



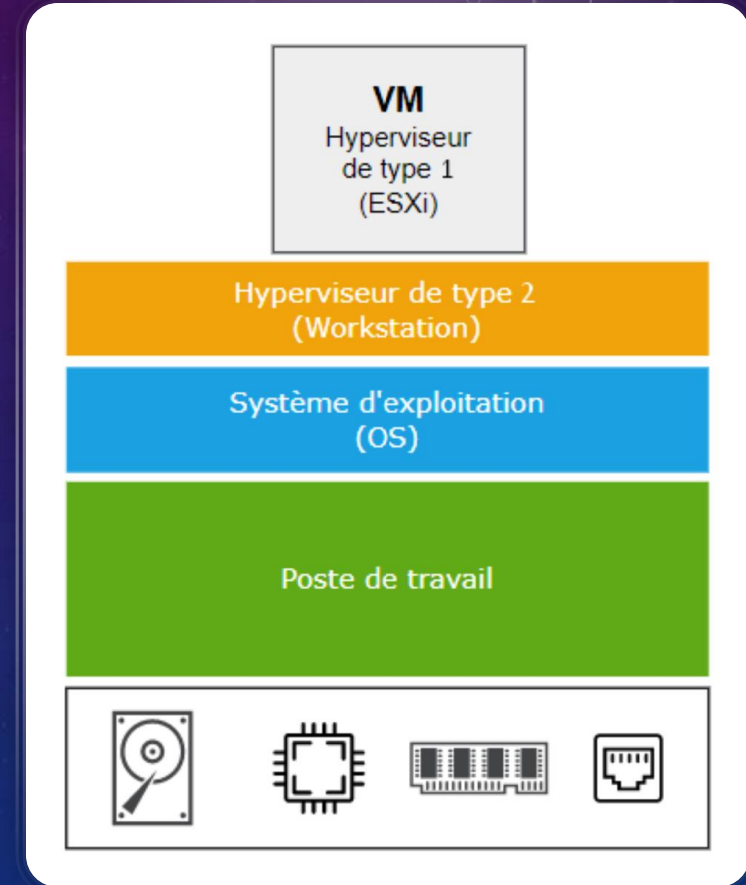
DÉPLOYER UNE INFRASTRUCTURE RÉSEAU HUB AND SPOKE AVEC FW (PSFENSE)

PRISCILLA - RIM - VIRGINIE

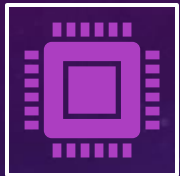
FRANCOIS - NACIM

À QUOI SERT LA VIRTUALISATION IMBRIQUÉE

- La virtualisation imbriquée, également connue sous le nom de virtualisation de deuxième niveau, est un concept dans lequel une machine virtuelle (VM) exécutant un hyperviseur est elle-même utilisée pour exécuter d'autres machines virtuelles. En d'autres termes, au lieu d'exécuter directement un système d'exploitation sur le matériel physique, vous exécutez un hyperviseur qui à son tour exécute d'autres machines virtuelles.
- La virtualisation imbriquée est souvent utilisée dans les scénarios de test et de développement, ainsi que dans les environnements de laboratoire.



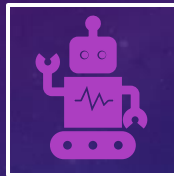
QUELQUES CAS D'UTILISATION ET AVANTAGES DE LA VIRTUALISATION IMBRIQUÉE :



Tests et développement : La virtualisation imbriquée permet aux développeurs et aux testeurs de créer des environnements isolés pour tester des logiciels ou des configurations réseau sans avoir besoin de matériel physique dédié pour chaque cas d'utilisation. Cela permet d'économiser du temps et des ressources.



Formation : Les environnements virtuels imbriqués sont souvent utilisés pour la formation, car ils permettent aux étudiants d'expérimenter avec différentes configurations et systèmes d'exploitation sans risque pour les machines physiques.



Isolation : En exécutant des machines virtuelles dans un environnement virtualisé, vous pouvez isoler chaque machine virtuelle les unes des autres, ce qui permet de limiter les risques de conflits ou de dommages causés par une machine virtuelle à une autre.



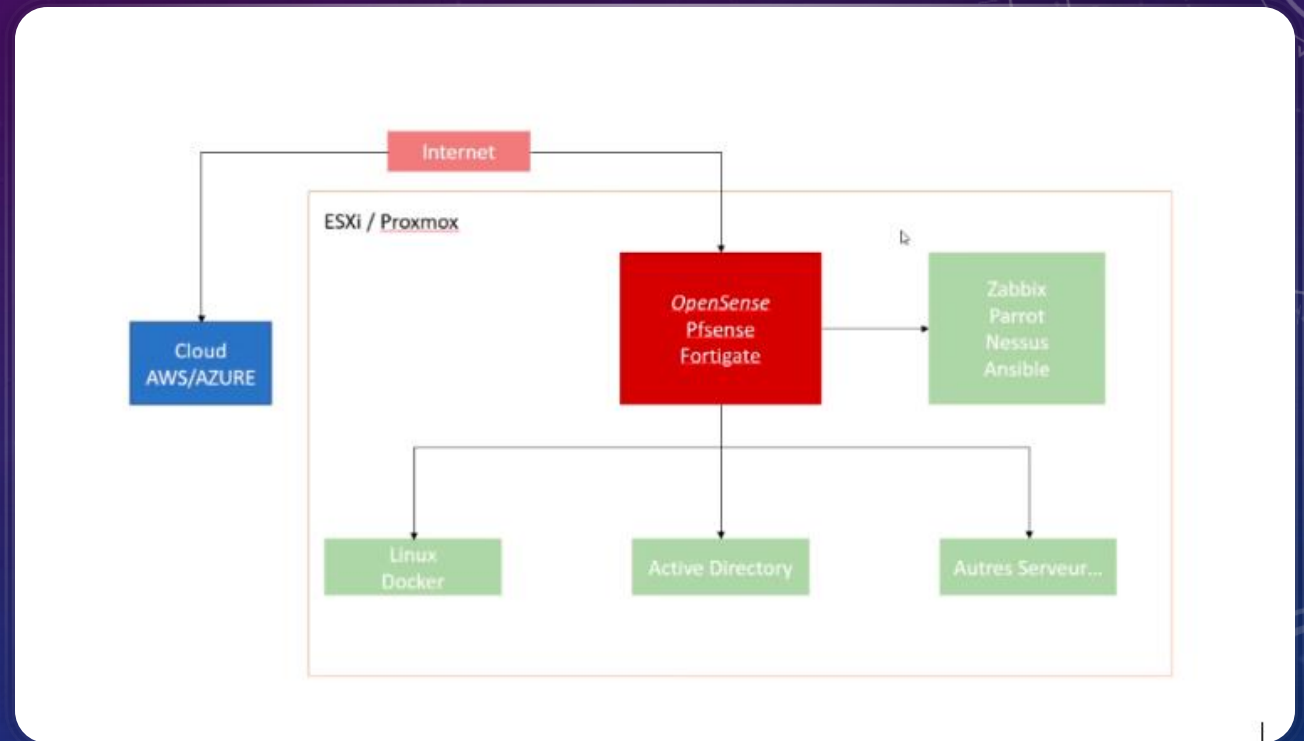
Déploiement rapide : La création de machines virtuelles à l'intérieur d'un environnement virtualisé est souvent plus rapide que le déploiement de machines physiques, ce qui permet de mettre en place des environnements de test et de développement rapidement et facilement.



Expérimentation et innovation : La virtualisation imbriquée permet aux utilisateurs d'expérimenter avec différentes configurations matérielles et logicielles, ce qui favorise l'innovation et l'exploration de nouvelles idées.

CONTEXTE

- Mise en place d'une architecture en étoile (hub en spoke).
- Virtualisation de machines dans un hyperviseur de type 1.
- Implémentation de pfsense comme point central du réseau pour gérer le trafic entre les différents serveurs. Il agira comme un concentrateur.



QU'EST-CE QUE ESXI ?

ESXI est un hyperviseur de type 1, qui s'exécute directement sur le matériel serveur sans nécessiter un système d'exploitation sous-jacent.

Il permet la création, la gestion et l'exécution de machines virtuelles.

Il offre une sécurité accrue et une performance optimisée grâce à son architecture minimaliste.

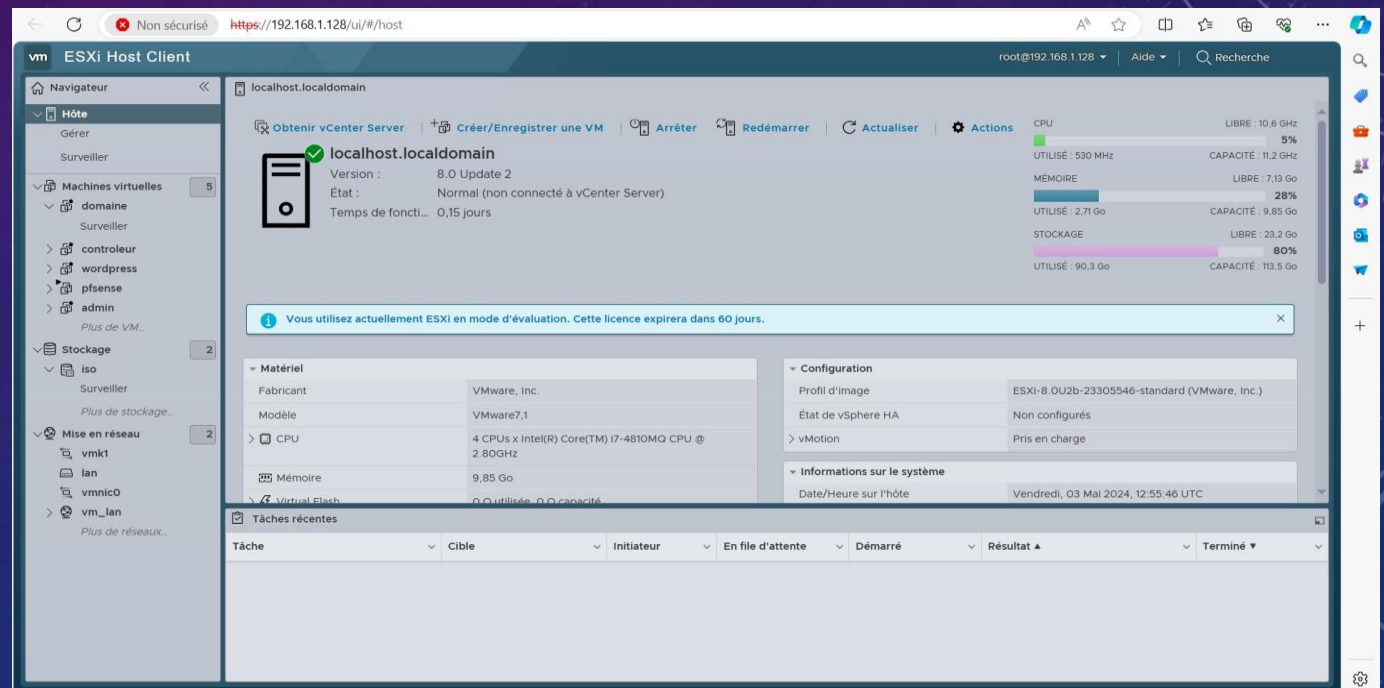
Géré via vCenter Server de VMware, qui permet une administration centralisée des ressources et des machines virtuelles.

Disponible en plusieurs éditions, certaines gratuites avec des fonctionnalités limitées et d'autres plus avancées nécessitant des licences.

INSTALLATION DE ESXI

Création d'un compte sur vmware et téléchargement de l'iso version 8.

Installation de l'iso sur Vmware.



CONFIGURATION REQUISES POUR ESXI

Configuration requises pour ESXI :

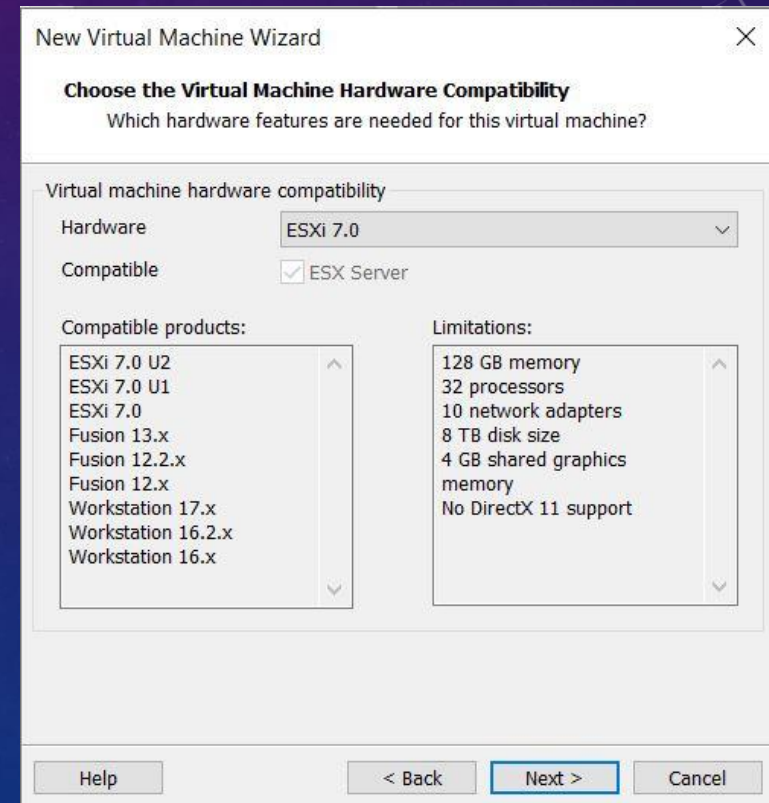
Ajout d'un disque dur de 100 GB pour les iso des vm et leur installation.

Problèmes rencontrés :

Cocher la case Intel VT -x/EPT pour lancer les vm et la virtualisation du processeur.

Virtualization engine

- ☒ Virtualize Intel VT-x/EPT or AMD-V/RVI
- ☐ Virtualize CPU performance counters
- ☐ Virtualize IOMMU (IO memory management unit)



The screenshot shows the 'New Virtual Machine Wizard' window, specifically the 'Choose the Virtual Machine Hardware Compatibility' step. The window title is 'New Virtual Machine Wizard'. Below the title bar, the text reads 'Choose the Virtual Machine Hardware Compatibility' and 'Which hardware features are needed for this virtual machine?'. The 'Virtual machine hardware compatibility' section has a 'Hardware' dropdown menu set to 'ESXi 7.0' and a 'Compatible' checkbox labeled 'ESX Server' which is checked. Below this, there are two lists: 'Compatible products:' and 'Limitations:'. The 'Compatible products:' list includes ESXi 7.0 U2, ESXi 7.0 U1, ESXi 7.0, Fusion 13.x, Fusion 12.2.x, Fusion 12.x, Workstation 17.x, Workstation 16.2.x, and Workstation 16.x. The 'Limitations:' list includes 128 GB memory, 32 processors, 10 network adapters, 8 TB disk size, 4 GB shared graphics memory, and No DirectX 11 support. At the bottom of the window, there are buttons for 'Help', '< Back', 'Next >', and 'Cancel'.

New Virtual Machine Wizard

Choose the Virtual Machine Hardware Compatibility
Which hardware features are needed for this virtual machine?

Virtual machine hardware compatibility

Hardware: ESXi 7.0

Compatible: ☒ ESX Server

Compatible products:

- ESXi 7.0 U2
- ESXi 7.0 U1
- ESXi 7.0
- Fusion 13.x
- Fusion 12.2.x
- Fusion 12.x
- Workstation 17.x
- Workstation 16.2.x
- Workstation 16.x

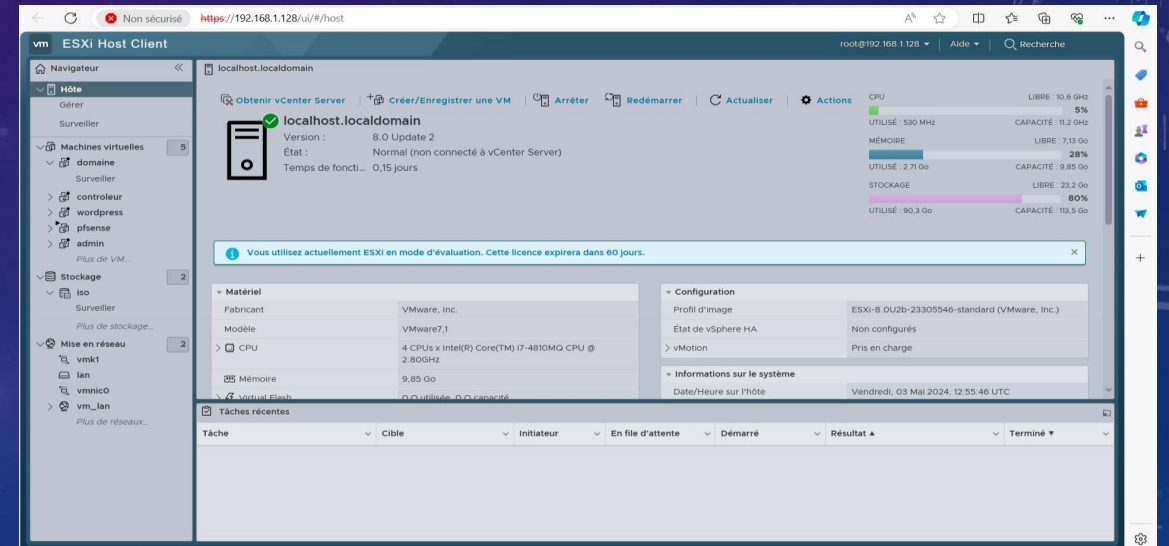
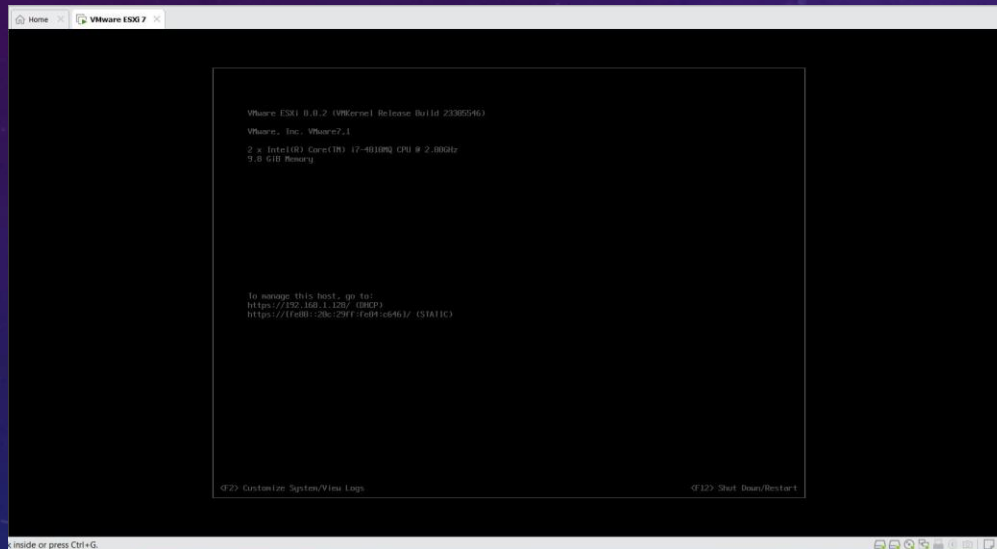
Limitations:

- 128 GB memory
- 32 processors
- 10 network adapters
- 8 TB disk size
- 4 GB shared graphics memory
- No DirectX 11 support

Help < Back Next > Cancel

CONNEXION A ESXI

Connexion sur `http :// 192.168.1.128`



VM ADMIN

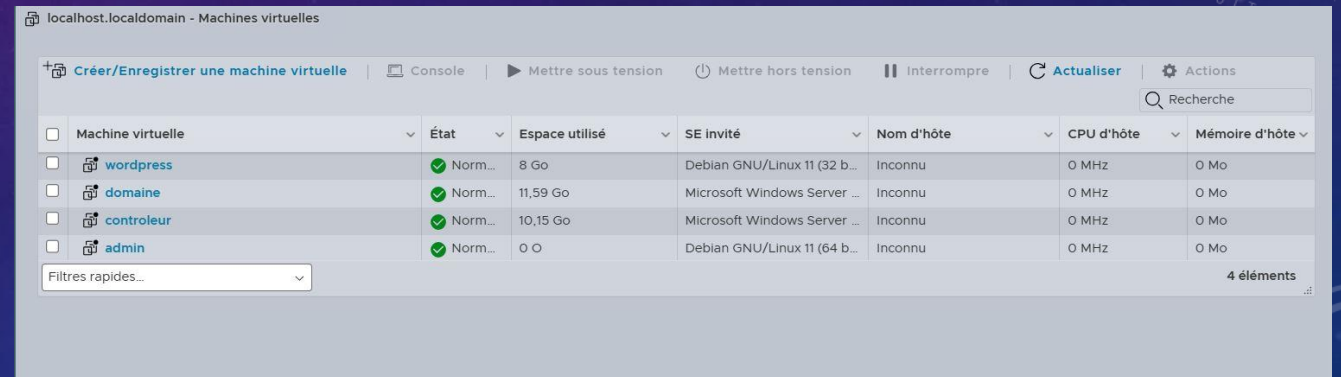
Installation du Serveur Debian 12 à partir d'un fichier ISO.

Il est connecté à pfSense et il est responsable de l'administration du système.

IP : 192.168.1.98

Configurations :

- Configuration d'un serveur SSH
- Configuration d'un serveur d'automatisation Ansible et ajout du client Wordpress avec test
- Ajout de tous les hôtes dans le fichier /etc/hosts et configuration du DNS Active Directory
- Déploiement du playbook sur le serveur client Debian "Wordpress" (HTTP)
- Ajout d'un pare-feu ufw avec une politique stricte
- Ajout d'un outil de supervision NETDATA



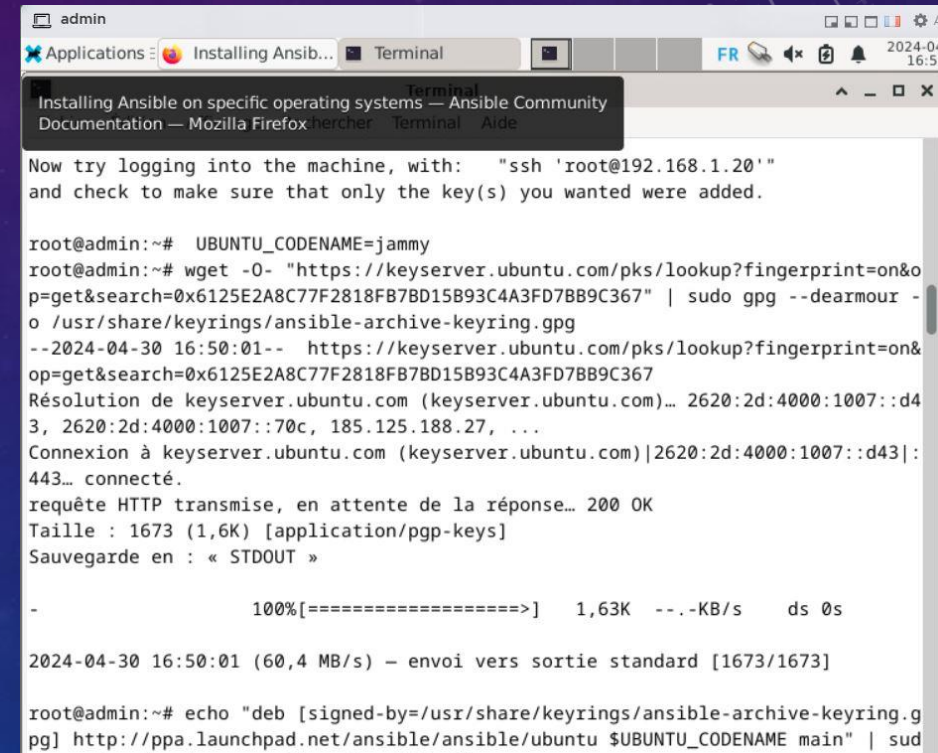
The screenshot shows the Proxmox VE web interface for managing virtual machines. The title bar indicates 'localhost.localdomain - Machines virtuelles'. The top navigation bar includes buttons for 'Créer/Enregistrer une machine virtuelle', 'Console', 'Mettre sous tension', 'Mettre hors tension', 'Interrompre', 'Actualiser', and 'Actions'. A search bar is also present. The main table lists four virtual machines with columns for checkboxes, names, status, disk space, SE invited, host name, CPU, and memory. All machines are in a 'Norm...' (Normal) state.

<input type="checkbox"/>	Machine virtuelle	État	Espace utilisé	SE invité	Nom d'hôte	CPU d'hôte	Mémoire d'hôte
<input type="checkbox"/>	wordpress	✓ Norm...	8 Go	Debian GNU/Linux 11 (32 b...	Inconnu	0 MHz	0 Mo
<input type="checkbox"/>	domaine	✓ Norm...	11,59 Go	Microsoft Windows Server ...	Inconnu	0 MHz	0 Mo
<input type="checkbox"/>	controleur	✓ Norm...	10,15 Go	Microsoft Windows Server ...	Inconnu	0 MHz	0 Mo
<input type="checkbox"/>	admin	✓ Norm...	0 O	Debian GNU/Linux 11 (64 b...	Inconnu	0 MHz	0 Mo

At the bottom of the table, there is a 'Filtres rapides...' dropdown menu and a note indicating '4 éléments'.

ANSIBLE

Ansible est un outil d'automatisation open-source utilisé pour la gestion de la configuration, le déploiement d'applications, et l'orchestration de tâches informatiques. Il utilise une architecture simple et sans agent, se fiant principalement à SSH pour se connecter aux serveurs et exécuter les configurations.



```
admin
Applications Installing Ansib... Terminal
Installing Ansible on specific operating systems — Ansible Community
Documentation — Mozilla Firefox hercher Terminal Aide

Now try logging into the machine, with: "ssh 'root@192.168.1.20'"
and check to make sure that only the key(s) you wanted were added.

root@admin:~# UBUNTU_CODENAME=jammy
root@admin:~# wget -O- "https://keyserver.ubuntu.com/pks/lookup?fingerprint=on&
p=get&search=0x6125E2A8C77F2818FB7BD15B93C4A3FD7BB9C367" | sudo gpg --dearmour -
o /usr/share/keyrings/ansible-archive-keyring.gpg
--2024-04-30 16:50:01-- https://keyserver.ubuntu.com/pks/lookup?fingerprint=on&
op=get&search=0x6125E2A8C77F2818FB7BD15B93C4A3FD7BB9C367
Résolution de keyserver.ubuntu.com (keyserver.ubuntu.com)... 2620:2d:4000:1007::d4
3, 2620:2d:4000:1007::70c, 185.125.188.27, ...
Connexion à keyserver.ubuntu.com (keyserver.ubuntu.com)|2620:2d:4000:1007::d43|:
443... connecté.
requête HTTP transmise, en attente de la réponse... 200 OK
Taille : 1673 (1,6K) [application/pgp-keys]
Sauvegarde en : « STDOUT »

- 100%[=====] 1,63K --.-KB/s ds 0s

2024-04-30 16:50:01 (60,4 MB/s) – envoi vers sortie standard [1673/1673]

root@admin:~# echo "deb [signed-by=/usr/share/keyrings/ansible-archive-keyring.g
pg] http://ppa.launchpad.net/ansible/ansible/ubuntu $UBUNTU_CODENAME main" | sud
```

PARE-FEU UFW

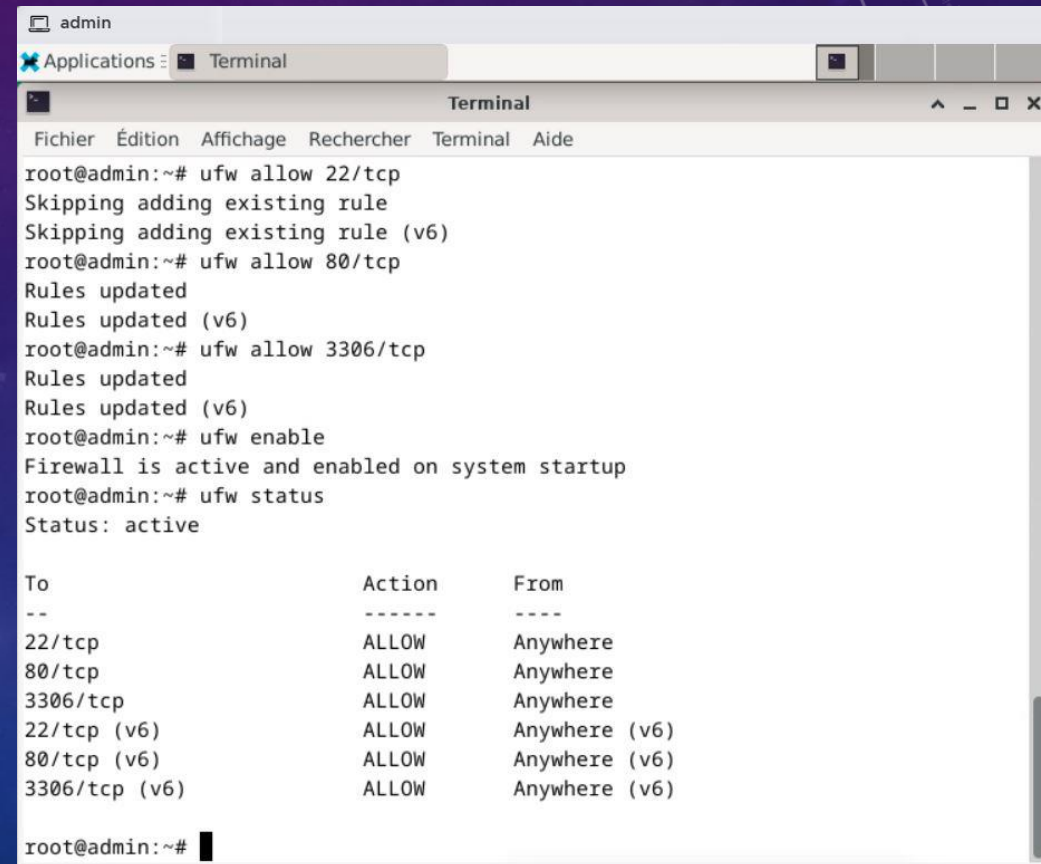
UFW est un outil de configuration de pare-feu pour les iptables qui est inclus dans Ubuntu par défaut.

Autorisations :

SSH port 22

HTTP port 80

MySQL port 3306

A terminal window titled 'admin' with a menu bar containing 'Applications', 'Terminal', and a search icon. The terminal shows a series of commands and their outputs for configuring UFW. The commands are: 'ufw allow 22/tcp', 'ufw allow 80/tcp', 'ufw allow 3306/tcp', 'ufw enable', and 'ufw status'. The outputs show that rules are being added or updated, and the firewall is successfully enabled. At the bottom, a table displays the current rules.

```
admin
Applications Terminal
Terminal
Fichier Édition Affichage Rechercher Terminal Aide
root@admin:~# ufw allow 22/tcp
Skipping adding existing rule
Skipping adding existing rule (v6)
root@admin:~# ufw allow 80/tcp
Rules updated
Rules updated (v6)
root@admin:~# ufw allow 3306/tcp
Rules updated
Rules updated (v6)
root@admin:~# ufw enable
Firewall is active and enabled on system startup
root@admin:~# ufw status
Status: active

To Action From
--
22/tcp ALLOW Anywhere
80/tcp ALLOW Anywhere
3306/tcp ALLOW Anywhere
22/tcp (v6) ALLOW Anywhere (v6)
80/tcp (v6) ALLOW Anywhere (v6)
3306/tcp (v6) ALLOW Anywhere (v6)

root@admin:~#
```


NETDATA

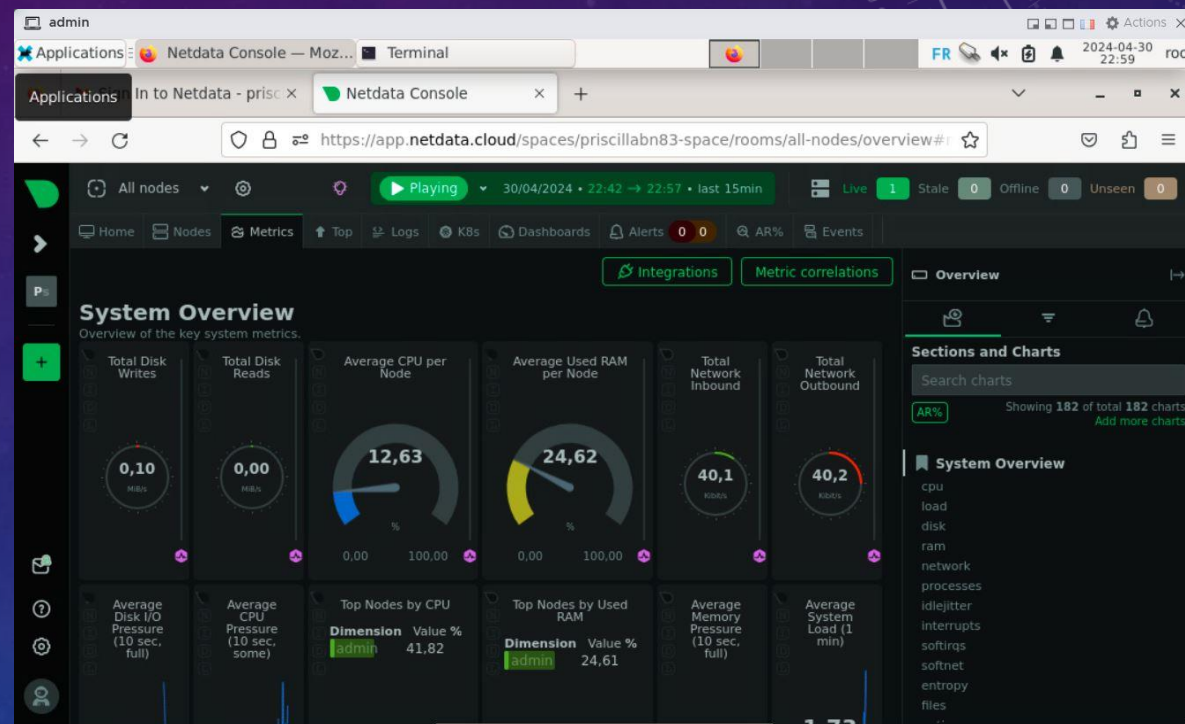
NETDATA est un agent de supervision.

Il va surveiller les performance, l'état et l'utilisation du serveur.

Mais aussi, il va collecter des données en temps réel, générer des alertes en cas de problème, et permettre de maintenir le serveur en bon état de fonctionnement.

Installation sur Linux :

```
Terminal
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
root@admin:~# wget -O /tmp/netdata-kickstart.sh https://get.netdata.cloud/kickstart.sh && sh /tmp/netdata-kickstart.sh --stable-channel --claim-token U7WzTnd-iD1P_WnPzqQD_F8SKMT3wXsEYibFy0hQj9SupphHj9NzGcEugdAbMgwy9m8rgwQGWEy4Kd6bCNz931vZ69nXoJxBK59YAa36-y_PKNK1Cv6T8PzML8G4bpdGeLK9gKM --claim-rooms 2a4ba9c6-0ed1-4bfb-af6-65dbe749030f --claim-url https://app.netdata.cloud
```



VM WORDPRESS

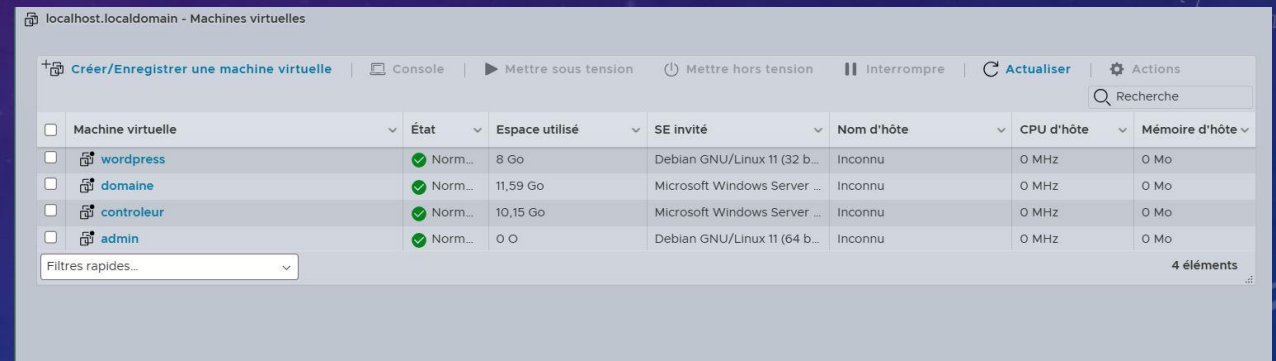
Installation du Serveur Debian 11 à partir d'un fichier ISO.

Il est connecté à pfSense et il est responsable du déploiement de Wordpress.

IP : 192.168.1.20

Configurations :

- Préparation du serveur avec une politique de base
- Configuration d'un serveur SSH avec lien vers le serveur Admin
- Établissement d'un lien avec le serveur Admin via Ansible
- Configuration du serveur Wordpress avec le déploiement Ansible
- Configuration du serveur HTTPS Wordpress (sans playbook)
- Ajout d'un pare-feu avec une politique stricte



The screenshot shows the Proxmox VE web interface for managing virtual machines. The title bar indicates 'localhost.localdomain - Machines virtuelles'. The interface includes a top navigation bar with buttons for 'Créer/Enregistrer une machine virtuelle', 'Console', 'Mettre sous tension', 'Mettre hors tension', 'Interrompre', 'Actualiser', and 'Actions'. Below this is a search bar labeled 'Recherche'. The main content area displays a table of virtual machines with columns for checkboxes, machine names, status, used space, SE invite, host name, host CPU, and host memory. Four machines are listed: 'wordpress', 'domaine', 'controleur', and 'admin'. All machines show a 'Norm...' status with a green checkmark. The 'admin' machine is highlighted. At the bottom left, there is a 'Filtres rapides...' dropdown menu. At the bottom right, it says '4 éléments'.

<input type="checkbox"/>	Machine virtuelle	État	Espace utilisé	SE invité	Nom d'hôte	CPU d'hôte	Mémoire d'hôte
<input type="checkbox"/>	wordpress	✓ Norm...	8 Go	Debian GNU/Linux 11 (32 b...	Inconnu	0 MHz	0 Mo
<input type="checkbox"/>	domaine	✓ Norm...	11,59 Go	Microsoft Windows Server ...	Inconnu	0 MHz	0 Mo
<input type="checkbox"/>	controleur	✓ Norm...	10,15 Go	Microsoft Windows Server ...	Inconnu	0 MHz	0 Mo
<input type="checkbox"/>	admin	✓ Norm...	0 0	Debian GNU/Linux 11 (64 b...	Inconnu	0 MHz	0 Mo

VM DOMAINE AD

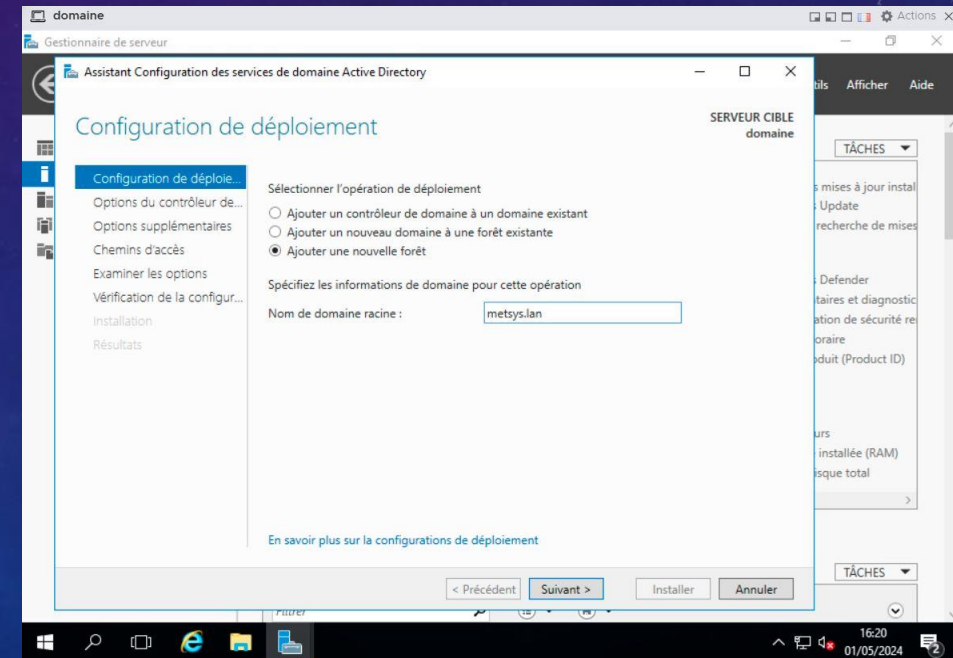
Installation du Serveur Windows 16 à partir d'un fichier ISO.

Il est connecté à pfSense et joue le rôle de domaine pour le réseau.

IP : 192.168.1.119

Configurations :

- Installation et préparation des paramètres de base (outils, IP statique, sauvegarde)
- Installation du rôle AD-DS avec configuration des paramètres DNS de base
- Ajout d'un agent de supervision NETDATA



AGENT DE SUPERVISION NETDATA SUR VM DOMAINE

Installation sur Windows :

Créer un compte

Téléchargement et installation de windows-exporter.exe
sur la vm

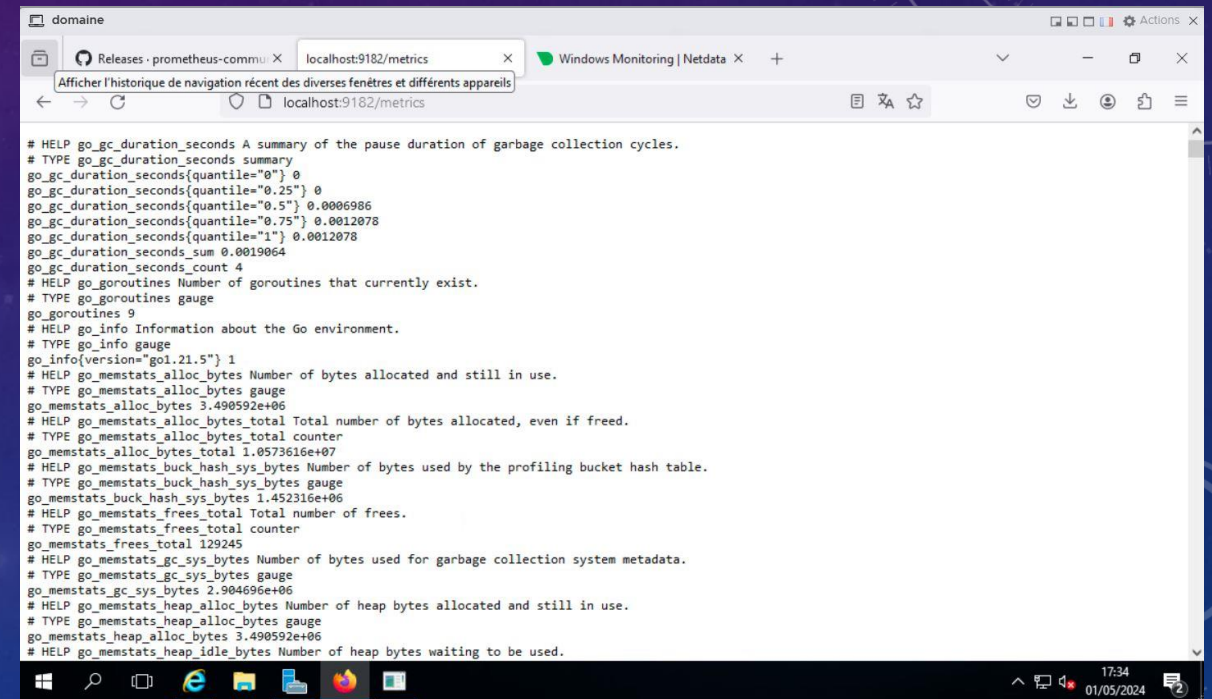
Se connecter à localhost:9182/metrics
pour lancer la supervision

Ensuite configurer les fichiers windows (metrics)

Sources :

https://github.com/prometheus-community/windows_exporter

https://learn.netdata.cloud/docs/collecting-metrics/windows-systems/windows?_gl=1*6bmc1p*_ga*NjYyMTUwODYwLjE3MTA4MzA4NDM.*_ga_J69Z2JCTFB*MTcxNDQ2NjMzNS4xNy4xLjE3MTQ0NjY5NDcuNTluMC4w#configuration



```
# HELP go_gc_duration_seconds A summary of the pause duration of garbage collection cycles.
# TYPE go_gc_duration_seconds summary
go_gc_duration_seconds{quantile="0"} 0
go_gc_duration_seconds{quantile="0.25"} 0
go_gc_duration_seconds{quantile="0.5"} 0.0006986
go_gc_duration_seconds{quantile="0.75"} 0.0012078
go_gc_duration_seconds{quantile="1"} 0.0012078
go_gc_duration_seconds_sum 0.0019064
go_gc_duration_seconds_count 4
# HELP go_goroutines Number of goroutines that currently exist.
# TYPE go_goroutines gauge
go_goroutines 9
# HELP go_info Information about the Go environment.
# TYPE go_info gauge
go_info{version="go1.21.5"} 1
# HELP go_memstats_alloc_bytes Number of bytes allocated and still in use.
# TYPE go_memstats_alloc_bytes gauge
go_memstats_alloc_bytes 3.490592e+06
# HELP go_memstats_alloc_bytes_total Total number of bytes allocated, even if freed.
# TYPE go_memstats_alloc_bytes_total counter
go_memstats_alloc_bytes_total 1.0573616e+07
# HELP go_memstats_buck_hash_sys_bytes Number of bytes used by the profiling bucket hash table.
# TYPE go_memstats_buck_hash_sys_bytes gauge
go_memstats_buck_hash_sys_bytes 1.452316e+06
# HELP go_memstats_frees_total Total number of frees.
# TYPE go_memstats_frees_total counter
go_memstats_frees_total 129245
# HELP go_memstats_gc_sys_bytes Number of bytes used for garbage collection system metadata.
# TYPE go_memstats_gc_sys_bytes gauge
go_memstats_gc_sys_bytes 2.904696e+06
# HELP go_memstats_heap_alloc_bytes Number of heap bytes allocated and still in use.
# TYPE go_memstats_heap_alloc_bytes gauge
go_memstats_heap_alloc_bytes 3.490592e+06
# HELP go_memstats_heap_idle_bytes Number of heap bytes waiting to be used.
```

VM CONTROLEUR DE DOMAINE AD

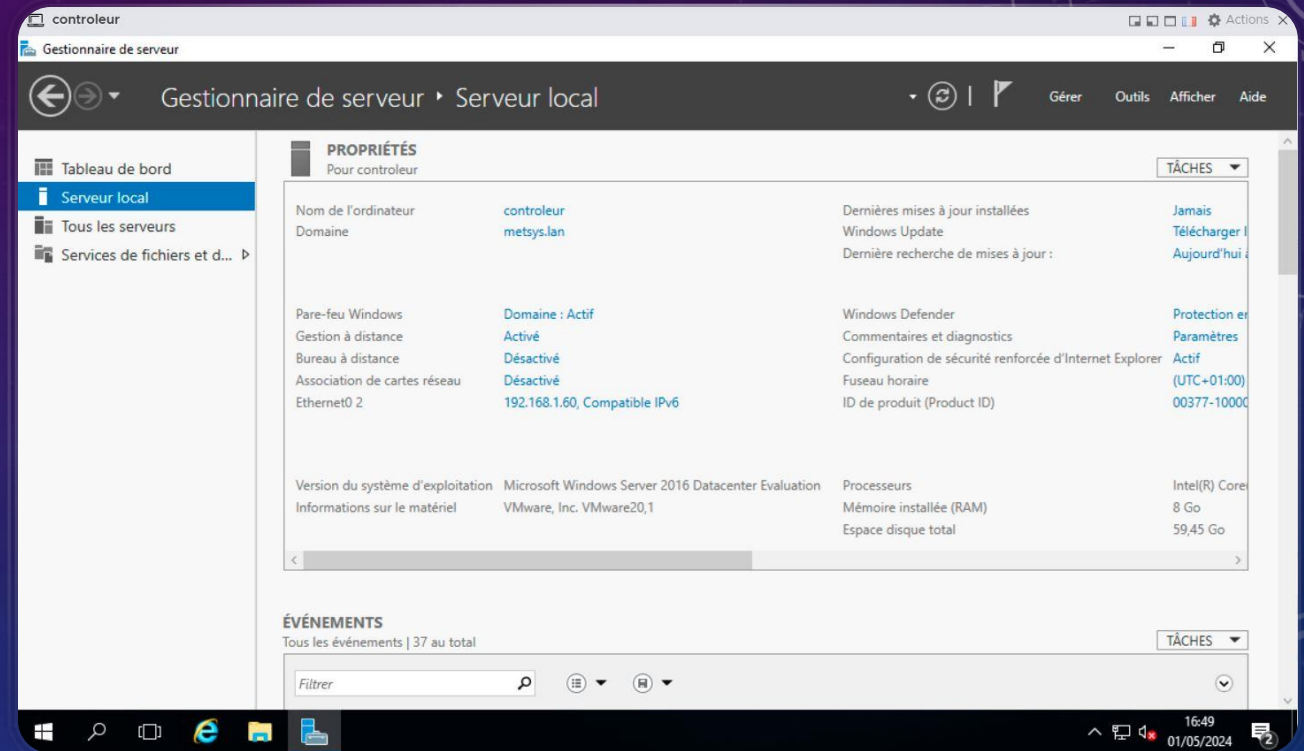
- Installation du Serveur Windows 16 à partir d'un fichier ISO.

- Il est également connecté à pfSense et agit comme contrôleur de domaine pour les services Active Directory.

- IP : 192.168.1.60

- Configurations :

- Installation et préparation des paramètres de base (outils, IP statique, sauvegarde)
- Lien vers le domaine Metsys.lan



PFSENSE

pfSense est un système d'exploitation open source ayant pour but la mise en place de routeur/pare-feu basé sur le système d'exploitation FreeBSD.

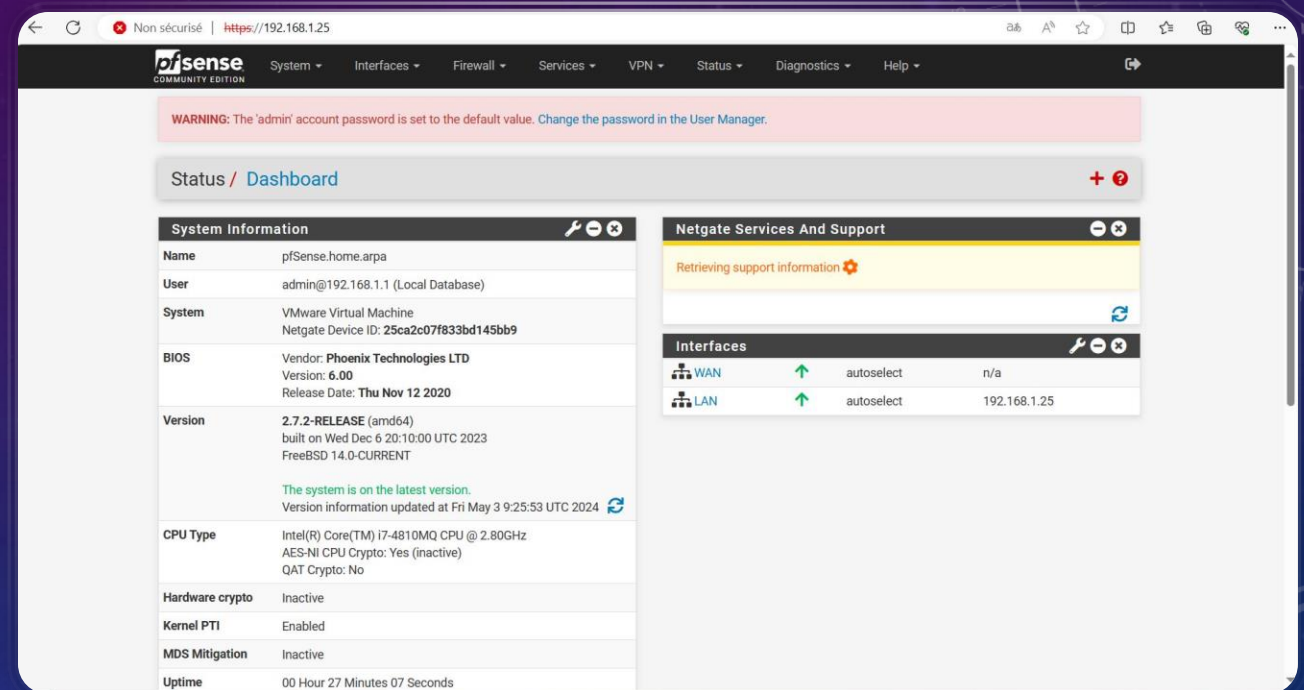
il utilise le pare-feu à états Packet Filter ainsi que des fonctions de routage et de NAT lui permettant de connecter plusieurs réseaux informatiques.

Connexion sur <http://192.168.1.25>

Configurations :

- Installation de l'iso sur esxi
- Assignment des interfaces wan et lan
- Attribution d'une ip à lan
- Configuration de règles de pare-feu sur pfSense

pour contrôler le trafic entre les différents serveurs et les clients.



MISE EN RESEAU

- Ajout d'un commutateur LAN
- Création d'une deuxième carte réseau sur chaque vm et pfsense connectés au LAN
- Attribution de port vm_lan sur chaque vm et sur pfsense.

localhost.localdomain - Mise en réseau

Groupes de ports | Commutateurs virtuels | NIC physiques | NIC VMkernel | Piles TCP/IP | Règles du pare-feu

+ Ajouter un groupe de ports | Modifier les paramètres | Actualiser | Actions

Recherche

Nom	Ports actifs	ID du VLAN	Type	vSwitch	VM
vm_lan	0	0	Groupe de ports standard	lan	5
reseau_lan	1	0	Groupe de ports standard	lan	S/O
VM Network	0	0	Groupe de ports standard	vSwitch0	5
Management Network	1	0	Groupe de ports standard	vSwitch0	S/O

4 éléments

Tâches récentes

Tâche	Cible	Initiateur	En file d'attente	Démarré	Résultat	Terminé
Reconfig VM	domaine	root	03/05/2024 10:33:13	03/05/2024 10:33:13	Terminé	03/05/2024 10:33:13
Reconfig VM	controleur	root	03/05/2024 10:32:23	03/05/2024 10:32:23	Terminé	03/05/2024 10:32:23
Reconfig VM	admin	root	03/05/2024 10:28:44	03/05/2024 10:28:44	Terminé	03/05/2024 10:28:44
Reconfig VM	wordpress	root	03/05/2024 10:27:53	03/05/2024 10:27:53	Terminé	03/05/2024 10:27:53
Refresh Network System	localhost.localdomain	root	03/05/2024 10:15:51	03/05/2024 10:15:51	Terminé	03/05/2024 10:15:52
Update Port Group	localhost.localdomain	root	03/05/2024 10:15:51	03/05/2024 10:15:51	Terminé	03/05/2024 10:15:51

CONCLUSION

Nous venons d'avoir un bon aperçu des possibilités offertes par un hyperviseur de type 1 comme ESXi et sa suite vSphere. Son utilisation est fondamentalement différente de celle d'un hyperviseur de type 2.

L'hyperviseur de type 1 permet de **remplacer complètement une architecture physique** non seulement en la rendant robuste, résiliente, tolérante aux pannes, mais aussi en faisant des économies matérielles et d'énergie.