***Projet Intégré :***

2025/2026



**Coachs :**

**Dakhli Imen**

**Werghemmi Radhia**

**Les membres du groupe :**

Khadija Bessais

Emna Jbari

Mariem Rezgui

Abdalah Grissa

Yassin Filali

Mohamed Yassin Wesslati

**Système & Réseau**

**Table des matières :**

1. **Introduction et contexte du projet ........................................ 3**

## Contexte du projet…………………………………………..3

## Objectifs du projet…………………………………………….3

## Problématique…………………………………………………..3

## Choix techniques………………………………………………….3

1. **Architecture globale ........................................................ 4**

## 2.1 Schéma global de l’architecture réseau………………………………….

## 2.2 Description des différentes zones réseau……………………………… 5

1. **Réalisation ................................................................. 12**
   1. Mise en place et configuration du Réseau………………..12
      1. Backbone……………………………………………………………12
      2. Département Monitoring ..................................................16

3.1.3 Département Base de Données …………………………..17

3.1.4 Département partage et collaboration……………………………………18

3.1.5 Département Web………………………………………….. 20

3.2 Mise en place et déploiement de tous les services……………………….25

3.2.1 Département Monitoring……………………………..25

3.2.2 Département Web…………………………..29

3.2.3 Département partage et collaboration……………………..31

3.2.4 Département Base de Données    ………………………………………….. 32

3.3 Description des services…………………………………32

3.3.1 Département partage et collaboration  …………………33

3.3.2 Département Web ………………………………..34

3.3.3 Département Monitoring …………………………………..34

3.3.4 Département Base de Données ……………………………..36

3.4 Intégration de la sécurité ……………………………………………………..37

1. **Analyse et résultats ....................................................... 41**

4.1 Validation fonctionnelle par des tests…………………………………..41

**5. Conclusion et perspectives ................................................ 54**

# 1. Introduction et contexte du projet

## **1.1 Contexte du projet**

Ce projet vise la conception et la mise en œuvre d’une **infrastructure système et réseau multi-départements,** représentant le fonctionnement d’une entreprise réelle. L’infrastructure doit permettre l’interconnexion de plusieurs départements disposant de services spécifiques, tout en assurant une communication fiable et performante.

## **1.2 Objectifs du projet**

Les objectifs principaux de ce projet sont :

* Mettre en place une architecture réseau structurée et évolutive
* Interconnecter plusieurs départements via un backbone central
* Déployer des services réseau adaptés à chaque département
* Garantir la disponibilité des services et l’accès à Internet

## **1.3 Problématique**

La problématique du projet est la suivante :  
**Comment concevoir une infrastructure réseau permettant de relier efficacement plusieurs départements tout en assurant la disponibilité des services et une gestion optimale du réseau ?**

## **1.4 Choix techniques**

Pour répondre à cette problématique, les choix techniques suivants ont été adoptés, conformément au cahier des charges :

* Architecture basée sur un backbone central
* Routage dynamique à l’aide du protocole OSPF
* Segmentation du réseau par sous-réseaux IPv4
* Déploiement de services dédiés (Web, Base de données, NFS, Monitoring)
* Accès Internet centralisé via NAT

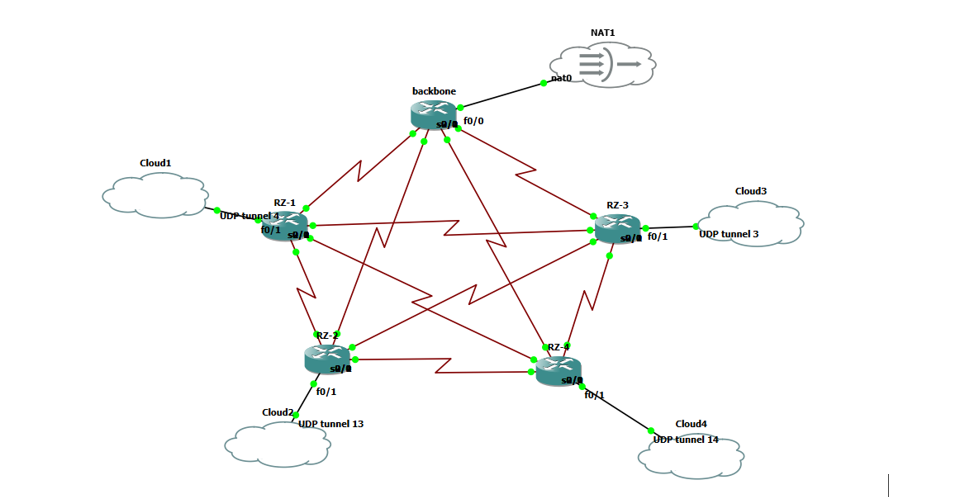
# 2. Architecture globale

## **2.1 Schéma global de l’architecture réseau**

L’architecture réseau mise en place repose sur un **backbone central** assurant l’interconnexion de l’ensemble des départements de l’entreprise. Le schéma présenté illustre la topologie du backbone, les liaisons entre les routeurs des différents départements, ainsi que la connexion vers Internet via un mécanisme NAT.

Ce schéma permet de visualiser la structure globale du réseau et le rôle central du backbone dans le routage et la communication inter-départements

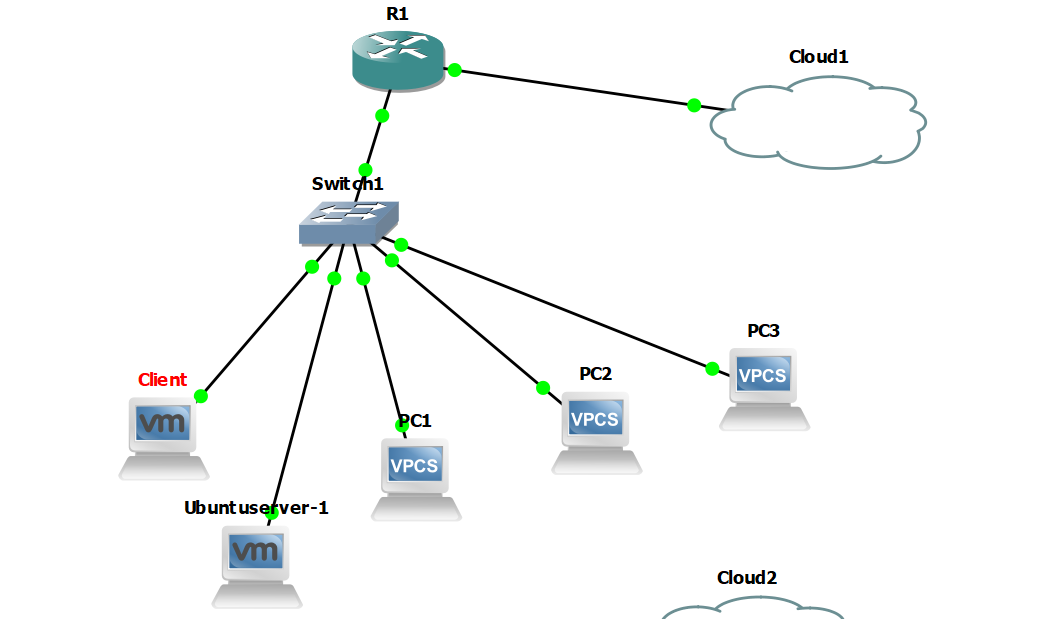
**Schéma global de l’architecture réseau – Backbone :**



* 4 routeurs représentant les 4 départements
* 1 routeur central Backbone
* 4 nœuds cloud reliés aux routeurs des départements (pour la communication)
* 1 NAT relié au backbone pour la connectivité à internet

## **2.2 Description des différentes zones réseau**

L’infrastructure réseau est divisée en plusieurs zones, chacune correspondant à un département fonctionnel spécifique. Cette segmentation permet une meilleure organisation du réseau, une gestion optimisée du trafic et une isolation logique des services.

* **Département Web** :
* 

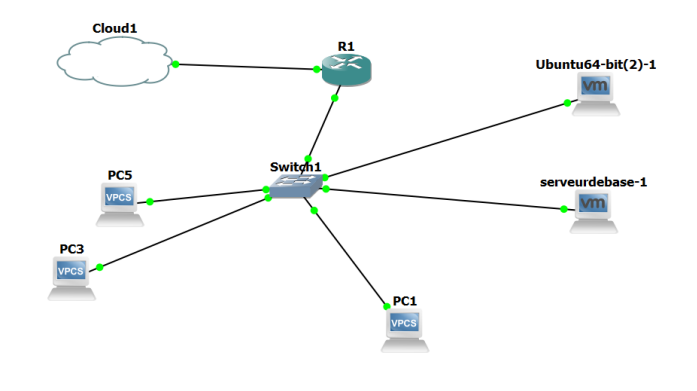
Mettre en place, dans **GNS3**, un **serveur Web Apache** accessible depuis un **client Ubuntu** au sein d’un même réseau local.

**2. Topologie du réseau**

**2.1 Équipements utilisés**

* Serveur Web (Ubuntu Server)
* Client (Ubuntu Desktop)
* Switch Ethernet (GNS3)
* Routeur Cisco
* **Département Base de Données :**

Le département Base de Données / Gestion est structuré autour d'une architecture client-serveur robuste



Un switch central assure l’interconnexion de tous les équipements du département.

Un routeur Cisco (R1) est connecté au switch et permet :

• La communication avec les autres départements (Web, Partage, Supervision) via le Backbone

. • Le routage dynamique des flux de données via le protocole OSPF.

**Équipements connectés :**

• serveur-db-1 : Serveur Ubuntu 64-bit hébergeant MySQL.

• PC1, PC2, PC3 : Postes utilisateurs (VPCS) pour les requêtes de gestion

. • Routeur R1 : Passerelle par défaut et point de sortie OSPF. 2.

**2.Équipements**

**Routeur**

• Modèle : Cisco 3745 (ou équivalent GNS3)

• Rôles : Routage inter-départements, Serveur DHCP pour les clients, OSPF Area0

**Serveur de Base de Données**

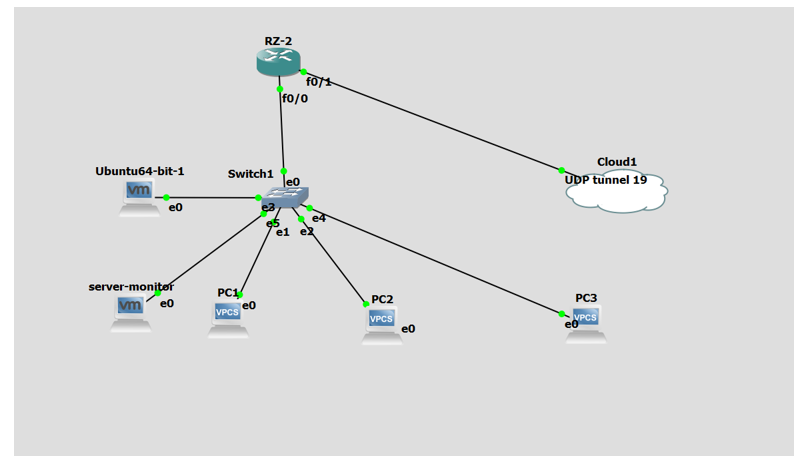
• Nom : serveur-db-1

• Système : Ubuntu Server

• Service : MySQL Server 8.0

• Rôle : Centralisation des données de l'entreprise et gestion des accès sécurisés

* **Département Monitoring :**

Le département **Monitoring** a pour objectif d’assurer la **supervision centralisée** de l’infrastructure réseau mise en place sous GNS3. 

* Un **switch central** assure l’interconnexion de tous les équipements du département.
* Un **routeur Cisco 3745 (RZ-2)** est connecté au switch et permet :
  + La communication avec les autres départements via le backbone.
  + L’accès au Cloud à travers un **tunnel UDP**.
* Les **clients** et le **serveur de supervision** sont directement connectés au switch.

Équipements connectés : - Server-monitor (serveur de monitoring) – Ubuntu64(VM client) - PC1, PC2, PC3 (postes utilisateurs – VPCS) - Routeur RZ-2 - Cloud (UDP tunnel )

## **2. Équipements**

Le département **Monitoring** est composé des équipements suivants :

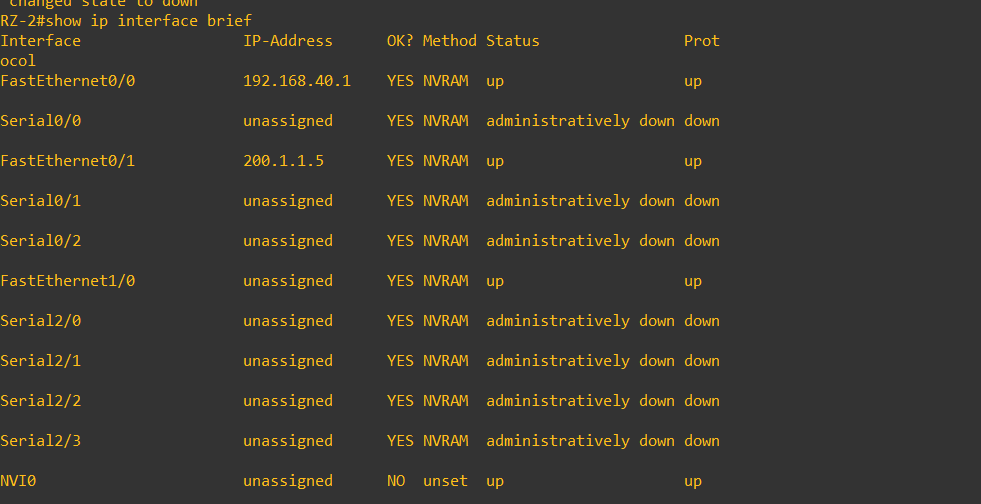
### **Routeur :**

Le routeur Cisco assure la **connectivité réseau** entre le département Monitoring et le backbone.

* Modèle : **Cisco 3745**
* Rôle :
  + Routage entre le réseau Monitoring et les autres département
  + Distribution automatique des adresses IP via **DHCP**
  + Accès aux services de monitoring

***Fonctions principales :***

* Protocole de routage : **OSPF**
* Service DHCP pour les hôtes du réseau Monitoring
* Interface entre le backbone et le réseau local



### **Server :**

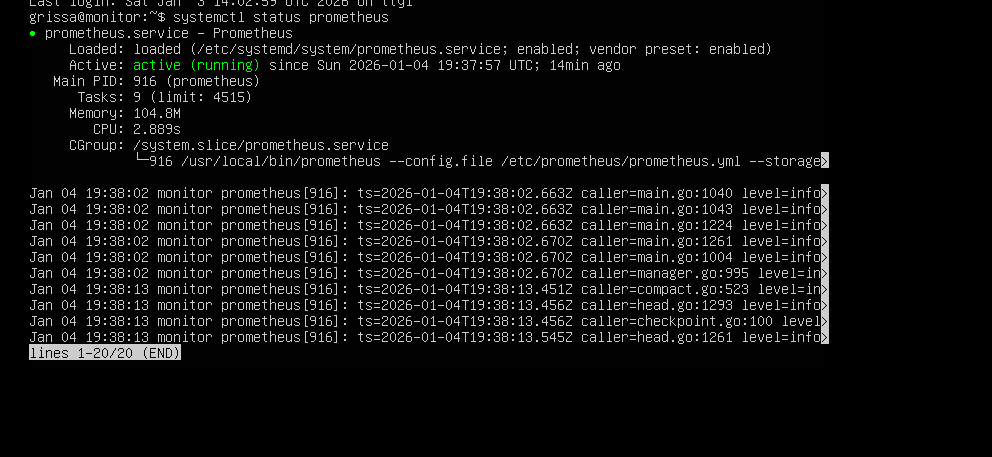
Le serveur de monitoring est une machine Linux (Ubuntu Server ou Ubuntu Desktop) dédiée à la **collecte et à la visualisation des métriques**.

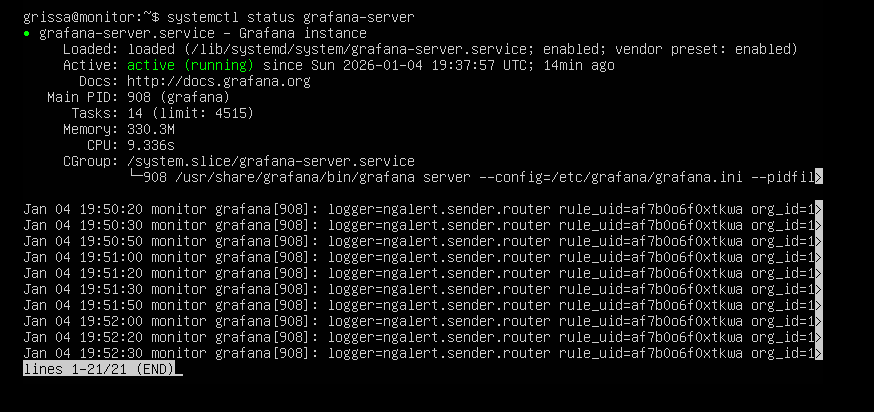
Nom : **server-monitor**

* Rôle :
  + Centralisation des données de monitoring
  + Supervision des serveurs et des routeurs
  + Accès aux tableaux de bord de monitoring

**Services installés :**

* **Prometheus** : collecte des métriques
* **Grafana** : visualisation des métriques
* **Node Exporter** : collecte des métriques locales





**Serveurs supervisés (VMs):**

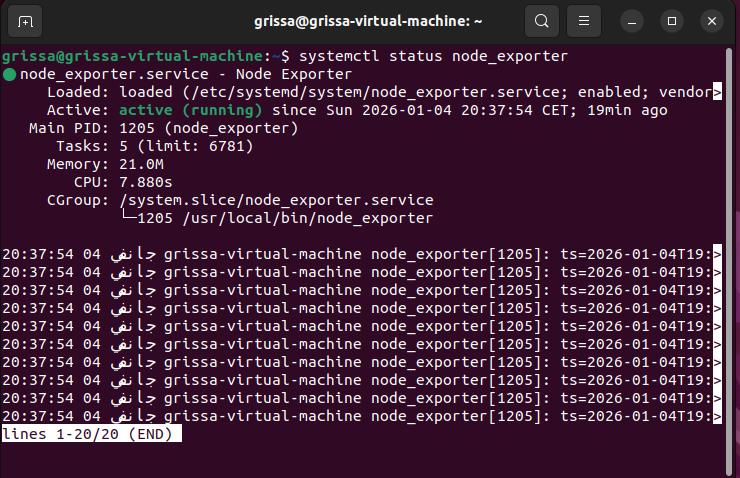
Les serveurs Linux des différents départements (Web, DB, NFS, Clients) sont supervisés par le système de monitoring.

**Rôles des serveurs :**

* Hébergement des services applicatifs
* Fourniture de données à superviser

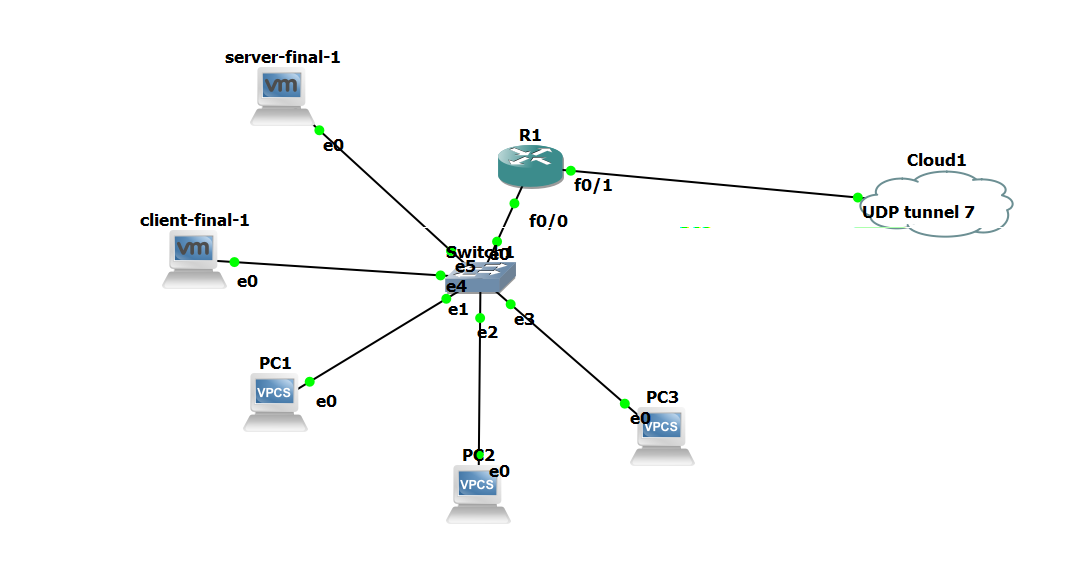
**Configuration de monitoring :**

* **Node Exporter installé**
* Exposition des métriques sur le port **9100**
* Communication avec le serveur de monitoring via le backbone



**Département partage et collaboration :**

Le département **Partage / Collaboration** est basé sur une topologie en étoile.



* Un **switch central** assure l’interconnexion de tous les équipements du département.
* Un **routeur Cisco 3745 (RZ-4)** est connecté au switch et permet :
  + La communication avec les autres départements via le backbone.
  + L’accès au Cloud à travers un **tunnel UDP**.
* Les **clients** et le **serveur de partage** sont directement connectés au switch.

Équipements connectés : - Server-final-1 (serveur de partage) - Client-final-1(VM client) - PC1, PC2, PC3 (postes utilisateurs – VPCS) - Routeur R1 - Cloud (UDP tunnel 7)

## **2. Équipements :**

### **Routeur :**

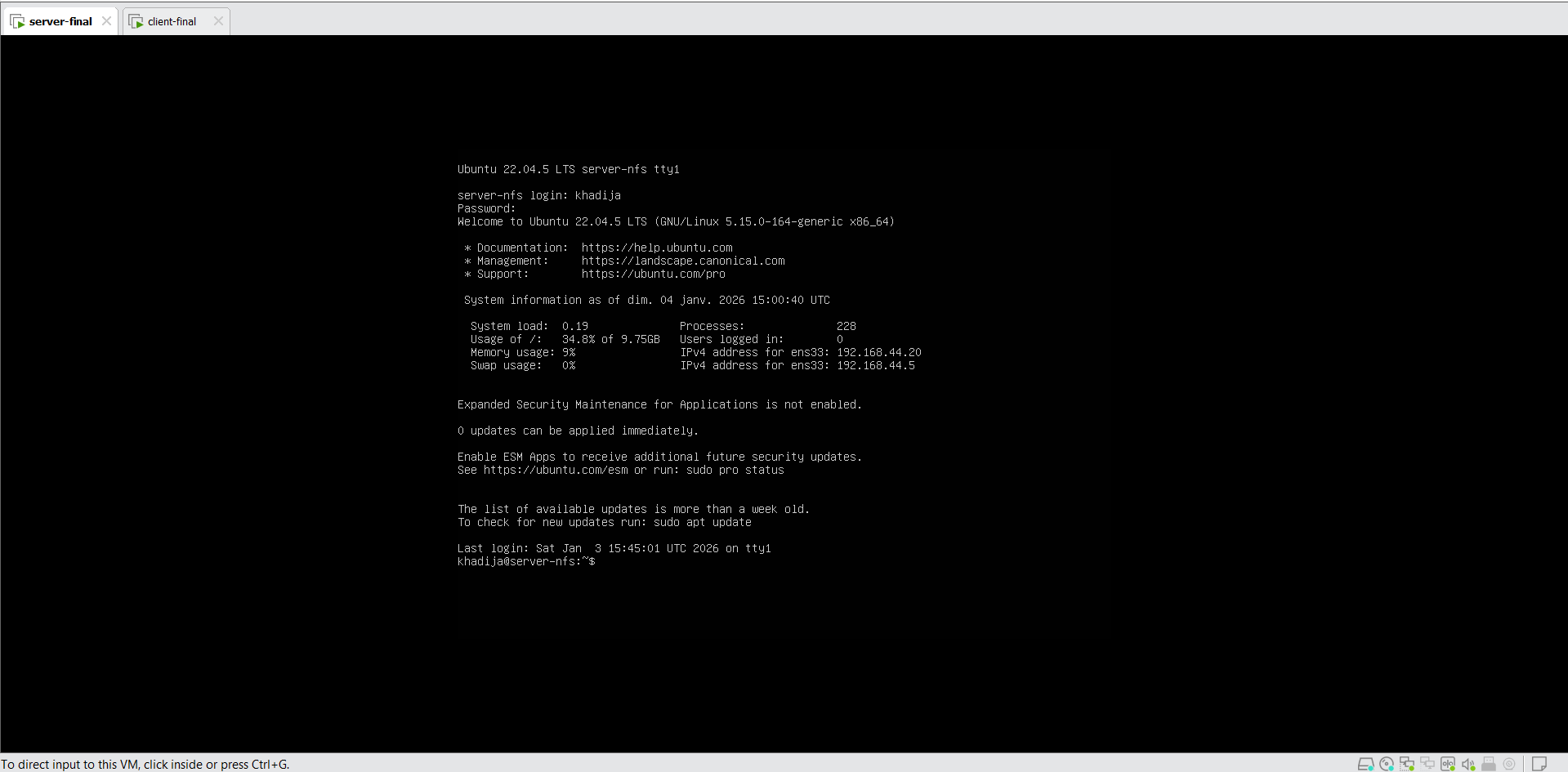
* Modèle : **Cisco 3745**
* Rôle :
  + Routage inter-départements
  + NAT
  + OSPF
  + Terminaison du tunnel UDP vers le Cloud

### **Switch :**

* Type : Switch Ethernet
* Rôle :
  + Interconnexion locale des clients et du serveur

### **Server :**

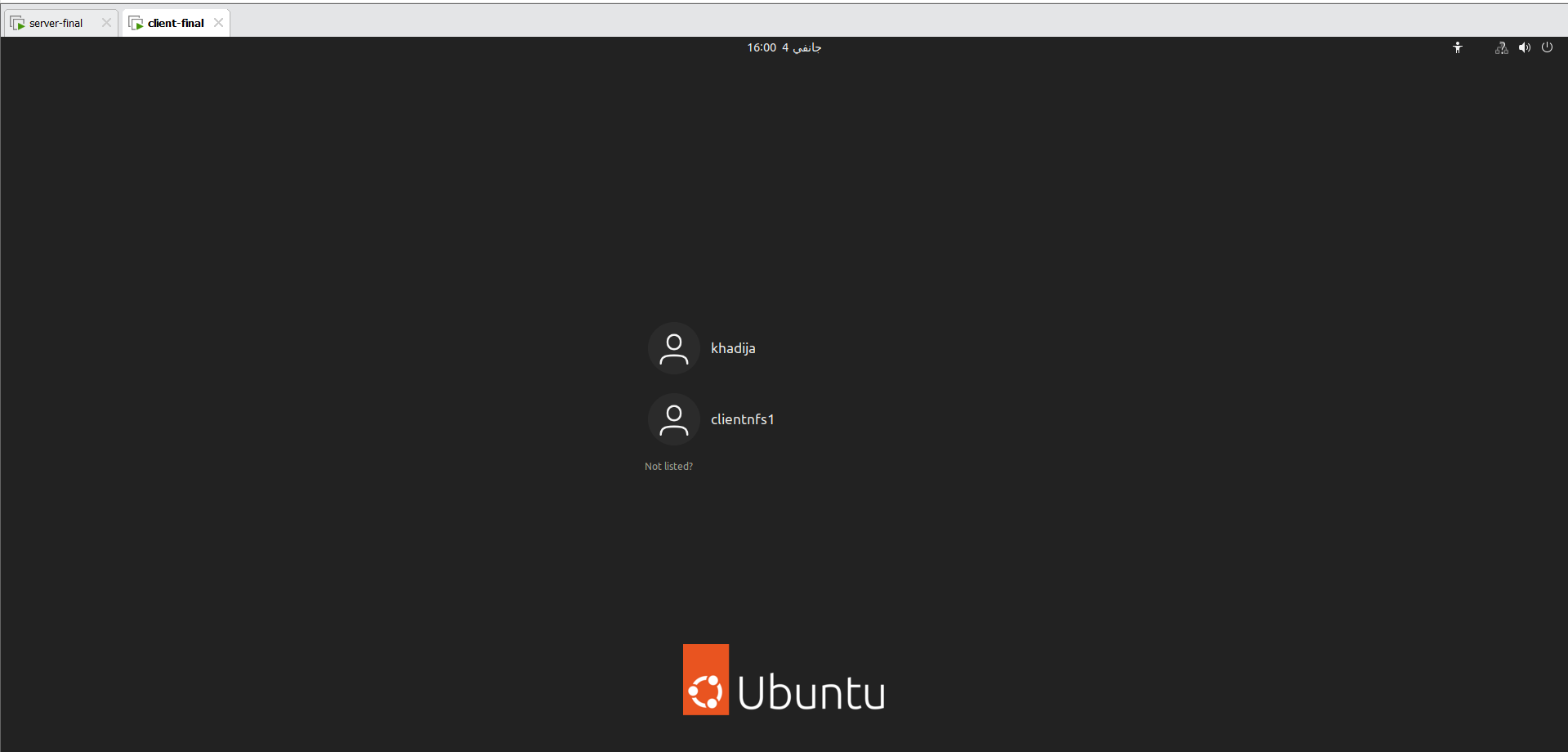
* Nom : server-final-1



* **Rôle :**
  + Hébergement des ressources partagées (ex : NFS / fichiers)

### **Clients :**

* client-final-1



* PC1, PC2, PC3 (VPCS)
* Rôle :
  + Accès aux services de partage et au réseau de l’entreprise
  + Accès au service Web
  + Accès à la base de données
  + Supervisés par le service de monitoring

**3. Réalisation**

**3.1 Mise en place et configuration du Réseau :**

**3.1.1 Backbone :**

Plan D’adressage :

Backbone :

|  |  |  |  |
| --- | --- | --- | --- |
| Interface | Connecté vers | Adresse | Sous Reseau |
| Serial 0/0 | RZ-1 | 200.10.0.2 | 200.10.0.0 /30 |
| Serial 0/1 | RZ-2 | 200.10.0.10 | 200.10.0.8 /30 |
| Serial 0/2 | RZ-3 | 200.10.0.6 | 200.10.0.4 /30 |
| Serial 2/0 | RZ-4 | 200.10.0.14 | 200.10.0.12/30 |
| FastEthernet0/0 | NAT | Adresse dynamique |  |

* RZ-1 : (Web)

|  |  |  |  |
| --- | --- | --- | --- |
| Interface | Connecté vers | Adresse | Sous Reseau |
| Serial 0/0 | Backbone | 200.10.0.1 | 200.10.0.0 /30 |
| Serial 0/1 | RZ-2 | 200.10.0.25 | 200.10.0.24 /30 |
| Serial 0/2 | RZ-3 | 200.10.0.29 | 200.10.0.28 /30 |
| Serial 2/0 | RZ-4 | 200.10.0.33 | 200.10.0.32/30 |
| FastEthernet0/1 | Cloud | 200.1.1.9 | 200.1.1.8 /30 |

* RZ-2 : (Monitoring)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Interface | Connecté vers | Adresse | Sous Reseau |  |
| Serial 0/0 | Backbone | 200.10.0.9 | 200.10.0.8 /30 |  |
| Serial 0/1 | RZ-1 | 200.10.0.26 | 200.10.0.24 /30 |  |
| Serial 0/2 | RZ-4 | 200.10.0.41 | 200.10.0.40 /30 |  |
| Serial 2/0 | RZ-3 | 200.10.0.37 | 200.10.0.36/30 |  |
| FastEthernet0/1 | Cloud | 200.1.1.6 | 200.1.1.4 /30 |  |

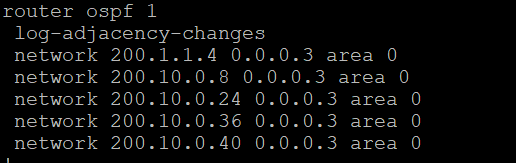
* RZ-3 : (Base de données)

|  |  |  |  |
| --- | --- | --- | --- |
| Interface | Connecté vers | Adresse | Sous Reseau |
| Serial 0/0 | Backbone | 200.10.0.5 | 200.10.0.4 /30 |
| Serial 0/1 | RZ-4 | 200.10.0.45 | 200.10.0.44 /30 |
| Serial 0/2 | RZ-1 | 200.10.0.30 | 200.10.0.28/30 |
| Serial 2/0 | RZ-2 | 200.10.0.38 | 200.10.0.36/30 |
| FastEthernet0/1 | Cloud | 200.1.1.13 | 200.1.1.12 /30 |

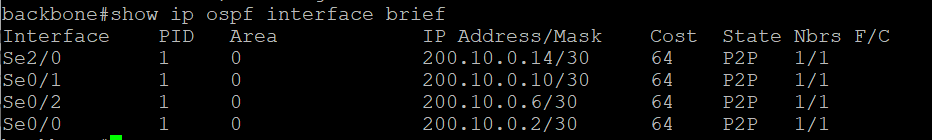
* RZ-4 : (NFS)

|  |  |  |  |
| --- | --- | --- | --- |
| Interface | Connecté vers | Adresse | Sous Reseau |
| Serial 0/0 | Backbone | 200.10.0.13 | 200.10.0.12 /30 |
| Serial 0/1 | RZ-3 | 200.10.0.46 | 200.10.0.44 /30 |
| Serial 0/2 | RZ-2 | 200.10.0.42 | 200.10.0.40 /30 |
| Serial 2/0 | RZ-1 | 200.10.0.34 | 200.10.0.32/30 |
| FastEthernet0/1 | Cloud | 200.1.1.1 | 200.1.1.0 /30 |

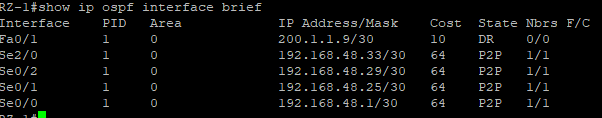
**Confguration OSPF (exemple pour RZ-4) :**



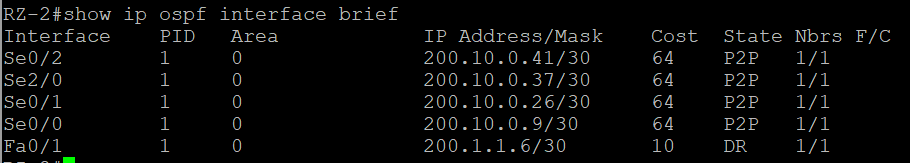
* Backbone :



* RZ-1 :



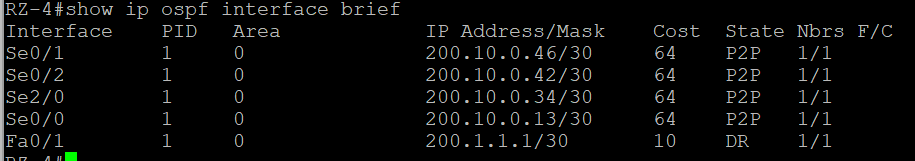
* RZ-2 :



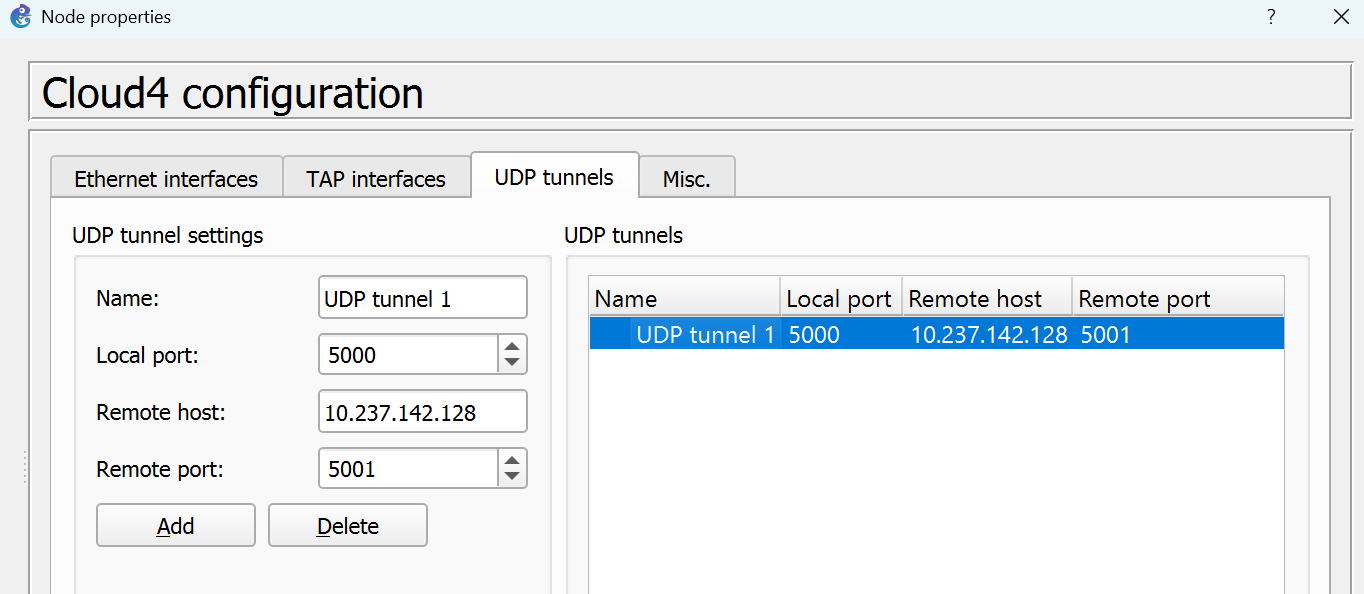
* RZ-3 :



* RZ-4 :

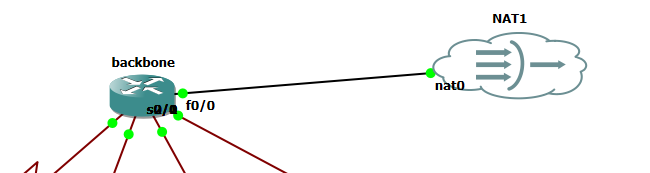


**Configuration Tunnel:**

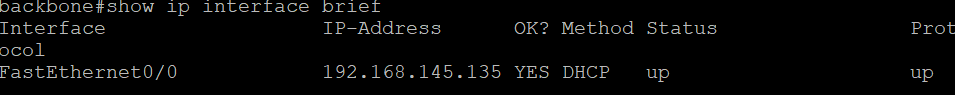


**Configuration Cloud NAT :**

Ajout d’un cloud NAT :



Donner une adresse dynamique à l’interface liée au NAT :



Configurer une default route via default gateway(192.168.145.2) :



Configurer le routeur backbone comme un routeur par defaut pour les autres routeurs



**3.1.2 Département Monitoring :**

## **Plan d’adressage**

Le département Monitoring utilise le plan d’adressage suivant :

* Réseau : **192.168.40.0/22**
* Masque : **255.255.252.0**
* Plage d’adresses utilisables : **192.168.40.1** → **192.168.43.254**

**Affectation des adresses :**

* Routeur : **192.168.40.1**

Client: **192.168.40.10**

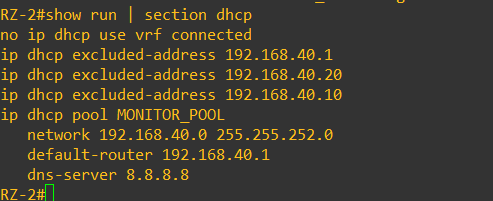
Serveur de monitoring : **192.168.40.20**

**Configuration DHCP**

Le routeur Cisco assure le rôle de **serveur DHCP** pour le réseau Monitoring.

Le service DHCP permet de distribuer automatiquement :

* Adresse IP
* Masque de sous-réseau
* Passerelle par défaut
* Serveur DNS

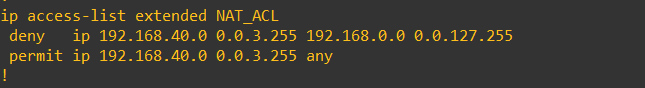


## **5. Configuration des listes de contrôle d’accès (ACL)**

Les **ACL (Access Control Lists)** sont utilisées pour **contrôler et sécuriser le trafic réseau** entre les différents départements.

Les ACL permettent :

* D’autoriser uniquement les services nécessaires
* De bloquer le trafic non autorisé
* De sécuriser les serveurs sensibles (DB, NFS)

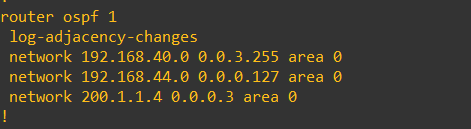


## **6. Configuration OSPF**

Le protocole **OSPF (Open Shortest Path First)** est utilisé pour assurer le **routage dynamique** entre les différents routeurs de l’infrastructure.

OSPF permet :

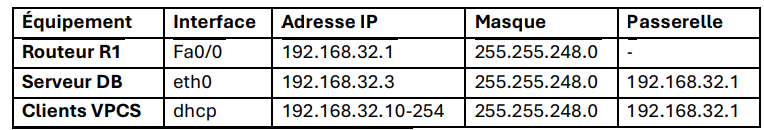
* L’échange automatique des routes
* Une meilleure évolutivité du réseau
* Une convergence rapide en cas de panne



**3.1.3 Département Base de Données :**

**Plan d’adressage :**

Le réseau utilise la plage 192.168.32.0/21, permettant d'accueillir jusqu'à 2046 hôtes.



**3.1.4 Département partage et collaboration :**

## . **Plan d’adressage :**

Réseau du département Partage / Collaboration :

* Réseau: **192.168.44.0/25**
* Masque : **255.255.255.128**
* Plage d’adresses utilisables : **192.168.44.1** → **192.168.44.126**

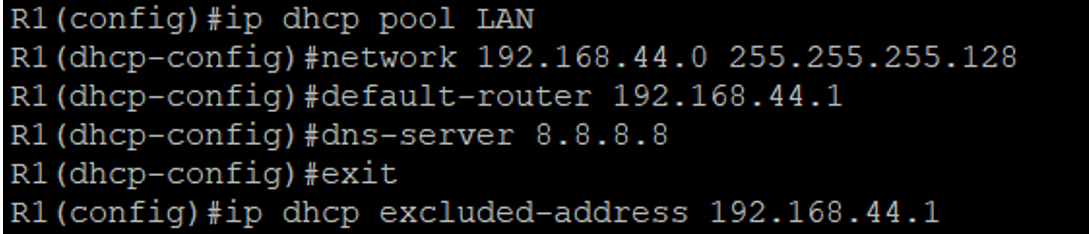
Affectation : - Routeur R1 (interface LAN) : **192.168.44.1** - Serveur de partage : **192.168.44.10** - Client-final-1(VM client) **192.168.40.20**- Clients : **via DHCP**

## **Configuration DHCP :**

Le routeur R1 joue le rôle de serveur DHCP pour le département.

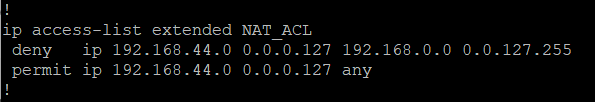
Objectifs : - Attribution automatique des adresses IP aux clients - Configuration automatique de la passerelle et du DNS

Paramètres DHCP : - Network : 192.168.44.0/25 - Default gateway : 192.168.44.1 - DNS : 8.8.8.8 - Exclusion : adresses statiques (routeur, serveur)



## **Configuration des listes de contrôle d’accès (ACL) :**

Une **liste de contrôle d’accès (ACL)** a été mise en place sur le routeur **R1** afin de contrôler le trafic réseau du département **Partage / Collaboration**.



**Objectifs de l’ACL**

* Autoriser le trafic nécessaire au bon fonctionnement du réseau
* Contrôler les communications entrantes et sortantes
* Renforcer la sécurité du département

**Principe de fonctionnement**

L’ACL est appliquée sur l’interface appropriée du routeur R1 et permet :

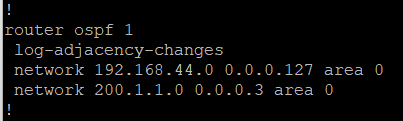
* Le passage des protocoles autorisés (ex : ICMP, OSPF, UDP selon le besoin)
* Le filtrage du trafic non souhaité
* Le maintien de la connectivité entre les départements autorisés

## **Configuration OSPF :**

Le protocole **OSPF** est utilisé pour le routage dynamique entre les départements.

Objectifs : - Échange automatique des routes - Adaptation dynamique en cas de changement de topologie

Paramètres : - Process ID : 1 - Area : 0 - Annonce du réseau 192.168.44.0/25

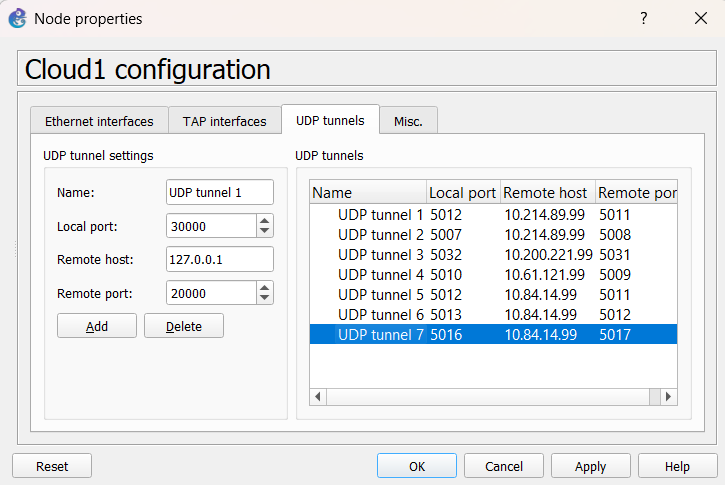


## **Configuration Cloud / Tunnel UDP :**

Un **tunnel UDP** est configuré entre le routeur R1 et le Cloud.

Rôle du tunnel : - Simuler une liaison WAN - Assurer la connectivité avec des réseaux distants

Caractéristiques : - Cloud : Cloud1 - Tunnel : UDP tunnel 7



**3.1.4 Département Web**

**CONFIGURATION DU ROUTEUR RZ-1**

**A screenshot of a computer error

AI-generated content may be incorrect.**

**Configuration DHCP pour les PCs clients**

1. *# Créer le pool DHCP*

A screen shot of a computer

AI-generated content may be incorrect.

1. *# Exclure les adresses statiques (serveurs)*

A screen shot of a computer

AI-generated content may be incorrect.

1. *# Sauvegarder la configuration*

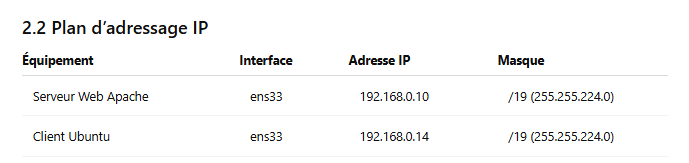
**A screen shot of a computer

AI-generated content may be incorrect.**

A screenshot of a computer

AI-generated content may be incorrect.

**Plan d’adressage IP**



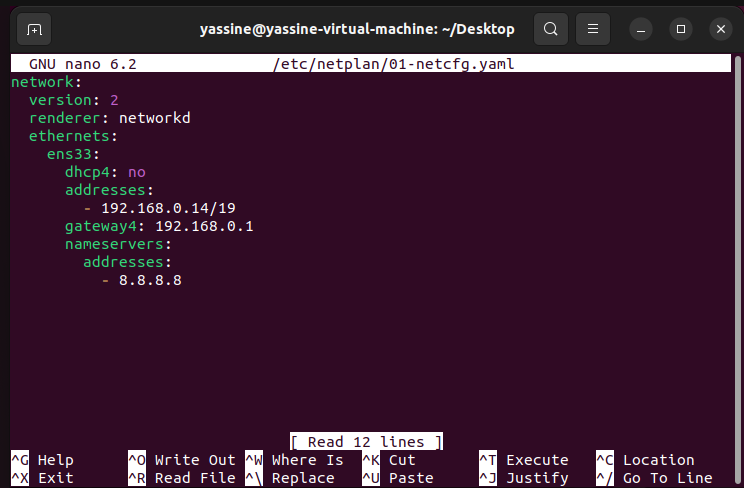
**Configuration réseau**

**3.1 Configuration du serveur Web (192.168.0.10)**

Fichier Netplan



**3.2 Configuration du client Ubuntu (192.168.0.14)**



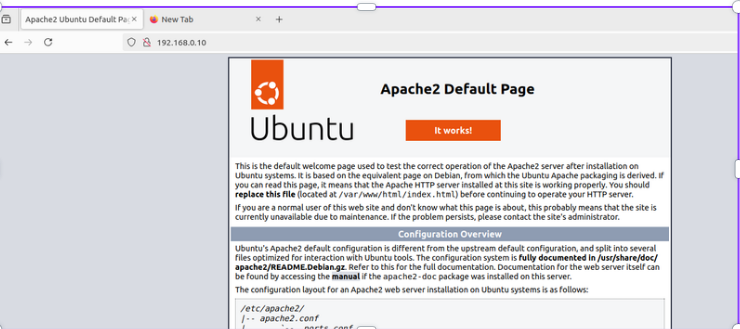
**4. Installation et configuration d’Apache**

4.1 Installation d’Apache : sudo apt install apache2 -y

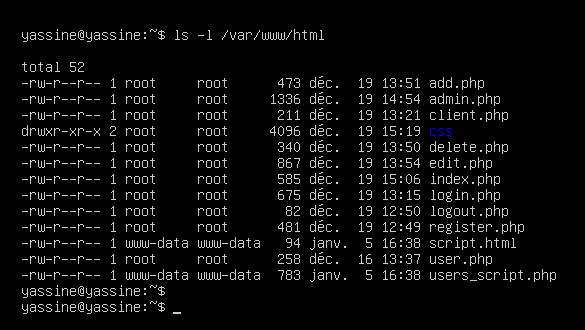
4.2 Vérification du service Apache : sudo systemctl status apache2

4.3 Démarrage automatique : sudo systemctl enable apache2

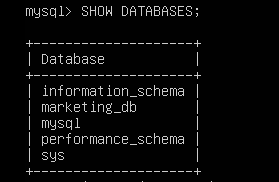
4.4 Page Web de test :



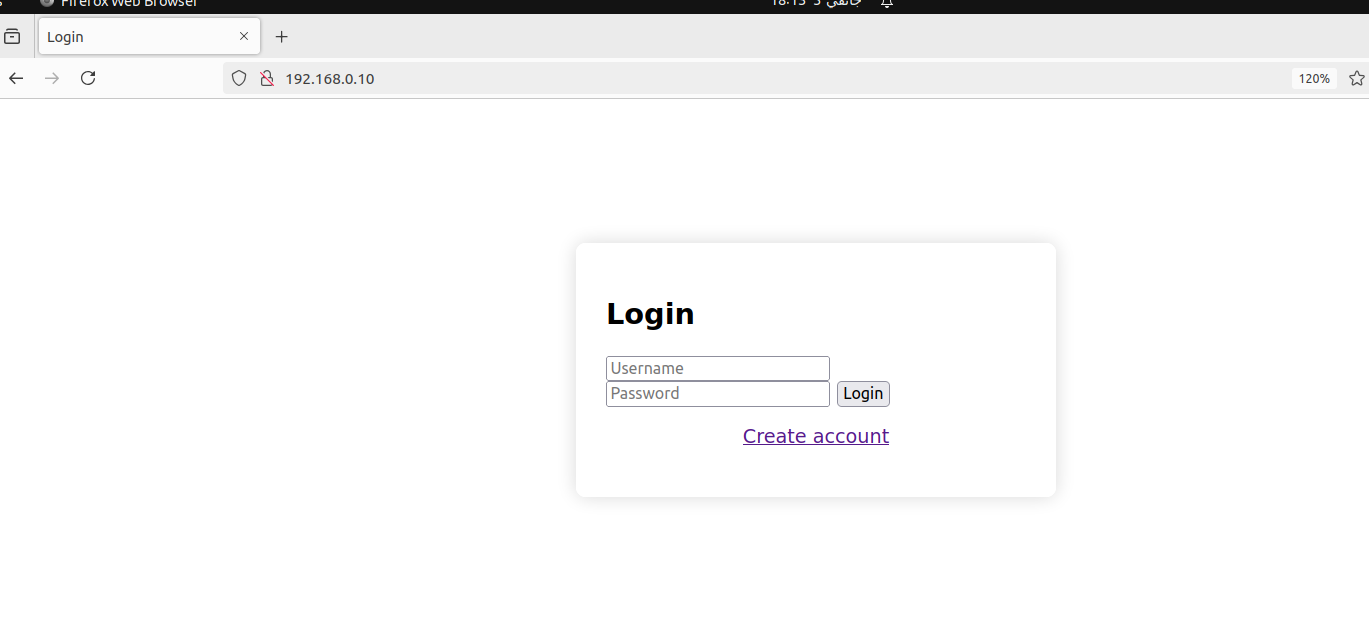
4.5 Creation site web on Ubunto Server :



**Creation Databases ( marketing\_db )** :



**Test le site web partie Client :**



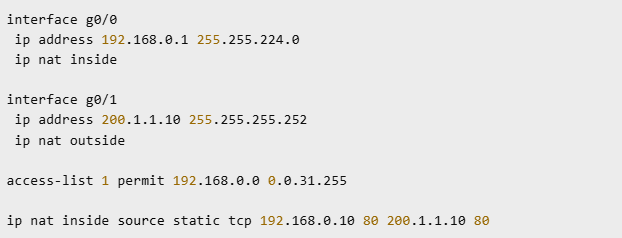
**5 . Configuration NAT et accès externe**

**Principe du NAT**

**Le routeur joue le rôle de passerelle entre le réseau interne (LAN) et le réseau backbone (WAN).**

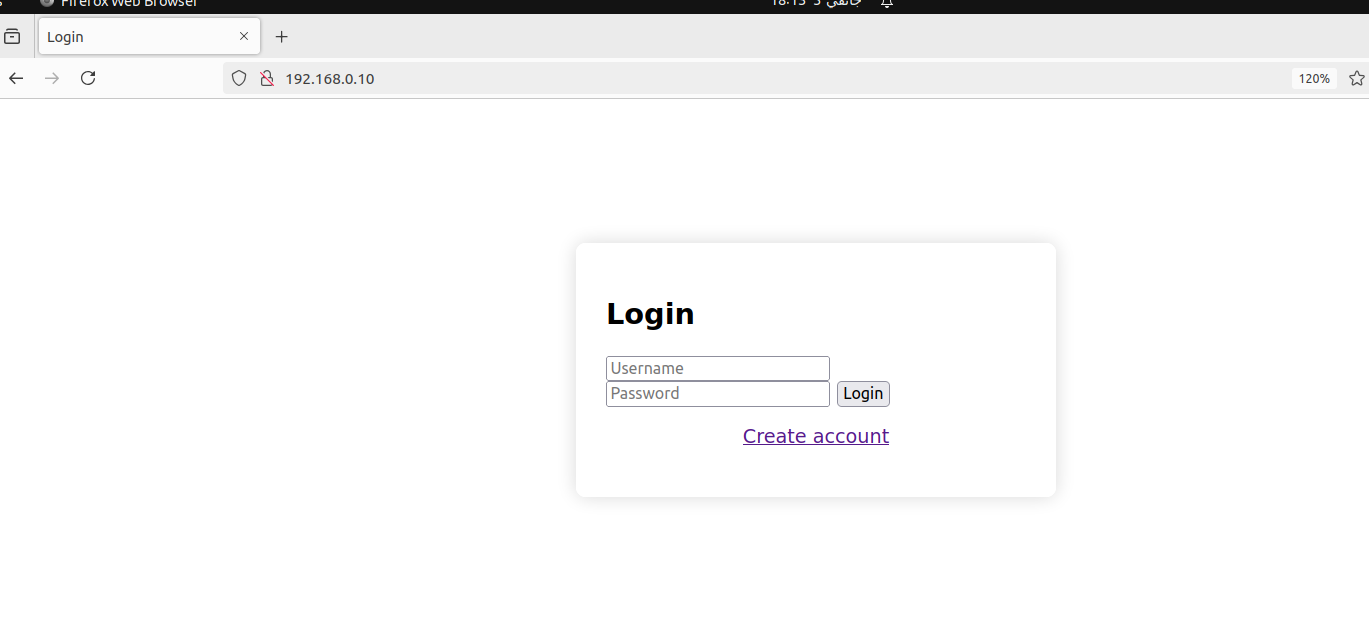
* **Adresse privée du serveur Web : 192.168.0.10**
* **Adresse publique NAT : 200.1.1.10**

6 . Exemple de configuration NAT:

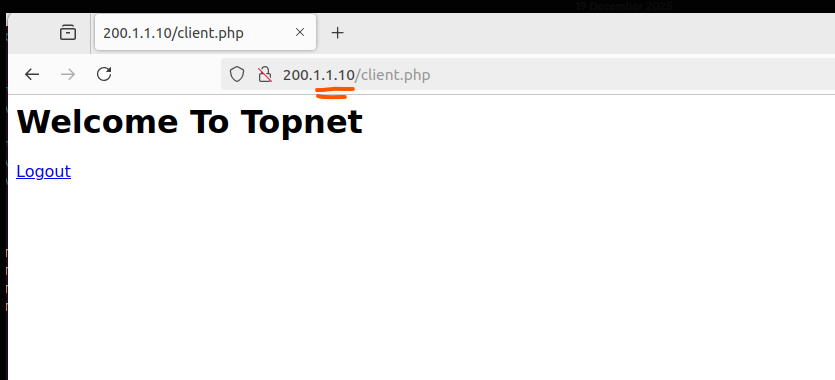


**7 . Tests de validation**

**Depuis le LAN : ( Accès local ) : 192.168.0.10**



**Accès externe via 200.1.1.10**

****

**3.2 Mise en place et déploiement de tous les services :**

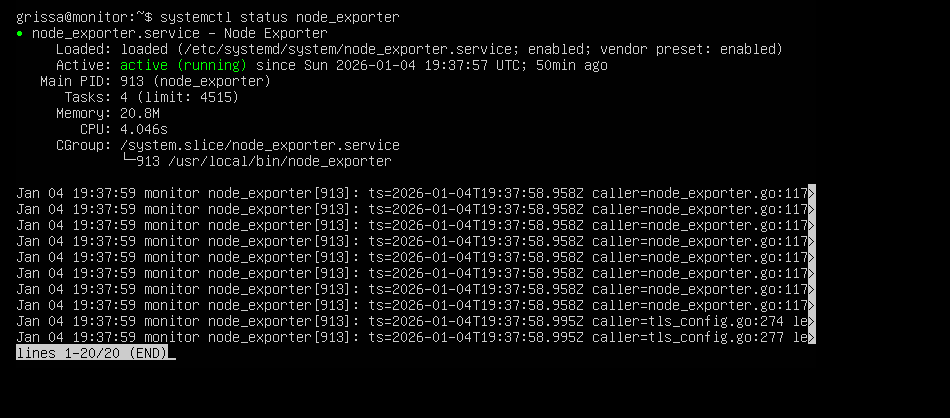
**3.2.1 Département Monitoring :**

**Monitoring des serveurs Linux :**

**Node Exporter :**

Node Exporter est installé sur chaque serveur Linux afin de collecter les métriques système.

* Port utilisé : 9100
* Démarrage automatique via system



**Métriques collectée :**

Les métriques collectées incluent :

* Utilisation CPU
* Mémoire RAM
* Espace disque

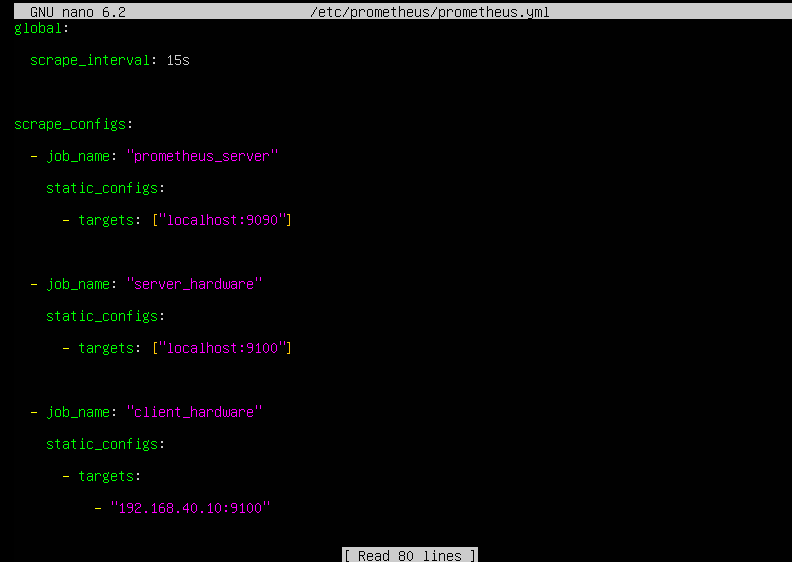


**Configuration de Prometheus :**

Prometheus est configuré pour collecter les métriques depuis :

**Node Exporter** (serveurs Linux)

Les équipements sont définis comme cibles dans le fichier prometheus.yml.

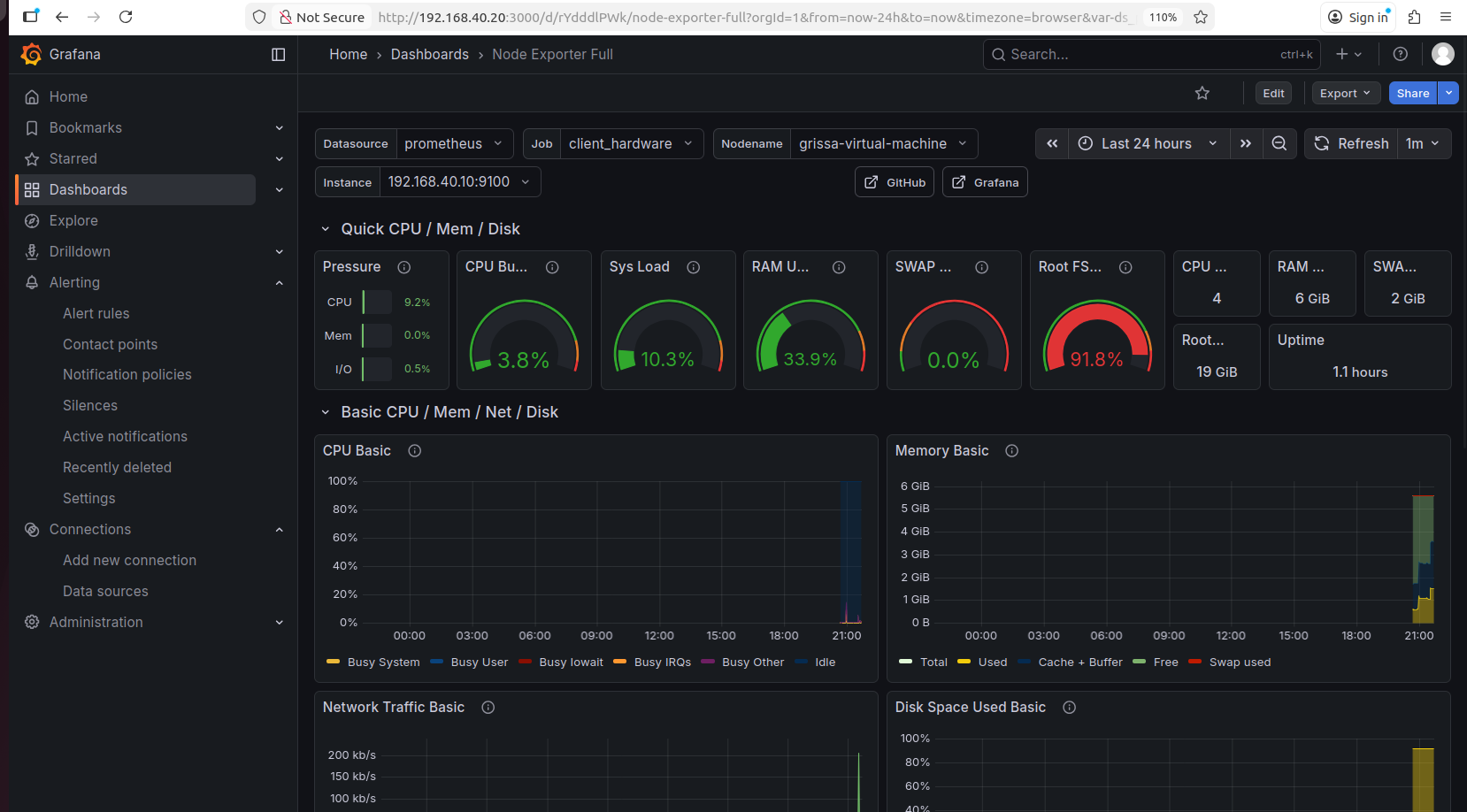


## **Visualisation avec Grafana :**

Grafana permet la visualisation des métriques collectées par Prometheus sous forme de tableaux de bord interactifs.

Les dashboards affichent :

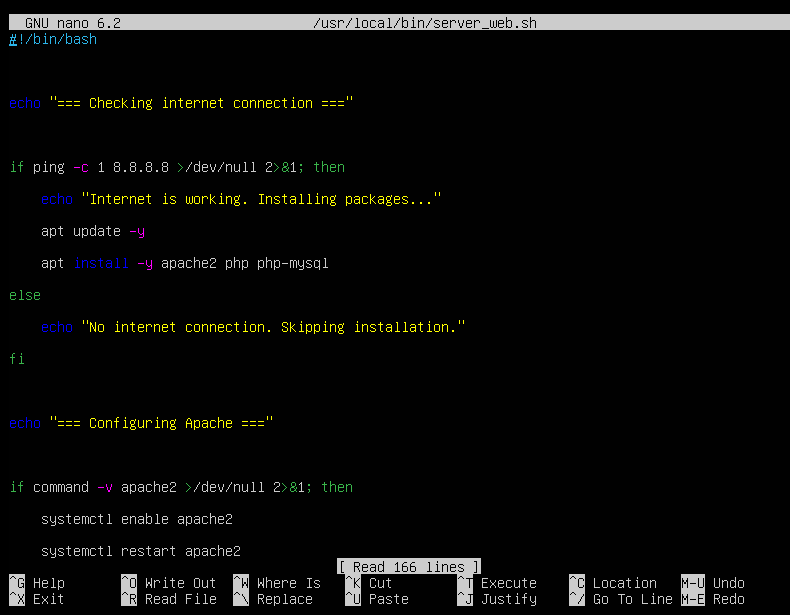
* + Les performances des serveurs
  + L’état des routeurs
  + Le trafic réseau



**3.2.2 Département Web :**

**Creation script :**

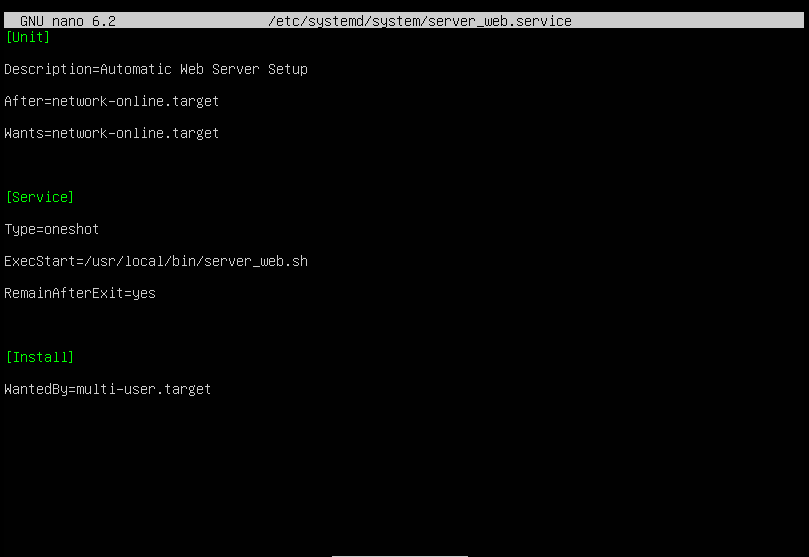
**sudo nano /usr/local/bin/server\_web.sh**

****

**sudo chmod +x /usr/local/bin/server\_web.sh**

Script exécuté automatiquement :

**sudo nano /etc/systemd/system/server\_web.service**

****

**Activation du service**

sudo systemctl daemon-reexec

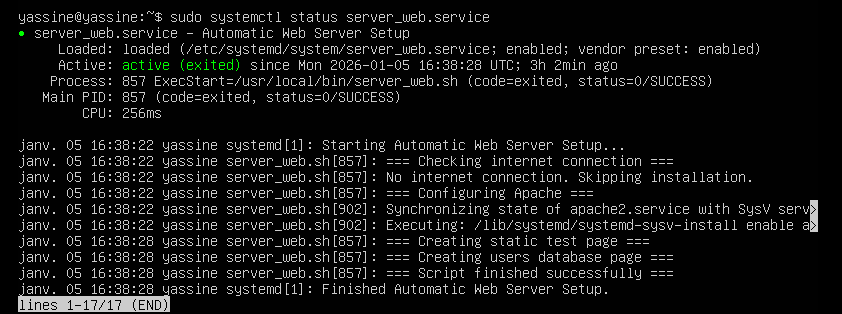
sudo systemctl daemon-reload

sudo systemctl enable server\_web.service

sudo systemctl start server\_web.service

**Vérification du service**

**sudo systemctl status server\_web.service**

****

**3.2.3 Département partage et collaboration :**

## **Configuration du service NFS (Partage de fichiers)**

Le service **NFS (Network File System)** a été mis en place afin de permettre le **partage de fichiers** entre le serveur et les clients du département **Partage / Collaboration**.

**Configuration du serveur NFS**

Le serveur **server-final-1** est configuré comme serveur NFS.

Actions réalisées :

* Installation du service NFS



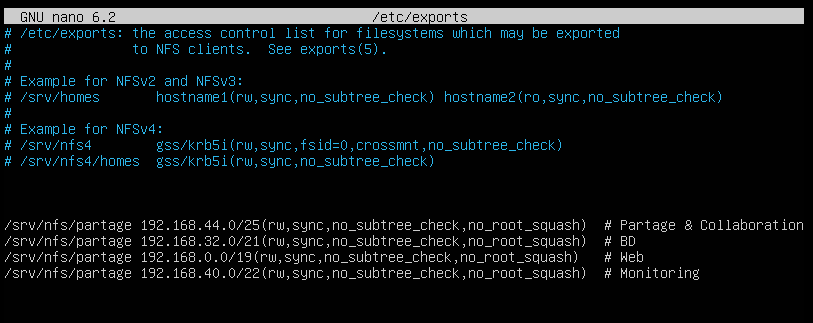
* Création d’un répertoire de partage



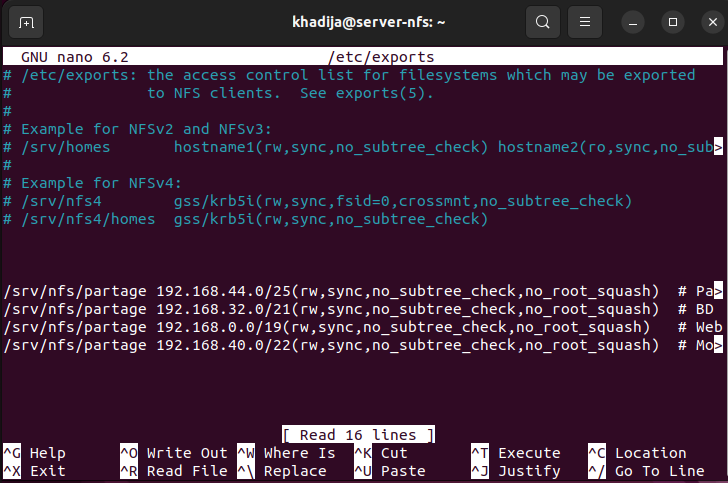


* Attribution des permissions nécessaires





* Autorisation de l’accès au réseau des départements



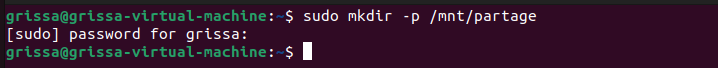
Le répertoire partagé est exporté de manière à être accessible par les clients autorisés du réseau **192.168.0.0/17**.

**Configuration des clients NFS**

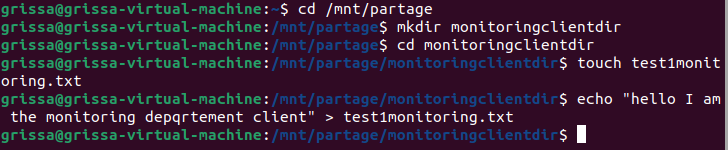
Les machines clientes (client-final-1, PC1, PC2, PC3) sont configurées pour :

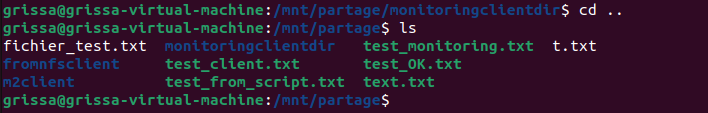
* Installer le client NFS



* Monter le répertoire partagé du serveur



* Accéder aux fichiers partagés via le point de montage local



**3.2.4 Département Base de Données :**

**Configuration des Services :**

**Automatisation (Script auto.sh) :**

L'installation et la sécurisation du serveur sont entièrement automatisées. Le script réalise :

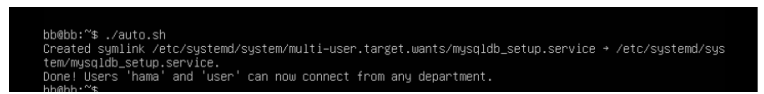
1. La mise à jour des dépôts et l'installation de mysql-server.

2. La configuration du bind-address sur 0.0.0.0 pour autoriser les connexions distantes.

3. La création d'un utilisateur administrateur (hama) et d'un utilisateur standard (user) autorisés pour tout le réseau de l'entreprise (192.168.%.%).

**Persistance (Service Systemd)**

Un service personnalisé mysqldb\_setup.service a été créé dans /etc/systemd/system/ pour garantir que les privilèges et les configurations sont maintenus après chaque redémarrage.



**3.3 Description de chaque service :**

**3.3.1 Département partage et collaboration :**

Le service **NFS (Network File System)** a été mis en place afin de permettre le partage centralisé de fichiers entre les différents utilisateurs du département ***Partage et Collaboration*.**Ce service facilite le travail collaboratif, l’accès aux ressources communes et la synchronisation des données au sein du réseau de l’entreprise.

Un serveur **NFS** dédié héberge un répertoire de partage accessible aux clients autorisés du réseau du département. Les postes clients montent ce répertoire distant comme un système de fichiers local, ce qui permet une utilisation transparente des fichiers (lecture, écriture, création et suppression selon les permissions définies).

L’accès au service est restreint au réseau du département **Partage et Collaboration**, garantissant ainsi la sécurité des données et empêchant les accès non autorisés. Les permissions sont gérées au niveau du système de fichiers afin d’assurer un contrôle précis des droits des utilisateurs.

Grâce à ce service, les membres du département peuvent :

* Partager des documents et ressources communes
* Travailler simultanément sur les mêmes fichiers
* Centraliser les données pour faciliter la sauvegarde et l’administration
* Améliorer la productivité et la collaboration entre les utilisateurs

**3.3.2 Département Web :**

**1.1 Description du serveur Web**

Le serveur Web est une machine Ubuntu Server ayant pour rôle principal d’héberger et de fournir des pages Web aux clients du réseau interne et externe.

Caractéristiques principales du serveur Web :

• **Adresse IP privée :** [**192.168.0.10**](http://192.168.0.10/)

• **Adresse IP publique (NAT) :** [**200.1.1.10**](http://200.1.1.10/)

• **Serveur Web utilisé :** Apache2

• **Base de données :** MySQL (marketing\_bd)

• **Gestion automatique :** service systemd personnalisé Le serveur Web assure les fonctions suivantes :

• Hébergement des fichiers Web dans le répertoire /var/www/html

• Réponse aux requêtes HTTP des clients

• Connexion à une base de données centralisée pour la gestion des données

• Disponibilité automatique au démarrage du système grâce à systemd Ce serveur constitue le cœur de l’architecture réseau et garantit l’accès aux services Web aussi bIen depuis le réseau local que depuis le backbone.

❤️

**3.3.3 Département Monitoring :**

**Prometheus  :**

C’est un système de monitoring et de collecte de métriques open-source.

**Rôle :**

● Collecter les métriques exposées par les exporters

● Stocker les données sous forme de séries temporelles

● Fournir les données aux outils de visualisation

**Fonctionnement :**

Prometheus interroge périodiquement les exporters via le protocole http

Les cibles à superviser sont définies dans le fichier prometheus.yml

**Ports utilisés :**

9090/TCP : interface web et API Prometheus

**Grafana :**

Grafana est un outil de visualisation permettant d’afficher les métriques collectées par Prometheus sous forme de tableaux de bord interactifs.

**Rôle :**

● Visualiser les données de monitoring

● Fournir des graphiques et indicateurs clairs

● Faciliter l’analyse des performances et de l’état du système

**Fonctionnement :**

Grafana se connecte à Prometheus comme source de données

**Les dashboards** :

sont configurés manuellement ou importés

**Ports utilisés :** 3000/TCP : interface web Grafana

**Node Exporter :** est un exporter Prometheus dédié à la supervision des serveurs Linux.

**Rôle :**

● Exposer les métriques système des serveurs

● Fournir des informations sur les ressources matérielles

**Métriques collectées :**

● Utilisation CPU

● Mémoire RAM

● Espace disque

● Uptime du système

**Ports utilisés :** 9100/TCP

**3.3.4 Département Base de Données :**

**mysqldb\_setup.service :**

Le service mysqldb\_setup est une unité de gestion système (Unit File) de type oneshot, conçue pour garantir l'automatisation et la persistance de la configuration du serveur de base de données. 1.

**Objectif du Service :**

Dans un environnement réseau complexe comme GNS3, certains paramètres ou privilèges peuvent être réinitialisés lors de redémarrages ou de changements d'interfaces. Ce service garantit que dès que le serveur Ubuntu démarre, les configurations critiques (ouverture du port, droits d'accès des départements Web et Partage) sont réappliquées sans intervention humaine.

**2. Fonctionnement Technique :**

Dépendances (After=) : Le service est configuré pour ne se lancer qu'après l'activation complète du réseau (network.target) et du service MySQL (mysql.service). Cela évite que le script ne tente de modifier la base de données alors que celle-ci n'est pas encore prête.

**Type oneshot :** Le service exécute le script auto.sh une seule fois au démarrage, puis s'arrête tout en restant considéré comme "actif" (RemainAfterExit=yes).

**Cible (WantedBy=) :** Il est rattaché au mode multi-utilisateur (multi-user.target), ce qui correspond au démarrage normal du serveur

**3. Tâches Automatisées par le Service :**

À chaque lancement, le service force l'exécution des commandes suivantes :

**Ouverture réseau** : Vérification que le bind-address est bien sur [**0.0.0.0**](https://l.facebook.com/l.php?u=http%3A%2F%2F0.0.0.0%2F%3Ffbclid%3DIwZXh0bgNhZW0CMTAAYnJpZBExUnAzNmI1TEVzZ2JSNUlSVXNydGMGYXBwX2lkEDIyMjAzOTE3ODgyMDA4OTIAAR4xU-bbblqt6cP0-xGsaaRSxLltz8m4HLPgqY8kNebCtr-DwTBPrDE8QpK9mg_aem_MbuR8O_V3yjFmri_ZbnmFg&h=AT2aoY5ucj1hhAsV8atqXK9QRfyShEKW69AGfMA7ac-fZtSxBlal7yPXY5YYLh34sAGWhy94iCHjnpaUuCLfBZGhuaGubzm3WUhvgrHZbWnecq6CTzNhpDc1XSA5UGkifmphTQ).

**Sécurité :** Application de la politique de mots de passe (LOW).

**Privilèges :** Recréation ou mise à jour des utilisateurs hama et user avec l'hôte % pour permettre l'accès au département Web.

**Firewall :** S'assure que la règle ufw sur le port 3306 est active.

**4.Intérêt pour le Projet**

Ce service apporte une robustesse industrielle au département de base de données. Il transforme un simple script manuel en un service système natif, assurant que même après une coupure de courant ou un redémarrage de la topologie GNS3, le serveur MySQL reste immédiatement prêt à répondre aux requêtes des autres départements.

Comment vérifier ce service sur votre terminal ? Vous pouvez montrer cette commande dans votre rapport pour prouver qu'il fonctionne :

Bash

systemctl status mysqldb\_setup.service

**(Si le service est bien installé, il doit afficher "active (exited)" en vert).**

**3.4 Intégration de la sécurité :**

## 

**Étape 1 – Définition du trafic à sécuriser (ACL)**  
Les listes de contrôle d’accès identifient le trafic LAN vers LAN qui doit être chiffré. Seules les communications entre les réseaux internes des départements sont concernées.

**Étape 2 – Paramètres de chiffrement (Transform-set)**  
Le transform-set définit les algorithmes utilisés pour protéger les données, notamment le chiffrement AES et le contrôle d’intégrité SHA-HMAC.

Dans cette configuration, le transform-set utilise :

* **AES** pour le chiffrement des données, assurant la confidentialité du trafic,
* **SHA-HMAC** pour vérifier l’intégrité et l’authenticité des paquets.

Le transform-set est associé à la crypto map et appliqué sur l’interface WAN, ce qui permet d’activer le chiffrement effectif du trafic LAN vers LAN.

match address 110 précise le trafic à chiffrer en associant l’ACL 110 au tunnel IPsec.

**Étape 3 – Création de la politique IPsec (Crypto map)**  
La crypto map associe le routeur distant, les paramètres de chiffrement et l’ACL afin de lier la sécurité au trafic réseau.

**« « crypto map VPNMAP 10 ipsec-isakmp « «**

Cette commande crée une politique IPsec nommée VPNMAP. Le numéro 10 définit la priorité de la règle, et ipsec-isakmp indique que la négociation se fait via ISAKMP (IKE).

**« « set peer 200.1.1.5 » »**

Cette commande spécifie l’adresse IP du routeur distant avec lequel le tunnel IPsec est établi.

**« « set transform-set ESP-AES » »**

Elle associe le transform-set à la crypto map, définissant les algorithmes de chiffrement et d’intégrité utilisés pour protéger les données.

**Étape 4 – Application sur l’interface WAN**

**« « interface f0/1 « «**

**« «  crypto map VPNMAP »»**

La crypto map est appliquée sur l’interface connectée au backbone, ce qui active le tunnel IPsec pour le trafic inter-départements.

**Étape 5 – Négociation sécurisée (ISAKMP)**

**“crypto isakmp policy 10 #** Crée une **politique ISAKMP**

**encr aes #** l’algorithme de **chiffrement**

**hash sha #** Spécifie l’algorithme de **hachage**

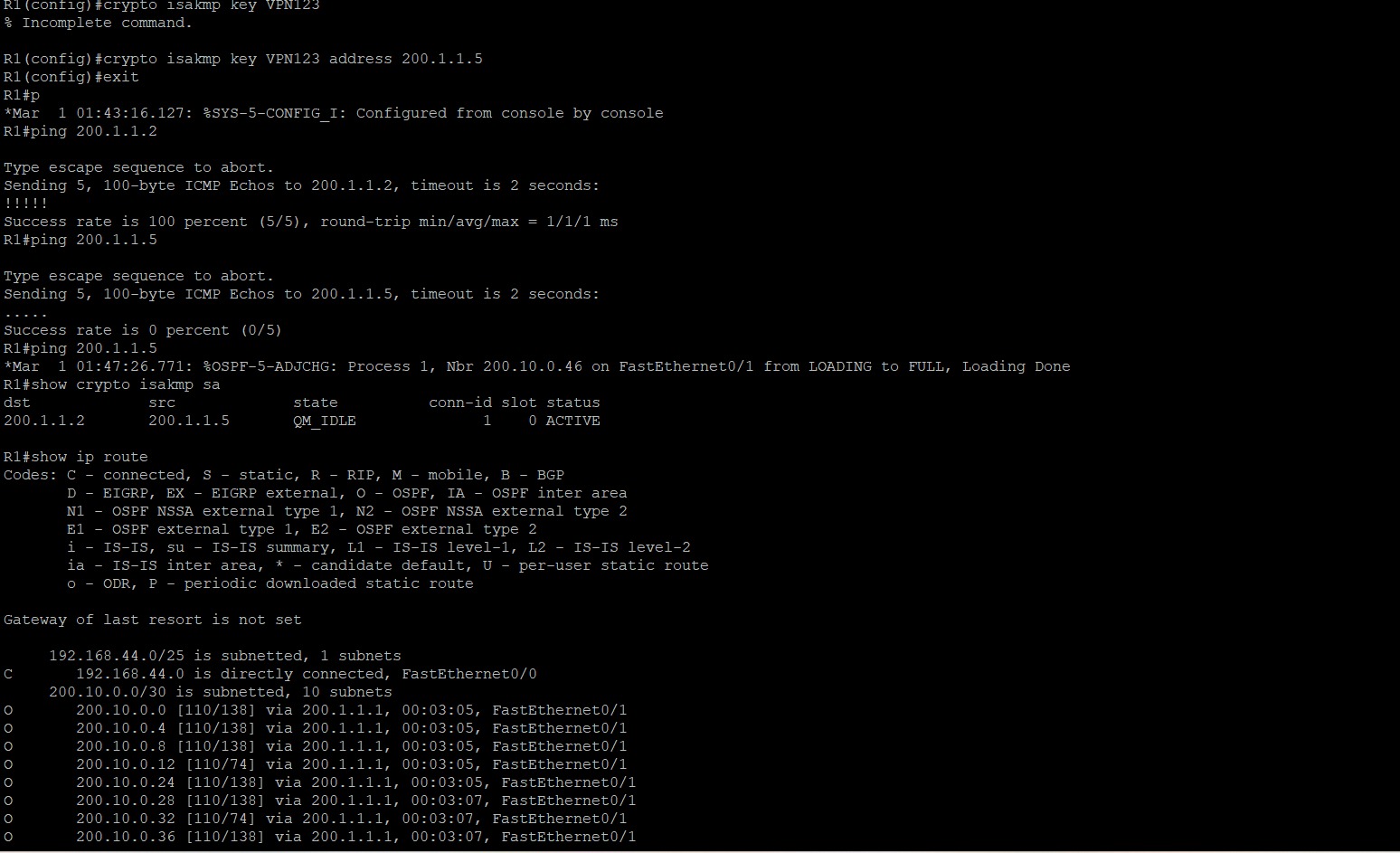
**authentication pre-share #** Indique que l’**authentification** entre les routeurs se fait

par **clé pré-partagée**.

**group 2 #** Définit le **groupe Diffie-Hellman**

**lifetime 86400 #** la **durée de validité**

La politique ISAKMP définit les paramètres de la phase 1 d’IPsec, permettant l’authentification des routeurs et l’établissement du tunnel sécurisé.

****

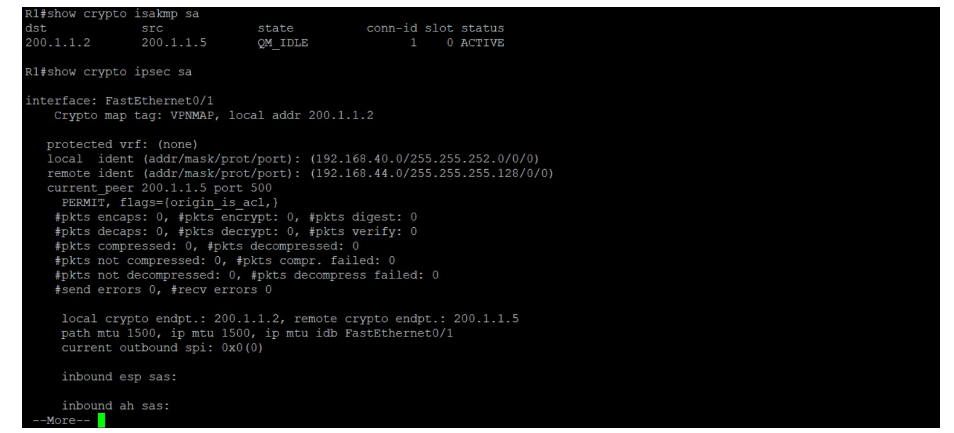
Cette capture montre la configuration de la clé IPsec, les tests de connectivité par ping entre les routeurs, ainsi que la vérification de l’établissement du tunnel IPsec. L’état QM\_IDLE confirme que la négociation IPsec est active, tandis que la table de routage affichée valide le bon fonctionnement du routage OSPF

**● L’état IPsec est actif**

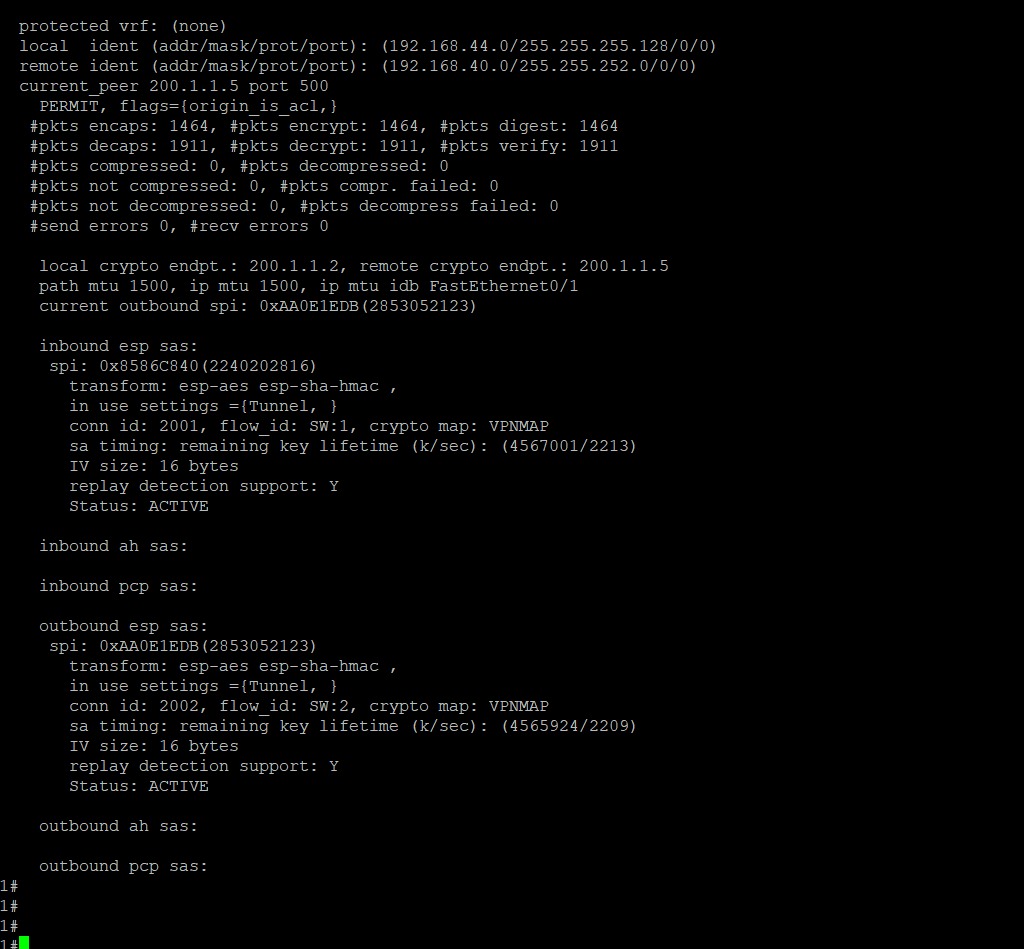
**● L’état** QM\_IDLE indique que le tunnel IPsec est **correctement établi et opérationnel**.

**● La** connectivité réseau est fonctionnelle

**● Le routage est opérationnel**



Les commandes show crypto isakmp sa et show crypto ipsec sa confirment que le tunnel IPsec est établi (QM\_IDLE)

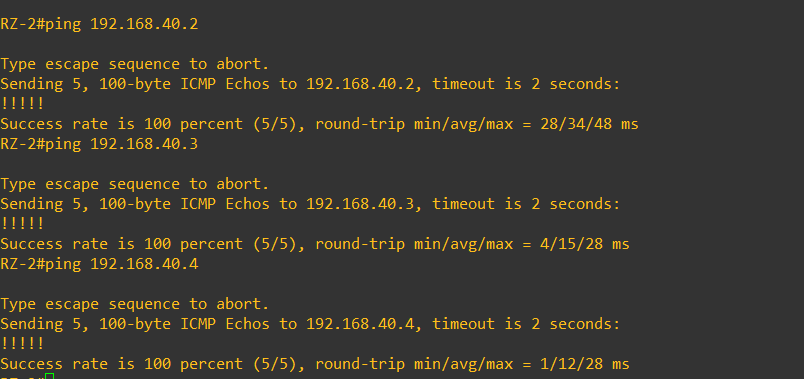


La commande show crypto ipsec sa confirme que le tunnel IPsec est actif et que le trafic est chiffré (encaps/decaps > 0)

**4. Analyse et résultats :**

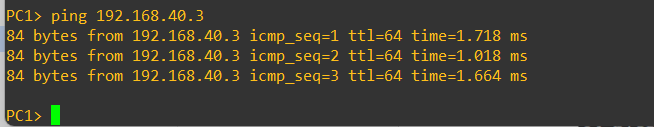
**4.1 Validation fonctionnelle par des tests :**

**Département Monitoring :**

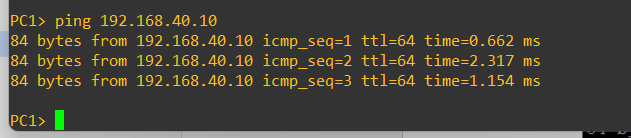


* Ping entre les vpcs

Pc1 -> pc2



Pc1 -> pc3

Pc1 -> vm client

Pc1 -> serveur

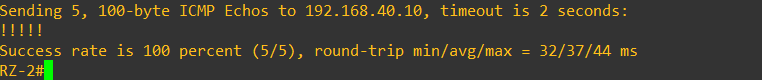


* Ping du routeur vers les vms

Serveur :

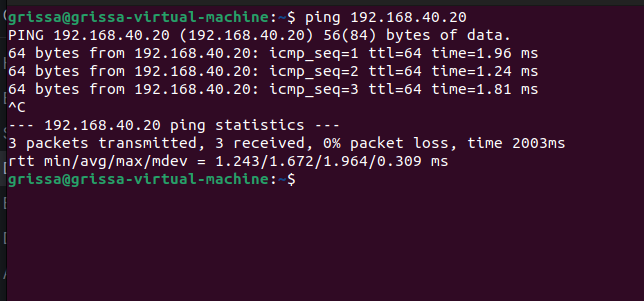


Client :

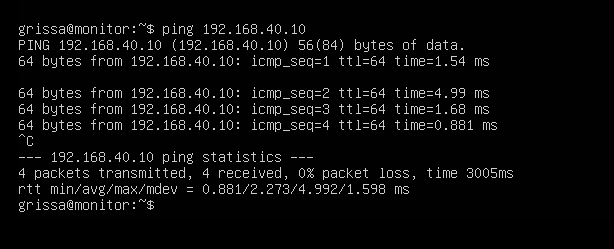


* Ping entre clients et serveur

Client->Serveur :



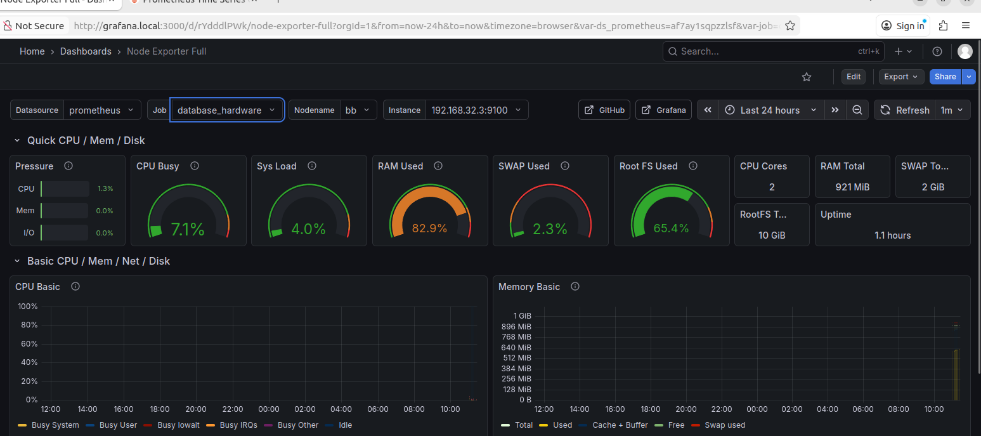
Serveur->Client :



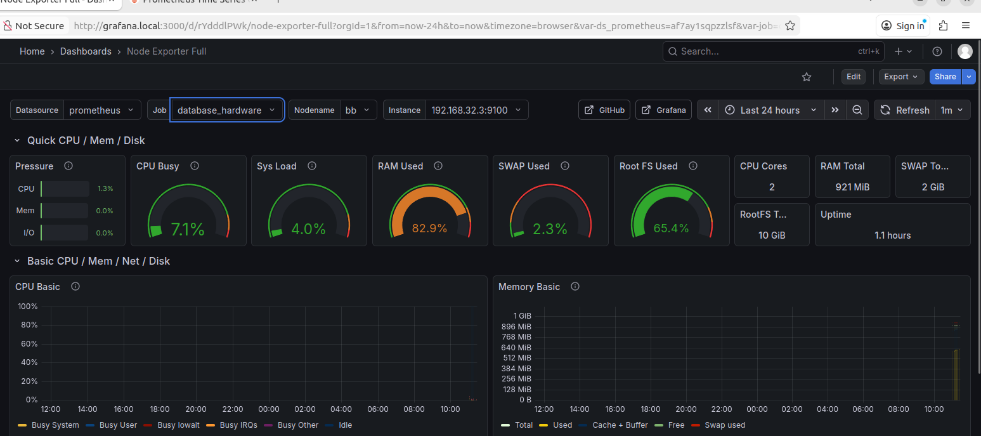
**Tests réalisés :**

Les tests suivants ont été réalisés :

* Vérification de l’accès aux métriques Node Exporter



* Vérification des cibles actives dans Prometheus
* Affichage correct des métriques dans Grafana

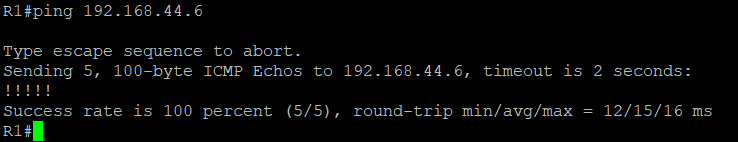


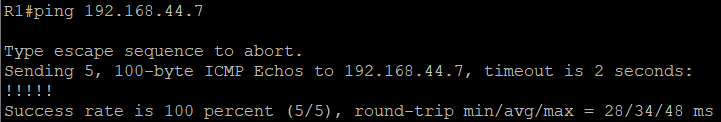
**Département partage et collaboration :**

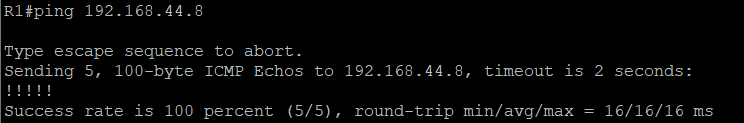
**Tests de validation réalisés :**

### Tests de connectivité

* Ping du routeur vers les vpcs





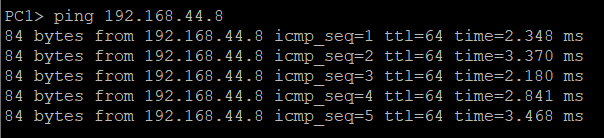


* Ping entre les vpcs

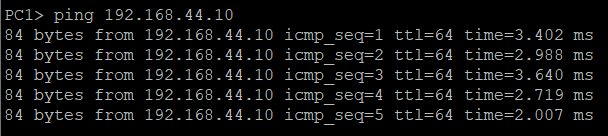
Pc1 -> pc2



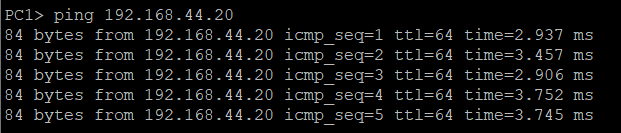
Pc1 -> pc3



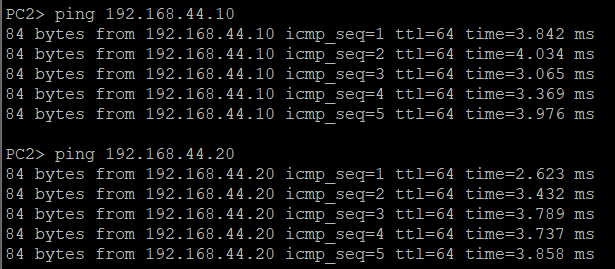
Pc1 -> vm client



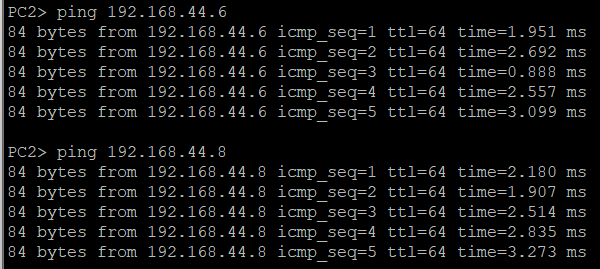
Pc1 -> serveur



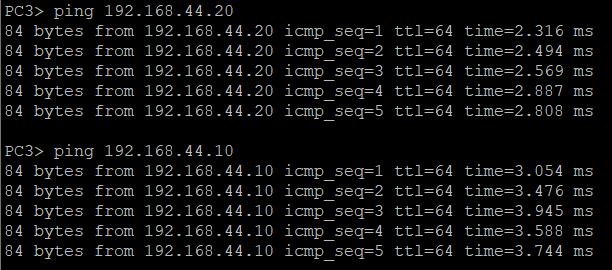
Pc2 -> vms



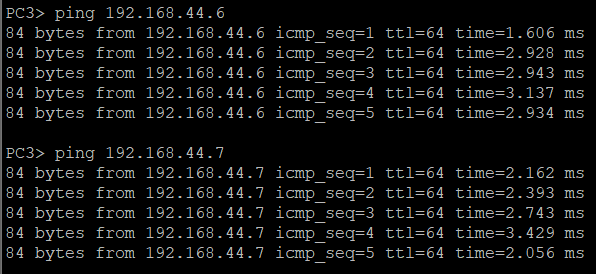
Pc2 -> vpcs



Pc3->vms

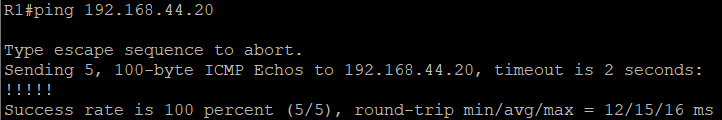


Pc3->vpcs

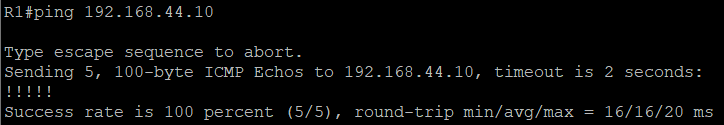


* Ping du routeur vers les vms

Serveur :

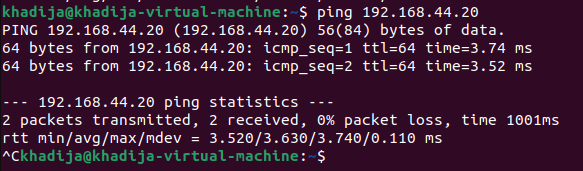


Client :

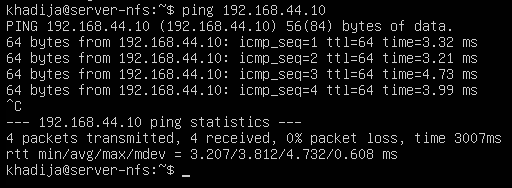


* Ping entre clients et serveur

Client->Serveur :

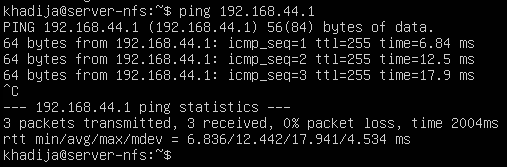


Serveur->Client :

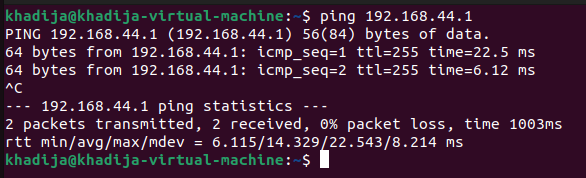


* Ping vers la passerelle (R1)

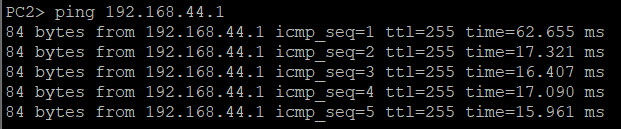
Serveur :



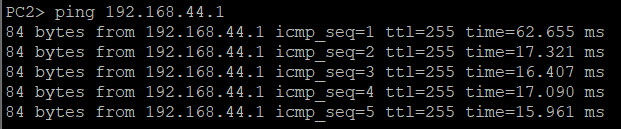
Client :



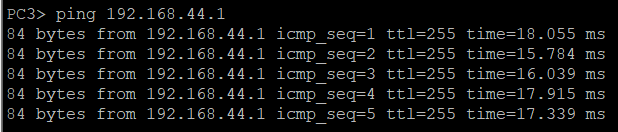
Pc1 :



Pc2 :



Pc3 :



### **Tests de services**

* Attribution d’adresse IP via DHCP



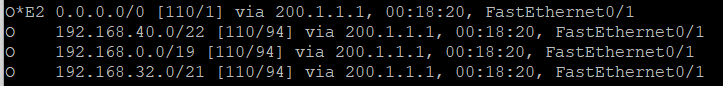




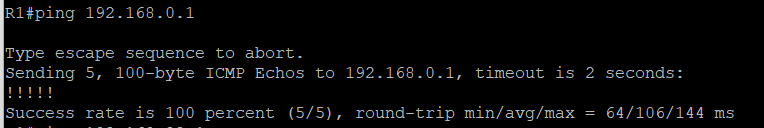
* Accès aux ressources partagées depuis les clients

### **Tests de routage**

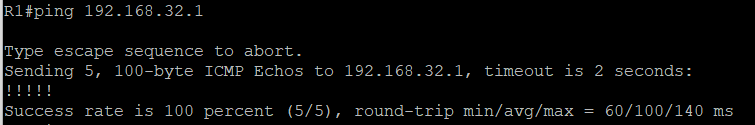
* Vérification des routes OSPF



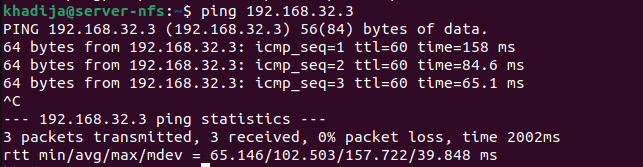
* Communication avec les autres départements via le backbone et le Cloud



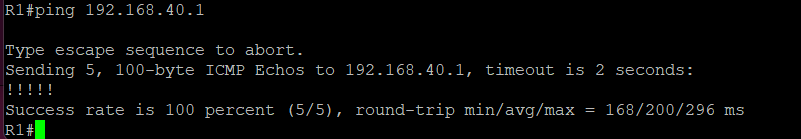
Département Base de Données routeur :



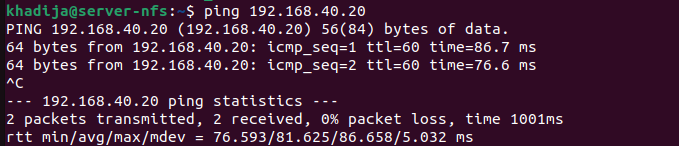
Serveur BD :



Département Monitoring routeur:



Serveur Monitoring :



**Résultat :** Tous les tests sont concluants - Le département Partage / Collaboration fonctionne correctement

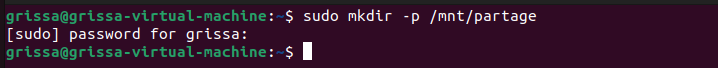
**Tests du service NFS**

Plusieurs tests ont été effectués afin de valider le bon fonctionnement du service NFS.

**Tests réalisés**

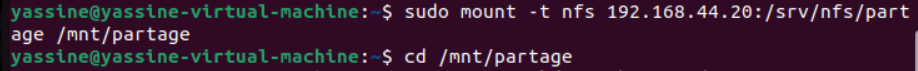
* Vérification du montage du partage NFS sur les clients

Depuis le département Monitoring :



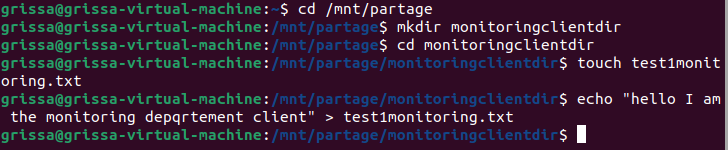


Depuis département Web :



* Création de fichiers depuis un client

Depuis le département Monitoring :

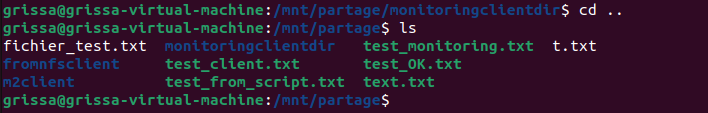


Depuis le département Web :

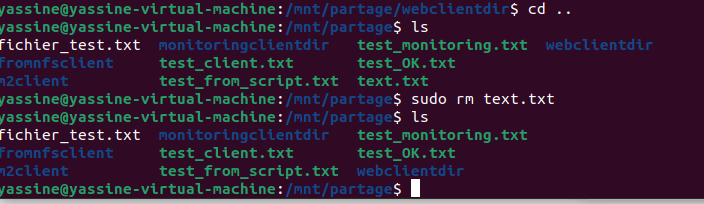


* Vérification de la visibilité des fichiers depuis les autres clients

Depuis le département Monitoring :

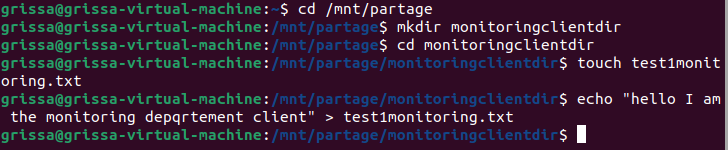


Depuis département Web :



* Test de lecture et d’écriture sur le répertoire partagé

Depuis le département Monitoring :

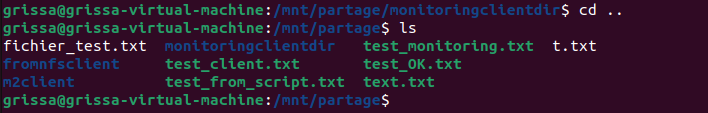


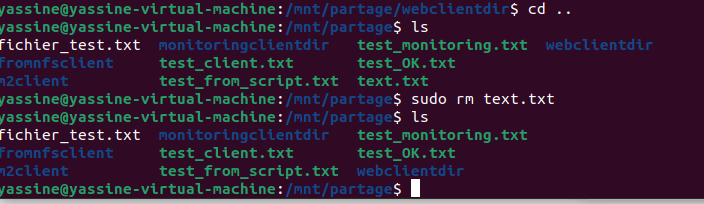
Depuis le département Web :



**Résultats**

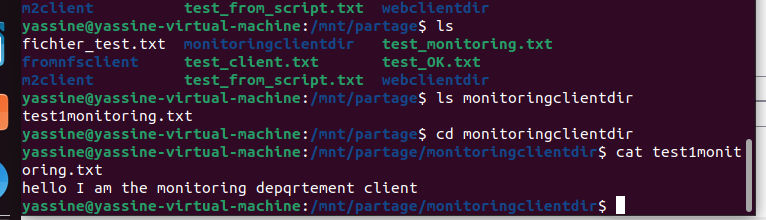
* Le répertoire partagé est accessible depuis tous les clients autorisés





* Les fichiers créés sur un client sont visibles sur les autres machines

Le client web accédé au répertoire crée par le client monitoring



**Département Web :**

**Testez depuis le PC1**

**A screenshot of a computer program

AI-generated content may be incorrect.**

**Testez depuis le PC2**

A screenshot of a computer

AI-generated content may be incorrect.

**Testez depuis le PC3**

A screenshot of a computer

AI-generated content may be incorrect.

\*) PING ip :

A screen shot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

\*) Verif si les PC ping Sur adress WEB



A screenshot of a computer screen

AI-generated content may be incorrect.

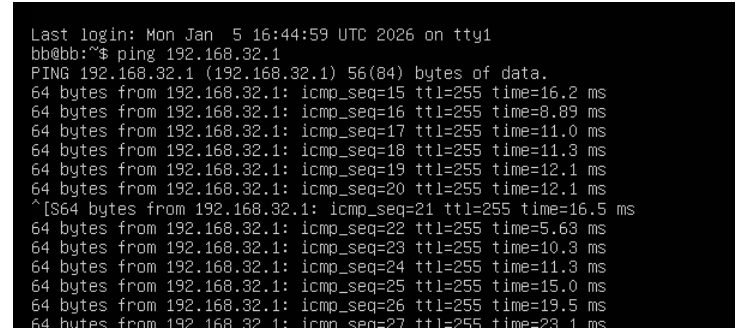
**Département Base de Données :**

**Tests de Validation :**

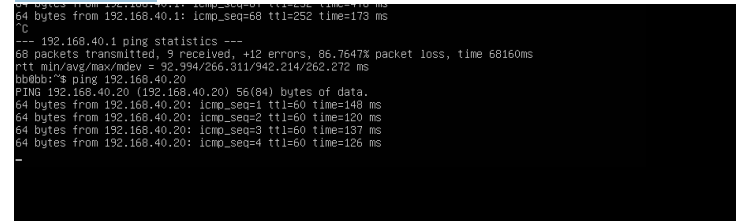
Plusieurs tests ont été effectués afin de valider le bon fonctionnement du département.

**Validation Réseau**

• **Ping vers la passerelle :** Validation de la communication locale avec R1.

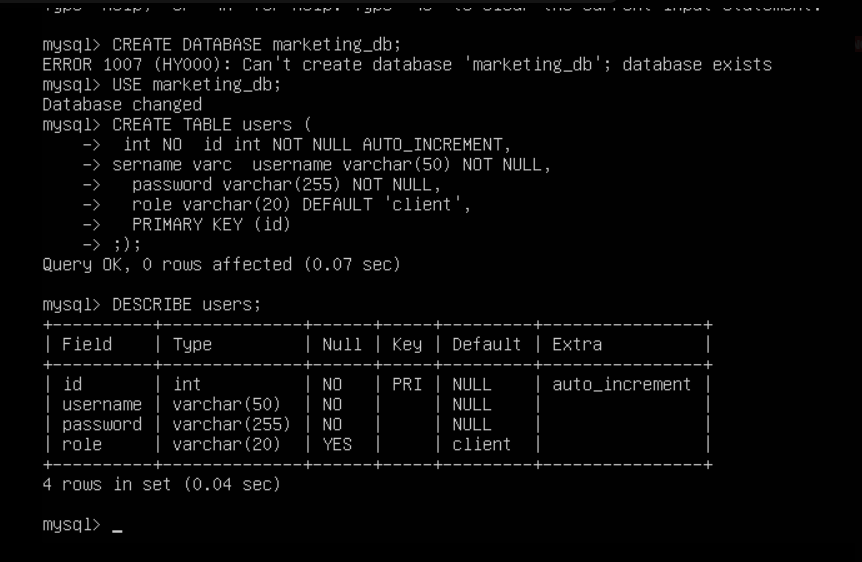
****

• **Ping inter-département :** Test réussi vers le département Partage (192.168.x.x) via le Backbone.

****

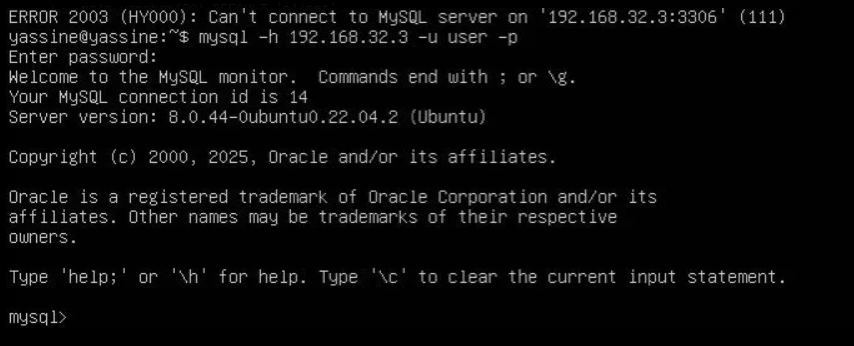
**Validation du Service MySQL**

• **Connexion locale :** Test de connexion réussi sur le serveur.



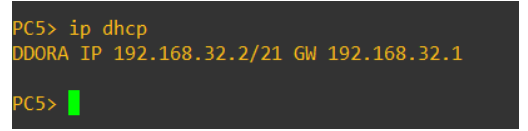
• **Connexion distante :** Vérification de l'accès depuis un client externe via le port

3306.

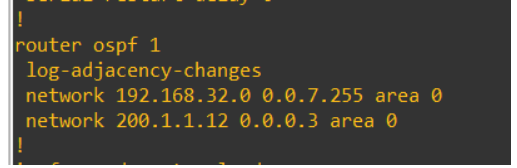
****

**Résultats des tests**

• **Attribution DHCP :** Les VPCS reçoivent correctement leurs IPs dans la plage /21.

****

**Routage OSPF :** La table de routage du routeur R1 contient les routes vers les autres zones.

****

**5 Conclusion et perspectives :**

**Conclusion**

Ce projet a permis de concevoir et de déployer une **infrastructure réseau multiservice complète**, représentative d’un environnement d’entreprise réel. L’architecture mise en place repose sur un **backbone OSPF** assurant un routage dynamique et hiérarchisé entre les différents départements de l’entreprise TechSolutions SARL.

La **segmentation du réseau par VLSM** a permis une utilisation optimale de l’adressage IP, tandis que la mise en œuvre des services (Web, Base de données, NFS et Monitoring) a répondu aux besoins fonctionnels de chaque département. L’accès à Internet a été assuré de manière sécurisée via un routeur NAT.

Sur le plan de la sécurité, l’intégration de **tunnels VPN IPsec site-à-site** entre le backbone et les départements a permis de garantir la confidentialité et l’intégrité des communications inter-départements, sans impacter le fonctionnement des équipements terminaux.

Le travail collaboratif a permis de répartir efficacement les responsabilités entre les membres du groupe, tout en assurant la cohérence globale de l’infrastructure. Les tests réalisés ont confirmé la **connectivité**, la **disponibilité des services** et le **bon fonctionnement des mécanismes de sécurité**.

## **Perspectives d’évolution :**

Plusieurs améliorations pourraient être envisagées pour faire évoluer cette infrastructure :

* **Renforcement de la sécurité**, par l’ajout de pare-feu dédiés, de listes de contrôle d’accès plus fines ou d’une authentification VPN basée sur certificats.
* **Haute disponibilité**, en mettant en place des mécanismes de redondance des routeurs et des serveurs critiques.
* **Supervision avancée**, avec des outils de monitoring plus complets (alertes automatiques, tableaux de bord centralisés).
* **Scalabilité**, permettant l’ajout de nouveaux départements, services ou utilisateurs sans remise en cause de l’architecture existante.
* **Virtualisation et cloud**, en migrant certains services vers des solutions virtualisées ou hybrides afin d’améliorer la flexibilité et la gestion des ressources.

**Ces perspectives permettraient d’aligner davantage l’infrastructure sur les standards professionnels et les besoins futurs de l’entreprise.**