

Projet 2A STI : Supervision et audit de la sécurité système dans un réseau

Diplôme d'Ingénieur, 4e année

Aymeric Berquin
&
Fayçal-Anoar Cherkaoui

Date de rendu de rapport : 12/02/2015

Remerciement

Nous remercions Monsieur Briffaut pour le temps et les ressources qu'il nous a consacré. Nous le remercions aussi pour toutes les connaissances qu'il nous a apportés.

Introduction

Dans le cadre de notre formation d'ingénieurs en Sécurité et Technologies Informatiques, un projet d'application sécurité nous est soumis. Dans notre cas il s'agit de concevoir une application client/-serveur permettant la supervision et l'audit de la sécurité dans un réseau. Il s'agit de nous mettre en situation de travail en binôme sur un projet donné et sur un moyen terme.

Table des matières

1	Installation des machines virtuelles	1
1.1	Installation du serveur Debian	1
1.2	Installation du client ubuntu	22
2	Git	29
2.1	Gérer les dépôts	29
2.2	Etat du dépôt	29
2.3	Gestion des fichiers	29
2.4	Gestion des commits	29
3	BDD	30
4	Client/Serveur	31
5	Interface WEB	32
6	Script	33
6.1	En Tant qu'utilisateur	33
6.2	En Tant qu'administrateur	33
7	Conclusion	34
8	Évolution temporelle	35
9	Bibliographie	36

Table des figures

1	choix de l'installation	1
2	choix de la langue	2
3	choix de la localisation géographique	3
4	Nom de l'hôte : hostname	4
5	Nom du domaine de la machine	5
6	Définition du mot de passe du compte root	6
7	Confirmation du mot de passe	7
8	Création d'un compte utilisateur	8
9	Choix du login du compte utilisateur précédemment créé	9
10	Définition du mot de passe pour le compte utilisateur	10
11	confirmation du mot de passe pour le compte utilisateur	11
12	Partitionnement du disque	12
13	Partitionnement du disque	13
14	Partitionnement du disque	14
15	Partitionnement du disque	15
16	Partitionnement du disque	16
17	Configuration de l'outil de gestion du paquet	17
18	Configuration de l'outil de gestion du paquet	18
19	configuration de l'outil de gestion du paquet	19
20	Sélection des logiciels	20

21	Installation du programme de démarrage GRUB	21
22	Fin de l'installation	22
23	interface de la machine virtuelle VMware	22
24	Choix de la langue d'installation	23
25	Prérequis pour l'installation	24
26	Type d'installation	24
27	Choix du fuseau horaire.	25
28	Disposition du clavier.	26
29	Création du client1.	27
30	Redémarrage de la machine.	28

1 Installation des machines virtuelles

1.1 Installation du serveur Debian

Installation d'un debian classique sans interface graphique, qui jouera le rôle du maitre.

On récupère l'iso depuis le site officiel : <http://www.ubuntu.com/download/desktop>.

On configure les caractéristiques suivantes :

- 1GB en RAM
- 1 processeur
- 20GB en disque dur

On choisi une installation sans interface graphique.

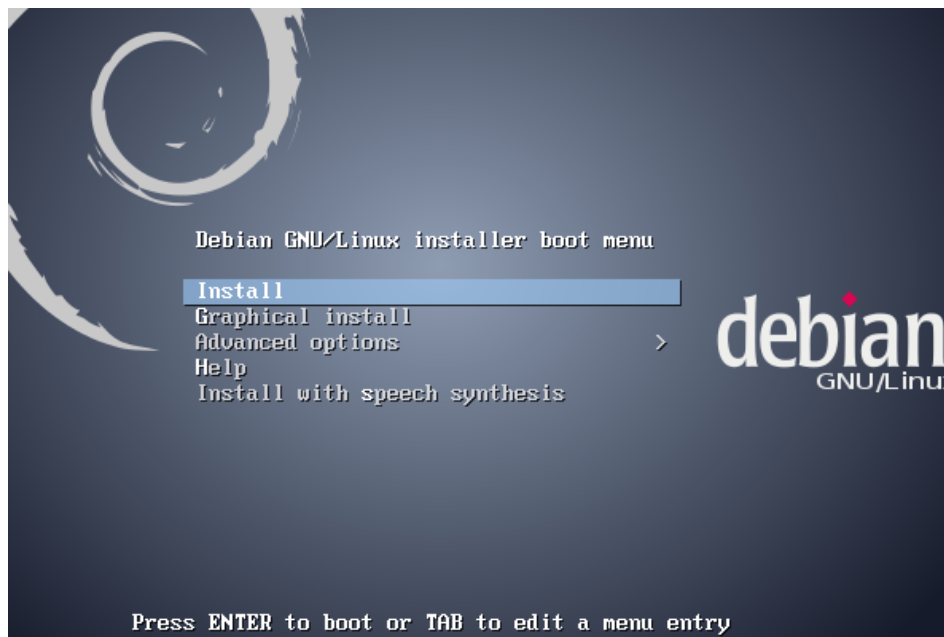


FIGURE 1 – choix de l'installation

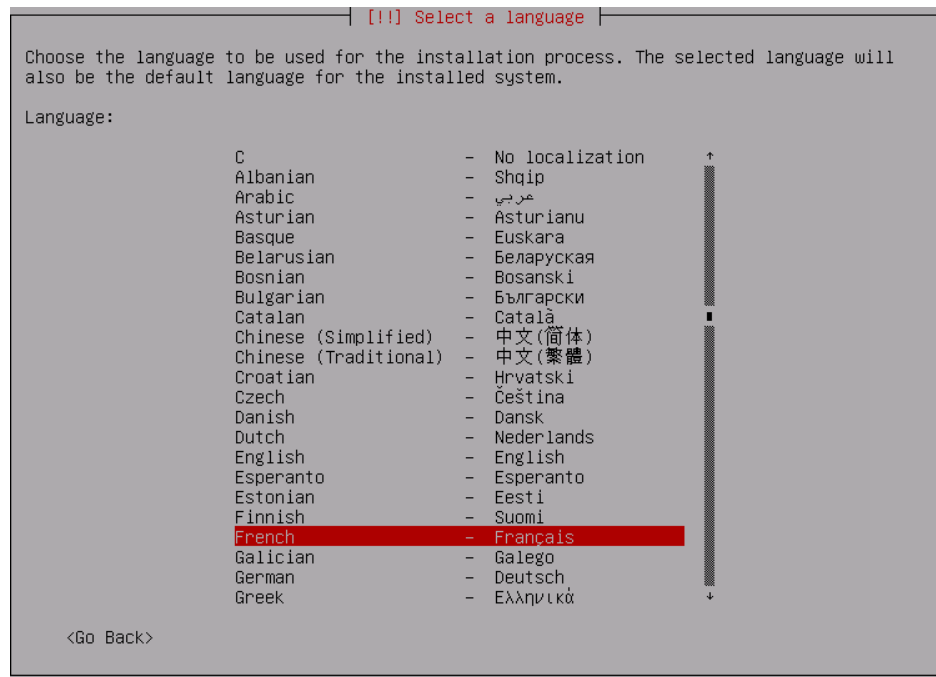


FIGURE 2 – choix de la langue

!!! Choix de votre situation géographique

Le pays choisi permet de définir le fuseau horaire et de déterminer les paramètres régionaux du système (« locale »). C'est le plus souvent le pays où vous vivez.

La courte liste affichée dépend de la langue précédemment choisie. Choisissez « Autre » si votre pays n'est pas affiché.

Pays (territoire ou région) :

Belgique
Canada
France
Luxembourg
Suisse
Autre

<Revenir en arrière>

FIGURE 3 – choix de la localisation géographique

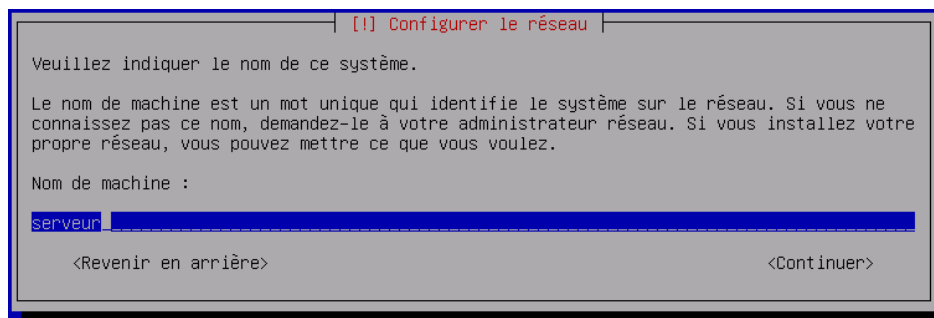


FIGURE 4 – Nom de l'hôte : hostname

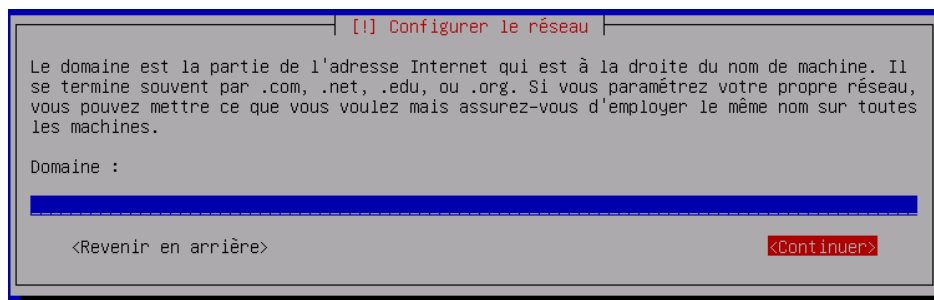


FIGURE 5 – Nom du domaine de la machine

[[!]] Créer les utilisateurs et choisir les mots de passe

Vous devez choisir un mot de passe pour le superutilisateur, le compte d'administration du système. Un utilisateur malintentionné ou peu expérimenté qui aurait accès à ce compte peut provoquer des désastres. En conséquence, ce mot de passe ne doit pas être facile à deviner, ni correspondre à un mot d'un dictionnaire ou vous être facilement associé.

Un bon mot de passe est composé de lettres, chiffres et signes de ponctuation. Il devra en outre être changé régulièrement.

Le superutilisateur (« root ») ne doit pas avoir de mot de passe vide. Si vous laissez ce champ vide, le compte du superutilisateur sera désactivé et le premier compte qui sera créé aura la possibilité d'obtenir les privilèges du superutilisateur avec la commande « sudo ».

Par sécurité, rien n'est affiché pendant la saisie.

Mot de passe du superutilisateur (« root ») :

<Revenir en arrière><Continuer>

FIGURE 6 – Définition du mot de passe du compte root

[!!] Créer les utilisateurs et choisir les mots de passe

Veuillez entrer à nouveau le mot de passe du superutilisateur afin de vérifier qu'il a été saisi correctement.

Confirmation du mot de passe :

<Revenir en arrière> <Continuer>

FIGURE 7 – Confirmation du mot de passe

[[!]] Créer les utilisateurs et choisir les mots de passe

Un compte d'utilisateur va être créé afin que vous puissiez disposer d'un compte différent de celui du superutilisateur (« root »), pour l'utilisation courante du système.

Veillez indiquer le nom complet du nouvel utilisateur. Cette information servira par exemple dans l'adresse origine des courriels émis ainsi que dans tout programme qui affiche ou se sert du nom complet. Votre propre nom est un bon choix.

Nom complet du nouvel utilisateur :

server

<Revenir en arrière> <Continuer>

FIGURE 8 – Création d'un compte utilisateur

[!!] Créer les utilisateurs et choisir les mots de passe

Veuillez choisir un identifiant (« login ») pour le nouveau compte. Votre prénom est un choix possible. Les identifiants doivent commencer par une lettre minuscule, suivie d'un nombre quelconque de chiffres et de lettres minuscules.

Identifiant pour le compte utilisateur :

server

<Revenir en arrière> <Continuer>

FIGURE 9 – Choix du login du compte utilisateur précédemment créé

[[!]] Créer les utilisateurs et choisir les mots de passe

Un bon mot de passe est composé de lettres, chiffres et signes de ponctuation. Il devra en outre être changé régulièrement.

Mot de passe pour le nouvel utilisateur :

<Revenir en arrière>

<Continuer>

FIGURE 10 – Définition du mot de passe pour le compte utilisateur

[[!]] Créer les utilisateurs et choisir les mots de passe

Veuillez entrer à nouveau le mot de passe pour l'utilisateur, afin de vérifier que votre saisie est correcte.

Confirmation du mot de passe :

<Revenir en arrière>

<Continuer>

FIGURE 11 – confirmation du mot de passe pour le compte utilisateur

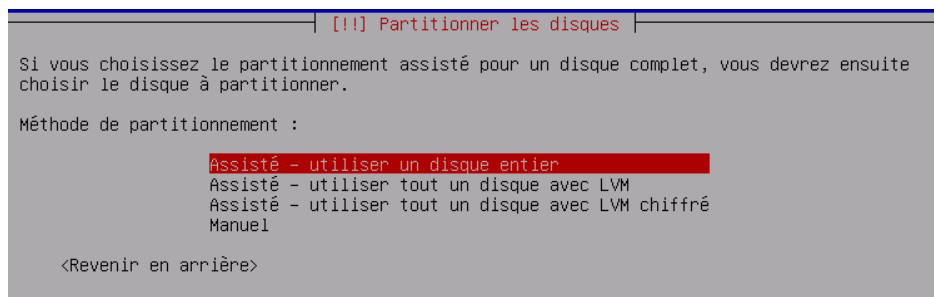


FIGURE 12 – Partitionnement du disque

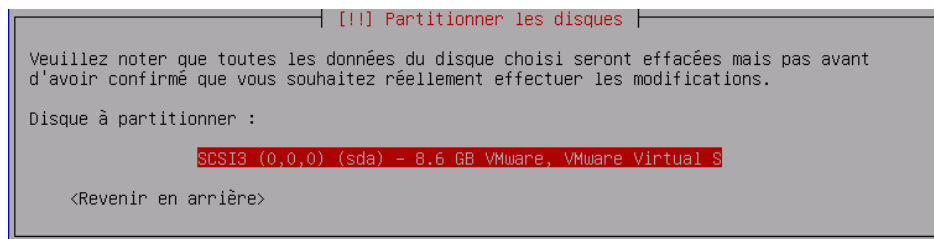


FIGURE 13 – Partitionnement du disque

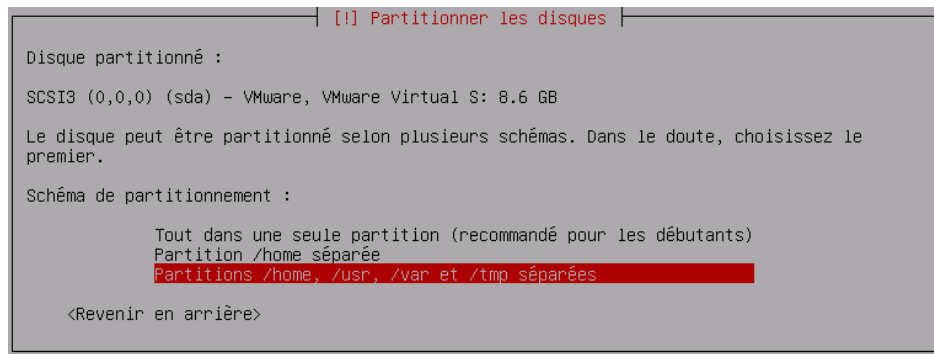


FIGURE 14 – Partitionnement du disque

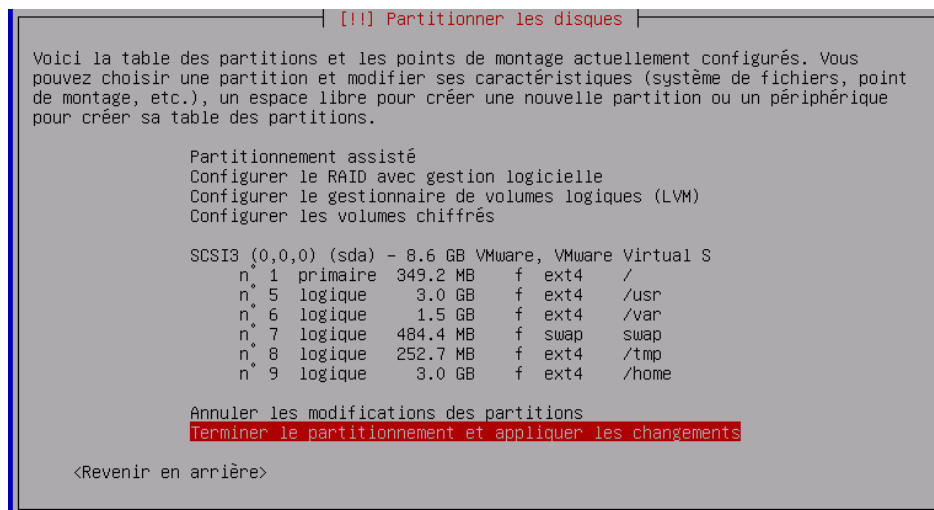


FIGURE 15 – Partitionnement du disque

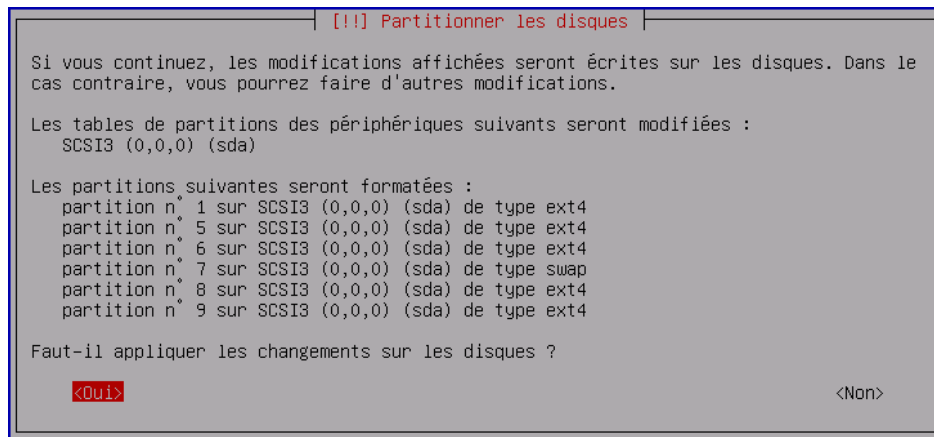


FIGURE 16 – Partitionnement du disque

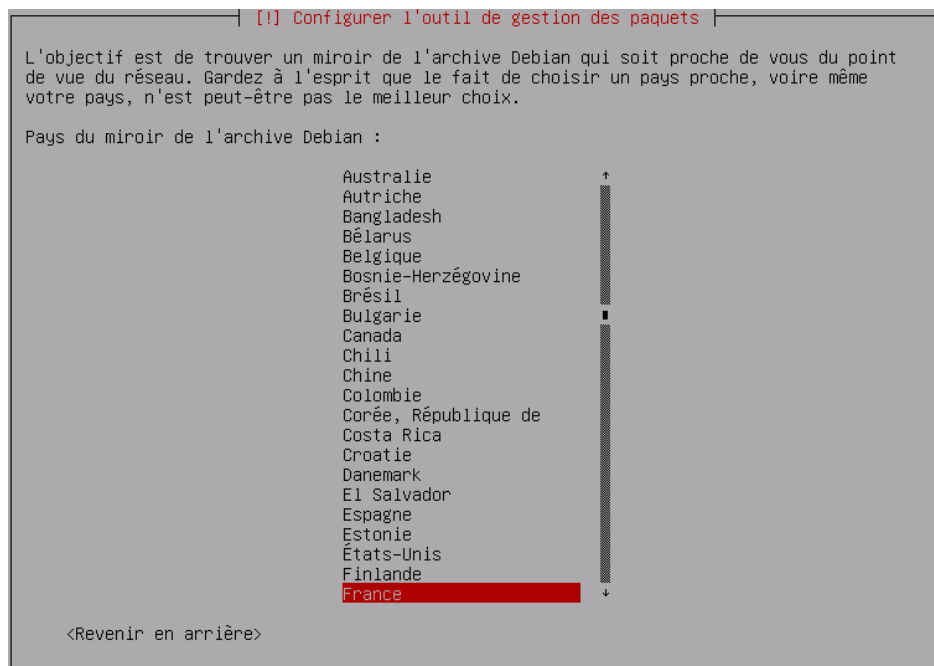


FIGURE 17 – Configuration de l'outil de gestion du paquet

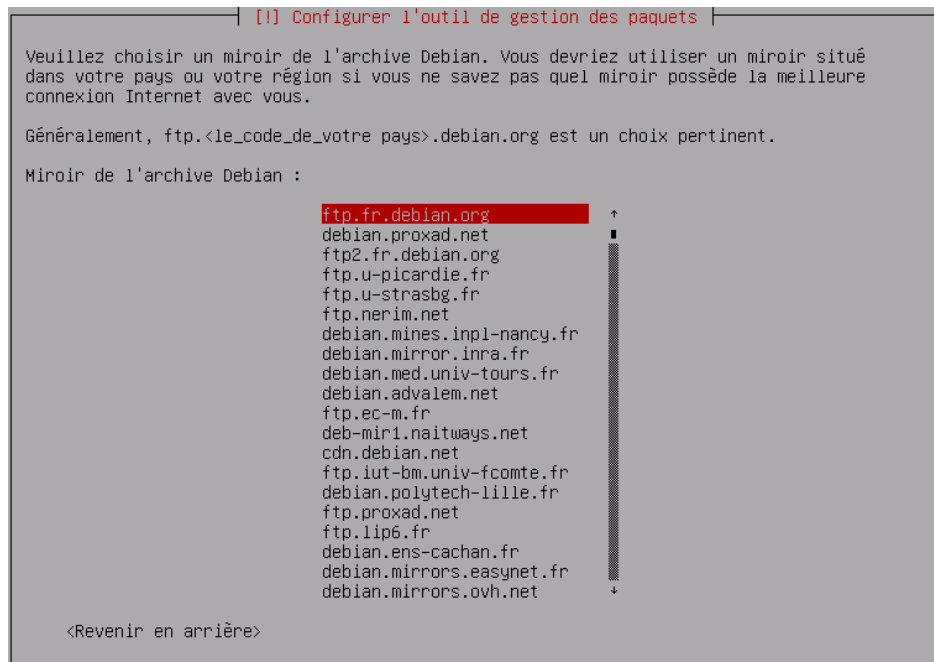


FIGURE 18 – Configuration de l’outil de gestion du paquet

[!] Configurer l'outil de gestion des paquets

Si vous avez besoin d'utiliser un mandataire HTTP (souvent appelé « proxy ») pour accéder au monde extérieur, indiquez ses paramètres ici. Sinon, laissez ce champ vide.

Les paramètres du mandataire doivent être indiqués avec la forme normalisée
« http://[[utilisateur] [:mot-de-passe]@]hôte[:port]/ ».

Mandataire HTTP (laisser vide si aucun) :

<Revenir en arrière>

<Continuer>

FIGURE 19 – configuration de l'outil de gestion du paquet

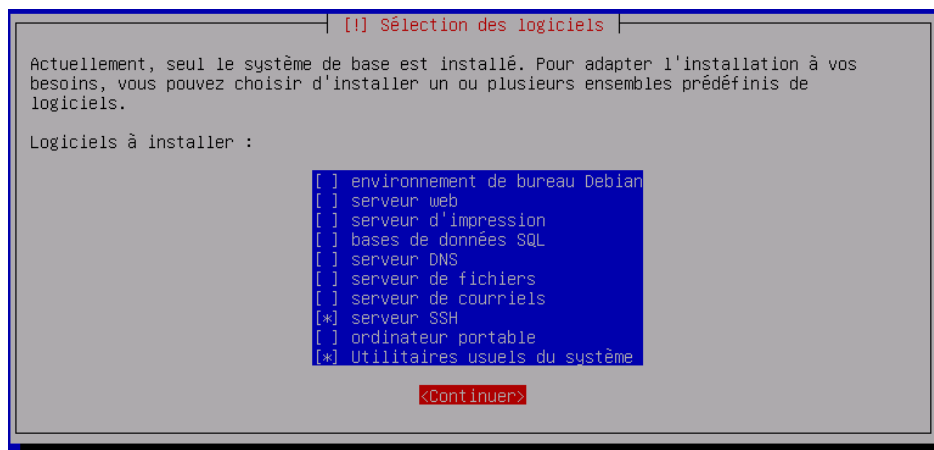


FIGURE 20 – Sélection des logiciels

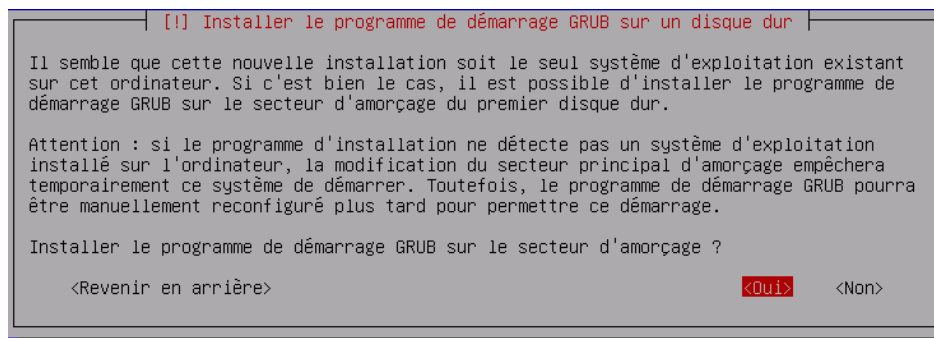


FIGURE 21 – Installation du programme de démarrage GRUB

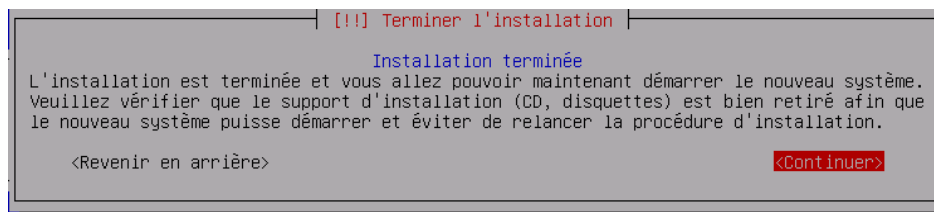


FIGURE 22 – Fin de l’installation

1.2 Installation du client ubuntu

On aura besoin d’installer deux machines virtuelles avec la dernière distribution Ubuntu stable. Elles auront pour nom client1 et client2.

Nous avons choisi d’utiliser un Xubuntu 14.04. A récupérer sur le site officiel : <http://www.ubuntu.com/download/>

Nom complet : user

Nom d’utilisateur : user

Mot de passe : resu

Hostname : client1

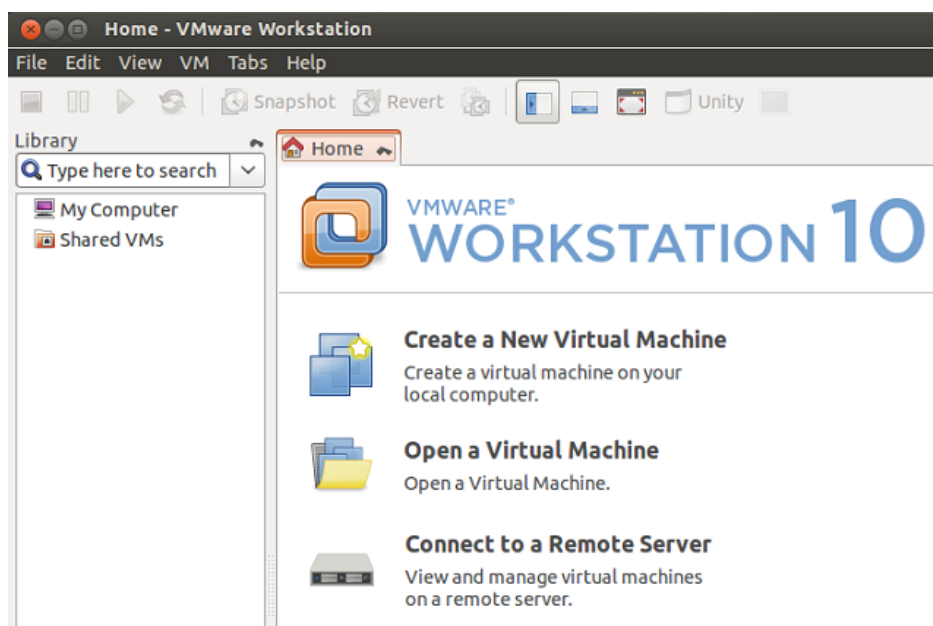


FIGURE 23 – interface de la machine virtuelle VMware

Elle aura pour configuration :

- 1GB en RAM
- 1 processeur
- 20GB en disque dur

On éditera la nouvelle machine virtuelle VMware dans laquelle en spécifiant le chemin de l’iso télé-chargé.

On démarre la machine virtuelle.

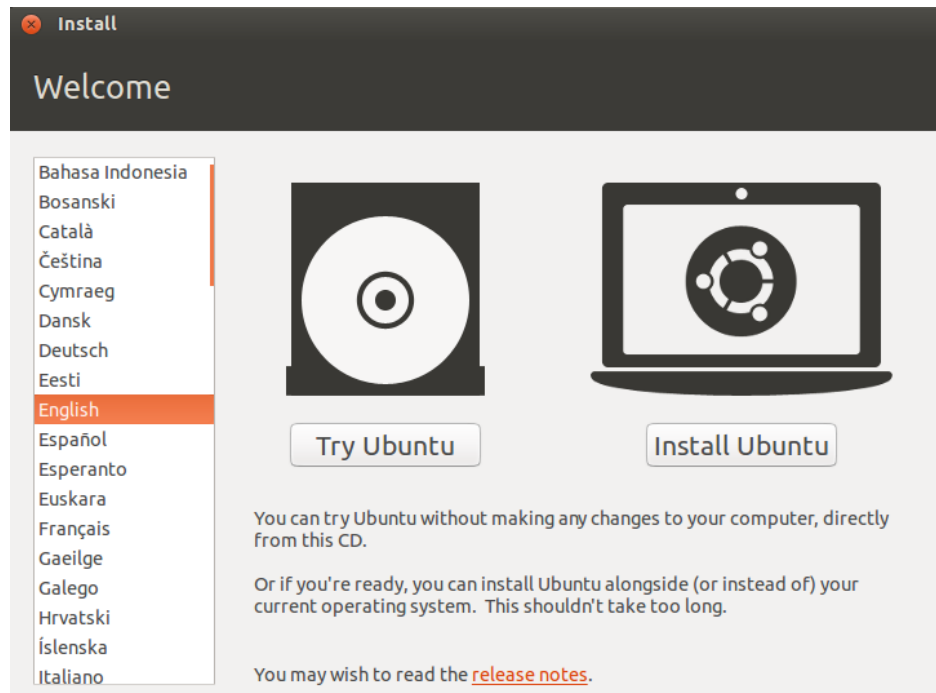


FIGURE 24 – Choix de la langue d’installation

Une nouvelle fenêtre s’affiche, on clique sur suivant.

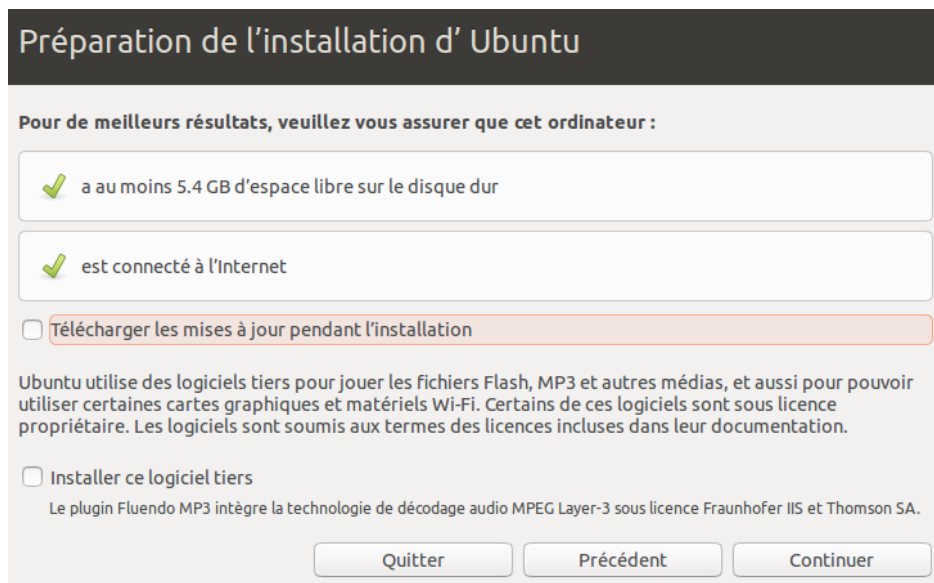


FIGURE 25 – Prérequis pour l'installation

On procédera à une installation par défaut.

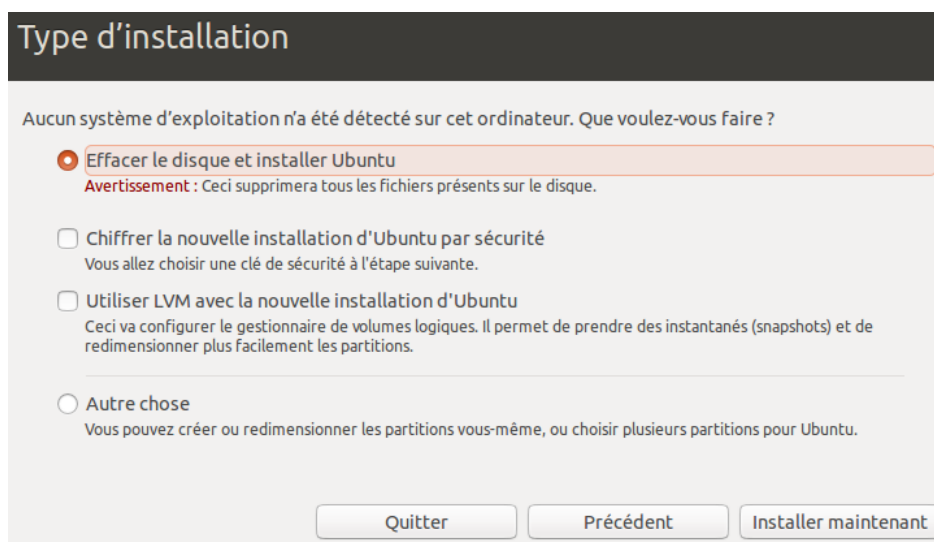


FIGURE 26 – Type d'installation

Une nouvelle fenêtre pour le choix du fuseau horaire. On choisie Paris.

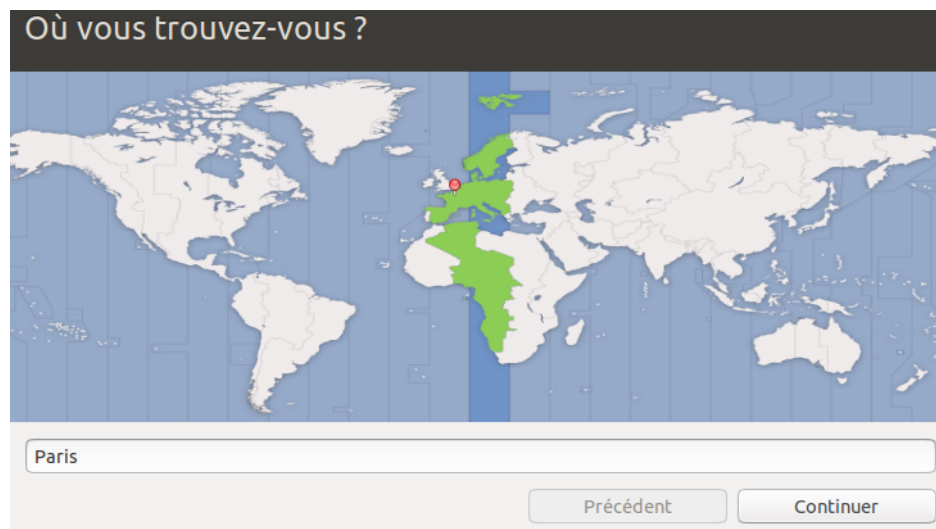


FIGURE 27 – Choix du fuseau horaire.

La nouvelle fenêtre qui s’affiche est pour le choix de la disposition du clavier.

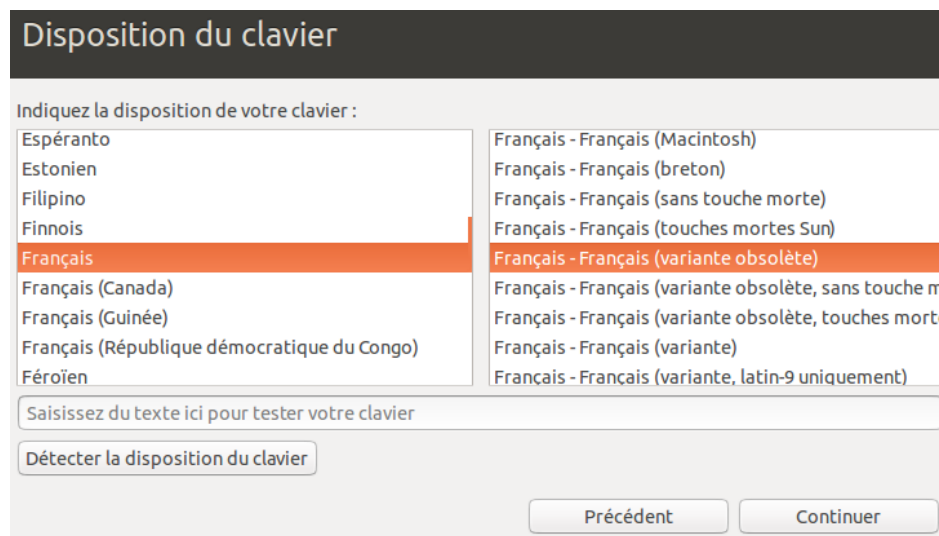


FIGURE 28 – Disposition du clavier.

On procède dans cette étape à la création du client1.

The screenshot shows a user creation window titled "Qui êtes vous ?". It contains several input fields and checkboxes. The "Votre nom" field is filled with "client1" and has a green checkmark. The "Le nom de votre ordinateur" field is also filled with "client1" and has a green checkmark, with a note below it stating "Le nom qu'il utilise pour communiquer avec d'autres ordinateurs." The "Choisissez un nom d'utilisateur" field is filled with "client1" and has a green checkmark. The "Choisissez un mot de passe" field is filled with six dots and has a red error message "Mot de passe trop faible". The "Confirmez votre mot de passe" field is filled with six dots and has a green checkmark. Below these fields are three radio buttons: "Ouvrir la session automatiquement", "Demander mon mot de passe pour ouvrir une session" (which is selected), and "Chiffrer mon dossier personnel". At the bottom right are two buttons: "Précédent" and "Continuer".

Qui êtes vous ?

Votre nom : client1 ✓

Le nom de votre ordinateur : client1 ✓
Le nom qu'il utilise pour communiquer avec d'autres ordinateurs.

Choisissez un nom d'utilisateur : client1 ✓

Choisissez un mot de passe : ●●●●●● Mot de passe trop faible

Confirmez votre mot de passe : ●●●●●● ✓

☐ Ouvrir la session automatiquement

☒ Demander mon mot de passe pour ouvrir une session

☐ Chiffrer mon dossier personnel

Précédent Continuer

FIGURE 29 – Création du client1.

On redémarre la machine.

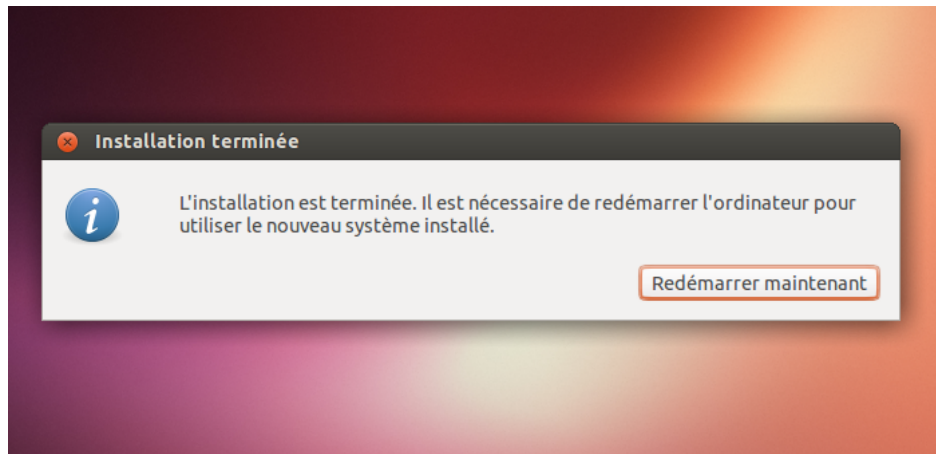


FIGURE 30 – Redémarrage de la machine.

On est arrivé à la fin de l'installation de la machine client1, pour le deuxième client il nous suffit de faire un clone du premier client. UN clic droit sur la machine client1 puis manage puis clone.

On démarre la machine clonée puis dans /etc/hostname on modifie le nom en la nommant client2.

```
vim /etc/hostname
```

2 Git

Nous avons décidé d'utiliser un serveur git pour gérer les sources.

Git est un logiciel de gestion de versions décentralisé. C'est-à-dire que le développement ne se fait pas sur un serveur centralisé, mais chaque personne peut développer sur son propre dépôt. Git facilite ensuite la fusion (merge) des différents dépôts.

Pour pouvoir utiliser Git, il suffit d'installer le paquet git :

```
apt-get install git
```

2.1 Gérer les dépôts

Pour pouvoir utiliser le Git il va falloir tout d'abord créer un dépôt.

```
mkdir proscan cd proscan git init
```

2.2 Etat du dépôt

```
git diff git diff <commit1> <commit2>
```

Le git offre la possibilité de trouver les changements effectués. SI vous avez des changements pas encore commités, la commande git diff affichera les modifications effectuées depuis le dernier commit.

```
git status
```

 Permet de savoir tout ce qui n'a pas encore été validé.

```
git log
```

 Liste les commits effectués dans le dépôt. Et ainsi voir les modifications faites dans quelle date et par qui.

2.3 Gestion des fichiers

Pour ajouter au git un dossier ou un fichier on utilise la commande :

```
git add <nom-du fichier-ou-du-dossier>
```

Pour ajouter tout le contenu d'un fichier ou d'un dossier :

```
git add *
```

Pour supprimer le fichier de l'ordinateur, ainsi que du dépôt git :

```
git rm <nom-fichier>
```

Pour dépolacer le fichier de l'ordinateur, ainsi que du dépôt Git :

```
git mv <nom-fichier> <nouvel-emplacement>
```

2.4 Gestion des commits

Met à jour votre dépôt local (à faire avant de commencer à modifier des fichiers pour être sûr de travailler sur leurs dernières versions et avant tout commit pour éviter les éventuels conflits avec des modifications effectuées par d'autres utilisateurs entre temps).

```
git pull
```

Créer un commit contenant fichier1 et fichier2. Ces fichiers auront dû être au préalable ajoutés au dépôt avec la commande git add. Il s'agit de la validation d'une transaction.

Pour envoyer un commit dans la branche principale du dépôt (master) :

```
git push origin master
```

3 Base De Données

3.1 Client

Table Client La table client est constituée de :

- id : identifiant auto-indexé, clé primaire
- ip : adresse ip du client
- hmac : hmac du client (unique)
- hostname : Nom d'hôte du client
- pid : pid du processus chargé de communiquer avec ce client

3.2 Script

Table Script La table script est constituée de :

- id : identifiant auto-indexé, clé primaire
- nom : Nom du script
- description : Description rapide du script
- code : code du script

3.3 Result

Table Result La table result qui enregistre les résultats des scripts est constituée de :

- id : identifiant auto-indexé, clé primaire
- idclient : Identifiant du client
- idscrip : Identifiant du script
- result : résultat du script

4 Client/Serveur

5 Interface WEB

6 Script

Permissions Bien que la majorité de nos scripts puissent s'exécuter avec les permissions d'un utilisateur, certain d'entre eux nécessitent les droits d'administrateur.

6.1 En Tant qu'utilisateur

N°	Résultats
1	Hostname, Interfaces réseaux, nom de la distribution, version de la distribution, version du noyau, table de routage.
2	Espace des partitions montées.
3	Affiche les connexions internet actives.
4	Processus actif.
5	Variables d'environnement.
6	Informations CPU, Interruptions, Mémoire utilisée, Fichiers Swaps, version du noyau, systèmes de fichiers montés, périphériques CPU, périphériques usb.
7	Affiche les processus en cours dans une arborescence qui commence à la racine.
8	Récupération de tous les fichiers d'extension ".log".
9	Table de routage.
10	interfaces réseaux.
11	User loggé, heure du dernier démarrage, affiche les processus morts, runlevel courant.
13	Liste des utilisateurs.
14	Affiche l'état de la mémoire de la partition courante.
17	Vérification de l'intégrité de /bin, /usr/bin, /sbin, /usr/sbin.

6.2 En Tant qu'administrateur

N°	Résultats
15	Affichage de la dernière connexion local.
16	Affiche les règles iptables pour filter, nat et mangle .

7 Conclusion

8 Bibliographie

Le "man" linux