

Mise en place d'une solution de sécurité pour la virtualisation des réseaux

Réalisé par :

Abdelkarim BARRANE

Achraf BAHANE

Sommaire

1.Introduction

- i) Introduction générale
- ii) Les solutions

2.Sécurité dans la virtualisation

- i) Les risques
- j) Les solutions de sécurité (outils techniques)

3.Installation

- i) L'outil Xen
- ii) Téléchargement et Installation des outils

4.Conclusion

1. Introduction

1.1 Introduction générale :

Ensemble des technologies matérielles et logiciels qui permettent de faire fonctionner plusieurs systèmes d'exploitation et plusieurs applications sur une même machine, séparément les uns des autres, comme s'ils fonctionnaient sur des machines physiques distinctes. Les entreprises peuvent exécuter simultanément plusieurs systèmes d'exploitation et applications sur le même ordinateur/serveur en toute sécurité afin d'accroître l'utilisation et la flexibilité du matériel.

On parle de :

Machine hôte : machine exécutant les différents systèmes virtuels.

Machine invitée : machine virtuelle s'exécutant dans l'environnement de virtualisation.

Il existe plusieurs types de virtualisation afin de permettre l'optimisation du système informatique.

La virtualisation hardware :

C'est l'un des types de virtualisation les plus courants, car il est lié à la **disponibilité des applications** et à l'utilisation du matériel. . Tous les serveurs physiques sont regroupés en un seul grand serveur physique. Ainsi, le processeur fonctionne de manière plus efficace et plus efficiente. Chaque petit serveur peut héberger une machine virtuelle, il s'agit d'un conteneur de logiciels totalement isolé et doté d'un système d'exploitation et d'applications propres. Mais l'ensemble du cluster de serveurs est traité comme un seul dispositif par n'importe quel processus demandant le matériel.

L'accès à la machine virtuelle (ou VM) et à la machine hôte (ou au serveur) est facilité par un logiciel appelé **Hyperviseur**. Cette couche d'abstraction agit comme un lien entre le matériel et l'environnement virtuel et distribue les ressources matérielles telles que l'utilisation du CPU, l'allocation de mémoire entre les différents environnements virtuels.

La virtualisation de serveur :

La virtualisation de serveur permet de regrouper plusieurs serveurs physiques sous-employés sur un seul hôte qui exécute des systèmes virtuels. Il permet aussi de réduire la consommation électrique et le nombre d'administrateurs. Il participe beaucoup à la réalisation des économies (locaux, consommation électrique).

La virtualisation d'application :

Elle permet de séparer complètement l'application du système d'exploitation hôte et des autres applications présentes afin d'éviter les conflits. En outre elle peut être définie comme la technologie qui permet de séparer l'environnement du bureau et des applications associées de la machine physique.

La virtualisation des postes de travail :

La virtualisation des postes de travail permet aux administrateurs systèmes et réseaux de gérer beaucoup plus facilement les postes de travail de l'entreprise et de répondre avec flexibilité aux demandes des utilisateurs. Un poste de travail virtualisé ou bureau virtuel peut être hébergé soit directement sur l'ordinateur du client soit sur un serveur dans le centre de données.

La virtualisation de stockage :

La virtualisation des stockages permet d'exploiter au maximum les ressources, d'exploiter au mieux le stockage des disques durs. Dans un premier temps pour centraliser et sécuriser les données, il faudrait que le centre de données s'équipe d'un **SAN** (Storage Area Network). Un des plus grands défis de la virtualisation reste le stockage. Dans les faits, c'est le plus souvent le stockage qui fait exploser les coûts, et crée des engorgements et des pertes de performances. L'infrastructure, en l'occurrence le stockage, s'il est mal dimensionné, ralentit les applications. Le **NAS** (Network Attached Storage) est effectivement un élément de stockage attaché directement au réseau local d'une entreprise. Il se configure par le biais d'une application web comme le navigateur par exemple.

La virtualisation de réseau :

Substitue une infrastructure physique du réseau par plusieurs **réseaux virtuels isolés (VLAN)** qui peuvent coexister sur un même commutateur réseau.

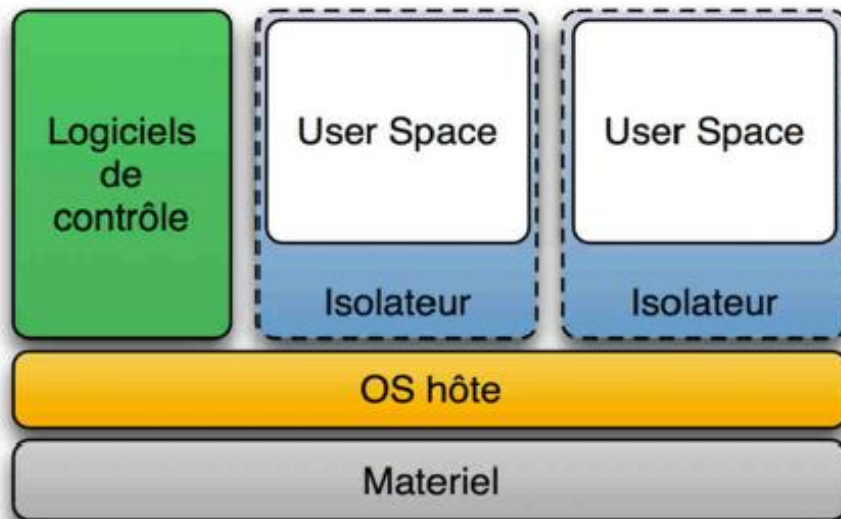
1.2 Les solutions :

La virtualisation Consiste à simuler, au sein d'un serveur physique, l'existence de plusieurs systèmes d'exploitation cloisonnés et mutualisés. On distingue trois grandes catégories de solutions de virtualisation, dont les domaines d'applications sont différents :

- _ L'isolation ou container
- _ La para-virtualisation ou hyperviseur
- _ La virtualisation complète

La virtualisation par container ou isolation :

Un isolateur est un logiciel permettant d'isoler l'exécution des applications dans ce que l'on appelle des contextes ou bien zones d'exécution. L'isolateur permet ainsi de faire tourner plusieurs fois la même application dans un mode multi-instance (plusieurs instances d'exécution) même si elle n'était pas conçue pour ça.



Uniquement liés aux systèmes Linux, les isolateurs sont en fait composés de plusieurs éléments et peuvent prendre plusieurs formes.

Linux V Server : isolation des processus en espace utilisateur

Chroot : Isolation changement de racine

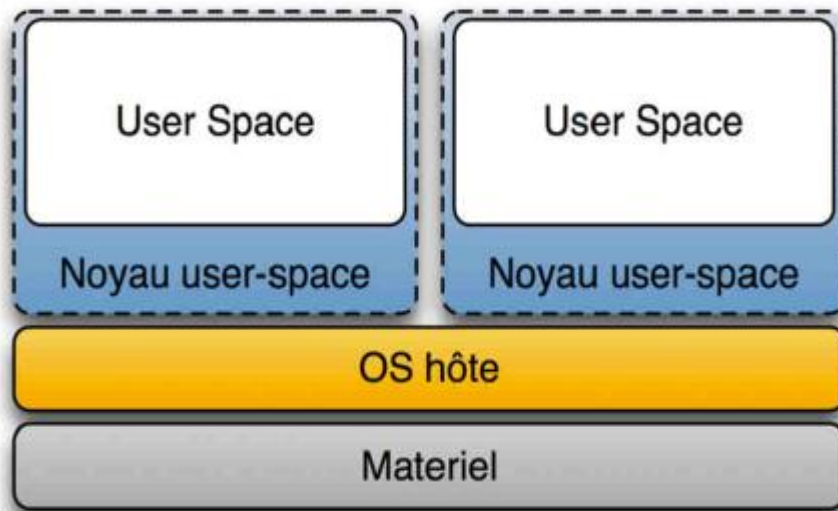
BSD Jail : isolation en espace utilisateur

Open VZ : libre partitionnement au niveau du noyau sous Linux

La virtualisation par noyau en espace utilisateur :

Un noyau en espace utilisateur (user-space) tourne comme une application en espace utilisateur de l'OS hôte. Le noyau user-space a donc son propre espace utilisateur dans lequel il contrôle ses applications. Cette solution est très peu performante, car deux noyaux sont empilés et l'isolation des environnements n'est pas gérée et

l'indépendance par rapport au système hôte est inexistante. Elle sert surtout au développement du noyau.



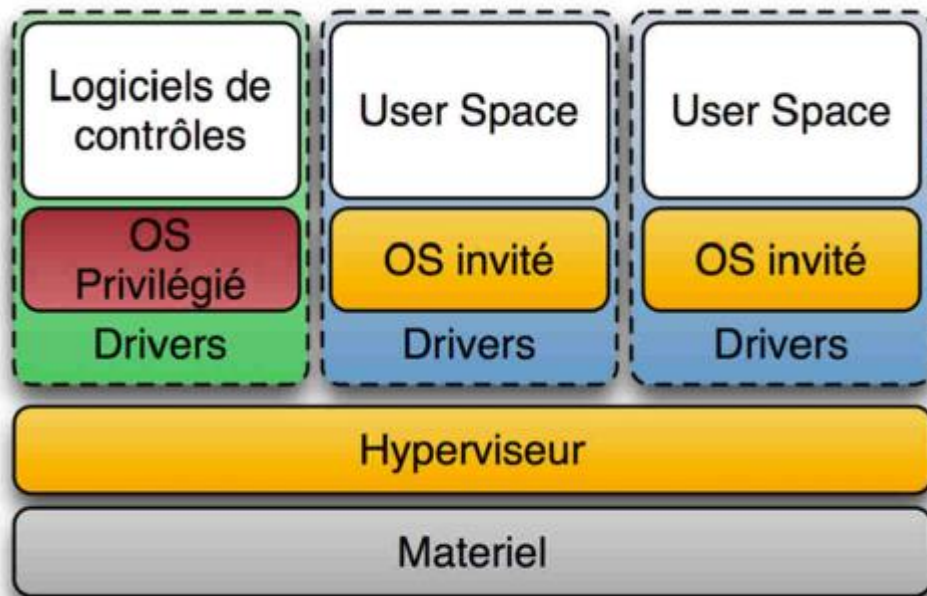
Elle sert surtout au développement du noyau.

User Mode Linux : noyau tournant en espace utilisateur

Cooperative Linux ou coLinux : noyau coopératif avec un hôte Windows.

La paravirtualisation, Hyperviseur type 1 :

Un hyperviseur de « type 1 » est un hyperviseur s'exécutant directement sur une plateforme matérielle. Il implémente la plupart des services que fournissent les noyaux de systèmes d'exploitation courants, entre autres : la gestion mémoire complète des machines virtuelles ainsi que leur ordonnancement. Il peut être assimilé à un noyau allégé et optimisé, il n'est donc pas dépendant d'un système d'exploitation classique pour fonctionner.



Actuellement l'hyperviseur est la méthode de virtualisation d'infrastructure la plus performante mais elle a pour inconvénient d'être contraignante et onéreuse. Les systèmes d'exploitation invités doivent généralement être adaptés à la couche de virtualisation, ils ont donc « conscience » d'être virtualisés.

XEN : libre, hyperviseur supportant des noyaux Linux, Plan9, NetBSD, etc.

Oracle VM : propriétaire, hyperviseur sur plateforme x86

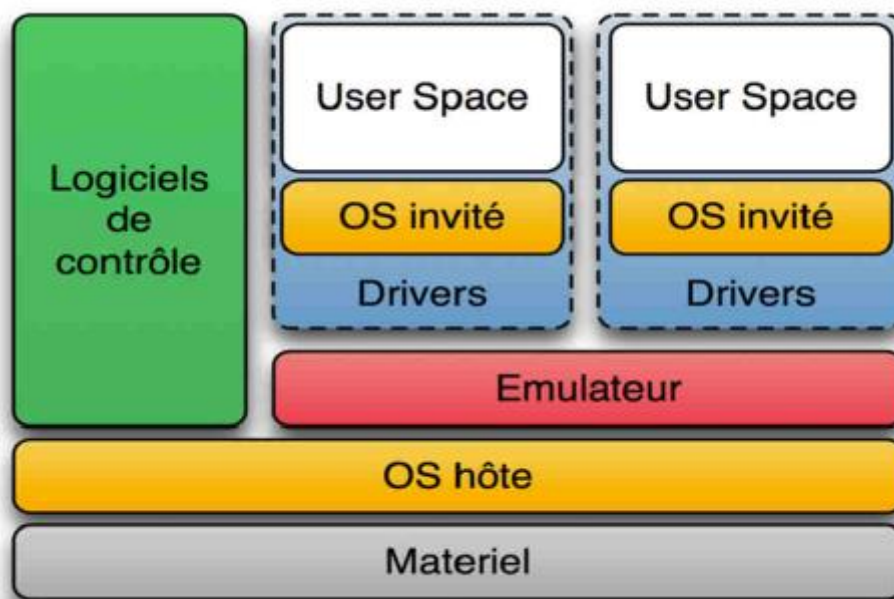
VMware : propriétaire, hyperviseur sur plateforme x86 (produits *ESX* et *ESXi-gratuit*)

Hyper V server : propriétaire hyperviseur sur plateforme x64 uniquement

KVM : libre, module noyau Linux tirant parti des instructions de virtualisation des processeurs Intel et AMD (Intel VT ou AMD-V)

La Virtualisation complète, Hyperviseur type 2 :

Un hyperviseur de « type 2 » est un émulateur s'exécutant par-dessus un système d'exploitation classique (hôte) comme n'importe quel autre programme. Il utilise les services fournis par le système d'exploitation hôte pour gérer de la mémoire et l'ordonnancement des machines virtuelles. Les systèmes d'exploitation invités n'ont pas conscience d'être virtualisés, ces derniers croient dialoguer directement avec ledit matériel.



Cette solution isole bien les OS invités, mais elle a un coût en performance. Ce coût peut être très élevé si le processeur doit être émulé, comme cela est le cas dans l'émulation. En échange cette solution permet de faire cohabiter plusieurs OS hétérogènes sur une même machine grâce à une isolation complète.

QEMU : émulateur de plateformes x86, PPC, Sparc

Bochs : émulateur de plateforme x86

Virtual Box : émulateur de plateforme x86

Oracle VM : émulateur de plateforme x86 (hyperviseur et guest)

VMware : émulateur de plateforme x86 (produits *VMware Server*, *VMware Player* et *VMware Workstation*)

Hyper V pour Windows server : hyperviseur sur plateforme x64 uniquement

MAC on Linux : émulateur de plateforme Mac OS sur Linux PPC

2. Sécurité de la virtualisation :

2.1 Les risques :

Les risques liés à la virtualisation des systèmes viennent s'ajouter aux risques « classiques » d'un système d'information. Dans le cas d'un choix d'architecture regroupant plusieurs systèmes sur une même machine, on doit ainsi considérer :

- les risques pouvant toucher un système ;
- ceux portant sur la couche d'abstraction ;
- les risques induits par la combinaison des deux.

De plus, le fait de regrouper plusieurs services sur un même matériel augmente les risques portant sur chacun. Il est donc important de connaître l'ensemble des risques pour en maîtriser l'impact en termes de confidentialité, d'intégrité et de disponibilité des données et des applications.

Risque 1 : Risque accru de compromission des systèmes :

On entend ici par « **compromission** » la prise de contrôle par un acteur malveillant d'une brique utilisée dans le système virtualisé. Il peut s'agir d'une compromission d'un système invité depuis un autre système invité, ou du système hôte depuis un système invité. On remarque qu'une compromission du **système hôte** peut éventuellement entraîner une compromission de **l'ensemble des systèmes** s'exécutant sur la machine. On note également que plus la compromission touche le système en **profondeur**, plus elle aura de conséquences sur les capacités de remise en service ultérieure du système.

Les solutions permettant d'empêcher une compromission sont souvent délicates à mettre en œuvre. Il s'agira de **diminuer** au maximum la surface d'attaque. Il conviendra notamment que chaque brique (matériel, système d'exploitation hôte, systèmes d'exploitation invités etc.) soit à jour de tous les correctifs de sécurité. En particulier, l'emploi d'une solution de virtualisation imposant aux systèmes invités de fonctionner dans des configurations obsolètes n'est pas acceptable.

Risque 2 : Accroissement du risque d'indisponibilité :

Comme évoqué précédemment, une **compromission** peut engendrer une **indisponibilité** d'un service. Cependant, ce risque peut apparaître, même en l'absence de compromission. Ainsi, si d'une part un problème de la virtualisation est l'utilisation plus intensive des ressources informatiques, d'autre part, la panne d'une ressource commune peut engendrer **l'indisponibilité simultanée** de plusieurs systèmes.

Là encore, les préconisations faites au point précédent s'appliquent. De plus, si des besoins en disponibilité diffèrent sensiblement d'une application à une autre, il peut être préférable de **placer sur des machines dédiées celles dont les besoins en disponibilité sont les plus élevés**.

Risque 3 : Complexité de l'administration et de la mise en œuvre :

Lorsqu'une solution de virtualisation est utilisée, il est nécessaire d'administrer d'une part les différents systèmes invités, mais également la couche d'abstraction. Le choix d'administration d'un système à distance ou non doit être fait en considérant tous les risques induits. Parmi de tels risques, on trouve **l'usurpation du rôle d'administrateur** permise suite à la mise en place d'un mécanisme d'authentification trop

faible, **la perte de confidentialité et/ou d'intégrité** d'une commande circulant sur le réseau, **la perte de traçabilité** des opérations d'administration. Il convient ainsi de bien sécuriser l'ensemble des interfaces de gestion et de tracer toute action réalisée par leur biais.

Risque 4 : Incapacité à gérer voire à comprendre les erreurs :

Les problèmes de fonctionnement et les erreurs peuvent être complexes à gérer techniquement dans une architecture s'appuyant sur une solution de virtualisation. Par exemple, les erreurs qui pourraient survenir lors de **l'arrêt puis la relance d'une instance** seront soit rapportées au système hôte que l'instance quitte, soit au système hôte qui est en train de l'accueillir. Sans la prise en compte globale des **erreurs d'un système** s'appuyant sur la virtualisation, il se peut que des informations pertinentes permettant d'identifier leur cause soient perdues, ou a minima, que leur synthèse ne puisse pas être réalisée. Il convient donc de mettre en place une centralisation et une corrélation des journaux sur l'ensemble des systèmes.

2.2 Les solutions de sécurité (outils techniques):

Politique d'authentification :

Aspect essentiel dans la protection des données, des solutions d'authentification sécurisée sont proposées sur le marché.

Intel Cloud SSO (Single Sign-On) est une solution pour automatiser l'accès aux services dans le cloud en mode SaaS. Ce service permet à la fois de s'authentifier pour accéder à un service cloud, mais permet aussi de gérer les autorisations.

Politique de pare-feu et de détection des intrusions :

Si un événement arrive et qu'il ne correspond pas à un des modèles connus, alors il s'agit probablement d'une attaque. Il existe plusieurs solutions pour bloquer les intrusions avec des politiques de pare-feu et de détection. La solution **Virtual PF** est une solution gratuite et fiable qui donne un pare-feu et un IPS efficace.

Protection des infrastructures virtuelles :

La sécurité des environnements virtuels est primordiale : les attaques sont nombreuses sur les instances de Machines Virtuelles (application, système d'exploitation). La signature future de VM identifiable par un catalogue de VM de l'entreprise (pour ne pas se les faire voler) pourrait constituer une bonne solution. En attendant, plusieurs solutions sont proposées sur le marché : **CloudPassage** améliore la sécurité des serveurs dans le cloud avec une nouvelle version de ses outils de sécurité SaaS **Halo** appelée **NetSec**. L'idée est de sécuriser l'image de base et que celle-ci s'adapte automatiquement, donc de manière élastique lorsque le nombre d'instance augmente ou diminue.

Protection de la messagerie :

Dans les entreprises, la messagerie est souvent l'un des premiers éléments en extérieur dans le cloud. Les informations circulant dans les mails sont loin d'être sûrs, c'est pourquoi des solutions de sécurité de messagerie sont proposées : **OpenText Managed File Transfer** est une solution pour gérer les échanges de fichiers volumineux de l'entreprise de manière sécurisée. Elle s'intègre à Microsoft Outlook et simplifie les questions liées à la taille des pièces jointes.

3. Installation

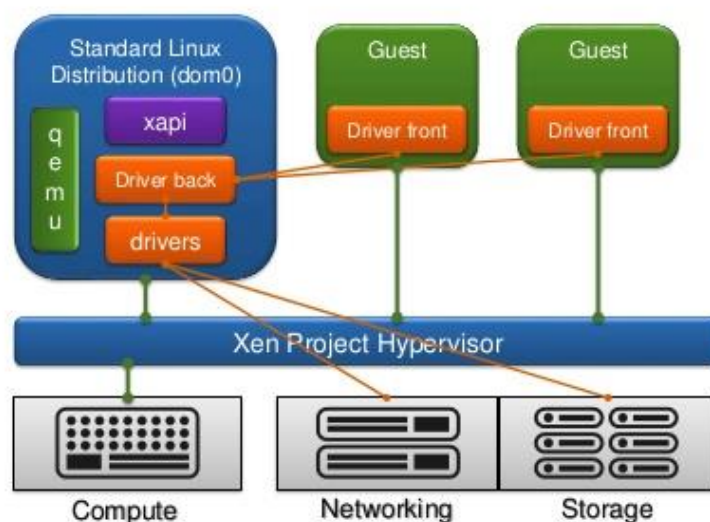
3.1 L'outil Xen :

Xen est un logiciel libre de virtualisation, plus précisément un hyperviseur de machine virtuelle. **Xen** permet d'exécuter plusieurs systèmes d'exploitation (et leurs applications) de manière isolée sur une même machine physique sur plate-forme x86, x86-64. Les systèmes d'exploitation invités partagent ainsi les ressources de la machine hôte.

Xen est un « paravirtualiseur » ou un « hyperviseur type 1 » de machines virtuelles. Les systèmes d'exploitation invités ont « conscience » du Xen sous-jacent, ils ont besoin d'être « portés » (adaptés) pour fonctionner sur Xen. Linux, NetBSD, FreeBSD, Plan 9 et GNU Hurd peuvent d'ores et déjà fonctionner sur Xen.

Produits : [XenServer](#), [XenDesktop](#), [XenApp](#), [Xen Motion](#), [Xen Orchestra](#)

Simplified XenServer Architecture Diagram

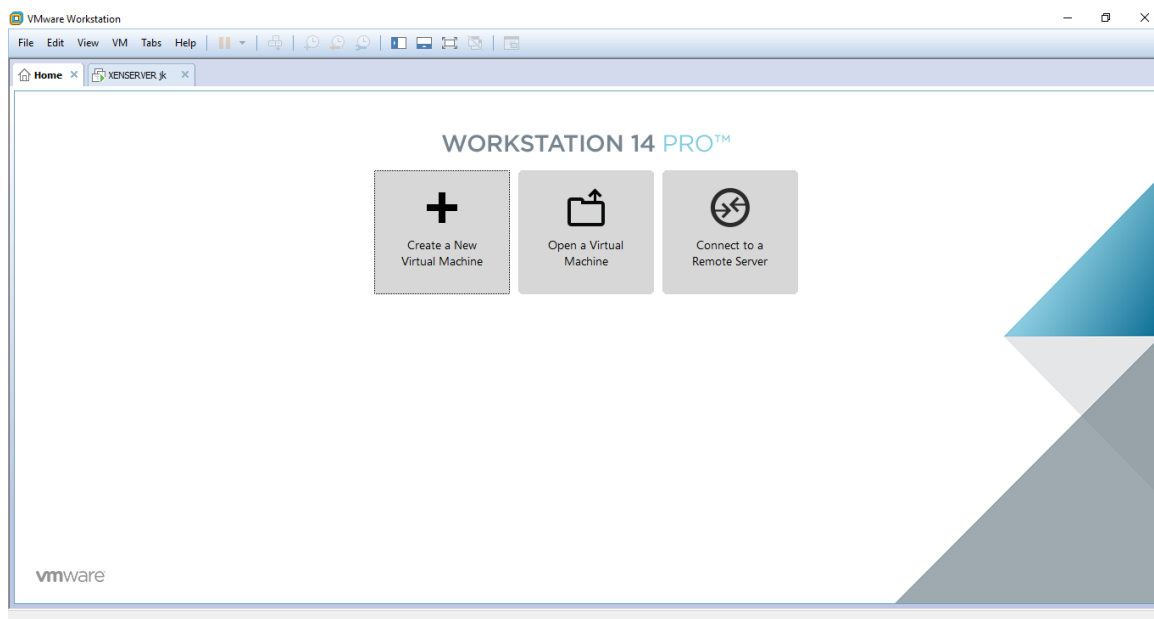


Open@Citrix

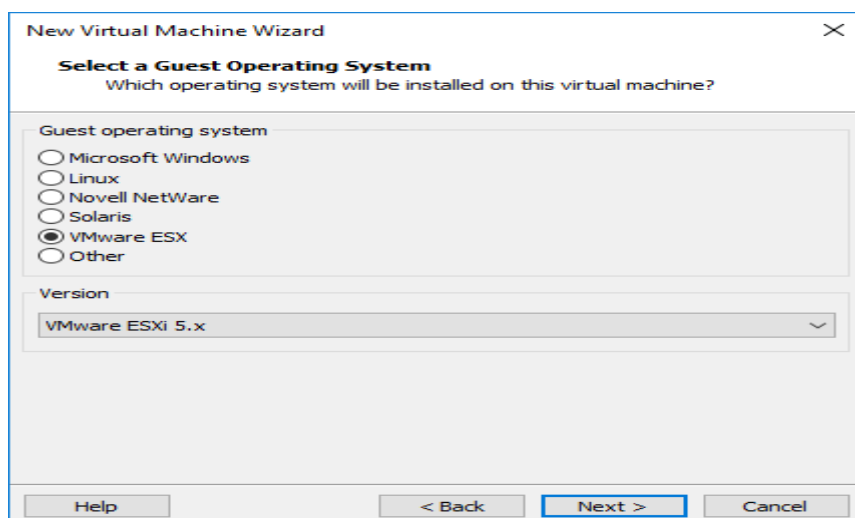
3.2 Téléchargement et installation des outils :

Téléchargement et installation de XenServer :

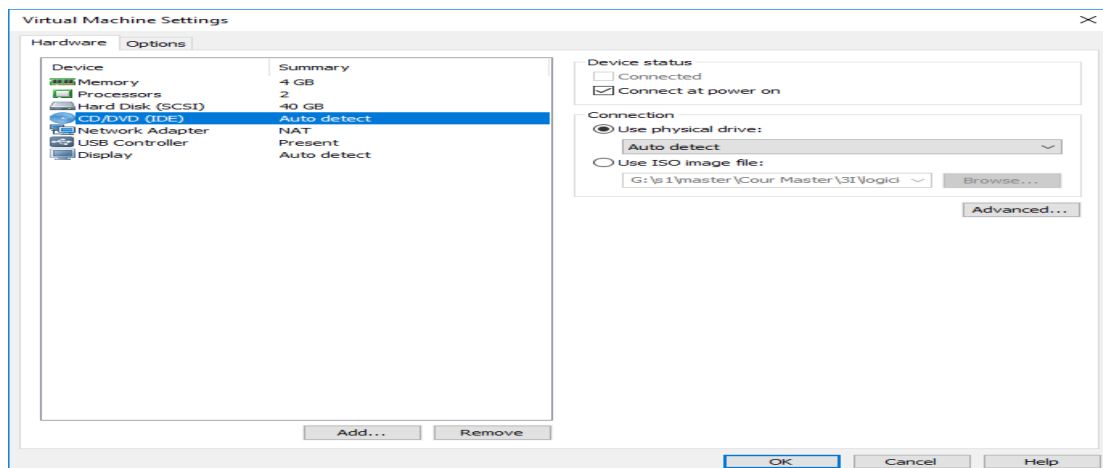
On accède au site officiel de Citrix pour télécharger l'iso de XenServer, ensuite on démarre VMware pour créer notre nouvelle VM, :



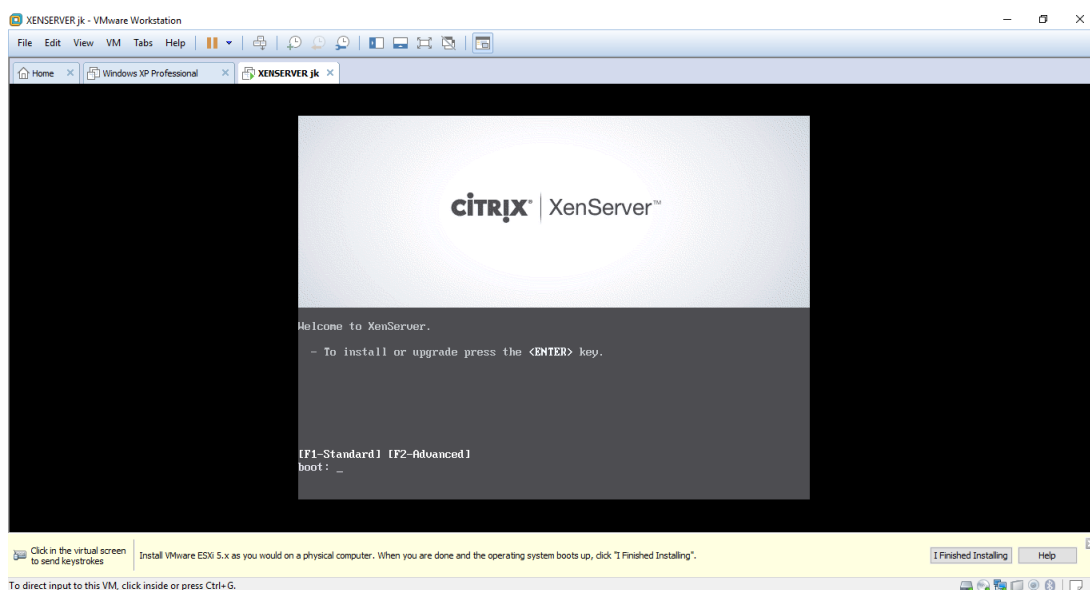
Dans cette étape de création on met VMware ESX version 5.X :



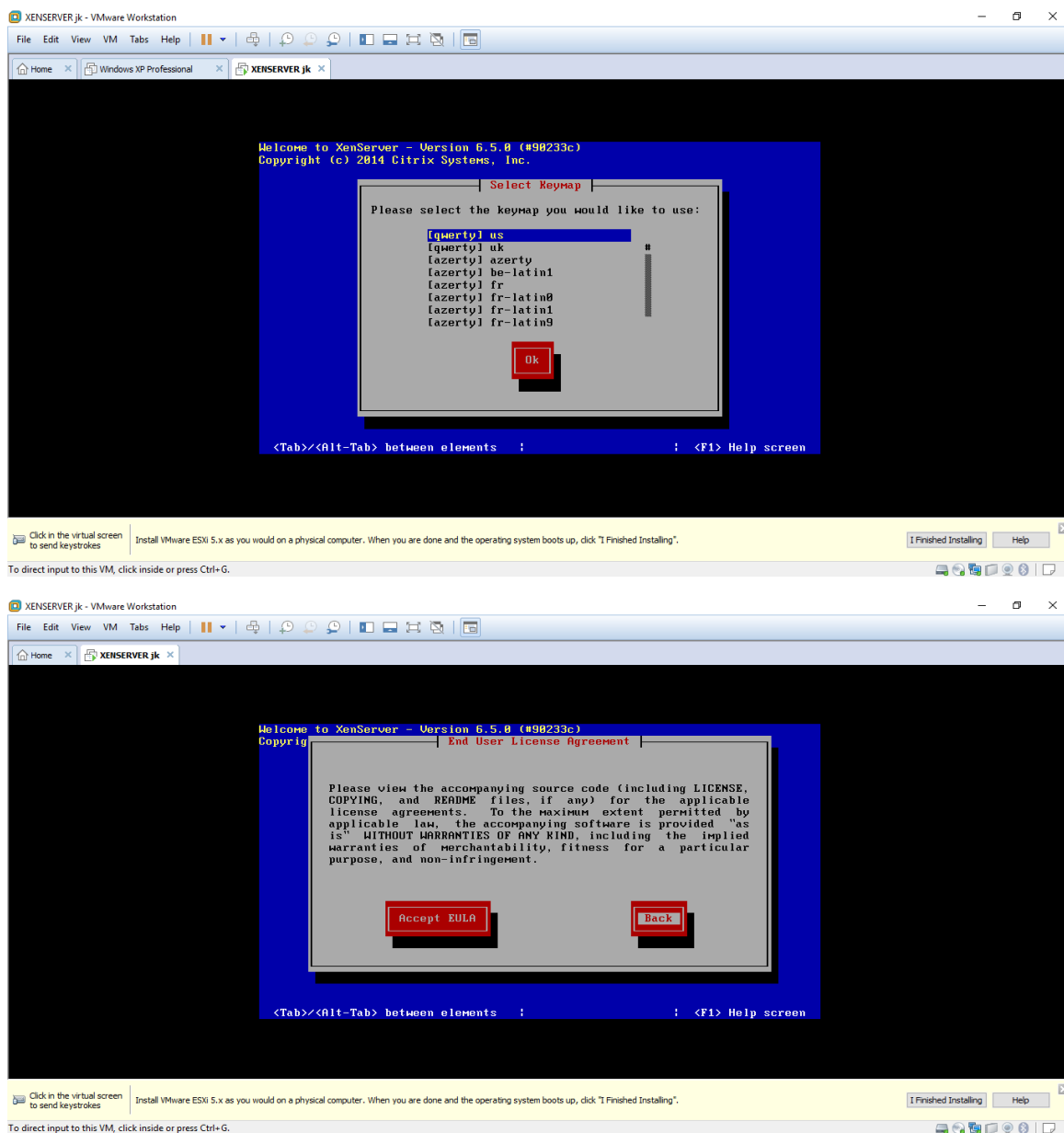
Ensuite on ajoute l'image iso de XenServer :



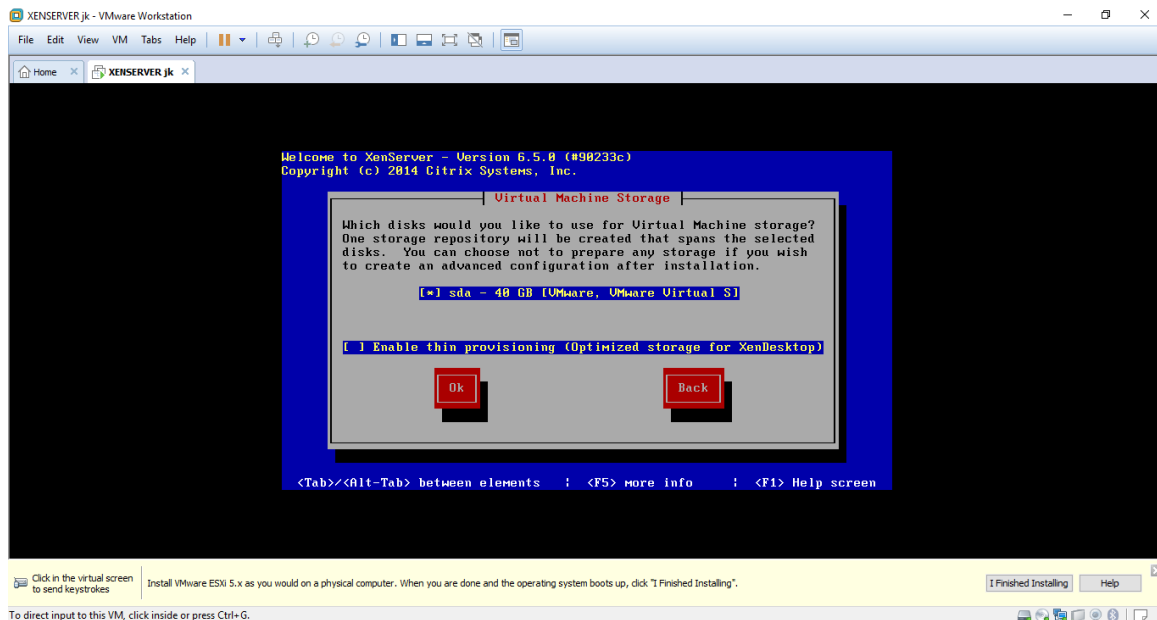
On démarre la machine virtuelle :



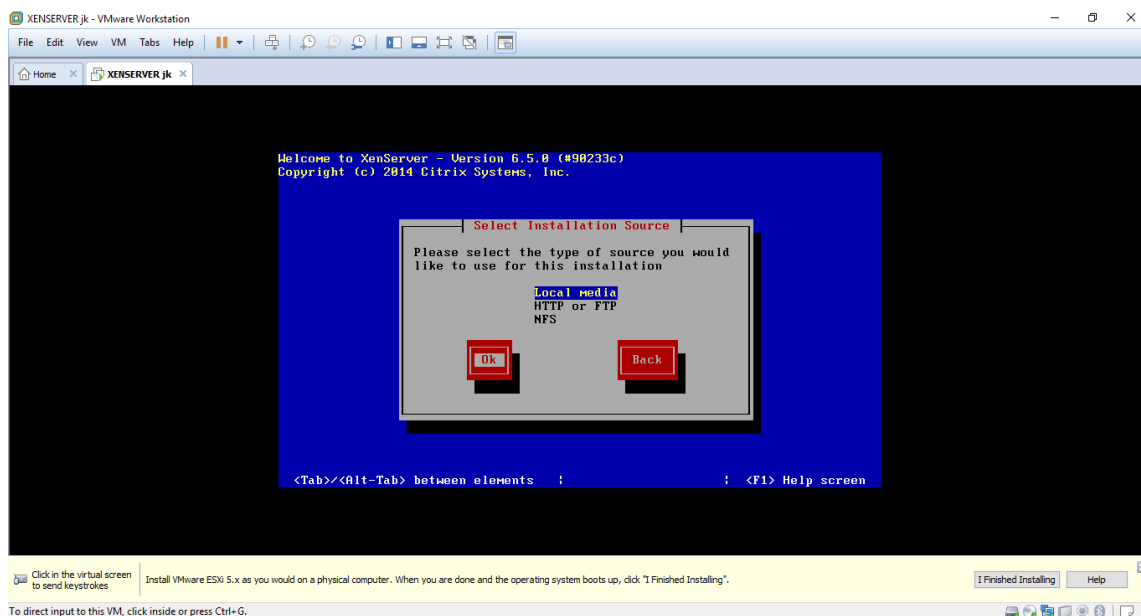
On modifie le clavier et accepte la licence :



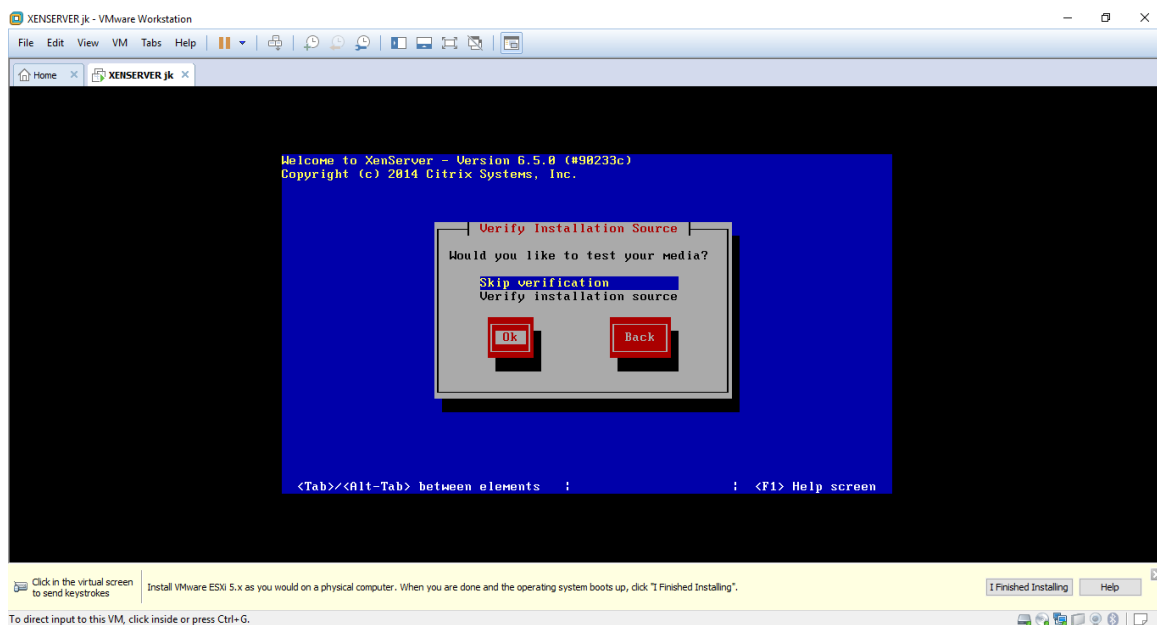
Choisir l'unité de stockage pour le stockage virtuel de la machine :



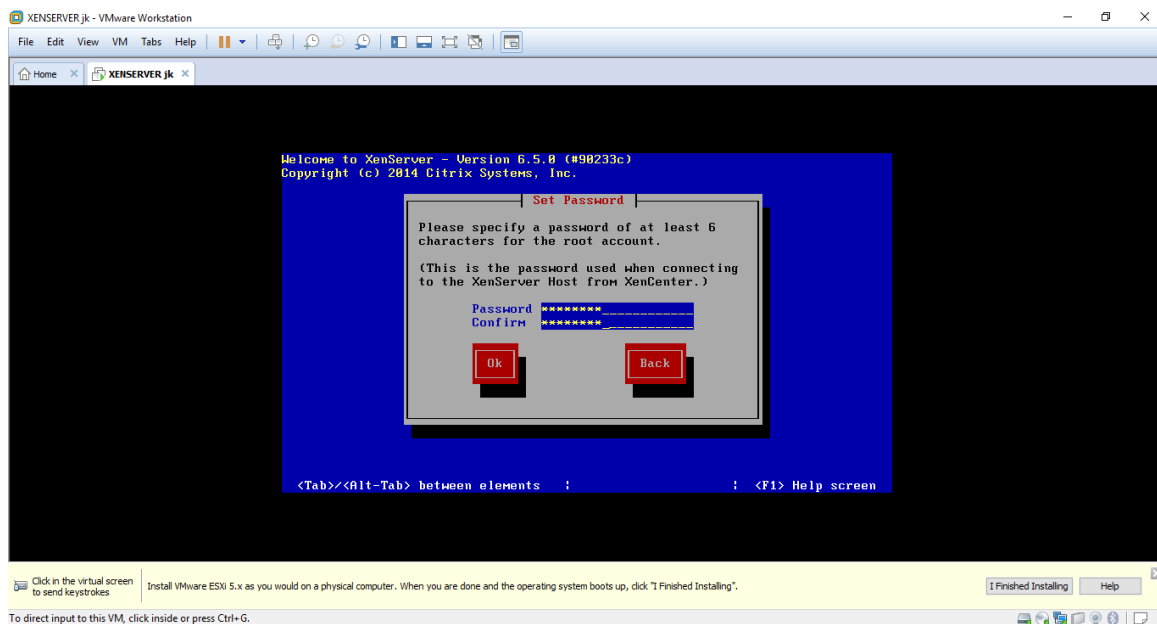
Sélectionner la source du média d'installation :



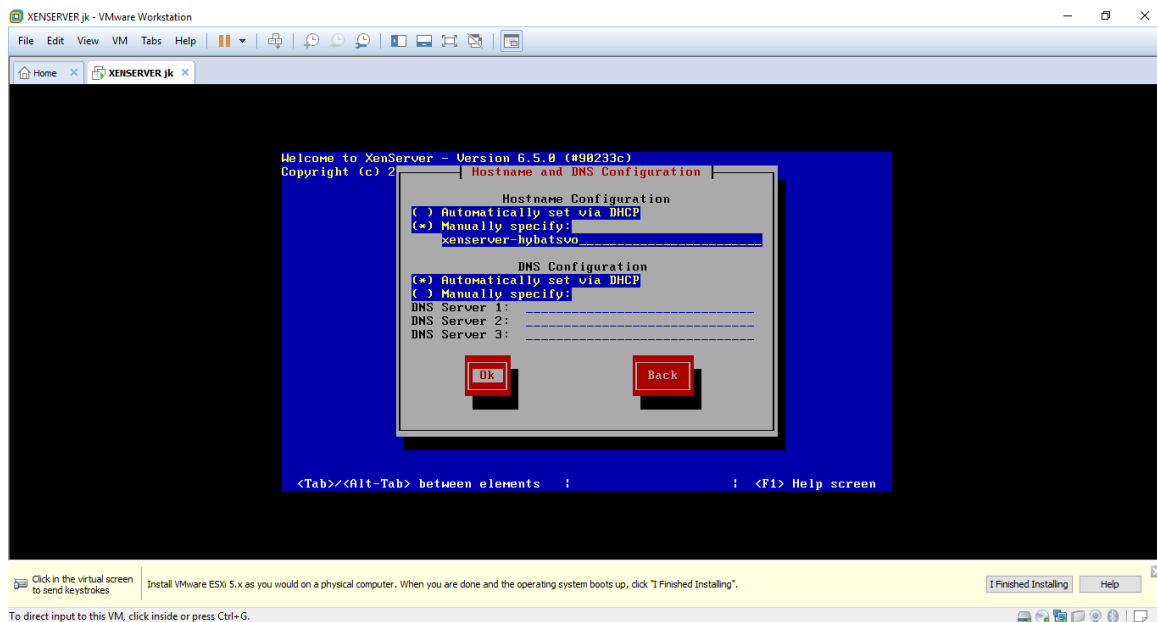
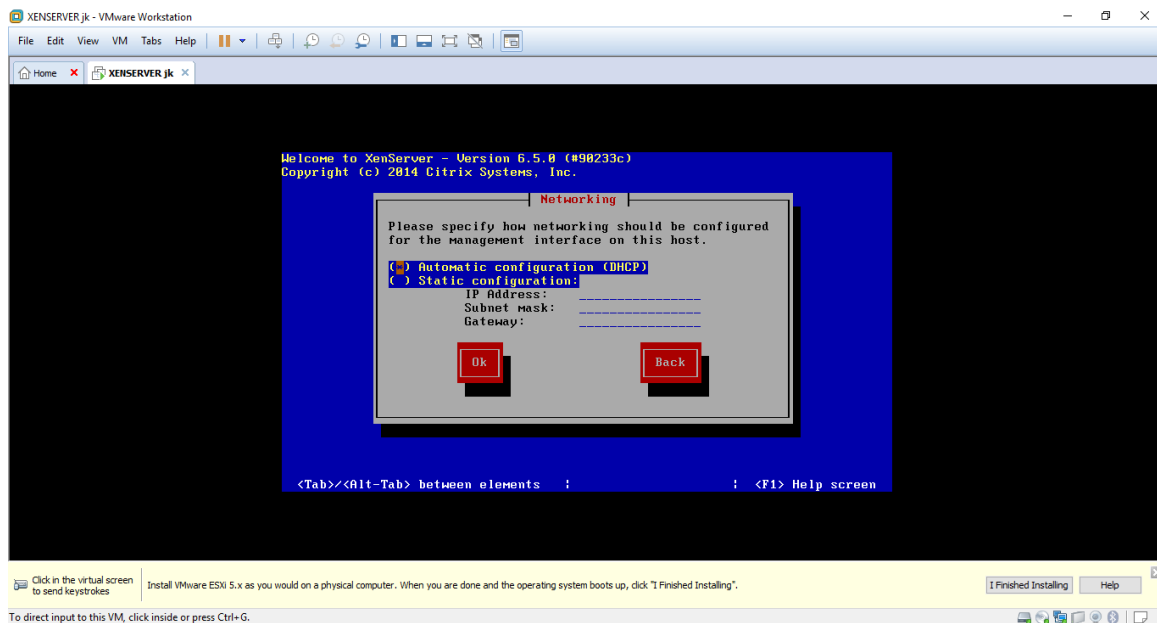
Choisir Skip verification :



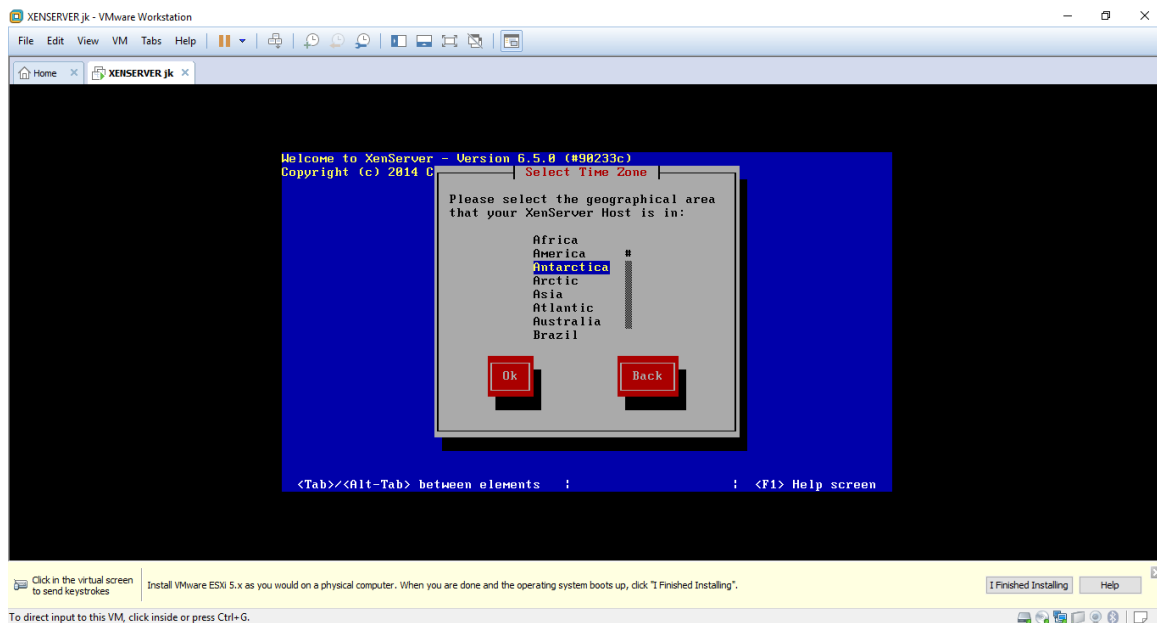
Saisir le mot de passe :



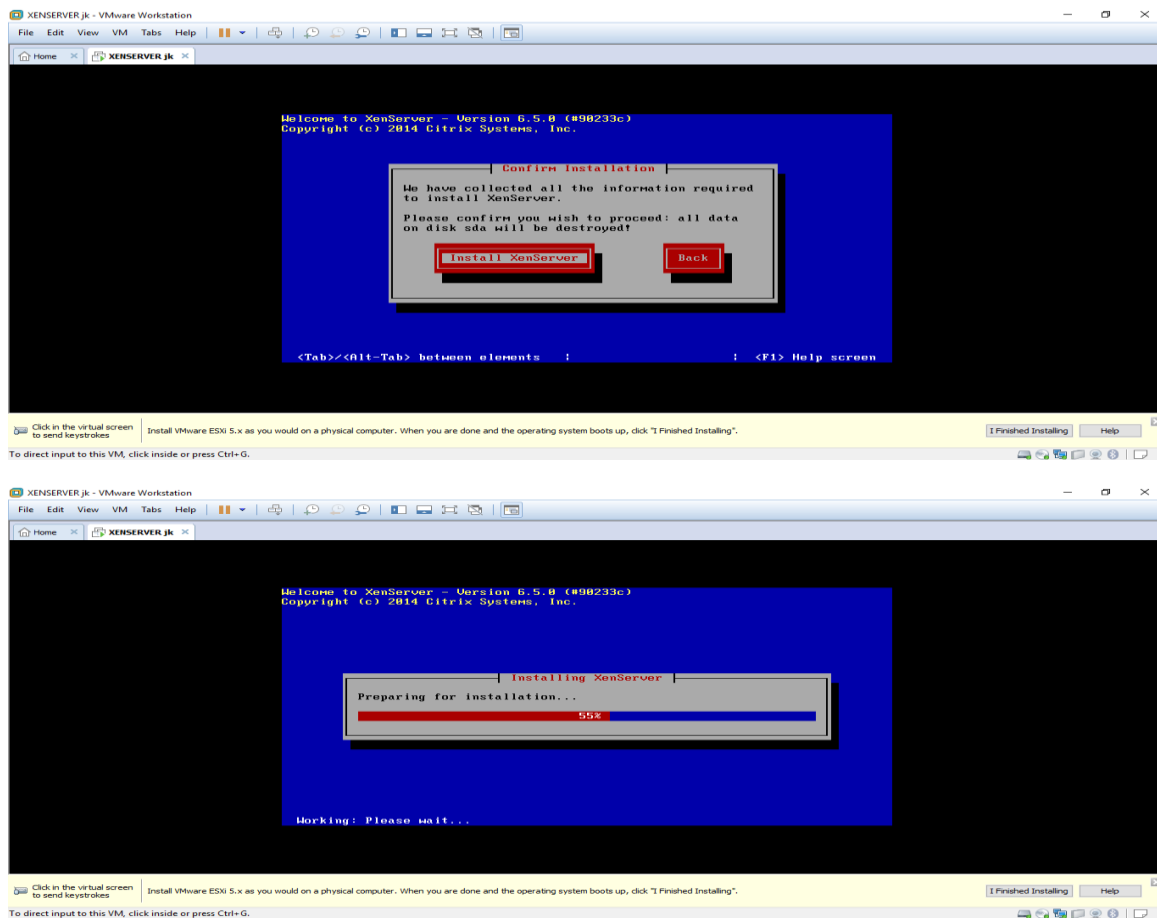
Configuration réseau :



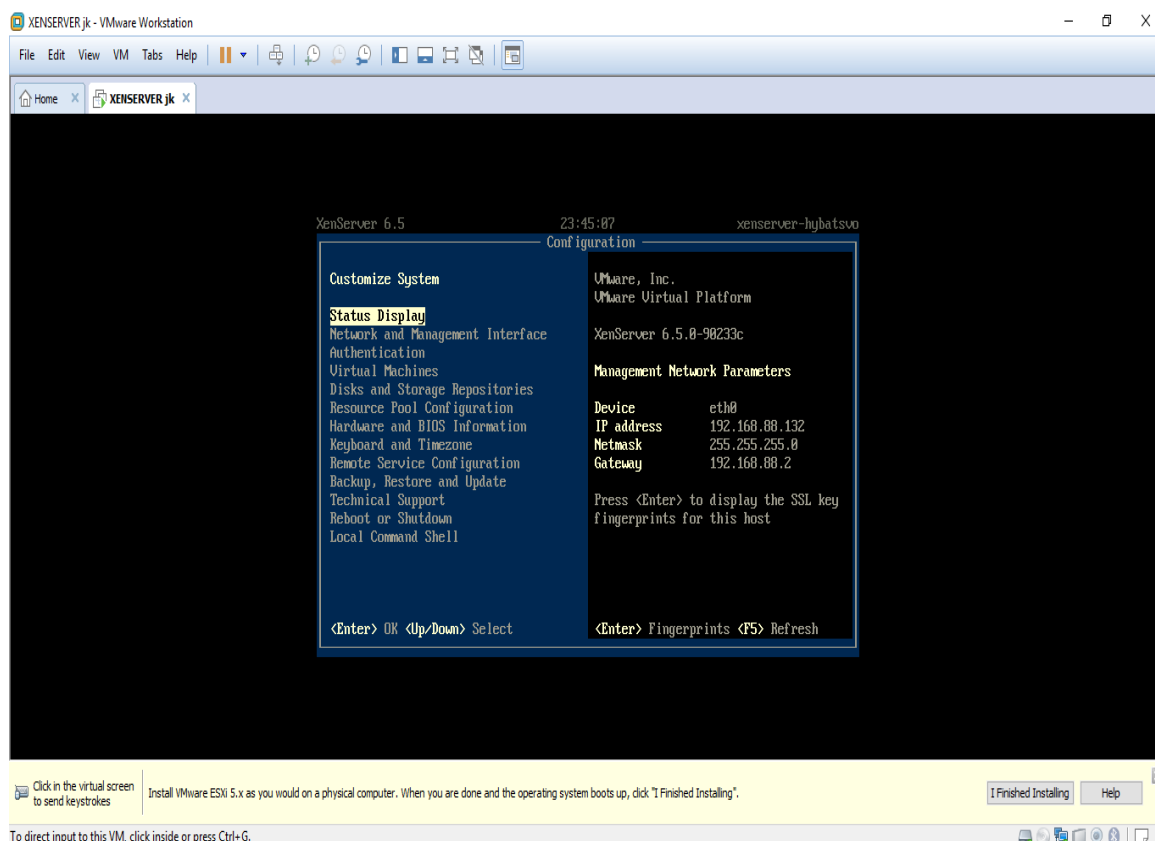
Choisir le pays :



Lancer l'installation :



Quand l'installation se termine voici la page du serveur qui apparaît :



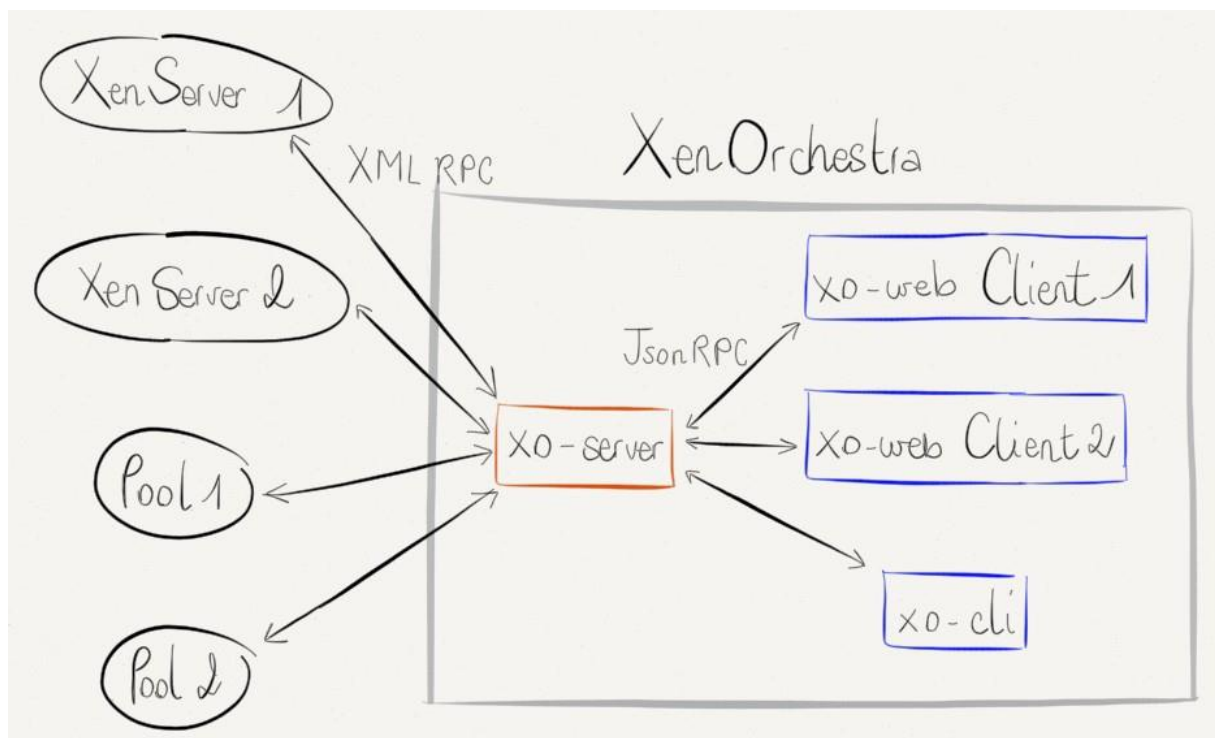
Téléchargement et installation de Xen-Orchestra :

XO est une interface Web permettant de visualiser et d'administrer vos hôtes XenServer (ou compatibles XAPI). Aucun agent n'est requis pour que cela fonctionne.

Il vise à être facile à utiliser sur tout appareil prenant en charge les technologies Web modernes (HTML 5, CSS 3, JavaScript), tel que votre ordinateur de bureau ou votre smartphone.



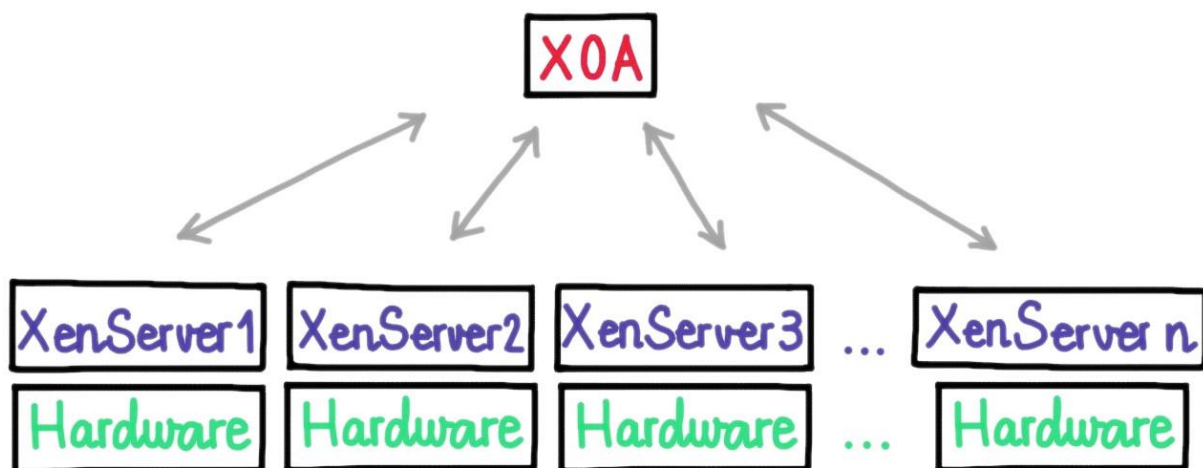
Xen Orchestra lui-même est conçu comme une solution modulaire. Chaque partie à son rôle : Le noyau est "xo-server" - un démon traitant directement avec des hôtes compatibles XenServer ou XAPI. C'est là que les utilisateurs sont stockés et c'est le point central pour communiquer avec l'ensemble de votre infrastructure Xen. L'interface Web est "xo-web" - elle s'exécute directement à partir de votre navigateur. La connexion avec xo-server se fait via WebSockets. "xo-cli" est un module permettant d'envoyer des commandes directement à partir de la ligne de commande.



L'appliance virtuelle **Xen Orchestra (XOA)** est une machine virtuelle sur laquelle Xen Orchestra est déjà installé, ce qui permet de l'utiliser immédiatement.

C'est le moyen le plus simple d'essayer Xen Orchestra rapidement.

Votre XOA est connecté à tous vos hôtes ou au maître de pool uniquement si vous utilisez des pools dans XenServer :

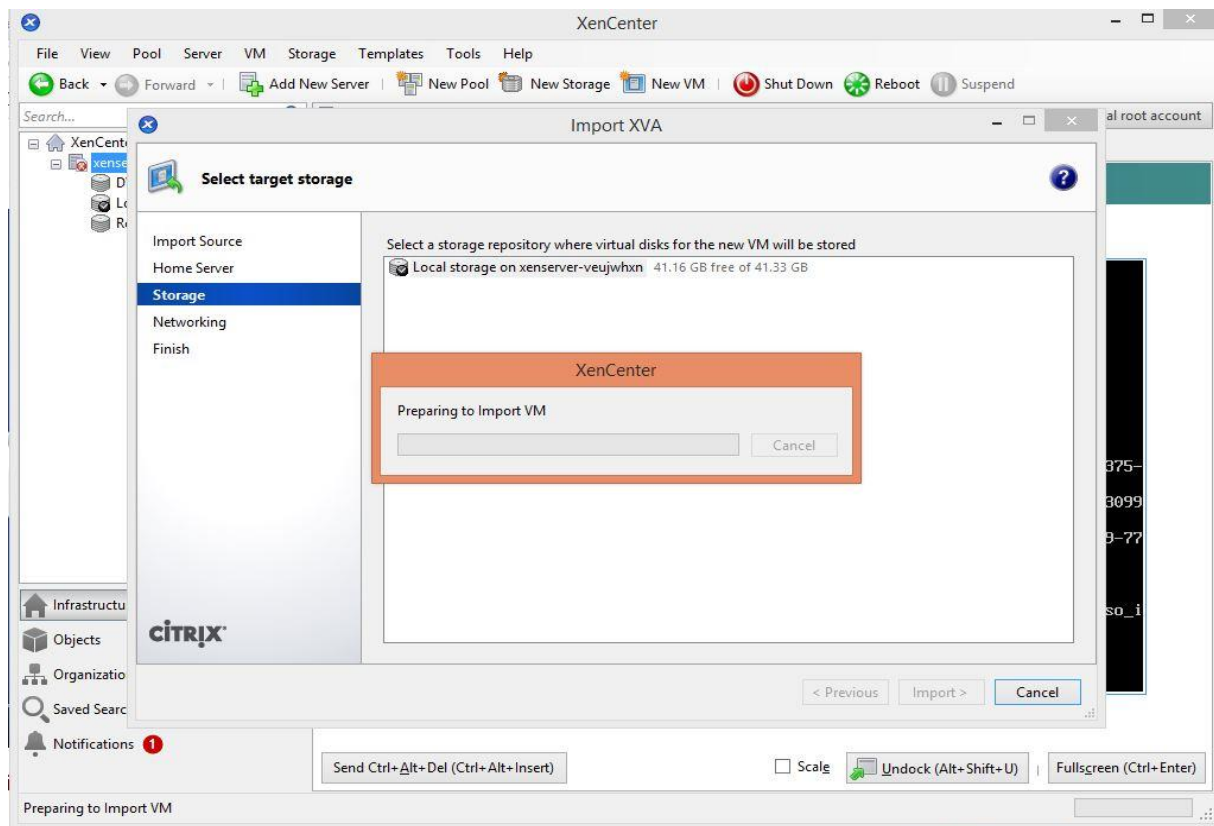


Installation :

Téléchargez XOA sur xen-orchestra.com. Une fois que vous avez obtenu le fichier XVA, vous pouvez l'importer avec `xe vm-import nom_fichier = xoa_unified.xva` ou via XenCenter.

Une fois la machine virtuelle importée, il vous suffit de la démarrer avec `xe vm-start vm = "XOA Unified"` ou via XenCenter.

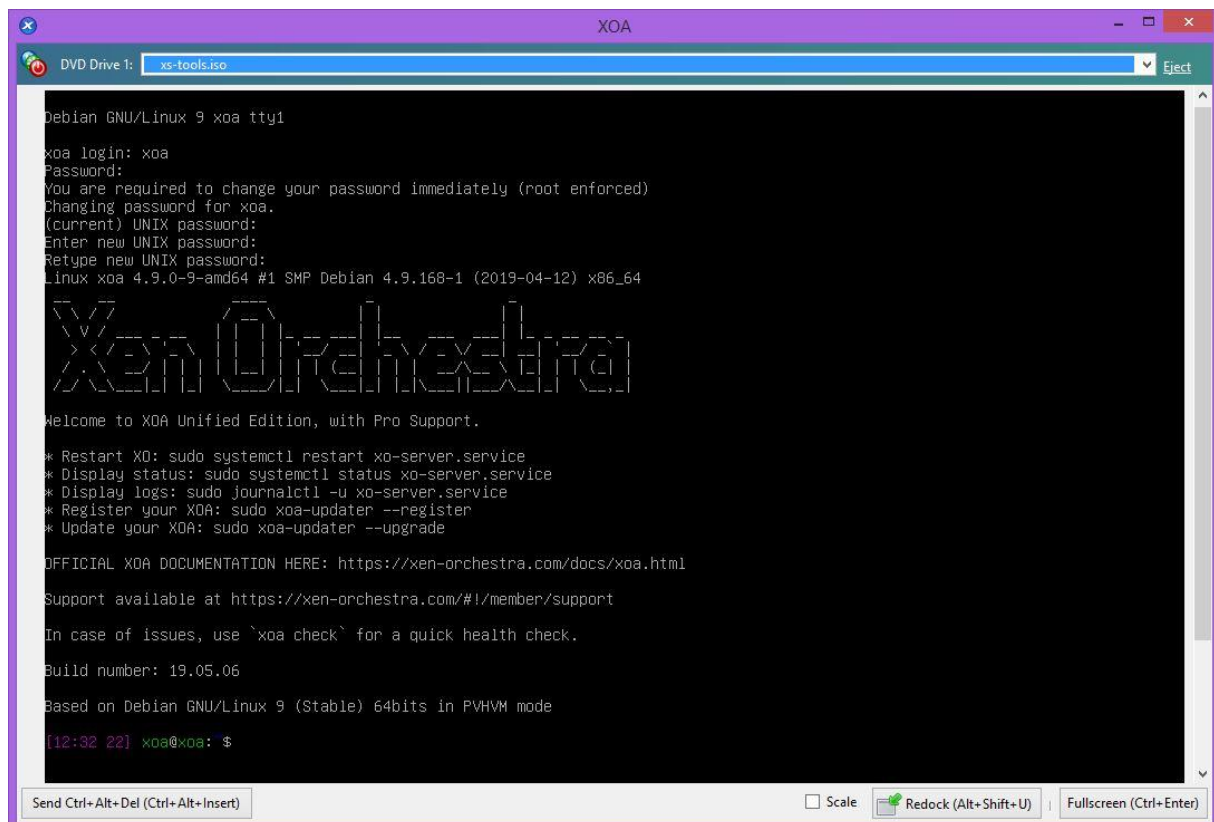
Importation du fichier xva :



Création de la iso repository dans la XenServer console :



1er Login à XO :

A screenshot of the XO login screen. The window title is 'XOA'. The top bar shows 'DVD Drive 1: xs-tools.iso' and an 'Eject' button. The main terminal area shows the login process for 'xoa' on a Debian GNU/Linux 9 system. It prompts for a password, enforces a password change, and displays the 'Xen Orchestra' logo. Below the logo, it says 'Welcome to XOA Unified Edition, with Pro Support.' and lists several commands for managing the service. It also provides links for documentation and support, and mentions the build number and PVHVM mode. The prompt is 'xoa@xoa: \$'.

```
Debian GNU/Linux 9 xoa tty1
xoa login: xoa
Password:
You are required to change your password immediately (root enforced)
Changing password for xoa.
(current) UNIX password:
Enter new UNIX password:
Retype new UNIX password:
Linux xoa 4.9.0-9-amd64 #1 SMP Debian 4.9.168-1 (2019-04-12) x86_64

Xen Orchestra

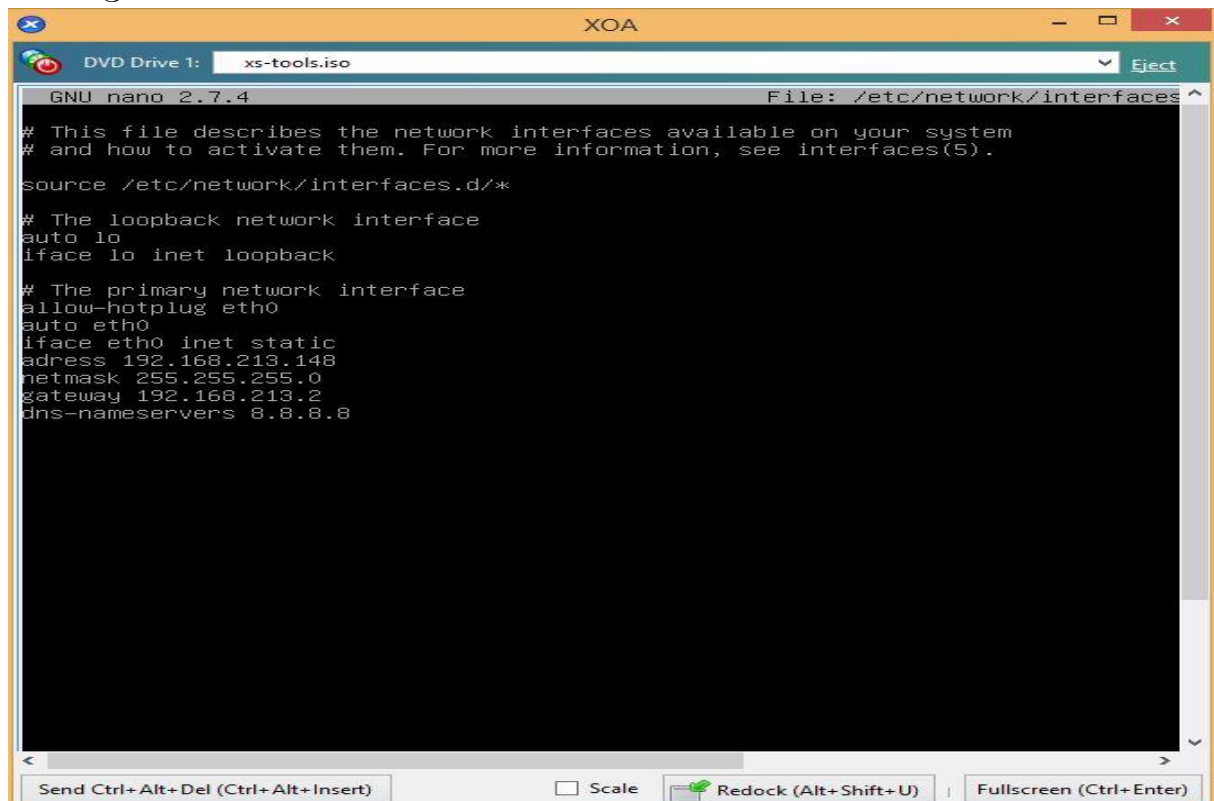
Welcome to XOA Unified Edition, with Pro Support.

* Restart XO: sudo systemctl restart xo-server.service
* Display status: sudo systemctl status xo-server.service
* Display logs: sudo journalctl -u xo-server.service
* Register your XOA: sudo xoa-updater --register
* Update your XOA: sudo xoa-updater --upgrade

OFFICIAL XOA DOCUMENTATION HERE: https://xen-orchestra.com/docs/xoa.html
Support available at https://xen-orchestra.com/#/member/support
In case of issues, use `xoa check` for a quick health check.
Build number: 19.05.06
Based on Debian GNU/Linux 9 (Stable) 64bits in PVHVM mode

[12:32 22] xoa@xoa: $
```

Configuration réseau du XO :

A screenshot of the XO network configuration screen. The window title is 'XOA'. The top bar shows 'DVD Drive 1: xs-tools.iso' and an 'Eject' button. The main terminal area shows the 'nano' editor editing the file '/etc/network/interfaces'. The content of the file is visible, showing the configuration for the loopback interface 'lo' and the primary network interface 'eth0'. The prompt is 'xoa@xoa: \$'.

```
GNU nano 2.7.4 File: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

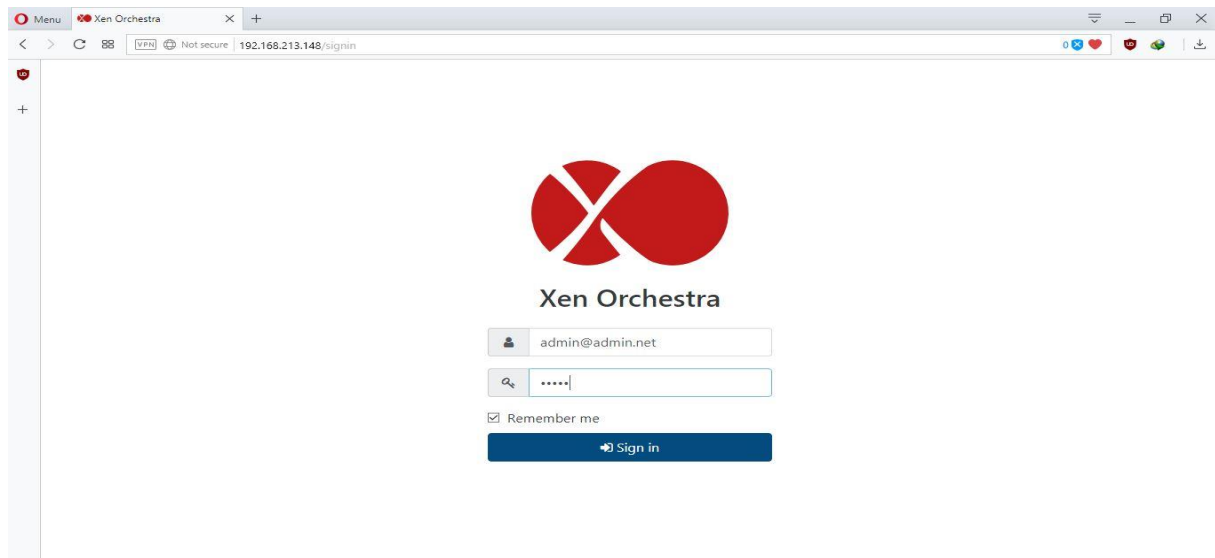
source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

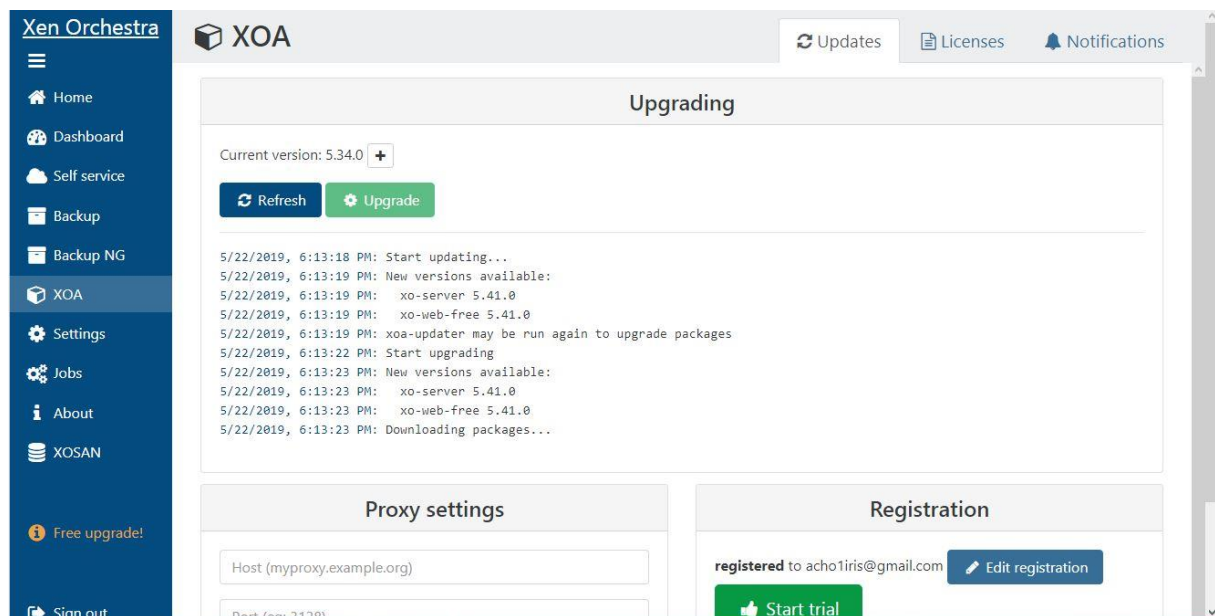
# The primary network interface
allow-hotplug eth0
auto eth0
iface eth0 inet static
address 192.168.213.148
netmask 255.255.255.0
gateway 192.168.213.2
dns-nameservers 8.8.8.8

xoa@xoa: $
```

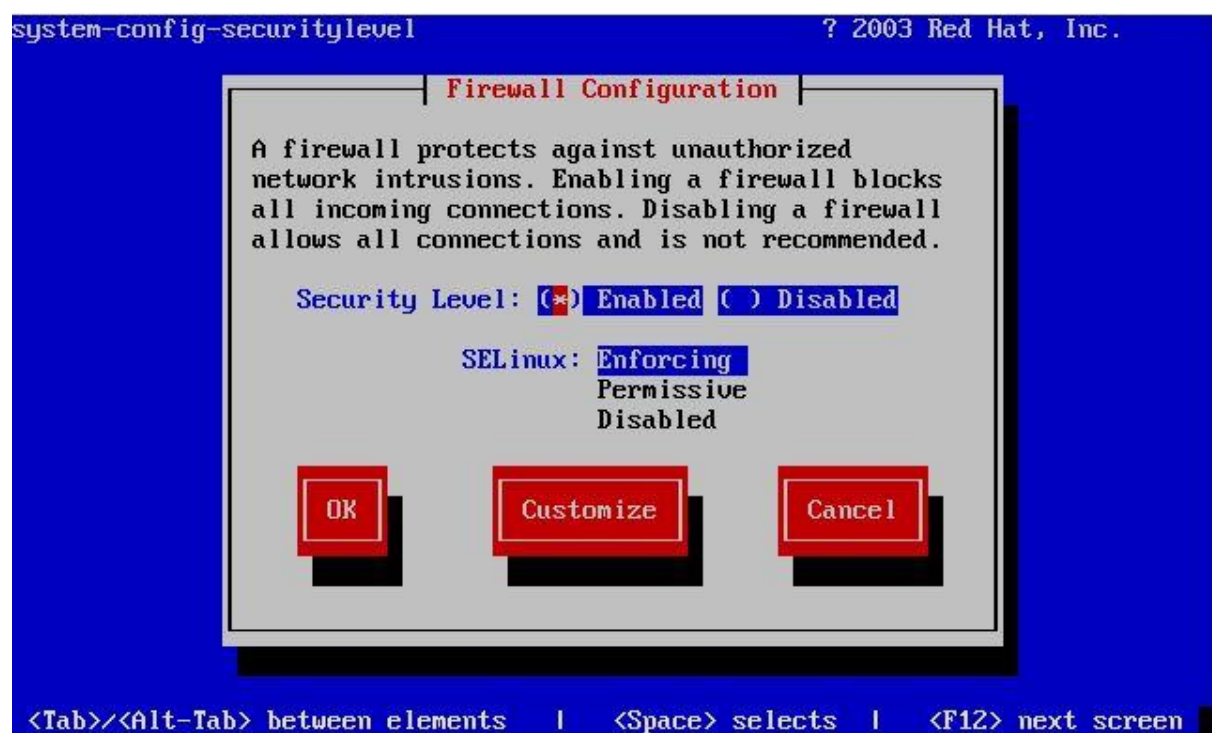
Login Web dans XO :



Mise à jour et optimisation dans XOA :



Installation de iptables dans XO :





Le résultat :

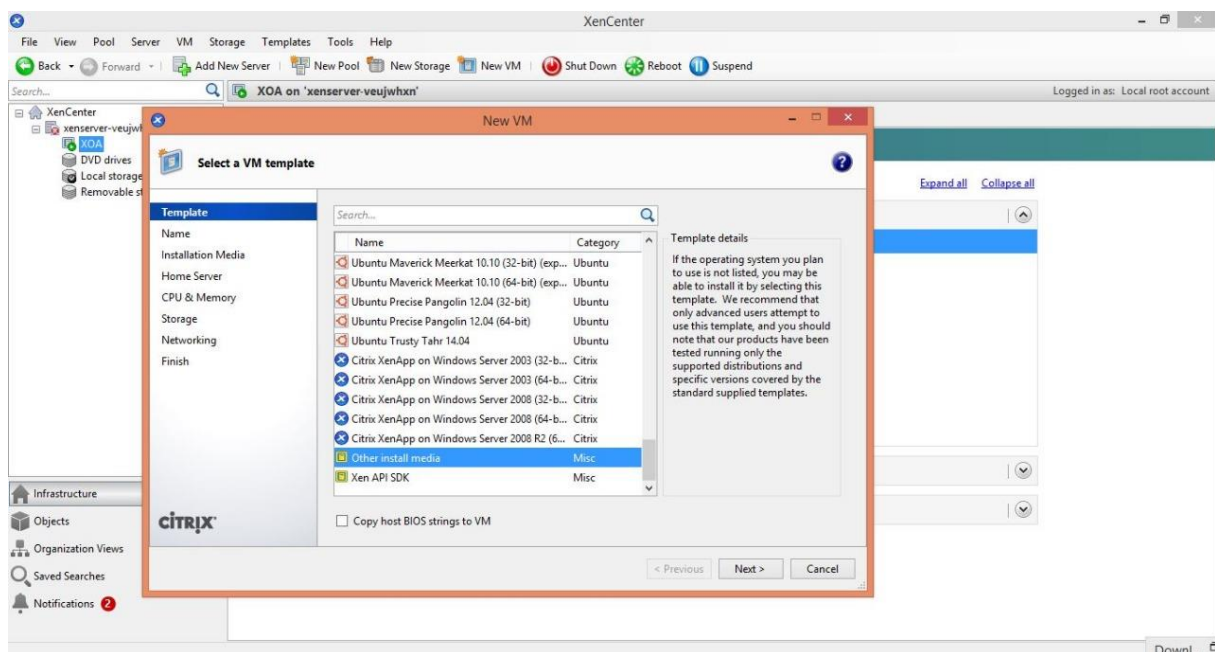
```
# Firewall configuration written by system-config-securitylevel
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -p 50 -j ACCEPT
-A RH-Firewall-1-INPUT -p 51 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp --dport 5353 -d 224.0.0.251 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m udp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m tcp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 694 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 443 -j ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
[root@xenserver-veujwhxn ~]# more /etc/sysconfig/iptables
```


Installation et configuration de Virtual pf :

Virtual pf est un firewall et IPS (Système de prévention d'intrusions) dédié aux environnements de virtualisation



Installation :



New VM

Name the new virtual machine

Template

Name

Installation Media

Home Server

CPU & Memory

Storage

Networking

Finish

Enter a name that will help you to identify the virtual machine later. This could be a name that describes its software and hardware such as RHEL DHCP Server, Win2K3 XenApp Server or Exchange 2007 Client Access Server. This name will also be displayed in XenCenter's Resources pane and can be changed later.

You can also add a more detailed description of the VM, if you wish.

Name:

VirtualIPF

Description:

Firewall & HIPS

CITRIX

< Previous

Next >

Cancel

New VM

Locate the operating system installation media

Template

Name

Installation Media

Home Server

CPU & Memory

Storage

Networking

Finish

Select the installation method for the operating system software you want to install on the new VM.

☒ Install from ISO library or DVD drive:

DVD drive 0 on xenserver-veujwhxn

[New ISO library...](#)

☐ Boot from network

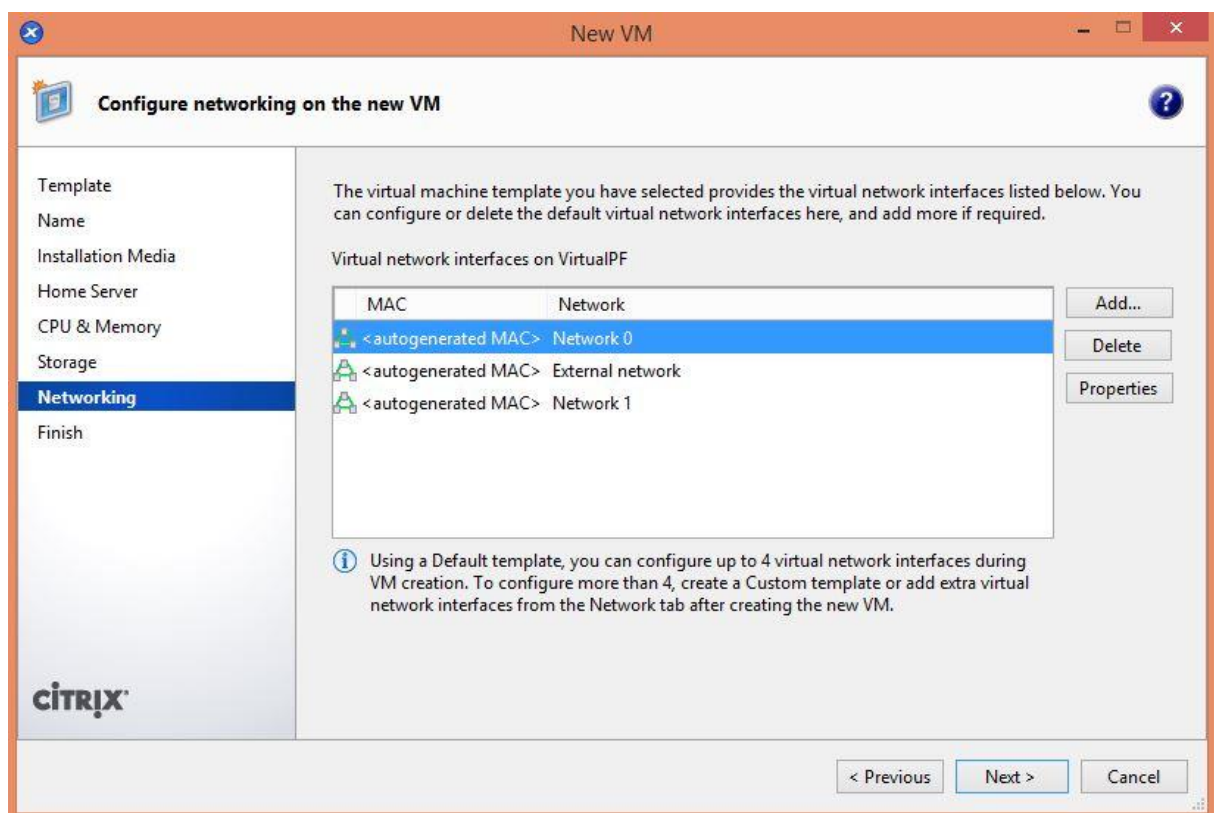
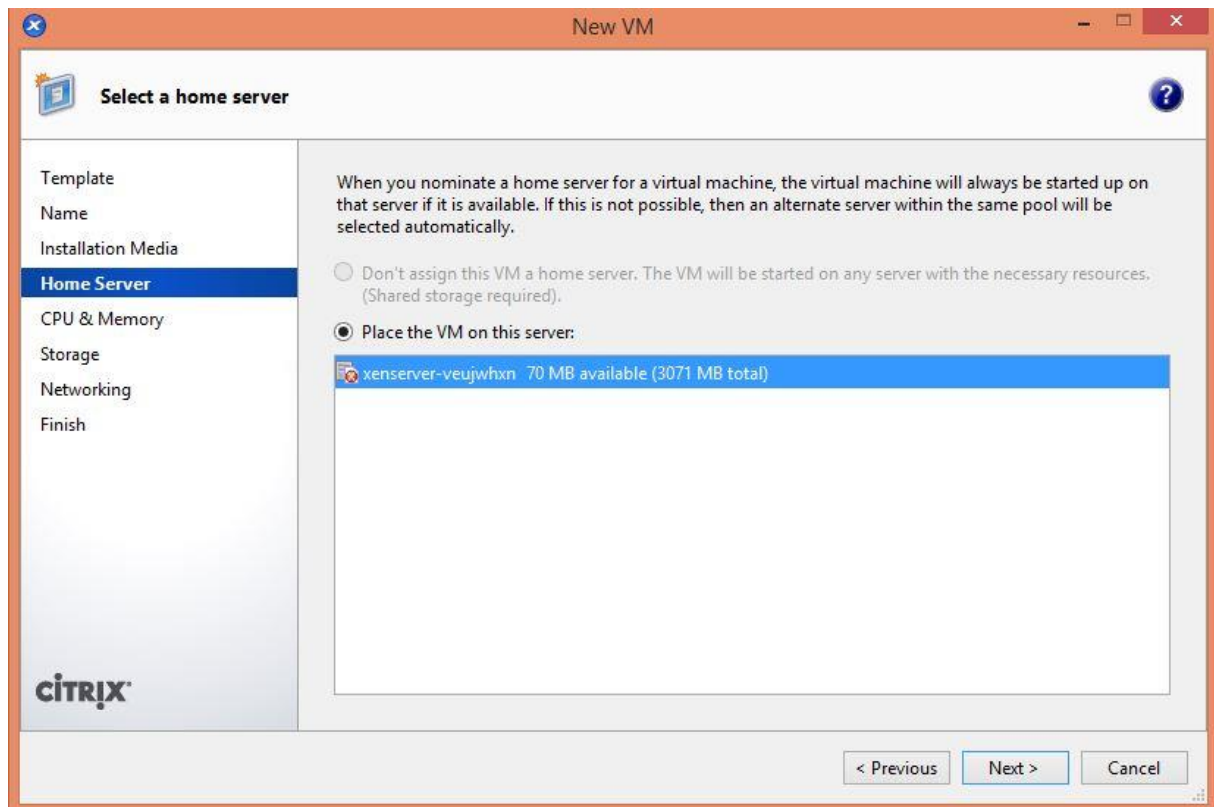
CITRIX

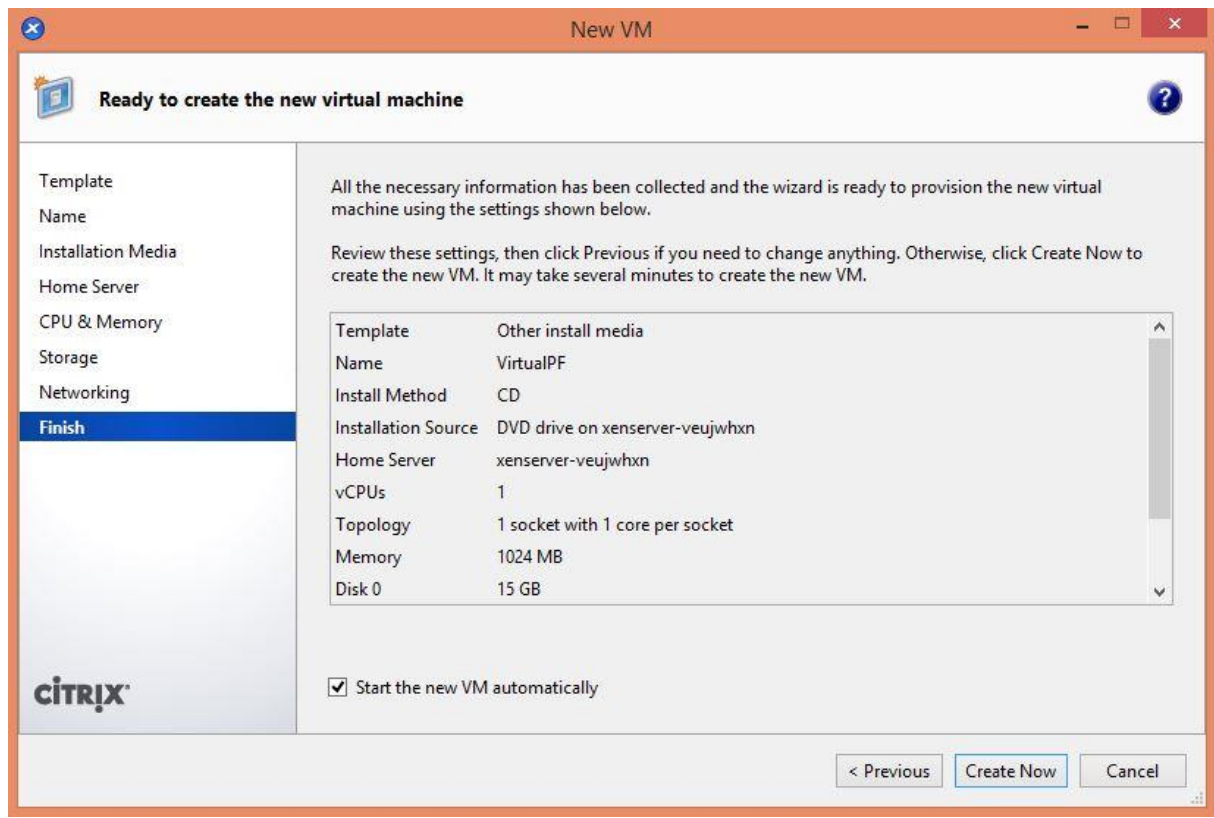
< Previous

Next >

Cancel

32





Résultat :



VirtualPF is now rebooting

After the reboot is complete, Set up interfaces and IP addresses via console. Afterwards the web GUI will be accessible.

You might need to acknowledge the HTTPS certificate if your browser reports it as untrusted. This is normal as a self-signed certificate is used by default.

DEFAULT Username: admin
DEFAULT Password: virtualpf

Installation complete
Press [Enter] to reboot...
Remove VirtualPF installer ISO after shutdown...

VLAN Capable interfaces:

No VLAN capable interfaces detected.

If you do not know the names of your interfaces, you may choose to use auto-detection. In that case, disconnect all interfaces now before hitting 'a' to initiate auto detection.

Enter the WAN interface name or 'a' for auto-detection: xn0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(or nothing if finished): xn1

Enter the Optional 1 interface name or 'a' for auto-detection
(or nothing if finished):

The interfaces will be assigned as follows:

WAN -> xn0
LAN -> xn1

Do you want to proceed [y/n]?


```
***** Welcome to VirtualPF TEFLON 1.0 (amd64) on VirtualPF *****

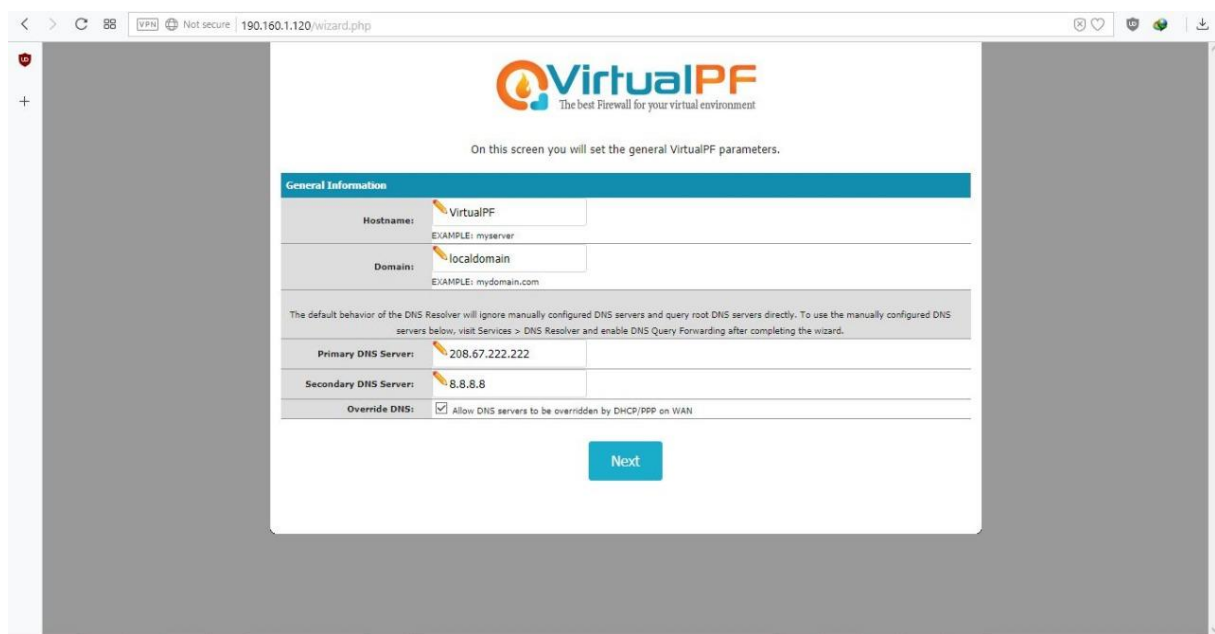
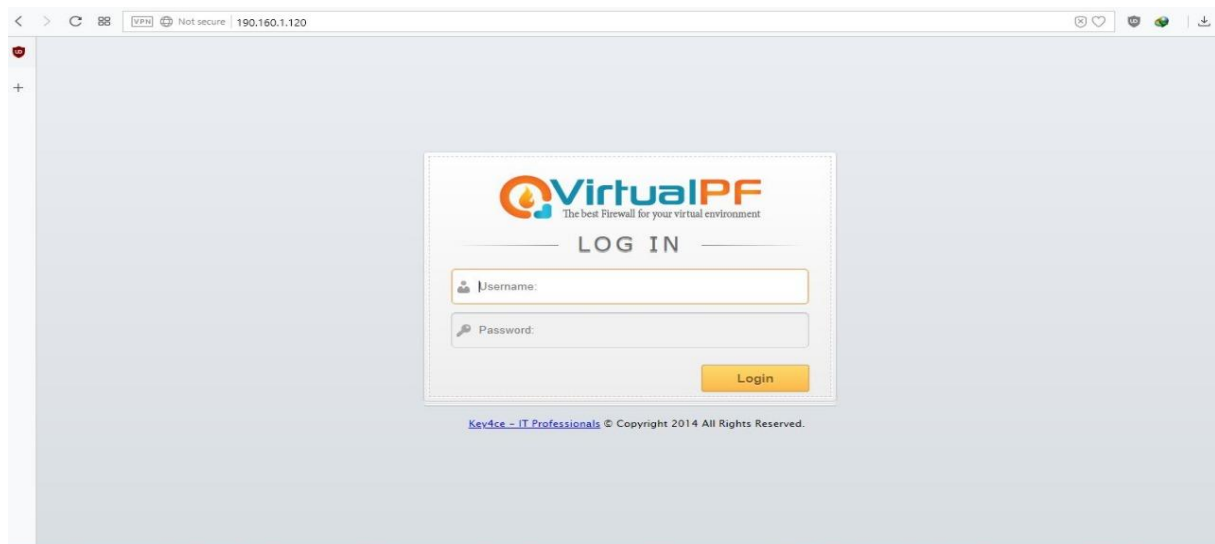
|| Citrix Xen host detected! ||
||-----||
|| support@virtualpf.com ||
|| www.virtualpf.com ||
||-----||

WAN (wan) -> xn0 ->
LAN (lan) -> xn1 -> v4/DHCP4: 190.160.1.120/24

0) Logout (SSH only)
1) Assign Interfaces
2) Set interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host

8) Shell
9) pfTop
10) Filter Logs
11) Restart webConfigurator
12) VirtualPF Developer Shell
13) Upgrade from console
14) Enable Secure Shell (sshd)
15) Restore recent configuration
16) Restart PHP-FPM

Enter an option: █
```



VirtualPF
The best Firewall for your virtual environment

On this screen we will configure the Wide Area Network information.

Configure WAN Interface

SelectedType: DHCP

General configuration

MAC Address:
This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections). Enter a MAC address in the following format: XX:XX:XX:XX:XX:XX or leave blank.

MTU:
Set the MTU of the WAN interface. If you leave this field blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.

MSS:
If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If you leave this field blank, an MSS of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed. This should match the above MTU value in most all cases.

Static IP Configuration

IP Address: /

Upstream Gateway:

VirtualPF
The best Firewall for your virtual environment

System Firewall Services Status Diagnostics Help

Status: Dashboard

Add Widget Add column Delete column

System Information

Name	VirtualPF.localdomain
Version	TEFLOW 1.0 (amd64) built on Fri Jan 30 08:12:14 CET 2015 FreeBSD 10.1-RELEASE-p3
Platform	VirtualPF
CPU Type	Intel(R) Core(TM) i3 CPU M 350 @ 2.27GHz
Uptime	00 Hour 09 Minutes 23 Seconds
Current date/time	Thu May 23 7:56:48 UTC 2019
DNS server(s)	
Last config change	Thu May 23 7:54:38 UTC 2019
State table size	0% (73/98000) Show states
MBUF Usage	1% (256/26564)
Load average	0.07, 0.18, 0.12
CPU usage	0%
Memory usage	

Interfaces

WAN (DHCP)	manual
LAN (DHCP)	190.160.1.120

Carp Status
No CARP Interfaces Defined. [Click here to configure CARP.](#)

Traffic Graphs

Current WAN Traffic
In: 0 Kbps Out: 0 Kbps
Switch to bytes AutoScale (up) Graph shows last 1200 seconds

Current LAN Traffic
In: 6 Kbps Out: 11 Kbps
Switch to bytes AutoScale (up) Graph shows last 1200 seconds

Gateways

Name	RTT	Loss	Status
WAN_DHCP	~	~	Unknown
LAN_DHCP	~	~	Unknown
LAN_DHCP6	~	~	Unknown

Firewall Logs

Act	Time	IF	Source	Destination
✓	May 23 07:50	WAN	0.0.0.0	255.255.255.255:87
✓	May 23 07:50	LAN	fe80::74b8:8467...	ff02::1:3:63b5
✓	May 23 07:50	LAN	fe80::74b8:8467...	ff02::1:3:63b5
✓	May 23 07:50	WAN	0.0.0.0	255.255.255.255:87
✓	May 23 07:50	WAN	0.0.0.0	255.255.255.255:87
✓	May 23 07:50	WAN	0.0.0.0	255.255.255.255:87
✓	May 23 07:50	WAN	0.0.0.0	255.255.255.255:87
✓	May 23 07:49	WAN	0.0.0.0	255.255.255.255:87

4. Conclusion

La virtualisation permet d'assurer une très grande souplesse au niveau des ressources allouables à une solution ou à un client. L'indépendance des solutions matérielles et logicielles permet de donner toute la puissance requise à la bonne exécution du service.

De nombreuses nouvelles solutions pour aboutir aux problèmes de sécurité du cloud ont vu le jour ces derniers mois. La sécurité est en effet un des facteurs primordiaux pour la continuité du développement du cloud computing. C'est pourquoi les fournisseurs doivent garantir une sécurisation suffisante des données (intégrité et confidentialité).