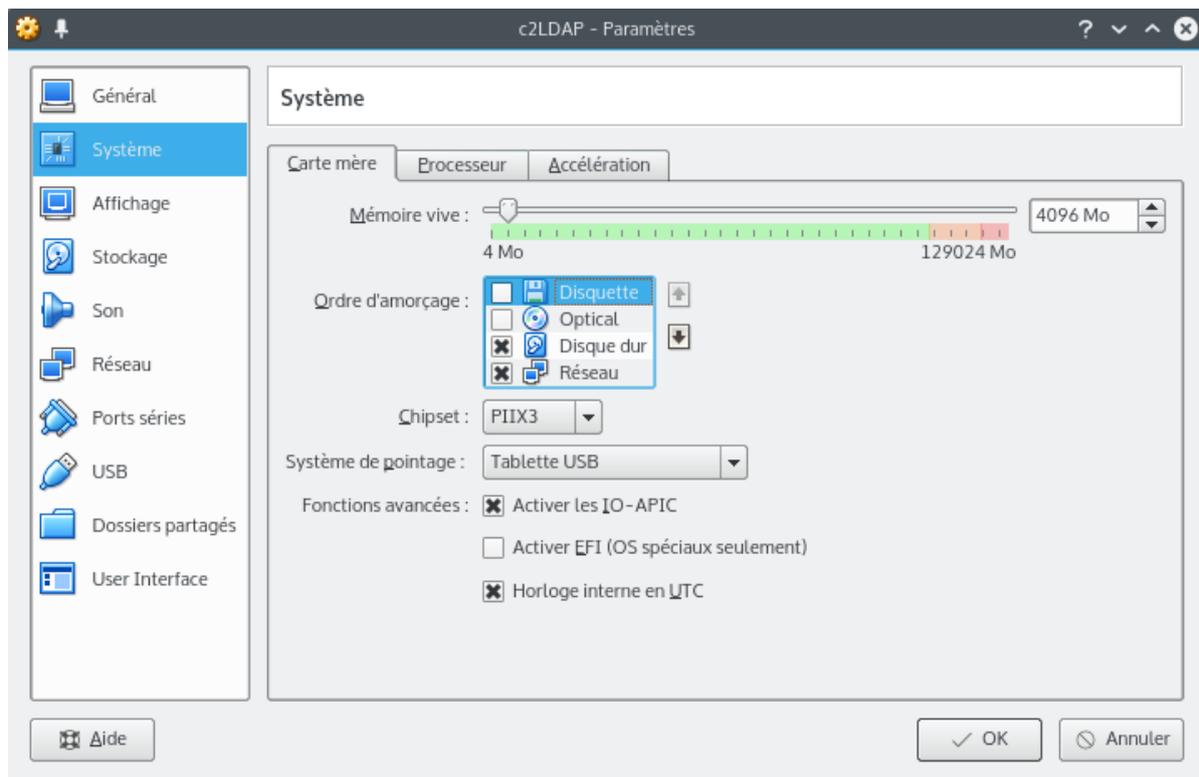


FIGURE 5 – Configuration de la séquence de démarrage

Dans la rubrique “Système / Processeur”, vous pouvez augmenter le nombre de processeurs (cœurs) alloués à votre machine virtuelle lorsqu’elle est démarrée (cf. figure 6).

Étape 24 – Configuration de la nouvelle machine : le réseau (2/2)

Dans la rubrique “Réseau”, activez la carte réseau n°1 et affectez-lui comme mode d’accès “Réseau interne” (cf. figure 7). Cela permettra de placer votre nouvelle machine sur le même réseau que ssLDAP.

 N’oubliez pas de régénérer l’adresse MAC de votre carte réseau en cliquant sur le bouton “Avancé” puis sur l’icône bleue à droite de “Adresse MAC”.

Étape 25 – Fin de configuration

La configuration de votre nouvelle machine c2LDAP est maintenant terminée. Fermez la fenêtre de configuration en cliquant sur le bouton OK en bas à droite de celle-ci.

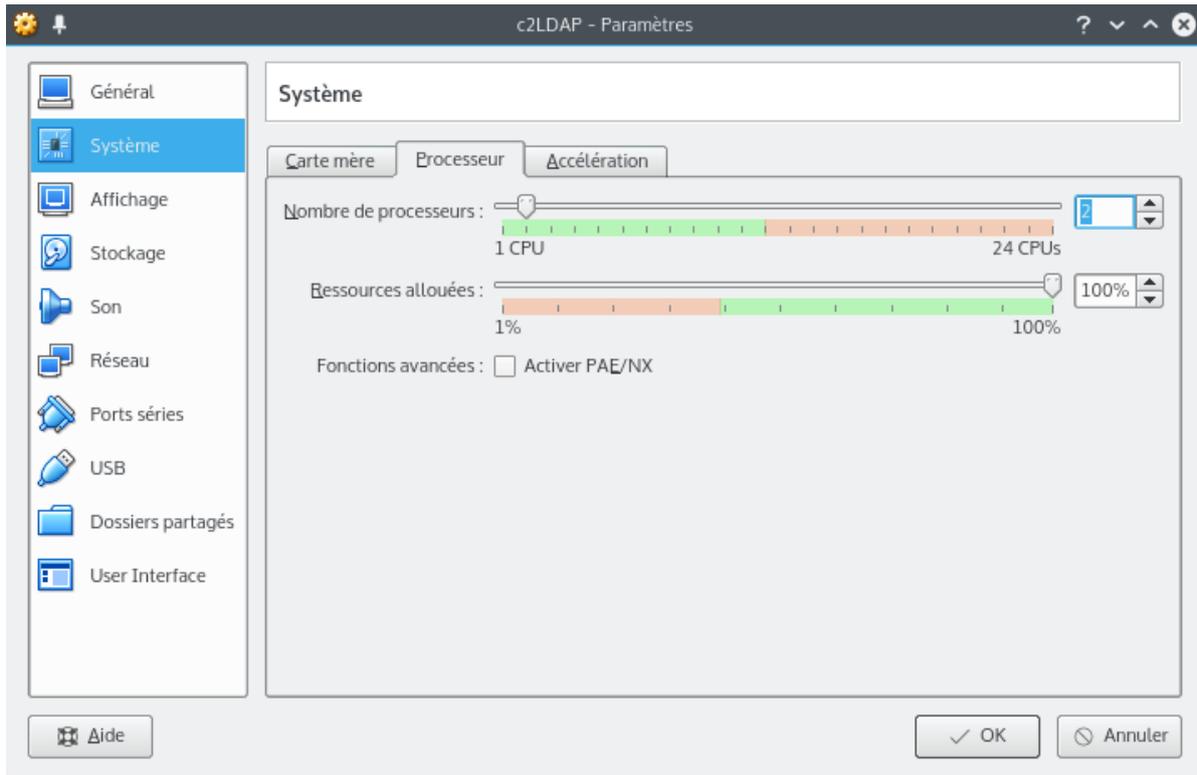


FIGURE 6 – Configuration des processeurs

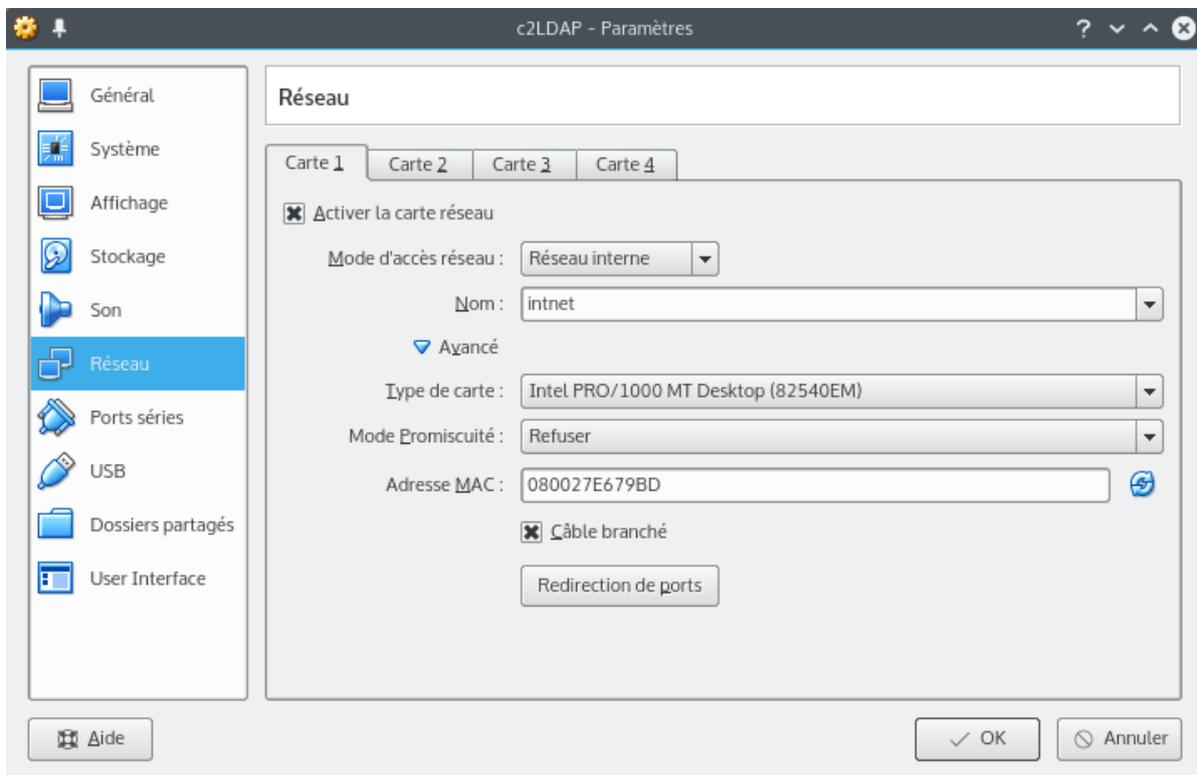


FIGURE 7 – Configuration du réseau – carte 1

Étape 26 – Déploiement

Démarrez votre nouvelle machine virtuelle. Celle-ci va vous demander d'insérer le DVD d'un système d'exploitation. Cliquez sur "annulez". Votre machine va alors booter sur le réseau et s'installer automatiquement.

Étape 27 – Test de bonne installation

Vous pouvez maintenant démarrer la machine que vous venez de déployer. Elle bootera en mode graphique. Vous pourrez vous logger en `root`, dont le mot de passe est `fai`. Dans une console, allez dans le répertoire `/var/log/fai/localhost/last`. Vous y trouverez tous les logs d'installation. Inspectez-les pour vérifier qu'il n'y a pas eu d'erreur lors de l'installation. Notamment, dans le fichier `fcopy.log` sont indiqués les fichiers copiés par la commande `fcopy`. Vérifiez que ceux que vous aviez spécifiés dans vos scripts ont bien été copiés. Dans `shell.log`, vous trouverez les logs des scripts eux-mêmes. Là encore, vérifiez qu'il n'y a pas eu d'erreur (la cas échéant, elles se situent dans les étapes 17 à 20). Vous pouvez également vérifier que les packages dont vous avez demandé l'installation dans l'étape 13 ont bien été installés en faisant des `grep` dans le fichier `software.log`. Si ce n'est pas le cas, vous avez dû faire une erreur de syntaxe dans votre fichier `X3I015` de l'étape 13.

Étape 28 – Test de bonne installation (bis)

Testez si vous pouvez vous logger en mode graphique en tant que `student3` (ou tout autre utilisateur que vous aviez créé via la commande `ldapadduser`). Si vous ne parvenez pas à vous connecter en tant que `student3`, connectez-vous en tant que `root` et « déboguez », par exemple :

- vous pouvez vérifier que les répertoires distants ont bien été montés sur votre nouvelle machine.
- vous pouvez vérifier que `su - student3` fonctionne correctement.