

## SOMMAIRE:

### Plan

#### I-Installation de PROXMOX depuis l'ISO

- 1-Configuration du réseau
- 2-Création du Linux Bridge
- 3-Création d'un Linux bond

#### II-Création et utilisation d'une VM

- 1-Création de la VM proprement dite
- 2-Démarrage de la VM créée
- 3-Modification de réglages d'une VM
- 4-Ajout d'un disque à la VM
- 5-Cloner une VM
- 6-Migrer une VM
- 7-Créer un template
- 8-Création d'un conteneur
- 9-Sauvegarde d'une VM

#### A/Création d'un cluster

#### B/Stockage Ceph

#### C/Firewall Open Sense virtualisé

#### D/Activer et Configurer le pare-feu (Firewall) sous Proxmox

#### E/Quelques commandes utiles pour PROXMOX

#### F/Comparaison: PROXMOX vs VMware

# PROXMOX

## Installation depuis l'ISO

Voici l'écran de démarrage :



Après avoir démarré, on a le premier écran d'installation suivant :



**END USER LICENSE AGREEMENT (EULA)**

END USER LICENSE AGREEMENT (EULA) FOR PROXMOX VIRTUAL ENVIRONMENT (PROXMOX VE)

By using Proxmox VE software you agree that you accept this EULA, and that you have read and understand the terms and conditions. This also applies for individuals acting on behalf of entities. This EULA does not provide any rights to Support Subscriptions Services as software maintenance, updates and support. Please review the Support Subscriptions Agreements for these terms and conditions. The EULA applies to any version of Proxmox VE and any related update source code and structure (the "Programs"), regardless of the delivery mechanism.

1. License. Proxmox Server Solutions GmbH (Proxmox) grants to you a perpetual, worldwide license to the Programs pursuant to the GNU Affero General Public License V3. The license agreement for each component is located in the software component's source code and permits you to run, copy, modify, and redistribute the software component (certain debugging, testing, and other binary only components may be excluded from the exception of certain binary only firmware components and the Proxmox images (e.g. Proxmox logo). The license rights for the binary only firmware components are located within the components. This EULA pertains solely to the Programs and does not limit your rights under, or grant you rights that supersede, the license terms of any particular component.

2. Limited Warranty. The Programs and the components are provided and licensed "as is" without warranty of any kind, expressed or implied, including the implied warranties of merchantability, non-infringement or fitness for a particular purpose. Neither Proxmox nor its affiliates warrants that the functions contained in the Programs will meet your requirements or that the operation of the Programs will be entirely error free, appear or perform precisely as described in the accompanying documentation, or comply with regulatory requirements.

3. Limitation of Liability. To the maximum extent permitted under applicable law, under no

Next | Previous | I agree

Puis :

**Proxmox Virtual Environment (PVE)**

The Proxmox Installer automatically partitions your hard disk. It installs all required packages and makes the system bootable from the hard disk. All existing partitions and data will be lost.

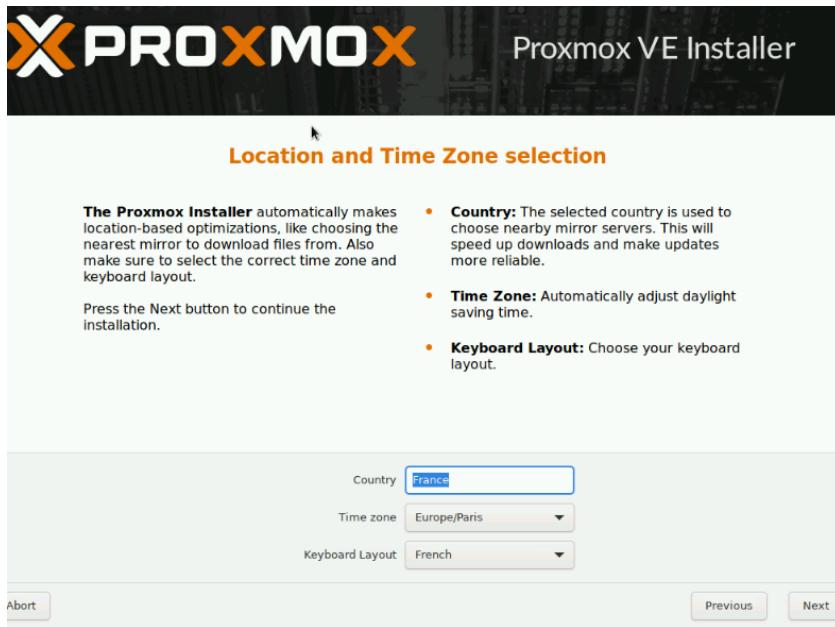
Press the Next button to continue the installation.

- **Please verify the installation target**  
The displayed hard disk will be used for the installation.  
Warning: All existing partitions and data will be lost.
- **Automatic hardware detection**  
The installer automatically configures your hardware.
- **Graphical user interface**  
Final configuration will be done on the graphical user interface, via a web browser.

Target Harddisk: /dev/sda (500.00GiB, PERC H730P Mini) ▾ Options

Abort | Previous | Next

Proxmox effacera d'éventuelles données présentes.



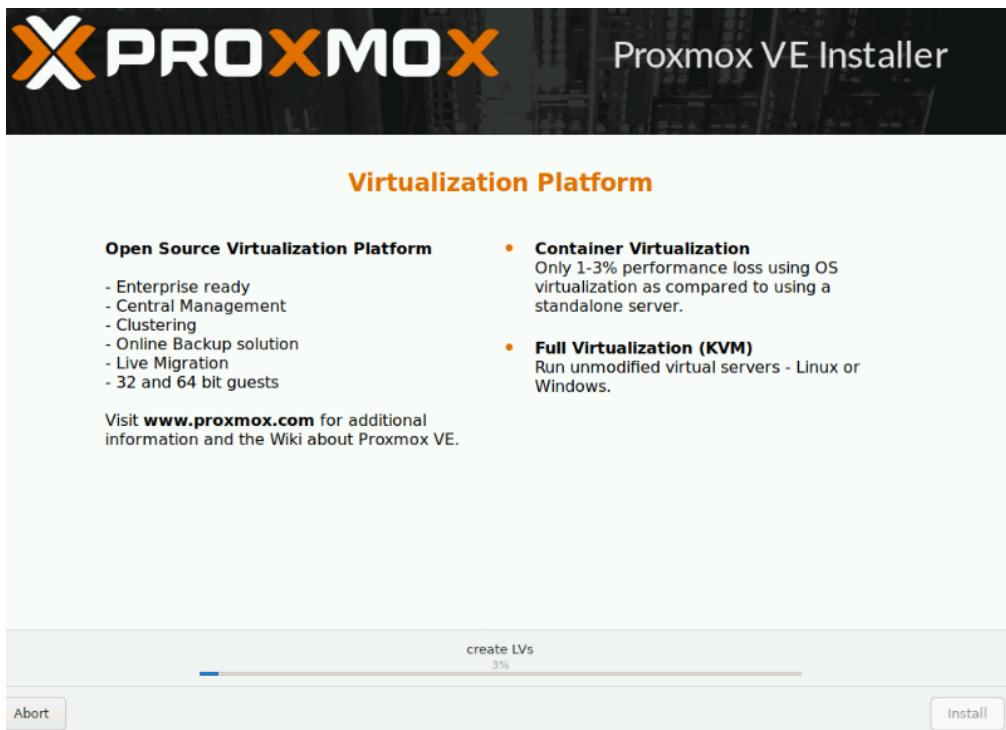
Il faudra ensuite renseigner le mot de passe et l'adresse mail de l'administrateur :



On peut ensuite personnaliser le nom de machine (FQDN) ainsi que les réglages réseau :



L'installation s'effectue ensuite automatiquement :



L'écran en fin d'installation vous aurez l'écran suivant vous rappelant l'URL d'accès à l'interface d'administration :

```

-----
[ Welcome to the Proxmox Virtual Environment. Please use your web browser to
  configure this server - connect to:
  https://10.202.19.12:8006/
-----]
[ pve8 login:

d_sas_fp.c:151:32
[   1.928277] index 1 is out of range for type 'MR_LD_SPAN'
[   1.928347] =====
[   1.928424] =====
[ Found volume group "ceph-af2b31e5-d5d5-4132-9621-a1db5abad
[ Found volume group "ceph-659a2726-0730-4e40-9c14-adc84f79b
[ Found volume group "ceph-4aad2f3b-a986-4aa6-bca4-67406b512
[ Found volume group "ceph-c204d49a-b2cf-45f4-b497-8568017ca
[ Found volume group "pve" using metadata type lvm2
[   1 logical volume(s) in volume group "ceph-af2b31e5-d5d5-41
[   0 logical volume(s) in volume group "ceph-659a2726-0730-4e
[   1 logical volume(s) in volume group "ceph-4aad2f3b-a986-4a
[   0 logical volume(s) in volume group "ceph-c204d49a-b2cf-45
[   3 logical volume(s) in volume group "pve" now active
[   3.391389] sd 9:0:0:0: [sdal] No Caching mode page found
[   3.391653] sd 9:0:0:0: [sdal] Assuming drive cache: write
[ /dev/mapper/pve-root: clean, 49581/6291456 files, 1175614/25
[   4.668659] ACPI Error: No handler for Region ISYS1 (000
[   4.668901] ACPI Error: Region IPMI (ID=7) has no handler
[   4.669300] ACPI Error: Aborting method \_SB.PMIO._GHL du
[   4.669702] ACPI Error: Aborting method \_SB.PMIO._PMC du

```

## 1-Configuration du réseau dans PROXMOX

La gestion des cartes réseau se gère depuis système → réseau :

Name	Type	Active	Autostart	VLAN a...	Ports/Slaves	Bond Mode	CIDR	Gateway
eno1	Network Device	Yes	No	No				
eno2	Network Device	No	No	No				
enp2s0f0np0	Network Device	No	No	No				
enp2s0f1np1	Network Device	No	No	No				
vmb0	Linux Bridge	Yes	Yes	No	eno1		10.202.19.10/16	10.202.255.254

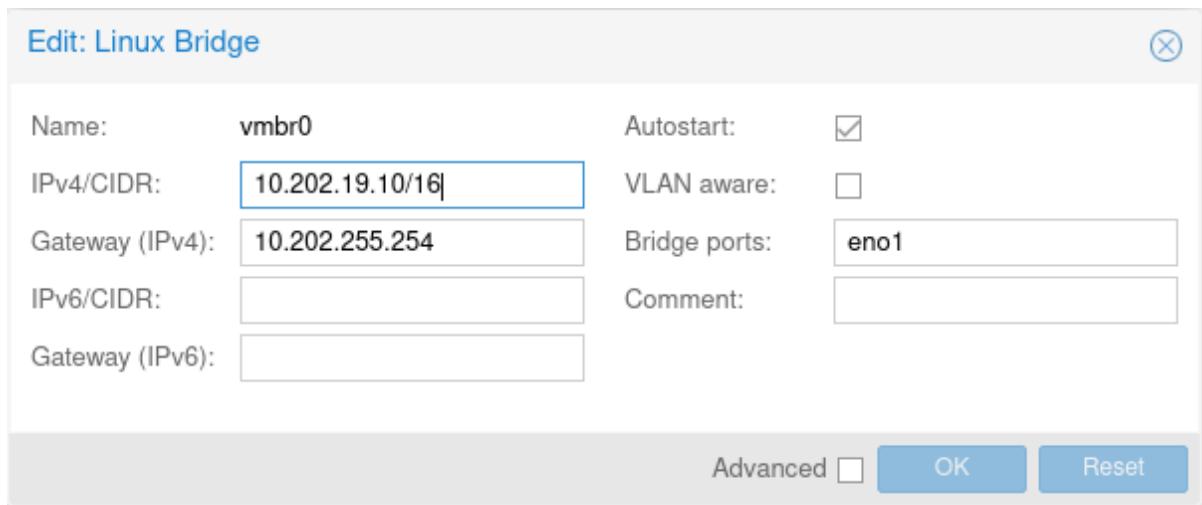
Pour pouvoir utiliser le réseau avec une VM, il faudra créer un Bridge ou utiliser un Bond.

Le Bridge est une carte virtuelle permettant la création d'un pont entre une carte virtuelle, utilisée par une ou plusieurs VM et une carte réelle. En cas de présence de plusieurs cartes réseau physiques, certaines VM pourront utiliser une carte précise pendant que d'autres VM pourront utiliser une autre carte.

Si l'installation de Proxmox s'est faite depuis le CD, l'installation aura automatiquement créé un bridge. Sinon il faudra créer un Linux Bridge (ou un bond).

## 2-Création du Linux Bridge

Pour créer le bridge, il faudra cliquer sur « créer » et sélectionner « Linux Bridge » dans le menu serveur → système → réseau.



Le bridge sera connecté sur la première interface réseau.

## 3-Création d'un Linux bond

Un Linux Bond va permettre de faire du bonding avec plusieurs cartes réseau. Ceci va agréger plusieurs cartes entre elles pour être vues comme un seul adaptateur réseau. On peut utiliser les modes suivants :

- **balance-rr** : transmission des paquets séquentiellement sur chaque carte. Ce mode permet la répartition de charge (load-balancing) et la tolérance de panne ;
- **active-backup** : un seul des liens est utilisé en même temps. En cas de panne, l'autre lien prend le relais. Ce mode permet la tolérance de pannes ;

The screenshot shows the Monitrix interface with the following details:

- Server View:** Datacenter (MonCluster) - serveur1
- Node 'serveur1' Overview:**
  - Search:** Create, Revert, Edit, Remove, Apply Configuration
  - Summary:** Shows basic information about the node.
  - Notes:**
  - Shell:**
  - System:**
    - Network:** This is the selected tab, highlighted in blue. It lists network interfaces:
 

Name	Type	Active	Autostart	VLAN a...	Ports/Slaves	Bond Mode	CIDR	Gateway	Comm...
eno1	Network Device	Yes	No	No					
eno2	Network Device	No	No	No					
enp2s0f0np0	Network Device	No	No	No					
enp2s0f1np1	Network Device	No	No	No					
<b>vmb0</b>	Linux Bridge	Yes	Yes	No	eno1		10.202.19.10/16	10.202.255.254	
    - Certificates:**
    - DNS:**

## Création et utilisation d'une VM

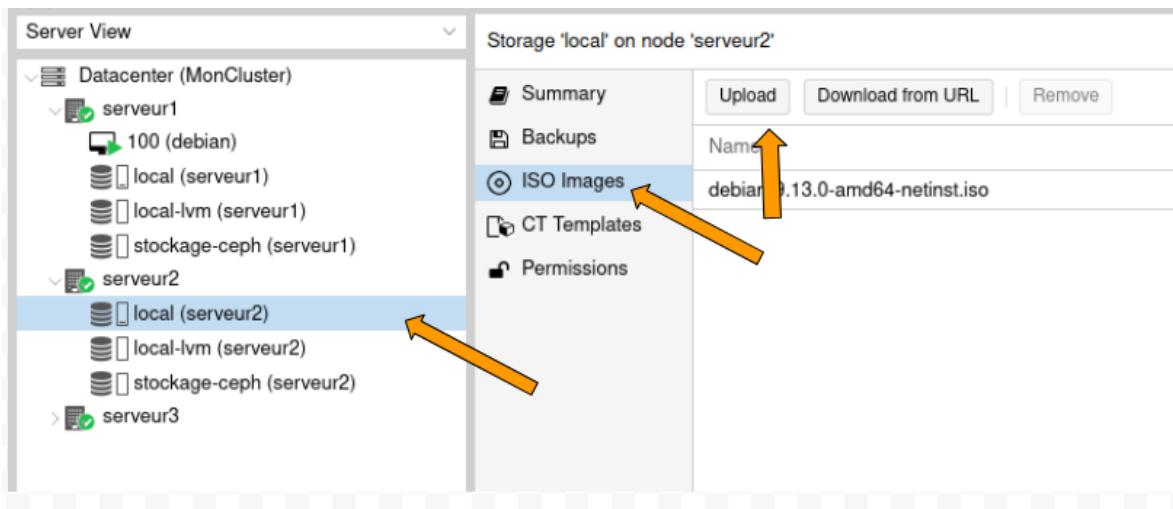
Avant de créer une VM, nous allons commencer par uploader un fichier ISO qui nous permettra de procéder à l'installation de notre OS virtualisé depuis un média d'installation.

Si nous cliquons sur l'onglet « Stockage » de notre datacenter, nous verrons un stockage local(serveur1), et un stockage local-lvm(serveur1).

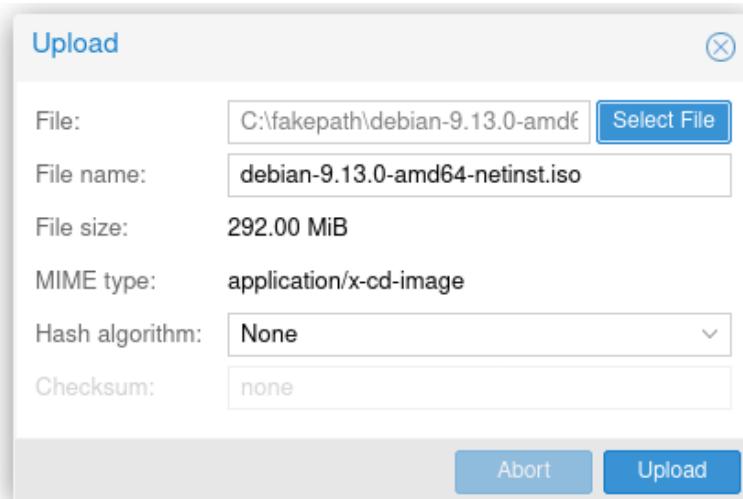
The screenshot shows the Monitrix interface with the following details:

- Server View:** Datacenter (MonCluster) - serveur1, serveur2, serveur3
- Storage 'local' on node 'serveur2' Overview:**
  - Summary:** This is the selected tab, highlighted in blue.
  - Backups**
  - ISO Images**
  - CT Templates**
  - Permissions**
- Status:** Enabled, Active, Content, Type, Usage
- Usage:** A bar chart showing disk usage from 80 G to 120 G. The bar is filled with a green gradient.

Pour pouvoir uploader un ISO, il faut se rendre depuis le menu de gauche dans datacenter → serveur1 → le stockage concerné, puis contenu, et enfin cliquer sur « uploader » :



Une boîte de dialogue vous demandera de sélectionner le fichier (soit fichier ISO, soit fichier de conteneur).



Si on va dans le stockage local-lvm, les boutons upload et templates seront grisés, car vous ne pouvez pas stocker d'ISO ou templates de conteneurs dans un volume LVM.

Les données sont stockées dans `/var/lib/vz/template/iso` pour les fichiers ISO, et dans `/var/lib/vz/template/cache` pour les templates de conteneurs ou dans les dossiers équivalents du magasin de données.

L'ISO sera alors disponible et visible.

Task viewer: Copy data

Output Status

Stop

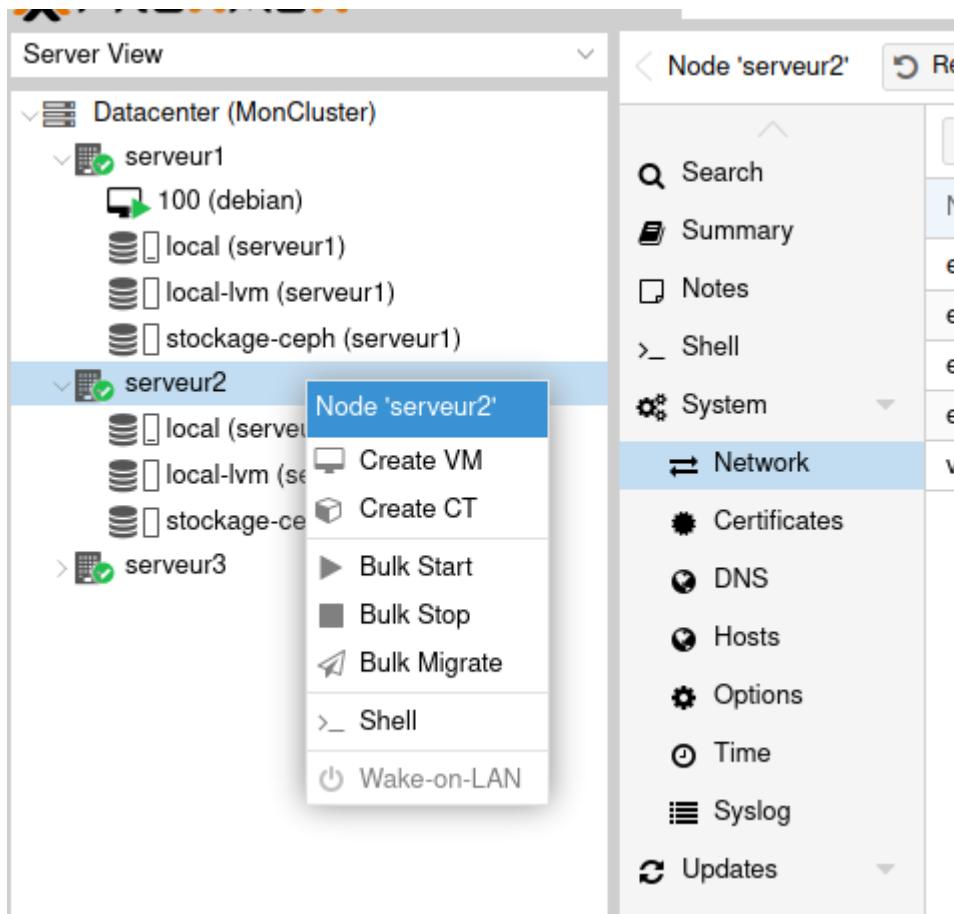
```
starting file import from: /var/tmp/pveupload-19d7e87d9df0b2a93f4033313a64a181
target node: serveur2
target file: /var/lib/vz/template/iso/debian-9.13.0-amd64-netinst.iso
file size is: 306184192
command: /usr/bin/scp -o BatchMode=yes -p -- /var/tmp/pveupload-19d7e87d9df0b2a93f4033313a64a181 [10.202.19.11]:/var/lib/vz/template/iso/deb
finished file import successfully
TASK OK
```

The screenshot shows the Proxmox VE interface. On the left, the 'Server View' tree shows three nodes: 'Datacenter (MonCluster)', 'serveur1', and 'serveur2'. 'serveur2' is expanded, showing its storage volumes: '100 (debian)', 'local (serveur1)', 'local-lvm (serveur1)', and 'stockage-ceph (serveur1)'. The 'Storage' tab for 'serveur2' is selected, displaying the 'ISO Images' section. An ISO image named 'debian-9.13.0-amd64-netinst.iso' is listed. There are tabs for 'Summary', 'Backups', 'CT Templates', and 'Permissions'.

## 1-Création de la VM proprement dite

Nous pouvons ensuite passer à la création de notre VM proprement dite en cliquant sur « Créer VM » dans la barre en haut ou via le bouton droit sur le nom de votre serveur à gauche.





Depuis la fenêtre de création de VM, sur le premier écran, nous pourrons choisir le serveur s'il y en a plusieurs, dans notre cas serveur2. Il restera à renseigner le nom de la VM :

Create: Virtual Machine

General OS System Disks CPU Memory Network Confirm

Node: serveur2 Resource Pool:   
VM ID: 101  
Name: vm.ndeye

Start at boot:  Start/Shutdown order: any  
Startup delay: default  
Shutdown timeout: default

Help Advanced Back Next

Cocher l'écran « Advanced », nous permettra de cocher démarrer au boot. Cette option permet de démarrer automatiquement la VM si l'hôte est redémarré.

Create: Virtual Machine

General OS System Disks CPU Memory Network Confirm

Node: serveur2 Resource Pool:   
VM ID: 101  
Name: vm.ndeye

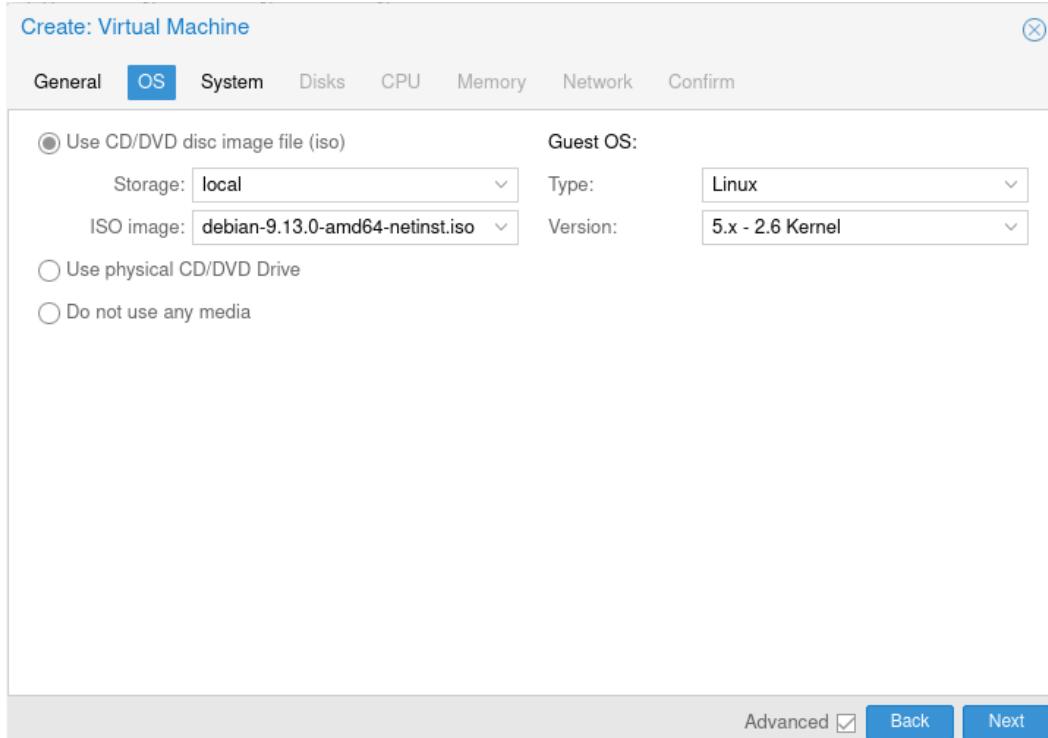
Start at boot:  Start/Shutdown order: any  
Startup delay: default  
Shutdown timeout: default

Help Advanced Back Next

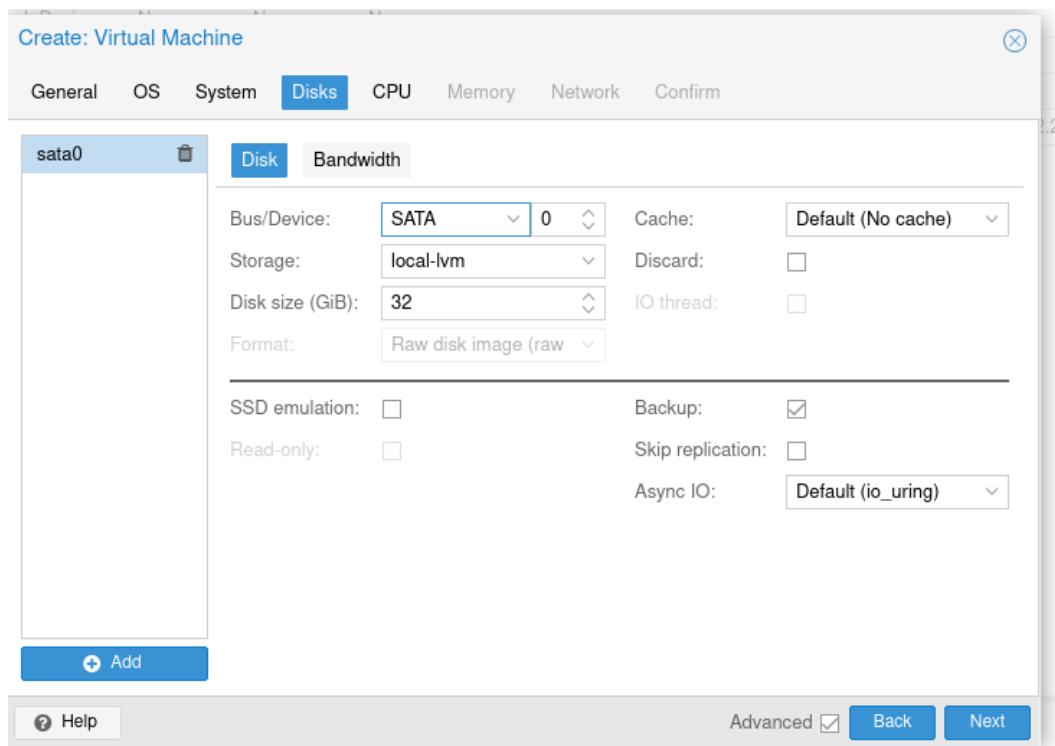


Le second écran demande :

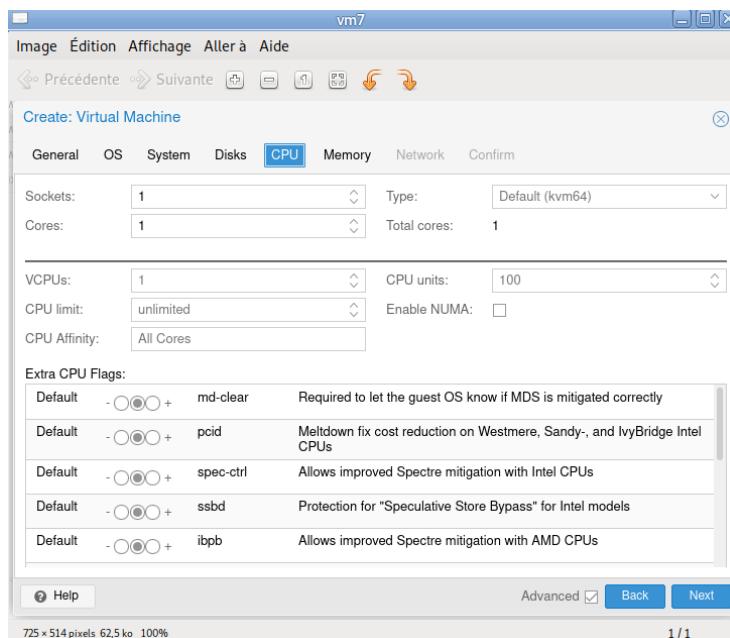
- une image disque : il nous faudra sélectionner l'ISO et avant l'espace de stockage (local ou autre) ;
- le type d'OS : choix entre Linux/Windows/Solaris/Other.



Sur l'écran suivant, nous allons créer un disque virtuel. Par défaut, celui-ci sera en SCSI , on peut utiliser un disque SATA, IDE, ou VirtIO :



On peut ensuite effectuer les réglages CPU (nombre de cœurs, socket, son type)



L'écran suivant permettra de choisir la taille mémoire :

Create: Virtual Machine

General OS System Disks CPU Memory Network Confirm

Memory (MiB):  ⌂

Minimum memory (MiB):  ⌂

Shares:  ⌂

Ballooning Device:

Help Advanced  Back Next

L'écran suivant concerne les réglages réseau :

Create: Virtual Machine

General OS System Disks CPU Memory Network Confirm

No network device

Bridge:  Model:

VLAN Tag:  MAC address:

Firewall:

---

Disconnect:  Data limit (MB/s):

Seul le mode pont est disponible.

Ensuite l'écran récapitulatif de la VM.

Create: Virtual Machine (X)

General OS System Disks CPU Memory Network Confirm

Key ↑	Value
cores	1
ide2	local:iso/debian-9.13.0-amd64-netinst.iso,media=cdrom
memory	512
name	vm.ndeye
net0	virtio,bridge=vmbr0,firewall=1
nodename	serveur2
numa	0
ostype	I26
sata0	local-lvm:32
scsihw	virtio-scsi-single
sockets	1
vmid	101

Start after created

Advanced  Back Finish

Une fois la VM créée, elle apparaîtra sur la partie gauche, et son tableau de bord dans la partie droite en la sélectionnant :

The screenshot shows the Proxmox Virtual Environment interface. On the left, the 'Vue Serveur' sidebar is open, showing a tree structure of Datacenter, server1, and server2. Under server1, there are several storage volumes like local (srv1), local-lvm (srv1), and stockage-ceph (srv1). Under server2, there are VMs: 100 (debian), 102 (test), local (serveur1), local-lvm (serveur1), and stockage-ceph (serveur1). A specific VM, '100 (testVM)', is selected and highlighted in blue. The main panel displays the 'Résumé' (Summary) tab for this VM. It shows the VM name 'testVM', its status as 'stopped', and its node as 'srv1'. Resource usage statistics are also provided: CPU utilization at 0.00% of 1 CPU(s), memory utilization at 0.00% (0 B of 512.00 MiB), and disk size at 32.00 GiB. Below the summary, there's a 'Notes' section which is currently empty. At the bottom, there are tabs for 'Tâches' (Tasks) and 'Journaux du cluster' (Cluster logs), with 'Tâches' being the active tab.

L'onglet options permettra notamment de :

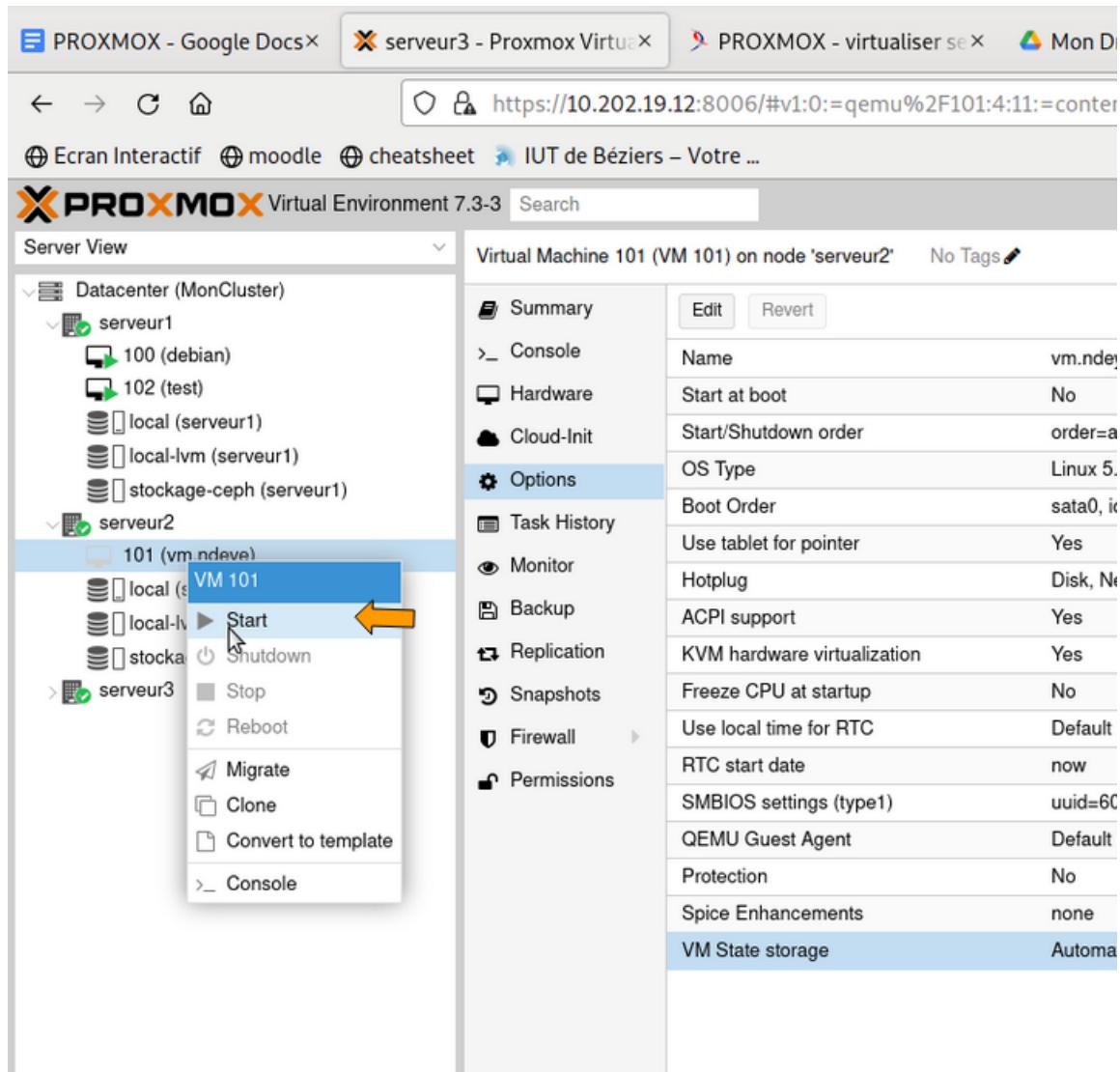
- démarrer la VM au démarrage de l'hyperviseur ;
- changer l'ordre des périphériques de boot ;
- gérer la prise en compte de l'heure.

The screenshot shows the Proxmox Virtual Environment interface with the 'Virtual Machine 101 (VM 101) on node 'serveur2'' selected in the left sidebar. The main panel shows the 'Options' tab for this VM. The configuration settings listed include:

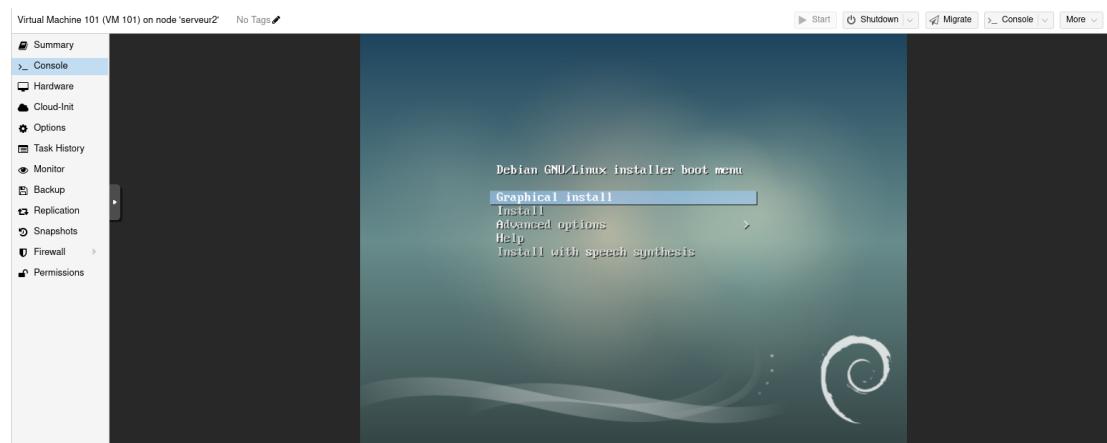
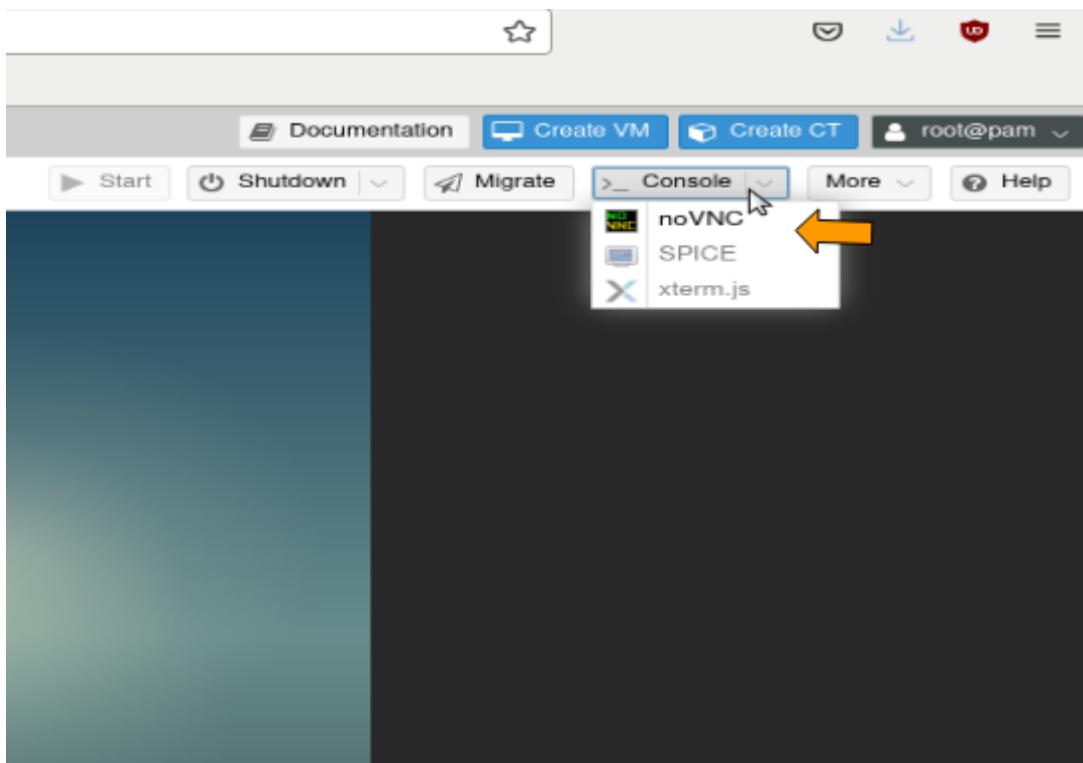
Name	vm.ndeye
Start at boot	No
Start/Shutdown order	order=any
OS Type	Linux 5.x - 2.6 Kernel
Boot Order	sata0, ide2, net0
Use tablet for pointer	Yes
Hotplug	Disk, Network, USB
ACPI support	Yes
KVM hardware virtualization	Yes
Freeze CPU at startup	No
Use local time for RTC	Default (Enabled for Windows)
RTC start date	now
SMBIOS settings (type1)	uuid=60e758b3-35d2-4e6e-8bc4-2fda31201b
QEMU Guest Agent	Default (Disabled)
Protection	No

## 2-Démarrage de la VM créée

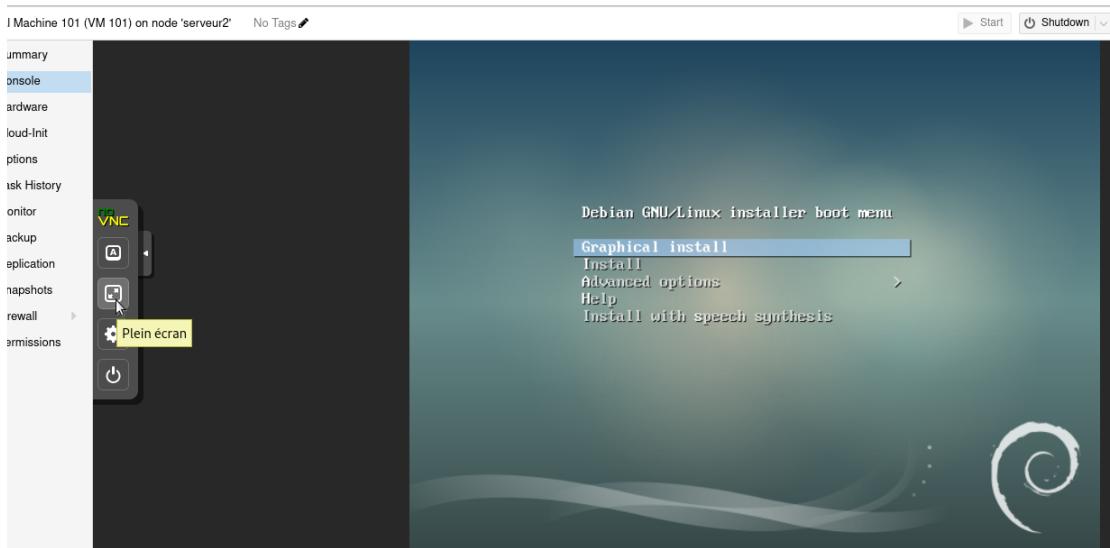
Pour démarrer celle-ci, il suffit de se placer sur la VM apparaissant à gauche, et de cliquer bouton de droite démarrer :



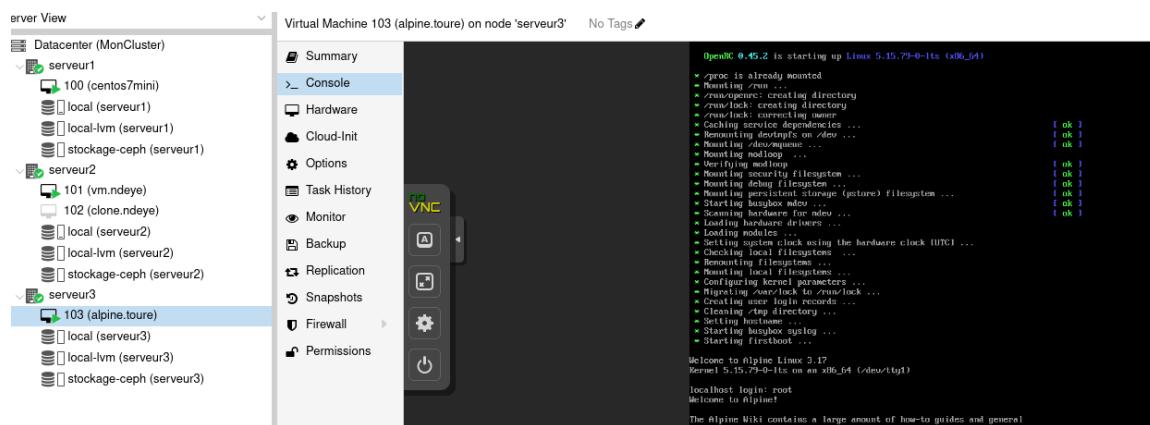
Une fois celle-ci démarrée, on pourra voir la console en cliquant « console », ou ouvrir une fenêtre de console en allant dans le menu console → NoVNC (NoVNC est un client et une bibliothèque VNC en JavaScript) :



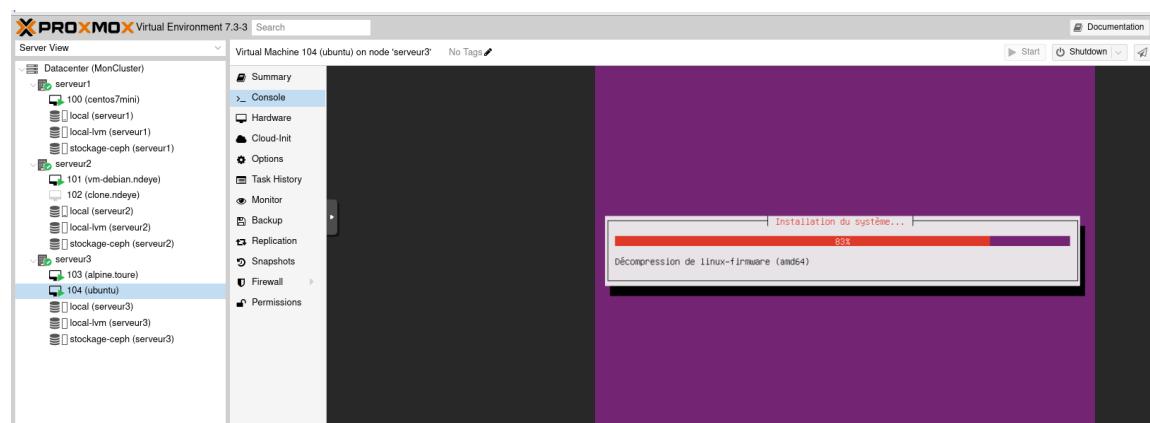
On peut passer en plein écran en cliquant sur la flèche dans la fenêtre NoVNC :



J'en ai créé une autre qui s'appelle: alpine.toure



Une Vm Ubuntu aussi



J'arrive à faire un ping de 8.8.8.8

```

root@104 (apprme.tware):
[ 104 (ubuntu)
local (serveur3)
local-lvm (serveur3)
stockage-ceph (serveur3)

  Firewall
  Permissions

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/<package>/copyright.

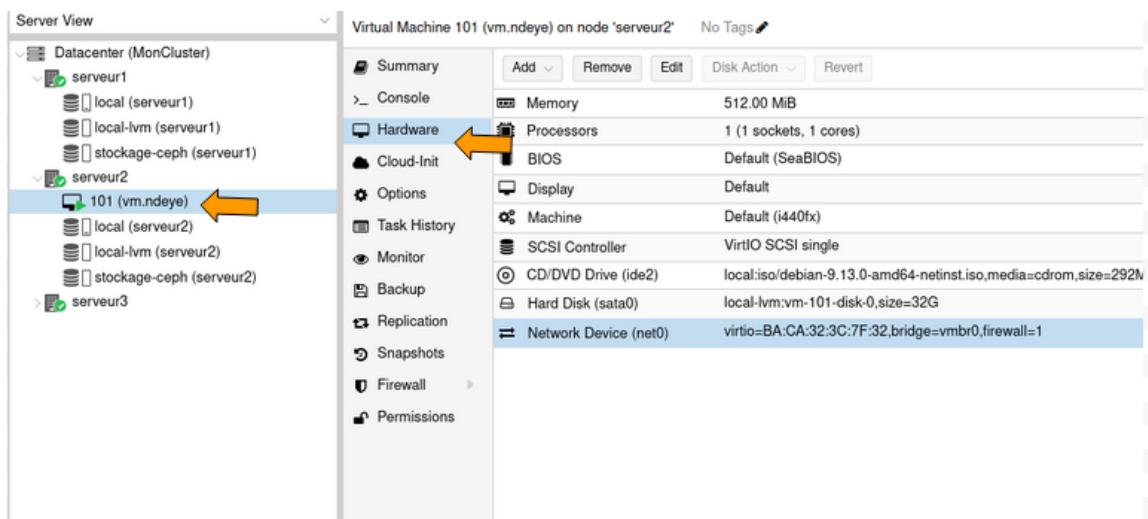
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

test@ubuntu:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 octets de 8.8.8.8 : icmp_seq=1 ttl=110 temps=5.41 ns
64 octets de 8.8.8.8 : icmp_seq=2 ttl=110 temps=5.50 ns
64 octets de 8.8.8.8 : icmp_seq=3 ttl=110 temps=5.82 ns
...
4 paquets transmis, 3 reçus, 25 % paquets perdus, temps 3017 ms
rtt min/moy/max/ndev = 5.406/5.600/5.815/0.166 ns
test@ubuntu:~$
```

### 3-Modification de réglages d'une VM

Pour changer les réglages d'une VM, il nous faudra cliquer dessus dans la partie gauche, puis sélectionner matériel à droite :



Un double-clic sur l'élément à modifier donnera accès au réglage de celui-ci.

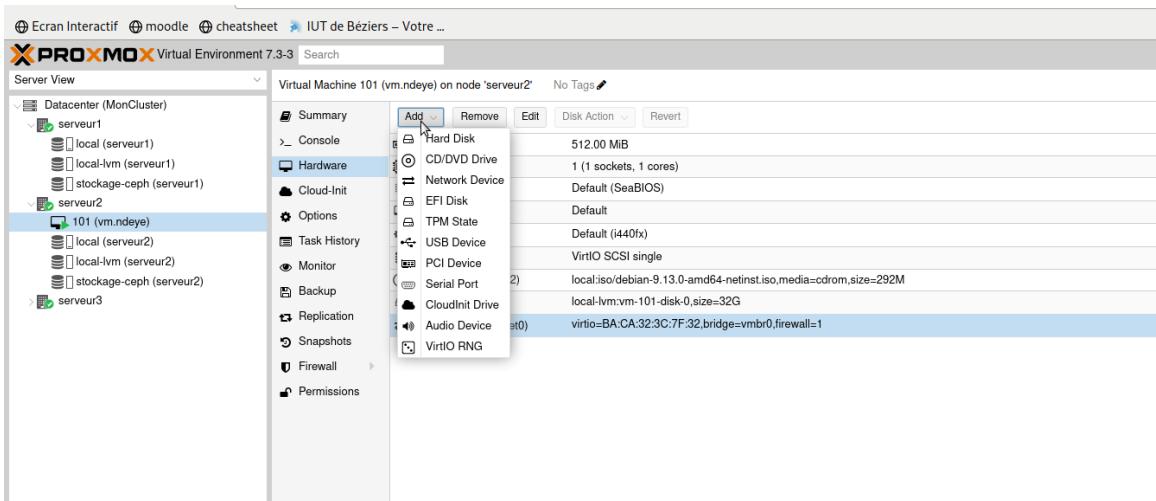
Exemple pour la carte réseau :

**Edit: Network Device**

Bridge:	vmbr0	Model:	VirtIO (paravirtualized)
VLAN Tag:	no VLAN	MAC address:	BA:CA:32:3C:7F:32
Firewall:	<input checked="" type="checkbox"/>		
Disconnect:	<input type="checkbox"/>	Rate limit (MB/s):	unlimited
MTU:	1500 (1 = bridge MTU)	Multiqueue:	

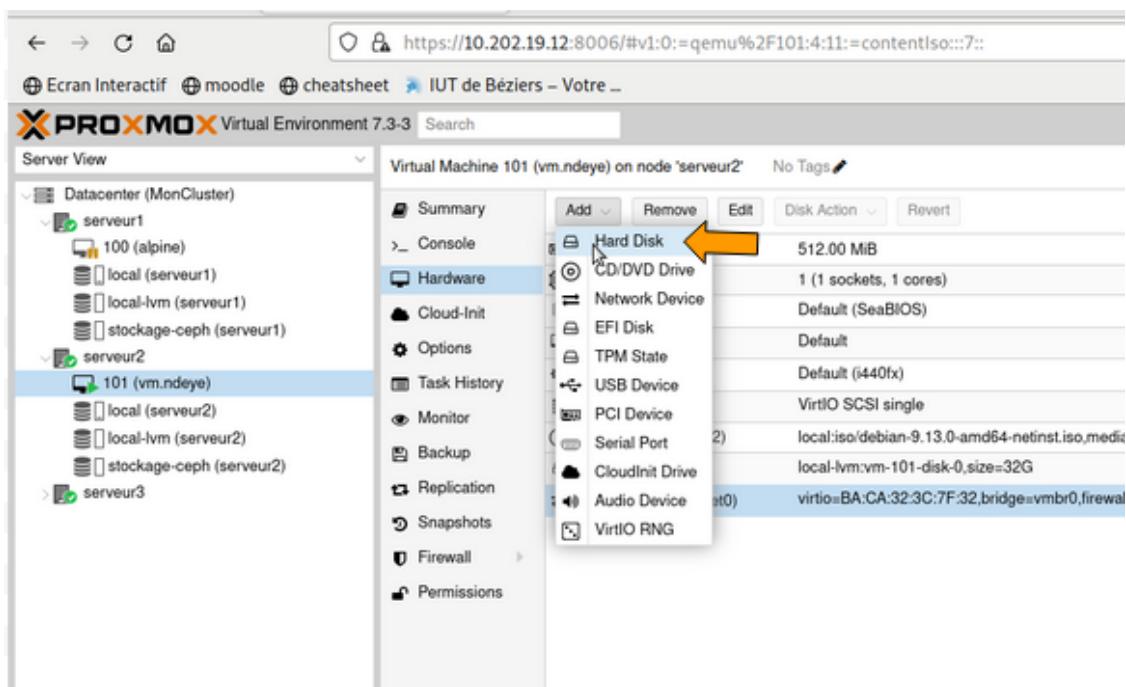
**Help** Advanced  **OK** **Reset**

Pour ajouter ou retirer un élément, cela se passe dans la ligne au-dessus des éléments de la VM :



#### 4-Ajout d'un disque à la VM

Pour ajouter un disque à la VM, il faudra aller dans le menu de la machine  
→ matériel :



On aura alors l'écran de création de disque comme déjà vu dans la partie création d'une VM :

### Add: Hard Disk

**Disk** Bandwidth

Bus/Device:	SCSI	Cache:	Default (No cache)
SCSI Controller:	VirtIO SCSI single	Discard:	<input type="checkbox"/>
Storage:	local-lvm	IO thread:	<input checked="" type="checkbox"/>
Disk size (GiB):	32		
Format:	Raw disk image (raw)		
SSD emulation:	<input type="checkbox"/>	Backup:	<input checked="" type="checkbox"/>
Read-only:	<input type="checkbox"/>	Skip replication:	<input type="checkbox"/>
	Async IO: Default (io_uring)		

**Help** Advanced  **Add**

On pourrait alors voir le disque supplémentaire dans l'onglet local-lvm du serveur :

The screenshot shows the Oracle VM Server interface. On the left, the navigation tree displays a Datacenter (MonCluster) containing several servers: serveur1, serveur2, and serveur3. Under serveur2, the VM 101 (vm.ndeye) is selected. The main pane shows the 'Summary' tab of the VM configuration. In the 'Hardware' section, under 'Disk Action', there is a list of disk configurations:

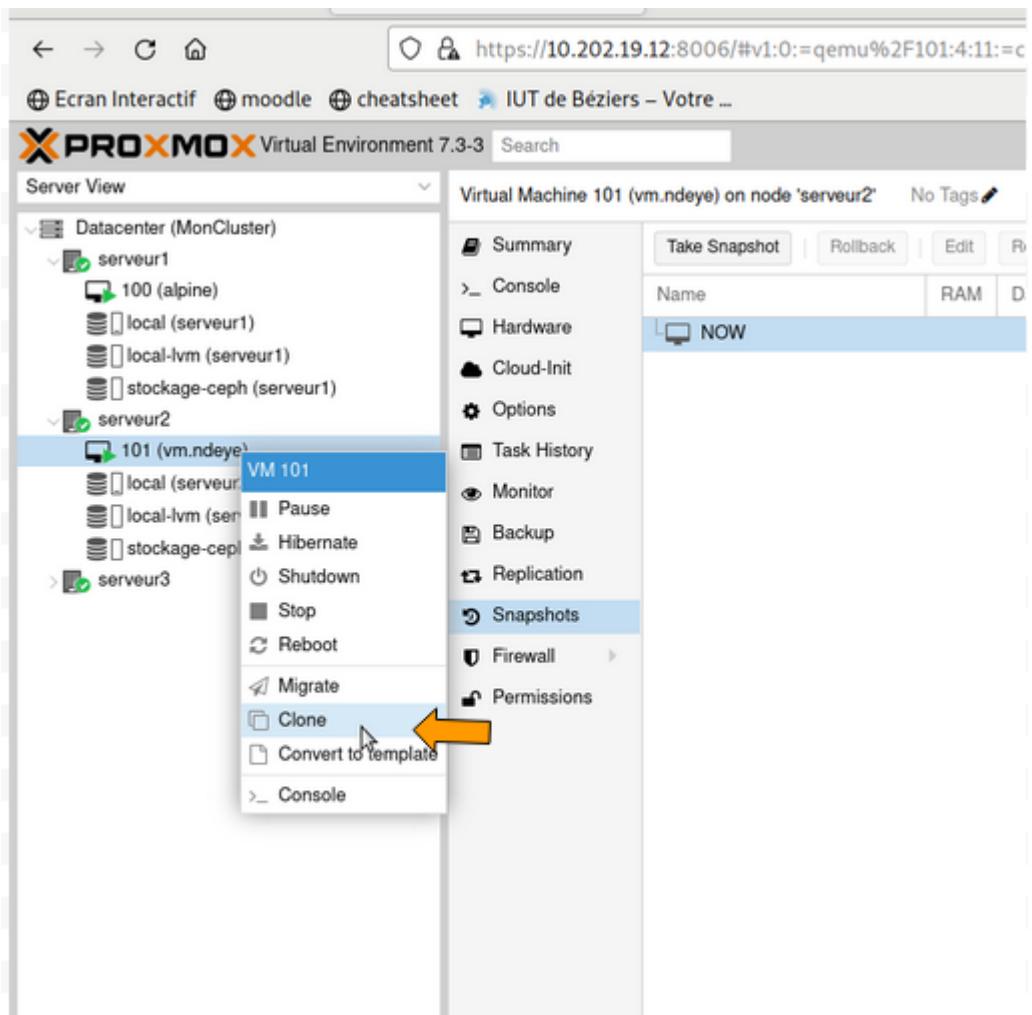
Device	Description
Memory	512.00 MiB
Processors	1 (1 sockets, 1 cores)
BIOS	Default (SeaBIOS)
Display	Default
Machine	Default (i440fx)
SCSI Controller	VirtIO SCSI single
CD/DVD Drive (ide2)	local:iso/debian-9.13.0-amd64-netinst.iso,media=cdrom,size=292M
Hard Disk (sata0)	local-lvm:vm-101-disk-0,size=32G
Hard Disk (scsi2)	local-lvm:vm-101-disk-1,size=32G
Network Device (net0)	virtio=BA:CA:32:3C:7F:32,bridge=vmb0,firewall=1

A yellow arrow points to the 'local-lvm:vm-101-disk-1' entry, indicating the newly added LVM disk.

## 5-Cloner une VM

Cloner une VM permet d'en faire une copie. Cette copie sera alors autonome par rapport à sa source. Celle-ci aura sa propre vie et les mêmes réglages que la VM source, du moins tant qu'on ne les change pas.

Pour cloner une VM, il faudra cliquer sur le bouton droit sur le nom de la VM :



On a ensuite l'écran suivant :

Clone VM 101

Target node:	serveur2	Target Storage:	Same as source
VM ID:	102	Format:	QEMU image format (qc)
Name:	clone.ndeye		
Resource Pool:			

**Help** **Clone**

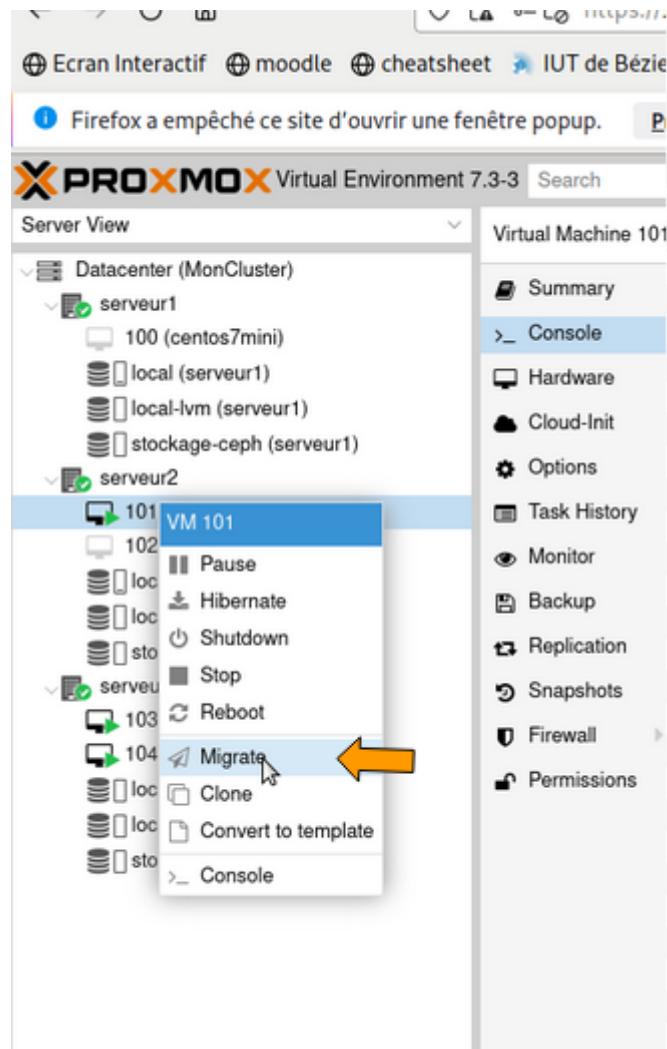
Il faudra choisir le stockage cible, le nom de la VM, et éventuellement le nœud s'il y a plusieurs hyperviseurs en cluster et que nous souhaitons effectuer la copie sur un autre nœud.



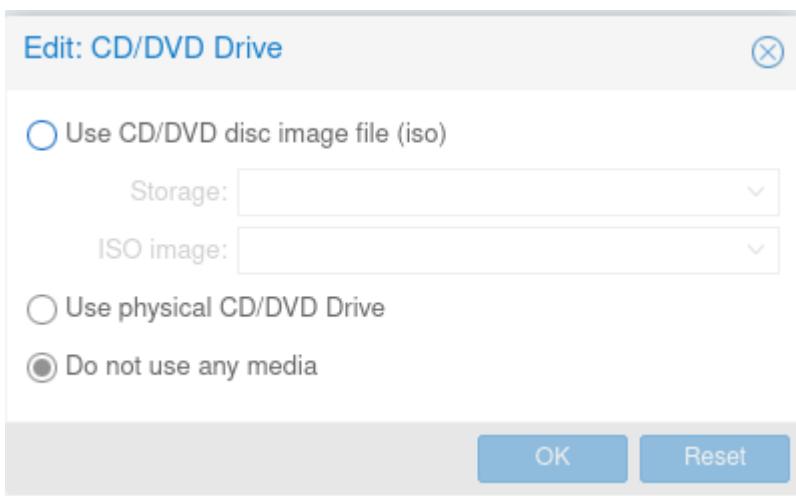
## 6-Migrer une VM

Migrer une VM consistera à cloner celle-ci vers un autre nœud (un autre hyperviseur du datacenter) en activant celui-ci et supprimant la VM du nœud source. Ceci peut se faire à chaud c'est-à-dire VM en activité.

Pour migrer une VM, il faudra cliquer bouton droite sur celle-ci, puis choisir « migration »



Avant ça, il faut le détacher du CD/DVD



Il nous restera à sélectionner le nœud de destination :

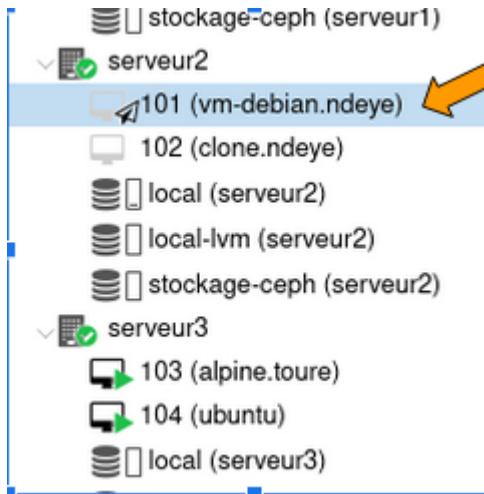
Node ↑	Memory usage	CPU usage
serveur1	2.1%	0.1% of 32 ...
serveur3	2.6 %	0.2% of 32 ...

Task viewer: VM 101 - Migrate (serveur2 ---> serveur3)

Output Status

Stop

```
2022-12-12 14:22:24 starting migration of VM 101 to node 'serveur3' (10.202.19.12)
2022-12-12 14:22:24 found local disk 'local-lvm:vm-101-disk-0' (in current VM config)
2022-12-12 14:22:24 found local disk 'local-lvm:vm-101-disk-1' (in current VM config)
2022-12-12 14:22:24 copying local disk images
2022-12-12 14:22:26 Logical volume "vm-101-disk-0" created.
```



J'ai pu constater une erreur de migration avec une VM liée à un ISO dans un espace local :

Task viewer: VM 101 - Migrate (serveur2 ---> serveur3)

Output	Status
<button>Stop</button>	
<pre>2022-12-12 14:22:24 starting migration of VM 101 to node 'serveur3' (10.202.19.12) 2022-12-12 14:22:24 found local disk 'local-lvm:vm-101-disk-0' (in current VM config) 2022-12-12 14:22:24 found local disk 'local-lvm:vm-101-disk-1' (in current VM config) 2022-12-12 14:22:24 copying local disk images 2022-12-12 14:22:26 Logical volume "vm-101-disk-0" created. send/receive failed, cleaning up snapshot(s)... 2022-12-12 14:25:33 ERROR: storage migration for 'local-lvm:vm-101-disk-0' to storage 'local-lvm' failed - command 'set -o pipefail &amp;&amp; pvesm export local-lvm:vm-101-disk-0' failed 2022-12-12 14:25:33 aborting phase 1 - cleanup resources 2022-12-12 14:25:33 ERROR: migration aborted (duration 00:03:09): storage migration for 'local-lvm:vm-101-disk-0' to storage 'local-lvm' failed - command 'set -o pipefail &amp;&amp; pvesm export local-lvm:vm-101-disk-0' failed TASK ERROR: migration aborted</pre>	<button>(X)</button>

Au bout d'un certain temps, le message « VM 101- Migration » apparut dans la liste des tâches,

## Task viewer: VM 101 - Migrate

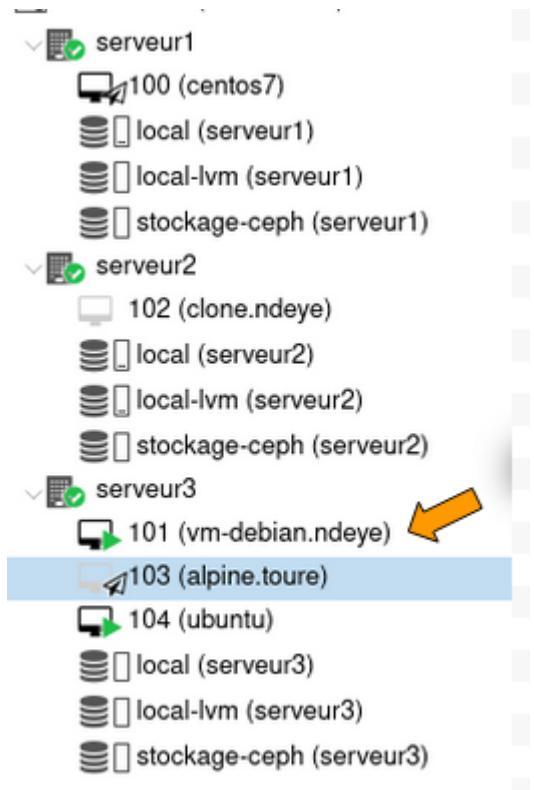
Output Status

Stop

```
2022-12-12 14:29:13 volume pve/vm-101-disk-0 already exists - importing with a different name
2022-12-12 14:29:13 Logical volume "vm-101-disk-1" created.
2022-12-12 14:34:08 524288+0 records in
2022-12-12 14:34:08 524288+0 records out
2022-12-12 14:34:08 34359738368 bytes (34 GB, 32 GiB) copied, 294.791 s, 117 MB/s
2022-12-12 14:34:09 36+1283269 records in
2022-12-12 14:34:09 36+1283269 records out
2022-12-12 14:34:09 34359738368 bytes (34 GB, 32 GiB) copied, 294.929 s, 117 MB/s
2022-12-12 14:34:09 successfully imported 'local-lvm:vm-101-disk-1'
2022-12-12 14:34:09 volume 'local-lvm:vm-101-disk-0' is 'local-lvm:vm-101-disk-1' on the target
2022-12-12 14:34:10 volume pve/vm-101-disk-1 already exists - importing with a different name
2022-12-12 14:34:10 Logical volume "vm-101-disk-2" created.
2022-12-12 14:39:05 524288+0 records in
2022-12-12 14:39:05 524288+0 records out
2022-12-12 14:39:05 34359738368 bytes (34 GB, 32 GiB) copied, 294.967 s, 116 MB/s
2022-12-12 14:39:05 33+2043231 records in
2022-12-12 14:39:05 33+2043231 records out
2022-12-12 14:39:05 34359738368 bytes (34 GB, 32 GiB) copied, 294.496 s, 117 MB/s
2022-12-12 14:39:05 successfully imported 'local-lvm:vm-101-disk-2'
2022-12-12 14:39:05 volume 'local-lvm:vm-101-disk-1' is 'local-lvm:vm-101-disk-2' on the target
Logical volume "vm-101-disk-0" successfully removed
Logical volume "vm-101-disk-1" successfully removed
2022-12-12 14:39:06 migration finished successfully (duration 00:09:54)
TASK OK
```

Dec 12 14:29:12	Dec 12 14:39:06	serveur2	root@pam	VM 101 - Migrate
Dec 12 14:28:21	Dec 12 14:28:27	serveur1	root@pam	VM/CT 100 - Console

On voit maintenant qu'il se trouve dans le serveur 3



La migration a duré 9 min

Task viewer: VM 101 - Migrate	
	Status
<a href="#">Stop</a>	
Status	stopped: OK
Task type	qmigrate
User name	root@pam
Node	serveur2
Process ID	1120924
Start Time	2022-12-12 14:29:12
End Time	2022-12-12 14:39:06
Duration	9m 54s
Unique task ID	UPID:serveur2:00111A9C:0199A751:63972CA8:qmigrate:101:root@pam

Il est également possible effectuer une migration en ligne de commande avec la commande qm:

```
qm migrate [id VM][destination] --online --with-local-disks
```

```
qm migrate 101 serveur3 --online --with-local-disks
```

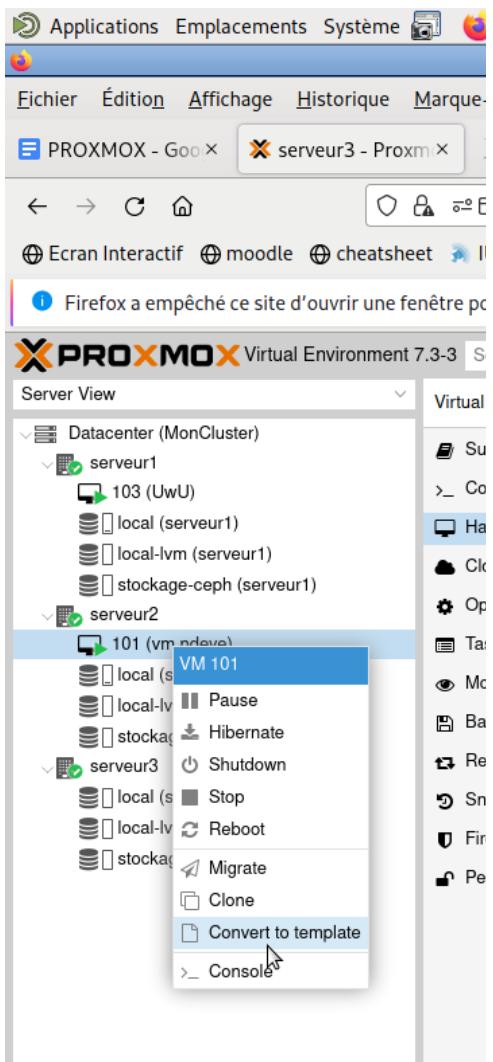
Les paramètres fournis dans l'exemple ci-dessus :

- 101 : id de la VM ;
- serveur3 : serveur de destination ;
- --online : permet la migration d'une VM active ;
- --with local-disks : permet de migrer également les disques locaux.

## 7-Créer un template

Un template, aussi appelé appliance, est une VM qui servira de modèle. Cela peut être utile pour préparer un modèle de VM qui sera ensuite dupliqué.

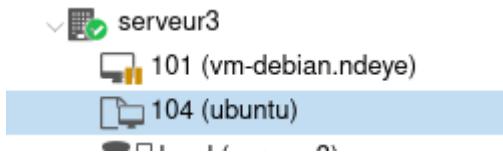
Pour ce faire, il faudra cliquer dessus via le bouton droit et sélectionnez convertir en template :



Une demande de confirmation est envoyé



La conversion d'une VM va changer son icône en icône .



Il ne s'agit pas de juste changer l'icône.

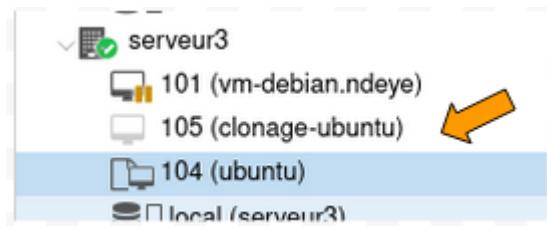
On voit une option supplémentaire intéressante :

Clone VM Template 104

Target node:	serveur3	Mode:	Linked Clone
VM ID:	105	Target Storage:	Same as source
Name:	clonage_ubuntu	Format:	QEMU image format (qc)
Resource Pool:		Clone	

On peut sélectionner deux modes :

- clonage lié : un snapshot est créé sur la VM source. La VM destination utilisera son propre snapshot dépendant du disque d'origine de la VM source. Les deux VM vont avoir leur propre existence, seront autonomes, mais la VM destination est dépendante de la VM source du fait que son disque est un snapshot de celui de la VM source ;
- clonage intégral : la VM est clonée intégralement.

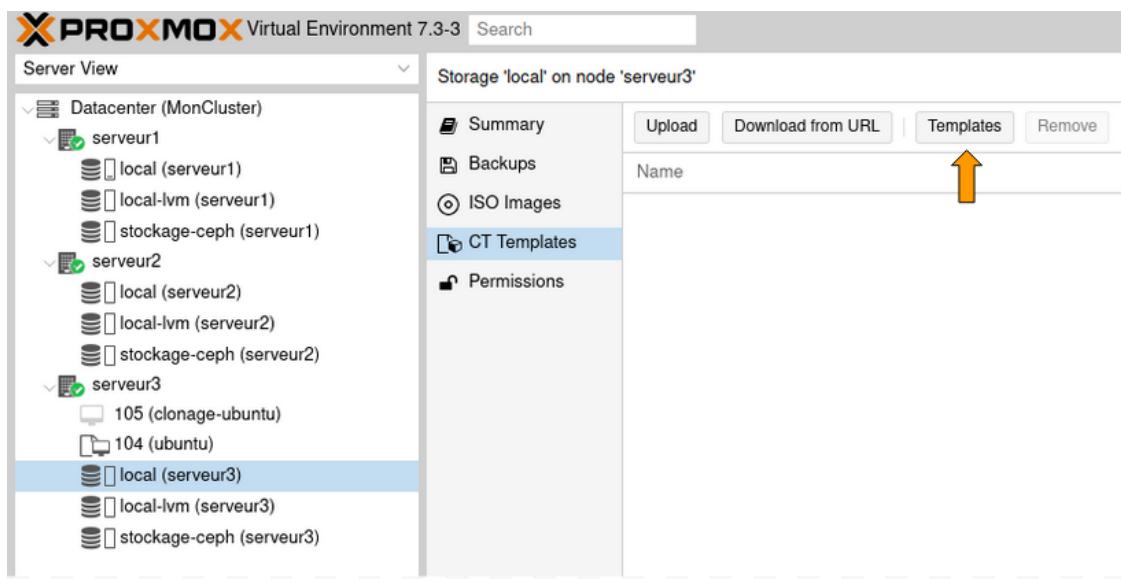


## 8-Création d'un conteneur

### Un template de conteneurs

Avant de pouvoir créer un conteneur, il faut un template qui servira de modèle.

On peut en récupérer en cliquant « template » en allant dans le serveur (serveur3 dans notre cas) → local → contenu :



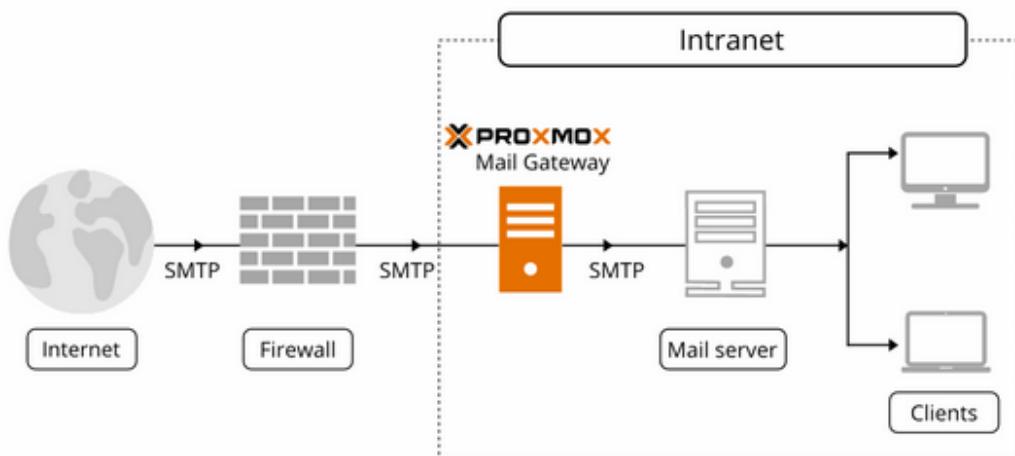
Les templates proposés sont divisés en deux sections :

- la section system ;
- la section mail.

Templates			
Type	Package	Version	Description
[+] Section: mail (2 Items)			
lxc	proxmox-mailgateway-7.0-standard	7.0-1	Proxmox Mailgateway 7.0
lxc	proxmox-mailgateway-6.4-standard	6.4-1	Proxmox Mailgateway 6.4
[+] Section: system (26 Items)			
lxc	fedora-37-default	20221119	LXC default image for fedora 37 (20221119)
lxc	debian-10-standard	10.7-1	Debian 10 Buster (standard)
lxc	centos-8-default	20201210	LXC default image for centos 8 (20201210)
lxc	debian-11-standard	11.3-1	Debian 11 Bullseye (standard)
lxc	alpine-3.14-default	20210623	LXC default image for alpine 3.14 (20210623)
lxc	archlinux-base	202211...	ArchLinux base image.
lxc	ubuntu-22.10-standard	22.10-1	Ubuntu 22.10 Kinetic (standard)
lxc	centos-9-stream-default	20221109	LXC default image for centos 9-stream (20221109)
lxc	opensuse-15.4-default	20221109	LXC default image for opensuse 15.4 (20221109)
lxc	fedora-35-default	20211111	LXC default image for fedora 35 (20211111)
lxc	centos-7-default	20190926	LXC default image for centos 7 (20190926)
lxc	rockylinux-8-default	20210929	LXC default image for rockylinux 8 (20210929)
lxc	opensuse-15.3-default	20210925	LXC default image for opensuse 15.3 (20210925)
lxc	fedora-36-default	20220622	LXC default image for fedora 36 (20220622)

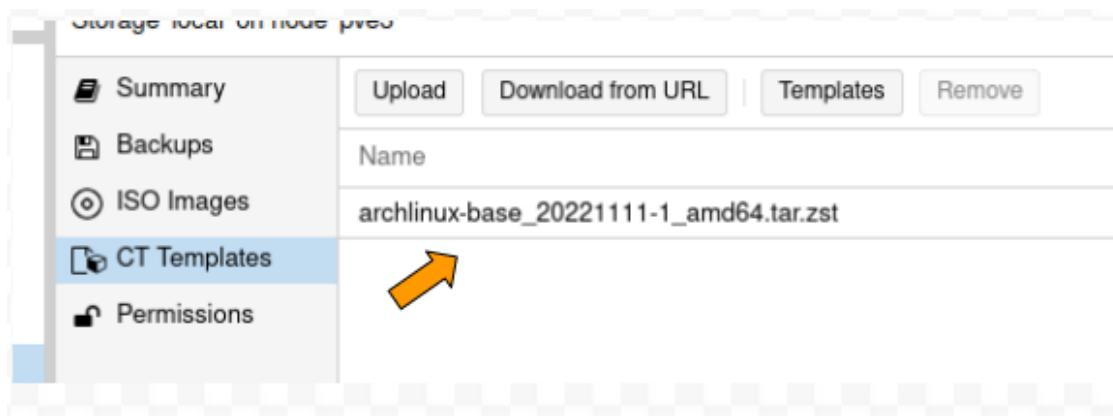
La section system contient des images telles que Centos6 7, Fedora28, Alpine 3.8.

La section mail contient des images telles que proxmox-mailgateway (pour analyser le contenu des mails, détecter les liens de phishing, les pièces jointes infectées et les virus) et d'autres versions, c'est-à-dire des templates tout faits prêts à utilisation.



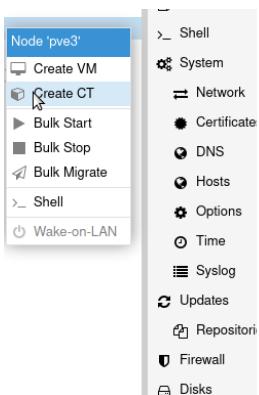
Les templates uploadés seront téléchargés dans `/var/lib/vz/template/cache` ou dans le dossier `template/cache` de l'espace de stockage.

Une fois le template uploadé, on peut le voir et éventuellement le supprimer depuis l'espace de stockage local →dans la section « Templates de conteneurs » :



## 9-Création du conteneur proprement dit

La création du conteneur se fera par le clic en haut à droite à côté de créer VM.



Dans le premier écran, il faudra sélectionner :

- le nœud de destination en cas de plusieurs serveurs ;
- le nom du conteneur ;

- son mot de passe ;
- éventuellement une clé SSH.

Create: LXC Container

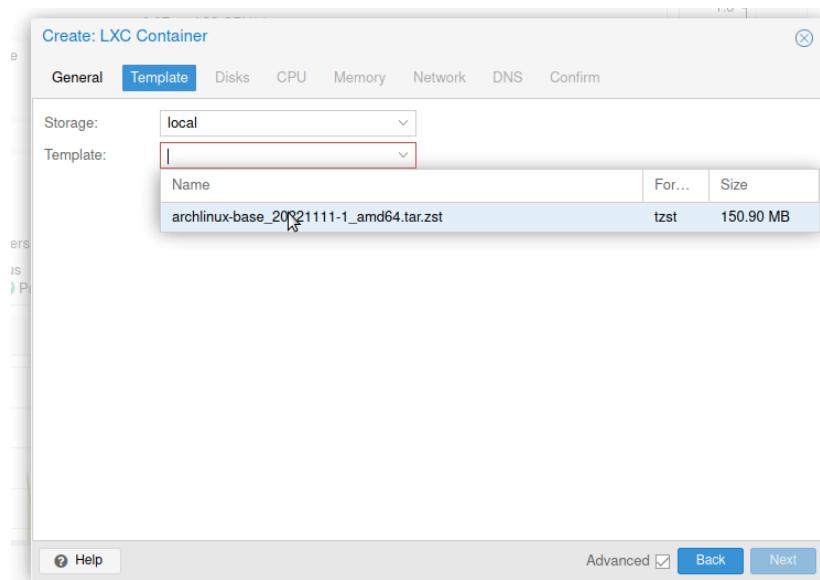
General    Template    Disks    CPU    Memory    Network    DNS    Confirm

Node:	pve3	Resource Pool:	
CT ID:	100	Password:	*****
Hostname:	container.ndeye	Confirm password:	*****
Unprivileged container:	<input checked="" type="checkbox"/>	SSH public key:	
Nesting:	<input checked="" type="checkbox"/>	<input type="button" value="Load SSH Key File"/>	

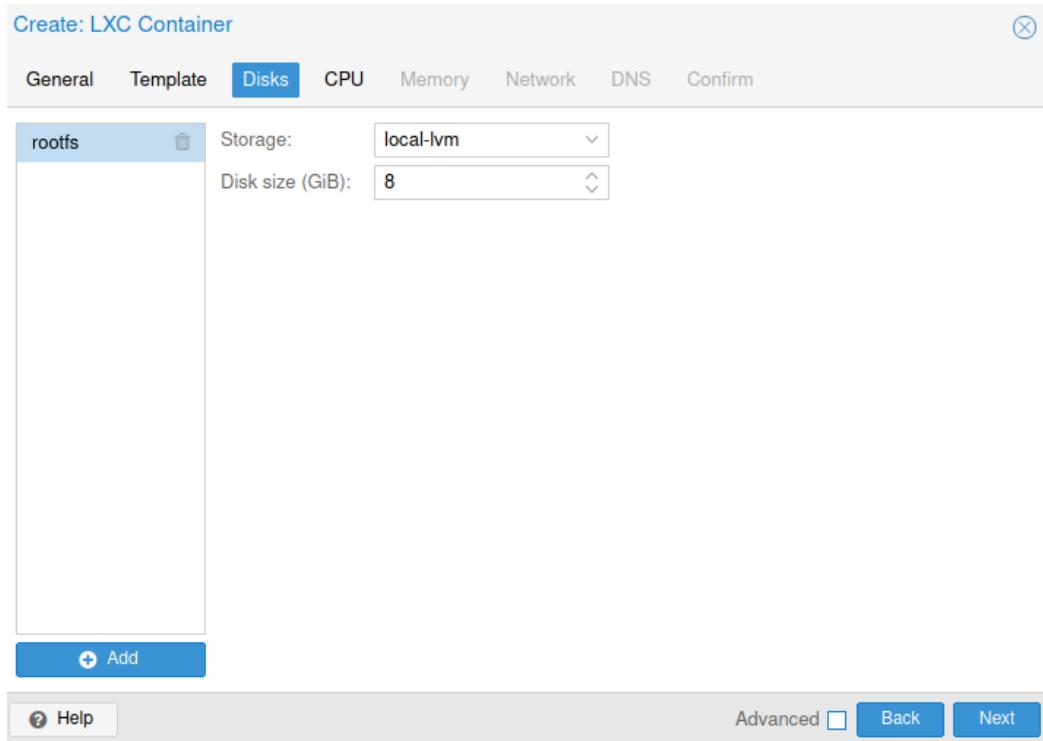
Advanced  Back

Cocher « unprivileged container » est recommandé en termes de sécurité.  
Un « privileged container » aura un UUID de 0.

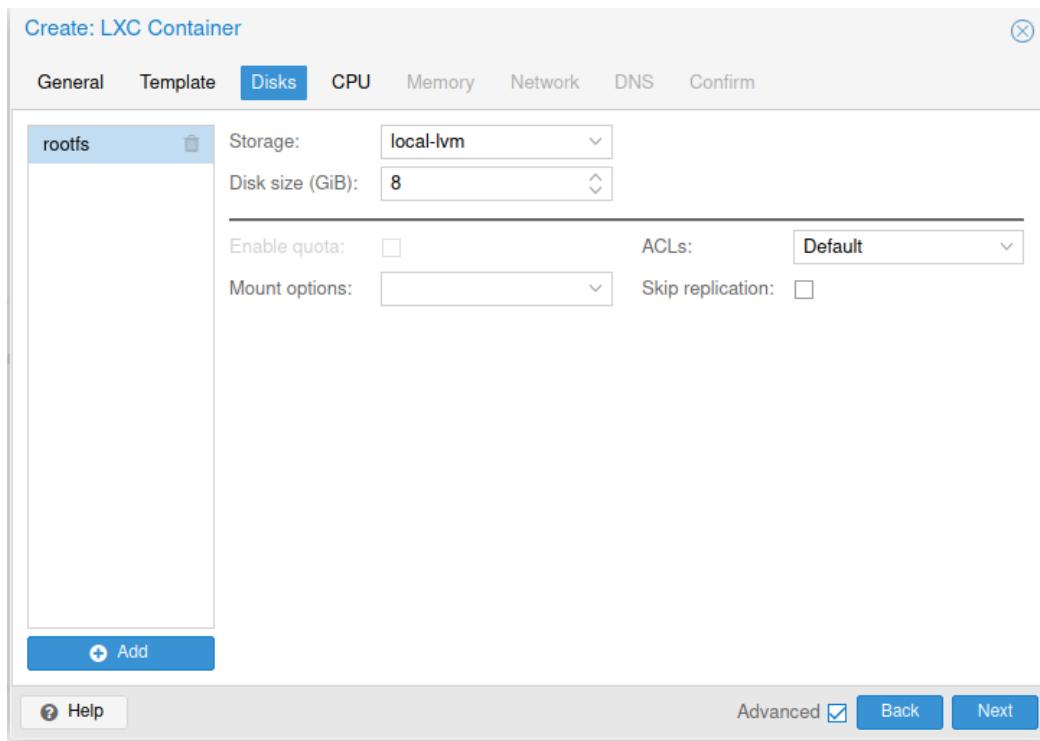
Sur le second écran, on sélectionne le stockage de destination, le modèle de conteneur :



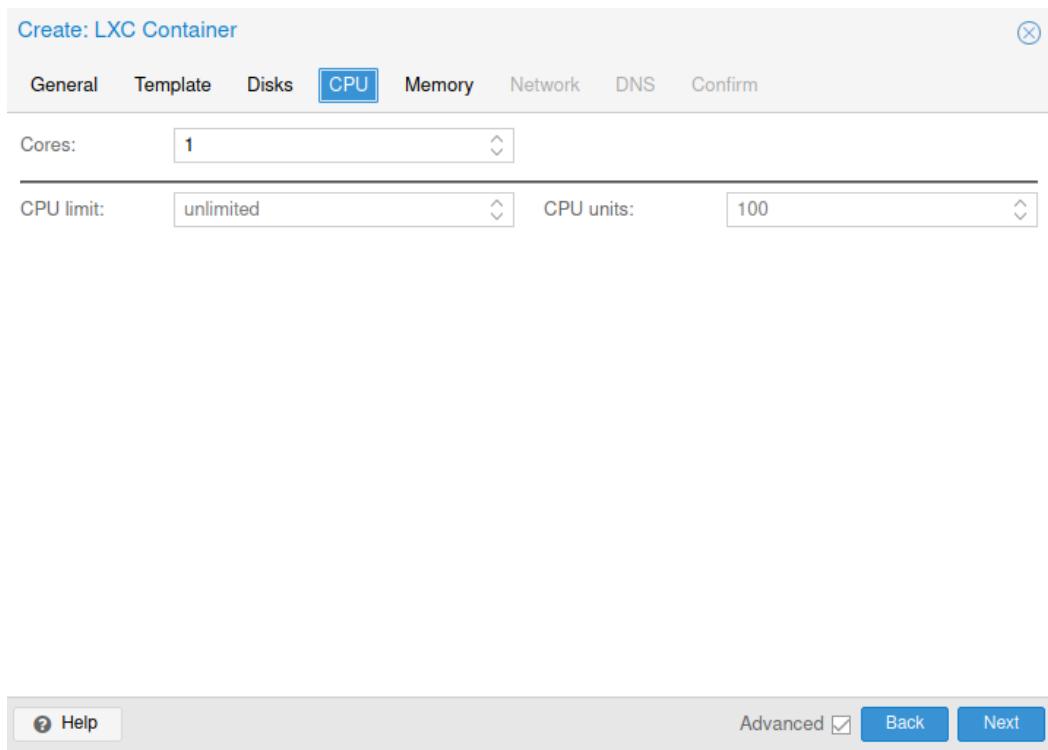
On peut ensuite sélectionner la taille du disque :



Cocher «advanced » permettra d'activer le quota, de gérer les ACL.



On sélectionne enfin le nombre de coeurs et la mémoire affectée au conteneur :



Les options avancées permettent de mettre une limite CPU.

L'écran suivant permettra de fixer la mémoire dédiée au conteneur ainsi que son swap :

Create: LXC Container

General   Template   Disks   CPU   **Memory**   Network   DNS   Confirm

Memory (MiB):  Swap (MiB):

Help Advanced Back Next

L'écran suivant concerne le réseau :

Create: LXC Container

General   Template   Disks   CPU   Memory   **Network**   DNS   Confirm

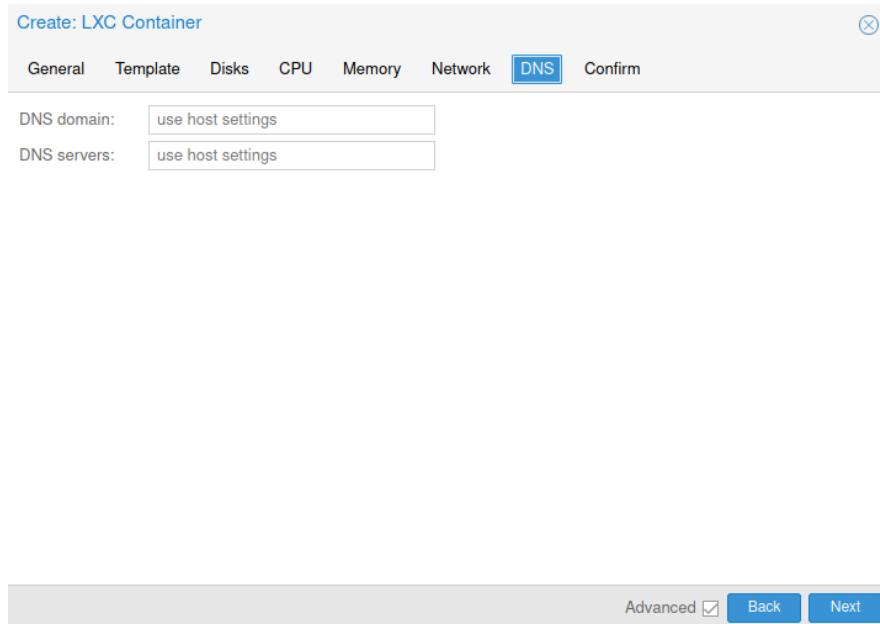
Name:  MAC address:  Bridge:  VLAN Tag:  Firewall:

IPv4:  Static  DHCP IPv4/CIDR:  Gateway (IPv4):   
IPv6:  Static  DHCP  SLAAC IPv6/CIDR:  Gateway (IPv6):

MTU:  Rate limit (MB/s):

Help Advanced Back Next

Et enfin les DNS :



On a ensuite l'écran de résumé, avec une case permettant le démarrage du conteneur juste après sa création :

Create: LXC Container

General Template Disks CPU Memory Network DNS **Confirm**

Key ↑	Value
cores	1
features	nesting=1
hostname	container.ndeye
memory	512
net0	name=eth0,bridge=vmbr0,firewall=1
nodename	pve3
ostemplate	local:vztmpl/archlinux-base_20221111-1_amd64.tar.zst
pool	
rootfs	local-lvm:8
swap	512
unprivileged	1
vmid	100

Start after created

Advanced  Back Finish

Le conteneur en création :

Task viewer: CT 100 - Create

Output Status

Stop

```
Logical volume "vm-100-disk-0" created.
Creating filesystem with 2097152 4k blocks and 524288 inodes
Filesystem UUID: 1eb91212-4e33-4835-91db-7de407be6c8e
Superblock backups stored on blocks:
      32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632
extracting archive '/var/lib/vz/template/cache/archlinux-base_20221111-1_amd64.tar.zst'
Total bytes read: 567818240 (542MiB, 313MiB/s)
Detected container architecture: amd64
Creating SSH host key 'ssh_host_dsa_key' - this may take some time ...
done: SHA256:xbuwgqjlutNwaroKedXGhb5MB4+7DWuHOBjhOQyeq2o root@container
Creating SSH host key 'ssh_host_ecdsa_key' - this may take some time ...
done: SHA256:DE/BHSI8kAKEzgOfvwM0igo3LKMfneiVZTLq2S9A8jY root@container
Creating SSH host key 'ssh_host_rsa_key' - this may take some time ...
done: SHA256:xh5N8+PvoexQltunR853cQfbAlAXta2R0zCWxEjZOTY root@container
Creating SSH host key 'ssh_host_ed25519_key' - this may take some time ...
done: SHA256:7KOOb9JiAKU78hrQEJFjumXie2GYKKhjlp0DptlY/Fg root@container
TASK OK
```

Une fois le conteneur créé, il apparaît et est manipulable comme une VM.

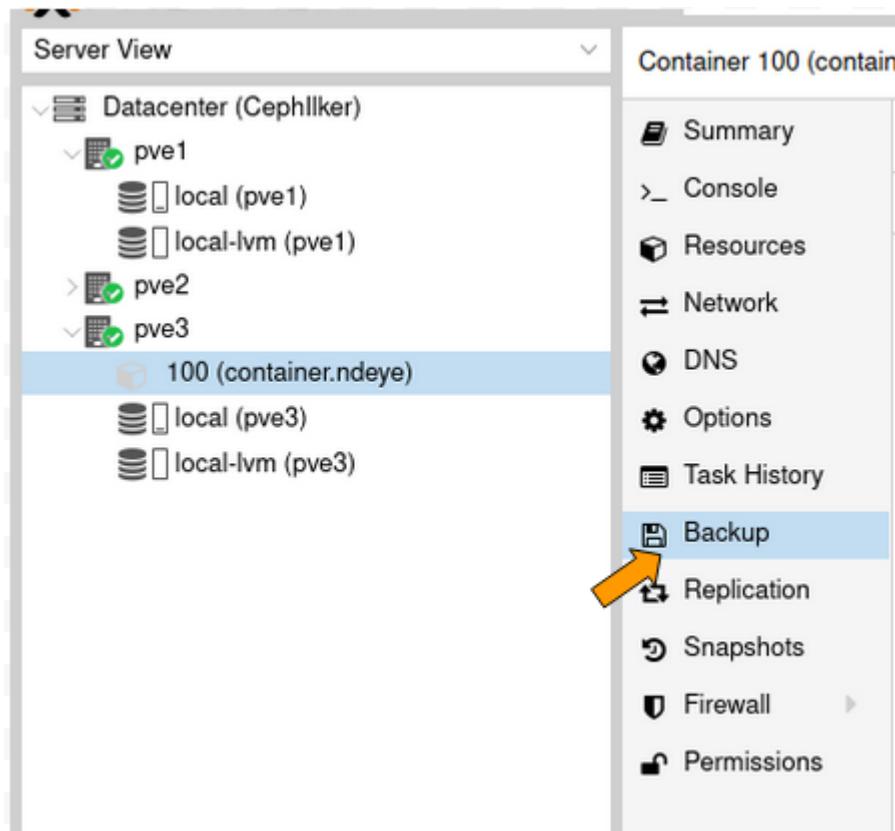
Le disque du conteneur se trouvera dans l'espace de stockage dans le dossier `images/[id conteneur]/vm-disk-[id].raw`.

Le fichier de configuration se trouvera dans `/etc/pve/lxc/[id].conf`.

Une fois le conteneur démarré, il faudra y accéder soit en SSH, soit avec « XtermJS » ou « NoVNC » depuis le menu console.

## Sauvegarde d'une VM

Pour sauvegarder une VM ou un conteneur, il faut cliquer sur celui-ci/celle-ci, puis sélectionner « Sauvegarder » dans le menu de droite :

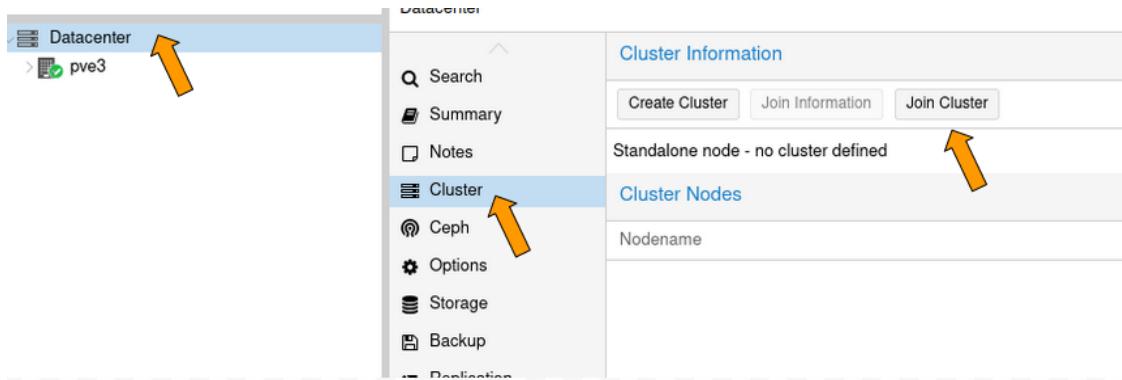


Ceci peut se faire à chaud ou à froid. Une fois la sauvegarde effectuée, celle-ci apparaîtra dans le menu. Le clic sur « Restaurer » permettra la restauration de la sauvegarde.

## A/Création d'un cluster

Nous commençons par préparer un hyperviseur supplémentaire sur une autre machine.

Une fois le second serveur préparé, il faudra aller sur datacenter → cluster puis « créer un cluster » sur le premier nœud :



Il sera demandé le nom du cluster :

**Create Cluster**

Cluster Name:	Moncluster
Cluster Network:	Link: 0 10.202.19.12
Add Multiple links are used as failover, lower numbers have higher priority.	

Help Create

Il n'est pas nécessaire de renseigner l'adresse du cluster.

Cluster en cours de création :

Task viewer: Create Cluster

Output Status

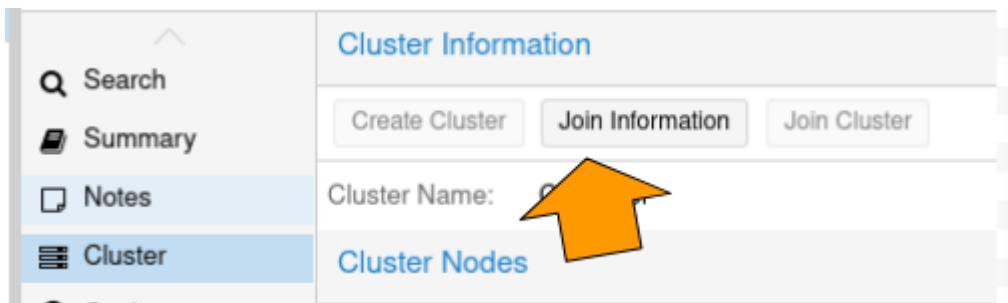
Stop

```
Corosync Cluster Engine Authentication key generator.  
Gathering 2048 bits for key from /dev/urandom.  
Writing corosync key to /etc/corosync/authkey.  
Writing corosync config to /etc/pve/corosync.conf  
Restart corosync and cluster filesystem  
TASK OK
```

Le nom du cluster apparaîtra entre parenthèses à côté de datacenter :

Cluster Information				
Create Cluster		Join Information	Join Cluster	
Cluster Name: Moncluster			Config Version: 1	

Intégrons maintenant notre serveur supplémentaire après sa préparation depuis le menu datacenter → cluster, en cliquant sur joindre le cluster :



On trouve les informations dans datacenter → cluster → information de jonction sur le premier serveur, à côté du bouton de création de cluster :

**Cluster Join Information**

Copy the Join Information here and use it on the node you want to add.

IP Address:	10.202.19.12
Fingerprint:	4D:5C:12:70:FA:03:FA:0A:A6:B6:7F:5A:11:7F:64:2F:1A:5D:39:7F:87:04:11:0A:20:B2:38:6A:4B:6F:3D:00
Join Information:	eyJpcEFkZHJlc3MiOiIxMC4yMDluMTkuMTIiLCJmaW5nZXJwcmludC16jREOjVDOjEyOjcwOkZBOjAzOkZBOjBBOkE2okl2OjdGOjExOjdGOjY0OjGOjFB0jVEOjM5OjdGOjg3OjA0OjExOjBBOjlwOklyOjM4OjZBOjRCOjZG OjNEOjAwliwicGVlckxpbtzljp7ljAiOiIxMC4yMDluMTkuMTIifSwicmluZ19hZGRyljblijEwLjlwMi4xOS4xMiJdLCJ0 b3RlbSl6ev.lz7WNhdXRoloiib24ilC.libHVzdGVvX25hbWliOiiD7XRoSWxr7XlilC.JbnRlcmlhY2UiOnsiMC16ev

**Copy Information**

On copie le champ information va automatiquement renseigner le champ empreinte et l'adresse IP, il restera à rentrer le mot de passe.

Machine en cours de jonction :

The screenshot shows the Proxmox VE interface. In the center, a modal window titled "Task viewer: Joindre le Cluster" is open, showing the log of a node addition process. The log includes steps like establishing an API connection, logging in, requesting node addition, stopping the pve-cluster service, backing up old database, waiting for quorum, generating new node files, merging authorized SSH keys, and restarting services. Below this window, there's a table titled "Tâches" (Tasks) and "Journaux du cluster" (Cluster logs). The table lists several recent tasks, each with a timestamp, node name, user, task type, and status.

Nous voyons ensuite les 3 serveurs dans le cluster depuis n'importe lequel des hyperviseurs (dans la liste des nœuds du menu cluster et dans la partie gauche) :

The screenshot shows the Proxmox VE 7.3-3 interface. On the left, the "Server View" sidebar shows a tree structure of nodes under "Datacenter (MonCluster)". The nodes listed are "serveur1", "serveur2", and "serveur3". The "serveur3" node is currently selected. The main right panel is titled "Node 'serveur3'" and contains a search bar. Below the search bar is a navigation menu with options: Summary, Notes, Shell, System (with a dropdown arrow), and Network. To the right of the menu is a table titled "Type ↑ Description" which lists two storage entries: "storage local (serveur3)" and "storage local-lvm (serveur3)".

## B/Stockage Ceph

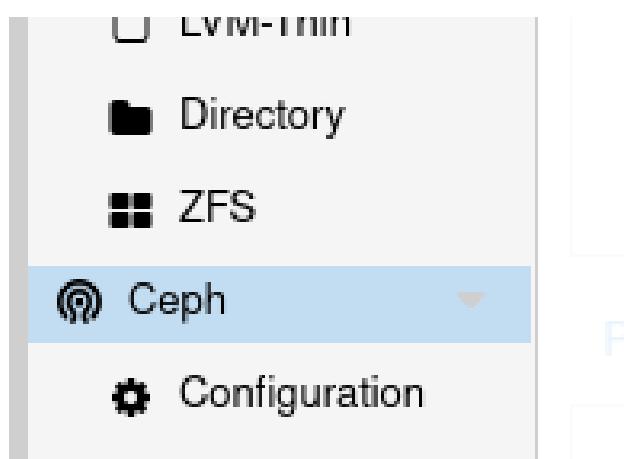
Ceph nous permettra d'avoir un espace de stockage distribué et répliqué.

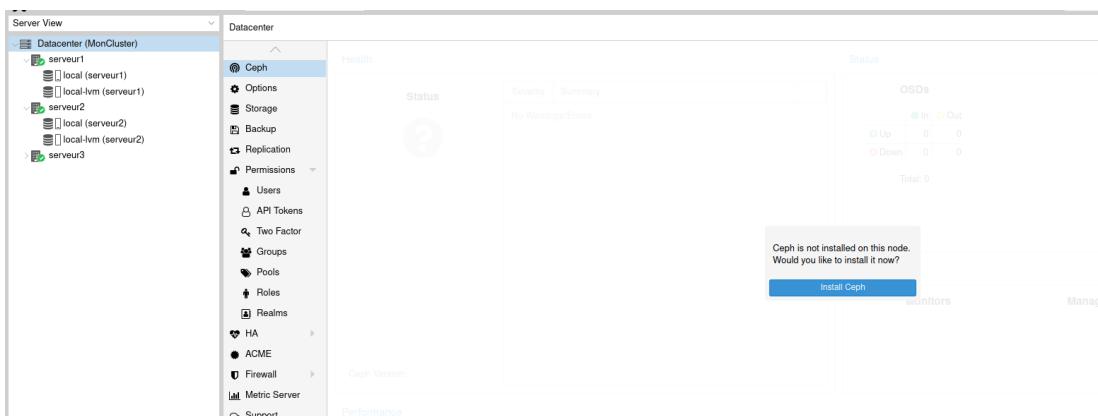
Pour l'exploiter, il nous faudra trois nœuds pour garantir le quorum (nombre minimum de ressources pour qu'un vote puisse être légitime et

éviter un split-brain) et minimum un disque dur libre par nœud. Ceph est composé de plusieurs démons, répartis sur plusieurs machines.

- **Mon** : monitor : ce sont les chefs d'orchestre du cluster Ceph. S'il n'y a pas de moniteur disponible, il n'y a pas d'accès au cluster Ceph. Pour assurer la pérennité du cluster, les moniteurs doivent être sur des machines indépendantes et en nombre impair. Un minimum de trois moniteurs est recommandé.
- **Osd** : démon OSD (object Storage Device) : Il y a un démon OSD par volume OSD. Ce démon est chargé du stockage, de la réPLICATION, et de la redistribution des données en cas de défaillance. Il fournit les informations de monitoring aux monitors.
- **Mds** : Meta Data Service : nécessaire à l'utilisation de CephFS. Va stocker les métadonnées de tous les fichiers et permettre le support de POSIX.
- **Cephfs** : filesystem POSIX fourni avec Ceph et s'appuyant sur le stockage Ceph (objet ou bloc). C'est la couche de plus haut niveau.

Si vous allez dans la partie Ceph du tableau de bord :



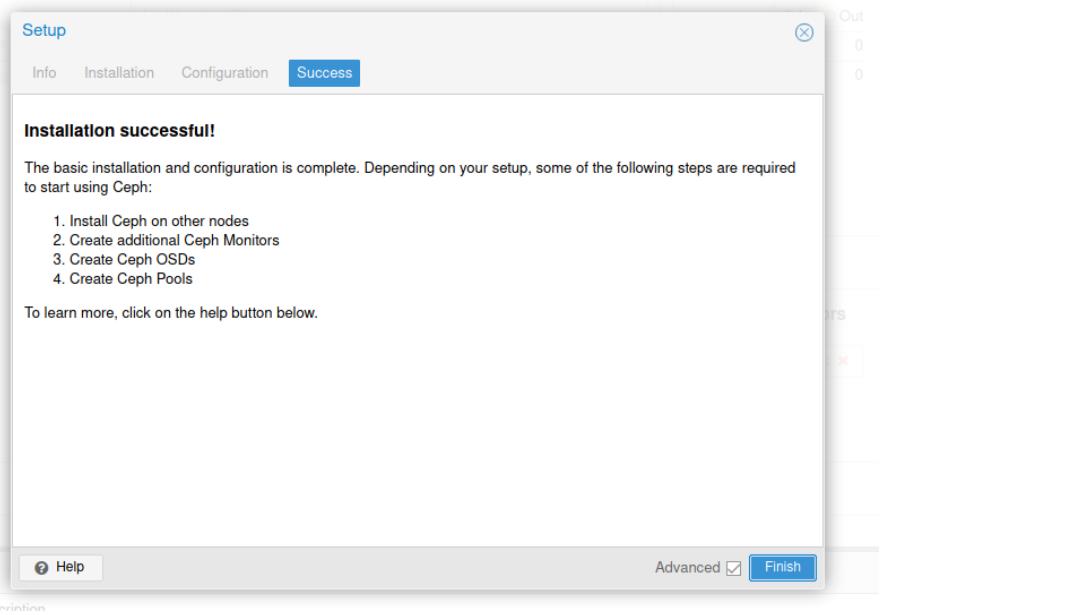


Setup X

Info Installation Configuration Success

```
ceph ceph-base ceph-mds ceph-mgr ceph-mgr-modules-core ceph-mon
ceph-osd ceph-volume cryptsetup-bin libdouble-conversion3 libfmt7
libparted2 libpcre2-16-0 libqt5core5a libqt5dbus5 libqt5network5
libsqLite3-mod-ceph libthrift-0.13.0 nvme-cll parted
python-pastedeploy-tpl python3-bcrypt python3-bs4 python3-cffi-backend
python3-cherrypy3 python3-cryptography python3-dateutil
python3-distutils python3-lib2to3 python3-logutils python3-mako
python3-markupsafe python3-natsort python3-openssl python3-paste
python3-pastedeploy python3-pecan python3-simplegeneric
python3-singledispatch python3-soupsieve python3-tempita
python3-waitress python3-weboob python3-webtest python3-werkzeug
shared-mime-info sudo uuid-runtime
The following packages will be upgraded:
ceph-common ceph-fuse libcephfs2 librados2 libradosstriper1 librbd1
librbd2 python3-ceph argparse python3-ceph-common python3-cephfs
python3-rados python3-rbd python3-rgw
13 upgraded, 48 newly installed, 0 to remove and 0 not upgraded.
Need to get 95.6 MB of archives.
After this operation, 314 MB of additional disk space will be used.
Do you want to continue? [Y/n] 
```

Advanced  Next



Nous pouvons ensuite voir le moniteur dans le panneau Ceph :

The screenshot shows the Proxmox VE interface with the 'Datacenter' view selected. In the left sidebar, 'Ceph' is highlighted under 'Cluster'. The main area shows a 'Health' section with a yellow exclamation mark icon and the status 'HEALTH\_WARN'. A table summary shows 'OSD count 0 < osd\_pool\_default\_size 3'. To the right, there's a 'Status' section for 'OSDs' with a table showing 0 Up and 0 Down OSDs. Below the interface is a terminal window displaying the output of the 'ceph status' command:

```

permitted by applicable law.
Last login: Fri Dec  9 14:58:50 CET 2022 on pts/1
root@serveur1:~# ceph status
cluster:
  id:      f91cfcc7a-4eb7-4d88-a223-222e2b83efbb
  health:  HEALTH_WARN
            Reduced data availability: 1 pg inactive
            Degraded data redundancy: 16 pgs undersized

  services:
    mon: 3 daemons, quorum localhost,serveur2,serveur3 (age 31m)
    mgr: localhost(active, since 102m), standbys: serveur2, serveur3
    osd: 3 osds: 3 up (since 12m), 3 in (since 12m)

  data:
    pools:  2 pools, 129 pgs
    objects: 2 objects, 449 KiB
    usage:   64 MiB used, 559 GiB / 559 GiB avail
    pgs:    0.775% pgs not active
            113 active+clean
            15  active+undersized
            1   undersized+peered

```

Nous pouvons voir un « health warn », le cluster Ceph ne comprenant qu'un moniteur et aucun osd.

Nous allons ensuite procéder à la création d'un osd dans ceph → osd :

The screenshot shows the Gnome System Settings window with the 'Disks' option selected in the sidebar. In the main area, there is a table titled 'Create: OSD' with columns for Name, Class, OSD Type, and Status. A single row named 'default' is listed. An orange arrow points to the 'Create: OSD' button at the top right of the table area. The table has a dashed border.

Create: Ceph OSD

Disk:	No Disks unused	DB Disk:	use OSD disk
		DB size (GiB):	Automatic
Encrypt OSD:	<input checked="" type="checkbox"/>	WAL Disk:	use OSD/DB disk
Device Class:	auto detect	WAL size (GiB):	Automatic

Note: Ceph is not compatible with disks backed by a hardware RAID controller. For details see [the reference documentation](#).

Help Advanced Create

Nous allons ensuite dans l'onglet CephFS. Il va nous falloir créer tout d'abord un serveur de métadonnées (MDS) :

Une fois le MDS créé, on pourra créer le CephFS.

Task viewer: CephFS cephfs - Créer

**Sortie**    **Statut**

Stopper

```
creating data pool 'cephfs_data'...
creating metadata pool 'cephfs_metadata'...
configuring new CephFS 'cephfs'
Successfully create CephFS 'cephfs'
Adding 'cephfs' to storage configuration...
Waiting for an MDS to become active
Waiting for an MDS to become active
TASK OK
```

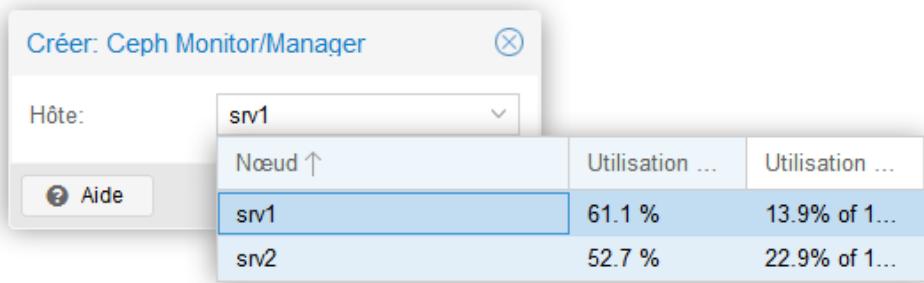
Depuis srv2, nous pouvons voir la présence du CephFS :

Heure de début ..	Heure de fin	Noeud	Utilisateur	Description	Statut
Mars 27 09:23:19	Mars 27 09:23:38	srv1	root@pam	CephFS cephfs - Créer	OK
Mars 27 09:23:03	Mars 27 09:23:05	srv1	root@pam	Ceph Metadata Server mds.srv1 - Créer	OK
Mars 27 09:21:07	Mars 27 09:22:17	srv2	root@pam	Ceph OSD sdb - Créer	OK
Mars 27 09:19:53	Mars 27 09:20:20	srv2	root@pam	Ceph Monitor mon.srv2 - Créer	OK
Mars 27 09:16:34	Mars 27 09:18:22	srv1	root@pam	Ceph OSD sdb - Créer	OK

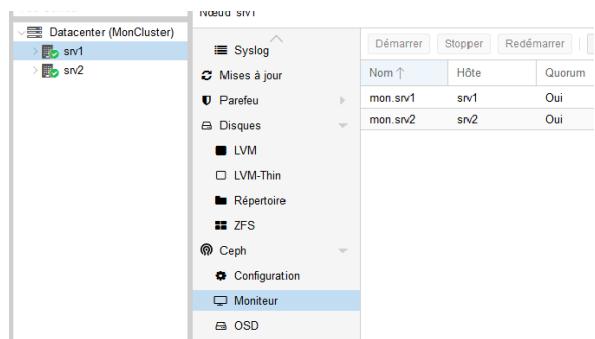
On ajoute un MDS sur srv2 pour la redondance.

On crée un pool de trois machines avec un minimum de deux.

On crée ensuite un moniteur sur le second serveur :



Le moniteur va être créé :



Pour créer l'osd du second serveur, il faudra utiliser son interface web. On pourra ensuite voir les osd des deux serveurs :

Name	Type	C...	OSD...	Status	weight	Reweight	Utilisé		Latence (ms)
							%	Total	
default	root			up	1	5,03	19.90 GiB	0	
srv2	host	osd	hdd bluestore	up	1	5,03	19.90 GiB	0	
osd.1									
srv1	host	osd	hdd bluestore	up	1	5,03	19.90 GiB	0	
osd.0									

**Tâches** Journaux du cluster

Heure de début ↓	Heure de fin	Nœud	Utilisateur	Description	Statut
Mars 23 13:06:56	Mars 23 13:07:57	srv2	root@pam	Ceph OSD sdb - Créer	OK
Mars 23 13:04:24	Mars 23 13:04:55	srv2	root@pam	Ceph Monitor mon.srv2 - Créer	OK
Mars 23 12:41:02	Mars 23 12:43:01	srv2	root@pam	Joindre le Cluster	OK
Mars 23 12:40:07	Mars 23 12:40:14	srv1	root@pam	Créer Cluster	OK
Mars 23 12:36:11	Mars 23 12:36:11	srv2	root@pam	Démarrer toutes les VMs et les conteneurs	OK

Une fois l'espace de stockage Ceph créé, il va falloir l'ajouter depuis Datacenter → stockage :

Type	Content	Path/Target
Directory	VZDump backup file, ISO image, Container template	/var/lib/vz
LVM-Thin	Disk image, Container	

Comme montré ci-dessus, il va falloir sélectionner « RBD », ce qui ouvrira l'écran suivant :

Ajouter: RBD

ID:	espace_ceph	Nœuds:	Tout (Aucune restriction)
Pool:	cephfs_data	Activer:	<input checked="" type="checkbox"/>
Monitor(s):	srv1,srv2,srv3	Contenu:	Image disque
Utilisateur:	admin	KRBD:	<input type="checkbox"/>

Use Proxmox VE managed hyper-converged ceph pool

[Aide](#) [Ajouter](#)

Le pool du CephFS créé précédemment est automatiquement sélectionné. Reste à sélectionner le contenu du stockage : image disque ou conteneur.

Le CephFS est alors disponible pour le stockage de VM :

## C/Firewall Open Sense virtualisé:

**OPNsense** est une plate-forme de routage et de pare-feu open source. On peut faire du filtrage par source et destination au niveau des adresses IP, protocole IP, port source et destination des protocoles TCP et UDP.

- Capacité à limiter le nombre de connexions règle par règle.

Les configurations pour avoir deux réseaux différents un LAN et un WAN

Comment connecter une des interfaces physique de notre serveur à une interface virtuelle directement.

On va utiliser des switchs virtuels que PROXMOX nous offre.

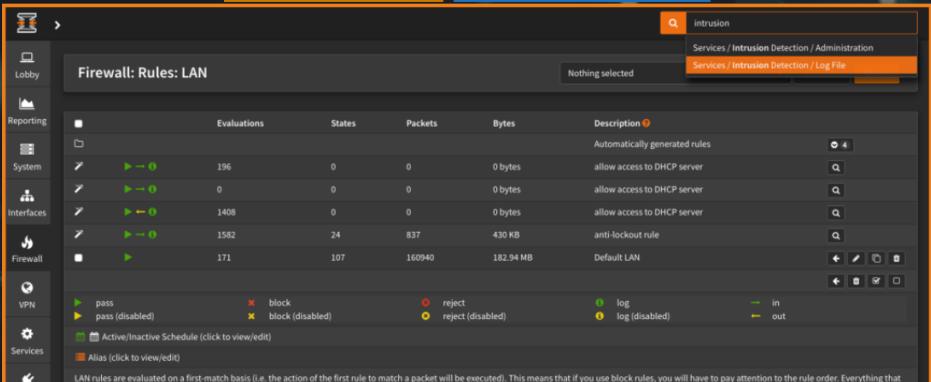
Je vais sur le site de opensense,

 [About](#) [Users](#) [Developers](#) [Partners](#) [Support](#) [Blog](#) [Download](#) [Official Shop](#) [Donate](#)

# Secure Your Network with ease

From Virtual Private Networking to Intrusion Detection, Best in class, FREE Open Source Project.

[Download OPNsense®](#) [Sign-up for ETPRO Telemetry](#)



The screenshot shows the OPNsense web interface under the Firewall section. It displays a list of LAN rules. The columns are labeled: Evaluations, States, Packets, Bytes, and Description. There are five rules listed:

- Automatically generated rules (4)
- allow access to DHCP server (0 evaluations, 0 states, 0 packets, 0 bytes)
- allow access to DHCP server (0 evaluations, 0 states, 0 packets, 0 bytes)
- allow access to DHCP server (1408 evaluations, 0 states, 0 packets, 0 bytes)
- anti-lockout rule (1582 evaluations, 24 states, 837 packets, 430 KB bytes)
- Default LAN (171 evaluations, 107 states, 160940 packets, 182.94 MB bytes)

Below the table, there are icons for pass, block, reject, log, and in/out directions, along with Active/Inactive Schedule and Alias links.

Ensuite je le télécharge

 [About](#) [Users](#) [Developers](#) [Partners](#) [Support](#) [Blog](#) [Download](#) [Official Shop](#) [Donate](#)

## Fast download selector

### Architecture

System architecture.

amd64

### Select the image type:

- dvd: ISO Installer image with live system capabilities running in VGA mode. On amd64, UEFI boot is supported as well.
- vga: USB Installer image with live system capabilities running in VGA mode as GPT boot. On amd64, UEFI boot is supported as well.
- serial: USB Installer image with live system capabilities running in serial console (115200) mode as MBR boot.
- nano: a preinstalled serial image for USB sticks, SD or CF cards as MBR boot. These Images are 3G in size and automatically adapt to the installed media size after first boot.

dvd

### Mirror Location

OPNsense can be downloaded from a large range of mirrors located in different countries, you may want to select the fastest options for your location.

Hiho.ch

[Download](#)

### Checksum verification

Checksum files next to the Images may not prove authenticity of Images

on any particular mirror. The checksums can also be found in the forum

[announcements](#) [mailing lists](#) [blog posts](#) or [GitHub](#). Please [double check](#).

Après l'avoir téléchargé, je vais dans:

Storage 'local' on node 'pve3'

	Name
	OPNsense-22.7-OpenSSL-dvd-amd64.iso
	ubuntu-20.04-legacy-server-amd64.iso

Et je fais un upload

Upload

File: C:\fakepath\OPNsense-22.7-Op

File name: OPNsense-22.7-OpenSSL-dvd-amd64.iso

File size: 1.31 GiB

MIME type: application/x-cd-image

Hash algorithm: None

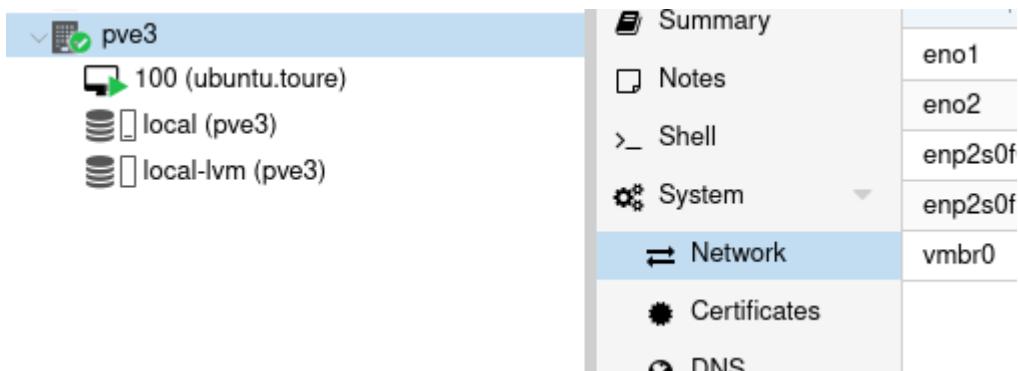
Checksum: none

Task viewer: Copy data

```
starting file import from: /var/tmp/pveupload-69157ac61329458c73db8a0f9d802eb7
target node: pve3
target file: /var/lib/vz/template/iso/OPNsense-22.7-OpenSSL-dvd-amd64.iso
file size is: 1410926592
command: cp -- /var/tmp/pveupload-69157ac61329458c73db8a0f9d802eb7 /var/lib/vz/template/iso/OPNsense-22.7-OpenSSL-dvd-amd64.iso
finished file import successfully
TASK OK
```

Maintenant que notre ISO est prêt, on va venir préparer PROXMOX pour la configuration du réseau.

On va dans l'onglet NETWORK



On voit un Bridge avec l'interface sur laquelle il a trouvé la connexion lors de son installation.

Name ↑	Type	Active	Autostart	VLAN a...	Ports/Slaves	Bond Mode	CIDR	Gateway
eno1	Network Device	No	No	No				
eno2	Network Device	No	No	No				
enp2s0f0np0	Network Device	Yes	No	No				
enp2s0f1np1	Network Device	No	No	No				
vmbr0	Linux Bridge	Yes	Yes	No	enp2s0f0np0		10.202.19.12/16	10.202.255.254

Il utilise le port **enp2s0f0np0** qui est marqué actif en haut, il est connecté au réseau LAN. Et c'est ce port qui me permet d'accéder à la fois à PROXMOX et ses VM, d'accéder à mon réseau et à Internet.

Maintenant on va créer un nouveau bridge.

https://10.202.19.12:8006/#v1:0:=node%2Fp

eatsheet IUT de Béziers – Votre ...

nement 7.3-3 Search

Node 'pve3'

Search Summary Notes Shell System Network Certificates DNS Hosts Options Time

Create Revert Ed

- Linux Bridge
- Linux Bond
- Linux VLAN
- OVS Bridge
- OVS Bond
- OVS IntPort
- LinJx Bridge

### Edit: Linux Bridge

Name: vmbr1 Autostart:

IPv4/CIDR:  VLAN aware:

Gateway (IPv4):  Bridge ports: enp2s0f1np1

IPv6/CIDR:  Comment:

Gateway (IPv6):

---

MTU: 1500

Advanced  OK Reset

Votre ...

Name ↑	Type	Active	Autostart	VLAN a...	Ports/Slaves	Bond Mode	CIDR	Gateway
eno1	Network Device	No	No	No				
eno2	Network Device	No	No	No				
enp2s0f0np0	Network Device	Yes	No	No				
enp2s0f1np1	Network Device	No	No	No				
vmbr0	Linux Bridge	Yes	Yes	No	enp2s0f0np0		10.202.19.12/16	10.202.255.254
vmbr1	Linux Bridge	No	Yes	No	eno1			

Ce vmbr1 va être le switch sur lequel va venir connecter mon interface WAN à la fois physiquement et également du côté de OPENSENSE

S'il ya une erreur, il faut faire un ssh du PROXMOX et mettre cette commande:

```
apt-get install ifupdown2
```

On voit maintenant que eno1 est connecté

Name ↑	Type	Active	Autostart	VLAN a...
eno1	Network Device	Yes	No	No
eno2	Network Device	No	No	No
enp2s0f0np0	Network Device	Yes	No	No
enp2s0f1np1	Network Device	Yes	No	No
vmbr0	Linux Bridge	No	No	No
vmbr1	Linux Bridge	No	No	No

On va créer une autre VM

Create: Virtual Machine

General OS System Disks CPU Memory Network Confirm

Node: pve3 Resource Pool:

VM ID: 101

Name: opensense

---

Start at boot:  Start/Shutdown order: any

Startup delay: default

Shutdown timeout: default

Help Advanced  Back Next

Create: Virtual Machine

General OS System Disks CPU Memory Network Confirm

Use CD/DVD disc image file (iso) Guest OS:

Storage: local Type: Linux

ISO image: e-22.7-OpenSSL-dvd-amd64.iso Version: 5.x - 2.6 Kernel

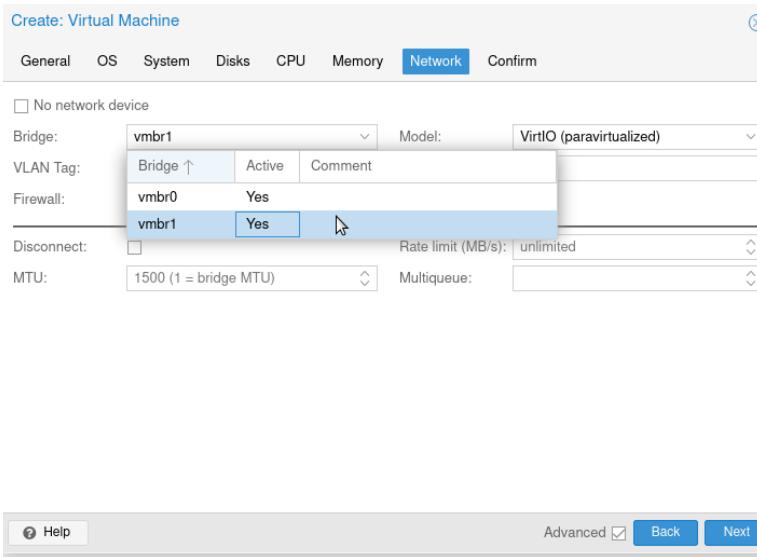
Use physical CD Name

Do not use any

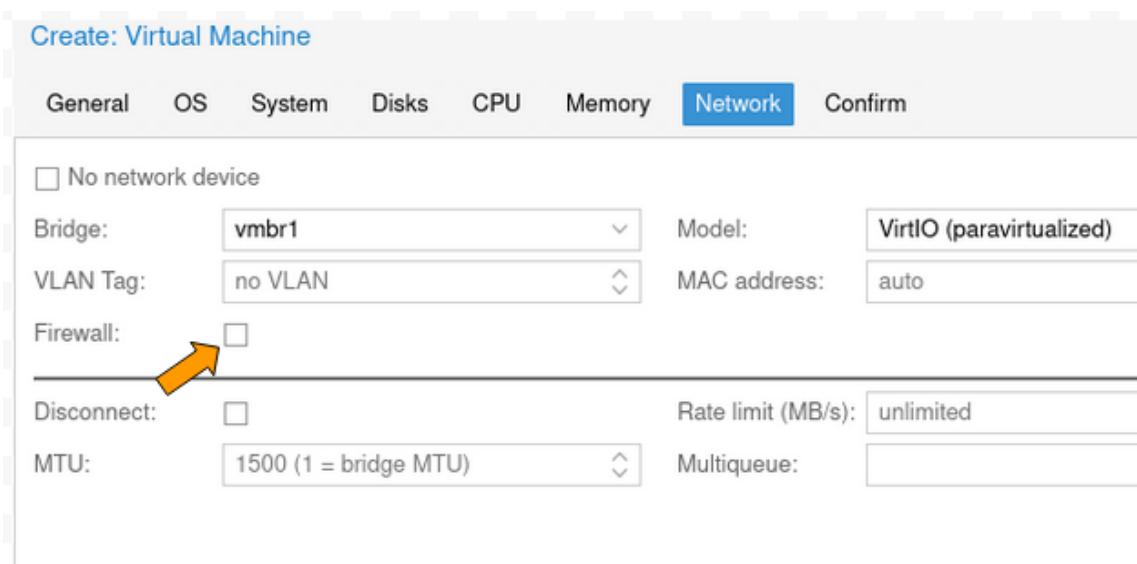
Name	Type	Size
OPNsense-22.7-OpenSSL-dvd-amd64.iso	iso	1.41 GB
ubuntu-20.04-legacy-server-amd64.iso	iso	825.23 MB

Advanced  Back Next

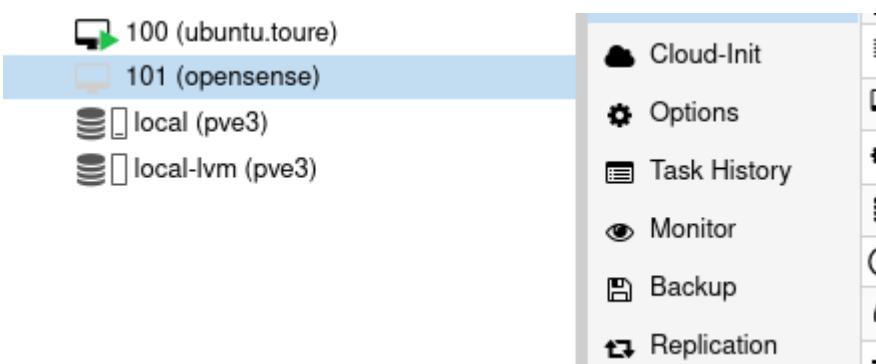
On choisit notre bridge qu'on a créé



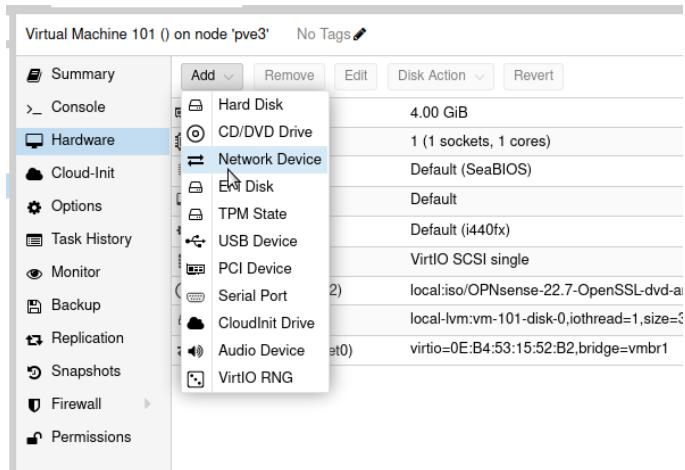
Et on désactive le firewall



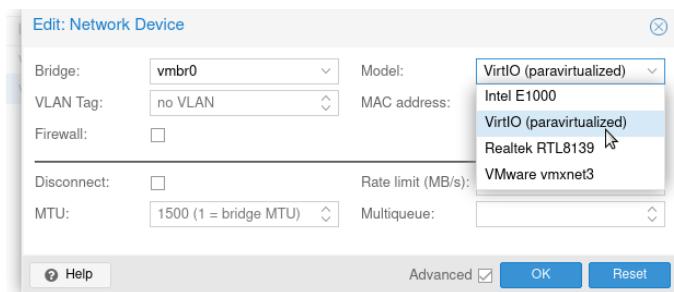
La VM est créé



On va venir ajouter une nouvelle interface



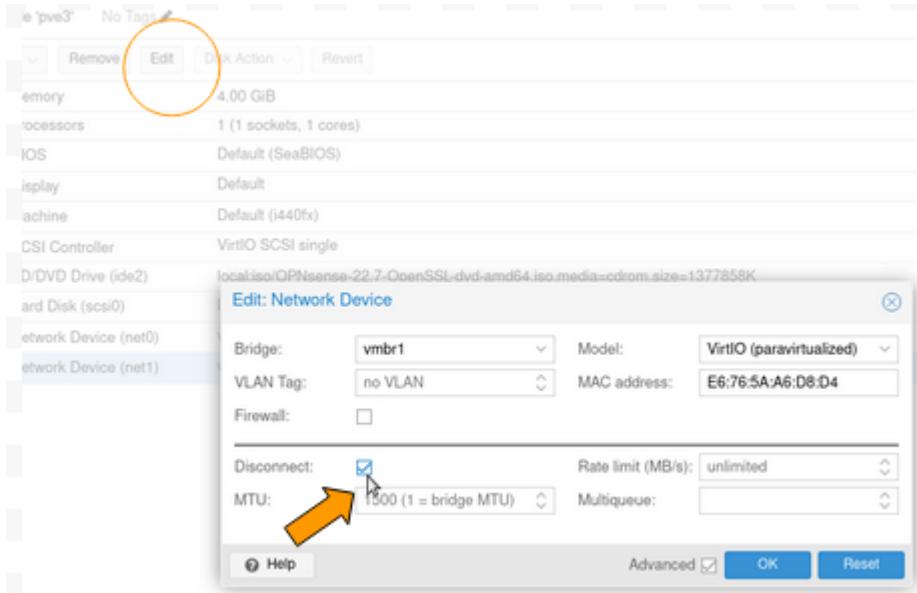
On choisit vmbr0, VirtIO(paravirtualized) et on n'oublie pas de désactiver le firewall



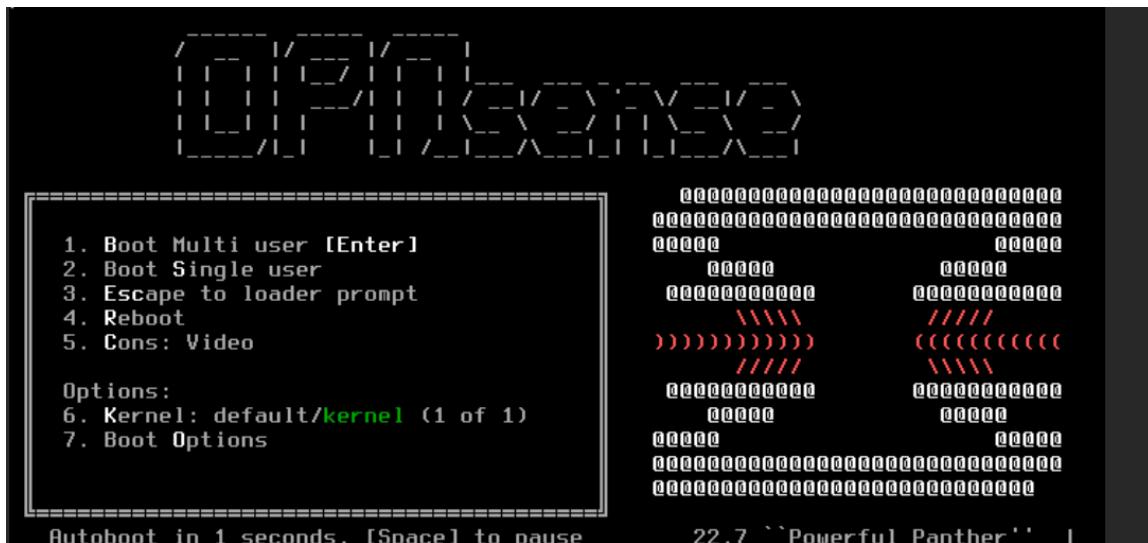
On voit ici les 2 interfaces réseau nécessaire au fonctionnement du VM

CD/DVD Drive (ide2)	local:iso/OPNsense-22.7-OpenSSL-dvd-amd64.iso,media=cdrom
Hard Disk (scsi0)	local-lvm:vm-101-disk-0,iothread=1,size=32G
Network Device (net0)	virtio=0E:B4:53:15:52:B2,bridge=vmbr1
Network Device (net1)	virtio=E6:76:5A:A6:D8:D4,bridge=vmbr0

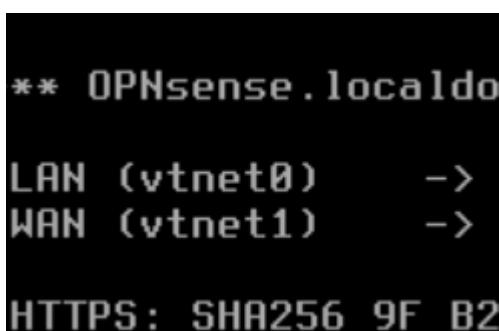
Pour faire mes configurations directement, je vais dans EDIT pour déconnecter les interfaces physiques de cet manière la VM va voir les interfaces réseau mais simulera le fait que le cable n'est pas connecté



On va démarrer la machine.



Là on voit bien nos 2 interfaces



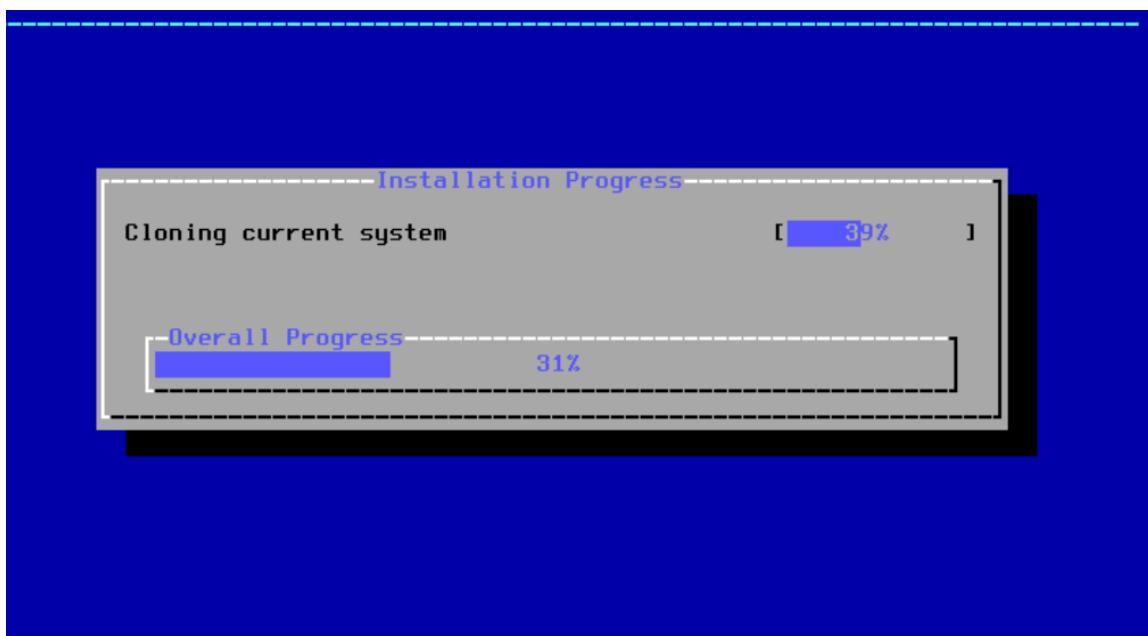
Pour se loguer: c'est **installer**, et le mot de passe :**opensense**

```
SSH:      SHA256 o2sRagHKeIy1I06bmWVBaq9D
SSH:      SHA256 NUjeWEHTnZmwbozVrW+21wb6
SSH:      SHA256 f7911cappbVoca3/czdJU+DH
pw: no such user `installer'

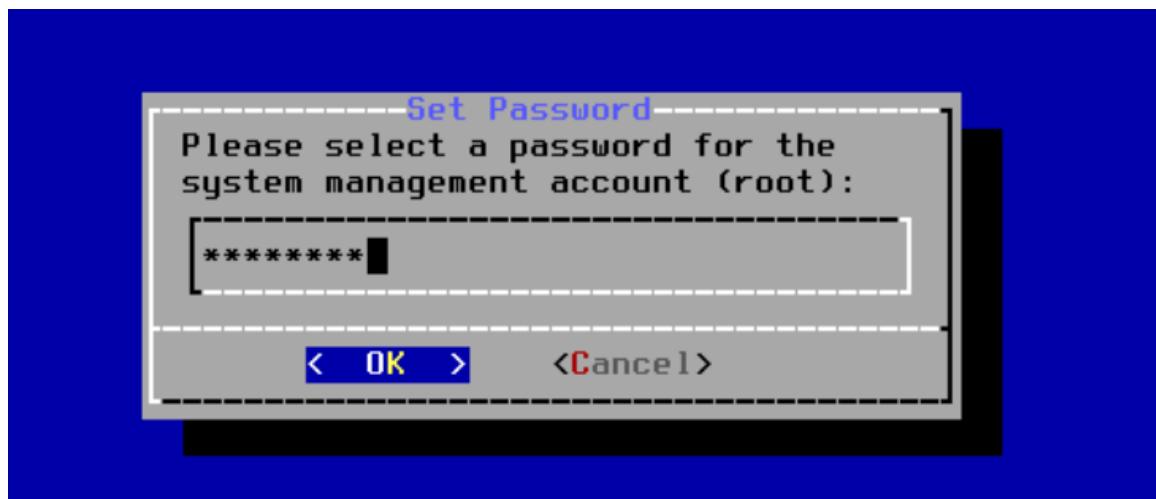
Welcome! OPNsense is running in live mode.
login as 'root' to continue in live mode or
installation. Use the default or previously
both accounts. Remote login via SSH is

FreeBSD/amd64 (OPNsense.localdomain) (tty1)

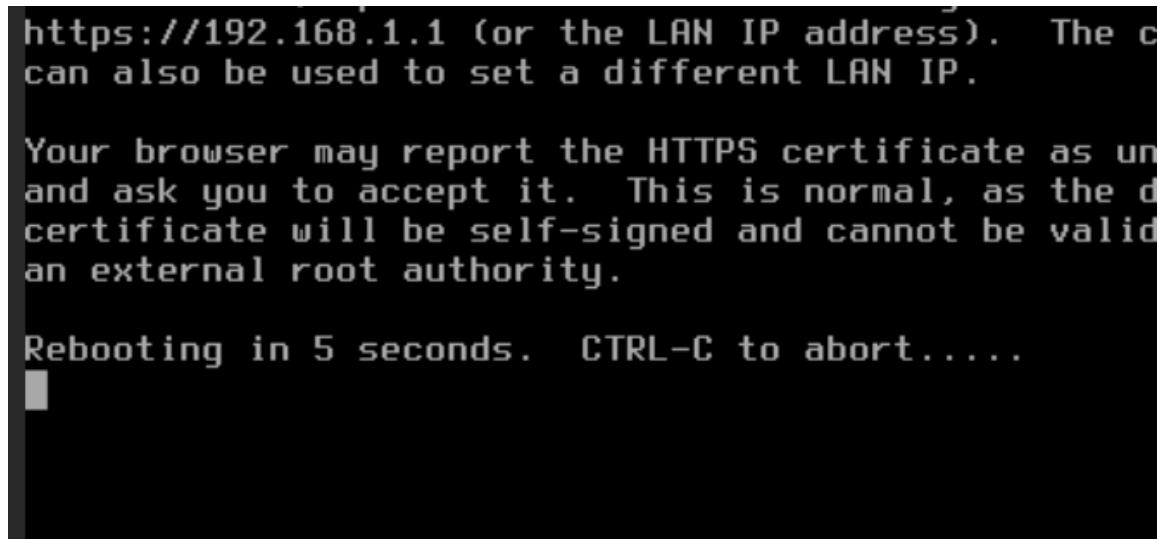
login: installer
Password:■
```



J'entre le mot de passe: **rootroot**



On reboot, et il s'installe



On se connecte avec l'utilisateur `root` et le mot de passe défini tout à l'heure

```
LAN (vtnet0)      -> v4: 192.168.1.1/24
WAN (vtnet1)      ->

HTTPS: SHA256 9F B2 71 2E CD 3E 97 D3 66 3B C5 AE 27 C9 B2 13
D7 A2 76 B1 89 80 CF 56 26 DA 5F B2 24 FF B3 6D
```

FreeBSD/amd64 (OPNsense.localdomain) (ttyv0)

```
login: root
Password: ■
```

Website:	https://opnsense.org/	oooo	oooo
Handbook:	https://docs.opnsense.org/	000\ \	///000
Forums:	https://forum.opnsense.org/	)())())()	(((((
Code:	https://github.com/opnsense	000//	\\\000
Twitter:	https://twitter.com/opnsense	0000	0000

\*\*\* OPNsense.localdomain: OPNsense 22.7 (amd64/ OpenSSL) \*\*\*

```
LAN (vtnet0)      -> v4: 192.168.1.1/24
WAN (vtnet1)      ->
```

```
HTTPS: SHA256 9F B2 71 2E CD 3E 97 D3 66 3B C5 AE 27 C9 B2 13
D7 A2 76 B1 89 80 CF 56 26 DA 5F B2 24 FF B3 6D
```

- |                              |                         |
|------------------------------|-------------------------|
| 0) Logout                    | 7) Ping host            |
| 1) Assign interfaces         | 8) Shell                |
| 2) Set interface IP address  | 9) pfTop                |
| 3) Reset the root password   | 10) Firewall log        |
| 4) Reset to factory defaults | 11) Reload all services |
| 5) Power off system          | 12) Update from console |
| 6) Reboot system             | 13) Restore a backup    |

```
Enter an option: ■
```

Avec l'option 2, on va venir configurer l'interface LAN

voici les configurations

6) Reboot system

13) Restore a backup

Enter an option: 2

Configure IPv4 address LAN interface via DHCP? [y/N] n

Enter the new LAN IPv4 address. Press <ENTER> for none:  
> 10.202.19.7

Subnet masks are entered as bit counts (like CIDR notation).

e.g. 255.255.255.0 = 24

255.255.0.0 = 16

255.0.0.0 = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):  
> 16

For a WAN, enter the new LAN IPv4 upstream gateway address.

For a LAN, press <ENTER> for none:

> █

Enter the new LAN IPv4 subnet bit count (1 to 32):  
> 16

For a WAN, enter the new LAN IPv4 upstream gateway address.

For a LAN, press <ENTER> for none:

>

Configure IPv6 address LAN interface via DHCP6? [y/N] n

Enter the new LAN IPv6 address. Press <ENTER> for none:  
>

Do you want to enable the DHCP server on LAN? [y/N] n

Do you want to change the web GUI protocol from HTTPS to HTTP? [y/N] n

Do you want to generate a new self-signed web GUI certificate? [y/N] n

Restore web GUI access defaults? [y/N] n █

```
https://10.202.19.7

*** OPNsense.localdomain: OPNsense 22.7 (amd64/OpenSSL) ***

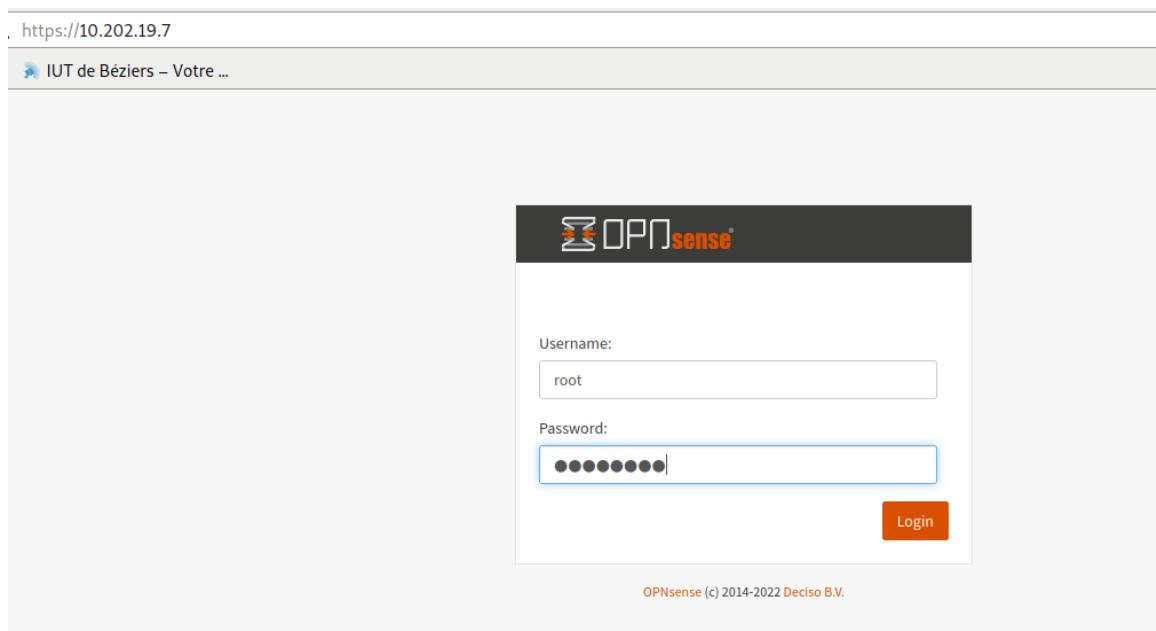
LAN (vtnet0)    -> v4: 10.202.19.7/16

HTTPS: SHA256 BD 30 DE F3 35 B2 73 B5 9C CC F9 23 D8 0F 42 7D
       AD 05 CF A6 5E C4 71 5F D3 90 10 2B 12 89 C3 69

0) Logout                      7) Ping host
1) Assign interfaces           8) Shell
2) Set interface IP address   9) pfTop
3) Reset the root password    10) Firewall log
4) Reset to factory defaults  11) Reload all services
5) Power off system            12) Update from console
6) Reboot system                13) Restore a backup

Enter an option: ■
```

Je vais sur le navigateur et j'écris l'@IP:10.202.19.7



The screenshot shows the OPNsense web interface at <https://10.202.19.7/wizard.php?xml=system>. The left sidebar contains navigation links for Lobby, Reporting, System (Access, Configuration, Firmware, Gateways, High Availability, Routes, Settings, Trust, Wizard), Interfaces (Firewall, VPN, Services, Power, Help), and a bottom section for Help. The main content area is titled "System: Wizard: General Setup" and displays the message: "This wizard will guide you through the initial system configuration. The wizard may be stopped at any time by clicking the logo image at the top of the screen." A large empty box is present for configuration steps, and a "Next" button is located at the bottom right.

On se laisse guider en appuyant sur NEXT

#### System: Wizard: General Setup

This wizard will guide you through the initial system configuration. The wizard may be stopped at any time by clicking the logo image at the top of the screen.

Next

## System: Wizard: General Information

General Information	
Hostname:	OPNsense
Domain:	localdomain
Language:	French
Primary DNS Server:	1.1.1.1
Secondary DNS Server:	1.0.0.1
Override DNS:	<input checked="" type="checkbox"/> Allow DNS servers to be overridden by DHCP/PPP on WAN
Unbound DNS	
Enable Resolver:	<input checked="" type="checkbox"/>
Enable DNSSEC Support:	<input type="checkbox"/>
Harden DNSSEC data:	<input type="checkbox"/>
<b>Next</b>	

## System: Wizard: Time Server Information

Time server hostname:	0.opnsense.pool.ntp.org 1.opnsense.pool.ntp.org 2. ...
Enter the hostname (FQDN) of the time server.	
Timezone:	Europe/Paris
<b>Next</b>	

Voici les paramètres de configuration WAN

## Système: Assistant: Configurer l'interface WAN

Type de configuration IPv4:

**Configuration générale**

Adresse MAC:

Ce champ peut être utilisé pour modifier ("spoof") l'adresse MAC de l'interface WAN (peut être xx:xx:xx ou laissez vide).

MTU (Maximum Transmission Unit):

Définissez la MTU de l'interface WAN. Si vous laissez ce champ vide, une MTU de 1492 octets sera utilisée.

MSS:

Si vous entrez une valeur dans ce champ, le bridage MSS des connexions TCP avec la valeur entrée sera appliquée. La valeur par défaut est de 1492 octets pour PPPoE et de 1500 octets pour tous les autres types de connexion.

**Configuration IP statique**

Adresse IP:

## Système: Assistant: Configurer l'interface LAN

Adresse IP LAN:   
(Laisser vide pour aucun)

Masque de sous-réseau:

On fait suivant pour conserver le même mot de passe

Mot de passe Root:	<input type="text"/>
(Laisser vide pour garder l'actuel(le))	
Confirmation Mot de passe Root:	<input type="text"/>
<b>Suivant</b>	

Ecran Interactif   moodle   cheatsheet   IUT de Béziers – Votre ...  
**OPNsense** <

root@OPNsense

Accueil

- Tableau de bord
- Licence
- Mot de passe
- Déconnexion
- Rapports
- Système
- Interfaces
- Pare-feu
- VPN
- Services
- Alimentation
- Aide

Configuration initiale terminée!

**OPNsense®**

Félicitations! OPNsense est maintenant configuré.

Veuillez envisager de faire un don au projet pour nous aider à payer nos frais généraux. Consultez [notre site internet](#) pour faire un don ou acheter des services d'assistance OPNsense disponibles.

Cliquer pour continuer vers le [tableau de bord](#). Or click to [check for updates](#).

## On peut faire de la NAT avec le Pare-feu

**Pare-feu: NAT: Sortant**

Mode

<input checked="" type="radio"/> Génération automatique des règles NAT sortantes (aucune règle manuelle ne peut être utilisée)	<input type="radio"/> Génération de règles NAT sortantes hybrides (les règles générées automatiquement sont appliquées après les règles manuelles)
<input type="radio"/> Génération manuelle de règles NAT sortantes (aucune règle automatique n'est générée)	<input type="radio"/> Désactiver la création de règle NAT sortante (NAT sortant est désactivé)

**Sauvegarder**

Règles automatiques

Interface	Réseaux source	Port Source	Destination	Port de Destination	Adresse NAT
-----------	----------------	-------------	-------------	---------------------	-------------

## On peut faire la redirection de port

The screenshot shows the OPNsense firewall configuration interface. On the left, a sidebar menu is open under the 'Pare-feu' section, with 'Redirection de port' highlighted. A blue arrow points from this menu item to the main content area. The main area is titled 'Pare-feu: NAT: Redirection de port'. It displays a table of redirection rules:

Source	Destination	NAT
Interface: LAN, Proto: TCP, Ports: *, Adresse: LAN adresse	Ports: 80, 443, Adresse: Non redirigé	IP: *, Ports: *, Description: Règle anti-Lockout
Règle activée	Disabled no redirect	Règle liée: Règle anti-Lockout
Règle désactivée		Disabled linked rule

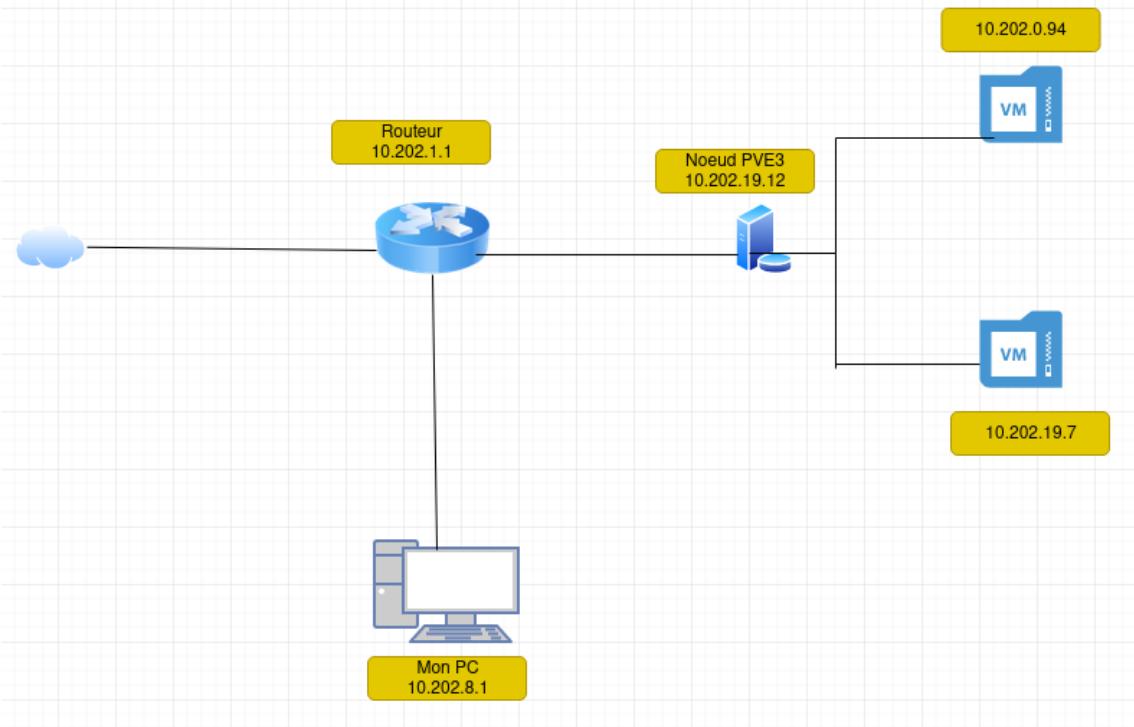
At the bottom right of the table, there is a red arrow pointing to a '+' button for adding new rules.

## D/Activer et Configurer le pare-feu (Firewall) sous Proxmox

Le Pare-feu Proxmox est une fonction de sécurité qui permet une protection simple et efficace de tout trafic interne et externe. On peut sécuriser des hôtes, des VM, des conteneurs et tout un cluster via des règles.

On va s'appuyer sur “**iptables**”(une application qui gère les tables de règles de pare-feu)

Voici mon schéma réseau:



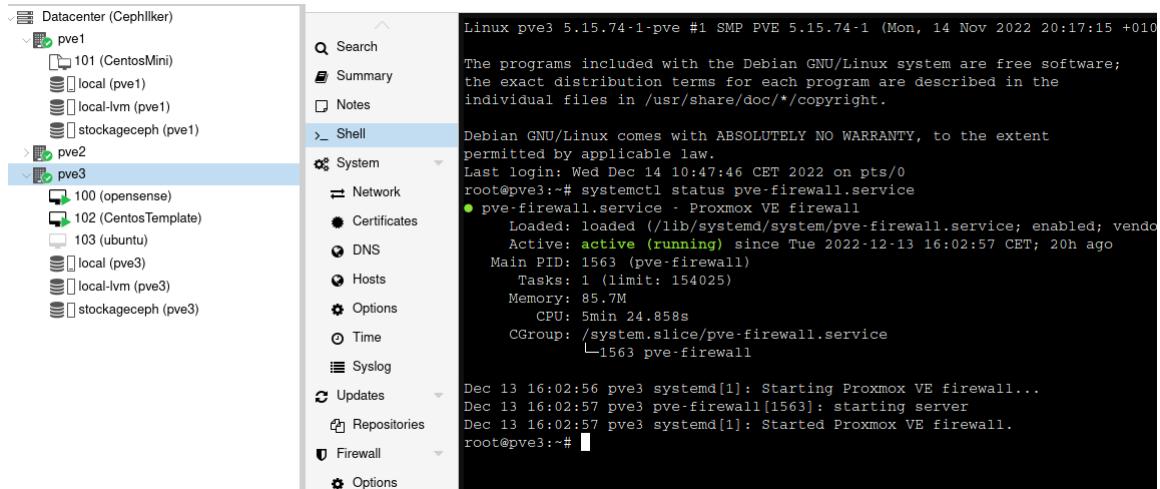
Avant cela je vais tester la connectivité en faisant des ping

```

test@232-22:~$ ping 10.202.19.7
PING 10.202.19.7 (10.202.19.7) 56(84) bytes of data.
64 bytes from 10.202.19.7: icmp_seq=1 ttl=64 time=0.594 ms
64 bytes from 10.202.19.7: icmp_seq=2 ttl=64 time=0.549 ms
^C PROXMOX ☆ 🌐
--- 10.202.19.7 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1012ms
rtt min/avg/max/mdev = 0.549/0.571/0.594/0.022 ms + B I U A
test@232-22:~$ ping 10.202.19.12
PING 10.202.19.12 (10.202.19.12) 56(84) bytes of data.
64 bytes from 10.202.19.12: icmp_seq=1 ttl=64 time=0.551 ms
64 bytes from 10.202.19.12: icmp_seq=2 ttl=64 time=0.600 ms
^C --- 10.202.19.12 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1028ms
rtt min/avg/max/mdev = 0.551/0.575/0.600/0.024 ms
test@232-22:~$ ping 10.202.0.94
PING 10.202.0.94 (10.202.0.94) 56(84) bytes of data.
64 bytes from 10.202.0.94: icmp_seq=1 ttl=64 time=0.550 ms
64 bytes from 10.202.0.94: icmp_seq=2 ttl=64 time=0.559 ms
^C --- 10.202.0.94 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1012ms

```

Maintenant je vais voir le status de mon pare-feu avec la commande:  
**systemctl status pve-firewall.service**



On voit avec la commande `pve-firewall status` que le service firewall est bien en cours d'exécution mais il est désactivé (aucune règle de pare-feu n'est activé).

```
root@pve3:~# pve-firewall status
Status: disabled/running
root@pve3:~#
```

Dans la zone Datacenter, le firewall n'est pas activé

The screenshot shows the Proxmox VE interface. On the left, the 'Server View' sidebar lists nodes: pve1, pve2, and pve3. pve1 contains hosts 101 (CentosMini), local (pve1), local-lvm (pve1), and storageceph (pve1). pve3 contains hosts 100 (opensense), 102 (CentosTemplate), 103 (ubuntu), local (pve3), local-lvm (pve3), and storageceph (pve3). The main panel is titled 'Datacenter' and shows the 'Edit' configuration for the 'Firewall' section. The 'Firewall' tab is selected, showing the following settings:

Firewall	No
eBtables	Yes
Log rate limit	Default (enable=1,rate1/second,burst=5)
Input Policy	DROP
Output Policy	ACCEPT

The sidebar on the right lists various management options: Ceph, Options, Storage, Backup, Replication, Permissions (Users, API Tokens, Two Factor, Groups, Pools, Roles, Realms), HA, ACME, Firewall, Options, and Security Group. The 'Firewall' option is highlighted with an orange arrow.

Maintenant on va configurer les 2 règles prioritaires sur le pare-feu.

The screenshot shows the 'Firewall' configuration screen. The left sidebar is identical to the previous one. The main area displays a table of firewall rules. At the top of the table, there are buttons: 'Add' (highlighted with an orange arrow), 'Copy', 'Insert: Security Group', 'Remove', and 'Edit'. The table columns are: On, Type, Action, Macro, Interface, and Protocol. The first rule listed is:

On	Type	Action	Macro	Interface	Protocol

The sidebar on the right includes the 'Status: stopped' status indicator, followed by the same management options as before: Ceph, Options, Storage, Backup, Replication, Permissions (Users, API Tokens, Two Factor, Groups, Pools, Roles, Realms), HA, ACME, Firewall, Options, and Security Group. The 'Firewall' option is again highlighted with an orange arrow.

On va accepter tout trafic entrant vers le port 8006 (le port d'écoute pour accéder à l'interface web), protocole TCP.

Afin de rendre actif la nouvelle règle , on n'oublie pas de cocher “enable”

Add: Rule

Direction:	in	Enable:	<input checked="" type="checkbox"/>
Action:	ACCEPT	Macro:	
Interface:		Protocol:	tcp
Source:		Source port:	
Destination:		Dest. port:	8006
Comment:			
Log level:	nolog		
<input type="checkbox"/> Advanced <input checked="" type="checkbox"/> Add			

On fait de même pour le protocole SSH: port de destination 22

Add: Rule

Direction:	in	Enable:	<input checked="" type="checkbox"/>
Action:	ACCEPT	Macro:	
Interface:		Protocol:	tcp
Source:		Source port:	
Destination:		Dest. port:	22
Comment:			
Log level:	nolog		
<input type="checkbox"/> Advanced <input checked="" type="checkbox"/> Add			

Afin d'activer le pare-feu, on vient dans:

Replication

Permissions

Users

API Tokens

Two Factor

Groups

Pools

Roles

Realms

HA

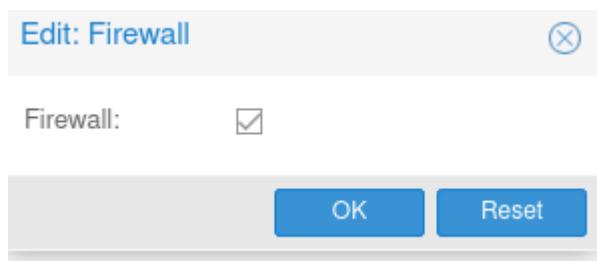
ACME

Firewall

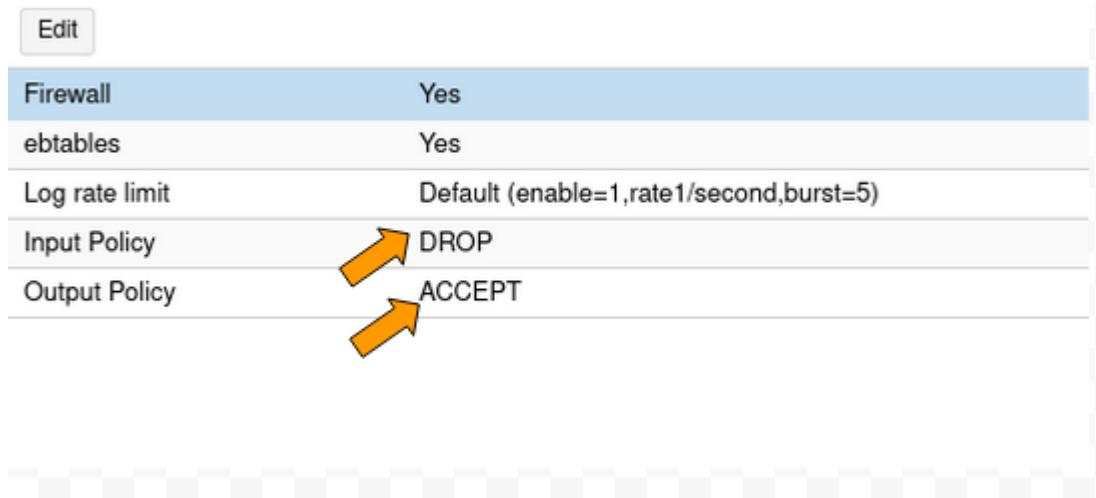
Options

Security Group

	Edit
Firewall	No
ebtables	Yes
Log rate limit	Default (enable=1,rate1/sec)
Input Policy	DROP
Output Policy	ACCEPT



Maintenant tout trafic entrant ne correspondant pas à ces 2 règles sont rejettés mais tout trafic sortant est accepté



Si je refais la même commande comme précédemment sur mon hôte je vois que le pare-feu est en cours d'exécution avec des règles activés

```
root@pve3:~# pve-firewall status
Status: enabled/running
root@pve3:~#
```

Et maintenant si je refais un ping depuis mon ordinateur vers le PROXMOX on remarque que ça ne passe plus car le ping ne faisait pas partie des règles.

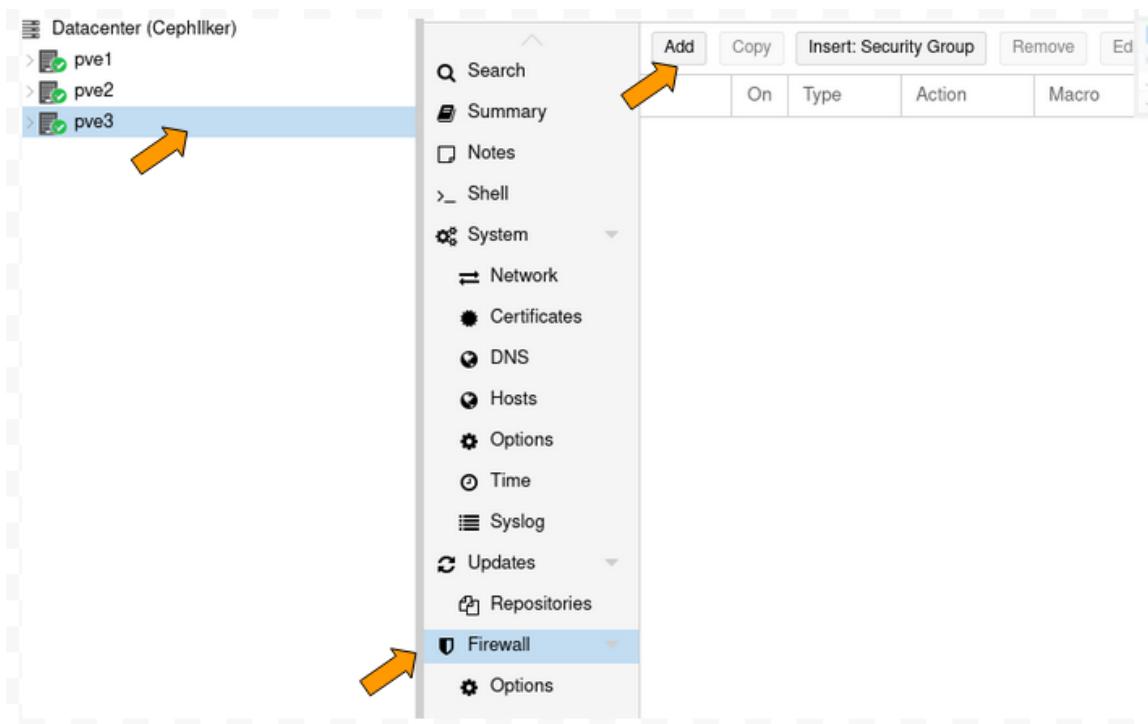
```
root@232-22:/home/test# ping 10.202.19.12
PING 10.202.19.12 (10.202.19.12) 56(84) bytes of data.
^C
--- 10.202.19.12 ping statistics ---
26 packets transmitted, 0 received, 100% packet loss, time 25589ms
root@232-22:/home/test#
```

Mais pour les 2 VM la liaison marche

```
root@232-22:/home/test# ping 10.202.19.7
PING 10.202.19.7 (10.202.19.7) 56(84) bytes of data.
64 bytes from 10.202.19.7: icmp_seq=1 ttl=64 time=0.747 ms
64 bytes from 10.202.19.7: icmp_seq=2 ttl=64 time=0.509 ms
^C
--- 10.202.19.7 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1009ms
rtt min/avg/max/mdev = 0.509/0.620/0.747/0.119
```

Pour autoriser le ping, on va ajouter une règle.

J'effectue la même démarche mais cette fois ci sur l'hôte



Je précise l'adresse de mon PC: 10.202.8.1

Add: Rule

Direction:	in	Enable:	<input checked="" type="checkbox"/>
Action:	ACCEPT	Macro:	Ping
Interface:		Protocol:	
Source:	10.202.8.1	Source port:	
Destination:		Dest. port:	
Comment:			
Log level:	nolog		
<input type="checkbox"/> Advanced <input type="button" value="Add"/>			

arch mmary tes ell stem	<input type="button" value="Add"/> <input type="button" value="Copy"/> <input type="button" value="Insert: Security Group"/> <input type="button" value="Remove"/> <input type="button" value="Edit"/>									
	On	Type	Action	Macro	Interface	Protocol	Source	S.Port	Des	
	≡ 0	<input checked="" type="checkbox"/>	in	ACCEPT	Ping				10.202.8.1	

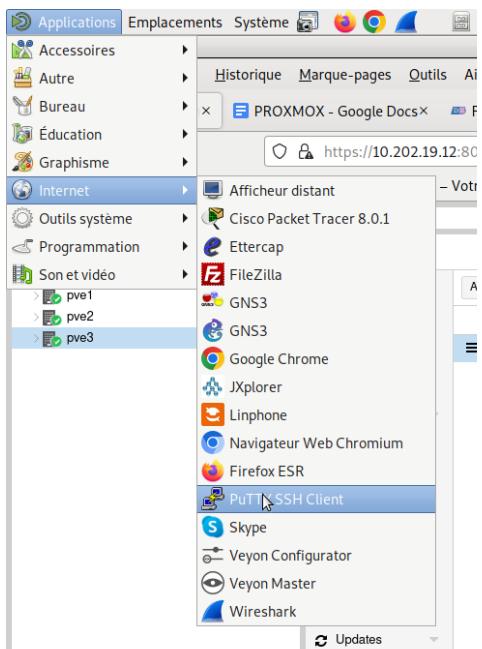
On voit que maintenant le ping marche

```

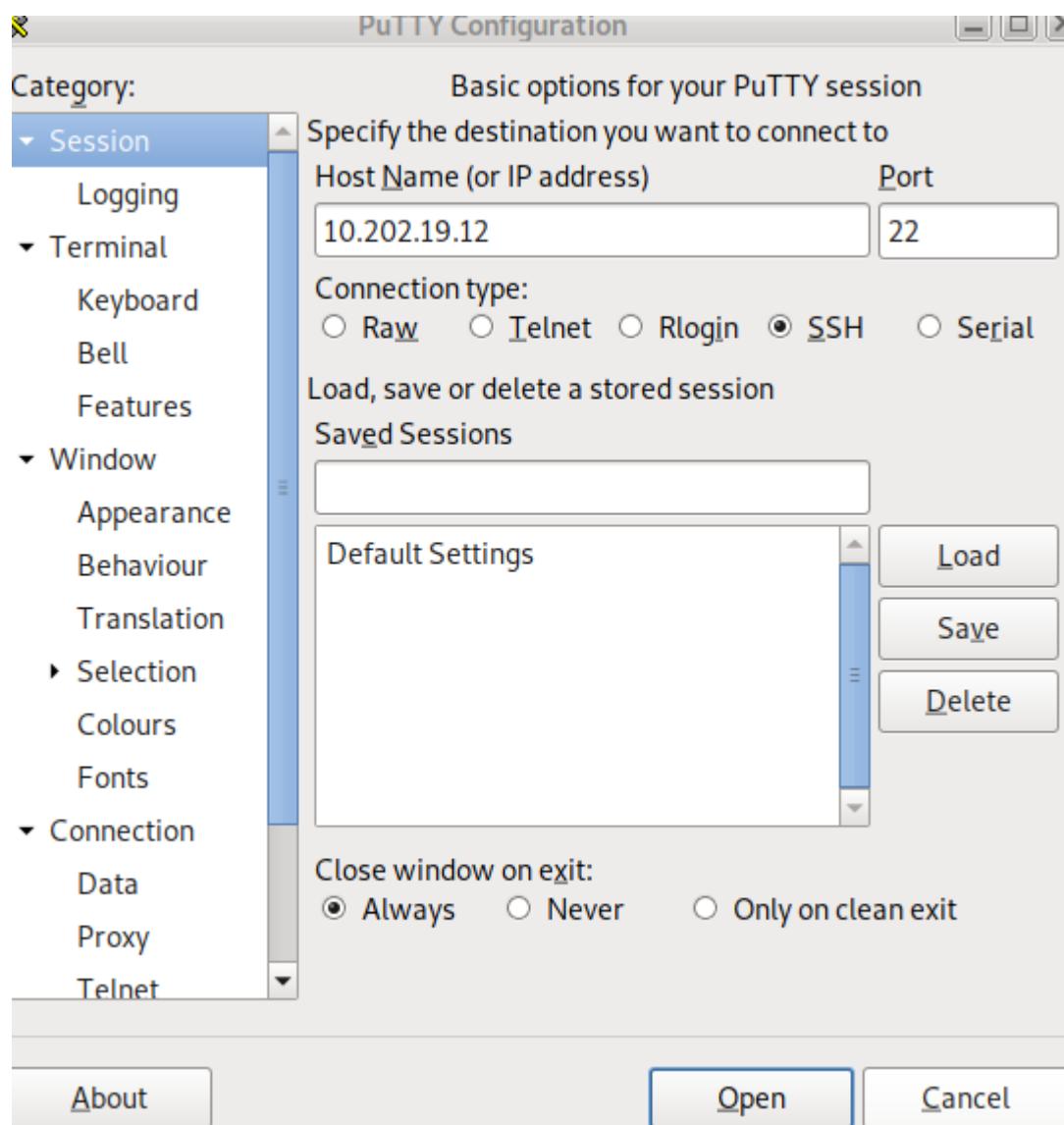
root@232-22:/home/test# ping 10.202.19.12
PING 10.202.19.12 (10.202.19.12) 56(84) bytes of data.
64 bytes from 10.202.19.12: icmp_seq=1 ttl=64 time=0.491 ms
64 bytes from 10.202.19.12: icmp_seq=2 ttl=64 time=0.607 ms
64 bytes from 10.202.19.12: icmp_seq=3 ttl=64 time=0.590 ms
^C
--- 10.202.19.12 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2056ms
rtt min/avg/max/mdev = 0.491/0.562/0.607/0.051 ms
root@232-22:/home/test#

```

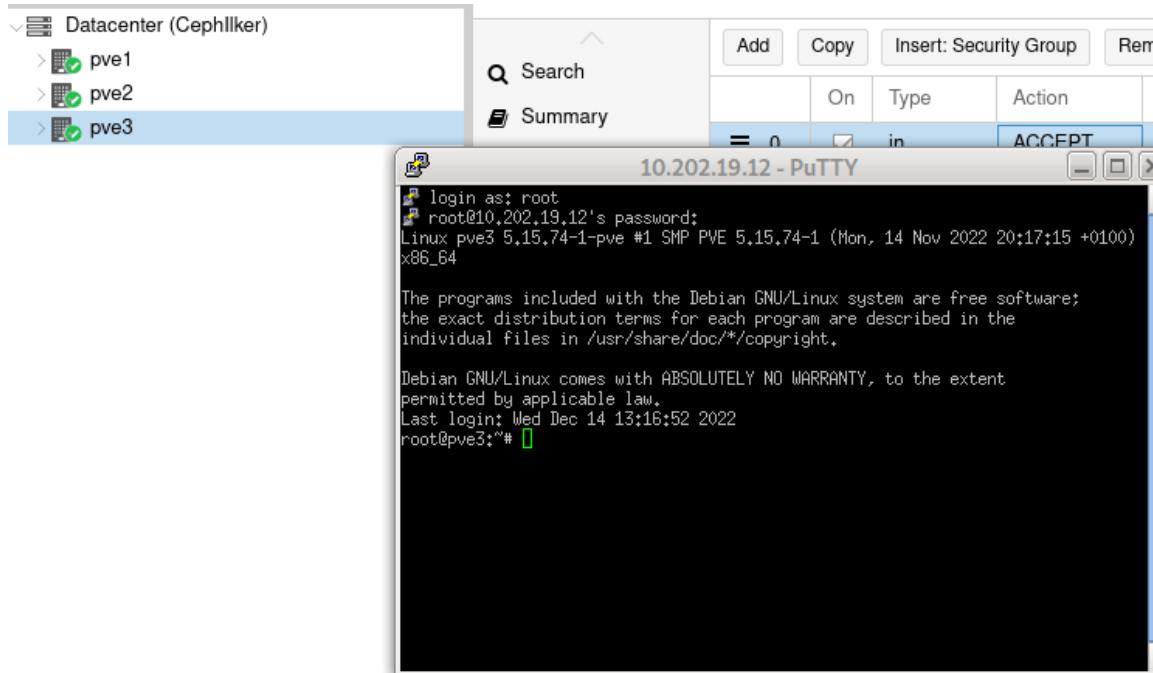
Essayons d'utiliser le protocole SSH maintenant. Pour cela j'utilise le client Putty



Je mets l'adresse IP de mon PROXMOX



On voit bien que j'arrive à accéder à mon serveur



Pour protéger mes VM, aussi j'active juste le Pare-feu dans OPTIONS, puis je fais EDIT

	Value
Firewall	Yes
DHCP	Yes
NDP	Yes
Router Advertisement	No
MAC filter	Yes
IP filter	No
log_level_in	nolog
log_level_out	nolog
Input Policy	DROP
Output Policy	ACCEPT

J'essaye maintenant d'accéder dans le dossier /etc/pve/firewall dans mon hôte.

Et je vois qu'il y a 2 fichiers

- le 100.fw: qui contient les règles du pare-feu configurer pour la vm dont l'ID est 100

- Le cluster/fw: inclut la configuration à l'échelle du cluster pour notre pare-feu.

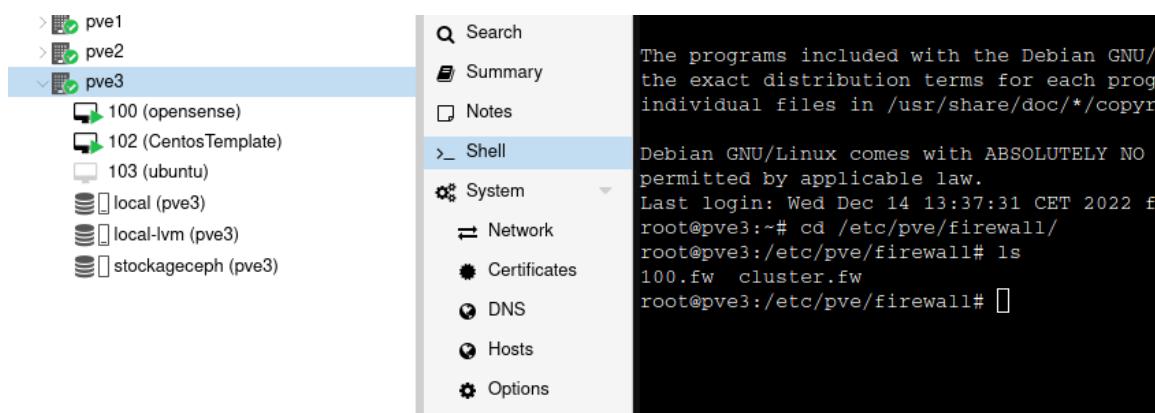
```
root@pve3:/etc/pve/firewall# cat cluster/fw
[OPTIONS]

enable: 1

[RULES]

IN ACCEPT -p tcp -dport 22 -log nolog
IN ACCEPT -p tcp -dport 8006 -log nolog

root@pve3:/etc/pve/firewall# 
```



## E/Quelques commandes utiles pour PROXMOX

- Pour lister les VM: `qm list`

```
root@pve3:~# qm list
    VMID NAME          STATUS     MEM (MB)   BOOTDISK (GB) PID
      100 opensense    running    4096           32.00 2756
      102 CentosTemplate running    8112             8.00 2831
      103 ubuntu       stopped    2048           32.00 0
root@pve3:~# 
```

- Pour arrêter une VM: `qm stop [ID_du_VM]`
- Pour afficher la somme de mémoire allouée aux VM et aux CT: `grep -R memory /etc/pve/local | awk '{sum += $NF } END {print sum;}'`

```
root@pve3:~# grep -R memory /etc/pve/local | awk '{sum += $NF } END {print sum}
```

14256

```
root@pve3:~#
```

- Pour afficher la liste triée des vmid: `cat /etc/pve/.vmplist | grep node | cut -d ":" -f2 | sort -n`

```
14256
root@pve3:~# cat /etc/pve/.vmplist | grep node | cut -d ":" -f2 | sort -n
100
101
102
103
root@pve3:~#
```

- Pour afficher la liste triée des machines virtuelles comme le type vmid proxmox\_host: `cat /etc/pve/.vmplist | grep node | tr -d ":"| awk '{print $1" "$4" "$6 }' | sort -n | column -t`

```
root@pve3:~# cat /etc/pve/.vmplist | grep node | tr -d ":"| awk '{print $1" "$4" "$6 }' | sort -n | column -t
100 pve3 qemu
101 pve1 qemu
102 pve3 qemu
103 pve3 qemu
root@pve3:~#
```

- Pour afficher la liste triée des machines virtuelles comme vmid proxmox\_host type vm\_name: `for i in $(cat /etc/pve/.vmplist | grep node | cut -d ":" -f2 | sort -n);do NAME=$(grep -R 'name:' /etc/pve/nodes/*/*/$i.conf | awk {'print $2'}); INFO=$(grep $i /etc/pve/.vmplist | grep node | tr -d ":"| awk '{print $1"\t$4"\t$6 }'); printf "%s\t%s\n" "$INFO" "$NAME" ;done`

```
root@pve3:~# for i in $(cat /etc/pve/.vmplist | grep node | cut -d ":" -f2 | sort -n);do NAME=$(grep -R 'name:' /etc/pve/nodes/*/*/$i.conf | awk {'print $2'}); INFO=$(grep $i /etc/pve/.vmplist | grep node | tr -d ":"| awk '{print $1"\t$4"\t$6 }'); printf "%s\t%s\n" "$INFO" "$NAME" ;done
100 pve3 qemu opensense
101 pve1 qemu CentosMini
102 pve3 qemu CentosTemplate
103 pve3 qemu ubuntu
root@pve3:~#
```

- Pour savoir la mémoire d'une VM: `qm config 100 | grep ^memory`

```
root@pve3:~# qm config 100 | grep ^memory
memory: 4096
root@pve3:~#
```

- Pour voir la version: **pveversion**

```
USAGE: pveversion [--verbose]
root@pve3:~# pveversion
pve-manager/7.3-3/c3928077 (running kernel: 5.15.74-1-pve
root@pve3:~#
```

Pour mettre à niveau un nœud Proxmox, utilisez la commande suivante: **pveupgrade**

```
root@pve3:~# pveupgrade
Starting system upgrade: apt-get dist-upgrade
error reading cached package status in /var/lib/pve-manager/pkgupdates
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.

Your System is up-to-date

root@pve3:~#
```

Pour vérifier les performances du nœud Proxmox, utilisez la commande suivante : **pveperf**

```
pvesh ls <api_path> [OPTIONS] [FORMAT_OPTIONS]
root@pve3:~# pveperf
CPU BOGOMIPS:      191644.16
REGEX/SECOND:      3045181
HD SIZE:           93.93 GB (/dev/mapper/pve
BUFFERED READS:    535.12 MB/sec
AVERAGE SEEK TIME: 0.07 ms
FSYNCS/SECOND:     7461.11
DNS EXT:           46.43 ms
DNS INT:           0.37 ms (iutbeziers.fr)
root@pve3:~#
```

Pour créer un cluster: **pvecm create <cluster\_name>**

Pour vérifier l'état du cluster Proxmox : **pvecm statut**

```

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, t
permitted by applicable law.
Last login: Wed Dec 14 14:06:03 CET 2022 on pts/1
root@pve3:~# pvecm status
Cluster information
-----
Name: CephHilker
Config Version: 3
Transport: knet
Secure auth: on

Quorum information
-----
Date: Wed Dec 14 14:35:17 2022
Quorum provider: corosync_votequorum
Nodes: 2
Node ID: 0x00000003
Ring ID: 1.2f
Quorate: Yes

Votequorum information
-----
Expected votes: 3
Highest expected: 3
Total votes: 2
Quorum: 2
Flags: Quorate

Membership information
-----
  Nodeid   Votes Name
0x00000001      1 10.202.19.10
0x00000003      1 10.202.19.12 (local)
root@pve3:~#

```

Pour ajouter un nœud au cluster Proxmox :`pvecm add <ip_of_existing_node>`

Pour afficher une liste des nœuds Proxmox :`pvecm nodes`

```

root@pve3:~# pvecm nodes

Membership information
-----
  Nodeid   Votes Name
    1      1 pve1
    3      1 pve3 (local)
root@pve3:~#

```

Pour voir une liste des stockages attachés avec Proxmox :

```

root@pve3:~# pvesm status
Name          Type    Status     Total        Used       Available      %
local         dir     active    98497780    5715500    87732732    5.80%
local-lvm     lvmthin active   389967872    7331395    382636476    1.88%
stockageceph  rbd     active   619833193    2886441    616946752    0.47%
root@pve3:~#

```

## E/ PROXMOX vs VMWare

<u>PROXMOX</u>	<u>VMware</u>
<b>Licence Libre [support payant possible]</b>	<b>Licence payante et chères [vSphere, vSAN, vCSA, NSX, Tanzu-kubernetes]</b>
<b>Basé sur Debian Linux KVM</b>	<b>Basé sur VMKernel</b>
<b>Support maximum de CPUs 768</b>	<b>Support maximum des CPUs 768</b>
<b>Mémoire maximale supportée 12TB</b>	<b>Mémoire maximale supportée 24TB</b>
<b>32 hôtes par cluster (maximum)</b>	<b>96 hôtes par cluster (maximum)</b>
<b>L'interface graphique de Proxmox est encore en évolution et il manque certaines options de configuration avancées via l'interface graphique.</b>	<b>Le client web VSphere est assez intuitif et permet une configuration avancée via une interface graphique.</b>
<b>N'importe quel nœud de PROXMOX peut gérer une grappe, ce qui est une flexibilité agréable à avoir au cas où le nœud maître tomberait en panne</b>	<b>Nécessite un nœud maître pour un clustering et un HA fiables</b>
<b>Stockage distribué [CEPH]</b>	<b>Stockage distribué [vSAN]</b>
<b>Infrastructure Hyper-Convergée [CEPH]</b>	<b>Infrastructure Hyper-Convergée [vSAN]</b>

<b>Firewall (VM, hôtes et clusters) ==&gt; Sans licence</b>	<b>Firewall (VM, hôtes et clusters) ==&gt; Licence supplémentaire</b>
<b>Équilibrage de charge: DRS</b>	<b>Équilibrage de charge: Non</b>
<b>Utilise le firewall de LINUX</b>	
<b>Console graphique de gestion ==&gt; intégrée sur tous les noeuds</b>	<b>Console graphique de gestion ==&gt; VM dédiée</b>
<b>Possibilité de sauvegarder l'enveloppe VM et le contenu</b>	<b>Pas la possibilité de sauvegarder l'enveloppe VM et le contenu</b>
<b>Back-ends de stockage [NFS, SMB/CIFS, GlusterFS, RBD, CephFS,ZFS,iSCSI</b>	<b>Back-ends de stockage [NFS, vSAN, iSCSI, FC]</b>
<b>Aucune exigences sur le matériel</b>	<b>Très fortes exigences sur le matériel (matrice de compatibilité exigeante)</b>
<b>Conteneurs: LXC (sans licence)</b>	<b>Conteneurs: LXC (Licence supplémentaire)</b>