Conception d'une infrastructure virtualisée résiliente – NovaSys

1. Contexte professionnel

L'entreprise NovaSys est une PME d'environ 30 employés spécialisée dans les services numériques. L'activité de l'entreprise repose fortement sur son système d'information, notamment pour : l'accès aux applications internes, le stockage et le partage de documents, la communication entre les équipes, l'administration du réseau.

Actuellement, l'entreprise possède deux serveurs physiques récents situés dans le même réseau local. Cependant, l'infrastructure présente plusieurs limites : absence de haute disponibilité, gestion des services dispersée, manque de centralisation de l'administration, faible résilience en cas de panne.

Afin d'améliorer la fiabilité, la sécurité et la gestion du système d'information, NovaSys souhaite mettre en place une infrastructure virtualisée résiliente basée sur un cluster d'hyperviseurs.

Cette nouvelle architecture devra permettre : l'hébergement des services essentiels, la continuité de service en cas de panne, la centralisation de l'administration, une meilleure gestion des ressources.

2. Analyse du besoin métier

NovaSys est une PME spécialisée dans les services numériques. L'entreprise possède environ 30 collaborateurs et dépend fortement de son système d'information pour le fonctionnement quotidien de ses activités. Les besoins identifiés incluent :

• centralisation des services : Actuellement, les services sont répartis sans organisation claire. La virtualisation permettra de regrouper les services dans un environnement contrôlé.

• amélioration de la sécurité : La segmentation et l'isolation des machines virtuelles permettront de limiter les risques en cas d'incident.

• simplification de l'administration : Une interface centralisée permettra de gérer l'ensemble des serveurs et machines virtuelles.

• continuité de service en cas de panne : L'infrastructure doit rester fonctionnelle même en cas de panne d'un serveur.

La virtualisation permet de répondre efficacement à ces exigences en consolidant les services sur une infrastructure unique tout en conservant l'isolation entre les applications.

3. Choix de la virtualisation

La virtualisation consiste à exécuter plusieurs machines virtuelles sur un même serveur physique.

Chaque machine virtuelle dispose de :

- Son propre système d'exploitation
- Ses ressources dédiées
- Un environnement isolé

Avantages

- Meilleure utilisation du matériel
- Réduction des coûts
- Déploiement rapide de nouveaux services
- Migration de machines virtuelles
- Isolation des applications

Hyperviseur retenu : Proxmox VE

Proxmox VE est une plateforme de virtualisation open source basée sur :

- **KVM** pour les machines virtuelles
- **LXC** pour les conteneurs
- **ZFS** pour la gestion du stockage

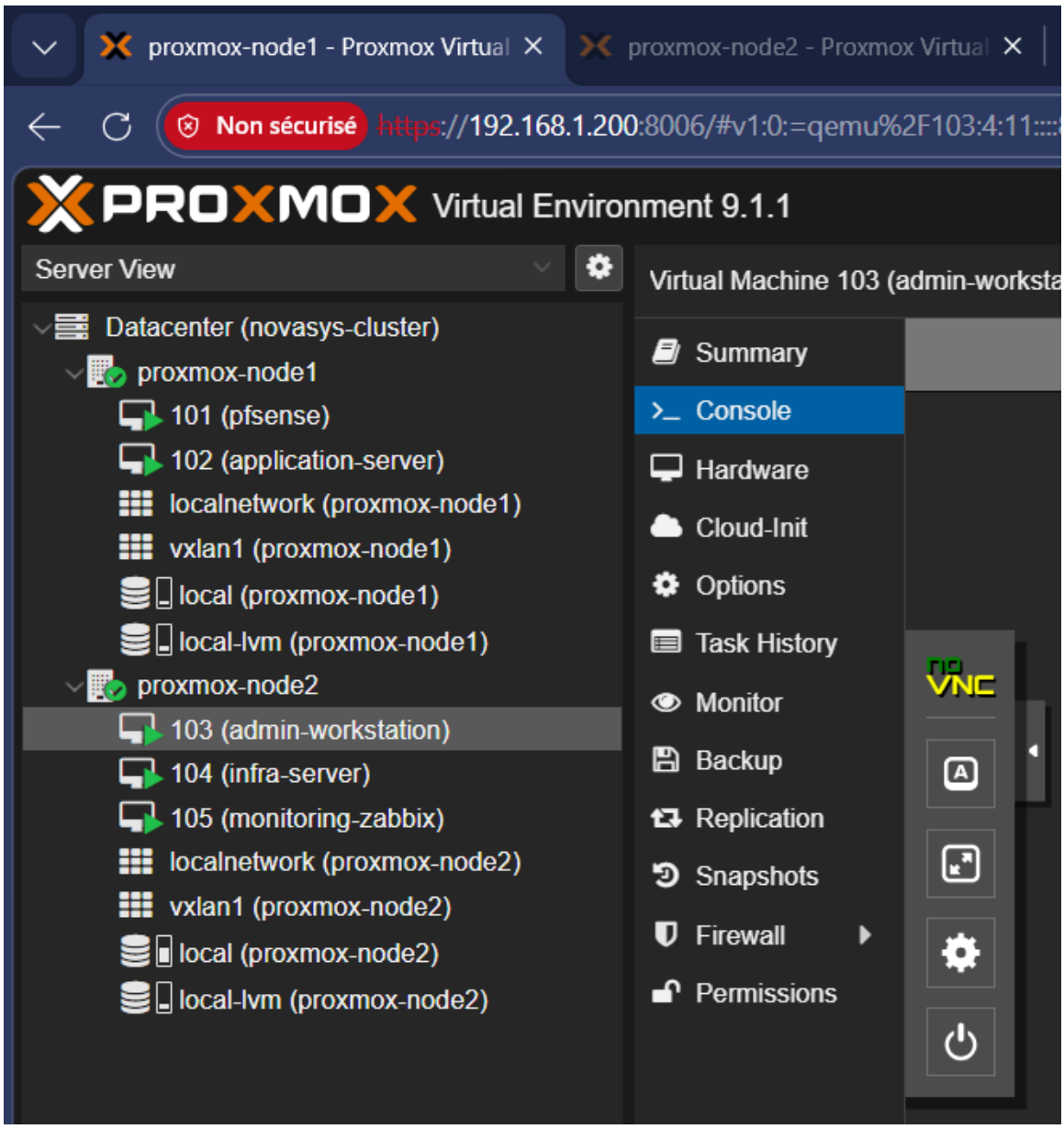
Fonctionnalités principales

- Gestion centralisée via interface web
- Cluster natif

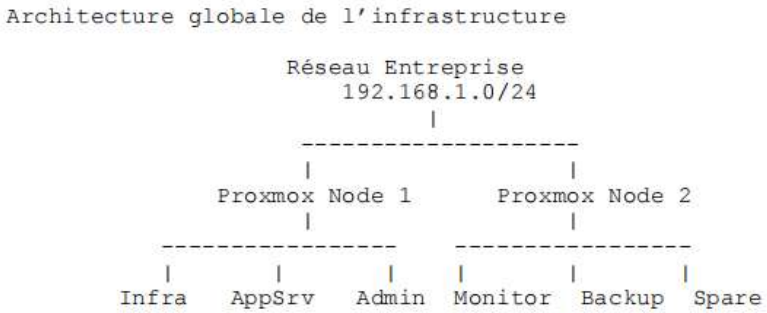
- Haute disponibilité
- Réplication des machines virtuelles
- Firewall intégré
- Sauvegarde intégrée

Ce choix permet d'obtenir une infrastructure professionnelle sans coût de licence.

4. Description des machines virtuelles :



Architecture générale



L'infrastructure repose sur deux serveurs physiques configurés en cluster Proxmox.

Serveurs physiques :

Serveur	**Rôle**
Proxmox-node1	Hyperviseur principal
Proxmox-node2	Hyperviseur secondaire

Les deux serveurs sont connectés sur le réseau interne et partagent :

- Le réseau de management
- Le réseau de machines virtuelles
- Le réseau de réplication

Machines virtuelles

Machine	Type	OS	Rôle
infra-server	VM	Debian / Ubuntu Server	Samba AD + DNS (authentification centralisée)
application-server	VM	Linux Server	Application interne entreprise
admin-workstation	VM	Linux Desktop (XFCE)	Poste graphique administration
monitoring-server	VM	Linux Server	Supervision infrastructure (Zabbix)

L'infrastructure comporte plusieurs machines virtuelles spécialisées :

- **Infra Server :**
    - Rôle :

- Serveur d'authentification
- Gestion des utilisateurs
- Services réseau
    - Services installés :

- Samba Active Directory
- DNS
- DHCP
    - Fonction :

- Centralisation de l'authentification
- Gestion des comptes utilisateurs

- **Application Server :** Ce serveur héberge l'application interne utilisée par les employés.

- Fonctions :
- Hébergement web
- Accès aux données métier
- Interaction avec la base de données

- Technologies possibles :
- Apache / Nginx
- Base de données MySQL ou PostgreSQL

- **Admin Workstation :** poste graphique dédié à l'administration de l'environnement.

    - Fonctions :

- Accès SSH
- Administration Proxmox
- Outils réseau

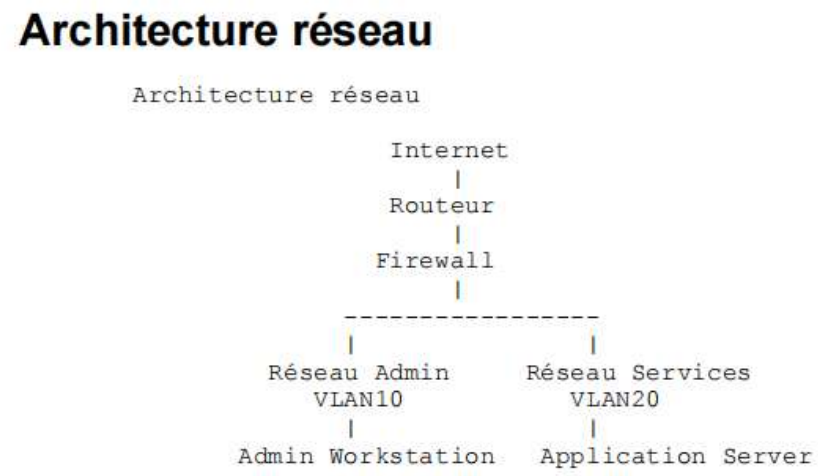
- **Monitoring Server :** surveillance des performances et des services via Zabbix.

    - Logiciels :

- Zabbix
- Prometheus
- Grafana
    - Fonctions :

- Surveillance des serveurs
- Alertes en cas de panne
- Visualisation des performances

Chaque machine est isolée afin de limiter l'impact d'un incident de sécurité.

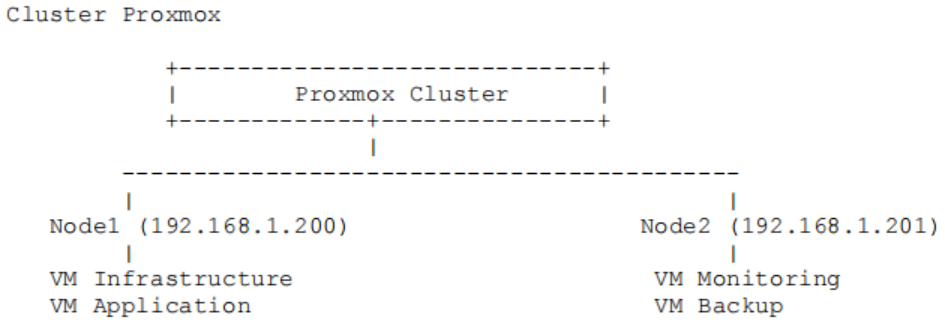


Le réseau est segmenté grâce à l'utilisation de VLAN.

Cette segmentation améliore :

- La sécurité
- La gestion du trafic
- L'isolation des services

5. Architecture du cluster



L'infrastructure repose sur une architecture de virtualisation basée sur l'hyperviseur Proxmox VE. Ce choix est motivé par plusieurs avantages :

- Hyperviseur open source professionnel
- Gestion intégrée des machines virtuelles et conteneurs
- Cluster intégré
- Support de la haute disponibilité
- Réplication de stockage
- Firewall intégré
- Interface web d'administration

Deux serveurs physiques constituent les nœuds du cluster :

- Proxmox-node1
- Proxmox-node2

Ces deux serveurs sont interconnectés via un réseau local interne et partagent une architecture réseau permettant la migration des machines virtuelles et la réplication des données.

Les objectifs principaux de l'architecture sont :

- Tolérance aux pannes
- Centralisation des services
- Isolation des rôles
- Facilité d'administration
- Supervision continue

6. Gestion des utilisateurs :

L’organisation des comptes suit le principe du moindre privilège (PoLP). Chaque utilisateur possède uniquement les droits nécessaires à l’exercice de ses fonctions. Les groupes principaux sont :

• **adminIT :** administration complète

• **dev :** accès aux services applicatifs

• **users :** accès utilisateur standard

Cette organisation permet de limiter les risques liés aux erreurs humaines ou aux compromissions de comptes

7. Sécurité de l’infrastructure :

Plusieurs mécanismes de sécurité sont mis en place :

• pare-feu réseau

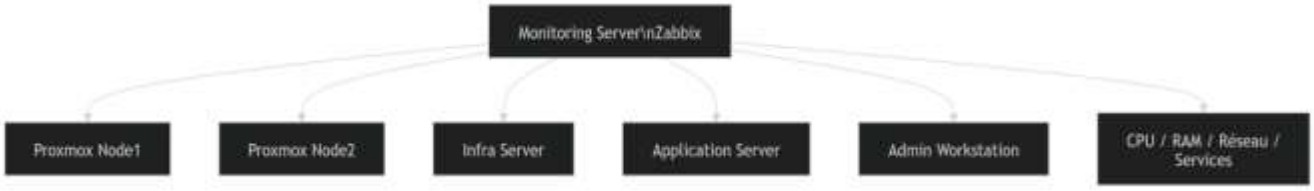
• authentification forte

• segmentation des services

• surveillance des accès

Les accès SSH sont restreints aux adresses autorisées et les tentatives de connexion suspectes sont bloquées automatiquement grâce à Fail2ban.

8. Supervision et monitoring :



La supervision de l'infrastructure est assurée par un serveur Zabbix. Ce système permet de surveiller les ressources des machines virtuelles et des serveurs physiques.

Les métriques surveillées incluent :

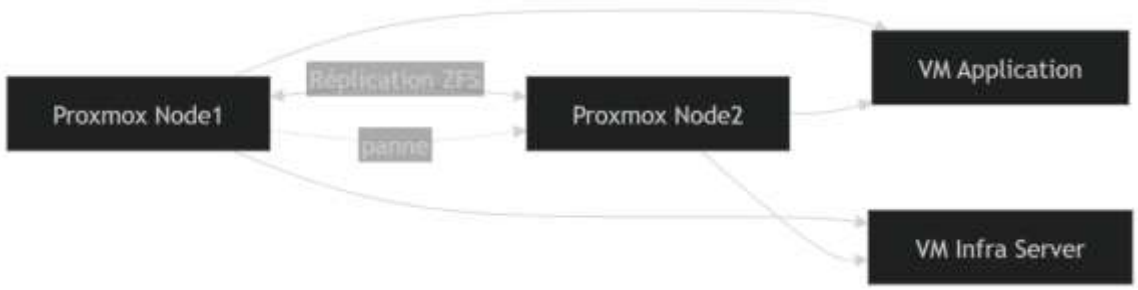
• utilisation CPU

• mémoire

• trafic réseau

• disponibilité des services

9. Stockage et réplication :



Le stockage repose sur ZFS, un système de fichiers avancé permettant la gestion de snapshots et la réplication des données entre les deux serveurs. Cette réplication garantit que les machines virtuelles peuvent redémarrer sur l'autre serveur en cas de panne.
Le RPO (Recovery Point Objective) est estimé à environ 5 minutes, ce qui signifie que la perte maximale de données en cas d'incident reste très limitée.

Technologie retenue : Stockage local avec réplication Proxmox.

Principe : Les disques des machines virtuelles sont répliqués entre les deux nœuds.

Objectif :

- RPO faible

- redémarrage possible des services sur le second serveur

- continuité de service

En cas de panne d'un nœud : les machines virtuelles peuvent être redémarrées sur l'autre serveur.

10.Gestion des utilisateurs et des droits (PoLP)

La gestion des accès repose sur le principe du moindre privilège (PoLP).
Chaque utilisateur possède uniquement les droits nécessaires à ses fonctions.

Responsable informatique : administration complète.
Techniciens : maintenance et supervision.
Utilisateurs : accès limité aux applications nécessaires.

11.Sécurité de l'infrastructure

Mesures mises en place :

Accès administratifs :

- accès SSH sécurisé

- authentification par clé possible

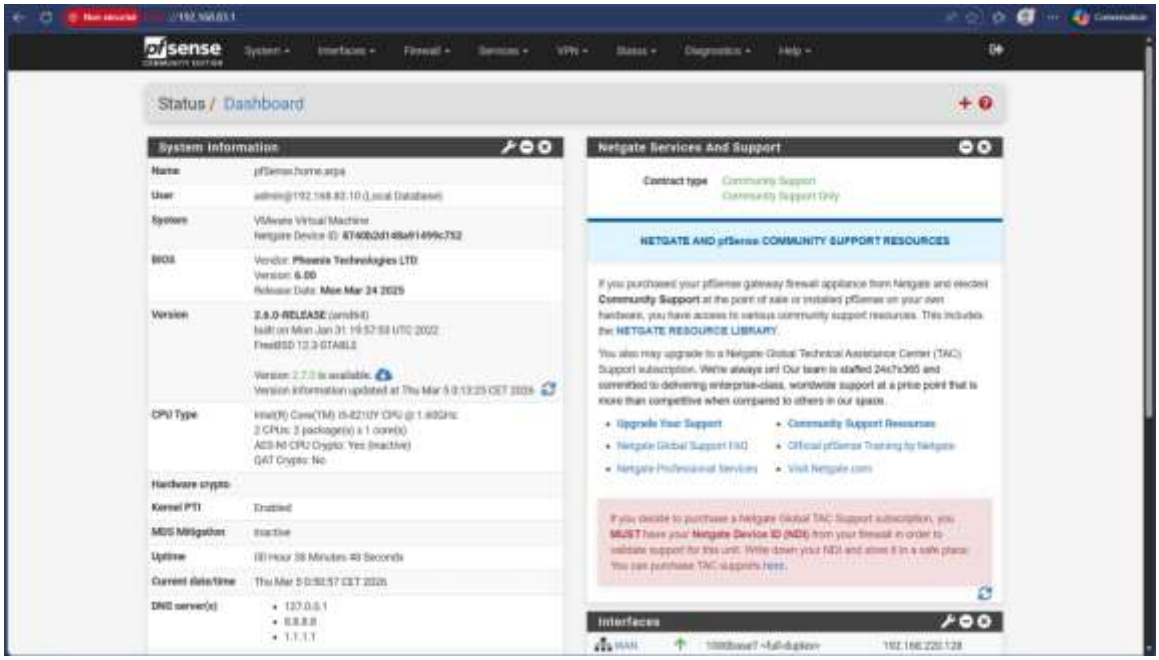
- restriction réseau

Protection :

- Firewall Proxmox

- Firewall Linux sur les VM

- Fail2ban pour prévenir les attaques brute force



Isolation :

- séparation des services par machines virtuelles

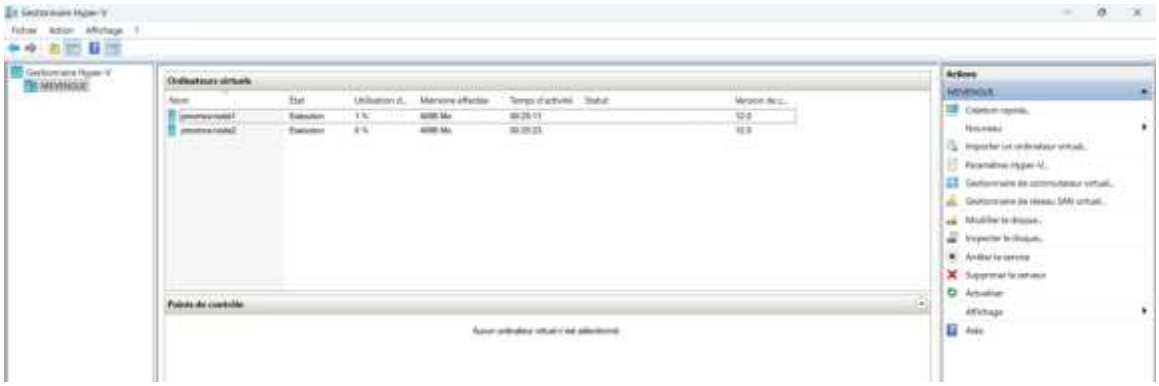
Supervision :

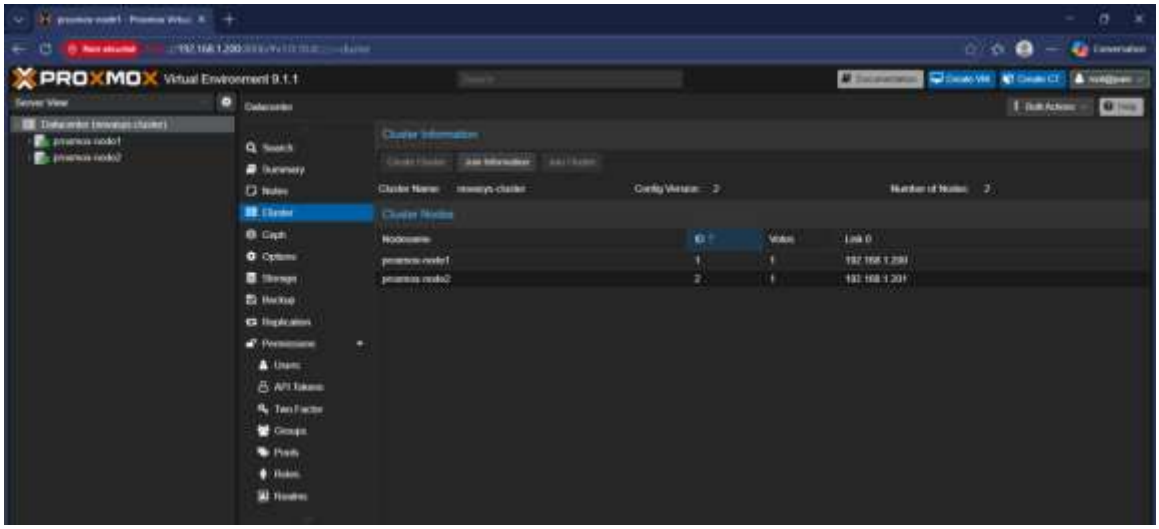
- serveur Zabbix pour surveiller CPU, RAM, réseau et disponibilité des services.

11. Plan de déploiement

Étape 1 :

Installation de **Proxmox VE** sur les deux serveurs physiques.

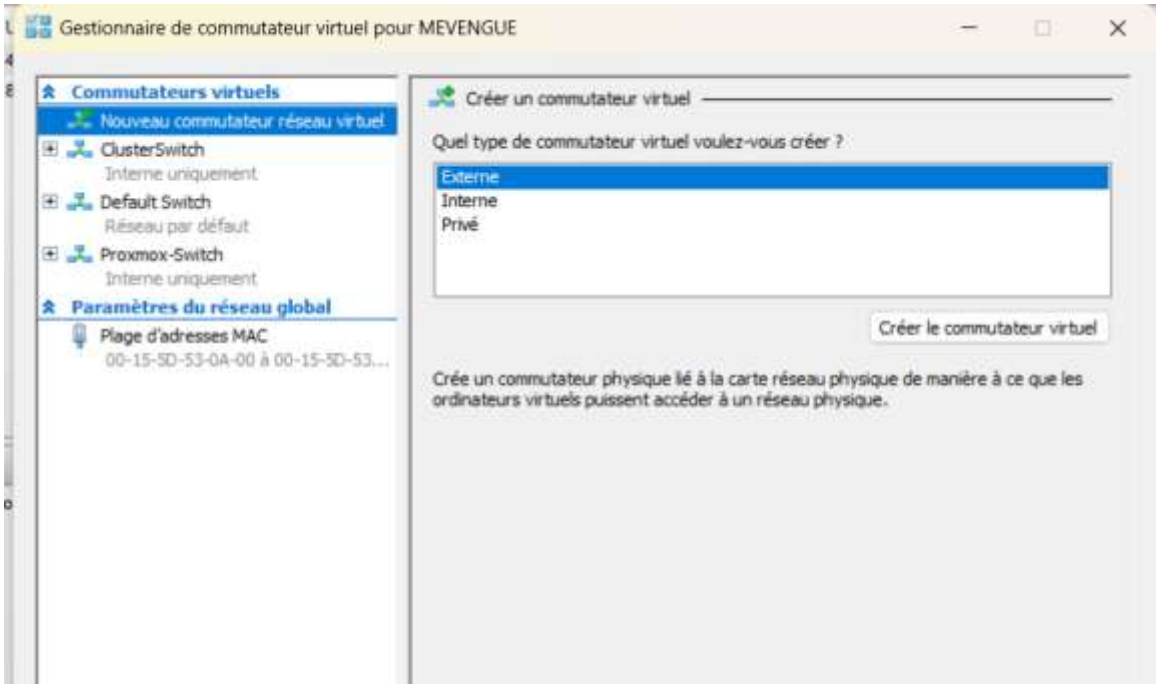


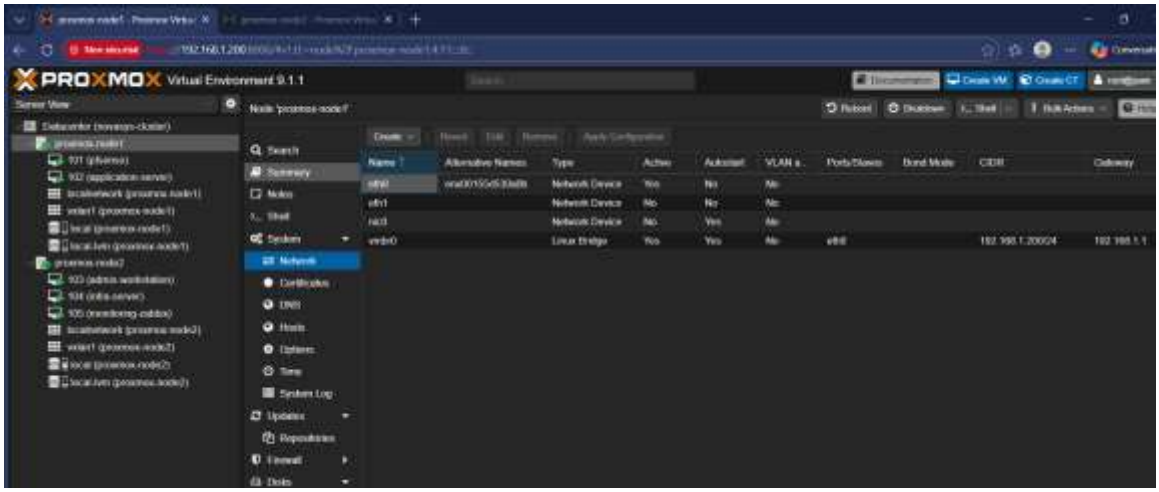


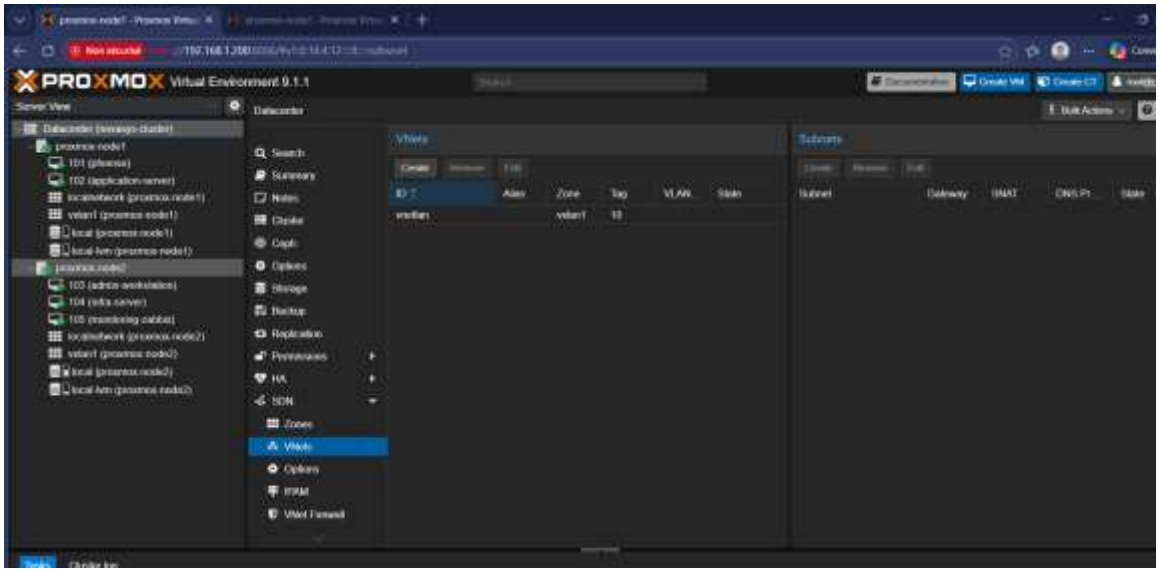
Étape 2 :

Configuration réseau :

- Interfaces réseau
- VLAN
- Bridge réseau

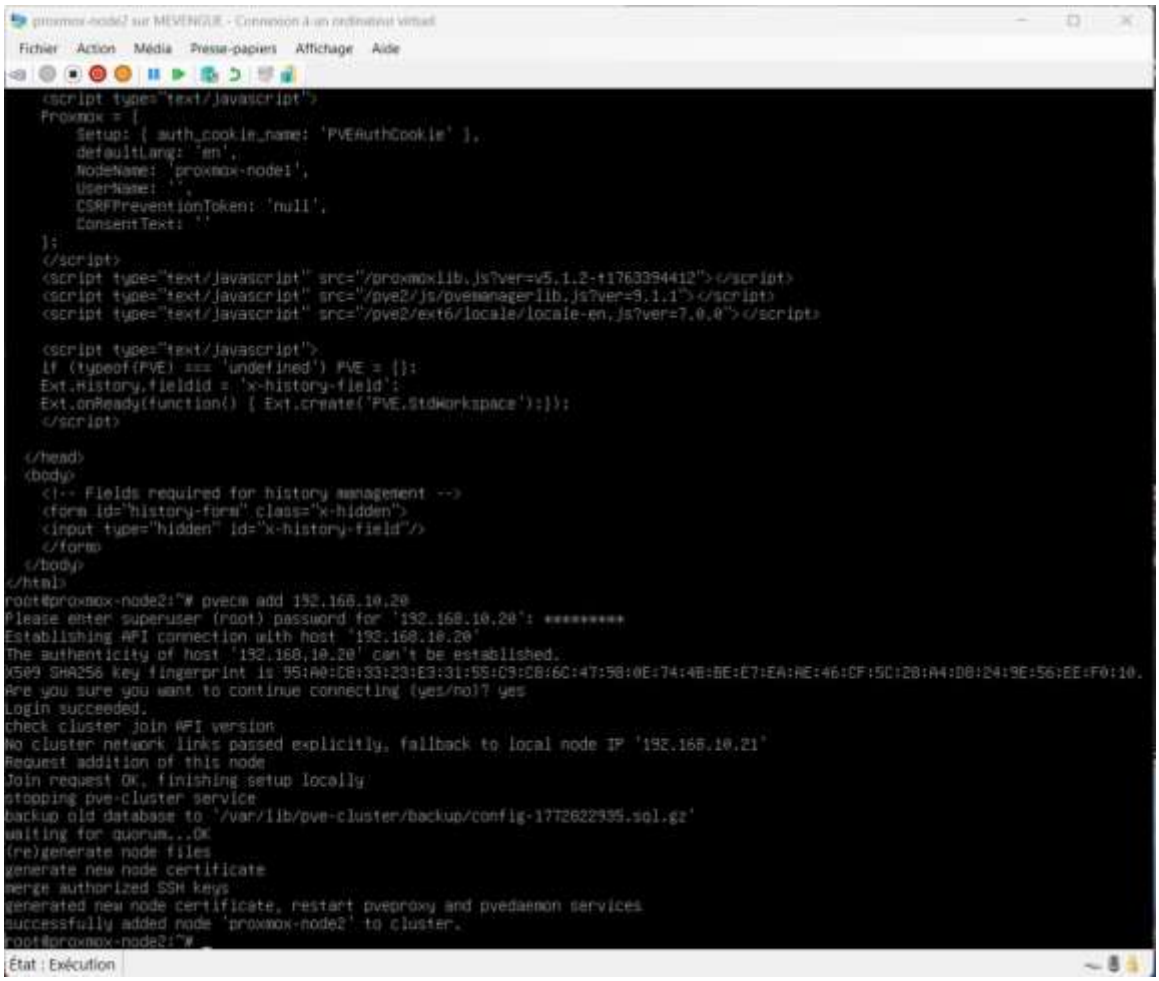

Gestionnaire de commutateur virtuel pour MEVENGUE
Commutateurs virtuels
Nouveau commutateur réseau virtuel
ClusterSwitch
Interne uniquement
Default Switch
Réseau par défaut
Proxmox-Switch
Interne uniquement
Paramètres du réseau global
Plage d'adresses MAC
00-15-5D-53-0A-00 à 00-15-5D-53...
Créer un commutateur virtuel
Quel type de commutateur virtuel voulez-vous créer ?
Externe
Interne
Privé
Créer le commutateur virtuel
Crée un commutateur physique lié à la carte réseau physique de manière à ce que les ordinateurs virtuels puissent accéder à un réseau physique.

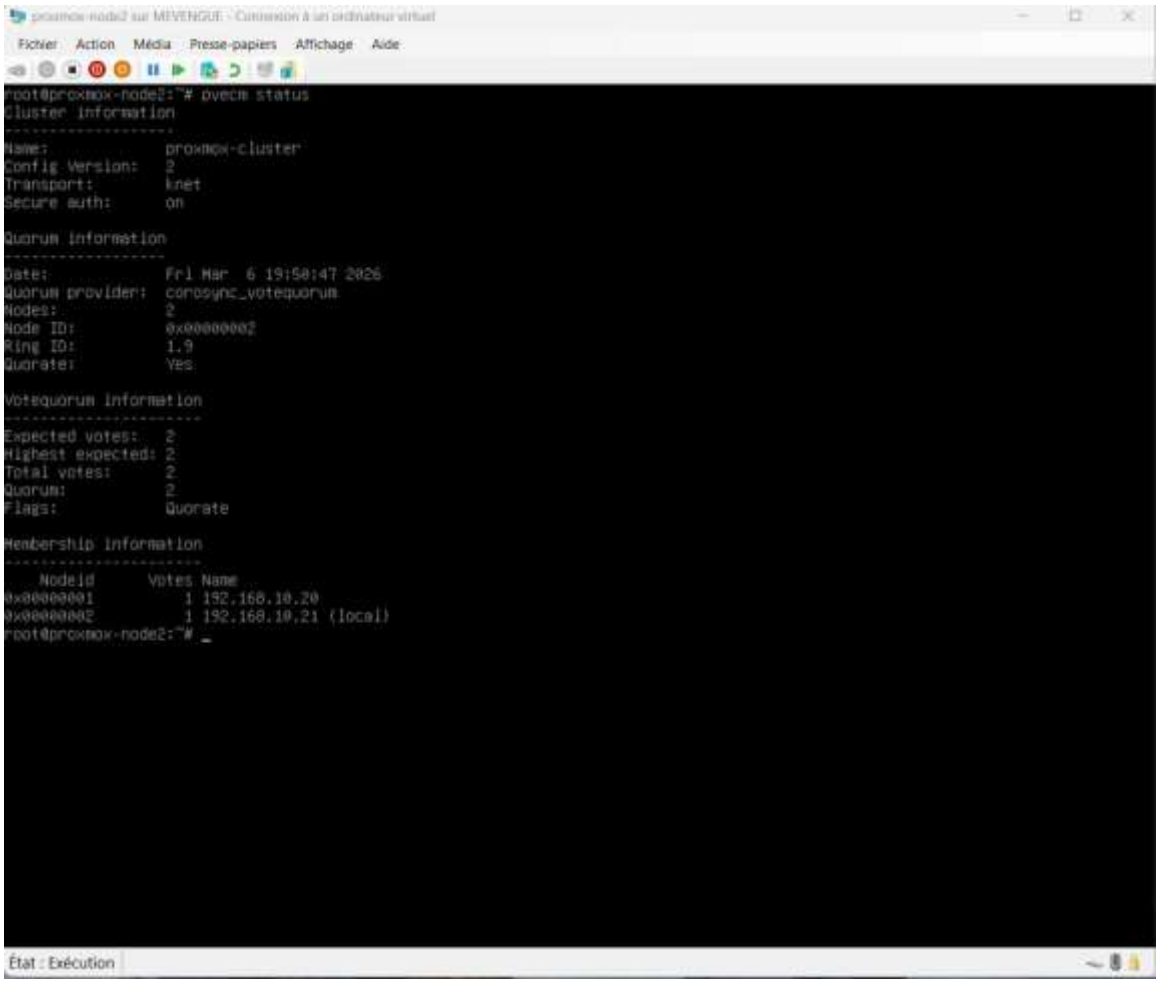

PROXMOX Virtual Environment 9.1.1



Étape 3 :

Création du **cluster Proxmox**.


proxmox-node2 sur MEVEN2UR - Connexion à un ordinateur virtuel
Fichier Action Média Presse-papiers Affichage Aide
<script type="text/javascript">
Proxmox = {
Setup: { auth_cookie_name: 'PVEAuthCookie' },
defaultLang: 'en',
NodeName: 'proxmox-node1',
UserName: '',
CSRFPreventionToken: 'null',
ConsentText: ''
};
</script>
<script type="text/javascript" src="/proxmoxlib.js?ver=v5.1.2-t1763394412"></script>
<script type="text/javascript" src="/pve2/js/pvemanagerlib.js?ver=9.1.1"></script>
<script type="text/javascript" src="/pve2/ext6/locale/locale-en.js?ver=7.0.0"></script>
<script type="text/javascript">
if (typeof(PVE) === 'undefined') PVE = {};
Ext.History.fieldid = 'x-history-field';
Ext.onReady(function() { Ext.create('PVE.StdWorkspace');});
</script>
</head>
<body>
<!-- Fields required for history management -->
<form id="history-form" class="x-hidden">
<input type="hidden" id="x-history-field"/>
</form>
</body>
</html>
root@proxmox-node2:~# pvecm add 192.168.10.20
Please enter superuser (root) password for '192.168.10.20': *********
Establishing API connection with host '192.168.10.20'
The authenticity of host '192.168.10.20' can't be established.
X509 SHA256 key fingerprint is 95:A0:C8:33:23:E3:31:55:C9:CB:6C:47:50:0E:74:4B:BE:E7:EA:AE:46:CF:5C:20:A4:D0:24:9E:56:EE:F0:10.
Are you sure you want to continue connecting (yes/no)? yes
Login succeeded.
check cluster join API version
No cluster network links passed explicitly, fallback to local node IP '192.168.10.21'
Request addition of this node
Join request OK, finishing setup locally
stopping pve-cluster service
backup old database to '/var/lib/pve-cluster/backup/config-1772622935.sql.gz'
waiting for quorum...OK
(re)generate node files
generate new node certificate
merge authorized SSH keys
generated new node certificate, restart pveproxy and pvedaemon services
successfully added node 'proxmox-node2' to cluster.
root@proxmox-node2:~#
État : Exécution



Étape 4

Configuration du stockage **ZFS** et de la réplication.

Étape 5

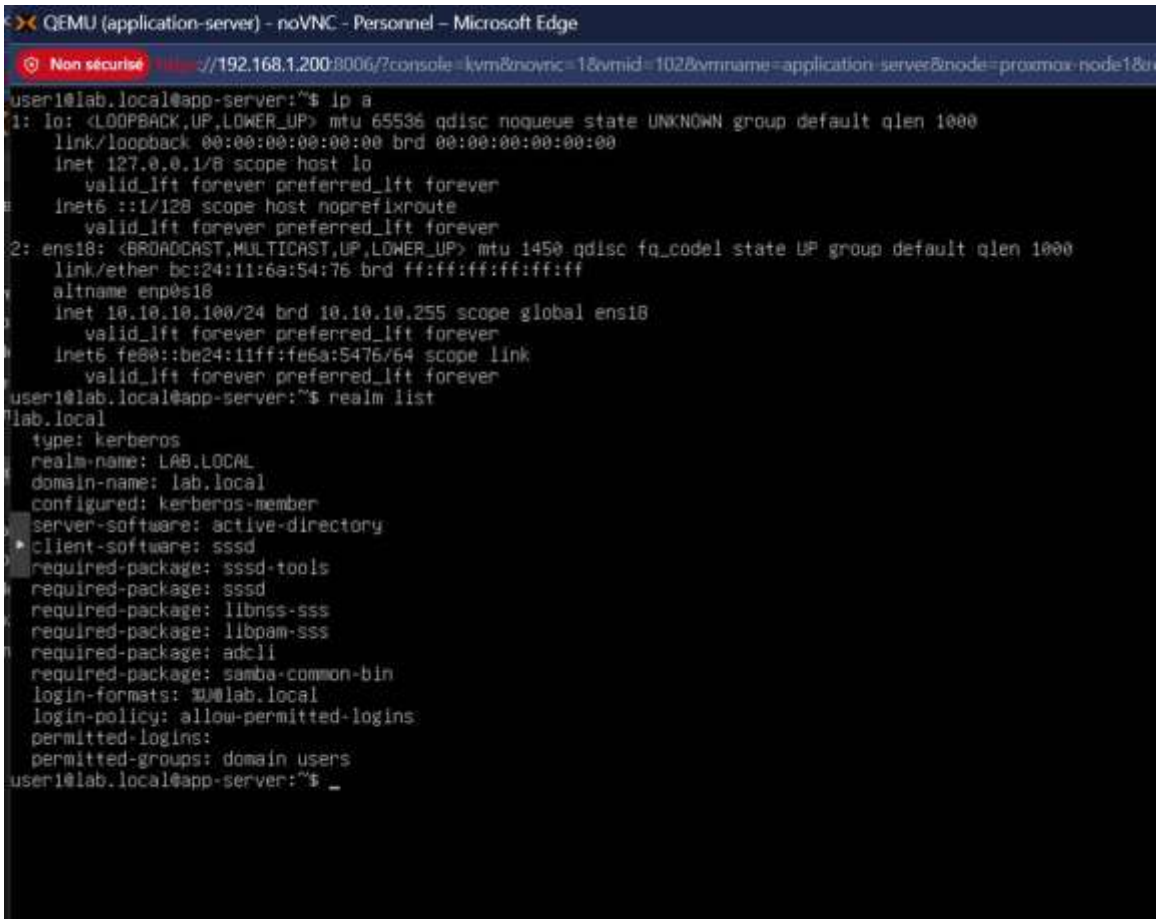
Déploiement des machines virtuelles :

- Infra Server
- Application Server
- Monitoring Server
- Admin Workstation

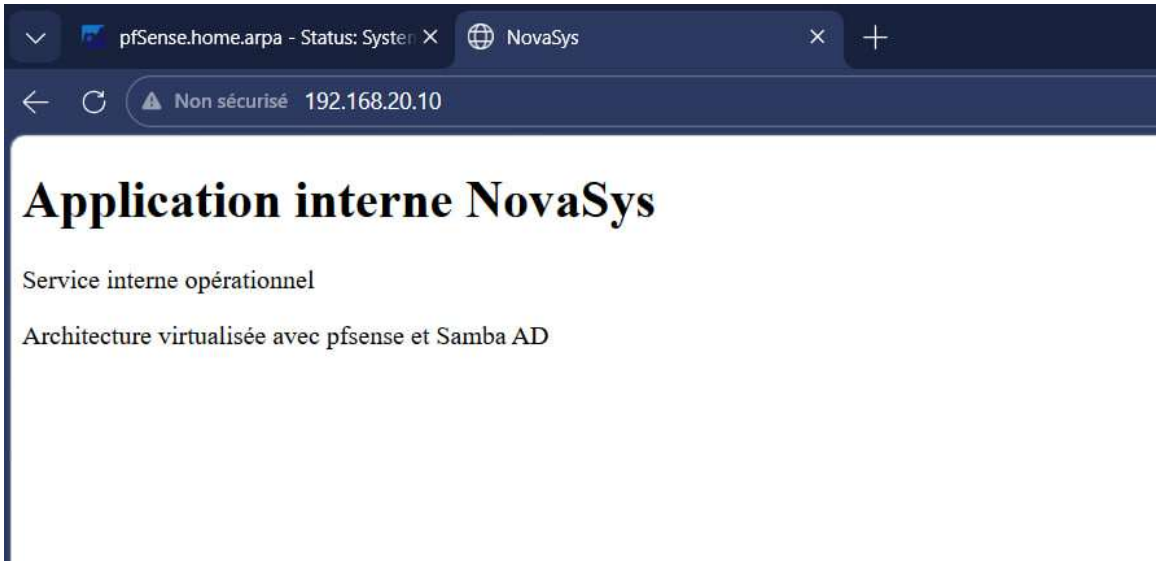
Étape 6

Installation des services :

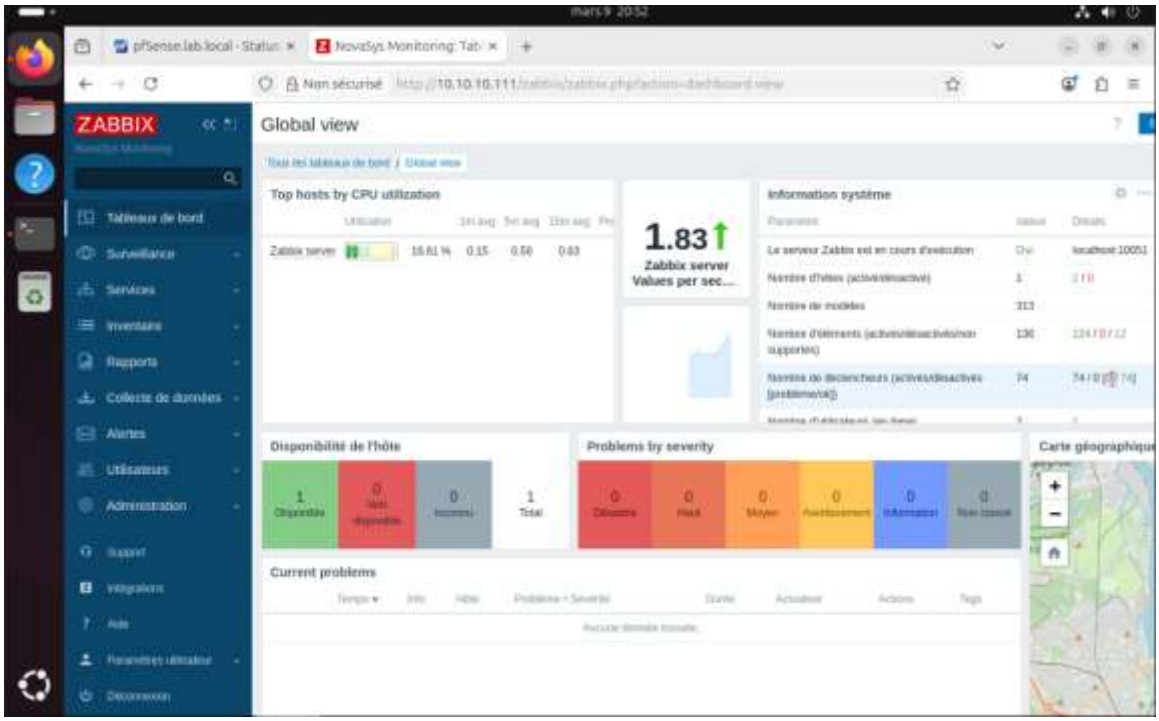
- Samba Active Directory



- Application interne



- Zabbix



Étape 7

Configuration sécurité :

- Firewall
- Fail2ban
- Gestion des accès

Utilisateur	Groupe	Accès
adminIT	ADMIN_IT	admin-workstation
dev1	DEVELOPERS	monitoring-server
user1	USERS	application-server

Étape 8

Tests :

- Test de réplication
- Test de redémarrage VM
- Test de basculement serveur

Conclusion :

La solution proposée permet à NovaSys de disposer d'une infrastructure moderne, sécurisée et résiliente. Grâce à : la virtualisation avec Proxmox, la réplication ZFS, la supervision, la segmentation réseau. Les services critiques de l'entreprise restent disponibles même en cas de panne d'un serveur.

Cette architecture offre également :

- Une meilleure administration
- Une évolutivité de l'infrastructure
- Une sécurité renforcée

Elle constitue une base solide pour l'évolution future du système d'information de l'entreprise.