SOCIÉTÉ NATIONALE DE RADIODIFFUSION ET DE TÉLÉVISION

ÉCOLE NATIONALE DES SCIENCES APPLIQUÉES DE KHOURIBGA

Conception et déploiement d'un cluster Proxmox VE : Mise en place d'une solution de virtualisation à haute disponibilité et tolérance aux pannes sur une infrastructure physique avec un stockage partagé NAS.

1er Année Cycle d'Ingénieur

Filière : Ingénierie des Réseaux Intelligents et Cybersécurité

Réaliser par:
ELOUAFI Aymane

Encadrant professionnel:
OUCHATER Rachid

RAPPORT DE STAGE D'INITIATION

Année Universitaire 2024|2025

Conception et déploiement d'un cluster Proxmox VE : Mise en place d'une solution de virtualisation à haute disponibilité et tolérance aux pannes sur une infrastructure physique avec un stockage partagé NAS.

Table des Matières

Table des Matières.....2
Organisme d'Accueil.....5
Services.....6
Télévision :.....6
Radios :.....7
1. Introduction :.....8
2. La virtualisation:.....10
2.1 – La virtualisation , qu'est-ce que c'est ?.....10
2.2 – Les différents types de virtualisation :.....10
2.3 – C'est quoi une machine virtuelle ?.....12
2.4 – Fonctionnement d'une machine virtuelle :.....13
2.5 – Avantages des machines virtuelles :.....14
2.6 – Un hyperviseur , qu'est-ce que c'est ?.....15
2.7 – Fonctionnement d'un hyperviseur :.....16
2.8 – Types d'hyperviseurs :.....17
2.8.1 – Hyperviseurs de type 1 :.....17
2.8.2 – Hyperviseurs de type 2 :.....17
3. Clustering :.....18
3.1 – Cluster informatique: qu'est-ce que c'est?.....18
3.2 – Types de cluster informatique : 19
3.3 – Fonctionnement d'un cluster :.....20
3.4 – Avantages et inconvénients d'un cluster :.....20
3.5 – Les clusters virtuels :.....21
3.6 – La haute disponibilité , qu'est-ce que c'est ?.....22
3.7 – Un cluster à haute disponibilité :.....22
3.8 – Qu'est-ce qu'un Quorum ?.....23

4. Stockage Partagé :.....24
4.1 – Qu’est-ce que le stockage partagé ?.....24
4.2 – Comment fonctionnent les espaces de stockage partagées ?.. 25
4.3 – SAN (Storage Area Network) :.....25
4.3.1 – Qu’est-ce que le stockage SAN ?.....25
4.3.2 – Quels sont les différents types de réseaux SAN ?.....26
4.4 – NAS (Network Attached Storage) :.....27
4.4.1 – Qu’est-ce que le stockage NAS ?.....27
4.4.2 – Histoire de NAS :.....28
4.4.3 – Fonctionnement d’un serveur NAS :.....28
4.4.4 – À quoi sert le stockage en réseau (NAS) ?.....30
4.4.5 – la différence entre NAS et SAN :.....30
4.4.6 – Quelles sont les limites du NAS sur site ?.....31
4.5 – RAID (Redundant Array of Independent Disks) :.....31
4.5.1 – Qu’est-ce que le RAID ?.....31
4.5.2 – Les configurations RAID les plus courantes :.....32
4.5.3 – Comparaison des configurations RAID :.....36
5. Proxmox VE :.....38
5.1 – Qu’est-ce que Proxmox VE ?.....38
5.2 – Caractéristiques principales de Proxmox VE :.....39
Cluster haute disponibilité.....39
Ligne de commande (CLI).....40
Interface de gestion web.....40
Options de stockage flexibles.....40
Migration en ligne temps réel.....40
Réseau virtualisé.....40
Administration basée sur les rôles.....41
5.3 – Comment installer Proxmox VE :.....41
5.3.1 – Configuration minimale requise pour l'évaluation :....42
5.3.2 – Préparation du support d'installation :.....42
6. Mise en œuvre Technique :.....45
6.1 – Architecture Physique et Planification Réseau :.....45
6.1.1 – Composant Physique :.....46
6.1.2 – Plan d'adressage réseau :.....49
6.2 – Configuration des Serveurs et du Cluster :.....51
Qu’est-ce qu’un commutateur KVM ?.....51
6.2.1 – Installation de Proxmox VE sur les deux serveurs :....52
6.2.2 – Configuration du Cluster :.....59
6.2.3 – Problématique de la haute disponibilité (HA) et du quorum :.....62
Pourquoi les clusters Proxmox VE à 2 nœuds peuvent être instables ?.....63
Quelles sont les solutions proposées pour permettre au nœud survivant de fonctionner ?.....64
6.3 – Intégration du Stockage NAS via NFS :.....67
6.3.1 – Configuration du NAS :.....67
6.3.2 – Ajout du stockage dans Proxmox VE :.....71
6.4 – Configuration des Services Réseau et du Pare-feu :.....72

6.4.1 - Création du réseau privé (NAT) :.....72
6.4.2 - Configuration du pare-feu Proxmox VE :.....74
6.5 - Gestion des Utilisateurs et des Permissions :.....75
Création de groupe , comptes utilisateurs et Attribution des rôles :.....76
6.6 - Gestion des ISO et des modèles de VM :.....78
7. Tests et Validation :.....79
7.1 - Création et Configuration d'une Machine Virtuelle (VM) :.. 79
7.2 - Test de la Haute Disponibilité (HA) :.....82
7.3 - Test de la Migration à Chaud (Live Migration) :.....84
7.4 - Test du Pare-feu (Firewal) :.....86
7.5 - Test du réseaux NAT :.....89
8. Conclusion :.....92
9. Références :.....94

Organisme d'Accueil

SNRT (SOCIÉTÉ NATIONALE DE RADIODIFFUSION ET DE TÉLÉVISION) :

La **Société nationale de radiodiffusion et de télévision (SNRT)** est une société de participation marocaine, à vocation audiovisuelle, dont le capital est détenu à 100% par l'État marocain. En 2007, le périmètre économique du groupe comprend plus de douze sociétés.

La SNRT est un membre actif de l'Union européenne de radio-télévision et un actionnaire de la chaîne d'information Euronews .

Histoire :

La SNRT trouve son origine dans la fondation de Radio Maroc le 15 février 1928, qui commence ses émissions le 13 avril de la même année. Son autorité de tutelle est alors l'Office chérifien des postes et télégraphes.

Le 22 octobre 1966, la Radiodiffusion Marocaine devient un établissement public doté de la personnalité civile et de l'autonomie financière. Mais le 1er janvier 1968 elle réintègre l'administration.

Le 28 décembre 1978, elle est rattachée à l'administration centrale du ministère de l'Information. Victime d'un certain immobilisme, et face à la libéralisation de l'audiovisuel marocain, la SNRT succède le 3 avril 2005 dans ses moyens et ses attributions à la Radiodiffusion télévision marocaine (RTM) qui était une administration publique, afin de résister à la concurrence. Depuis elle lance plusieurs initiatives. Ainsi elle modernise le matériel de la TVM.

1961 : création de **TVM** ;
2004 : création de **Laayoune TV** et **Al Maghribia** ;
2005 : création de **Arrabiaa/Athaqafia** ;
2006 : création de **Assadissa** et **Arryadia** ;
2008 : création de **Aflam TV** ;
2009 : création de **Tamazight TV** ;

2015 : apparition de **Al Aoula HD** ;
2017 : apparition de **Arryadia HD** et **Al Maghribia HD** ;
2018 : apparition de **Arrabiaa/Athaqafia HD**, **Assadissa HD**, **Tamazight HD** et **Laayoune TV HD**.
2021 :Acquisition par la SNRT des chaines de télévision 2M et Medi1 TV ainsi que de la station radio Medi1 Radio

Services

Télévision :

La SNRT possède huit chaînes de télévision :

- Al Aoula : 1re chaîne de télévision marocaine, chaîne généraliste ;
- Al Aoula Laayoune : chaîne régionale destinée au Sahara marocain :
- Arryadia : consacrée au sport, lancée en 2006 :
- Athaqafia : chaîne consacrée à la culture et au soutien scolaire ;
- Al Maghribia : généraliste et destinée à l'extérieur du Maroc, elle fut lancée le 18 novembre 2004 ;
- Assadissa : chaîne à vocation religieuse ;
- Aflam TV : chaîne consacrée en premier lieu au cinéma ;
- Tamazight : chaîne consacrée à la promotion de la culture amazighe.



Radios :

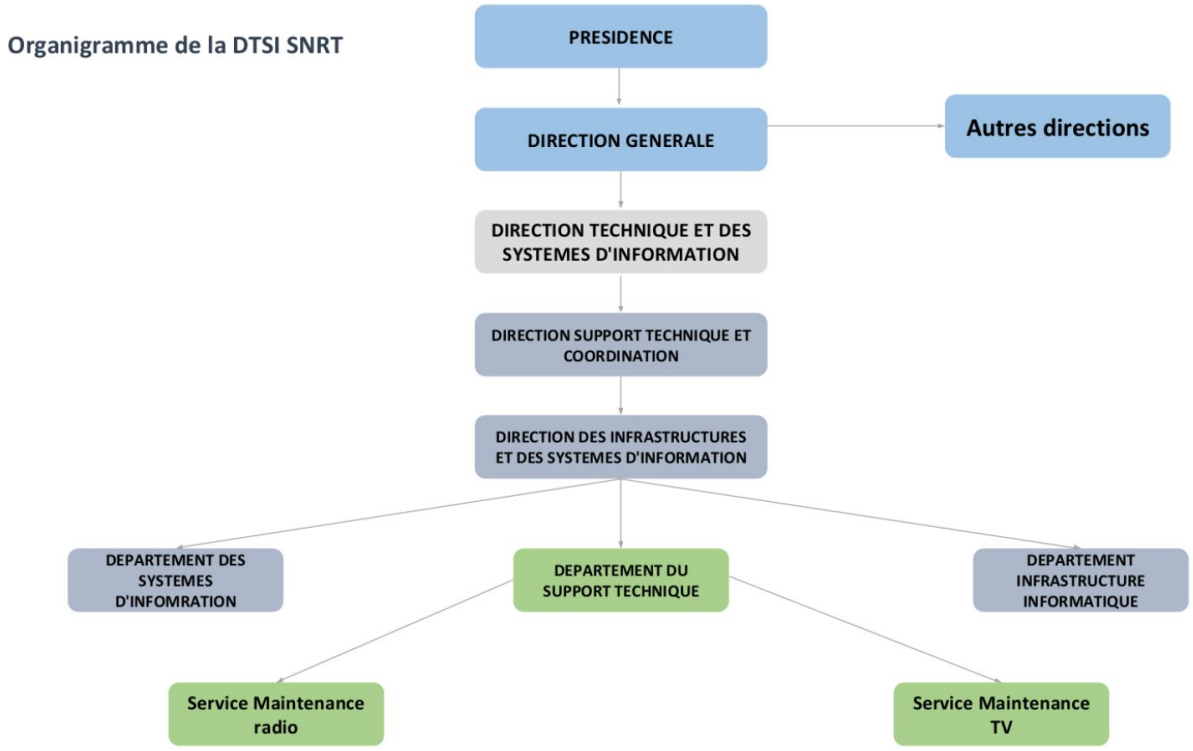
La *SNRT* dispose de plusieurs stations de radio :

Radio nationale marocaine	Chaîne Inter	Radio Amazigh	Radio Mohammed VI du Saint-Coran	Casa FM

Il existe des chaines régionales pour plusieurs villes :

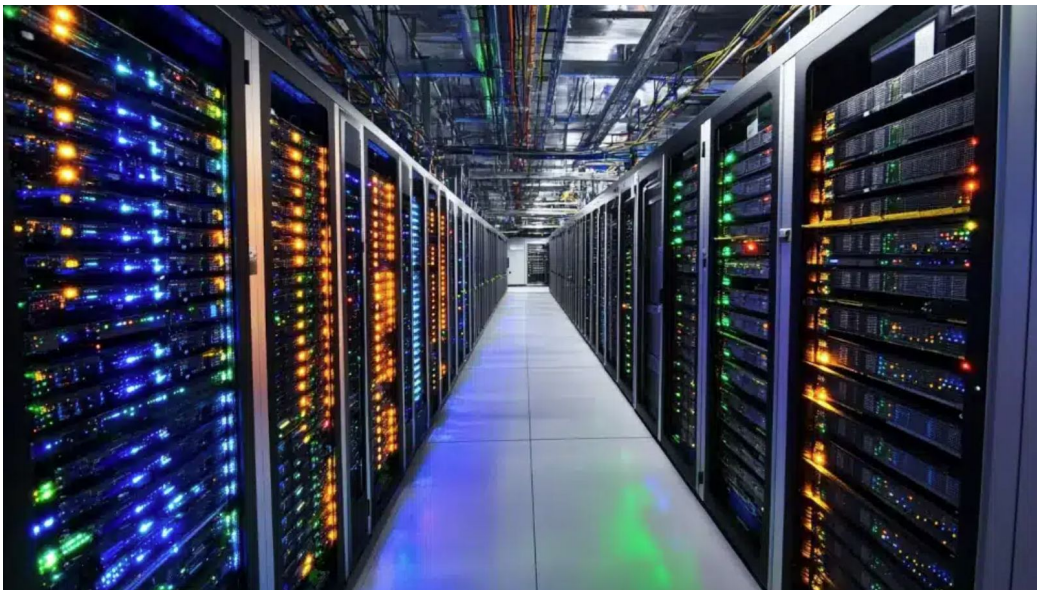
- Radio Agadir
- Radio Al Hoceima
- Radio Casablanca
- Radio Dakhla
- Radio Fès
- Radio Laâyoune
- Radio Marrakech
- Radio Meknès
- Radio Oujda
- Radio Tanger
- Radio Tétouan

Organigramme :



1. Introduction :

À l'ère de l'informatique moderne, la virtualisation est devenue une technologie incontournable, transformant radicalement la manière dont les entreprises gèrent leurs ressources IT. En dissociant les logiciels du matériel physique, la virtualisation permet non seulement d'optimiser l'utilisation des serveurs, mais aussi de garantir la résilience et la continuité des services.



C'est dans ce contexte que s'inscrit notre projet : la conception et la mise en œuvre d'une plateforme de virtualisation haute disponibilité. Pour cela, nous avons utilisé deux serveurs physiques HP ProLiant DL360p Gen8, configurés en cluster Proxmox VE. Pour le stockage partagé de nos machines virtuelles (VMs), nous avons choisi un serveur de stockage NAS LenovoEMC px6-300d, en utilisant le protocole NFS.

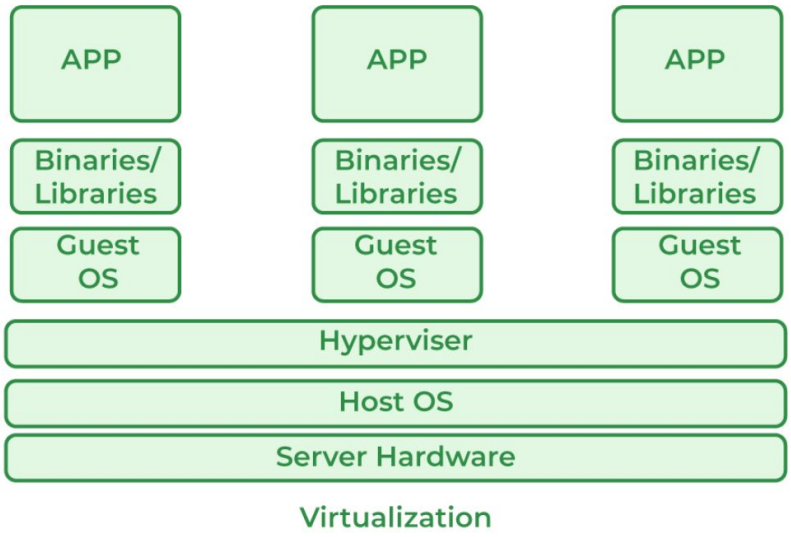
L'objectif principal de cette plateforme est de démontrer la capacité du système à assurer la continuité des opérations en cas de défaillance. Nous avons mis en place une configuration de haute disponibilité (HA) spécifique à notre cluster à deux nœuds. Cette

approche garantit que si l'un des serveurs physiques tombe en panne, les VMs actives seront automatiquement redémarrées sur le serveur de secours, minimisant ainsi les temps d'arrêt. Ce projet servira de modèle pour comprendre les défis et les solutions du clustering dans un environnement d'entreprise réel.

2. La virtualisation:

2.1 – La virtualisation , qu’est-ce que c’est ?

La **virtualisation** est une technologie qui permet de créer des environnements virtuels et simulés à partir d'une seule machine physique. Grâce à ce processus, les professionnels de l'informatique peuvent exploiter leurs investissements existants et optimiser toutes les capacités d'une machine physique en distribuant des ressources traditionnellement liées au matériel dans de nombreux environnements.



2.2 – Les différents types de virtualisation :

Il existe différents types de virtualisation :

Virtualisation des données : La virtualisation des données est un type de gestion des données qui intègre des données provenant de plusieurs applications et emplacements physiques. Cela se traduit par une utilisation sans réplication ou déplacement des données. Ce type de virtualisation crée une couche abstraite virtuelle unique

qui se connecte à différentes bases de données pour offrir une vue virtualisée des données.

Virtualisation des serveurs : La virtualisation des serveurs crée plusieurs instances d'un seul serveur. Celles-ci représentent un environnement virtuel. Dans chacun de ces environnements, un système d'exploitation distinct peut s'exécuter seul. Une seule machine d'exploitation peut ainsi effectuer le travail de nombreuses machines. Ainsi, la virtualisation des serveurs réduit la prolifération des données et permet d'économiser sur les dépenses d'exploitation.

Virtualisation des systèmes d'exploitation : La virtualisation des systèmes d'exploitation est similaire à la virtualisation des serveurs. Le système d'exploitation hôte est reconfiguré pour exécuter plusieurs systèmes d'exploitation isolés, tels que Linux et Windows, sur une seule machine. De ce fait, plusieurs utilisateurs peuvent travailler sur celle-ci dans différentes applications en même temps. Elle est également appelée « virtualisation au niveau du système d'exploitation ».

Virtualisation des postes de travail : La **virtualisation des postes de travail (poste VDI)** est un logiciel de virtualisation qui sépare l'environnement du poste de travail principal des autres périphériques qui l'utilisent. Elle permet d'économiser du temps et des ressources informatiques. En effet, un environnement de poste de travail est déployé sur plusieurs machines à la fois. Ce logiciel de virtualisation facilite également les protocoles suivants sur plusieurs postes de travail virtuels à la fois :

- déploiement de mises à jour ;
- correction de systèmes ;
- **ajout de protocoles de sécurité.**

Virtualisation réseau : La virtualisation réseau combine le matériel réseau et les fonctionnalités logicielles en une seule entité. Souvent associé à la virtualisation des ressources, elle combine plusieurs ressources qui sont ensuite divisées en segments distincts et affectées aux périphériques ou serveurs qui en ont besoin. Ce

type de virtualisation améliore la vitesse, l'évolutivité et la fiabilité du réseau.

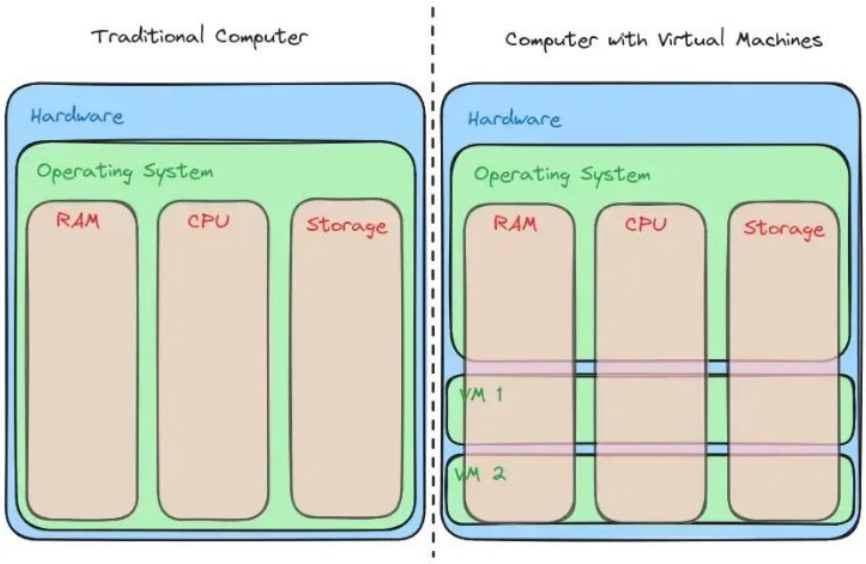
Virtualisation du stockage : La virtualisation du stockage regroupe des ressources de stockage provenant de plusieurs petits périphériques dans un seul grand périphérique de stockage. Les administrateurs peuvent utiliser ce stockage au besoin depuis une console centrale unique via des machines virtuelles et des serveurs physiques. Pour ce faire, le logiciel reçoit les requêtes de stockage et détermine quel périphérique dispose de la capacité nécessaire.

2.3 – C’est quoi une machine virtuelle ?

Une **machine virtuelle** est un environnement de calcul qui fonctionne comme un système isolé, avec son propre processeur, sa mémoire, son interface réseau et son espace de stockage, créé à partir d'un pool de ressources matérielles. L'**hyperviseur** est le logiciel qui isole les ressources de calcul nécessaires et qui permet la création et la gestion des machines virtuelles.

La machine physique qui exécute les machines virtuelles est appelée machine hôte, ordinateur hôte, système d'exploitation hôte, ou simplement hôte. Les nombreuses machines virtuelles qui utilisent les ressources sont des machines invitées, des ordinateurs invités, des systèmes d'exploitation invités ou simplement des invités. L'hyperviseur traite les ressources de calcul (processeur, mémoire, stockage) sous la forme d'un pool de ressources qui peut être déplacé sans difficulté entre les invités existants ou vers de nouvelles machines virtuelles.

Les machines virtuelles permettent d'exécuter simultanément plusieurs systèmes d'exploitation sur un seul ordinateur, comme une distribution Linux® sur un système macOS ou Windows. Chacun des systèmes d'exploitation s'exécute sur le matériel hôte comme le ferait tout autre type de système d'exploitation ou d'application. L'expérience de l'utilisateur final émulée au sein de la machine virtuelle est donc quasiment identique à celle qu'offre un système d'exploitation exécuté en temps réel sur une machine physique.



Resources allocation in a computer with and without VMs

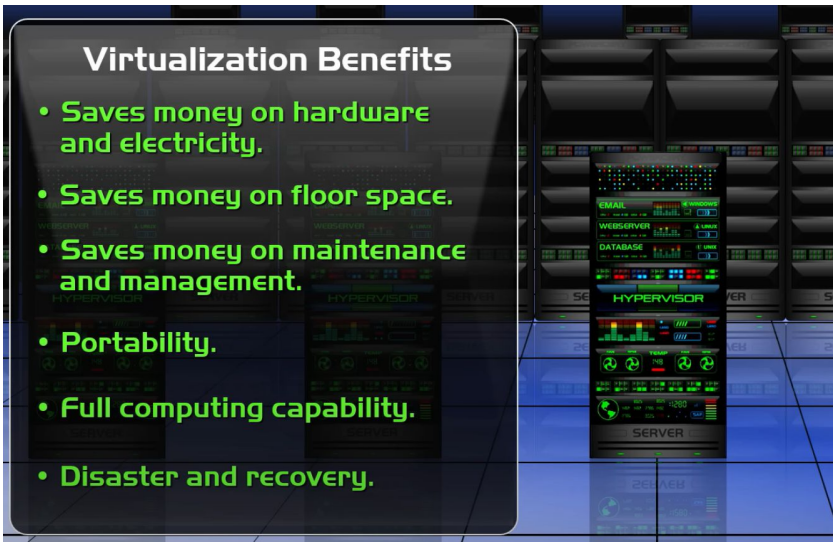
2.4 – Fonctionnement d'une machine virtuelle :

Une **machine virtuelle** peut être définie par un fichier numérique que l'on peut transférer d'un ordinateur à un autre, ouvrir sur l'un ou l'autre et utiliser de la même manière. L'hyperviseur se charge de gérer le matériel et de séparer les ressources physiques des environnements virtuels. Ces ressources sont partitionnées selon les besoins à partir de l'environnement physique et distribuées aux machines virtuelles. Le matériel se charge toujours de l'exécution, de sorte que le processeur continue d'exécuter les instructions demandées par les machines virtuelles, par exemple, tandis que l'hyperviseur gère l'ordonnancement.

Lors de l'exécution d'une machine virtuelle, si un utilisateur ou un programme lance une instruction qui sollicite des ressources supplémentaires de la part de l'environnement physique, l'hyperviseur ordonnance la demande auprès des ressources du système physique, afin que le système d'exploitation et les applications de

la machine virtuelle puissent accéder au pool partagé de ressources physiques.

2.5 – Avantages des machines virtuelles :



Avec la virtualisation, différents systèmes d'exploitation peuvent s'exécuter en parallèle et partager les mêmes ressources matérielles virtualisées. Sans cette technologie, un seul système d'exploitation peut s'exécuter sur le matériel.

La consolidation des serveurs est l'une des principales raisons qui justifient l'utilisation de machines virtuelles. La plupart des systèmes d'exploitation et des applications n'utilisent qu'une petite partie des ressources physiques disponibles lorsqu'ils sont déployés sur un système bare metal. La virtualisation des serveurs permet de disposer de nombreux serveurs virtuels sur chaque serveur physique, avec à la clé une optimisation de l'utilisation du matériel.

Il devient inutile d'acheter des ressources physiques supplémentaires, notamment des disques durs, et les besoins en matière d'alimentation, d'espace et de refroidissement dans le datacenter sont réduits. Les machines virtuelles offrent des fonctions de récupération après sinistre supplémentaires, car elles disposent de capacités de basculement et de redondance qu'il n'était auparavant possible d'obtenir qu'avec du matériel supplémentaire. Une machine virtuelle fournit un environnement isolé du reste du système. Ainsi, il ne peut y avoir aucune interférence entre les

programmes exécutés au sein d'une machine virtuelle et sur le matériel hôte.
Comme les machines virtuelles sont isolées, elles peuvent être utilisées pour tester de nouvelles applications ou mettre en place un environnement de production. Il est également possible d'exécuter une machine virtuelle réservée à un processus spécifique.

2.6 – Un hyperviseur , qu’est-ce que c’est ?



Un **hyperviseur** est un logiciel qui regroupe des ressources informatiques (calcul, mémoire, stockage) et qui les répartit entre plusieurs machines virtuelles. Cette technologie permet de virtualiser les ressources, ce qui signifie qu'il est possible de créer et d'exécuter de nombreuses machines virtuelles à partir d'une même machine physique.

Parfois appelé moniteur de machine virtuelle, un hyperviseur s'apparente à un superviseur chargé de répartir les composants des machines virtuelles. Il trouve ces ressources dans le matériel physique et les fournit simultanément à plusieurs machines virtuelles, ce qui permet d'en créer de nouvelles et de gérer celles qui existent déjà. Lorsqu'il est utilisé en tant qu'hyperviseur, le matériel physique est appelé « hôte », tandis que toutes les machines virtuelles qui utilisent ses ressources sont appelées « invités ».

2.7 – Fonctionnement d’un hyperviseur :

Pour exécuter des machines virtuelles, tous les hyperviseurs ont besoin de certains composants au niveau du système d'exploitation : gestionnaire de mémoire, ordonnanceur, pile d'entrées/sorties (E/S), pilotes de périphériques, gestionnaire de la sécurité, pile réseau, etc.

L'hyperviseur distribue à chaque machine virtuelle les ressources qui ont été allouées et gère la planification des ressources des machines virtuelles en fonction des ressources physiques. Le matériel se charge toujours de l'exécution, de sorte que le processeur continue d'exécuter les instructions demandées par les machines virtuelles, par exemple, tandis que l'hyperviseur gère la planification.

Différents systèmes d'exploitation peuvent s'exécuter en parallèle et partager les mêmes ressources matérielles virtualisées avec un hyperviseur. Il s'agit là d'un avantage clé de la virtualisation. Sans cette technologie, un seul système d'exploitation peut s'exécuter sur le matériel.

Il existe une multitude d'hyperviseurs, issus de la communauté Open Source ou proposés par des fournisseurs traditionnels. Vmware est l'un des principaux fournisseurs de solutions de virtualisation. L'entreprise propose notamment l'hyperviseur ESXi et la plateforme de virtualisation vSphere.

2.8 – Types d’hyperviseurs :

La virtualisation peut être effectuée au moyen d'hyperviseurs de type 1 ou de type 2.

2.8.1 – Hyperviseurs de type 1 :

Également appelés hyperviseurs natifs ou **bare metal**, les hyperviseurs de type 1 s'exécutent directement sur le matériel de l'hôte pour gérer des systèmes d'exploitation invités. Ce type

d'hyperviseur remplace le système d'exploitation hôte et planifie les ressources des machines virtuelles directement sur le matériel.Ces hyperviseurs sont les plus couramment utilisés dans les datacenters d'entreprise ou d'autres environnements basés sur un serveur.

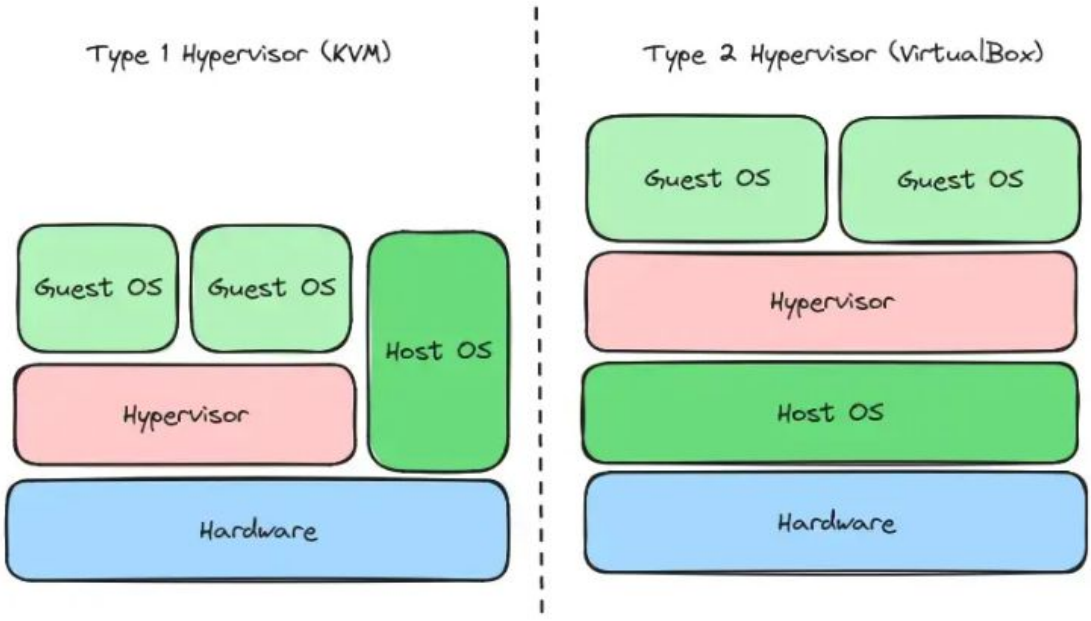
2.8.2 – Hyperviseurs de type 2 :

Également appelés hyperviseurs hébergés, les hyperviseurs de type 2 s'exécutent sur un système d'exploitation traditionnel en tant que couche logicielle ou application.

Ils fonctionnent en dissociant les systèmes d'exploitation invités du système d'exploitation hôte. Les ressources des machines virtuelles sont ordonnancées sur un système d'exploitation hôte, qui est ensuite exécuté sur le matériel.

Les hyperviseurs de type 2 sont plus adaptés pour les utilisateurs individuels qui souhaitent exécuter plusieurs systèmes d'exploitation sur un ordinateur personnel.

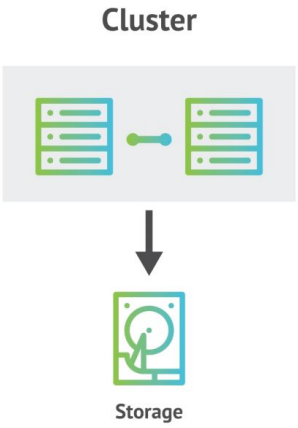
VMware Workstation et **Oracle VirtualBox** sont des hyperviseurs de type 2.



Architecture differences between a type 1 and a type 2 hypervisor

3. Clustering :

3.1 – Cluster informatique: qu’est-ce que c’est?



Les clusters en informatique sont des groupes de serveurs interconnectés qui collaborent pour améliorer la performance, la disponibilité et la fiabilité des systèmes.

Contrairement aux réseaux, où chaque ordinateur fonctionne indépendamment, et aux systèmes distribués, où les tâches sont réparties entre des ordinateurs dispersés, les clusters travaillent en étroite collaboration pour offrir une puissance de calcul collective, souvent dans le même lieu.

3.2 – Types de cluster informatique :

Les clusters informatiques peuvent être divisés en plusieurs types en fonction de leur but et de leurs caractéristiques. Chacun a ses propres avantages et inconvénients, ce qui les rend appropriés pour une variété de tâches.

Clusters à haute disponibilité

Ils sont conçus pour minimiser les temps d’arrêt du système. Ils assurent la redondance et le basculement automatique vers les nœuds de secours en cas de défaillance du matériel principal.

Les avantages sont la fiabilité et la continuité accrue des applications critiques.

Cependant, le principal inconvénient est le coût élevé associé à la nécessité de maintenir un grand nombre de ressources de réserve.

Clusters de calcul

Ils sont utilisés pour effectuer des calculs complexes en traitant des données en parallèle. Ils sont largement utilisés dans la recherche scientifique, la modélisation, le traitement des mégadonnées et l'exécution de tâches gourmandes en ressources telles que l'analyse de l'ADN ou la modélisation du changement climatique.

Clusters de stockage

Ils permettent une gestion et un traitement efficaces de grandes quantités de données. Ils sont utilisés pour créer des systèmes de stockage évolutifs qui peuvent s'adapter aux besoins croissants de l'entreprise.

Les appareils jouent un rôle clé dans la gestion et l'analyse du Big data (Big Data), permettant aux entreprises d'extraire des informations précieuses à partir d'énormes quantités d'informations.

Le principal avantage est leur capacité à fournir une capacité et une fiabilité élevées, mais ils peuvent également nécessiter des investissements importants dans le matériel et les logiciels.

3.3 – Fonctionnement d'un cluster :

Ils sont constitués de plusieurs composants clés qui assurent leur collaboration:

Les nœuds : Ce sont des serveurs distincts qui effectuent des tâches de calcul ou stockent des données. Ils peuvent être identiques (grappes homogènes) ou différents dans les caractéristiques (grappes hétérogènes), selon l'architecture du système.

Les réseaux : Ils relient les nœuds, ce qui leur permet d'échanger des données et d'effectuer des tâches en parallèle. Un réseau fiable à faible latence est essentiel au bon fonctionnement.

Logiciel de gestion : Pour gérer efficacement le cluster, vous utilisez un logiciel spécial qui répartit les tâches entre les nœuds, surveille leur état et permet de basculer automatiquement vers les nœuds de secours en cas de défaillance.

3.4 – Avantages et inconvénients d'un cluster :

Comme toute technologie, ils ont leurs avantages et leurs inconvénients qui doivent être pris en compte lors de leur utilisation.

Avantages:

Hautes performances: ils offrent des performances élevées grâce au traitement simultané des données sur plusieurs nœuds.

Évolutivité: possibilité d'ajouter facilement de nouveaux nœuds pour augmenter la puissance de traitement.

Flexibilité: ils peuvent être configurés pour effectuer diverses tâches telles que l'informatique scientifique, l'apprentissage automatique et l'analyse de données.

Rentabilité: l'utilisation de nœuds peu coûteux et l'utilisation efficace des ressources permettent de réduire les coûts de calcul.

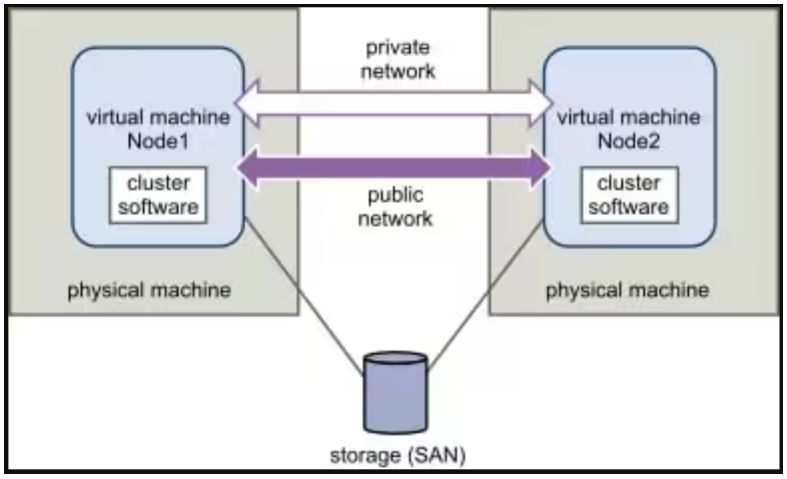
Défauts:

Complexité de la gestion: la gestion d'un grand nombre de nœuds et de logiciels peut être complexe et nécessiter des compétences particulières.

Disponibilité limitée: si un seul nœud échoue, cela peut affecter le fonctionnement de l'ensemble du cluster.

Complexité de la configuration: la configuration d'un cluster peut nécessiter des connaissances et du temps.

3.5 – Les clusters virtuels :



Les clusters sont conçus pour une haute disponibilité. Grâce à la technologie de virtualisation, ils gagnent en efficacité et en flexibilité. Les clusters virtuels sont constitués de machines virtuelles installées sur un ou plusieurs serveurs physiques. Ainsi, les machines virtuelles sont interconnectées logiquement par un réseau virtuel.

- Plusieurs machines virtuelles exécutant différents systèmes d'exploitation peuvent être déployées sur un même nœud physique.
- Le système d'exploitation invité peut différer du système d'exploitation hôte.
- Les machines virtuelles consolident plusieurs fonctionnalités sur un même serveur, ce qui améliore considérablement l'utilisation du serveur et la flexibilité des applications.
- Le nombre de nœuds d'un cluster virtuel peut croître de manière dynamique.
- La défaillance d'un nœud physique peut entraîner la désactivation de certaines des machines virtuelles installées sur ces nœuds. Cependant, une défaillance de machine virtuelle n'entraîne pas l'arrêt du système hôte.

3.6 – La haute disponibilité , qu’est-ce que c’est ?

La haute disponibilité est la capacité pour un système informatique à être accessible et fiable presque 100 % du temps, afin de réduire, voire éliminer, les temps d'arrêt. Elle garantit de deux façons qu'un système informatique fonctionne à son plus haut niveau de performances : le service ou serveur donné doit être accessible (ou disponible) à tout moment ou presque, sans interruption, et présenter des performances satisfaisantes sur une période donnée. La haute disponibilité va plus loin qu'un simple contrat de niveau de service (SLA) sur la disponibilité ou que les attentes définies entre un prestataire de services et son client. Elle garantit le bon fonctionnement, la résilience et la fiabilité des systèmes.

3.7 – Un cluster à haute disponibilité :

Les architectures à haute disponibilité exécutent des clusters de basculement actifs, afin d'intégrer la redondance et le basculement, voire d'éliminer complètement les temps d'arrêt.Les nœuds sont surveillés au sein du cluster, à la fois pour la disponibilité et les performances générales des applications, services et réseaux. Grâce au stockage partagé, la panne d'un nœud n'entraîne aucune perte de données, car tous les nœuds d'un cluster utilisent la même source de données. L'équilibrage de charge peut servir à gérer le trafic pour optimiser les performances.

3.8 – Qu'est-ce qu'un Quorum ?

Un quorum correspond au nombre minimal de votants nécessaire pour valider une décision.
Dans le cas d'un cluster, il faudra que + de 50 % des votants soient présents (ou disponibles) pour que le cluster puisse continuer à fonctionner.

Dans le cas d'un cluster, ces votants peuvent être :

- des serveurs (appelés nœuds quand ils font partie d'un cluster)
- un disque témoin
- OU un partage de fichier témoin

L'utilisation d'un Quorum dans un cluster est importante, car cela vous permet de fournir un ou plusieurs services hautement disponible(s) sans pour autant saturer les ressources de vos serveurs, ainsi que de détecter les serveurs défectueux dans un cluster.

Scénario de Perte:

Si un nombre suffisant de nœuds échouent et que le quorum n'est plus atteint, le cluster s'arrête pour éviter les problèmes de **split-brain**.

Exemple:

Dans un cluster à 3 nœuds, le quorum est atteint avec 2 nœuds actifs. Si un nœud tombe en panne, le cluster peut continuer à fonctionner car il maintient sa majorité. Cependant, si deux nœuds tombent en panne, le quorum n'est plus atteint et le cluster s'arrête.

4. Stockage Partagé :

4.1 – Qu’est-ce que le stockage partagé ?

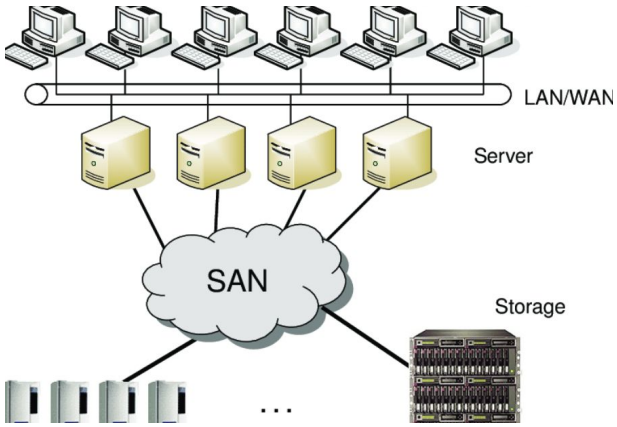
Le **stockage partagé** permet de consolider des fichiers et autres informations dans une ressource centrale accessible ou partageable par plusieurs utilisateurs et systèmes de données simultanément. Le rassemblement et le stockage des données dans une ressource unique et partagée rationalisent les processus d’archivage et de sauvegarde tout en simplifiant la sécurité des informations. Les solutions de stockage partagé comprennent le stockage **NAS (Network Attached Storage)**, le stockage **SAN (Storage Area Network)** et **le stockage RAID (Redundant Arrays of Independent Disks)**, ainsi que les serveurs de stockage dédiés et le stockage cloud.

4.2 – Comment fonctionnent les espaces de stockage partagées ?

L’accès aux informations d’une ressource de stockage partagé peut s’effectuer : directement via **un réseau local** ; **à distance via Internet à l’aide de protocoles de transfert de fichiers (FTP)** ou d’une **application de gestion du stockage** ; ou encore depuis des applications, par l’intermédiaire d’une **interface de programmation d’applications (API)**. Les utilisateurs et les applications doivent être authentifiés conformément aux règles de sécurité de l’entreprise avant de pouvoir accéder, modifier ou créer des fichiers sur le stockage partagé.

4.3 – SAN (Storage Area Network) :

4.3.1 – Qu’est-ce que le stockage SAN ?



Le **SAN (Storage Area Network)** est une **architecture de réseau de stockage commune** qui fournit un débit élevé et une faible latence pour les applications critiques.

Une disponibilité et une utilisation accrues des applications

Utilisés par la plupart des entreprises, les réseaux SAN stockent généralement les données vitales des clients de l'organisation sur des dispositifs et des serveurs distincts au sein d'un réseau virtuel. Les réseaux SAN déchargent ainsi l'entreprise de la fonction de stockage pour améliorer l'efficacité et isoler les pannes éventuelles. Les entreprises utilisent également les réseaux SAN pour améliorer les performances des applications critiques tout en augmentant leur disponibilité et leurs taux d'utilisation.

Dans le cas du SAN, les baies de stockage n'apparaissent pas comme des volumes partagés sur le réseau. Elles sont directement accessibles en mode bloc par le système de fichiers des serveurs. En clair, chaque serveur voit l'espace disque d'une baie SAN auquel il a accès comme son propre disque dur. L'administrateur doit donc définir très précisément les Logical Unit Number (LUN, unités logiques), le *masking* et le *zoning*, pour qu'un serveur Unix n'accède pas aux mêmes ressources qu'un serveur Windows utilisant un système de fichiers différent.

Une couverture étendue à plusieurs sites physiques

Les réseaux de stockage SAN peuvent couvrir plusieurs sites et s'appuient souvent sur la technologie **Fibre Channel (FC)**. Ils utilisent soit le protocole **FCP (Fibre Channel Protocol)**, soit des variantes propriétaires, en fonction du type de système qui s'y connecte. Le stockage SAN est particulièrement utile lorsque plusieurs personnes ont besoin de se connecter à plusieurs dispositifs de stockage en même temps.

4.3.2 – Quels sont les différents types de réseaux SAN ?

Les réseaux SAN utilisent quatre protocoles courants pour transporter les données :

1. FCP (Fibre Channel Protocol) – Largement adopté, le protocole FCP utilise le réseau Fibre Channel pour envoyer des commandes SCSI. Il permet de livrer à grande vitesse des données brutes par blocs, sans pertes, entre le stockage informatique et les serveurs.

2. iSCSI (Internet Small Computer System Interface) – Utilisé par environ une entreprise sur dix, le protocole iSCSI est moins coûteux que le protocole FCP. Le protocole iSCSI mappe les données de stockage de bloc à l'aide de commandes SCSI encapsulées dans une trame Ethernet, puis utilise un réseau Ethernet TCP/IP standard pour le transport.

3. FCoE (Fibre Channel over Ethernet) – Le protocole FCoE vise essentiellement à placer le protocole FCP sur un nouveau lien physique par câble Ethernet. Ce simple commutateur permet au réseau SAN d'utiliser moins de matériel et de câblage, avec une installation et une gestion plus faciles qu'avec les protocoles traditionnels. Il s'agit d'un protocole basé sur des normes qui élimine également la nécessité de gérer des réseaux LAN et SAN distincts.

4. FC-NVMe (Non-Volatile Memory Express Over Fibre Channel) – Le protocole FC-NVMe est un protocole d'interface qui permet d'accéder au stockage flash via un bus PCI Express (PCIe). Il améliore considérablement les performances par rapport aux architectures traditionnelles 100 % flash (AHCI). Alors que les AHCI sont limitées à une seule file d'attente de commandes en série, les NVMe peuvent gérer des dizaines de milliers de files d'attente parallèles gérant chacune des dizaines de milliers de commandes simultanées.

4.4 – NAS (Network Attached Storage) :

4.4.1 – Qu'est-ce que le stockage NAS ?

Un **serveur de stockage en réseau**, également appelé stockage en réseau NAS, boîtier de stockage en réseau ou plus simplement NAS (de l'anglais ***Network Attached Storage***), est un **serveur de fichiers** autonome, relié à un **réseau**, dont la principale fonction est le **stockage** de données en un **volume** centralisé pour des clients réseau hétérogènes.

Ce type de stockage est aujourd'hui principalement utilisé par les particuliers ou les petites entreprises, qui peuvent y voir une alternative à l'hébergement **cloud**.

4.4.2 – Histoire de NAS :

Dès **1983**, Novell lance les serveurs NetWare, permettant le développement des réseaux locaux. En **1984**, Sun Microsystems développe **NFS** qui permet le partage de fichiers à travers un réseau. Il est bientôt suivi par le LAN Manager de Microsoft et Novell.

3com (pour Windows) et **Auspex Systems** (pour Unix) sont les premiers à commercialiser les **NAS** dédiés au début des années **1990**. Quelques ingénieurs d'**Auspex** créent le **NetApp** Filer intégré qui fonctionne avec des clients Windows et Unix simultanément. NetApp et Celerra d'EMC occupent alors le marché.

4.4.3 – Fonctionnement d’un serveur NAS :

Comme un serveur de fichiers, le stockage en réseau NAS fournit des services à travers un réseau IP avec un ou plusieurs des protocoles suivants :

- Common Internet File System (CIFS), aussi nommé Server Message Block (SMB) ;
    - Les machines Microsoft Windows utilisent ce protocole.
- Network File System (NFS) ;
    - Les systèmes Linux et UNIX utilisent ce protocole. NFS fonctionne sur tout matériel, système d'exploitation ou architecture réseau.
- Apple Filing Protocol (AFP).
    - Il s'agit d'un protocole propriétaire pour les appareils Apple fonctionnant sous macOS.

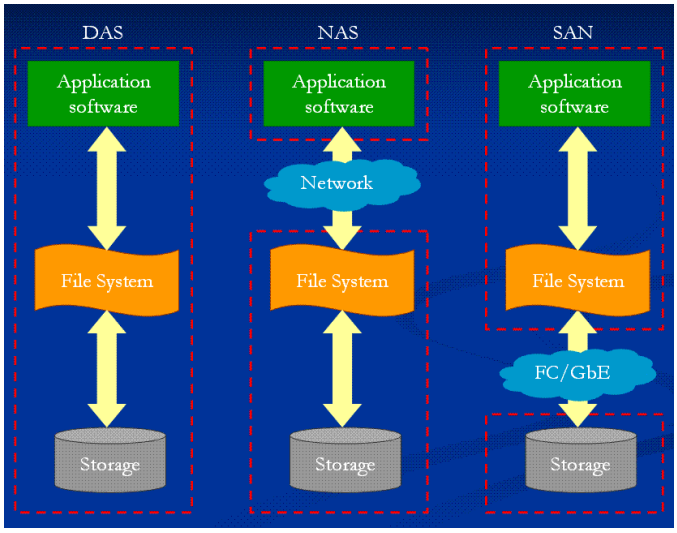
Parfois les fichiers sont disponibles *via* File Transfer Protocol (FTP), WebDAV et un gestionnaire de fichiers web. En général, le NAS est configuré *via* une interface web.

Le NAS se distingue :

- du Storage Area Network (SAN) qui utilise les protocoles comme SCSI, Fibre Channel, iSCSI, ATA over Ethernet (AoE) ou HyperSCSI à travers un réseau dédié ;

- du Direct Attached Storage (DAS), c'est-à-dire d'un disque dur directement connecté à l'ordinateur qui utilise les protocoles ATA, SATA, eSATA, SCSI, SAS et Fibre Channel *via* des câbles dédiés.

Le NAS peut s'intégrer à un SAN ou en être le point d'entrée.



_ Comparatif DAS/NAS/SAN _

4.4.4 – À quoi sert le stockage en réseau (NAS) ?

Les organisations utilisent les solutions NAS pour effectuer un certain nombre de tâches, dont les suivantes :

- Partage et stockage de fichiers.
- Créer des archives de données actives ou pour la sauvegarde des données et la reprise après sinistre.
- Héberger une infrastructure de bureau virtuel.
- Tester et développer des applications web et des applications web côté serveur.
- Diffuser de fichiers multimédia et des torrents.
- Stocker les images et les vidéos nécessitant un accès fréquent
- Créer un référentiel d'impression interne.

4.4.5 – la différence entre NAS et SAN :

Le NAS et le SAN sont tous deux des systèmes de stockage en réseau. Ils mettent en commun la capacité de stockage et la partagent avec les serveurs d'applications sur un réseau à haut débit. La principale différence entre eux est la manière dont l'utilisateur les perçoit. Pour les clients, le NAS fonctionne comme un système de fichiers et le SAN comme un système d'exploitation. Le NAS traite les demandes de fichiers individuelles, mais le SAN gère les demandes de blocs de données contigus. Les NAS et les SAN utilisent également des protocoles et des technologies sous-jacents différents. Le SAN est plus flexible pour les utilisateurs, mais il peut coûter plus cher à configurer et à gérer.

4.4.6 – Quelles sont les limites du NAS sur site ?

Le NAS est limité par son incapacité à fournir des performances à l'échelle.

Complexité de la gestion

La maintenance d'une infrastructure NAS sur site peut accroître la charge opérationnelle et réduire les budgets informatiques des organisations dont le budget et les ressources sont limités

Difficulté de mise à l'échelle

Les dispositifs NAS s'appuient sur des disques durs (HDD) pour servir les données. Malheureusement, si trop d'utilisateurs envoient des demandes de fichiers en même temps, le système NAS risque d'être submergé.

Aucune garantie de service

Le NAS ne peut offrir aucune garantie de service de stockage. Les utilisateurs peuvent rencontrer des problèmes tels que le décalage des données, des données manquantes et des pertes de données. Le NAS n'est pas assez fiable pour être utilisé pour des opérations stratégiques.

4.5 – RAID (Redundant Array of Independent Disks) :

4.5.1 – Qu’est-ce que le RAID ?

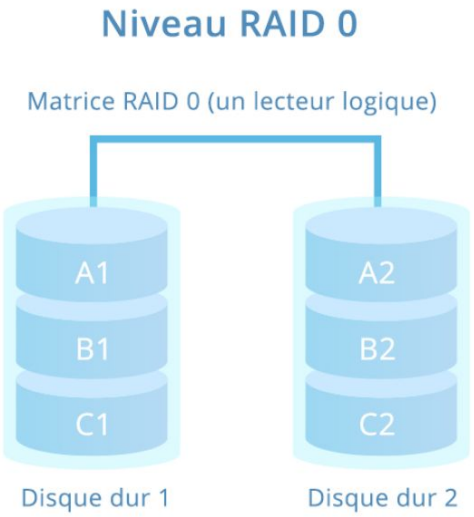
Le RAID informatique (**Redundant Array of Independent Disk**) est une technologie de virtualisation qui consiste à **répartir les données sur plusieurs disques durs séparés**. Le but est de pouvoir agir sur 3 points essentiels afin d’améliorer le système : **la performance, la sécurité, la tolérance aux pannes**.

RAID a été développé par trois informaticiens de l’Université de Californie à Berkeley en **1987**. Patterson, Gibson et Gatz ont établi une technologie permettant à **plusieurs disques durs d’être identifiés par le système comme une seule et unique entité**. Les résultats obtenus sur le système de stockage étaient les suivants : de meilleures performances, mais une mauvaise fiabilité. Afin d’apporter une amélioration sur la tolérance aux pannes, les informaticiens ont alors décidé d’adopter des architectures redondantes.

4.5.2 – Les configurations RAID les plus courantes :

Il existe plusieurs types de systèmes RAID qui agissent différemment selon la manière dont les données sont réparties sur le disque. Voici les plus courants :

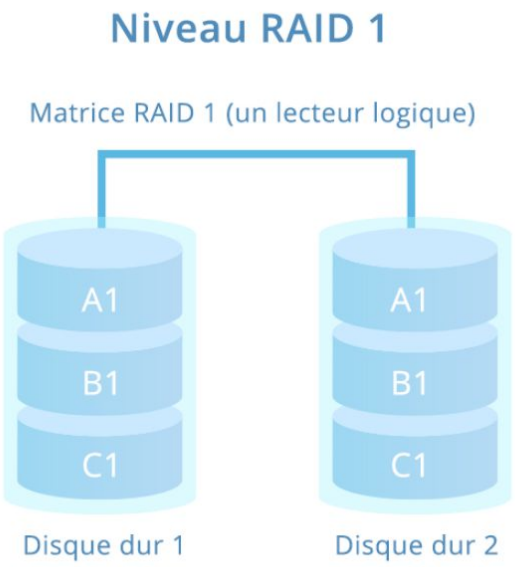
RAID 0



Le niveau RAID 0 ou volume agrégé par bandes (striping en anglais) est un système de répartition qui permet d'améliorer les performances du système. Il fonctionne en combinant au minimum deux disques durs fonctionnant simultanément. Alors, le stockage des données ainsi que les lectures et écritures sont exécutés en parallèle sur les disques. Selon le nombre de disques N, le serveur aura une performance N fois plus élevée et une vitesse de lecture et d'écriture N fois plus rapide.

Dans la configuration RAID 0, qui signifie zéro redondance, aucune donnée n'est dupliquée et il n'y a pas de perte de volume de stockage. Toutefois, ce manque de redondance peut affecter la sécurité des données, car si un disque venait à être défaillant, les données seront perdues.

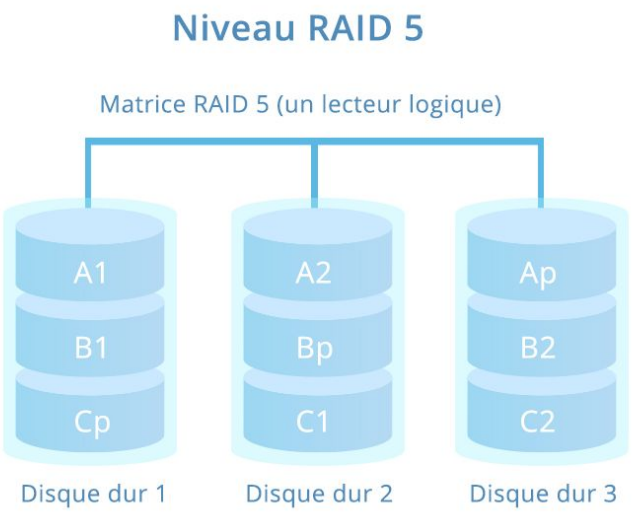
RAID 1



Le niveau RAID 1 ou disques en miroir (mirroring/shadowing en anglais) est un système de redondance qui permet d'améliorer la tolérance aux pannes matérielles. Comme son nom l'indique, le mirroring utilise un système de mise en miroir des données sur un minimum de deux disques durs. Ce qui signifie que les données sont dupliquées sur chaque disque, et peuvent être lues à partir de plusieurs disques (le lecteur d'origine et les lecteurs miroirs).

Comme toutes les données sont redondantes, le contenu est donc la même pour tous les disques. Si ce système de duplication est désavantageux pour l'espace de stockage, il reste cependant profitable pour la sécurité des données. Effectivement, même en cas de défaillance d'un des lecteurs, toutes les données sont stockées sur les autres lecteurs sans être affectée.

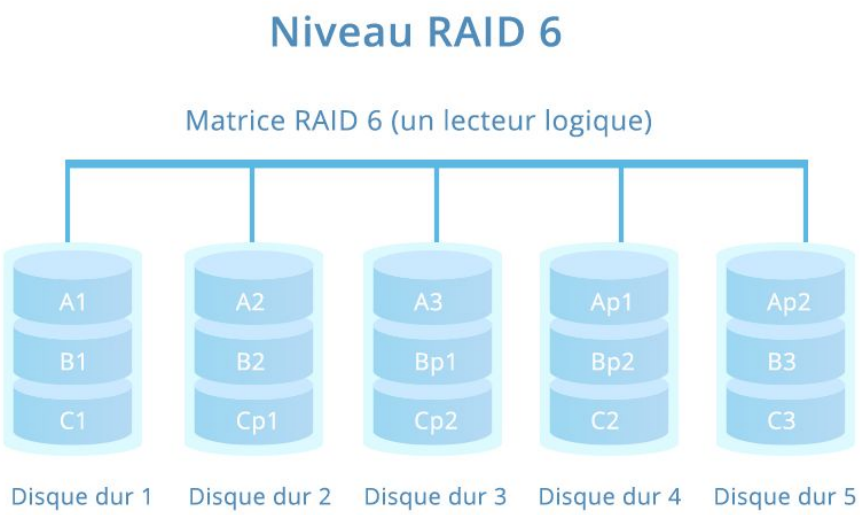
RAID 5



Le niveau RAID 5 ou volume agrégé par bandes à parité répartie est un système de répartition avec parité. Cette architecture utilise donc un stripping au niveau des blocs avec une parité distribuée.

Pour qu'il puisse fonctionner, un minimum de trois disques est nécessaire au niveau du système. Les données sont écrites de la même manière qu'un RAID 0 dans un bloc de données. En revanche, un autre bloc, le bloc de parité, sera ajouté par le contrôleur RAID. Ce bloc de parité agit comme un système de redondance RAID 1 pour protéger les données sur le disque. Dans ce cas, si un des disques est défaillant, les données peuvent être reconstituées sur un disque de remplacement grâce au bloc de parité.

RAID 6



Le RAID 6 est une évolution du RAID 5. Au lieu de dupliquer les données sur un disque, celui-ci les duplique sur N disques. La mise au point de cette technologie nécessite donc un minimum de 4 disques.

Au niveau de la sécurité, RAID 6 est donc N fois plus fiable que RAID 5, car il peut résister à la défaillance de N disques. Cependant, une baisse de performance peut être observée en raison du double calcul de parité.

RAID 10

Le niveau RAID 10 (ou RAID 1+0) est une combinaison du RAID 1 et du RAID 0. Dans une même grappe est effectuée la réplication du niveau 1; la mise en miroir du niveau 0, en revanche, est réalisée entre les grappes.

Pour pouvoir créer un volume RAID 10, il est nécessaire de disposer d'au moins 4 disques. Comme dans un niveau RAID 6, la moitié de l'espace de stockage est donc consacrée à la redondance. Toutefois, avec un niveau RAID 10, aucun calcul de parité n'est effectué, ce

qui garantit la performance du système. De plus, en cas de défaillance, la reconstruction des disques est nettement plus rapide.

4.5.3 – Comparaison des configurations RAID :

Certaines configurations RAID privilégient la sécurité des données, d'autres les performances ou l'accessibilité. Voici les propriétés qui permettent de différencier les niveaux RAID aujourd'hui.

Performances :

En termes de performances, les niveaux RAID 0 et RAID 10 sont les meilleurs. Effectivement, les disques travaillent simultanément dans ces configurations et il n'y a pas de calcul de parité.

Tolérance aux pannes :

Pour la tolérance aux pannes, il n'y a pas mieux que le niveau RAID 6. La redondance est effectuée sur tous les disques du serveur, ce qui signifie qu'une défaillance de N disques en même temps n'aurait aucun effet sur la fonctionnalité de la grappe.

Applications :

RAID 0 convient au stockage non critique comme les sauvegardes de fichier temporaires. Raid 1 est plus adapté aux bases de données ou applications qui nécessitent de petites capacités, mais une redondance complète des données. Quant à RAID 5, il est idéal pour les serveurs d'application ainsi que les serveurs de fichier ayant un nombre limité de disques. RAID 6, en revanche, convient aux applications avec un taux élevé de demandes de lectures, mais des demandes d'écritures plus faibles. Enfin, le niveau RAID 10 est destiné aux serveurs de base de données et d'applications avec un besoin de résilience importante et d'un bon débit de sortie.

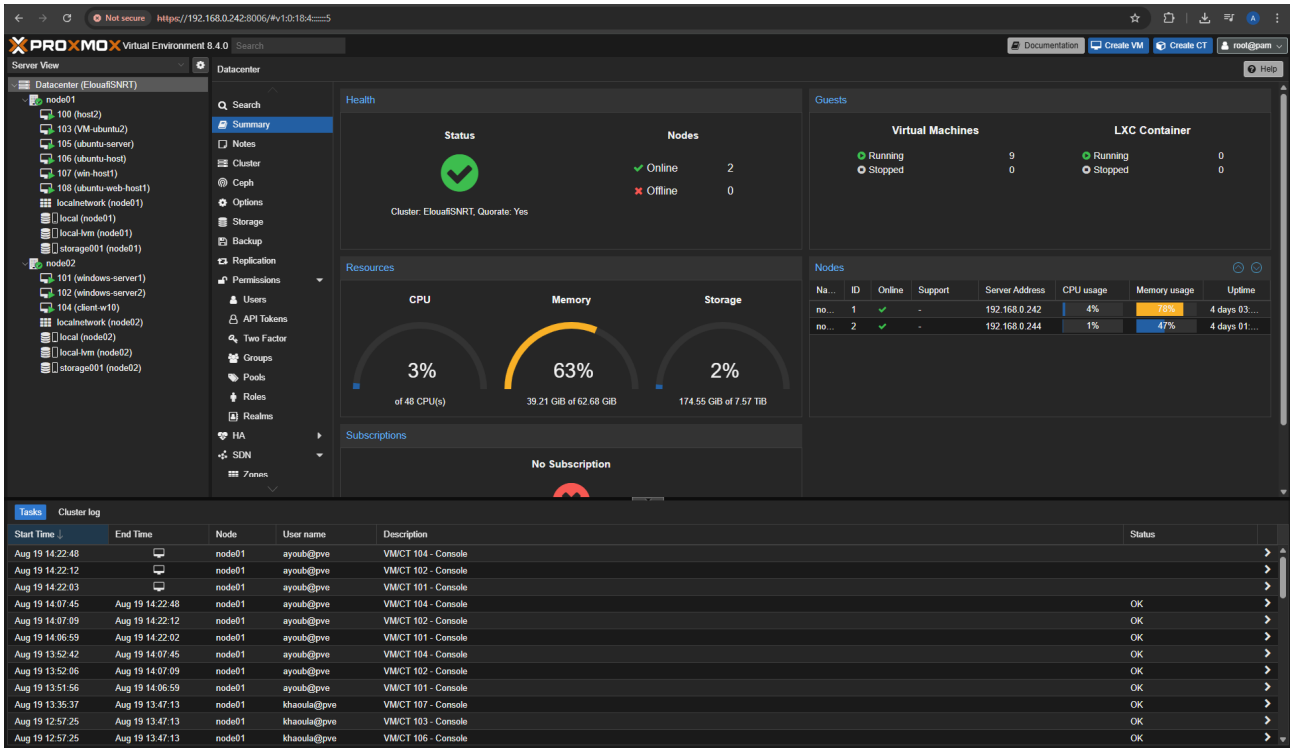
Coût :

En raison de la combinaison du stripping et de la mise en miroir, la configuration RAID 10 a un coût très élevé, tout comme le RAID 1.

S’ensuit, le RAID 6 qui a un coût élevé. En revanche, le coût du RAID 0 est faible, tandis que celui du RAID 5 est moyen.

5. Proxmox VE :

5.1 – Qu’est-ce que Proxmox VE ?



_ Proxmox VE Web Interface _

Proxmox Virtual Environment (PVE) est une solution de virtualisation libre et Open Source (licence AGPLv3) qui permet le déploiement de système virtualisés avec Linux **KVM** ou sur des **containers Linux LXC**, le stockage défini par logiciel et des capacités de mise en réseau de mise en réseau, sur une seule plateforme.

Proxmox permet donc de déployer des images KVM ou LXC qui peuvent être simplement paramétrées grâce à la puissante interface graphique intégrée au système.
L’interface permet une **gestion complète du réseau, des DNS, du stockage, ainsi que la définition d’autorisations sur mesure** pour répondre à vos besoins de virtualisation.

Proxmox Virtual Environment est constitué autour d'un socle Linux **Debian** auquel s'ajoute des composants développés par les équipes de Proxmox.

De nombreuses fonctionnalités avancées des hyperviseurs les plus connus (VMWare, Hyper-V) sont disponibles dans Proxmox et permettent une utilisation élaborée de la solution de virtualisaiton.

On pourra citer :

- Mise en cluster
- Haute disponibilité
- Réplication temps réel
- Utilisation de multiples solutions de stockage (LVM, BTRFS, NFS, SMB, GlusterFS, iSCSI, CephFS, RBD, …)
- Déploiement de Proxmox en SDN
- Multi-site
- Implémentation de iBGP/eBGP avec VXLAN / L2VPN / EVPN
- Intégration d'une solution de sauvegarde simple et efficace (avec Proxmox Backup Server)
- […]

5.2 – Caractéristiques principales de Proxmox VE :

Cluster haute disponibilité

- Gestion des paramètres HA pour KVM et LXC via GUI.
- Système de fichiers unique de Proxmox VE Cluster pmxcfs : Système de fichiers piloté par une base de données pour le stockage des fichiers de configuration, répliqué en temps réel sur tous les nœuds grâce à Corosync.
- Basé sur des technologies HA Linux éprouvées, fournissant un service HA stable et fiable.

Ligne de commande (CLI)

- Gérez tous les composants de votre environnement virtuel.
- CLI avec complétion intelligente des tabulations.
- Documentation complète des pages de manuel UNIX.

Interface de gestion web

- Intégré – pas besoin d'installer un outil de gestion séparé ou un nœud de gestion supplémentaire.
- Création rapide et facile de VMs et de conteneurs.
- Intégration transparente et gestion facile d'un cluster entier. d'un cluster entier.
- Interface rapide, axée sur la recherche, capable de gérer des milliers de VM.

Options de stockage flexibles

- Stockage local tel que ZFS (cryptage possible), Btrfs, LVM et LVMthin.
- Stockage partagé tel que CIFS, iSCSI ou NFS.
- Stockage distribué tel que Ceph RBD et CephFS.
- Prise en charge du cryptage pour Ceph OSD et ZFS.
- Nombre illimité de définitions de stockage (niveau cluster).

Migration en ligne temps réel

- Déplacez les machines virtuelles QEMU d'un hôte physique à un autre sans interruption de service.

Réseau virtualisé

- Options de configuration de réseau flexibles.
- Chaque hôte peut avoir jusqu'à 4094 ponts.

- Configuration TCP/IP simple.
- Support IPv4 et IPv6.
- Support pour les ponts et VLANs Linux.
- Intégration d'Open vSwitch.

Administration basée sur les rôles

- Gestion des utilisateurs et des autorisations pour tous les objets (VMs, systèmes de stockage, nœuds, etc.)
- Proxmox VE est livré avec un certain nombre de rôles prédéfinis (groupes de privilèges) qui couvrent les cas d'utilisation courants. Les privilèges contenus sont visibles dans l'interface graphique.
- Permissions pour contrôler l'accès aux objets (listes de contrôle d'accès). Chaque autorisation spécifie un sujet (utilisateur ou groupe) et un rôle (ensemble de privilèges) sur un chemin spécifique.

Pare-feu Proxmox VE intégré

- Prise en charge d'IPv4 et IPv6.
- Technologie Netfilter basée sur Linux. Pare-feu à gestion d'état fournissant une large bande passante.
- Distribué : avec la configuration principale dans le système de fichiers Proxmox VE en cluster et les règles iptable stockées dans les nœuds.
- Paramètrage à l'échelle du cluster.
- 3 niveaux de configuration (centre de données, hôte, VM/CT).
- Prise en charge des tables “brutes” ; permet la protection contre les attaques SYN flood.

5.3 – Comment installer Proxmox VE :

Proxmox recommande l'utilisation d'un matériel serveur de haute qualité pour l'exécution de Proxmox VE en production. Pour réduire

davantage l'impact d'une panne d'hôte, vous pouvez exécuter Proxmox VE dans un cluster avec des machines virtuelles et des conteneurs haute disponibilité (HA).

Proxmox VE peut utiliser le stockage local (DAS), le SAN, le NAS et le stockage distribué comme Ceph RBD.

5.3.1 – Configuration minimale requise pour l'évaluation :

Cette configuration minimale est fournie à des fins d'évaluation uniquement et ne doit pas être utilisée en production.

- **Processeur** : 64 bits (Intel 64 ou AMD64)
    - Processeur/carte mère compatible Intel VT/AMD-V pour la prise en charge complète de la virtualisation KVM
- **RAM** : 1 Go de RAM, plus RAM supplémentaire nécessaire pour les invités
- **Disque dur**
- **Une carte réseau (NIC)**

5.3.2 – Préparation du support d'installation :

Téléchargez **l'image ISO** du programme d'installation depuis : **https://www.proxmox.com/en/downloads/proxmox-virtual-environment/-iso**

Le support d'installation de Proxmox VE est une image ISO hybride.

Il fonctionne de deux manières :

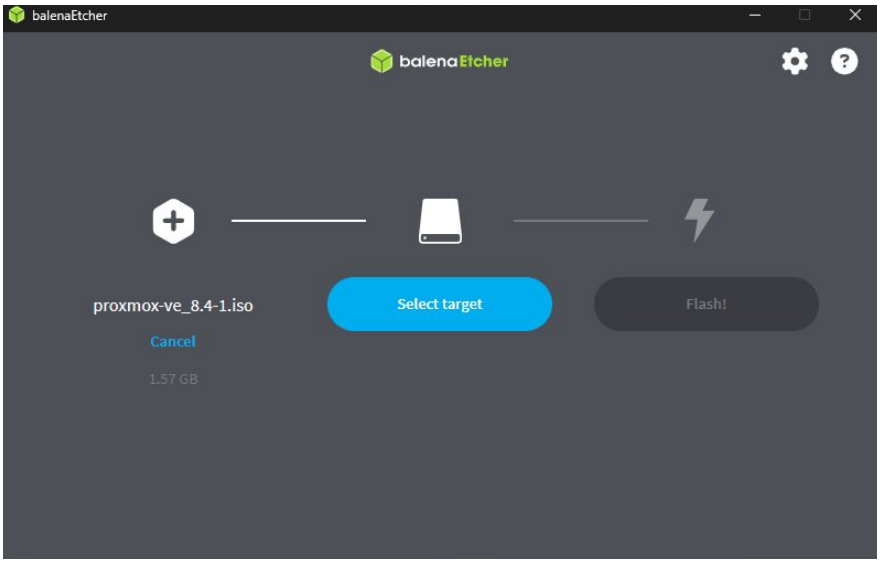
- Un fichier image ISO prêt à être gravé sur un CD ou un DVD ;
- Un fichier image IMG prêt à être copié sur une clé USB.

L'utilisation d'une clé USB pour installer Proxmox VE est recommandée, car c'est l'option la plus rapide.

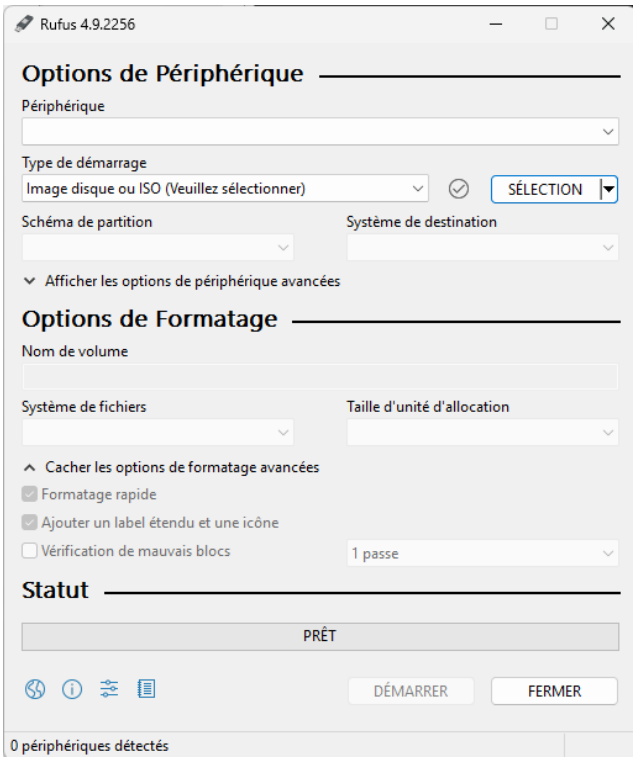
Instructions pour Windows :

Utilisation d'Etcher :

Etcher est prêt à l'emploi. Téléchargez Etcher depuis https://etcher.io. Il vous guidera tout au long du processus de sélection de l'ISO et de votre clé USB.



Utilisation de Rufus :



Rufus est une alternative plus légère, mais vous devez utiliser le mode DD pour le faire fonctionner. Téléchargez Rufus depuis https://rufus.ie/. Installez-le ou utilisez la version portable. Sélectionnez le lecteur de destination et le fichier ISO Proxmox VE.

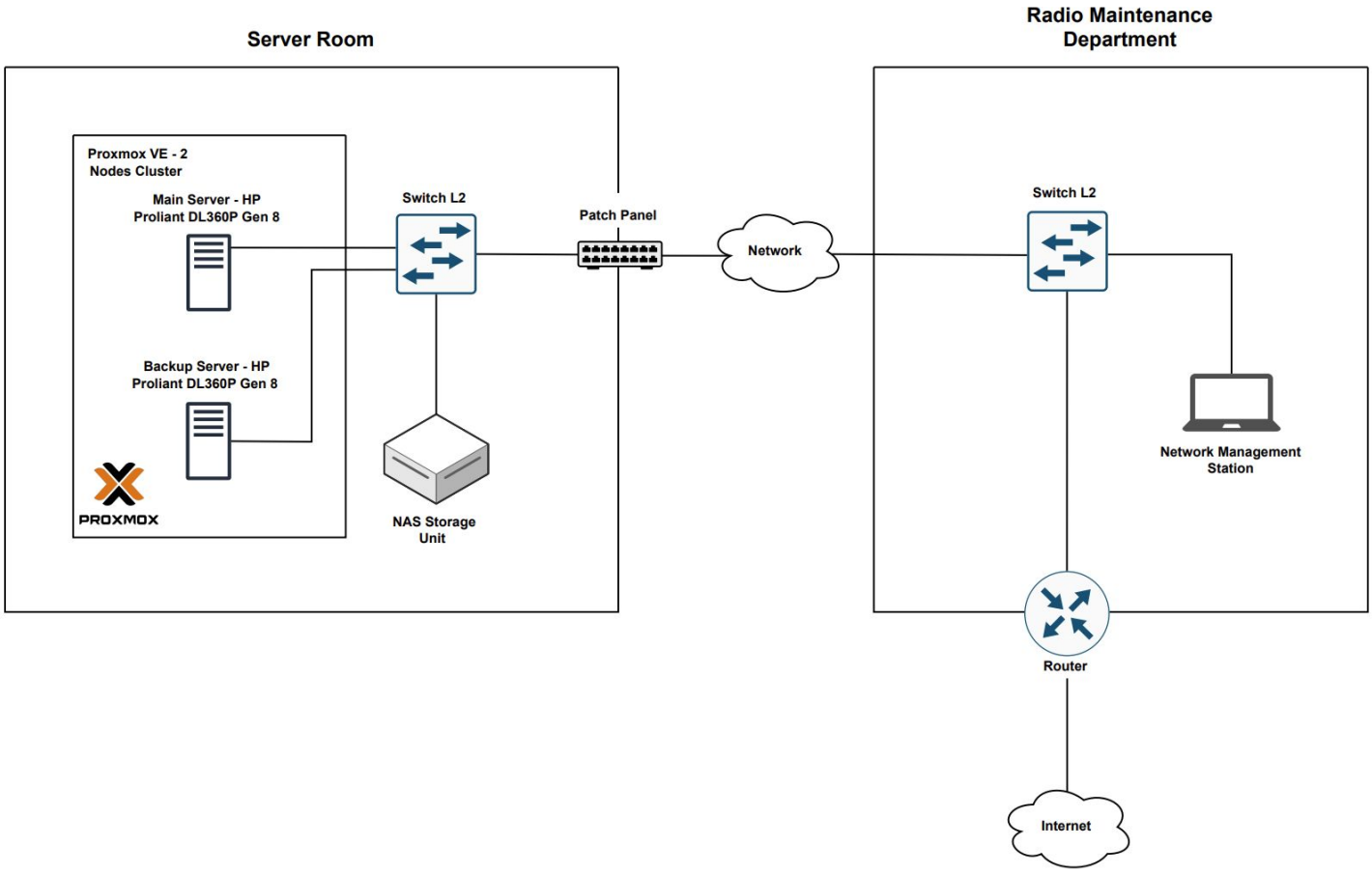
Important :

Une fois démarré, cliquez sur « Non » dans la boîte de dialogue vous demandant de télécharger une autre version de GRUB. Dans la boîte de dialogue suivante, sélectionnez le mode DD.

6. Mise en œuvre Technique :

Ce chapitre a pour objectif de détailler le processus technique de mise en œuvre de la plateforme de virtualisation. Il décrit de manière séquentielle chaque étape de la configuration du matériel et des logiciels, en passant de la préparation du stockage partagé à la création du cluster Proxmox. L'accent est mis sur les actions concrètes et les configurations spécifiques qui ont permis d'assembler tous les composants de l'infrastructure. Les résultats de ces configurations seront validés dans un chapitre ultérieur.

6.1 – Architecture Physique et Planification Réseau :



6.1.1 – Composant Physique :

- 2x Serveur HP ProLiant DL360p Gen8 :



Spécifications du Serveur :

- **Modèle** : HP ProLiant DL360p Gen8.
- **CPU** : 24 cœurs (2 Sockets) Intel Xeon E5-2620 v2, chacun cadencé à 2,10 GHz.
- **RAM** : 32 GiB.

Rappel :

Définition d'un Serveur informatique :

Un **serveur informatique** offre des services accessibles via un réseau. Il peut être matériel ou logiciel, c'est un ordinateur qui exécute des opérations suivant les requêtes effectuées par un autre ordinateur appelé « client ». C'est pourquoi on entend souvent parler de relation « client/serveur ». Par exemple, un utilisateur (côté client) va rechercher un site internet en utilisant un navigateur web, pour que ce dernier puisse l'afficher il va effectuer une requête au serveur HTTP qui est un serveur web.

- **Un Stockage NAS LenovoEMC px6-300d :**



Spécifications :

- Capacité : 7.7 TiB.

- **Switch (Commutateur réseau):**



Rappel :

Définition d'un Switch :

un **commutateur (ou switch en anglais)** est un équipement qui permet de créer des circuits virtuels entre deux périphériques (tels que des ordinateurs, des serveurs, des imprimantes, d'autres commutateurs, etc.) à l'aide de liens (câbles ou fibres) qui les relient à ces périphériques.

- Panneau de brassage (Patch Panel) :



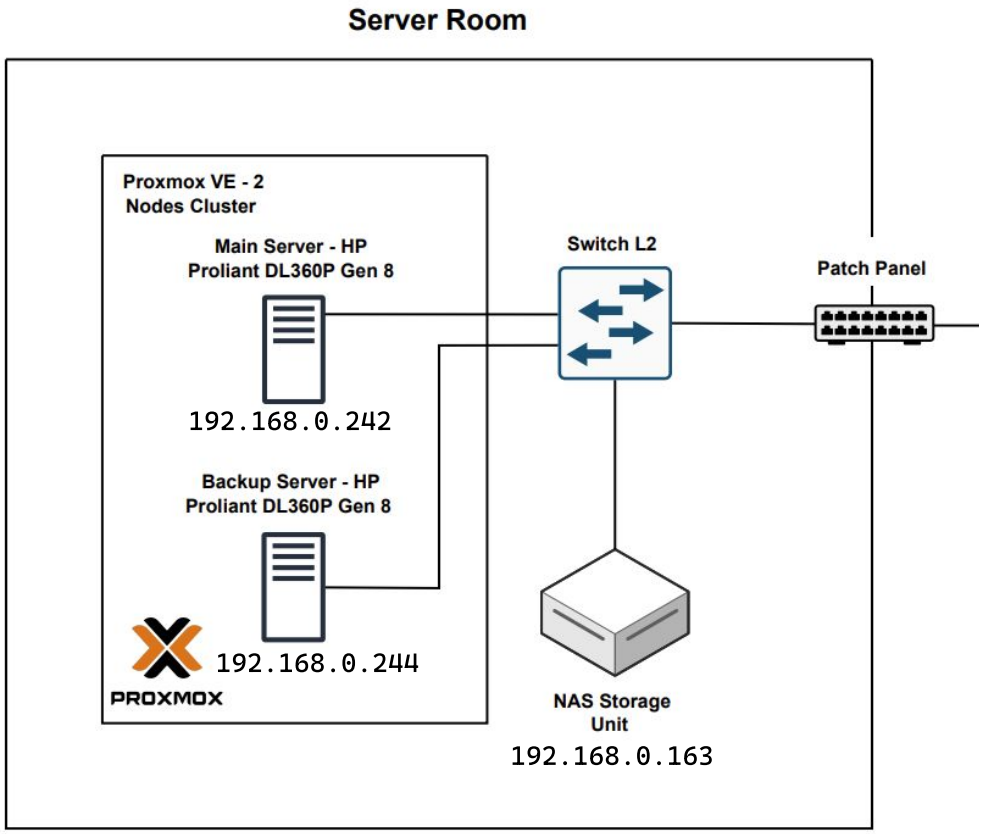
Rappel :

Qu'est-ce qu'un panneau de brassage ?

Un panneau de brassage, également appelé "patch bay", "patch field" ou "jack field", est un assemblage de matériel monté qui contient un nombre déterminé de ports pour connecter et gérer les câbles en fibre ou en cuivre entrants et sortants. Dans une infrastructure de centre de données typique, les panneaux de brassage sont souvent placés dans une armoire de câblage pour relier les racks entre eux. Chaque rack contient au moins un panneau de brassage, dont la partie arrière est reliée à un autre panneau. Ensuite, des câbles de raccordement sont nécessaires pour connecter les serveurs ou les commutateurs réseau aux ports situés sur la face frontale du panneau de brassage de chaque rack.

Un panneau de brassage peut fournir des méthodes de brassage d'interconnexion ou de connexion croisée pour épisser et terminer les câbles. Ce système fonctionne en terminant les éléments de câble et en acheminant les signaux vers la destination finale via les câbles de raccordement. Lorsqu'on utilise des panneaux de brassage, il suffit de brancher ou de débrancher les câbles de raccordement correspondants pour organiser les circuits, ce qui permet de créer des connexions flexibles et d'améliorer considérablement l'efficacité.

6.1.2 – Plan d'adressage réseau :



- **Adresse réseau** : 192.168.0.0\24
- **Gateway** : 192.168.0.1
- **Main Server** : 192.168.0.242 , **Numéro de Port** : 8006

```
C:\Users\elouafi>ssh root@192.168.0.242
root@192.168.0.242's password:
Linux node01 6.8.12-9-pve #1 SMP PREEMPT_DYNAMIC PMX 6.8.12-9 (2025-03-16T19:18Z) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Aug 22 10:17:47 2025
root@node01:~# ip A
Object "A" is unknown, try "ip help".
root@node01:~# ip a
10: vmbr0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 40:a8:f0:2d:ee:ac brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.242/24 scope global vmbr0
       valid_lft forever preferred_lft forever
    inet6 fe80::42a8:f0ff:fe2d:eeac/64 scope link
       valid_lft forever preferred_lft forever
```

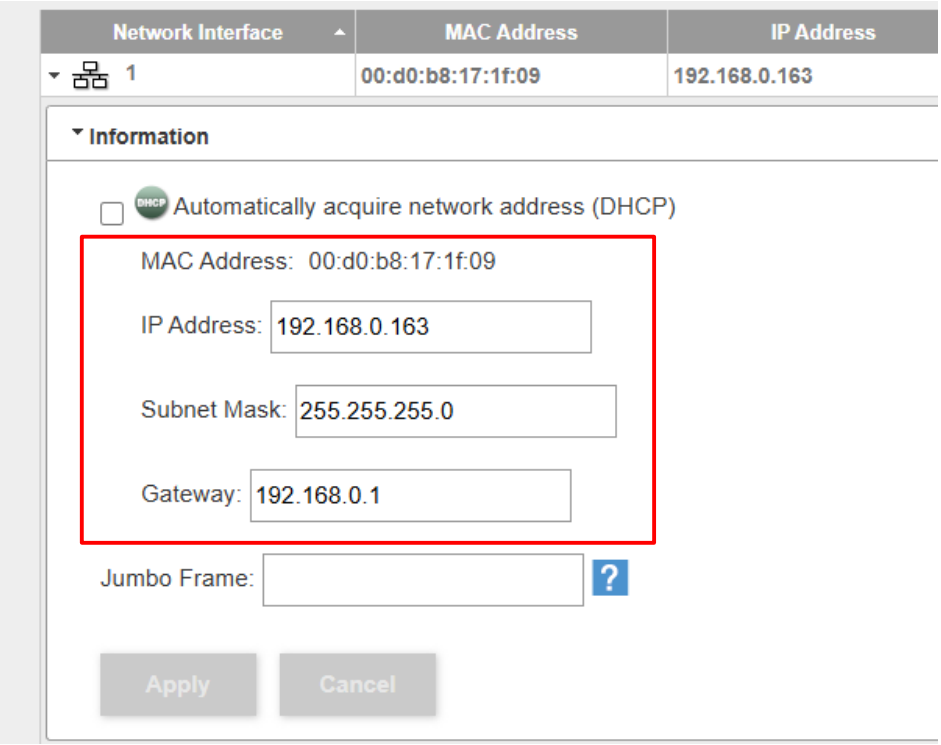
- **Backup Server** : 192.168.0.244 , **Numéro de Port** : 8006

```
C:\Users\elouafi>ssh root@192.168.0.244
root@192.168.0.244's password:
Linux node02 6.8.12-9-pve #1 SMP PREEMPT_DYNAMIC PMX 6.8.12-9 (2025-03-16T19:18Z) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Aug 13 13:36:34 2025
root@node02:~# ip a
10: vmbr0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 40:a8:f0:2d:ea:68 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.244/24 scope global vmbr0
       valid_lft forever preferred_lft forever
    inet6 fe80::42a8:f0ff:fe2d:ea68/64 scope link
       valid_lft forever preferred_lft forever
```

- **NAS Storage Unit** : 192.168.0.163



6.2 – Configuration des Serveurs et du Cluster :

Avant de procéder à l'installation et à la configuration de Proxmox VE sur les deux serveurs, nous avons installé un **console KVM** dans l'armoire serveur pour en permettre le contrôle direct.



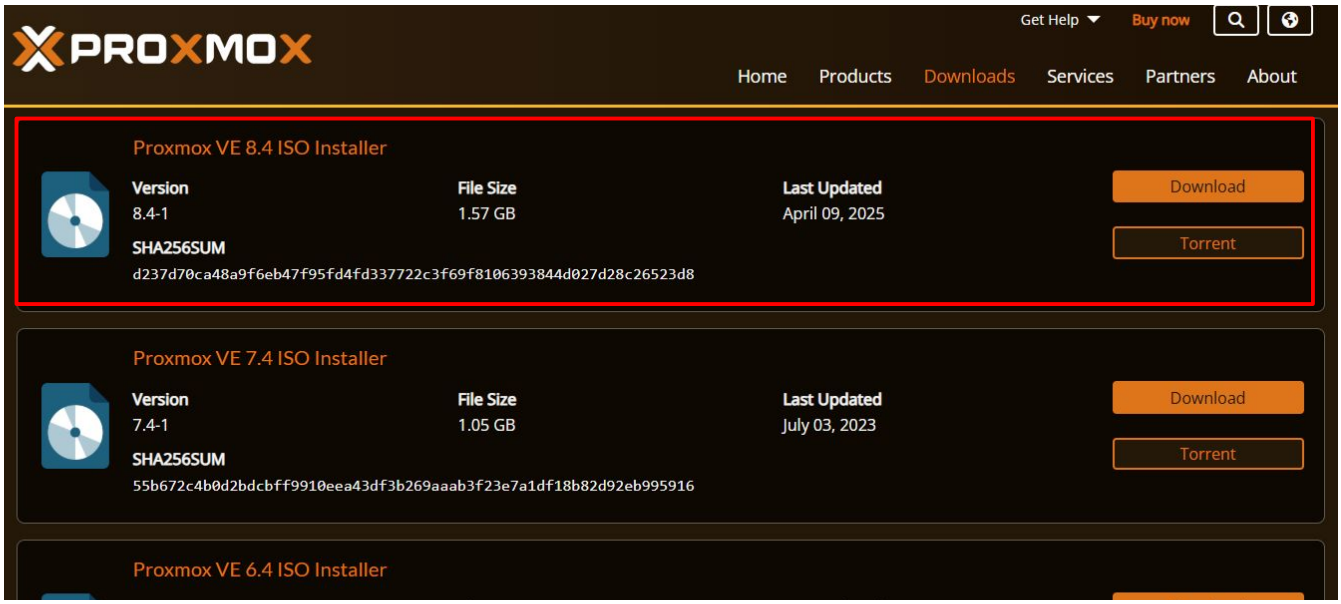
Qu’est-ce qu’un commutateur KVM ?

KVM signifie « **Clavier, Vidéo (moniteur), Souris** ». La principale fonction d’un commutateur KVM est de contrôler, de commuter et de gérer plusieurs PC ou serveurs à l’aide d’un seul clavier, d’un seul écran et d’une seule souris (également appelé « console »).

Ce dispositif améliore la productivité, économise de l’espace et de l’argent en vous permettant d’utiliser plusieurs ordinateurs avec un seul ensemble clavier, écran et souris. Cette fonction exclusive offre aux administrateurs informatiques une mise à jour et une maintenance centralisées en temps réel.

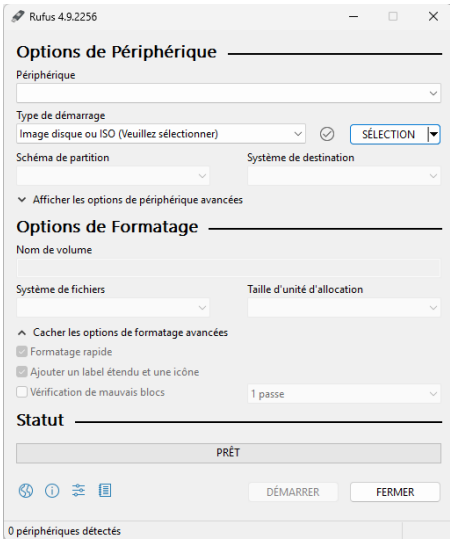
6.2.1 – Installation de Proxmox VE sur les deux serveurs :

Etape 1 : Télécharger Proxmox VE depuis le site : https://www.proxmox.com/en/downloads/proxmox-virtual-environment/iso





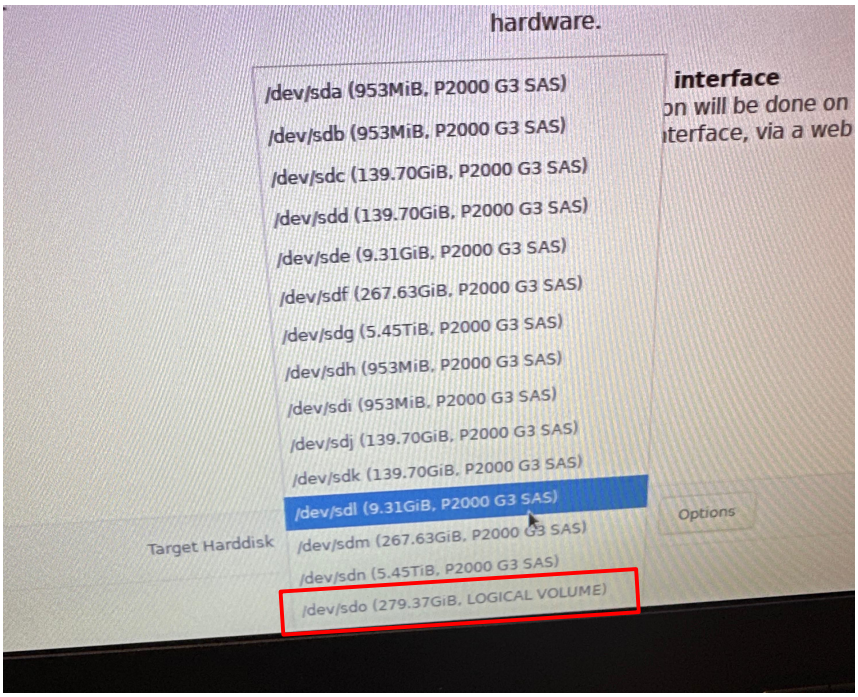
Etape 2 : Copié le fichier ISO sur une clé USB en utilisant Rufus ou BalenaEtcher .

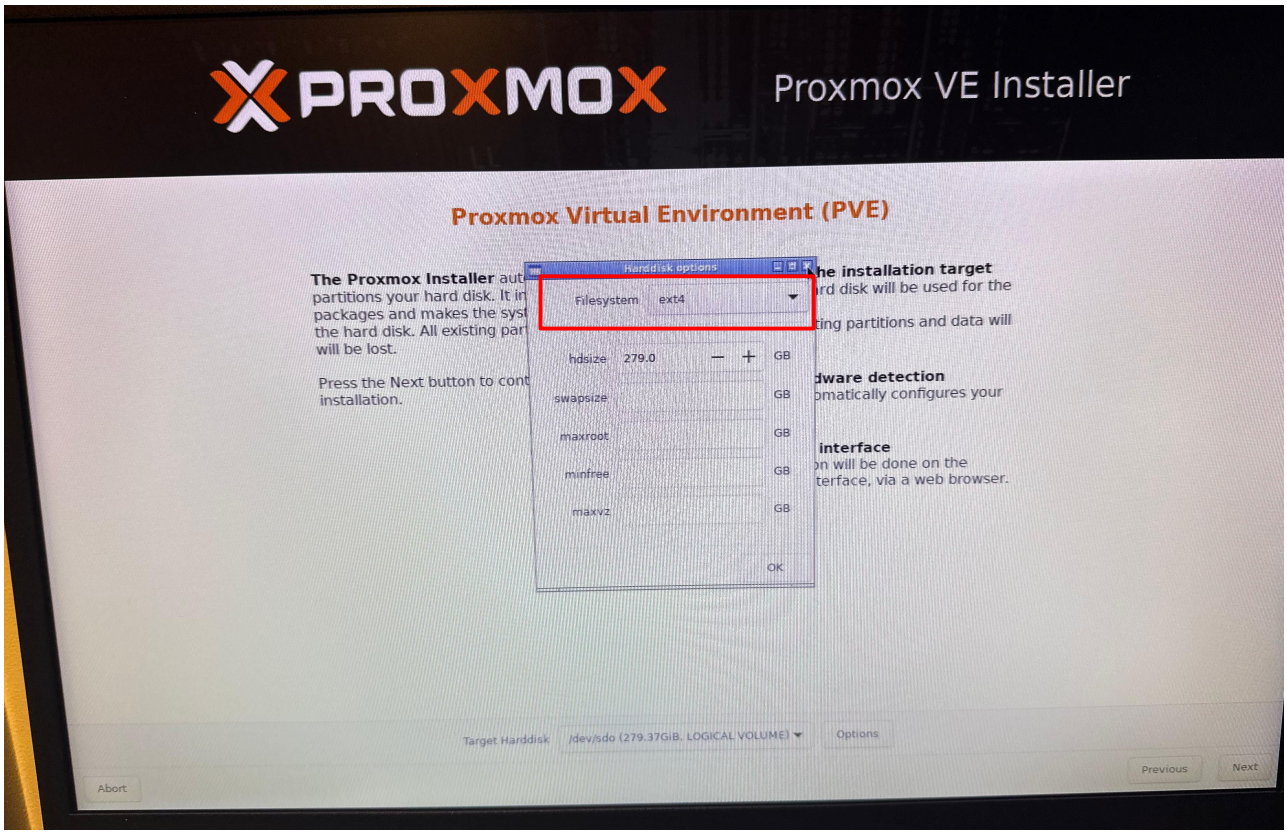


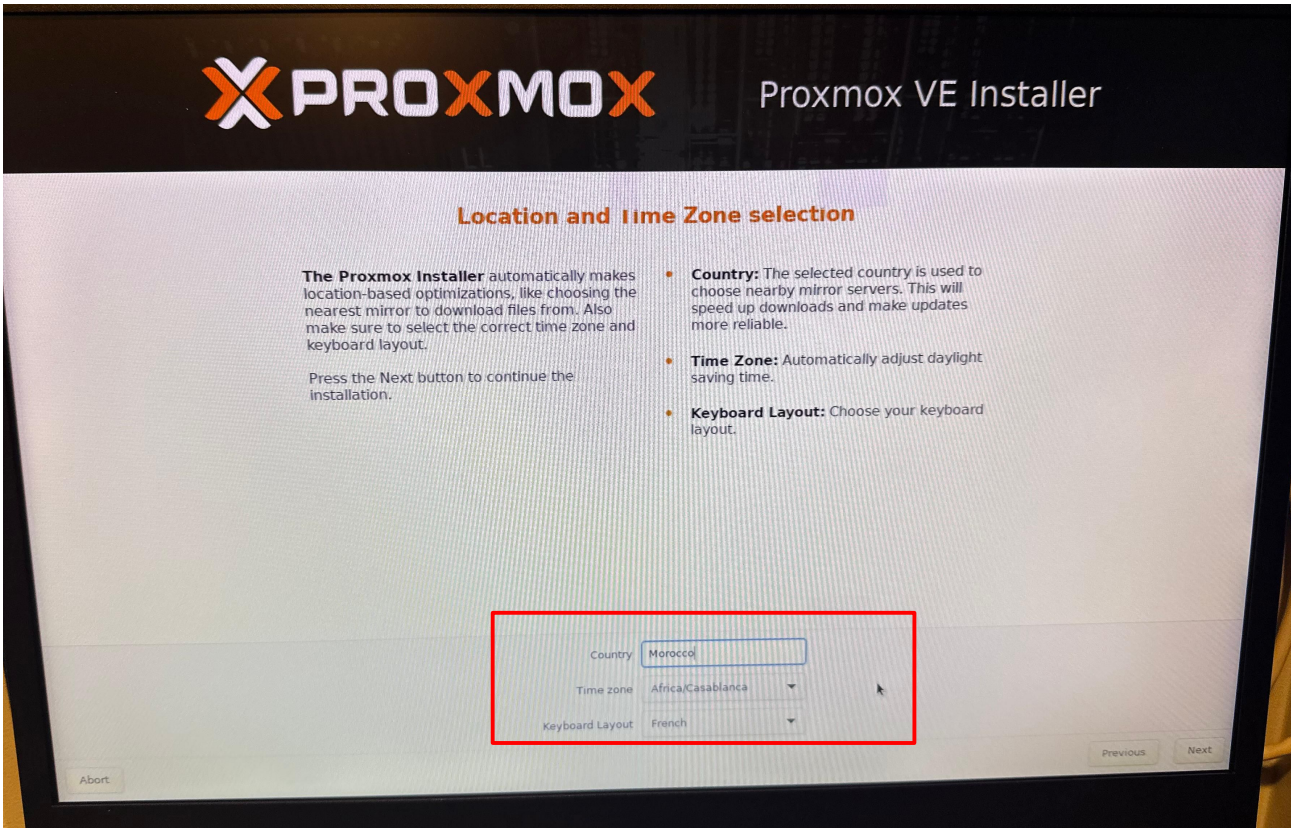
Etape 3 : Insérer la clé USB dans les deux Serveurs pour installer Proxmox VE .

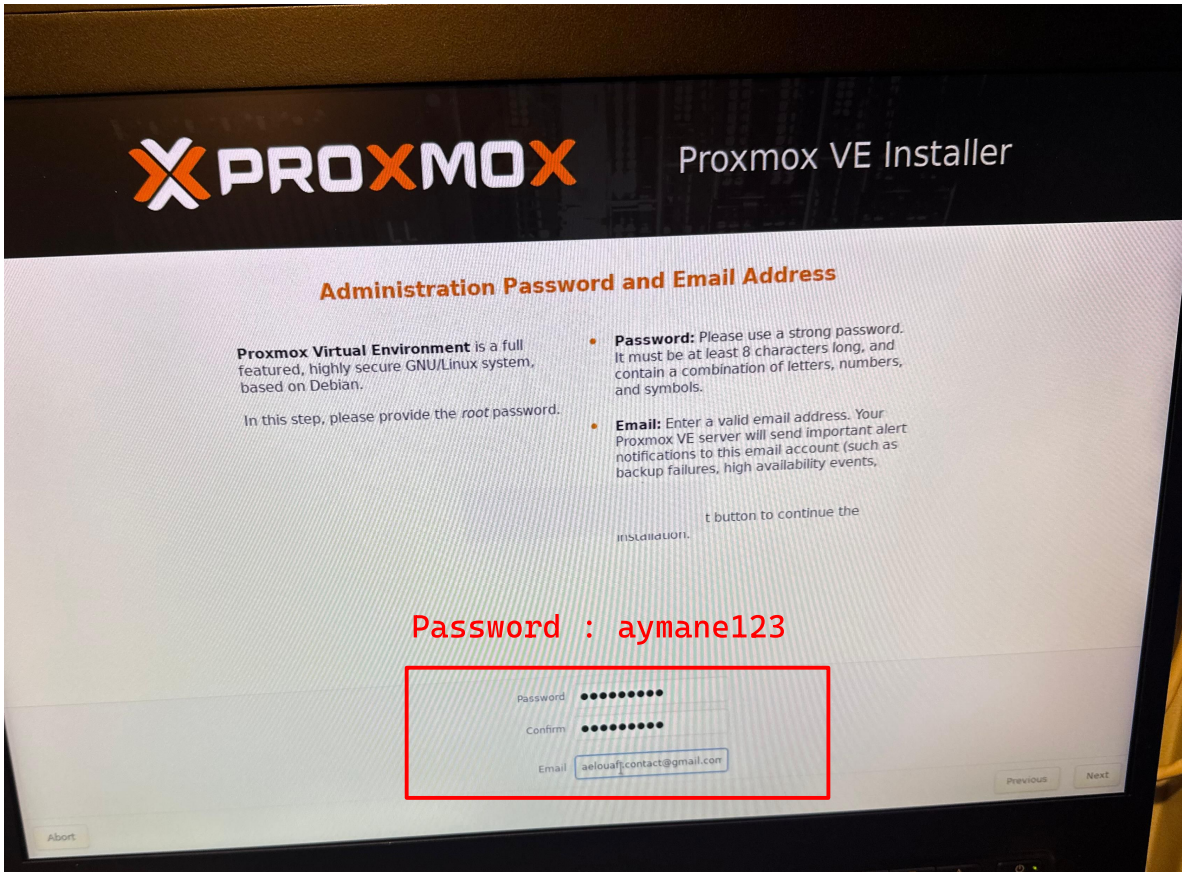
1er Serveur :

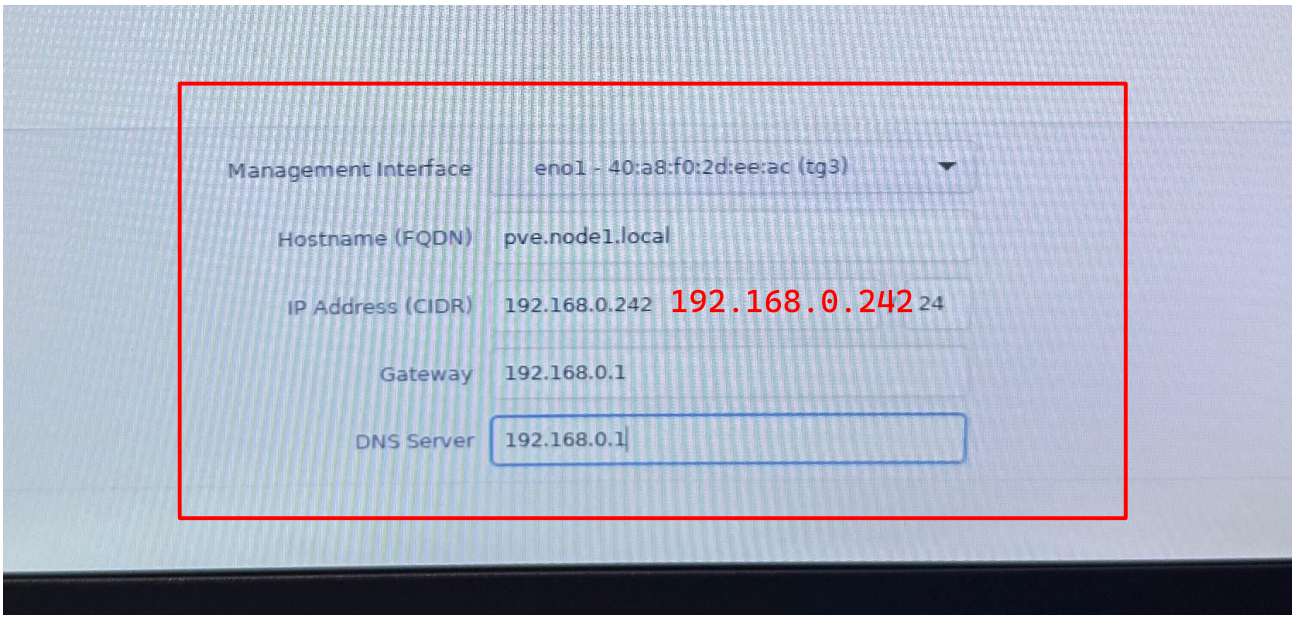


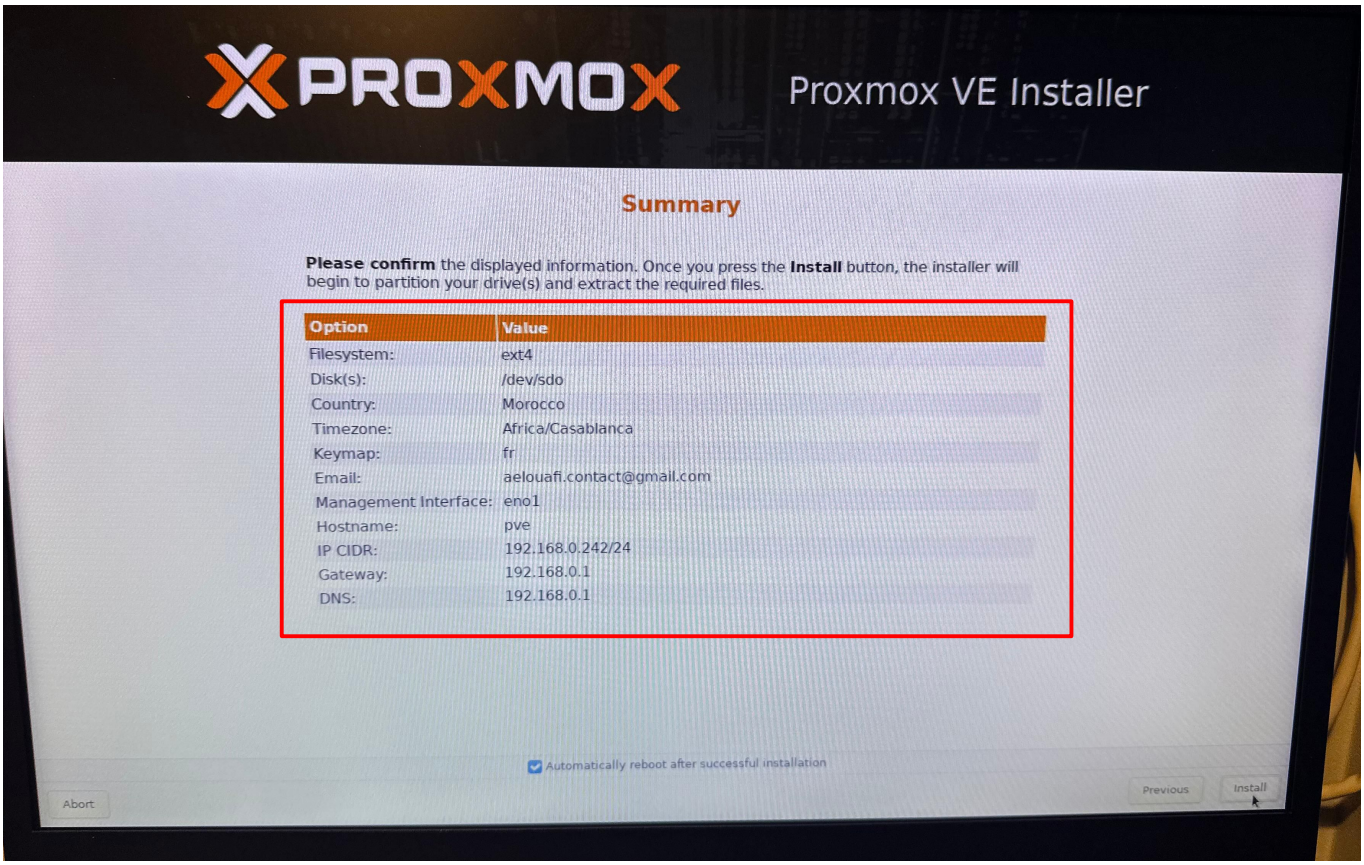


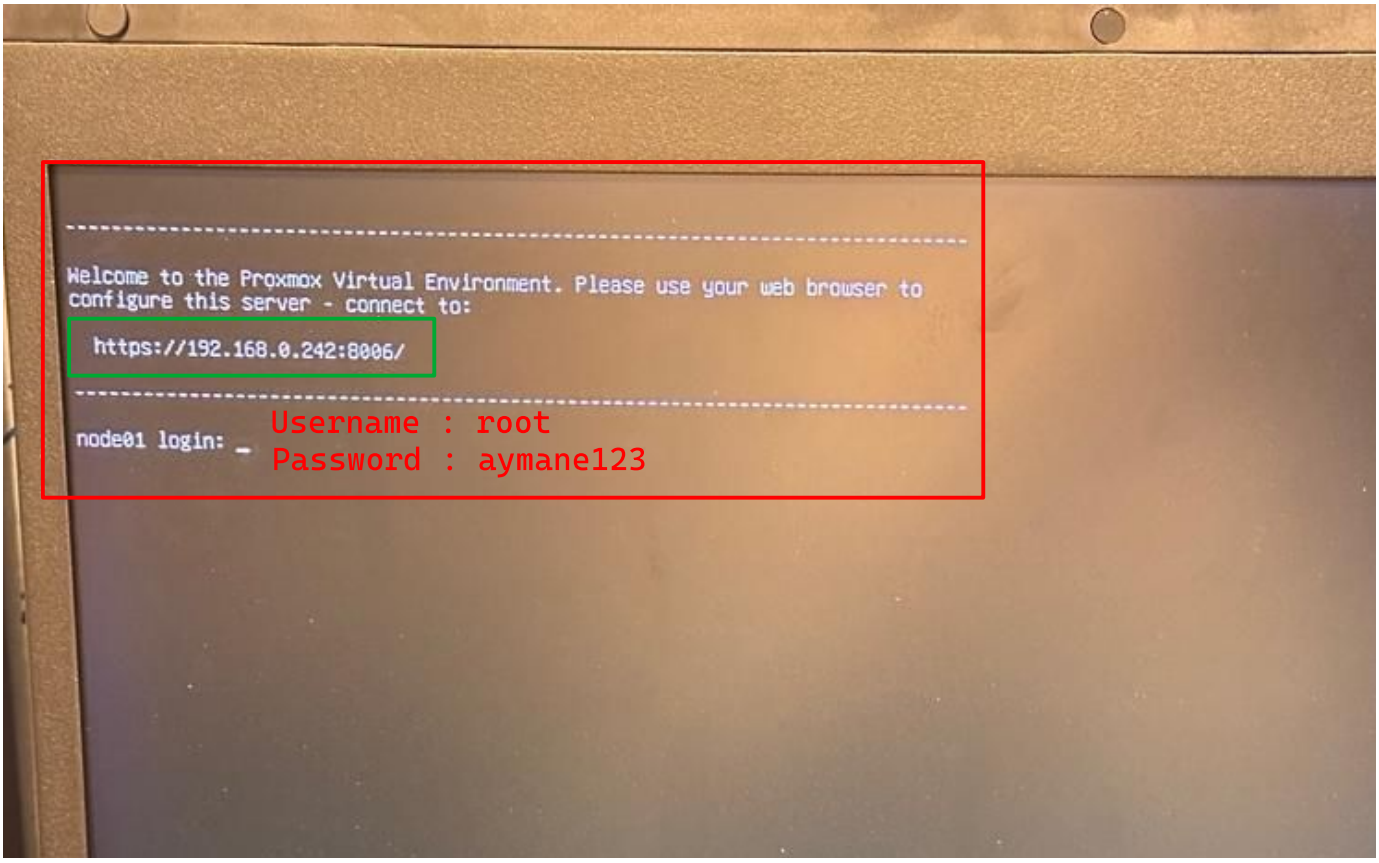

PROXMOX
Proxmox VE Installer
Proxmox Virtual Environment (PVE)
The Proxmox Installer aut
partitions your hard disk. It in
packages and makes the syst
the hard disk. All existing par
will be lost.
Press the Next button to cont
installation.
Harddisk options
Filesystem ext4
hdsize 279.0
swapsize
maxroot
minfree
maxvz
GB
OK
he installation target
rd disk will be used for the
ting partitions and data will
dware detection
omatically configures your
interface
n will be done on the
terface, via a web browser.
Target Harddisk /dev/sdo (279.37GiB, LOGICAL VOLUME)
Options
Abort
Previous
Next


PROXMOX
Proxmox VE Installer
Location and Time Zone selection
The Proxmox Installer automatically makes location-based optimizations, like choosing the nearest mirror to download files from. Also make sure to select the correct time zone and keyboard layout.
Press the Next button to continue the installation.
Country: The selected country is used to choose nearby mirror servers. This will speed up downloads and make updates more reliable.
Time Zone: Automatically adjust daylight saving time.
Keyboard Layout: Choose your keyboard layout.
Country Morocco
Time zone Africa/Casablanca
Keyboard Layout French
Abort
Previous
Next

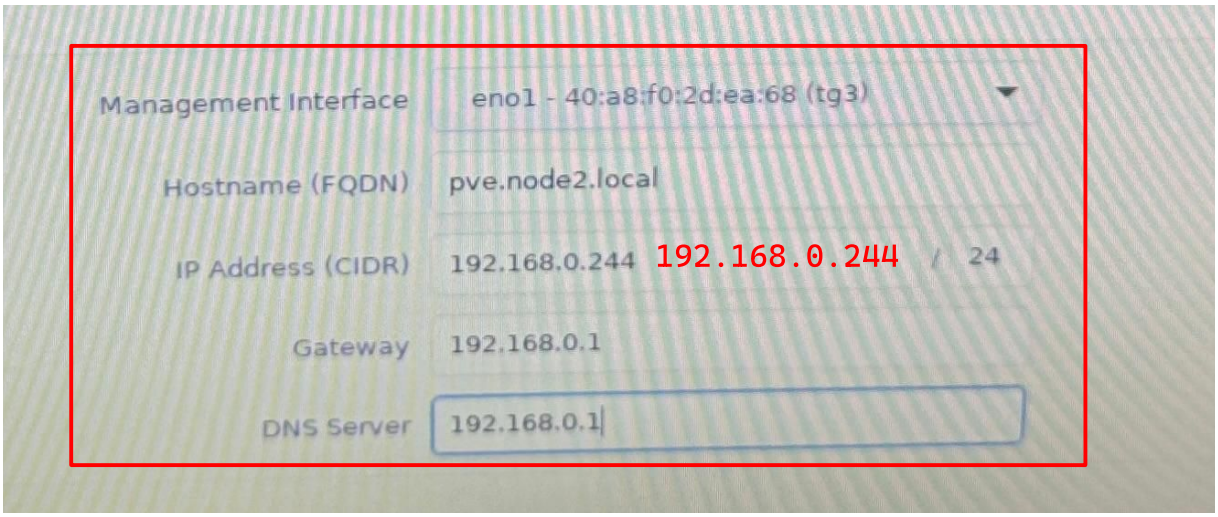

PROXMOX
Proxmox VE Installer
Administration Password and Email Address
Proxmox Virtual Environment is a full featured, highly secure GNU/Linux system, based on Debian.
In this step, please provide the root password.
Password: Please use a strong password. It must be at least 8 characters long, and contain a combination of letters, numbers, and symbols.
Email: Enter a valid email address. Your Proxmox VE server will send important alert notifications to this email account (such as backup failures, high availability events,
t button to continue the installation.
Password : aymane123
Password
Confirm
Email
aelouafi.contact@gmail.com
Abort
Previous
Next

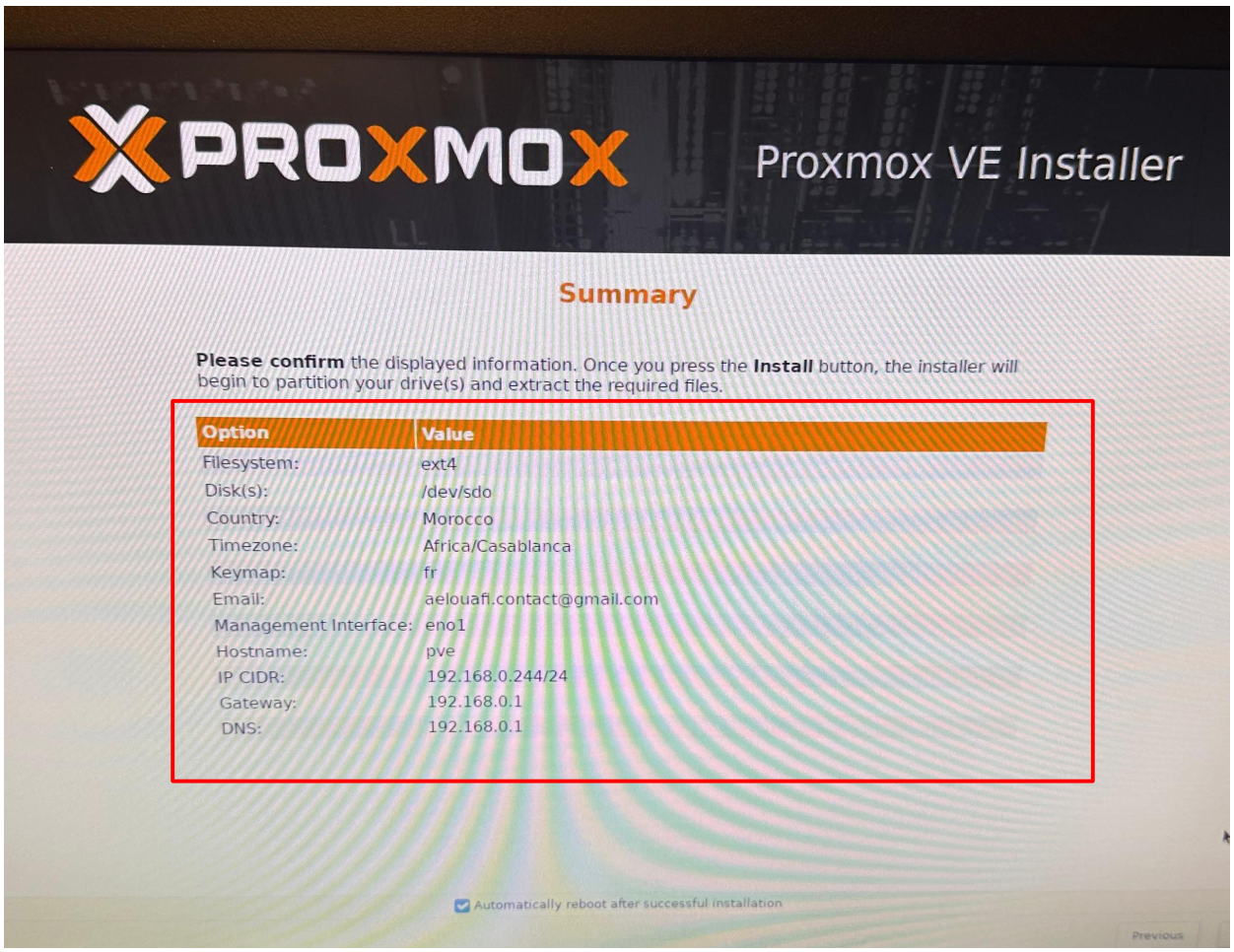

Management Interface
eno1 - 40:a8:f0:2d:ee:ac (tg3)
Hostname (FQDN)
pve.node1.local
IP Address (CIDR)
192.168.0.242
192.168.0.242 24
Gateway
192.168.0.1
DNS Server
192.168.0.1

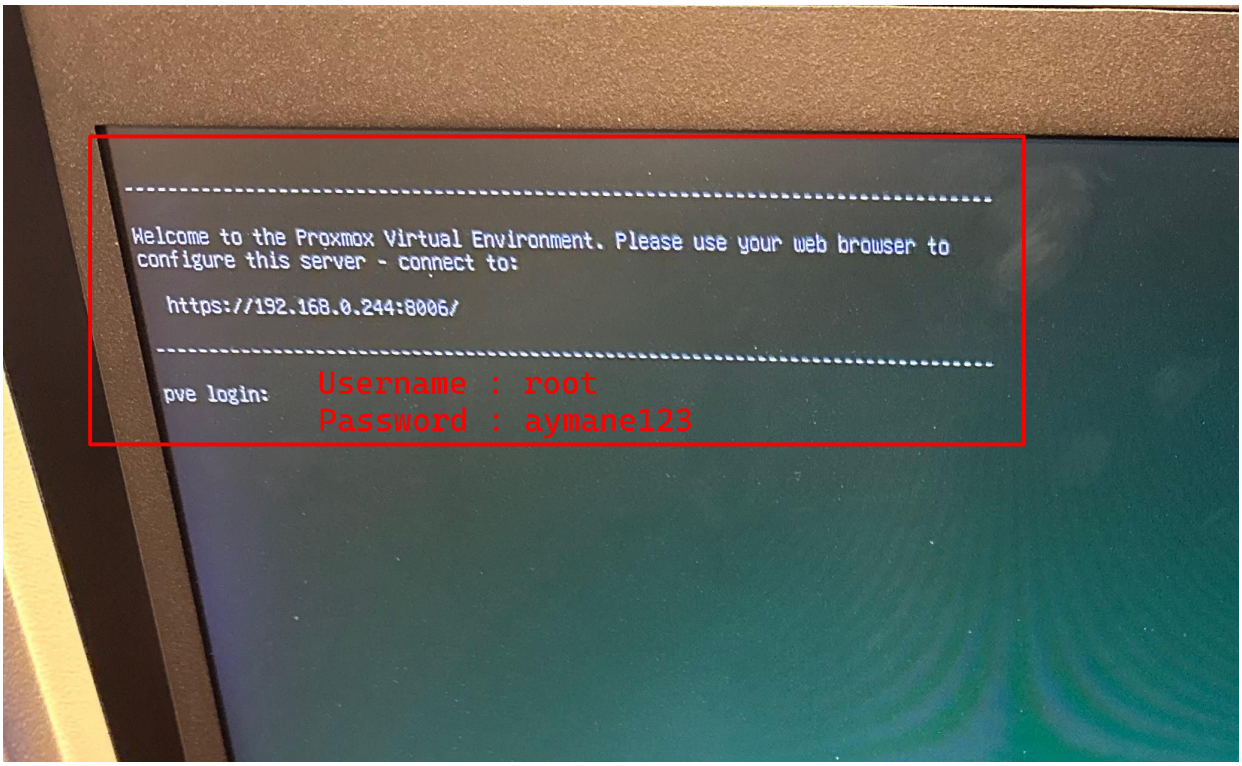

PROXMOX
Proxmox VE Installer
Summary
Please confirm the displayed information. Once you press the Install button, the installer will begin to partition your drive(s) and extract the required files.
Option
Value
Filesystem: ext4
Disk(s): /dev/sdo
Country: Morocco
Timezone: Africa/Casablanca
Keymap: fr
Email: aelouafi.contact@gmail.com
Management Interface: eno1
Hostname: pve
IP CIDR: 192.168.0.242/24
Gateway: 192.168.0.1
DNS: 192.168.0.1
Automatically reboot after successful installation
Abort
Previous
Install


Welcome to the Proxmox Virtual Environment. Please use your web browser to configure this server - connect to:
https://192.168.0.242:8006/
node01 login: _
Username : root
Password : aymane123

2éme Serveur : refaire les mêmes étapes .

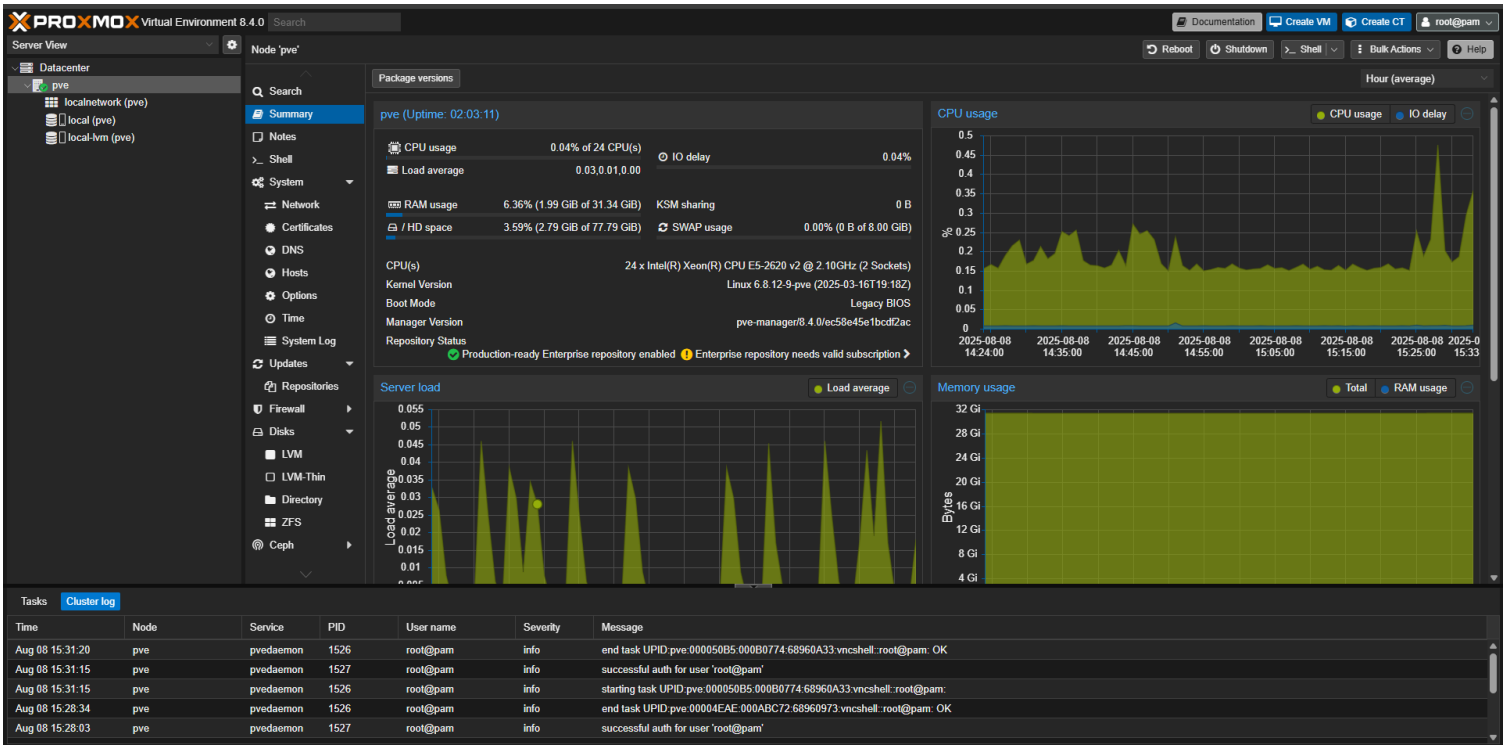






Interface Web des serveurs :

- serveur 1 : http://192.168.0.242:8006/
- serveur 2 : http://192.168.0.244:8006/



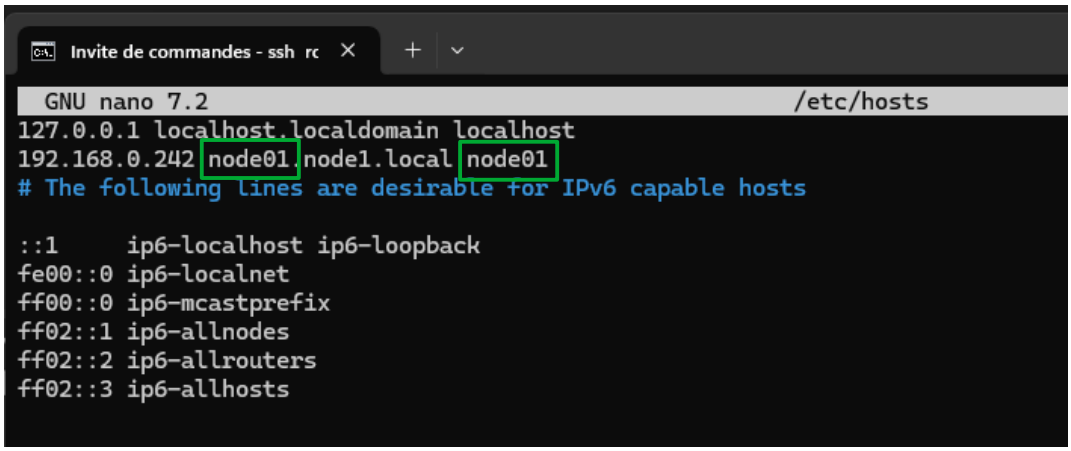
6.2.2 – Configuration du Cluster :

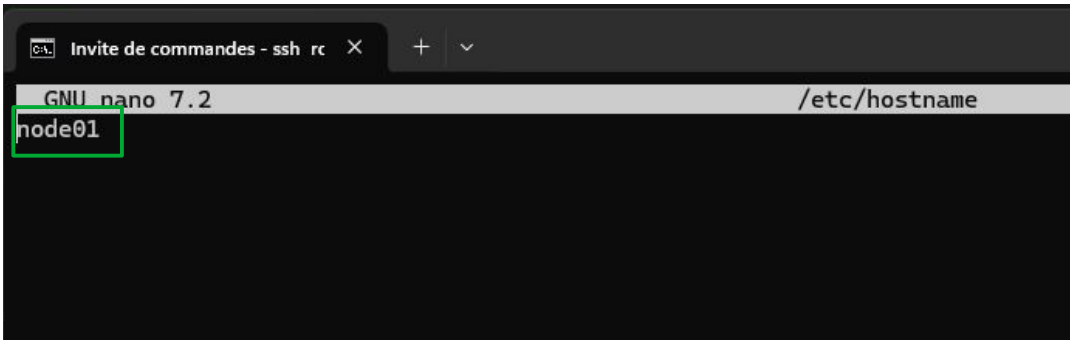
6.2.2.1 – Modification des noms de nœuds :

Avant la création du cluster, un problème a été identifié : les deux nœuds partageaient le même nom d'hôte (hostname : ‘**pve**’). Pour que le cluster puisse être créé, il a été nécessaire d'attribuer un nom unique à chaque nœud.

Pour cela , on doit modifier les fichiers /etc/host , /etc/hostname et /etc/postfix/main.cf , on a changé le **hostname** ‘pve’ vers ‘node01’ et ‘node02’.

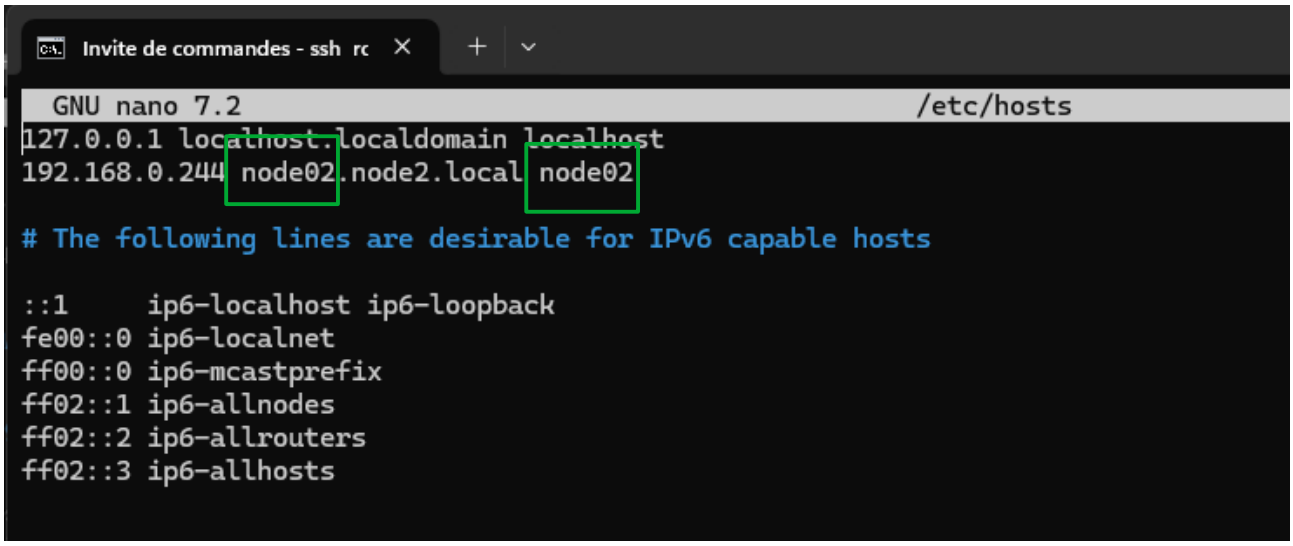
- Node01 :

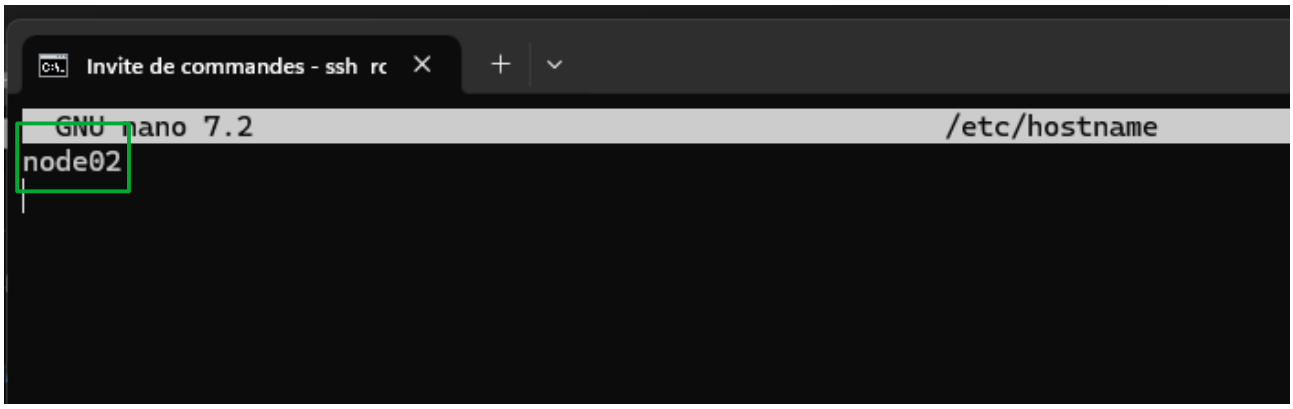


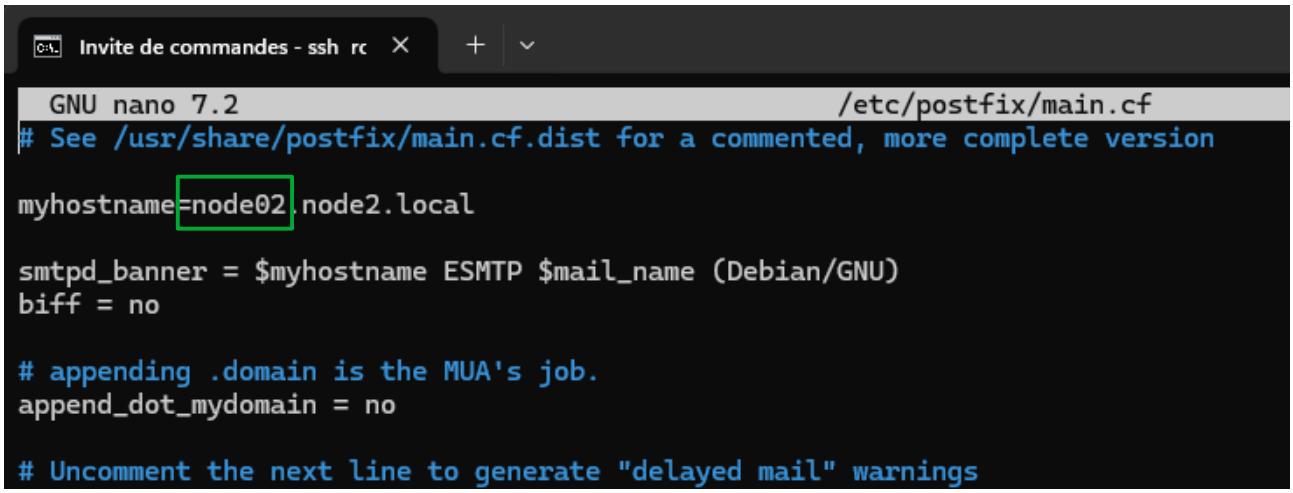




- Node02 :

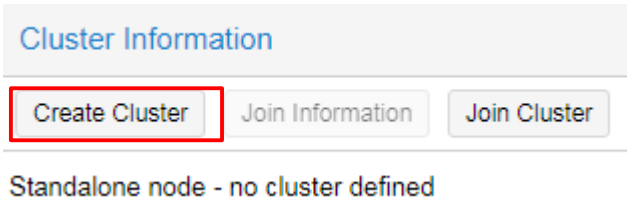

Invite de commandes - ssh rc
GNU nano 7.2 /etc/hosts
127.0.0.1 localhost.localdomain localhost
192.168.0.244 node02.node2.local node02
The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts

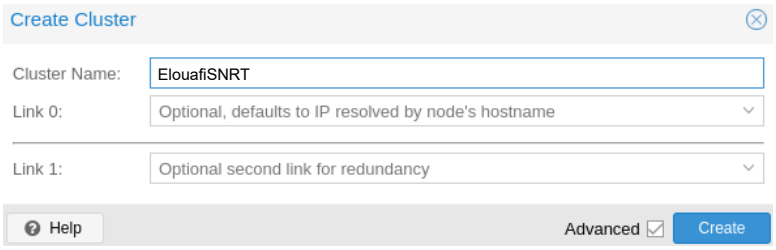

Invite de commandes - ssh rc
GNU nano 7.2 /etc/hostname
node02

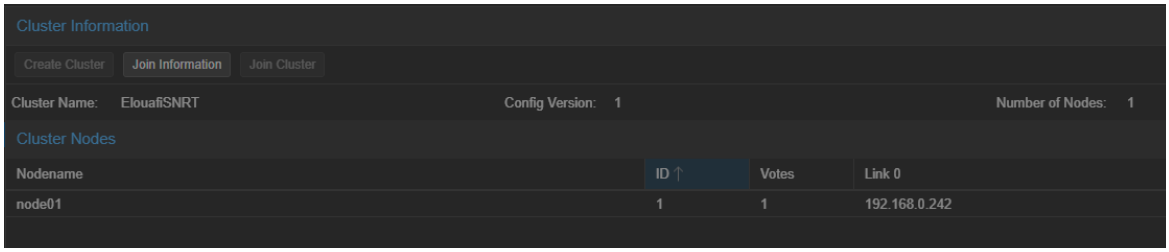

Invite de commandes - ssh rc
GNU nano 7.2 /etc/postfix/main.cf
# See /usr/share/postfix/main.cf.dist for a commented, more complete version
myhostname=node02.node2.local
smtpd_banner = $myhostname ESMTP $mail_name (Debian/GNU)
biff = no
# appending .domain is the MUA's job.
append_dot_mydomain = no
# Uncomment the next line to generate "delayed mail" warnings

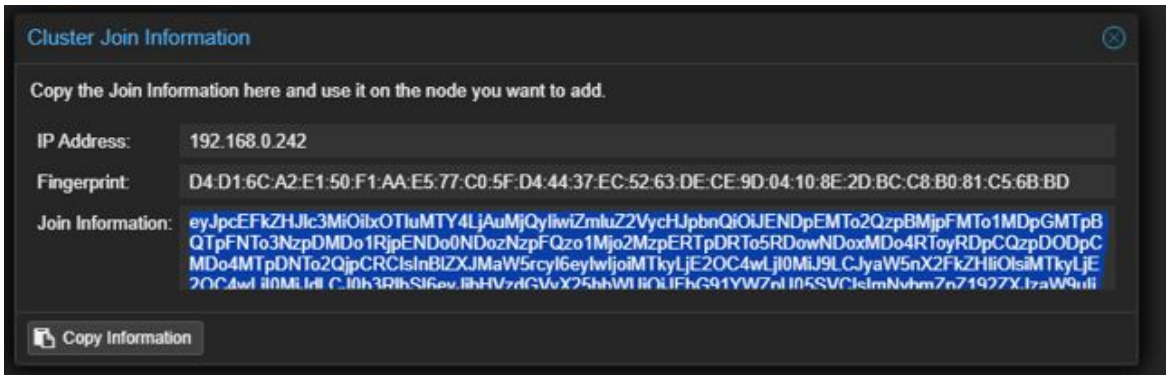
6.2.2.2 – Création du cluster :

Dans le 1er nœud (node01) :

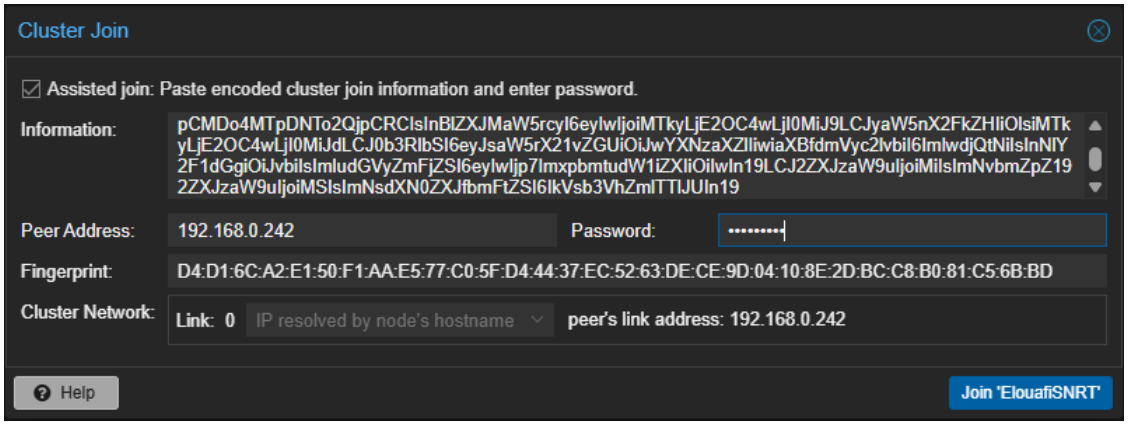


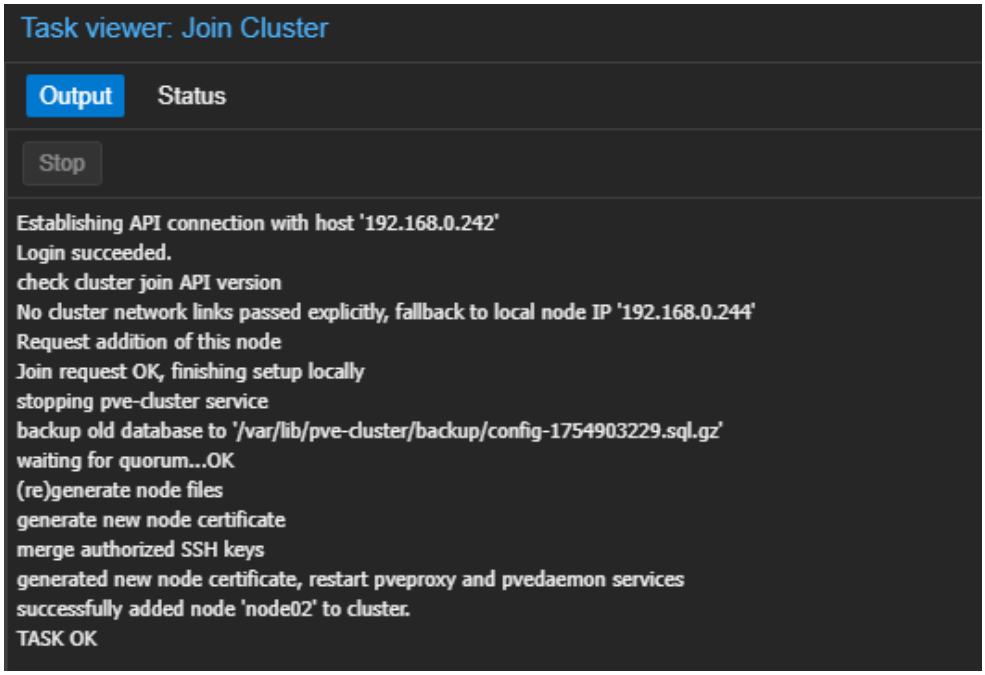


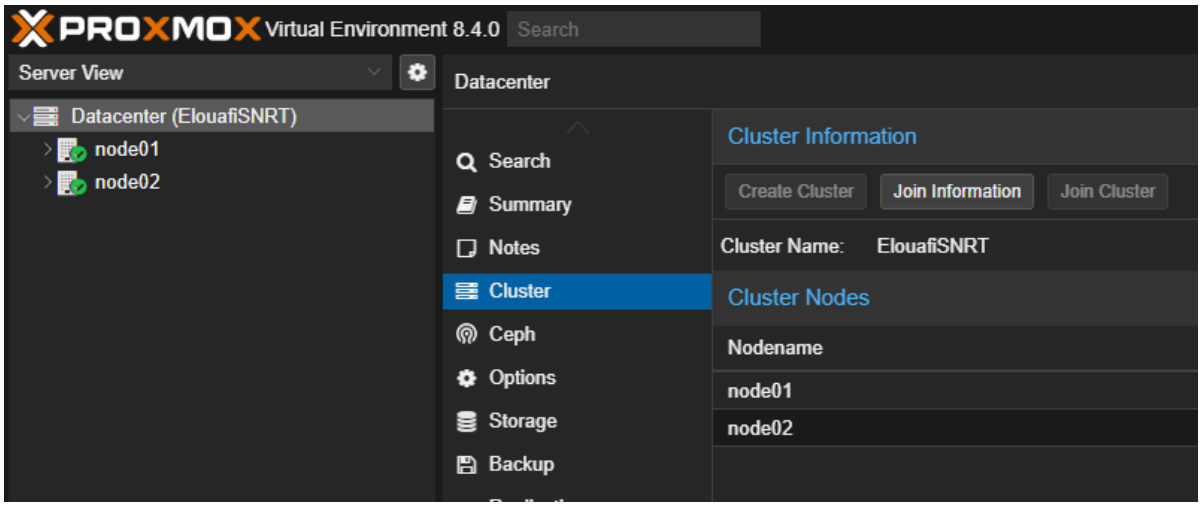




Dans le 2éme nœud (node02) :



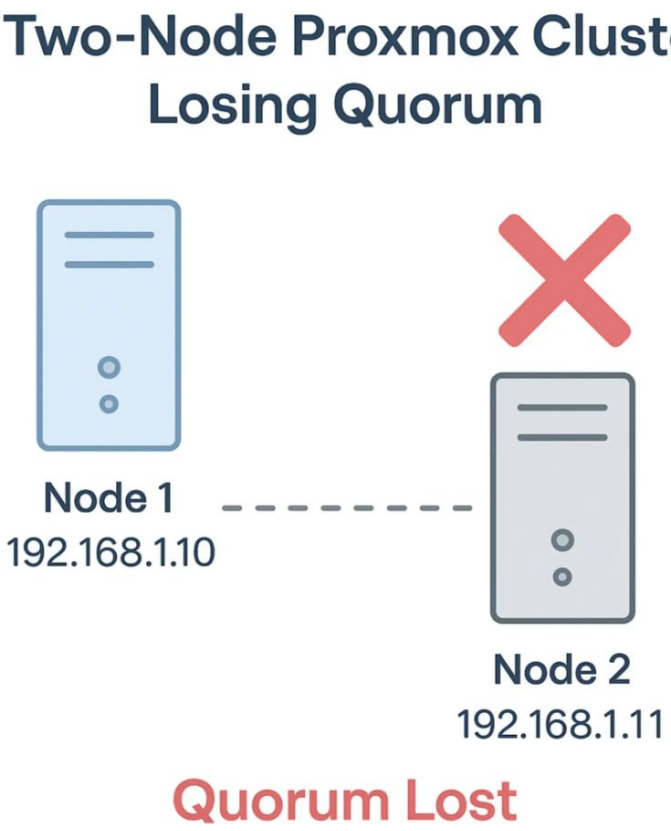




6.2.3 – Problématique de la haute disponibilité (HA) et du quorum :

Bien qu'un cluster Proxmox à deux nœuds soit entièrement pris en charge, il présente une limitation majeure : la perte de quorum. Si l'un des nœuds est hors ligne, le nœud restant perd sa majorité de vote, ce qui peut geler les charges de travail à haute disponibilité (HA) et bloquer les opérations du cluster jusqu'à la remise en ligne du nœud défaillant.

Pourquoi les clusters Proxmox VE à 2 nœuds peuvent être instables ?



Pour comprendre la limitation d'un cluster à deux nœuds, il est essentiel d'examiner le fonctionnement du quorum. Au sein de Proxmox VE, ce mécanisme est géré par Corosync, un service de communication qui utilise des canaux sécurisés pour maintenir le contact entre les nœuds. En plus d'assurer le suivi de l'état de chaque nœud, Corosync gère également un système de verrouillage distribué qui empêche plusieurs nœuds de modifier simultanément les fichiers de configuration, prévenant ainsi le risque de 'split-brain' et la corruption des données.

La règle de quorum exige une majorité des votes pour que le cluster reste opérationnel. Dans une configuration à deux nœuds, chaque serveur possède une voix. Par conséquent, si un nœud tombe en panne ou devient inaccessible, le nœud restant ne

dispose plus que de 50 % des voix, ce qui est insuffisant pour maintenir le quorum.

Dans une telle situation, le cluster perd le quorum, ce qui a plusieurs conséquences critiques pour le nœud survivant :

- **Gel des machines virtuelles (VMs)** gérées par la haute disponibilité (HA).
- **Blocage des modifications de configuration** dans l'interface graphique.
- **Interruption de toutes les opérations** au niveau du cluster jusqu'à ce que le quorum soit rétabli.

Quelles sont les solutions proposées pour permettre au nœud survivant de fonctionner ?

1ére solution : modification de la pondération des votes au sein du Corosync.

Afin de résoudre le problème de quorum dans notre cluster à deux nœuds, nous avons adopté une solution en modifiant la pondération des votes au sein de **Corosync**. Cette approche garantit que la haute disponibilité (HA) reste fonctionnelle en cas de défaillance d'un nœud.

La configuration des votes a été ajustée de la manière suivante :

- **Le nœud principal (le premier serveur) :** Se voit attribuer une seule voix.
- **Le nœud de secours (le deuxième serveur) :** Se voit attribuer **deux voix**.

La somme totale des votes du cluster est ainsi portée à trois. Si le nœud principal tombe en panne, le nœud de secours conserve ses deux voix, ce qui constitue une majorité de l'ensemble du cluster. Grâce à cette configuration, le cluster maintient son quorum même avec un seul nœud opérationnel.

Ainsi, en cas de défaillance imprévue du nœud principal, le gestionnaire HA du nœud de secours peut prendre des décisions, notamment en redémarrant automatiquement les machines virtuelles (VMs) qui étaient en cours d'exécution, assurant ainsi la continuité des services.

Configuration de la 1ére solution :

Avant:

```
root@node01:~# pvecm status
Cluster information
-------------------
Name:             ElouafiSNRT
Config Version:   2
Transport:        knet
Secure auth:      on

Quorum information
------------------
Date:             Mon Aug 11 10:15:26 2025
Quorum provider:  corosync_votequorum
Nodes:            2
Node ID:          0x00000001
Ring ID:          1.9
Quorate:          Yes

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

Membership information
----------------------
    Nodeid      Votes Name
0x00000001          1 192.168.0.242 (local)
0x00000002          1 192.168.0.244
root@node01:~#
```

Modifier le fichier /etc/pve/corosync.conf :

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Aug 15 11:38:56 +01 2025 from 192.168.0.244 on pts/0
root@node01:~# ls /etc/pve
authkey.pub      corosync.conf  firewall  local  mapping  openvz  pve-root-ca.p
authkey.pub.old  datacenter.cfg ha        lxc    nodes    priv    pve-www.key
root@node01:~# cd /etc/pve
root@node01:/etc/pve# cp corosync.conf corosync.new.conf
root@node01:/etc/pve# nano corosync.new.conf
root@node01:/etc/pve#
```

```
  GNU nano 7.2
logging {
  debug: off
  to_syslog: yes
}

nodelist {
  node {
    name: node01
    nodeid: 1
    quorum_votes: 1
    ring0_addr: 192.168.0.242
  }
  node {
    name: node02
    nodeid: 2
    quorum_votes: 1
    ring0_addr: 192.168.0.244
  }
}

quorum {
  provider: corosync_votequorum
}

totem {
  cluster_name: ElouafiSNRT
  config_version: 2
  interface {
    linknumber: 0
  }
  ip_version: ipv4-6
  link_mode: passive
  secauth: on
  version: 2
}
```

```
  GNU nano 7.2
logging {
  debug: off
  to_syslog: yes
}

nodelist {
  node {
    name: node01
    nodeid: 1
    quorum_votes: 2
    ring0_addr: 192.168.0.242
  }
  node {
    name: node02
    nodeid: 2
    quorum_votes: 1
    ring0_addr: 192.168.0.244
  }
}

quorum {
  provider: corosync_votequorum
}

totem {
  cluster_name: ElouafiSNRT
  config_version: 3
  interface {
    linknumber: 0
  }
  ip_version: ipv4-6
  link_mode: passive
  secauth: on
  version: 2
}
```

Cluster Nodes

Nodename	ID	Votes	Link 0
node01	1	2	192.168.0.242
node02	2	1	192.168.0.244

2éme solution : L’ajout d’un QDevice.

Un QDevice (Quorum Device) est un composant léger qui ajoute un troisième vote à votre cluster Proxmox, sans nécessiter un troisième nœud complet exécutant Proxmox VE.

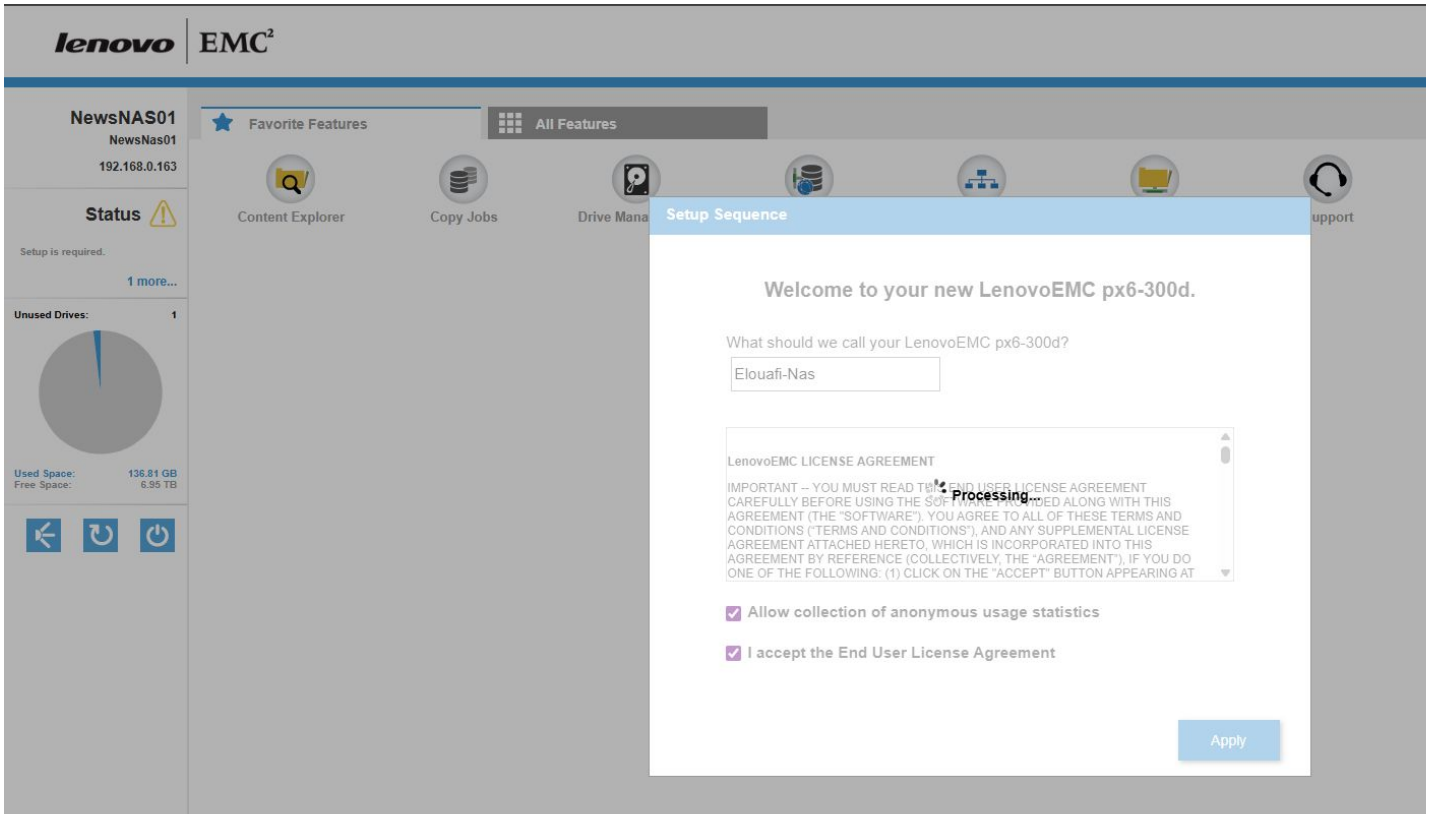
Il n'héberge pas de machines virtuelles, ne gère pas le stockage et n'exécute aucun service de cluster, hormis sa participation aux décisions de quorum. Son seul rôle est de servir de point de départage neutre lorsqu'un nœud devient inaccessible.

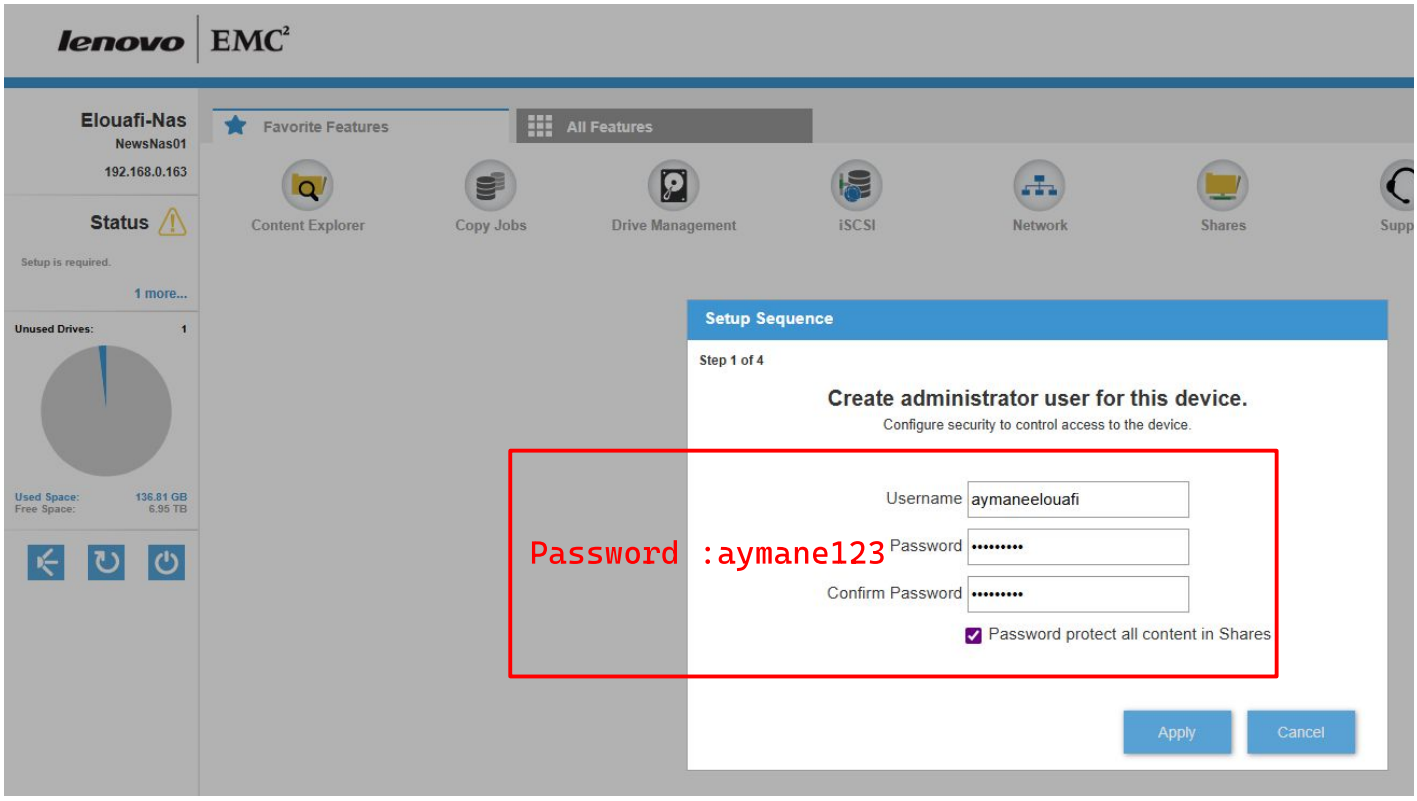
L'ajout d'un QDevice permet à votre cluster à deux nœuds de maintenir la stabilité en garantissant que le quorum reste atteint même en cas de déconnexion d'un nœud. Ceci est particulièrement important si vous utilisez la haute disponibilité (HA), car cela empêche les services et les machines virtuelles de se bloquer ou de devenir inaccessibles en raison d'une perte de quorum.

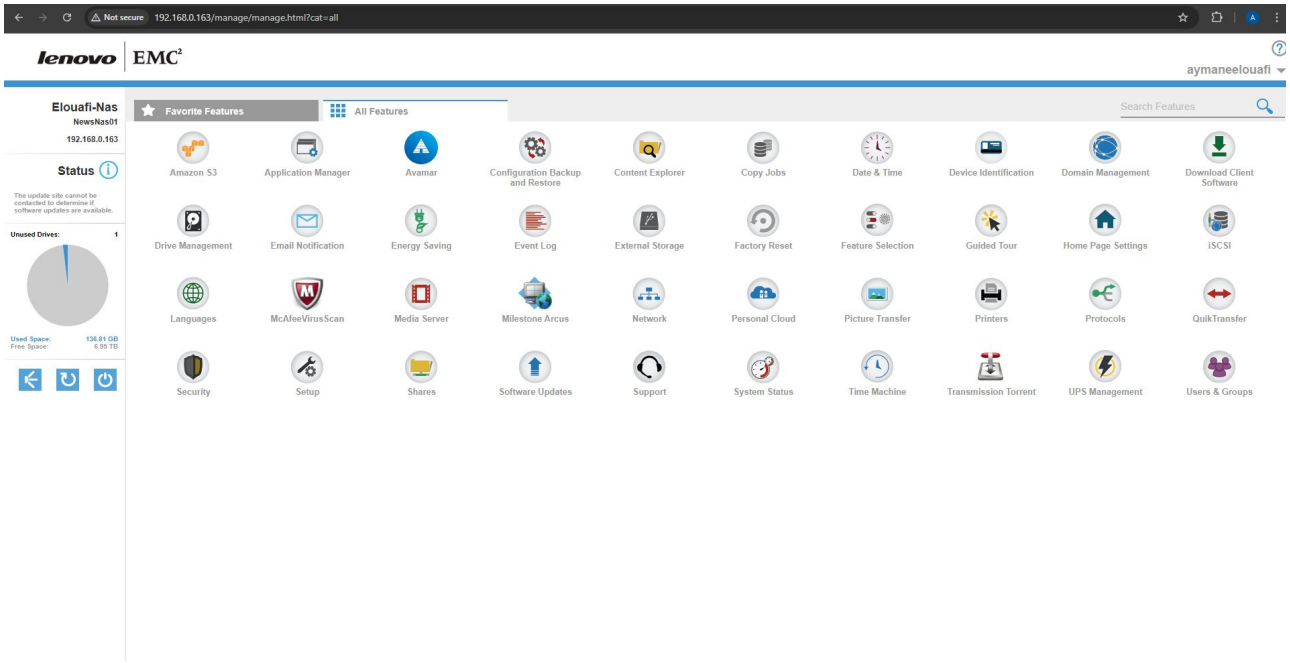
Vous pouvez héberger le QDevice sur presque n'importe quel système toujours actif, tel qu'une machine virtuelle, un NAS, un Raspberry Pi ou même un conteneur LXC basse consommation, à condition qu'il soit physiquement séparé de vos deux nœuds Proxmox et qu'il dispose d'une adresse IP statique accessible.

6.3 - Intégration du Stockage NAS via NFS :

6.3.1 - Configuration du NAS :



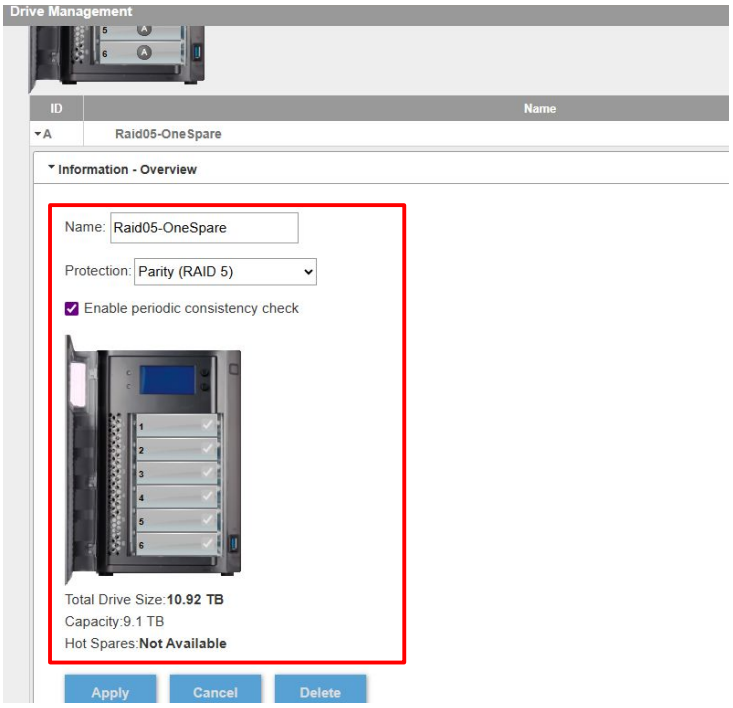


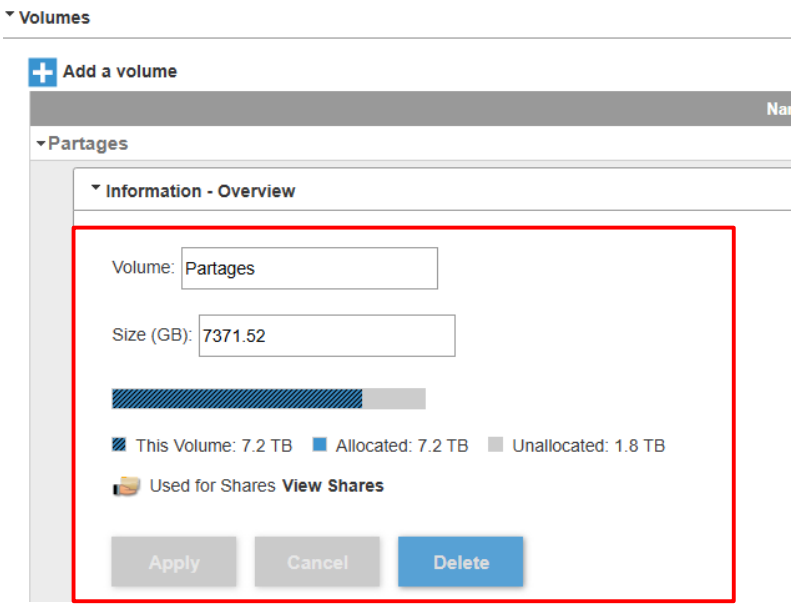


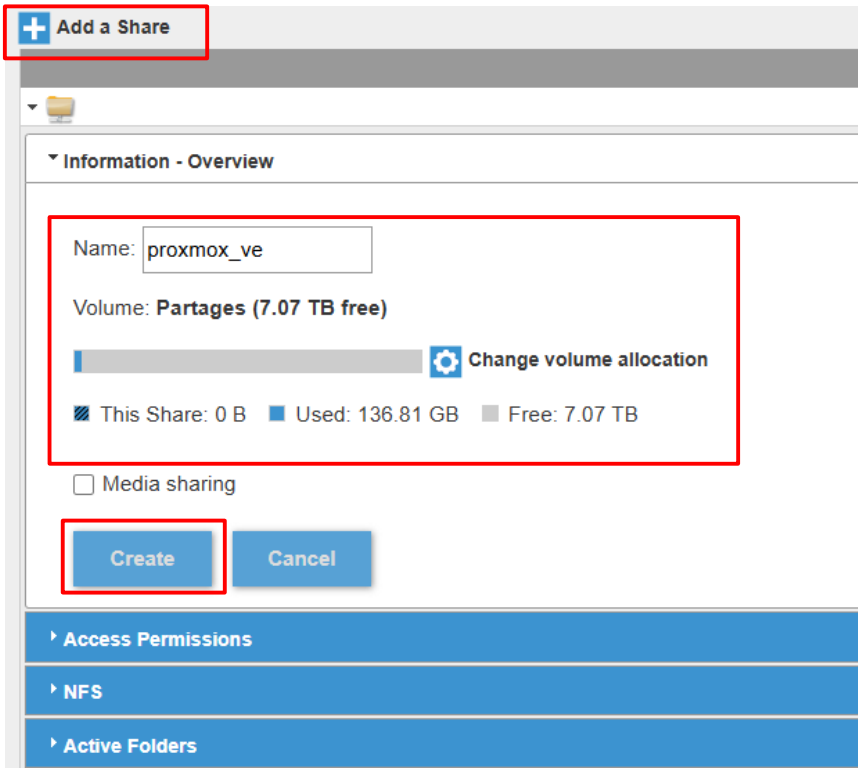
_ NAS Storage Web Interface _

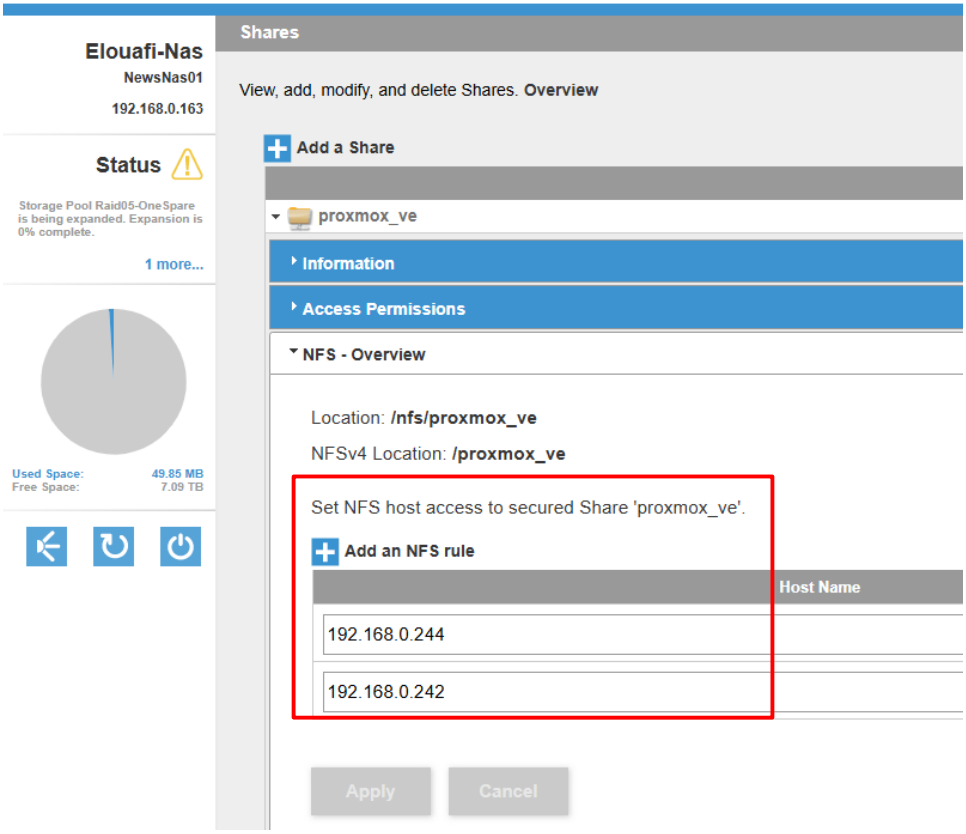
Un tableau **RAID 5**, nommé **"Raid05-OneSpare"**, a été créé à partir des disques physiques de l'unité de stockage, offrant une capacité de 9.1 TB pour la protection des données.

Sur ce tableau RAID 5, un volume logique a été défini pour servir d'espace de stockage principal pour le cluster Proxmox. Ce volume, nommé **"Partages"**, a été alloué pour une taille de 7.2 TB et constitue le pool de stockage central.

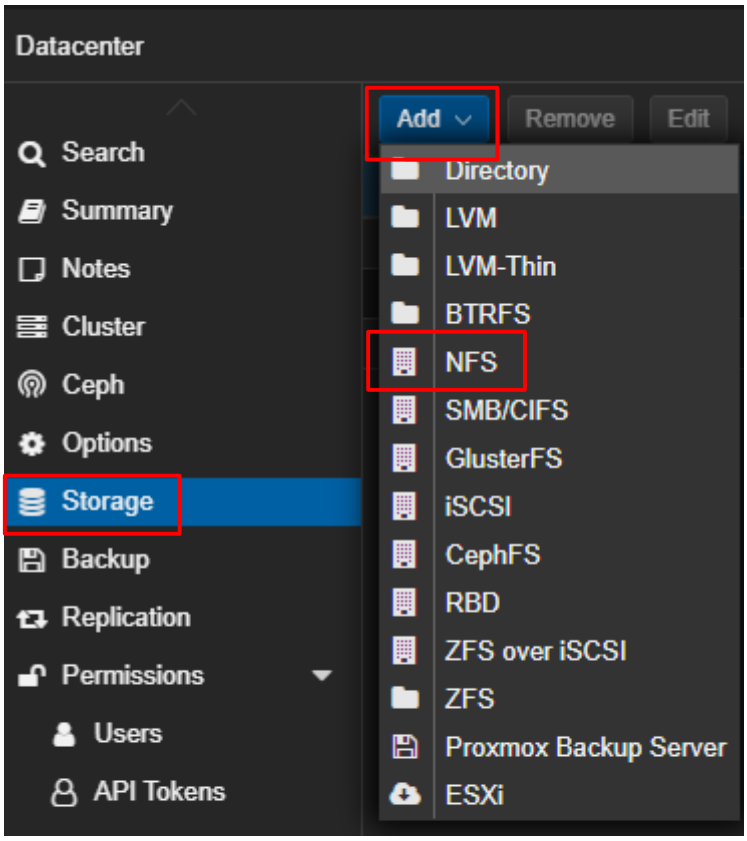


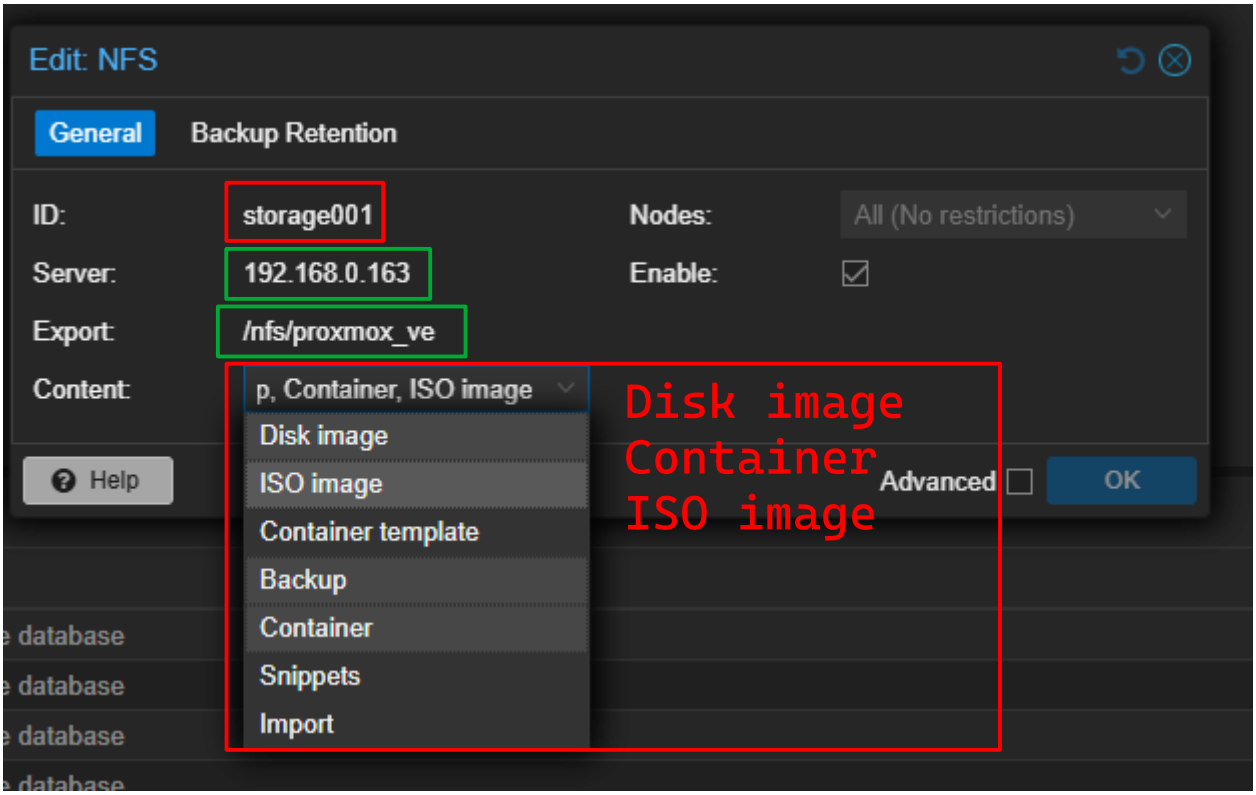


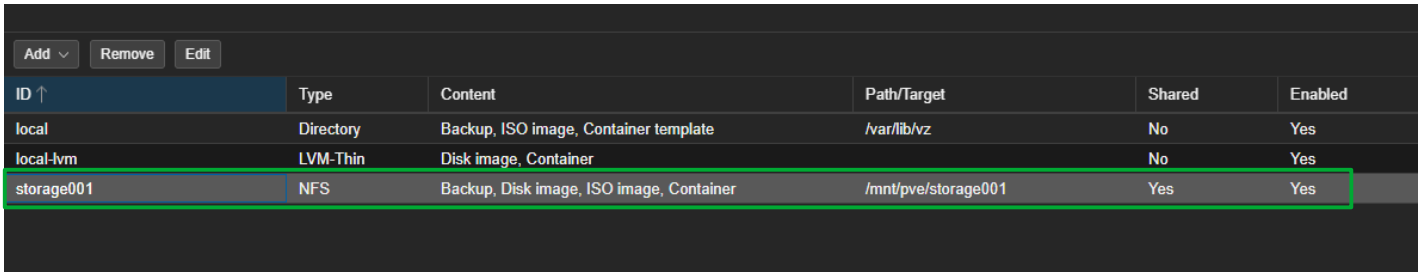

Add a Share
Information - Overview
Name: proxmox_ve
Volume: Partages (7.07 TB free)
Change volume allocation
This Share: 0 B
Used: 136.81 GB
Free: 7.07 TB
Media sharing
Create
Cancel
Access Permissions
NFS
Active Folders

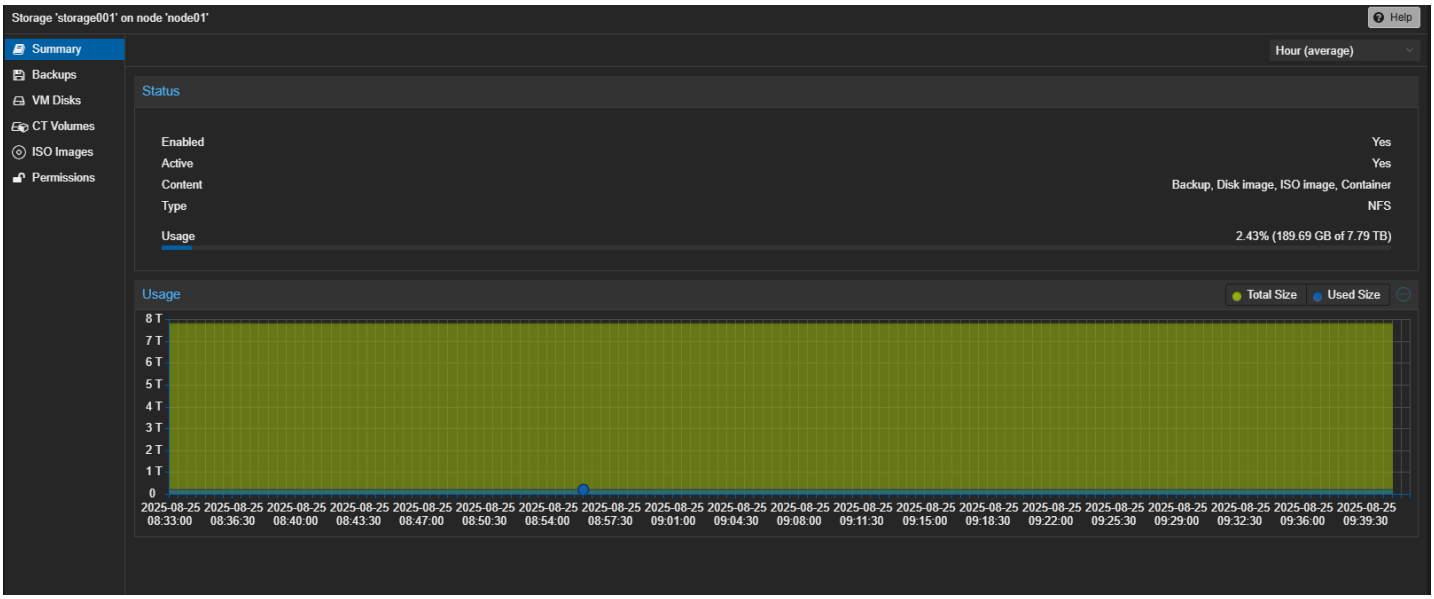

Elouafi-Nas
NewsNas01
192.168.0.163
Status
Storage Pool Raid05-OneSpare is being expanded. Expansion is 0% complete.
1 more...
Used Space: 49.85 MB
Free Space: 7.09 TB
Shares
View, add, modify, and delete Shares. Overview
Add a Share
proxmox_ve
Information
Access Permissions
NFS - Overview
Location: /nfs/proxmox_ve
NFSv4 Location: /proxmox_ve
Set NFS host access to secured Share 'proxmox_ve'.
Add an NFS rule
Host Name
192.168.0.244
192.168.0.242
Apply
Cancel

6.3.2 – Ajout du stockage dans Proxmox VE :



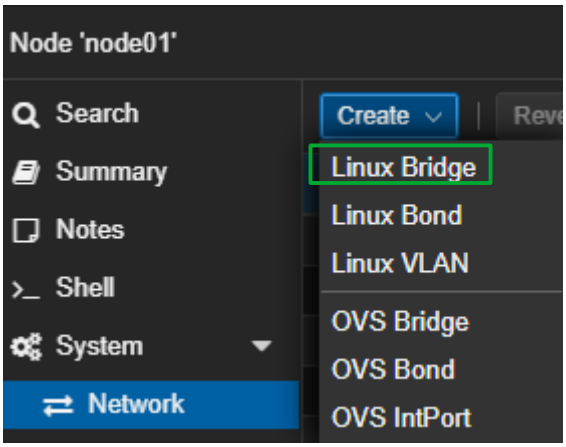




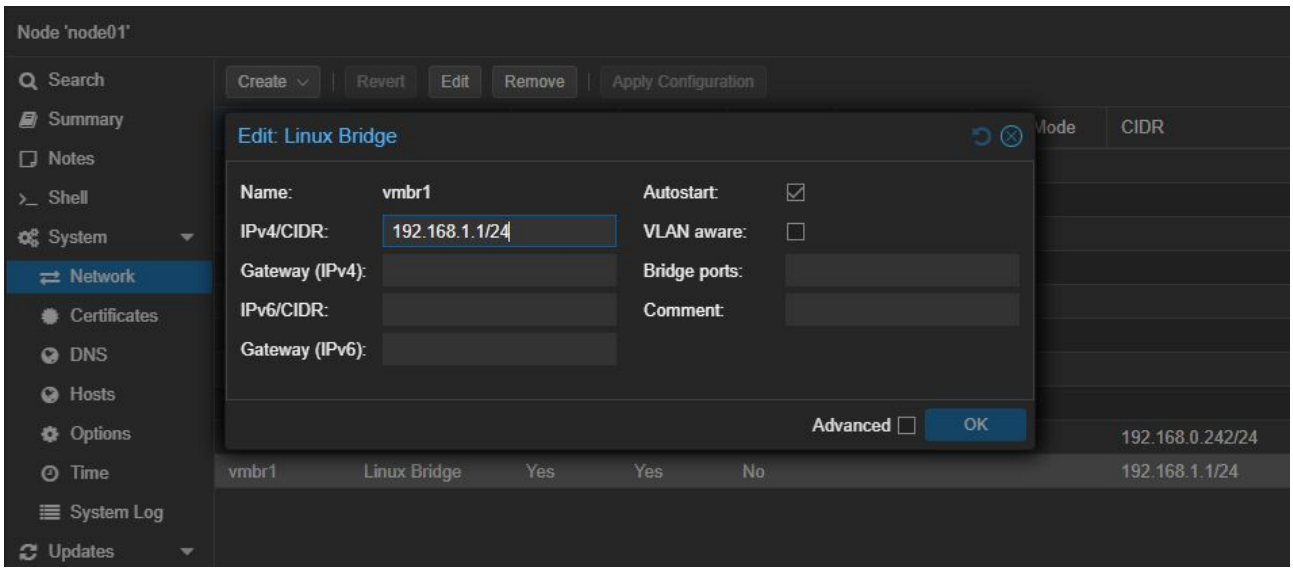


6.4 – Configuration des Services Réseau et du Pare-feu :

6.4.1 – Création du réseau privé (NAT) :



Ajouter une interface réseaux (Linux Bridge) **‘vmbr1’** :



* On va crée un réseau NAT : **192.168.1.0\24**

```
  GNU nano 7.2                                                /etc/network/i
iface eno2 inet manual

iface eno3 inet manual

iface eno4 inet manual

iface ens1f0 inet manual

iface ens1f1 inet manual

iface ens1f2 inet manual

iface ens1f3 inet manual

auto vmbr0
iface vmbr0 inet static
        address 192.168.0.242/24
        gateway 192.168.0.1
        bridge-ports eno1
        bridge-stp off
        bridge-fd 0

auto vmbr1
iface vmbr1 inet static
        address 192.168.1.1
        netmask 255.255.255.0
        bridge-ports none
        bridge-stp off
        bridge-fd 0

# NAT settings for vmbr1 interface
post-up echo 1 > /proc/sys/net/ipv4/ip_forward
post-up iptables -t nat -A POSTROUTING -s '192.168.1.0/24' -o vmbr0 -j MASQUERADE
post-down iptables -t nat -D POSTROUTING -s '192.168.1.0/24' -o vmbr0 -j MASQUERADE

source /etc/network/interfaces.d/*
```

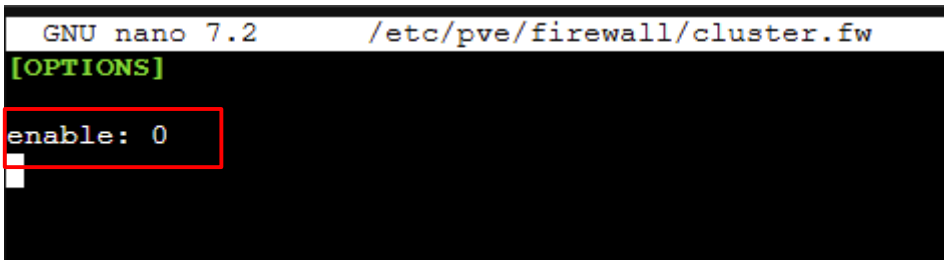
6.4.2 – Configuration du pare-feu Proxmox VE :

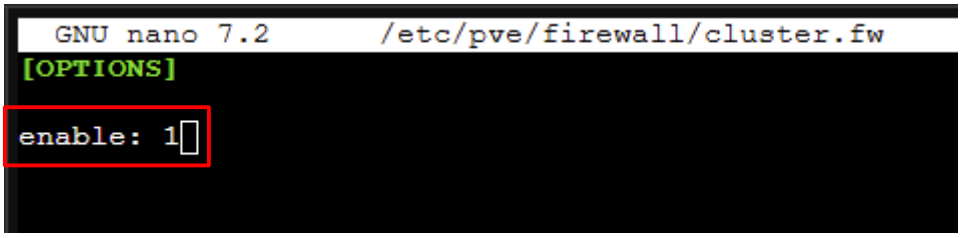
Le pare-feu Proxmox VE offre un moyen simple de protéger votre infrastructure informatique. Vous pouvez configurer des règles de pare-feu pour tous les hôtes d'un cluster, ou définir des règles pour les machines virtuelles et les conteneurs. Des fonctionnalités telles que les macros de pare-feu, les groupes de sécurité, les ensembles d'adresses IP et les alias simplifient cette tâche.

Bien que toute la configuration soit stockée sur le système de fichiers du cluster, le service de pare-feu basé sur iptables s'exécute sur chaque nœud du cluster, assurant ainsi une isolation complète entre les machines virtuelles. La nature distribuée de ce système offre également une bande passante bien supérieure à celle d'une solution de pare-feu centralisée.

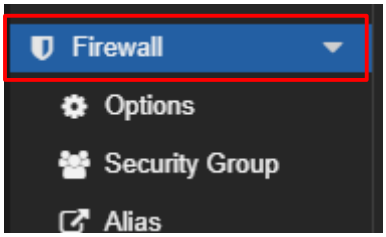
Le pare-feu prend entièrement en charge IPv4 et IPv6. La prise en charge d'IPv6 est totalement transparente et nous filtrons le trafic pour les deux protocoles par défaut. Il n'est donc pas nécessaire de maintenir un ensemble de règles différent pour IPv6.

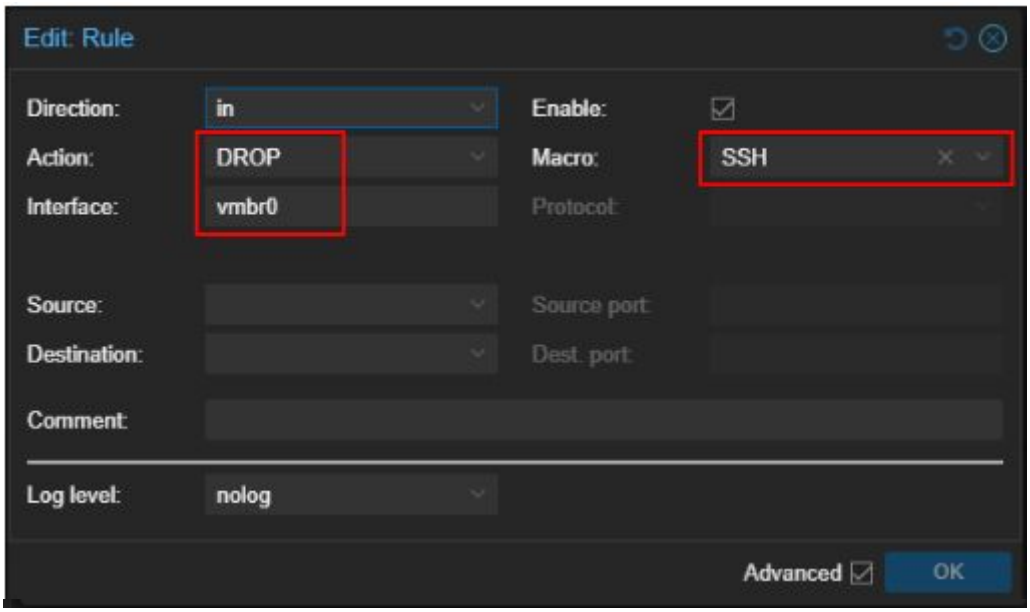
Pour activer le pare-feu (Firewall) , on utilise le fichier de configuration `/etc/pve/firewall/cluster.fw` :





Pour ajouter des règles (Add Rules) au niveau du Datacenter :





Désactiver la connection SSH au serveur



Si vous activez le pare-feu, le trafic vers tous les hôtes est bloqué par défaut. Les seules exceptions sont WebGUI (8006) et SSH (22) depuis votre réseau local.

6.5 – Gestion des Utilisateurs et des Permissions :

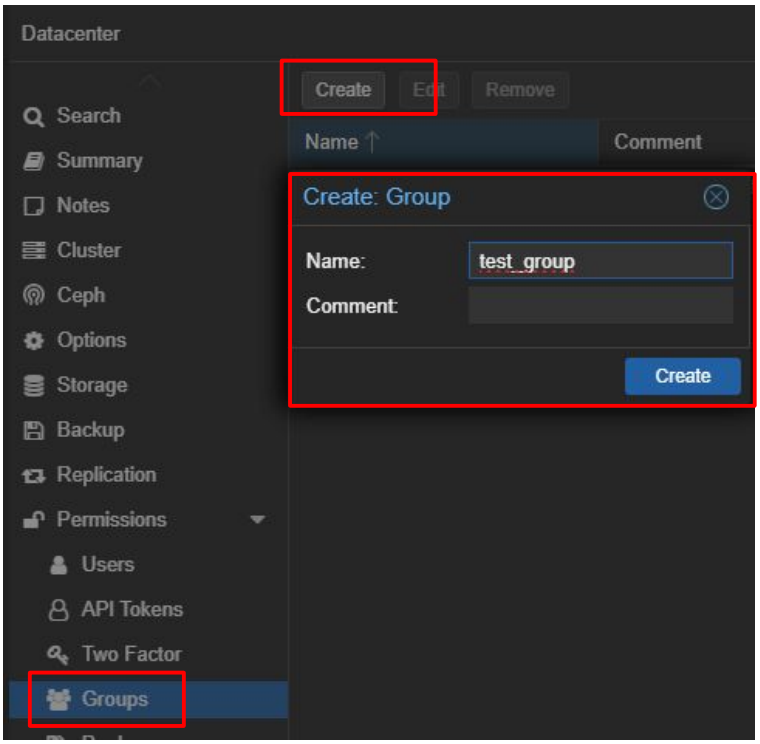
Proxmox VE prend en charge plusieurs sources d'authentification, par exemple Linux PAM, un serveur d'authentification Proxmox VE intégré, LDAP, Microsoft Active Directory et OpenID Connect.

Grâce à la gestion des utilisateurs et des autorisations basée sur les rôles pour tous les objets (VM, stockage, nœuds, etc.), un accès précis peut être défini.

Création de groupe , comptes utilisateurs et Attribution des rôles :

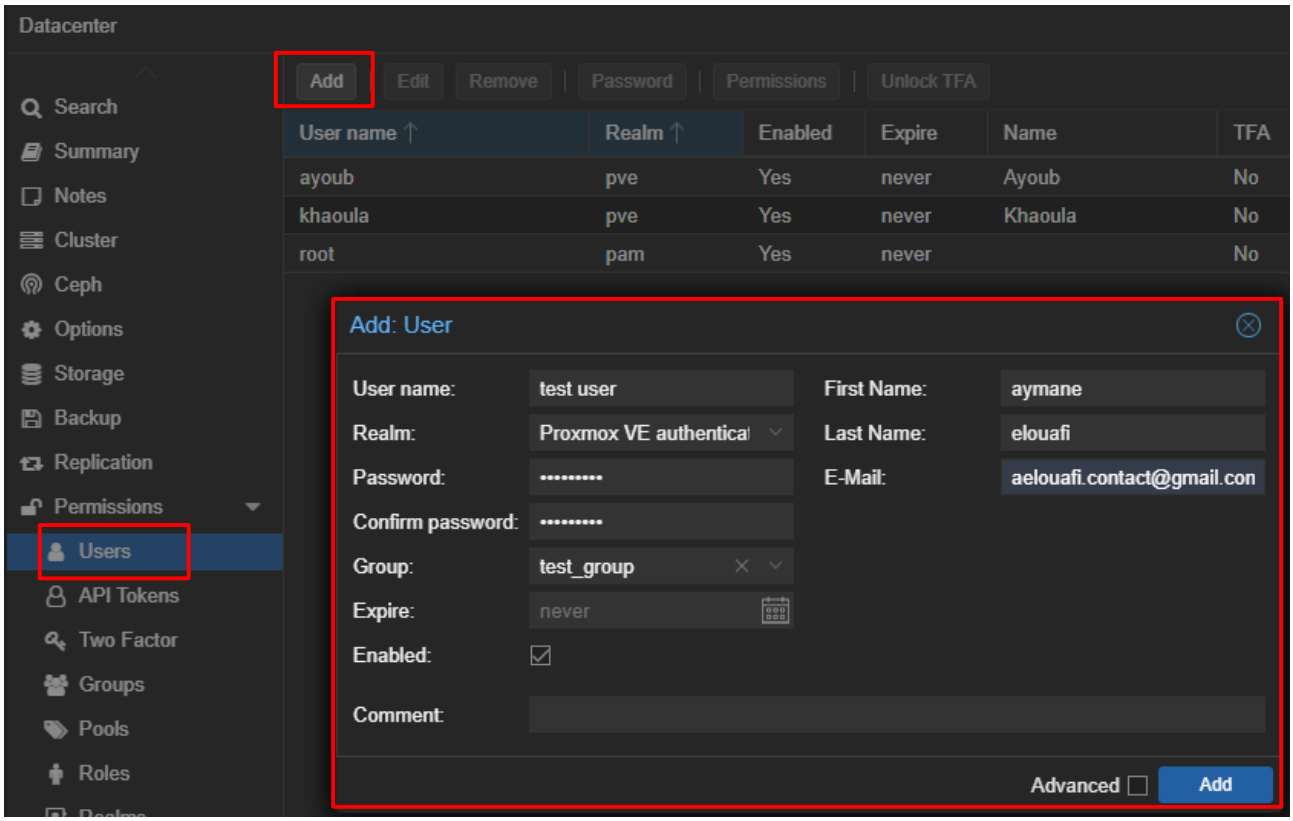
Chaque utilisateur peut appartenir à plusieurs groupes. Les groupes constituent la méthode privilégiée pour organiser les autorisations d'accès. Accordez toujours les autorisations à des groupes plutôt qu'à des utilisateurs individuels. Vous obtiendrez ainsi une liste de contrôle d'accès beaucoup plus facile à gérer.

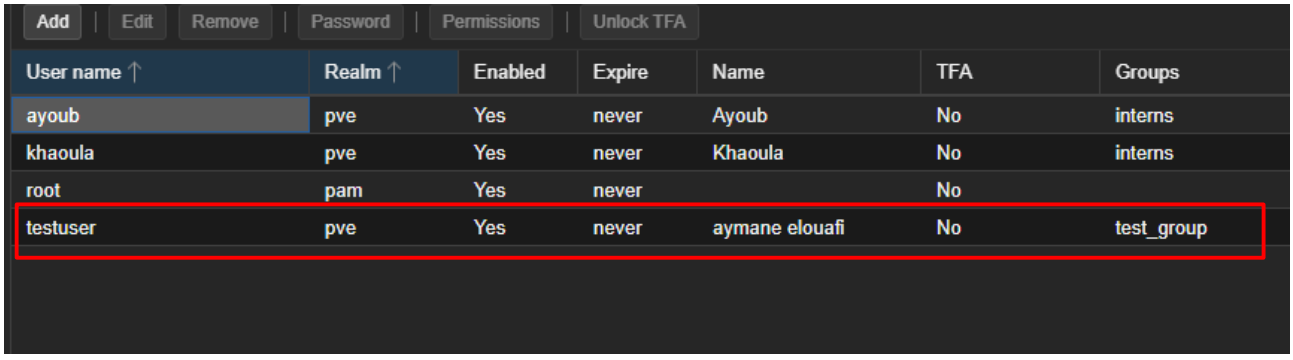
Création d’un Groupe :

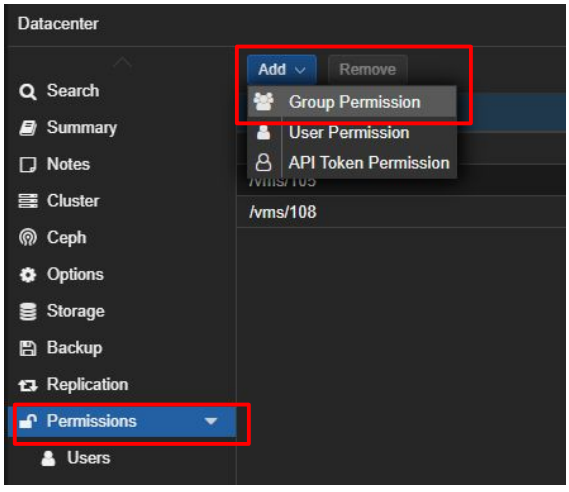


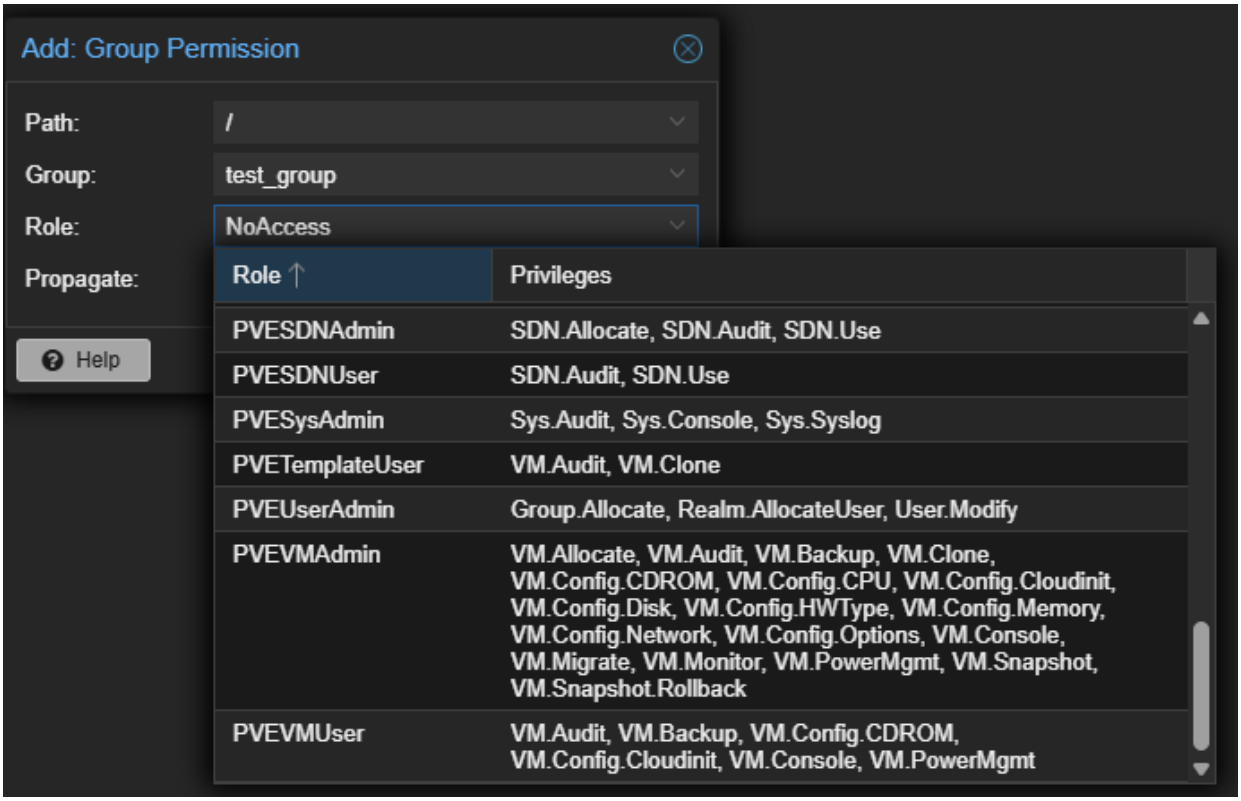


Création d'un compte et Attribution des rôles :



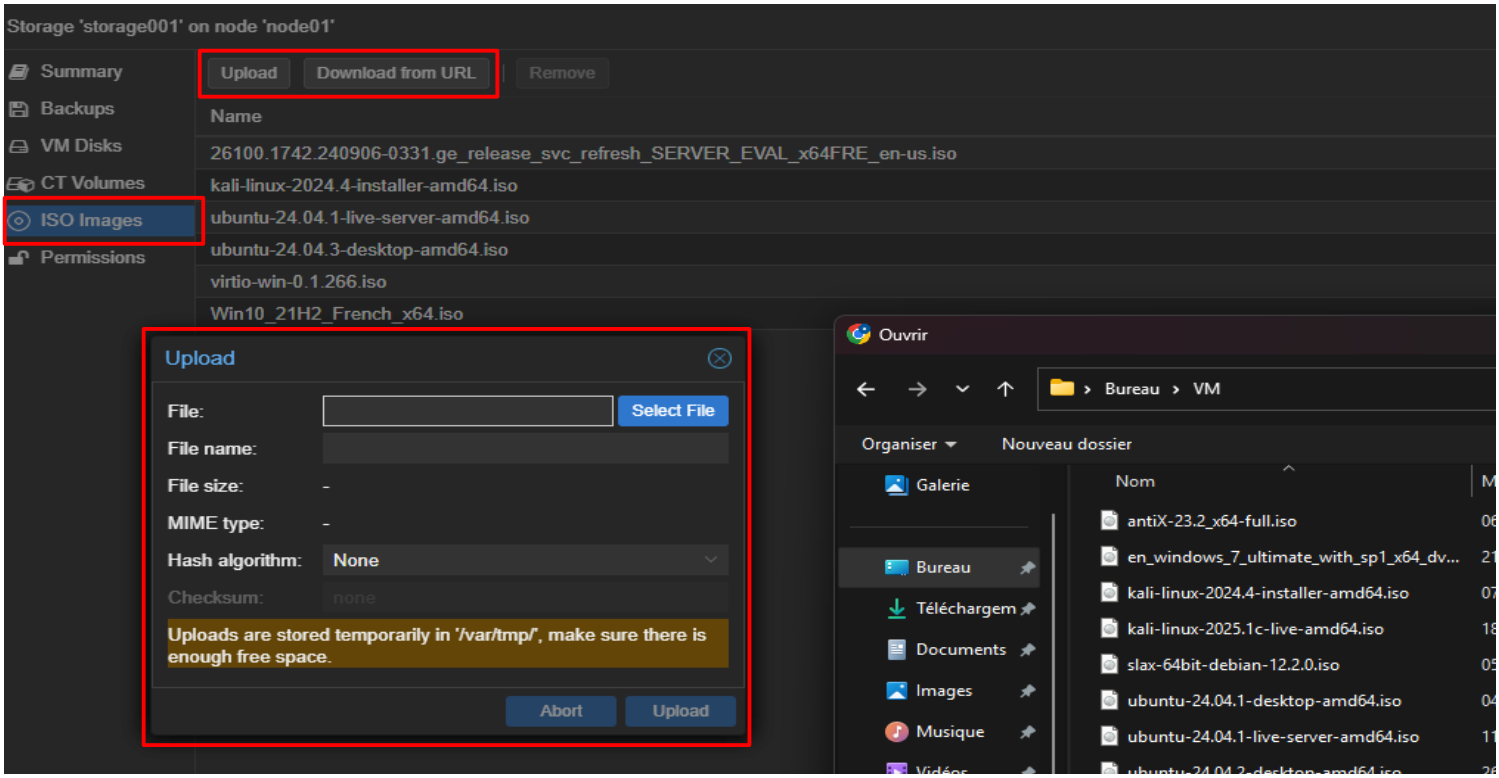






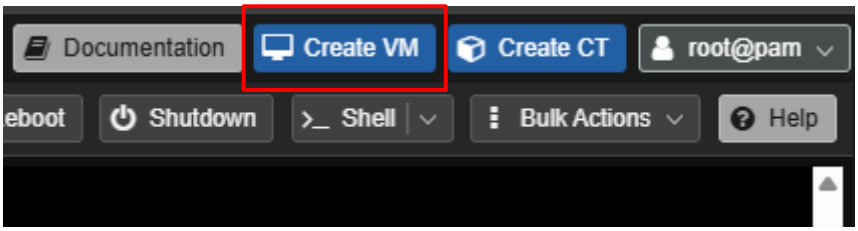
6.6 – Gestion des ISO et des modèles de VM :

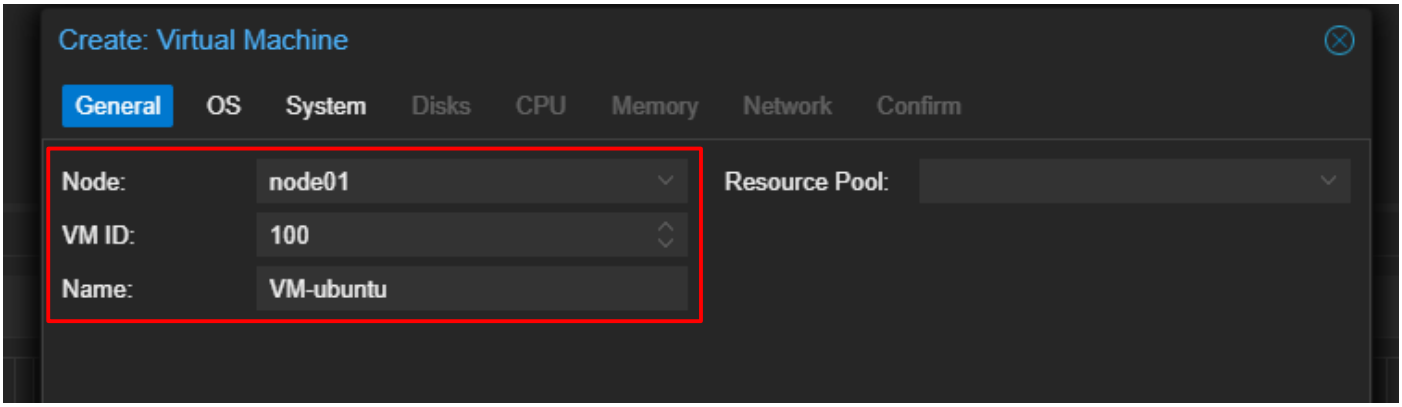
Comment les images ISO des systèmes d'exploitation ont été téléchargées et stockées sur le NAS pour faciliter la création des VM ?

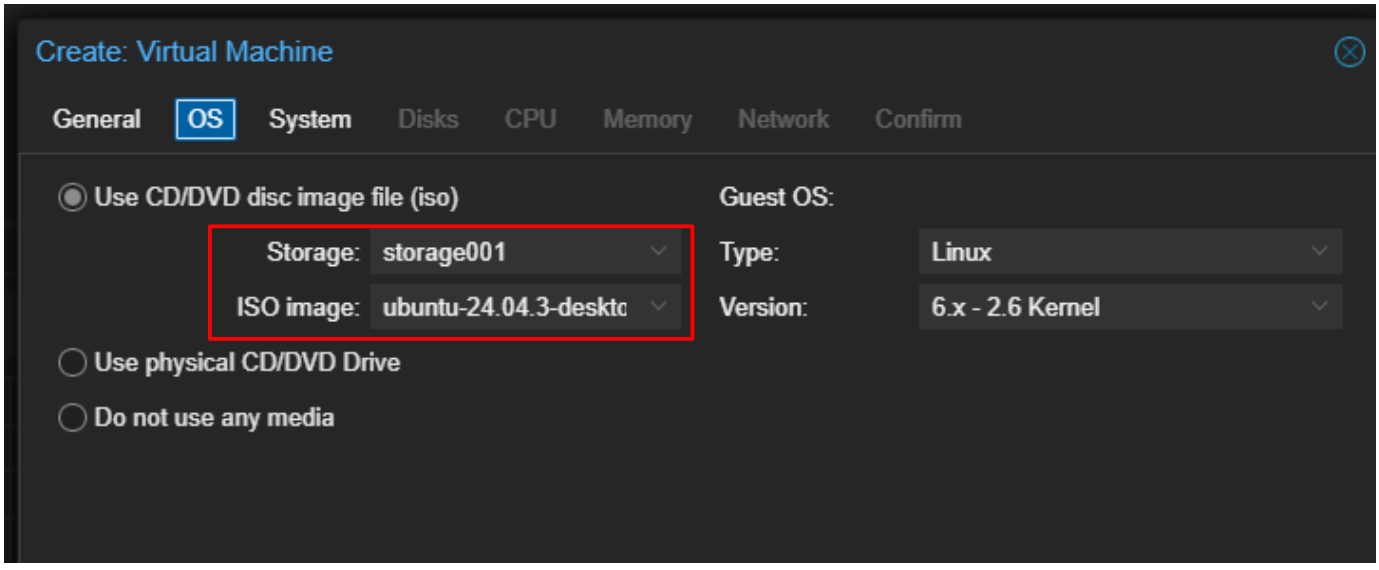


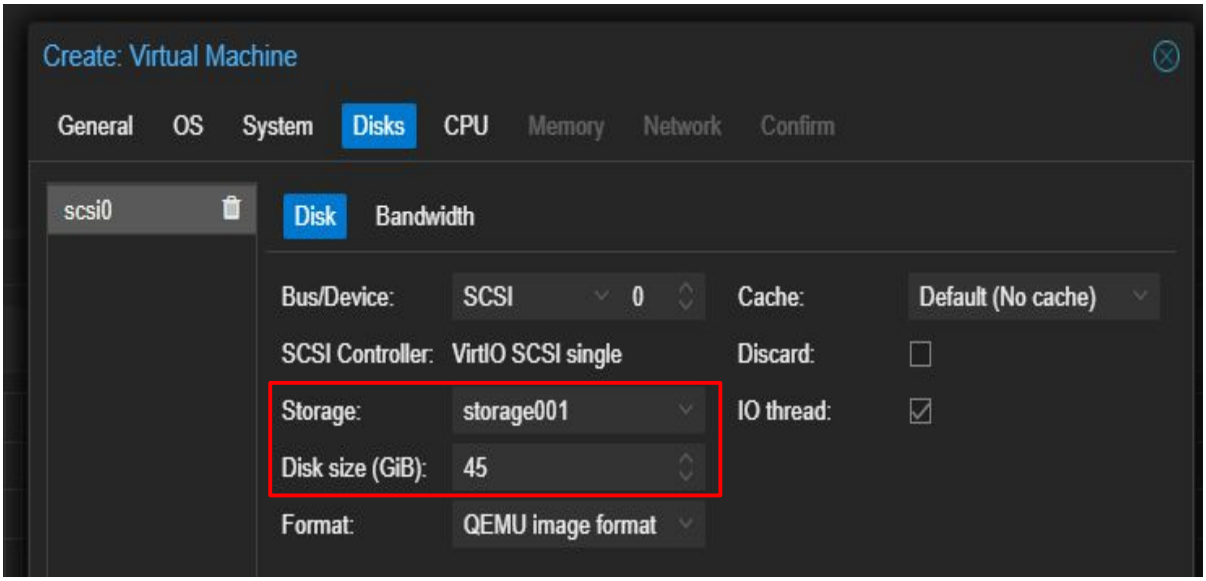
7. Tests et Validation :

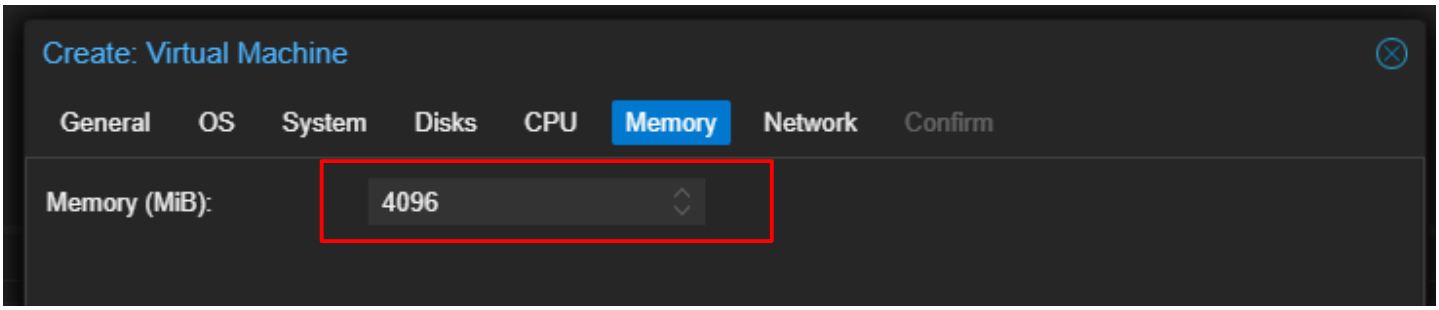
7.1 – Création et Configuration d'une Machine Virtuelle (VM) :

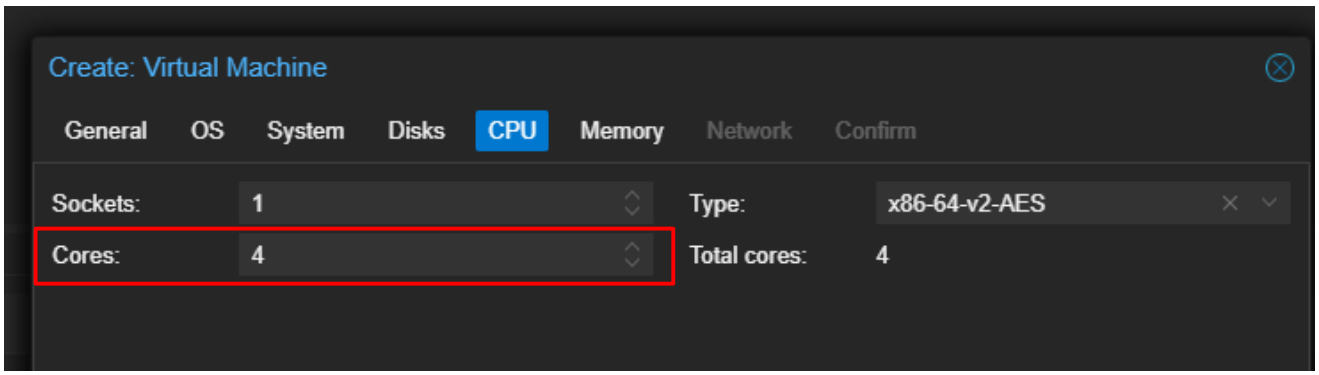


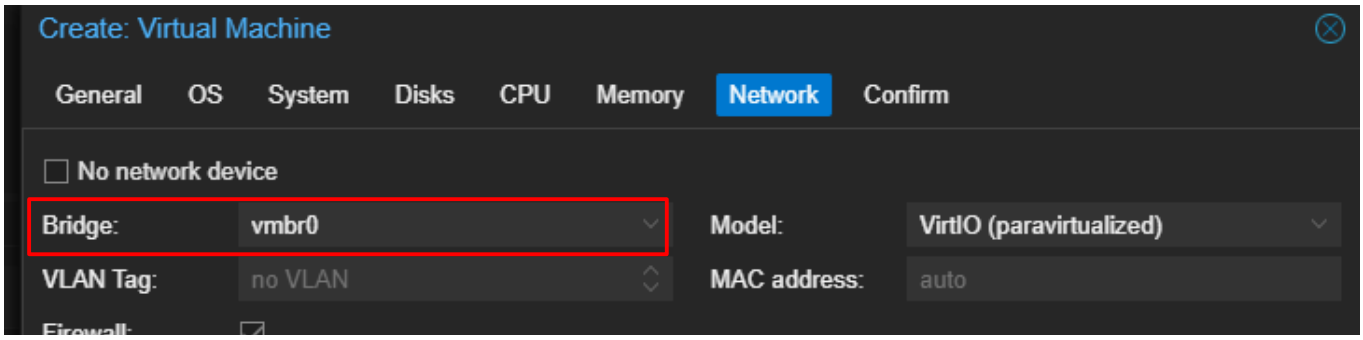


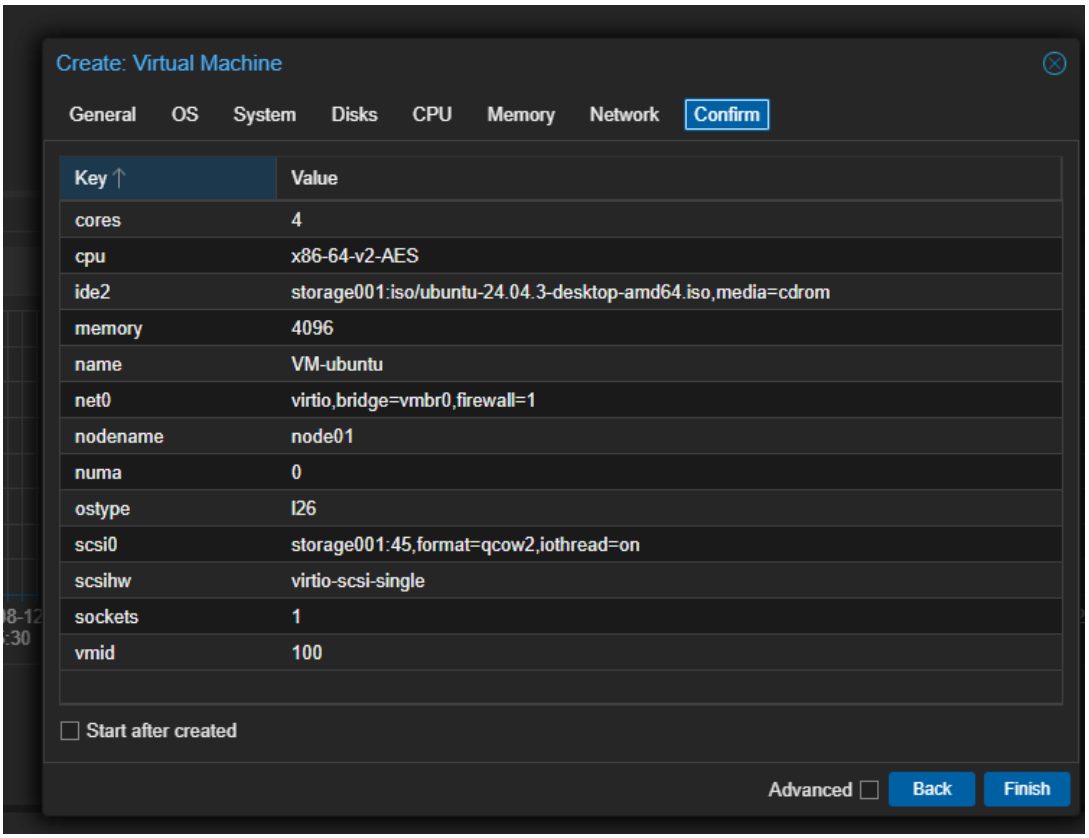


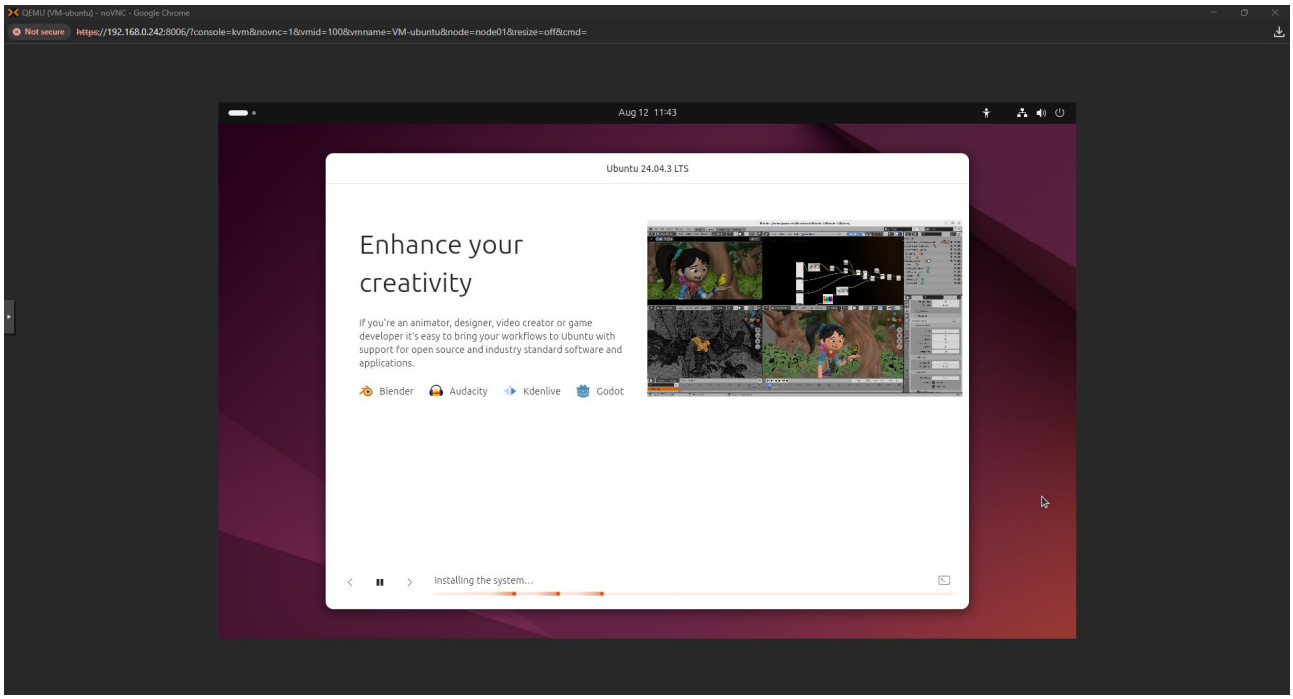

Create: Virtual Machine
General
OS
System
Disks
CPU
Memory
Network
Confirm
scsi0
Disk
Bandwidth
Bus/Device:
SCSI
0
Cache:
Default (No cache)
SCSI Controller:
VirtIO SCSI single
Discard:
Storage:
storage001
IO thread:
Disk size (GiB):
45
Format:
QEMU image format

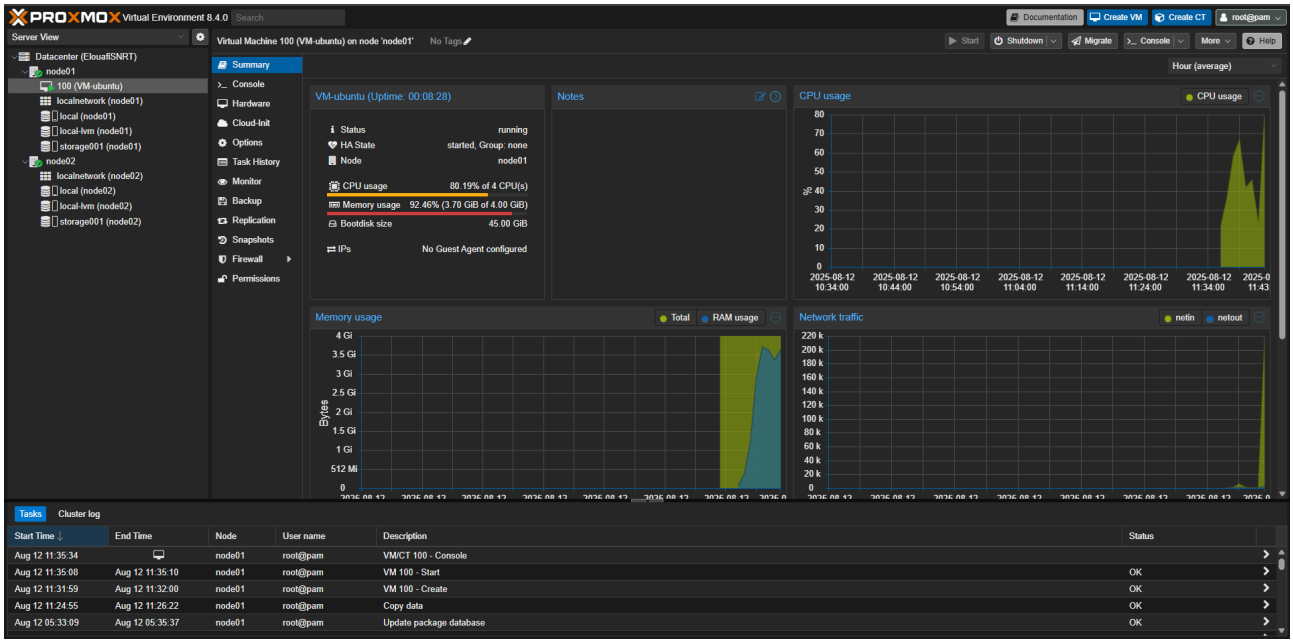

Create: Virtual Machine
General
OS
System
Disks
CPU
Memory
Network
Confirm
Memory (MiB):
4096


Create: Virtual Machine
General
OS
System
Disks
CPU
Memory
Network
Confirm
Sockets:
1
Type:
x86-64-v2-AES
Cores:
4
Total cores:
4


Create: Virtual Machine
General
OS
System
Disks
CPU
Memory
Network
Confirm
No network device
Bridge:
vmbr0
Model:
VirtIO (paravirtualized)
VLAN Tag:
no VLAN
MAC address:
auto

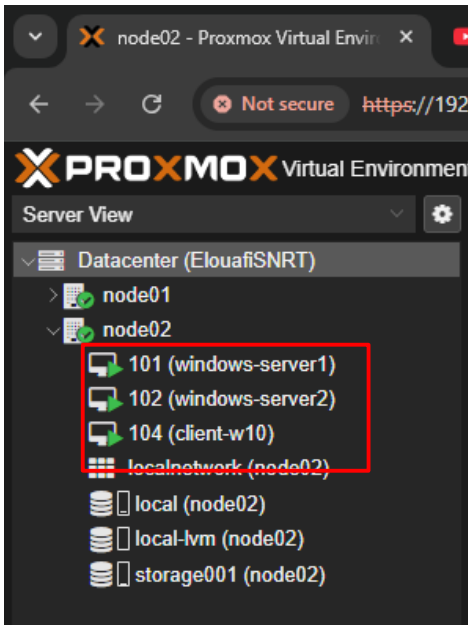

Create: Virtual Machine
General
OS
System
Disks
CPU
Memory
Network
Confirm
Key
Value
cores 4
cpu x86-64-v2-AES
ide2 storage001:iso/ubuntu-24.04.3-desktop-amd64.iso,media=cdrom
memory 4096
name VM-ubuntu
net0 virtio,bridge=vmbr0,firewall=1
nodename node01
numa 0
ostype l26
scsi0 storage001:45,format=qcow2,iothread=on
scsihw virtio-scsi-single
sockets 1
vmid 100
Start after created
Advanced
Back
Finish


Aug 12 11:43
Ubuntu 24.04.3 LTS
Enhance your creativity
If you're an animator, designer, video creator or game developer it's easy to bring your workflows to Ubuntu with support for open source and industry standard software and applications.
Blender
Audacity
Kdenlive
Godot
Installing the system...



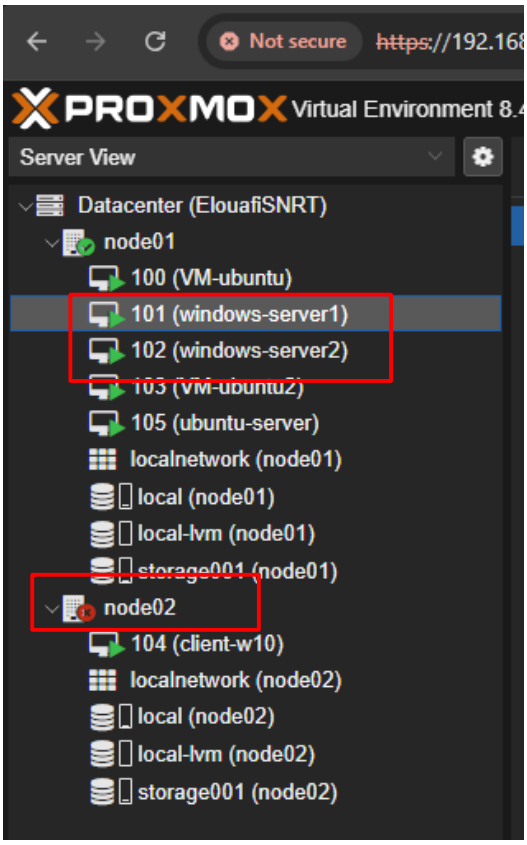
7.2 – Test de la Haute Disponibilité (HA) :

Avant d'arrêter le 2éme nœud :

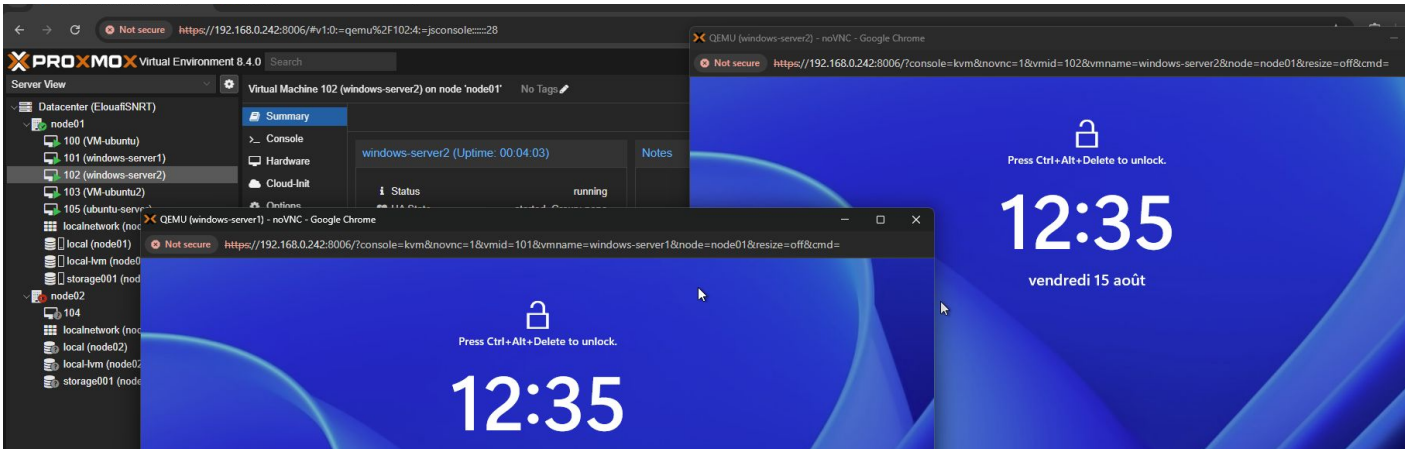


* On Activer le HA pour les deux Windows Server mais pas pour le client-w10

Après l'arrêt du 2éme nœud :

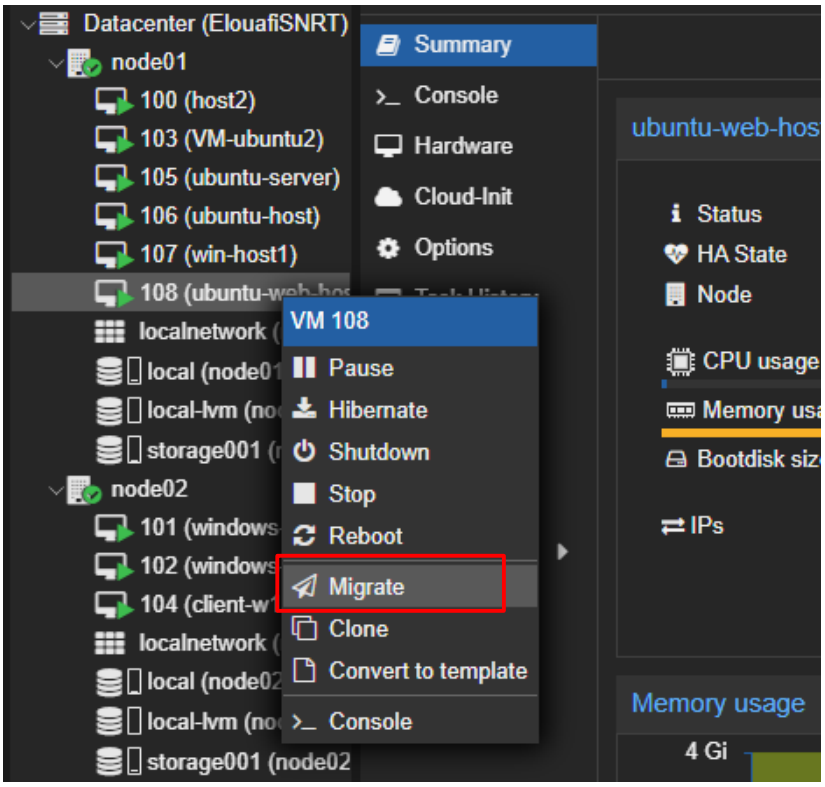


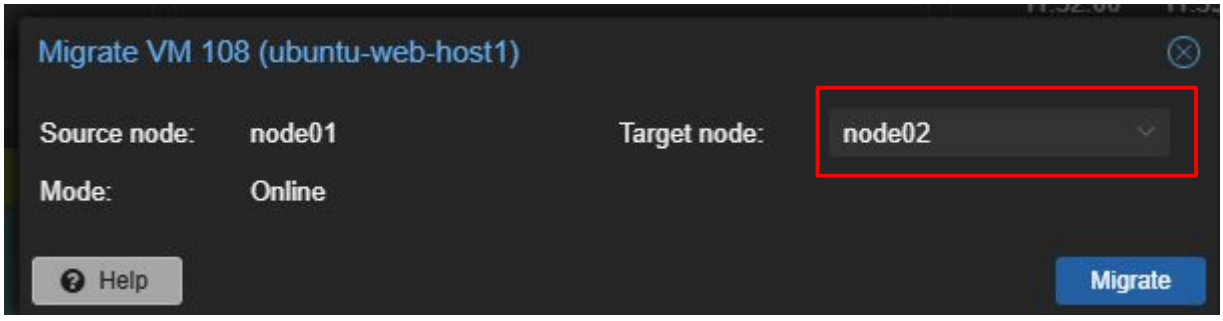
* le cluster reste stable et ne perd pas le quorom , avec la migration et le redémarrage avec succès des deux serveurs dans le 1er nœud (node01).

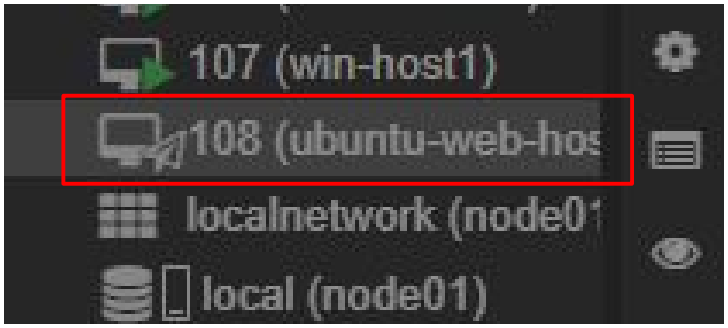


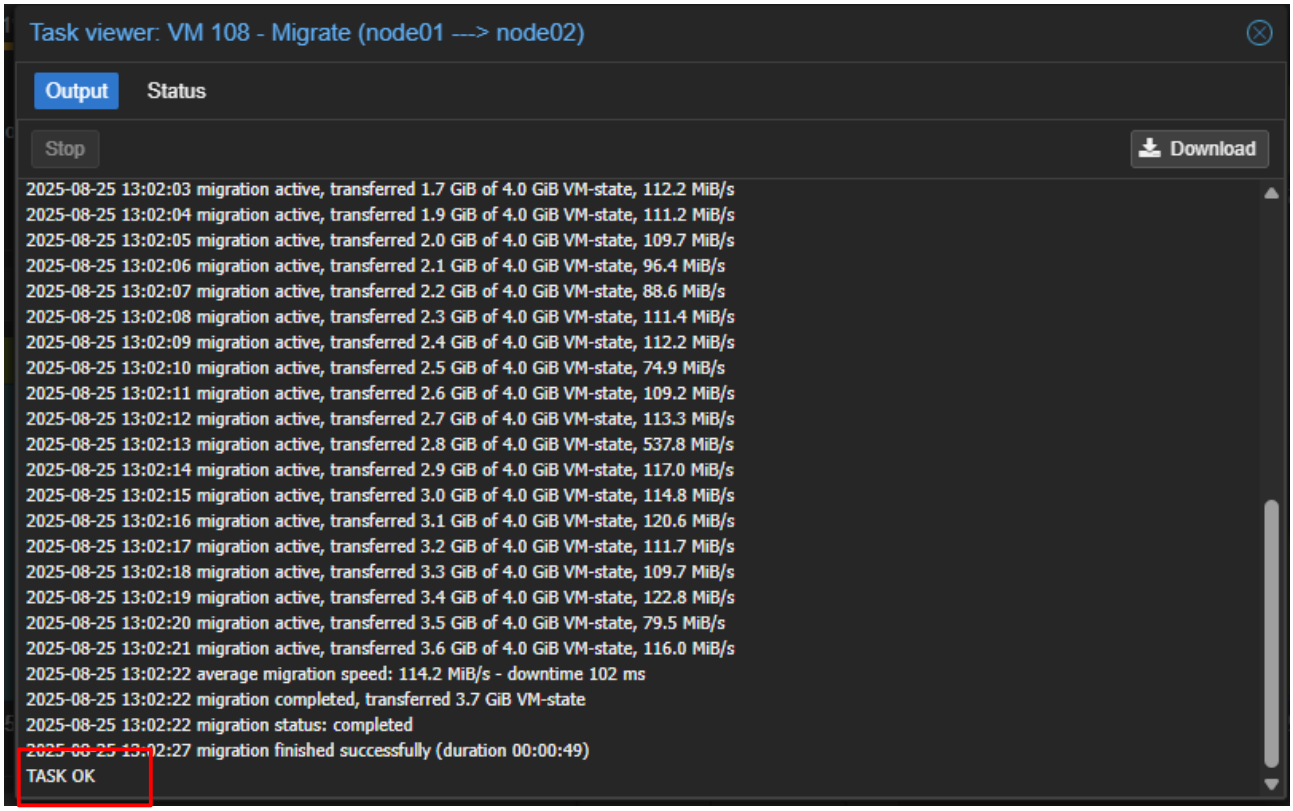
Aug 15 12:45:38	Aug 15 12:45:40	node02	root@pam	VM 102 - Start	OK
Aug 15 12:45:35	Aug 15 12:46:50	node01	root@pam	VM 102 - Migrate	OK
Aug 15 12:45:28	Aug 15 12:45:30	node02	root@pam	VM 101 - Start	OK
Aug 15 12:45:25	Aug 15 12:46:37	node01	root@pam	VM 101 - Migrate	OK
Aug 15 12:45:24	Aug 15 12:45:26	node01	root@pam	HA 102 - Migrate	OK
Aug 15 12:45:07	Aug 15 12:45:09	node01	root@pam	HA 101 - Migrate	OK

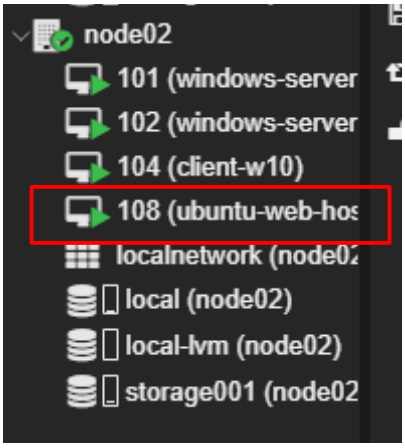
7.3 – Test de la Migration à Chaud (Live Migration) :

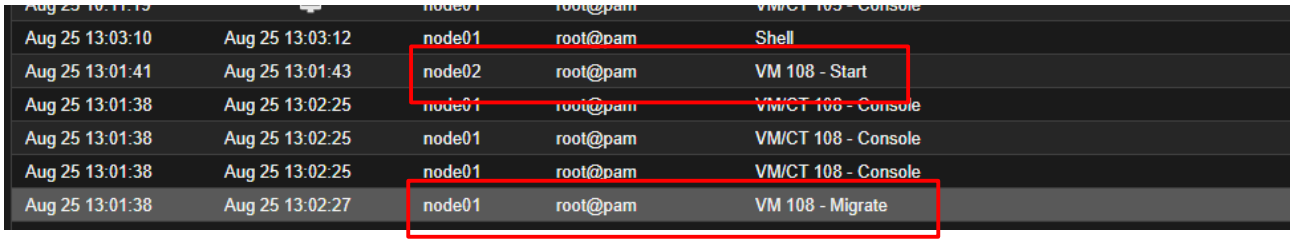







Task viewer: VM 108 - Migrate (node01 ---> node02)
Output
Status
Stop
Download
2025-08-25 13:02:03 migration active, transferred 1.7 GiB of 4.0 GiB VM-state, 112.2 MiB/s
2025-08-25 13:02:04 migration active, transferred 1.9 GiB of 4.0 GiB VM-state, 111.2 MiB/s
2025-08-25 13:02:05 migration active, transferred 2.0 GiB of 4.0 GiB VM-state, 109.7 MiB/s
2025-08-25 13:02:06 migration active, transferred 2.1 GiB of 4.0 GiB VM-state, 96.4 MiB/s
2025-08-25 13:02:07 migration active, transferred 2.2 GiB of 4.0 GiB VM-state, 88.6 MiB/s
2025-08-25 13:02:08 migration active, transferred 2.3 GiB of 4.0 GiB VM-state, 111.4 MiB/s
2025-08-25 13:02:09 migration active, transferred 2.4 GiB of 4.0 GiB VM-state, 112.2 MiB/s
2025-08-25 13:02:10 migration active, transferred 2.5 GiB of 4.0 GiB VM-state, 74.9 MiB/s
2025-08-25 13:02:11 migration active, transferred 2.6 GiB of 4.0 GiB VM-state, 109.2 MiB/s
2025-08-25 13:02:12 migration active, transferred 2.7 GiB of 4.0 GiB VM-state, 113.3 MiB/s
2025-08-25 13:02:13 migration active, transferred 2.8 GiB of 4.0 GiB VM-state, 537.8 MiB/s
2025-08-25 13:02:14 migration active, transferred 2.9 GiB of 4.0 GiB VM-state, 117.0 MiB/s
2025-08-25 13:02:15 migration active, transferred 3.0 GiB of 4.0 GiB VM-state, 114.8 MiB/s
2025-08-25 13:02:16 migration active, transferred 3.1 GiB of 4.0 GiB VM-state, 120.6 MiB/s
2025-08-25 13:02:17 migration active, transferred 3.2 GiB of 4.0 GiB VM-state, 111.7 MiB/s
2025-08-25 13:02:18 migration active, transferred 3.3 GiB of 4.0 GiB VM-state, 109.7 MiB/s
2025-08-25 13:02:19 migration active, transferred 3.4 GiB of 4.0 GiB VM-state, 122.8 MiB/s
2025-08-25 13:02:20 migration active, transferred 3.5 GiB of 4.0 GiB VM-state, 79.5 MiB/s
2025-08-25 13:02:21 migration active, transferred 3.6 GiB of 4.0 GiB VM-state, 116.0 MiB/s
2025-08-25 13:02:22 average migration speed: 114.2 MiB/s - downtime 102 ms
2025-08-25 13:02:22 migration completed, transferred 3.7 GiB VM-state
2025-08-25 13:02:22 migration status: completed
2025-08-25 13:02:27 migration finished successfully (duration 00:00:49)
TASK OK

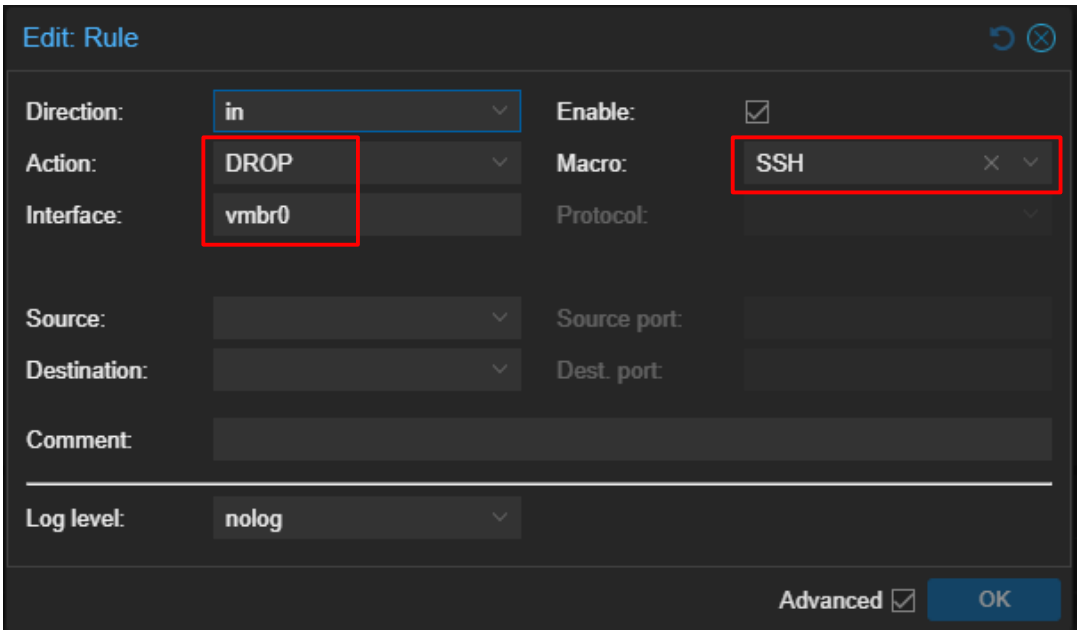

node02
101 (windows-server
102 (windows-server
104 (client-w10)
108 (ubuntu-web-hos
localnetwork (node02
local (node02)
local-lvm (node02)
storage001 (node02


Aug 25 13:03:10 Aug 25 13:03:12 node01 root@pam Shell
Aug 25 13:01:41 Aug 25 13:01:43 node02 root@pam VM 108 - Start
Aug 25 13:01:38 Aug 25 13:02:25 node01 root@pam VM/CT 108 - Console
Aug 25 13:01:38 Aug 25 13:02:25 node01 root@pam VM/CT 108 - Console
Aug 25 13:01:38 Aug 25 13:02:25 node01 root@pam VM/CT 108 - Console
Aug 25 13:01:38 Aug 25 13:02:27 node01 root@pam VM 108 - Migrate

7.4 – Test du Pare-feu (Firewal) :

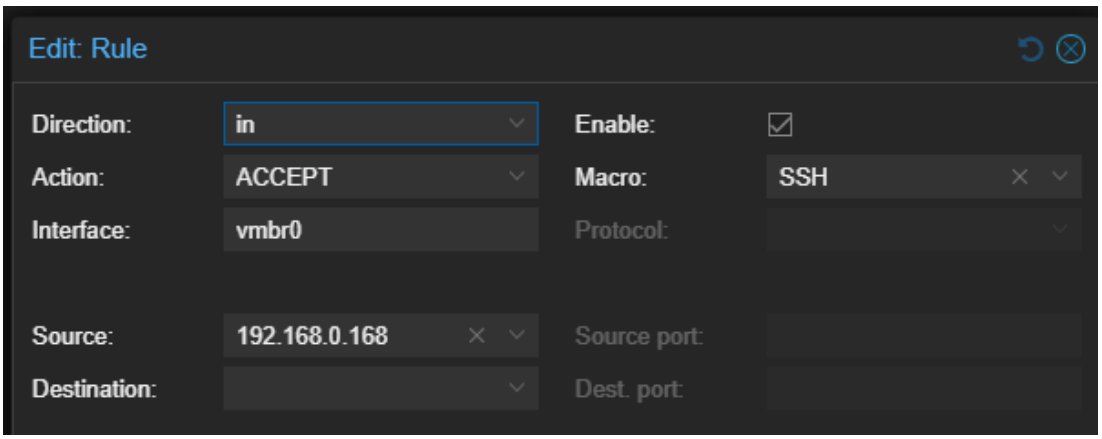
La validation du pare-feu sera effectuée en mettant en place des règles de sécurité pour limiter l'accès aux services du serveur. Cette démarche vise à garantir que seules les connexions provenant d'adresses IP autorisées sont acceptées.

1er règle Désactiver l'accès par SSH au cluster :




```
C:\Users\elouafi>ssh root@192.168.0.242
ssh: connect to host 192.168.0.242 port 22: Connection timed out
```

Accepter la connexion via SSH depuis un seul host 192.168.0.168/24 :



```
C:\Users\elouafi>ipconfig

Configuration IP de Windows


Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . : mshome.net
   Adresse IPv6 de liaison locale. . . . .: fe80::e6d8:8d9c:8f59:ef80%12
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.0.168
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 192.168.0.1
```

```
C:\Users\elouafi>ssh root@192.168.0.242
root@192.168.0.242's password:
Linux node01 6.8.12-9-pve #1 SMP PREEMPT_DYNAMIC PMX 6.8.12-9 (2025-03-16T19:18Z) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Aug 26 11:57:46 2025 from 192.168.0.242
root@node01:~#
```

Test depuis un host Ubuntu (192.168.0.171/24) non admis par le firewall :

```
host2@host2:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOW
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_code
    link/ether bc:24:11:97:a2:d9 brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet 192.168.0.171/24 brd 192.168.0.255 scope global dynamic n
       valid_lft 79331sec preferred_lft 79331sec
    inet6 fe80::b71c:e7e9:a14:eece/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
host2@host2:~$
```

```
host2@host2:~$ ssh root@192.168.0.242
ssh: connect to host 192.168.0.242 port 22: Connection timed out
host2@host2:~$
```

2ème règle Désactiver le ping (IMCP) et accepter le depuis un seul host 192.168.0.168/24:

```
C:\Users\elouafi>ping 192.168.0.242

Envoi d'une requête 'Ping'  192.168.0.242 avec 32 octets de données :
Réponse de 192.168.0.242 : octets=32 temps<1ms TTL=64
Réponse de 192.168.0.242 : octets=32 temps<1ms TTL=64
Réponse de 192.168.0.242 : octets=32 temps<1ms TTL=64
Réponse de 192.168.0.242 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 192.168.0.242:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\Users\elouafi>
```

depuis un host non-admis par le firewall :

```
host2@host2:~$ ping 192.168.0.242
PING 192.168.0.242 (192.168.0.242) 56(84) bytes of data.
^C
--- 192.168.0.242 ping statistics ---
70 packets transmitted, 0 received, 100% packet loss, time 70647ms

host2@host2:~$
```

Il est également possible de configurer les règles du pare-feu en éditant directement le fichier de configuration situé à /etc/pve/firewall/cluster.fw

```
  GNU nano 7.2
[OPTIONS]

enable: 1

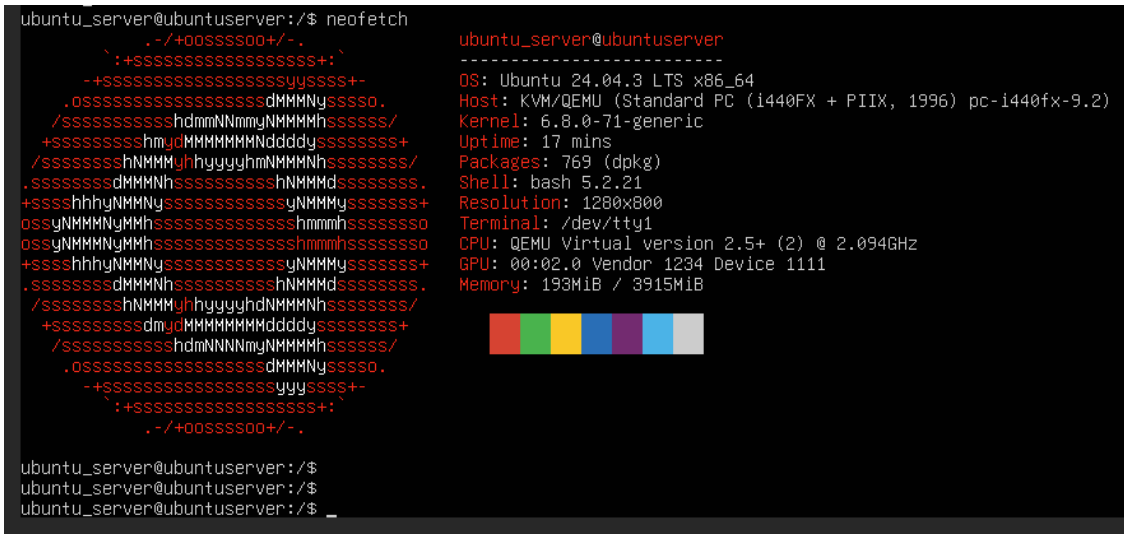
[RULES]

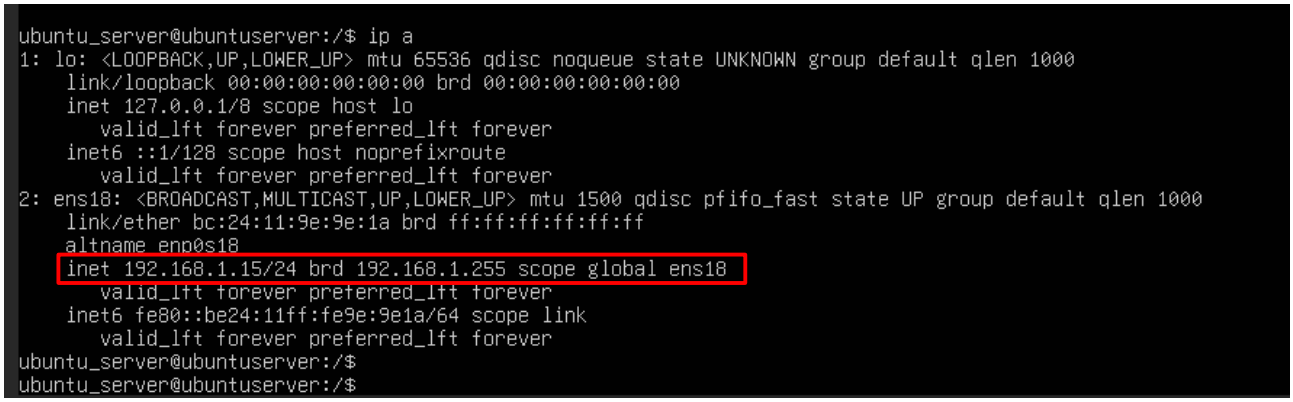
IN SSH(ACCEPT) -i vmbr0 -source 192.168.0.168 -log alert
IN ACCEPT -i vmbr0 -source 192.168.0.168 -p icmp -log alert
IN SSH(DROP) -i vmbr0 -log alert
```

7.5 – Test du réseaux NAT :

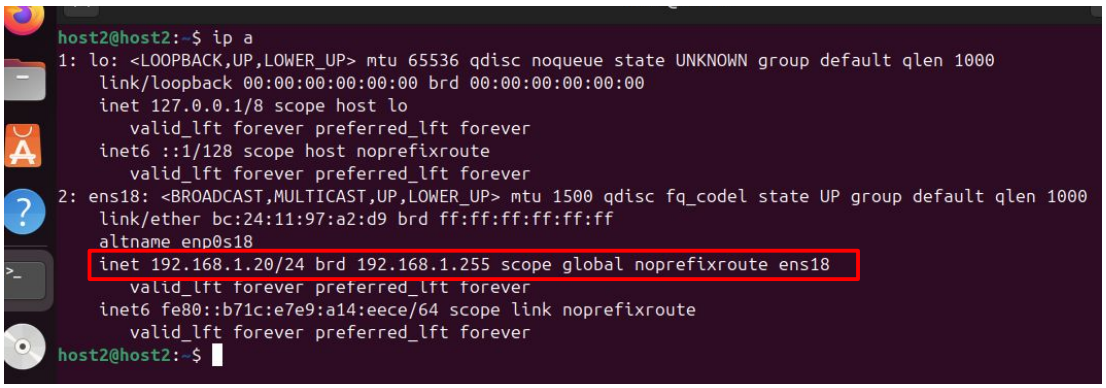
La validation du réseau NAT a été réalisée en déployant un serveur web sur une machine virtuelle (VM) sous Ubuntu Server. Pour vérifier que la connectivité était fonctionnelle, un client a été connecté au même sous-réseau 192.168.1.0/24 afin de s'assurer qu'il pouvait accéder à la page web hébergée.

Ubuntu Server :





Client :



```
host2@host2:~$ ping 192.168.1.15
PING 192.168.1.15 (192.168.1.15) 56(84) bytes of data.
64 bytes from 192.168.1.15: icmp_seq=1 ttl=64 time=0.724 ms
64 bytes from 192.168.1.15: icmp_seq=2 ttl=64 time=0.364 ms
64 bytes from 192.168.1.15: icmp_seq=3 ttl=64 time=0.412 ms
64 bytes from 192.168.1.15: icmp_seq=4 ttl=64 time=0.387 ms
64 bytes from 192.168.1.15: icmp_seq=5 ttl=64 time=0.444 ms
^C
--- 192.168.1.15 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4098ms
rtt min/avg/max/mdev = 0.364/0.466/0.724/0.131 ms
host2@host2:~$
```

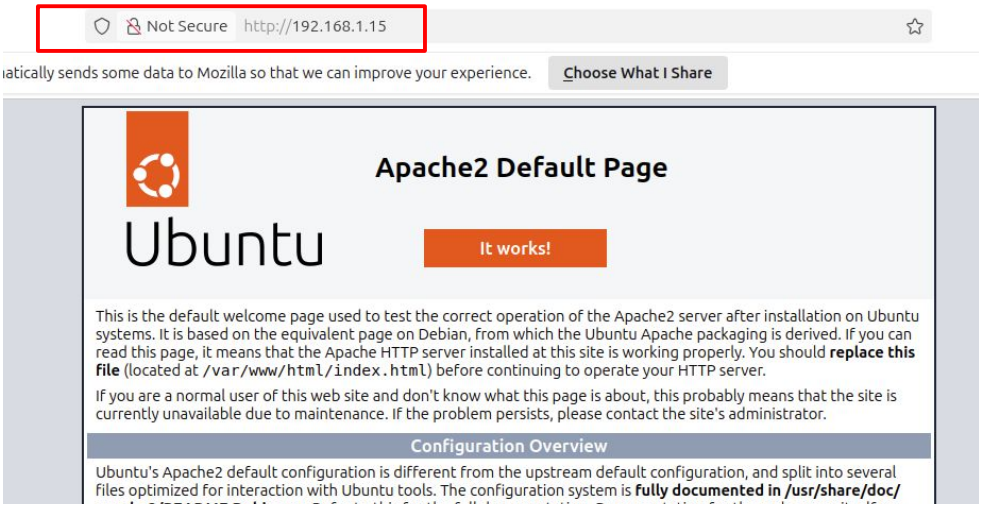
```
host2@host2:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=114 time=28.2 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=114 time=27.7 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=114 time=27.5 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=114 time=27.3 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=114 time=27.1 ms
^C
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4008ms
rtt min/avg/max/mdev = 27.061/27.554/28.224/0.391 ms
host2@host2:~$
```

Création du serveur web (Apache2) :

```
ubuntu_server@ubuntuserver:~$ sudo apt install apache2
[sudo] password for ubuntu_server:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libapr1t64 libaprutil1-dbd-sqlite3 libap
  liblua5.4-0 ssl-cert
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libapr1t64 libaprutil1-dbd-sqli
  liblua5.4-0 ssl-cert
0 upgraded, 10 newly installed, 0 to remove and 4 not upgraded.
Need to get 2,086 kB of archives.
After this operation, 8,090 kB of additional disk space will be used.
```

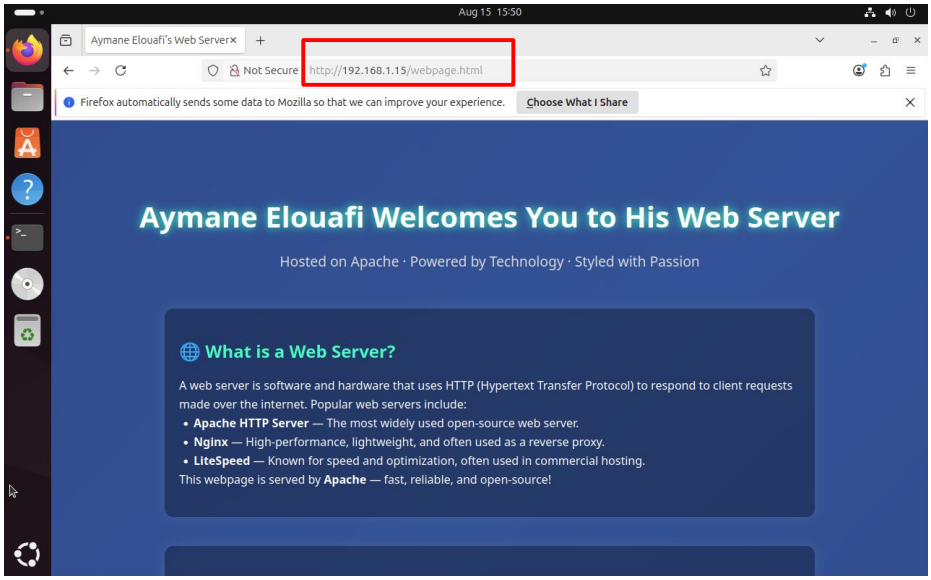
```
ubuntu_server@ubuntuserver:~$ sudo systemctl start apache2.service
ubuntu_server@ubuntuserver:~$ sudo systemctl enable apache2.service
Synchronizing state of apache2.service with SysV service script with /usr/lib/systemd/systemd-s
Executing: /usr/lib/systemd/systemd-sysv-install enable apache2
ubuntu_server@ubuntuserver:~$ sudo systemctl status apache2.service
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: enabled)
     Active: active (running) since Fri 2025-08-15 14:31:21 UTC; 1min 55s ago
       Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 2365 (apache2)
      Tasks: 55 (limit: 4605)
     Memory: 5.2M (peak: 5.6M)
        CPU: 134ms
     CGroup: /system.slice/apache2.service
             ├─2365 /usr/sbin/apache2 -k start
             ├─2368 /usr/sbin/apache2 -k start
             └─2369 /usr/sbin/apache2 -k start

Aug 15 14:31:21 ubuntuserver systemd[1]: Starting apache2.service - The Apache HTTP Server...
```



Editer le fichier /var/www/webpage.html





8. Conclusion :

Ce projet a permis de mettre en œuvre une plateforme de virtualisation à **haute disponibilité** et **tolérance aux pannes** reposant sur deux serveurs physiques HP ProLiant DL360p Gen8 et un stockage partagé de type NAS LenovoEMC px6-300d via NFS. L'objectif principal, à savoir démontrer la capacité du système à maintenir la **continuité des services en cas de défaillance**, a été atteint avec succès grâce à la configuration d'un cluster Proxmox VE et à l'intégration des mécanismes de haute disponibilité (HA). Les tests menés, incluant la **migration à chaud** et la validation du **basculement automatique**, ont confirmé la robustesse et la fiabilité de la solution déployée.

Sur le plan technique, ce travail a permis de traiter différentes problématiques concrètes : la configuration des serveurs et du cluster, l'intégration du stockage partagé, la mise en place du pare-feu, ainsi que la gestion des utilisateurs et des permissions. L'un des défis majeurs a résidé dans la gestion du **quorum dans une architecture à deux nœuds**, résolu par l'ajustement de la pondération des votes, garantissant ainsi la stabilité et la continuité du cluster. Ces étapes ont constitué une véritable **expérience pratique** en administration des systèmes virtualisés et en conception d'infrastructures tolérantes aux pannes.

Au-delà de la réussite technique, ce projet a également représenté une **opportunité d'apprentissage** approfondie. Il nous a permis de renforcer notre maîtrise des concepts de virtualisation, de clustering et de stockage partagé, tout en développant des compétences pratiques directement transférables au monde professionnel.

Enfin, plusieurs **pistes d'évolution** peuvent être envisagées afin d'optimiser et d'industrialiser cette plateforme. L'ajout d'un **QDevice** pour renforcer le quorum, l'implémentation d'une solution de **sauvegarde centralisée**, ou encore l'intégration de la **redondance**

réseau via le bonding des interfaces constitueraient des améliorations significatives pour préparer une exploitation en production. De plus, l’automatisation de certaines tâches administratives et l’intégration d’outils de supervision en temps réel pourraient contribuer à une gestion plus proactive et efficace de l’infrastructure.

9. Références :

https://www.redhat.com/fr/topics/virtualization/what-is-virtualization

https://www.nutanix.com/fr/info/virtualization

https://www.redhat.com/fr/topics/virtualization/what-is-a-virtual-machine

https://www.redhat.com/fr/topics/virtualization/what-is-a-hypervisor

https://sysracks.com/fr/blogue/cluster-informatique-quest-ce-que-cest/?srsltid=AfmBOorwc3Iy2z_xpEiJdh5V1O0iYOo_8MnQ56B12OKfZrS2DTsWUW4k

https://www.theseus.fi/bitstream/handle/10024/127326/Dudnik_Anastasia.pdf?sequence=1&isAllowed=y

https://www.redhat.com/fr/topics/linux/what-is-high-availability

https://www.informatiweb-pro.net/admin-systeme/win-server/ws-2012-2012-r2-a-quoi-servent-les-differents-types-de-quorum.html

https://learn.microsoft.com/fr-fr/windows-server/storage/storage-spaces/quorum

https://www.hpe.com/emea_africa/fr/what-is/shared-storage.html

https://www.hpe.com/emea_africa/fr/what-is/san-storage.html

https://fr.wikipedia.org/wiki/R%C3%A9seau_de_stockage_SAN

https://fr.wikipedia.org/wiki/Serveur_de_stockage_en_r%C3%A9seau

https://aws.amazon.com/fr/what-is/nas/

https://www.fs.com/fr/blog/complete-guide-to-server-raid-9104.html

https://dynfi.com/proxmox/qu-est-ce-que-proxmox/

https://www.syloe.com/glossaire/serveur-informatique/

https://fr.wikipedia.org/wiki/Commutateur_r%C3%A9seau

https://www.aten.com/fr/fr/resources/feature-articles/what-is-a-kvm-switch/

https://pve.proxmox.com/wiki/Renaming_a_PVE_node

https://edywerder.ch/proxmox-cluster-2-nodes/

https://pve.proxmox.com/wiki/Firewall