

Livrable intégrale

EPREUVE E6

(Situations Professionnelles)



Lycée Turgot
69 Rue Turbigo, 75003 Paris

BTS SIO 2A – PLOT 6

Chef de Projet : Hariharani THEIVENDRAM

Administratrice systèmes & réseaux : Aminata THIAM

Administrateur systèmes & réseaux : Omar SISSOKO



| | |
|---|-----------|
| Intégralité des documentations techniques | |
| Omar SISSOKO, Hariharani THEIVENDRAM, Aminata THIAM | |
| BTS SIO 2A | 2024/2025 |
| | |



| | | |
|------------|---|-----------|
| | Intégralité des documentations techniques | |
| | Omar SISSOKO, Hariharani THEIVENDRAM, Aminata THIAM | |
| BTS SIO 2A | | 2024/2025 |

SOMMAIRE

PLOT - 6

| | |
|---|-----------|
| 1. Cahier des charges (général)..... | 10 |
| 1.1. Contexte et objectif..... | 10 |
| 1.1.1. Contexte | 10 |
| 1.1.2. Objectifs | 10 |
| 1.1.3. Contraintes Techniques | 10 |
| 1.2. Ressources Nécessaires | 11 |
| 1.2.1. Ressources Matérielles | 11 |
| 1.2.2. Ressources Immatérielles | 11 |
| 1.2.3. Ressources Humaines..... | 11 |
| 2. Architecture réseau | 13 |
| 2.1. Infrastructure physique du PLOT 6 | 13 |
| 2.2. Infrastructure virtuelle individuel (plan d'adressage, liste des machines, schéma).... | 14 |
| 2.2.1. Omar | 14 |
| 2.2.2. Hariharani..... | 16 |
| 2.2.3. Aminata | 19 |
| 3. Planning..... | 21 |
| 3.1. Trello et la méthode Kanban | 21 |
| 3.2. Méthode Kanban (ou Kanboard) : | 22 |
| 3.3. Mise au point - Discord..... | 22 |
| 3.4. Délais et Planning | 22 |
| 4. Outils | 23 |

Omar SISSOKO

| | |
|--|-----------|
| 1. Inventaire avec GLPI + GLPI agent..... | 26 |
| 1.1. Cahier des charges | 26 |
| 1.1.1. Contexte et Objectifs..... | 26 |
| 1.1.2. Descriptions fonctionnelles des besoins | 26 |
| 1.1.3. Cahier des charges technique..... | 26 |
| 1.1.4. Planning prévisionnel | 27 |
| 1.2. Plan d'adressage..... | 27 |
| 1.3. Schéma réseau..... | 27 |



| | |
|--|-----------|
| 1.4. Documentation technique..... | 28 |
| 1.4.1. Installation en ligne de commande | 28 |
| 1.4.2. Installation graphique de GLPI | 32 |
| 1.4.3. Installation Agent GLPI | 37 |
| 1.5. Fiche procédure – utilisateur | 40 |
| 1.6. Cahier de recettes..... | 41 |
| 1.7. Cahier de test | 41 |
| 2. Chiffrement des données - VeraCrypt..... | 42 |
| 2.1. Cahier des charges | 42 |
| 2.1.1. Contexte et Objectifs..... | 42 |
| 2.1.2. Descriptions fonctionnelles des besoins | 42 |
| 2.1.3. Cahier des charges technique..... | 42 |
| 2.1.4. Planning prévisionnel | 43 |
| 2.2. Schéma réseau..... | 43 |
| 2.3. Documentation technique..... | 43 |
| 2.4. Fiche procédure – utilisateur | 46 |
| 2.5. Cahier de recettes..... | 47 |
| 2.6. Cahier de test | 47 |
| 3. OpenVPN | 48 |
| 3.1. Cahier des charges | 48 |
| 3.1.1. Contexte et Objectifs..... | 48 |
| 3.1.2. Descriptions fonctionnelles des besoins | 48 |
| 3.1.3. Cahier des charges technique..... | 48 |
| 3.1.4. Planning prévisionnel | 48 |
| 3.2. Plan d'adressage..... | 49 |
| 3.3. Schéma réseau..... | 49 |
| 3.4. Documentation technique..... | 50 |
| 3.5. Cahier de recettes..... | 61 |
| 3.6. Cahier de test | 61 |

| |
|-------------------------------|
| Hariharani THEIVENDRAM |
|-------------------------------|

| | |
|---|-----------|
| 4. Portail captif avec pfSense | 62 |
| 4.1. Cahier des charges | 62 |
| 4.1.1. Contexte et Objectifs..... | 62 |



| | |
|---|-----------|
| Intégralité des documentations techniques | |
| Omar SISSOKO, Hariharani THEIVENDRAM, Aminata THIAM | |
| BTS SIO 2A | 2024/2025 |
| | |

| | | |
|-----------|---|------------|
| 4.1.2. | Descriptions fonctionnelles des besoins | 62 |
| 4.1.3. | Cahier des charges technique..... | 63 |
| 4.1.4. | Planning prévisionnel | 63 |
| 4.2. | Plan d'adressage..... | 63 |
| 4.3. | Schéma réseau..... | 63 |
| 4.4. | Documentation technique..... | 64 |
| 4.4.1. | Pfsense - actif | 64 |
| 4.4.2. | Ubuntu - client | 64 |
| 4.5. | Fiche procédure – utilisateur | 77 |
| 4.6. | Cahier de recettes..... | 78 |
| 4.7. | Cahier de test | 78 |
| 5. | Supervision de l'espace disque avec Prometheus | 79 |
| 5.1. | Cahier des charges | 79 |
| 5.1.1. | Contexte et Objectifs..... | 79 |
| 5.1.2. | Descriptions fonctionnelles des besoins | 79 |
| 5.1.3. | Cahier des charges technique..... | 80 |
| 5.1.4. | Planning prévisionnel | 80 |
| 5.2. | Plan d'adressage..... | 80 |
| 5.3. | Schéma réseau..... | 81 |
| 5.4. | Documentation technique..... | 81 |
| 5.4.1. | Pré-requis | 81 |
| 5.4.2. | Prometheus | 82 |
| 5.4.3. | Node Exporter (client Linux) | 85 |
| 5.4.4. | Windows Exporter (client Windows) | 88 |
| 5.4.4. | Grafana..... | 89 |
| 5.4.5. | Alertmanager | 94 |
| 5.5. | Simulation d'espace disque faible | 98 |
| 5.6. | Cahier de recettes..... | 103 |
| 5.7. | Cahier de test | 103 |
| 6. | Analyse de vulnérabilités : Nessus | 104 |
| 6.1. | Cahier des charges | 104 |
| 6.1.1. | Contexte et Objectifs..... | 104 |
| 6.1.2. | Descriptions fonctionnelles des besoins | 104 |
| 6.1.3. | Cahier des charges technique..... | 104 |



| | |
|---|-----------|
| Intégralité des documentations techniques | |
| Omar SISSOKO, Hariharani THEIVENDRAM, Aminata THIAM | |
| BTS SIO 2A | 2024/2025 |
| | |

| | |
|--|------------|
| 6.1.4. Planning prévisionnel | 104 |
| 6.2. Plan d'adressage..... | 104 |
| 6.3. Schéma réseau..... | 105 |
| 6.4. Documentation technique..... | 105 |
| 6.4.1. Prérequis | 105 |
| 6.4.2. Choix de l'installation..... | 106 |
| 6.4.3. Installation du package..... | 106 |
| 6.4.4. Configuration initiale | 107 |
| 6.4.5. Optimisation et sécurisation..... | 108 |
| 6.4.6. Configuration du scanner | 108 |
| 6.5. Fiche procédure – utilisateur | 110 |
| 6.6. Cahier de recettes..... | 112 |
| 6.7. Cahier de test | 112 |
| 7. Snort..... | 113 |
| 7.1. Cahier des charges | 113 |
| 7.1.1. Contexte et Objectifs..... | 113 |
| 7.1.2. Descriptions fonctionnelles des besoins | 113 |
| 7.1.3. Cahier des charges technique..... | 113 |
| 7.1.4. Planning prévisionnel | 113 |
| 7.2. Plan d'adressage..... | 114 |
| 7.3. Schéma réseau..... | 114 |
| 7.4. Documentation technique..... | 114 |
| 7.4.1. Prérequis | 114 |
| 7.4.2. Installation..... | 115 |
| 7.4.3. Détection des attaques | 117 |
| 7.4.4. Configurer une règle de test | 117 |
| 7.4.5. Tester la configuration de Snort..... | 117 |
| 7.4.6. Tester Snort avec un ping | 118 |
| 7.4.7. Démarrer Snort en tant que service | 118 |
| 7.5. Cahier de recettes..... | 119 |
| 7.6. Cahier de test | 119 |
| 8. Fail2ban | 120 |
| 8.1. Cahier des charges | 120 |
| 8.1.1. Contexte et Objectifs..... | 120 |



| | |
|---|-----------|
| Intégralité des documentations techniques | |
| Omar SISSOKO, Hariharani THEIVENDRAM, Aminata THIAM | |
| BTS SIO 2A | 2024/2025 |
| | |

| | | |
|--------|---|-----|
| 8.1.2. | Descriptions fonctionnelles des besoins | 120 |
| 8.1.3. | Cahier des charges technique..... | 120 |
| 8.1.4. | Planning prévisionnel | 120 |
| 8.2. | Plan d'adressage..... | 121 |
| 8.3. | Schéma réseau..... | 121 |
| 8.4. | Documentation technique..... | 121 |
| 8.4.1. | Prérequis | 121 |
| 8.4.2. | Installation de Fail2Ban | 122 |
| 5.4.3. | Configuration de Fail2Ban | 122 |
| 5.4.5. | Activation et vérification | 123 |
| 5.4.6. | Installer OpenSSH | 124 |
| 5.4.6. | Simuler un banissement | 124 |
| 5.4.7. | Débannir une IP manuellement | 126 |
| 5.4.8. | Vérification des logs | 126 |
| 8.5. | Fiche procédure – utilisateur | 128 |
| 8.6. | Cahier de recettes..... | 129 |
| 8.7. | Cahier de test | 129 |

Aminata THIAM

| | | |
|-----------|---|------------|
| 9. | BackupManager | 130 |
| 9.1. | Cahier des charges | 130 |
| 9.1.1. | Contexte et Objectifs..... | 130 |
| 9.1.2. | Descriptions fonctionnelles des besoins | 130 |
| 9.1.3. | Cahier des charges technique..... | 130 |
| 9.1.4. | Planning prévisionnel | 131 |
| 9.2. | Plan d'adressage..... | 131 |
| 9.3. | Schéma réseau..... | 131 |
| 9.4. | Documentation technique..... | 131 |
| 9.4.1. | Installation du système d'exploitation Ubuntu | 131 |
| 9.4.2. | Installation de backup-manager | 131 |
| 9.4.3. | Configuration du répertoire de sauvegarde | 132 |
| 9.4.4. | Test de la Configuration | 133 |
| 9.4.5. | Restauration de la Sauvegarde..... | 133 |
| 9.5. | Cahier de recettes..... | 135 |



| | | |
|------------|---|------------|
| 9.6. | Cahier de test | 136 |
| 10. | Serveur LAMP | 137 |
| 10.1. | Cahier des charges | 137 |
| 10.1.1. | Contexte et Objectifs..... | 137 |
| 10.1.2. | Descriptions fonctionnelles des besoins | 137 |
| 10.1.3. | Cahier des charges technique..... | 137 |
| 10.1.4. | Planning prévisionnel | 138 |
| 10.2. | Plan d'adressage..... | 138 |
| 10. | Schéma réseau..... | 138 |
| 10.3. | Documentation technique..... | 138 |
| 10.3.1. | Installation et configuration d'une machine virtuelle Ubuntu sous Linux | 138 |
| 10.3.2. | Mise à jour des paquets | 139 |
| 10.3.3. | Installation des composants de LAMP..... | 139 |
| 10.4. | Cahier de recettes..... | 148 |
| 10.5. | Cahier de test | 149 |
| 11. | GLPI + agent..... | 150 |
| 11.1. | Cahier des charges | 150 |
| 11.1.1. | Contexte et Objectifs..... | 150 |
| 11.1.2. | Descriptions fonctionnelles des besoins | 150 |
| 11.1.3. | Cahier des charges technique..... | 150 |
| 11.1.4. | Planning prévisionnel | 151 |
| 11.2. | Plan d'adressage..... | 151 |
| 11.3. | Schéma réseau..... | 151 |
| 11.4. | Documentation technique..... | 152 |
| 11.4.1. | Installation d'un serveur GLPI sous Linux (ubuntu)..... | 152 |
| 11.4.2. | Agent GLPI sous Linux (ubuntu)..... | 154 |
| 11.4.3. | Installation de l'agent GLPI sous Windows..... | 156 |
| 11.5. | Fiche procédure – utilisateur | 159 |
| 11.6. | Cahier de recettes..... | 159 |
| 11.7. | Cahier de test | 159 |
| 12. | Règles de filtrage (pfSense)..... | 160 |
| 12.1. | Cahier des charges | 160 |
| 12.1.1. | Contexte et Objectifs..... | 160 |
| 12.1.2. | Descriptions fonctionnelles des besoins | 160 |



| | |
|---|-----------|
| Intégralité des documentations techniques | |
| Omar SISSOKO, Hariharani THEIVENDRAM, Aminata THIAM | |
| BTS SIO 2A | 2024/2025 |
| | |

| | |
|---|-----|
| 12.1.3. Cahier des charges technique..... | 160 |
| 12.1.4. Planning prévisionnel | 161 |
| 12.2. Plan d'adressage..... | 161 |
| 12.3. Schéma réseau..... | 161 |
| 12.4. Documentation technique..... | 162 |
| 12.4.1. Activer le NAT..... | 162 |
| 12.4.2. Autoriser le ping vers le WAN | 163 |
| 12.4.3. Bloquer l'accès à l'interface Web de pfSense depuis Internet..... | 164 |
| 12.4.4. Limiter la bande passante d'un client | 165 |
| 12.5. Cahier de recettes..... | 167 |
| 12.6. Cahier de test | 167 |



| | | |
|------------|---|-----------|
| | Intégralité des documentations techniques | |
| | Omar SISSOKO, Hariharani THEIVENDRAM, Aminata THIAM | |
| BTS SIO 2A | | 2024/2025 |

1. Cahier des charges (général)

1.1. Contexte et objectif

1.1.1. Contexte

L'entreprise **XYZ**, spécialisée dans le secteur des services numériques, souhaite renforcer son infrastructure informatique afin d'améliorer la gestion de ses actifs IT, la sécurité de son réseau et la supervision de ses services. Pour cela, elle a décidé de mettre en place une solution intégrée combinant plusieurs outils open-source.

En tant qu'**ingénieur système et réseau**, vous êtes chargé de concevoir et documenter l'ensemble de cette infrastructure dans un **cahier des charges détaillé**, en vue de sa mise en œuvre.

1.1.2. Objectifs

- **GLPI** pour l'inventaire et la gestion des incidents.
- **pfSense** avec un portail captif pour la gestion des utilisateurs et des accès réseau.
- **Prometheus** pour la supervision et l'analyse des performances des serveurs et services.
- **Nessus, Snort et Fail2Ban** pour la détection et la protection contre les cybermenaces.
- **WireGuard** pour sécuriser les connexions via un VPN.
- **LAMP** pour héberger les applications web internes.
- **BackupManager** pour automatiser la sauvegarde et la restauration des données critiques.

1.1.3. Contraintes Techniques

- **Langage et technologies :**
 - GLPI basé sur PHP et MySQL.
 - pfSense sur FreeBSD.
 - Prometheus avec alerting Grafana.
 - Nessus et Snort installés sur serveurs Linux.
 - WireGuard configuré sur un serveur Linux.
 - Stack LAMP : Linux, Apache, MySQL, PHP.
 - BackupManager sur Linux avec automatisation des sauvegardes.
- **Hébergement** : serveurs dédiés ou cloud (AWS, Azure, On-Premise).
- **Sécurité** : gestion des accès et des permissions, chiffrement des données.
- **Compatibilité** : intégration avec les systèmes et réseaux existants.

| | | |
|---|---|-----------|
| | Intégralité des documentations techniques | |
| Omar SISSOKO, Hariharani THEIVENDRAM, Aminata THIAM | | |
| BTS SIO 2A | | 2024/2025 |

1.2. Ressources Nécessaires

1.2.1. Ressources Matérielles

- **Serveurs physiques ou virtuels** pour héberger les différentes solutions : Proxmox
- **Postes client : Windows 10**
- **Équipements réseau** (routeurs, switchs, firewall).
- **Stockage** (NAS/SAN, disques durs, stockage cloud pour les sauvegardes).

1.2.2. Ressources Immatérielles

- **Licences et abonnements** (ex. : Nessus Essentials)
- **Systèmes d'exploitation et logiciels** (Linux, Windows, Apache, MySQL, PHP, etc.).
- **Documentation technique et guides d'utilisation.**
- **Plans de maintenance et mises à jour régulières des logiciels et systèmes.**

1.2.3. Ressources Humaines

- **Chef de projet** : supervision de l'implémentation et coordination des équipes.

Hariharni THEIVENDRAM

- **Administrateurs systèmes et réseaux** : installation, configuration et maintenance des services.

Aminata THIAM et Omar SISSOKO

- **Techniciens support** : gestion des incidents et assistance aux utilisateurs.

Omar SISSOKO

- **Responsable sécurité** : surveillance et analyse des vulnérabilités, mise en place des règles de protection.

Hariharani THEIVENDRAM

| | | | | | |
|---|--|---|---|------------|-----------|
|  | <table border="1"> <tr> <td data-bbox="541 101 1060 152">Intégralité des documentations techniques</td><td data-bbox="1060 101 1467 152">Omar SISSOKO, Hariharani THEIVENDRAM, Aminata THIAM</td></tr> <tr> <td data-bbox="541 152 1060 226">BTS SIO 2A</td><td data-bbox="1060 152 1467 226">2024/2025</td></tr> </table> | Intégralité des documentations techniques | Omar SISSOKO, Hariharani THEIVENDRAM, Aminata THIAM | BTS SIO 2A | 2024/2025 |
| Intégralité des documentations techniques | Omar SISSOKO, Hariharani THEIVENDRAM, Aminata THIAM | | | | |
| BTS SIO 2A | 2024/2025 | | | | |

Livrables

- Documentation technique et utilisateur
- Formation des administrateurs et utilisateurs

Critères de Validation

- Infrastructure fonctionnelle et sécurisée
- Performances et disponibilité optimales
- Protection efficace contre les menaces et attaques
- Sauvegarde et récupération des données sans perte
- Conformité aux besoins de l'entreprise

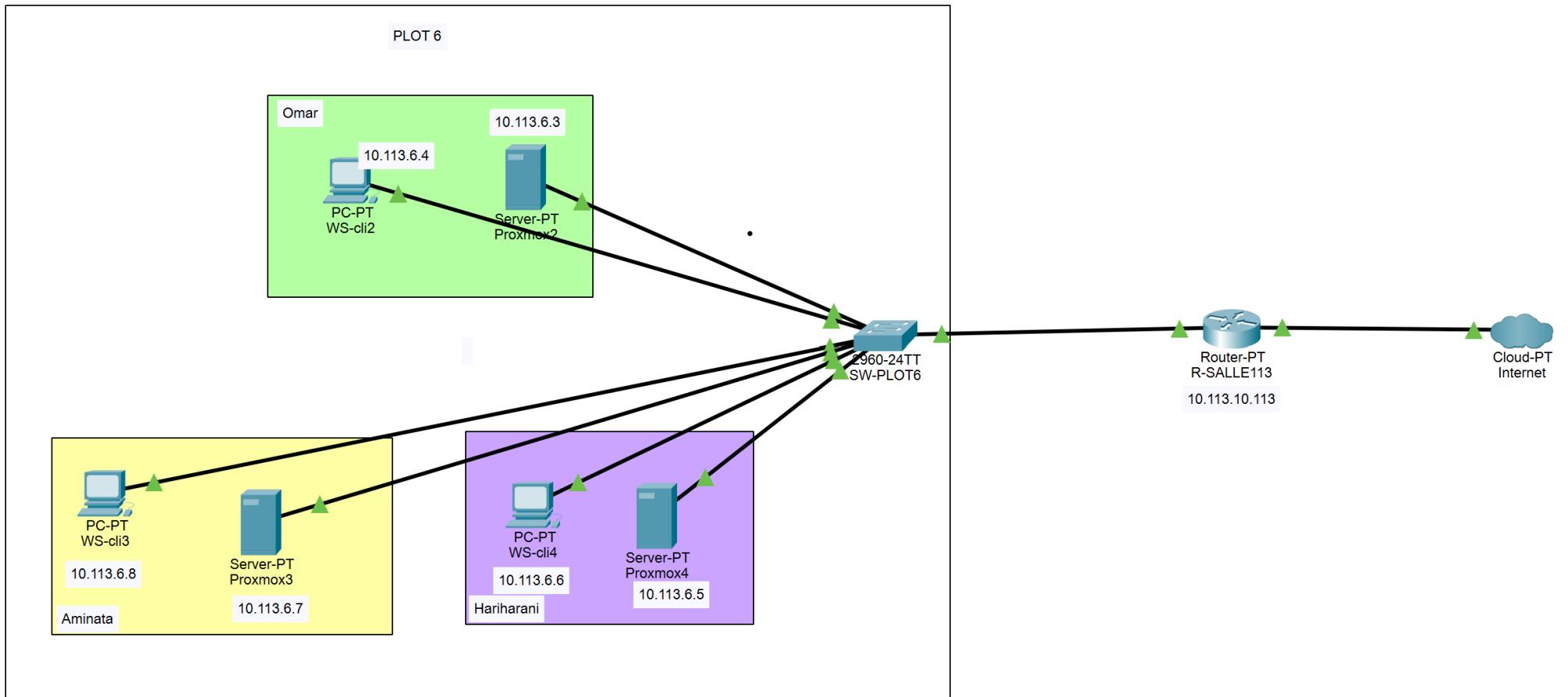
Annexes

- Schémas d'architecture réseau et sécurité
- Configurations détaillées des services
- Liste des contacts et parties prenantes



2. Architecture réseau

2.1. Infrastructure physique du PLOT 6



| | | | |
|--|---|--|-----------|
| | Hariharani THEIVENDRAM, Aminata THIAM, Omar SISSOKO | | |
| | Livrable - intégrale | | 2024-2025 |

2.2. Infrastructure virtuelle individuel (plan d'adressage, liste des machines, schéma)

2.2.1. Omar

Plan d'adressage

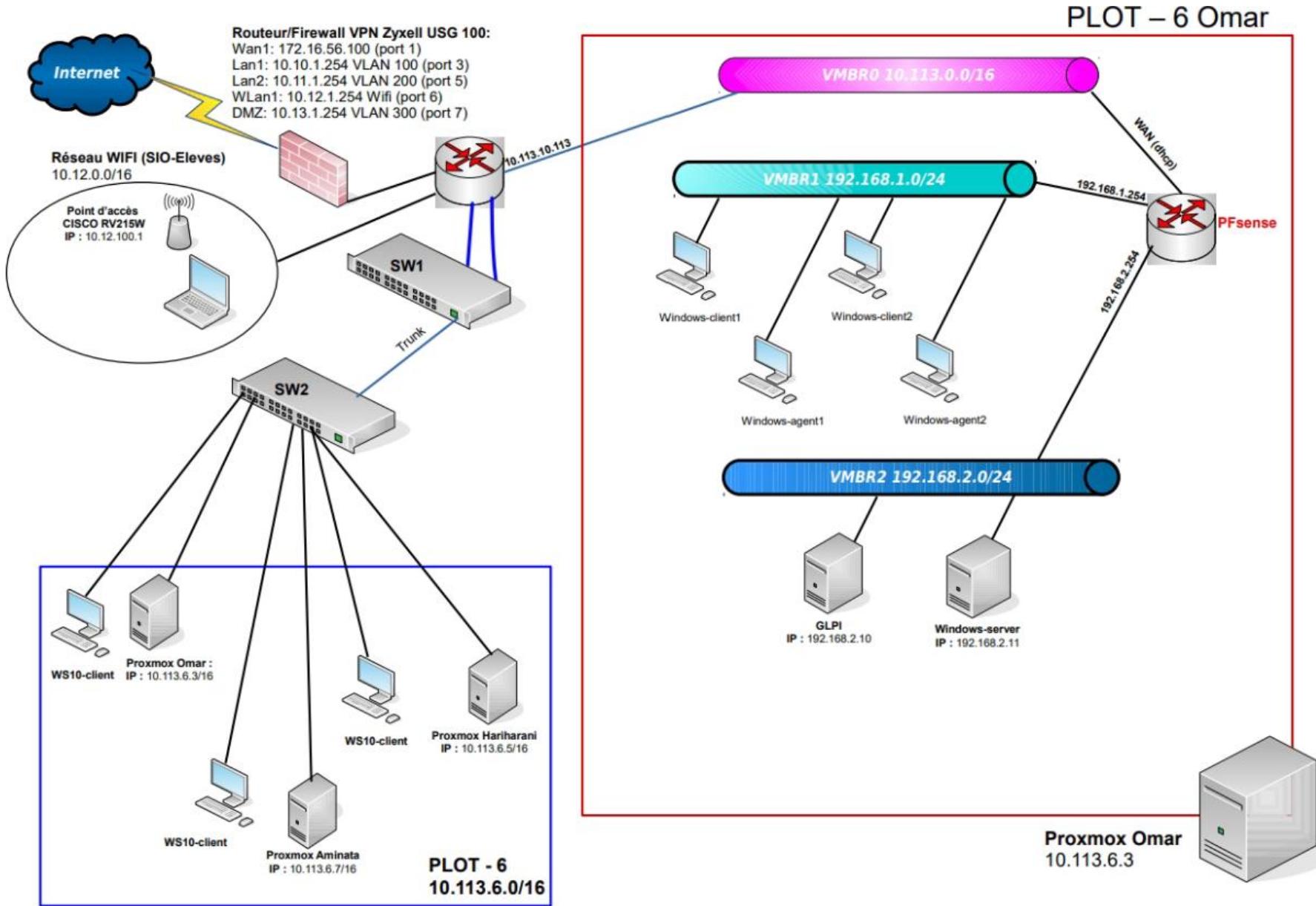
| @réseau | @passerelle | NIC | Machine/rôle | Plages d'adresses attribuables (DHCP) |
|----------------|--------------------|-------|---|---------------------------------------|
| 10.113.6.0/16 | 10.113.6.10 | VMBR0 | WAN accès vers l'extérieur | Pas de config DHCP |
| 192.168.1.0/24 | 192.168.1.254/24 | VMBR1 | Toutes les machines clientes | 192.168.1.21 à 192.168.1.253 |
| 192.168.2.0/24 | 192.168.2.254/24 | VMBR2 | Server GLPI :192.168.2.10 WINDOWS SERVER: 192.168.2.11 | |

Liste des machines

| Nom | ID | OS | Comptes | Stockage | RAM | CPU | NIC @MAC | Réseau | Services/Remarques |
|--------------------------------|-------|------------------------|-------------------------------------|----------|-----|--------------------------|---|-------------------------|---|
| Windows-Client1 | MV100 | Windows 10 | Diffère selon les user. Labo-113 | 32Go | 4Go | 2 processeurs 2 cœurs | BC:24:11:C9:8A:06 | VMBR1 | |
| Windows-Client2 | MV101 | Windows 10 | Diffère selon les user. Labo-113 | 32Go | 4Go | 2 processeurs 2 cœurs | BC:24:11:53:C9:A5 | VMBR1 | |
| Windows-Agent2 | MV102 | Windows 10 | Agent2 Labo-113 | 32Go | 4Go | 2 processeurs 2 cœurs | BC:24:11:B3:E6:94 | VMBR1 | |
| Windows-Agent1 | MV104 | Windows 10 | Agent1 Labo-113 | 32Go | 4Go | 2 processeurs 2 cœurs | BC:24:11:1B:88:35 | VMBR1 | |
| PFsense | MV105 | pfSense-CE-2.7.2 | admin pfsense | 32Go | 2Go | 2 processeurs 2 cœurs | BC:24:11:DA:E4:C9 BC:24:11:45:AB:6A BC:24:11:E7:B9:19 | VMBR0 VMBR1 VMBR2 | Em0 : DHCP - WAN Em1 : 192.168.1.254/24 Em2 : 192.168.2.254/24 |
| GLPI 192.168.2.10 | MV106 | Debian 12.7.0 | GLPI-OCS Labo-113 | 32Go | 4Go | 2 processeurs 2 cœurs | BC:24:11:B6:E2:0C | VMBR2 | |
| Windows-Server 192.168.2.11 | MV108 | Windows server 2019 | Omar/Administrateur Labo-113 | 32Go | 4Go | 2 processeurs 2 cœurs | BC:24:11:64:56:6C | VMBR1 | |



Schéma de l'infrastructure virtuelle



| | | | |
|--|---|--|-----------|
| | Hariharani THEIVENDRAM, Aminata THIAM, Omar SISSOKO | | |
| | Livrable - intégrale | | 2024-2025 |

2.2.2. Hariharani

Plan d'adressage

| @réseau | @passerelle | NIC | Machine/rôle | Plages d'adresses attribuables (DHCP) |
|-----------------|---------------------------|---------------------|--|--|
| 10.113.0.0/16 | Attribuer par DHCP | VMBR0 WAN | WAN accès vers l'extérieur | Config DHCP |
| 192.168.16.0/24 | 192.168.16.254/24 | VMBR1 IT | Interface graphique : http://192.168.16.254/ | Config DHCP 192.168.16.1 à 192.168.16.253 |
| 192.168.17.0/24 | 192.168.17.254/24 | VMBR2 SRV | Interface graphique : http://192.168.17.254/ SRV-Snort : 192.168.17.5 SRV-Prometheus : 192.168.17.10 SRV-Nessus : 192.168.17.15 SRV-Fail2ban : 192.168.17.20 SRV-LAMP-GLPI-BackupManager : 192.168.17.25 | Config DHCP 192.168.17.1 à 192.168.17.253 |
| 192.168.18.0/24 | 192.168.18.254/24 | VMBR3 TP | Interface graphique : http://192.168.18.254/ WS16-AD-tp : 192.168.18.10 | Config DHCP 192.168.18.1 à 192.168.18.253 |

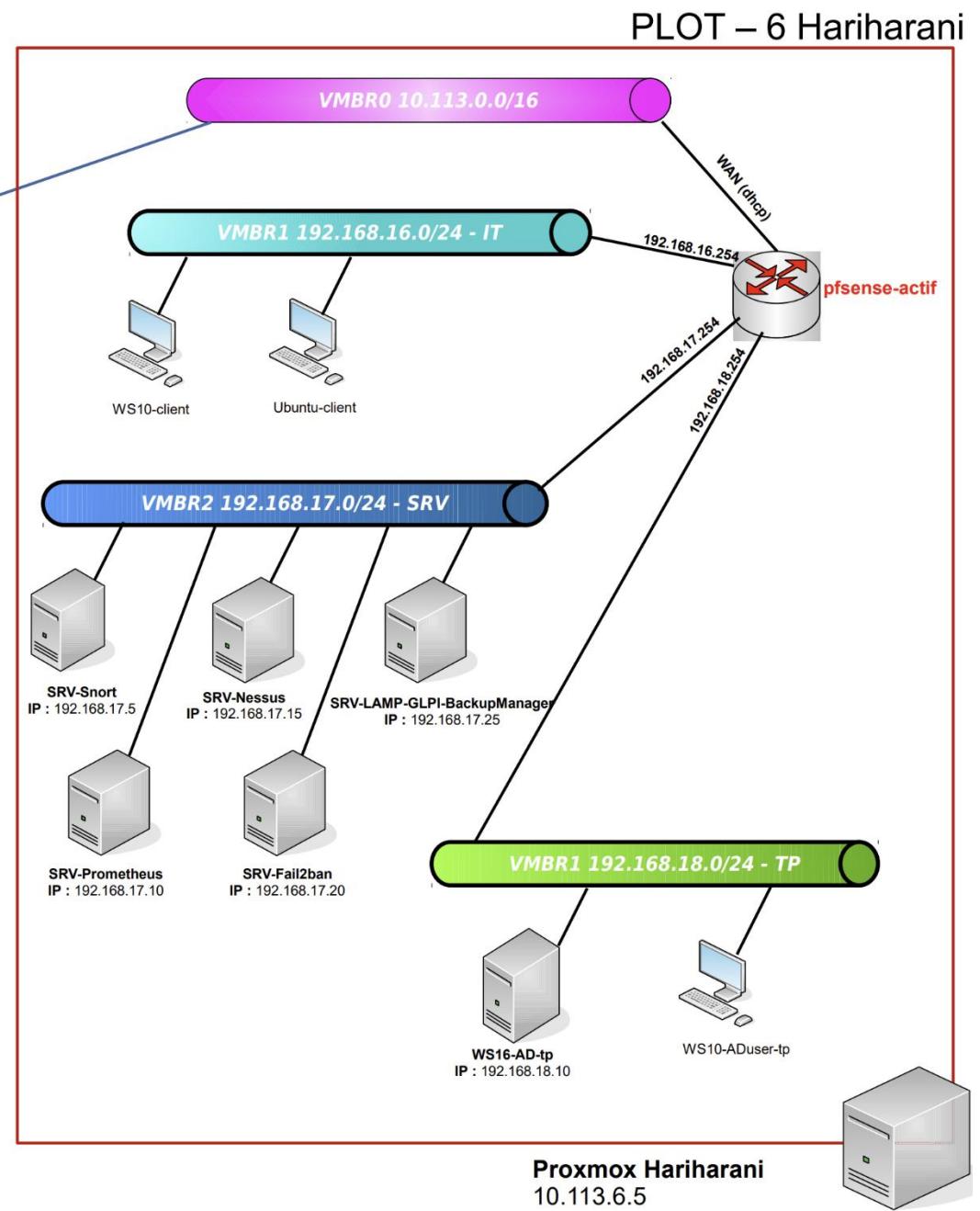
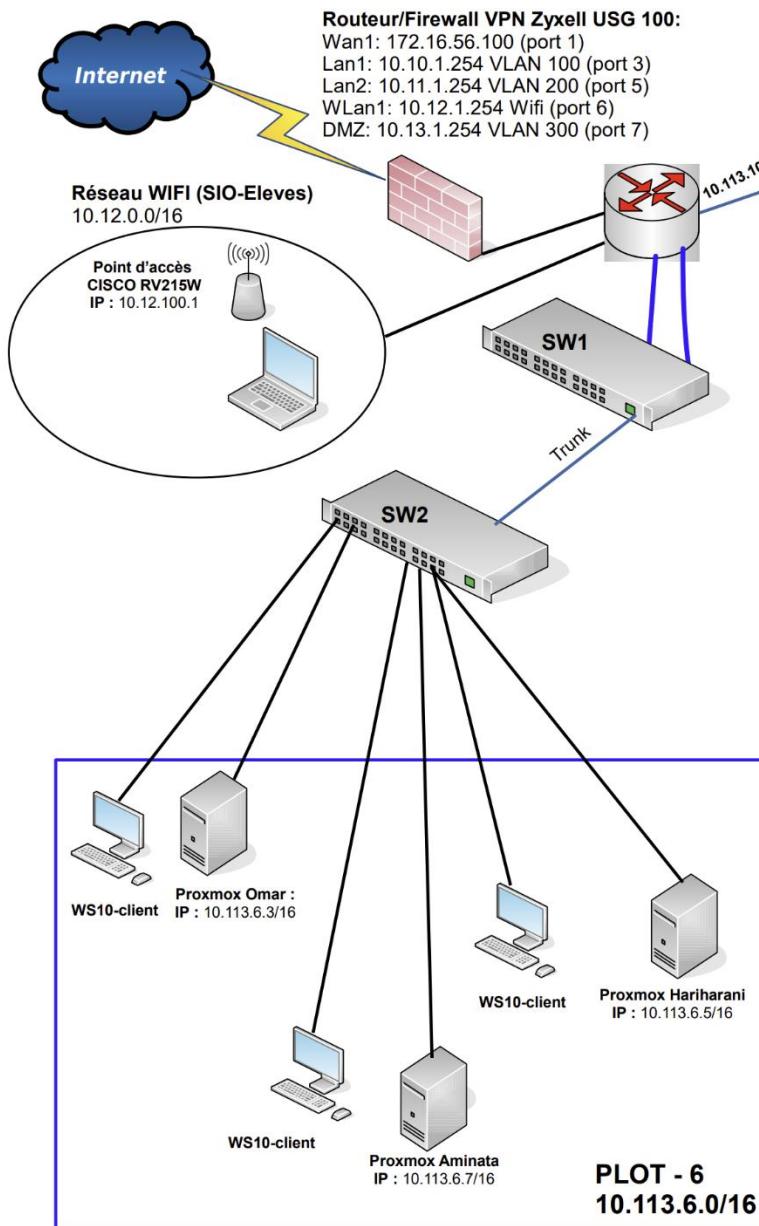
| | | |
|--|---|-----------|
| | Hariharani THEIVENDRAM, Aminata THIAM, Omar SISSOKO | |
| | Livrable - intégrale | 2024-2025 |

Liste des machines

| Nom | ID | OS | Comptes | Stockage | RAM | CPU | NIC @MAC | Réseau | Services/Remarques |
|--|-------|---------------------|--|----------|-----|---------------------------|--|----------------------------------|--|
| PfSense - actif 192.168.16.0/24 | MV200 | Pfsense 2.7.2 | Admin Labo-113 <i>Portail captif</i> Osissoko Labo-113 | 20Go | 1Go | 1 processeur 1 cœurs | BC:24:11:09:A5:6F BC:24:11:90:D7:FD BC:24:11:86:70:09 BC:24:11:5E:8C:CA | VMBR0 VMBR1 VMBR2 VMBR3 | Em0 : DHCP - WAN Em1 : 192.168.16.254/24 - IT Em2 : 192.168.17.254/24 - SRV Em3 : 192.168.18.254/24 - TP |
| WS10-client DHCP - 192.168.16.0/24 | MV110 | Windows 10 | harani Labo-113 | 25Go | 1Go | 1 processeur 1 cœurs | BC:24:11:51:EC:B9 | VMBR1 | Administrateur systèmes et réseaux Node exporter installé |
| Ubuntu-client DHCP - 192.168.16.0/24 | MV120 | Ubuntu 24.04 | User Labo-113 | 20Go | 1Go | 1 processeur 1 cœurs | BC:24:11:B2:53:2E | VMBR1 | Administrateur systèmes et réseaux Node exporter installé |
| SRV-Snort 192.168.17.5/24 | MV201 | Ubuntu 24.04 | User Labo-113 | 20Go | 2Go | 1 processeurs 1 coeurs | BC:24:11:4D:43:46 | VMBR2 | - Installation de Snort |
| SRV-Prometheus 192.168.17.10/24 | MV202 | Ubuntu 24.04 | User Labo-113 | 20Go | 4Go | 1 processeur 1 cœurs | BC:24:11:DD:08:F4 | VMBR2 | - Installation Prometheus, Grafana, node exporter, AlertManager - Alert : espace disque faible (20%) |
| SRV-Nessus 192.168.17.15/24 | MV203 | Ubuntu 24.04 | User Labo-113 | 50Go | 4Go | 2 processeurs 2 cœurs | BC:24:11:DD:08:F4 | VMBR2 | |
| SRV-Fail2ban 192.168.17.20/24 | MV204 | Debian 12.7.0 | root Labo-113 harani Labo-113 | 15Go | 2Go | 2 processeurs 2 cœurs | BC:24:11:5F:F2:A9 | VMBR2 | Installation de Fail2ban, SSH, Web, Mail |
| SRV-LAMP-GLPI-BackupManager 192.168.17.25/24 | MV205 | Ubuntu 24.04 | harani Labo-113 | 32Go | 2Go | 1 processeur 1 cœur | BC:24:11:5F:F2:A9 | VMBR2 | Installation LAMP, GLPI, BackupManager |
| WS16-AD-tp 192.168.18.10/24 | MV101 | Windows server 2016 | admin -113Labo | 64Go | 2Go | 1 processeur 1 cœur | BC:24:11:5E:A2:86 | VMBR3 | - Création OU=France, OU=Régions, OU=Départements - Création users + sessions |
| WS10-ADuser-tp DHCP - 192.168.18.0/24 | MV102 | Windows 10 | \$User Labo-113 (Adeline DAVID) | 25Go | 1Go | 1 processeur 1 cœurs | BC:24:11:0B:F9:07 | VMBR3 | - |



Schéma de l'infrastructure virtuelle



| | | | |
|--|---|--|-----------|
| | Hariharani THEIVENDRAM, Aminata THIAM, Omar SISSOKO | | |
| | Livrable - intégrale | | 2024-2025 |

2.2.3. Aminata

Plan d'adressage

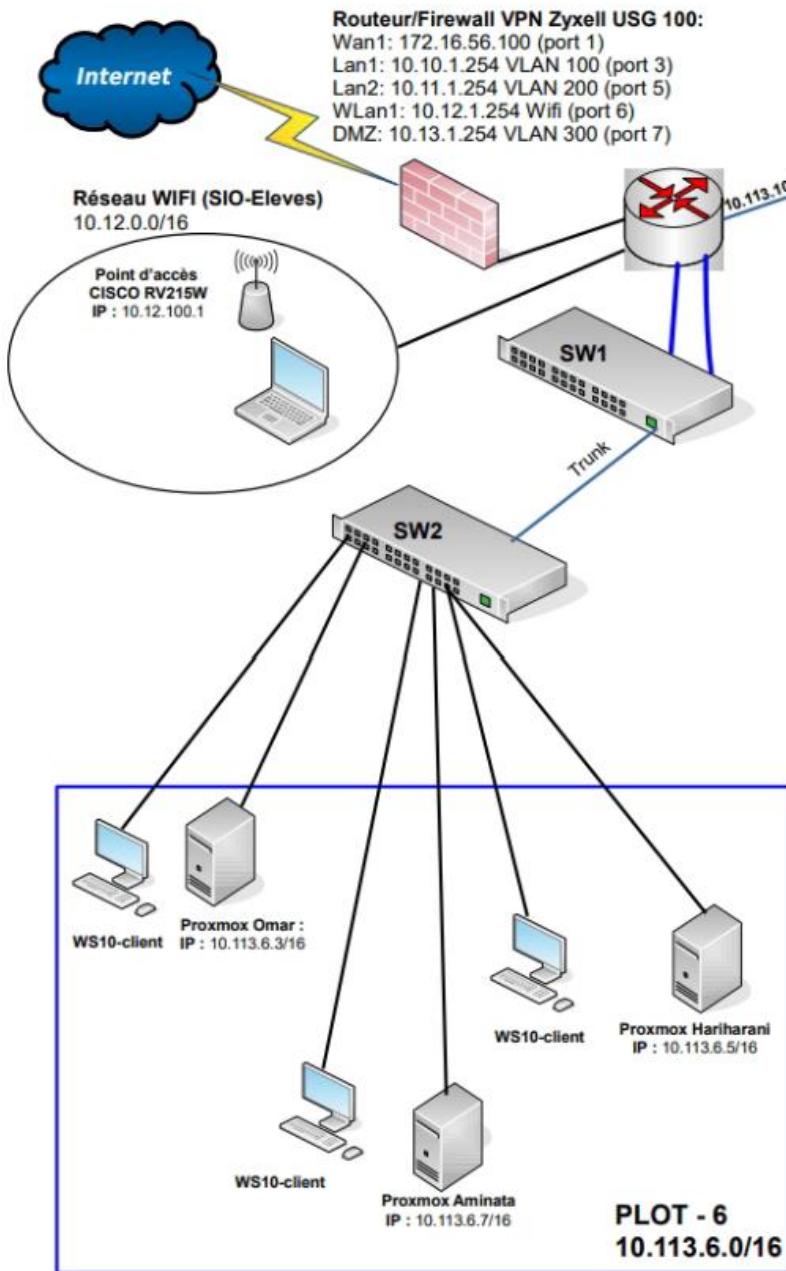
| @réseau | | @passerelle | NIC | Machine/rôle | Plages d'adresses attribuables (DHCP) |
|-----------------|--|--------------------|--------------|---|---------------------------------------|
| 10.113.6.0/16 | | 10.113.6.12 | VMBR0 | WAN accès vers l'extérieur | Pas de config DHCP |
| 192.168.31.0/24 | | 192.168.31.254 | VMBR1 IT | Machine cliente | DHCP 192.168.31.1 à 192.168.31.253 |
| 192.168.32.0/24 | | 192.168.32.254 | VMBR2 SRV | Ubu-Backup : 192.168.32.5 Serv-GLPI-LAMP : 192.168.32.10 Win-AD : 192.168.32.15 | DHCP 192.168.32.1 à 192.168.32.253 |

Liste des machines

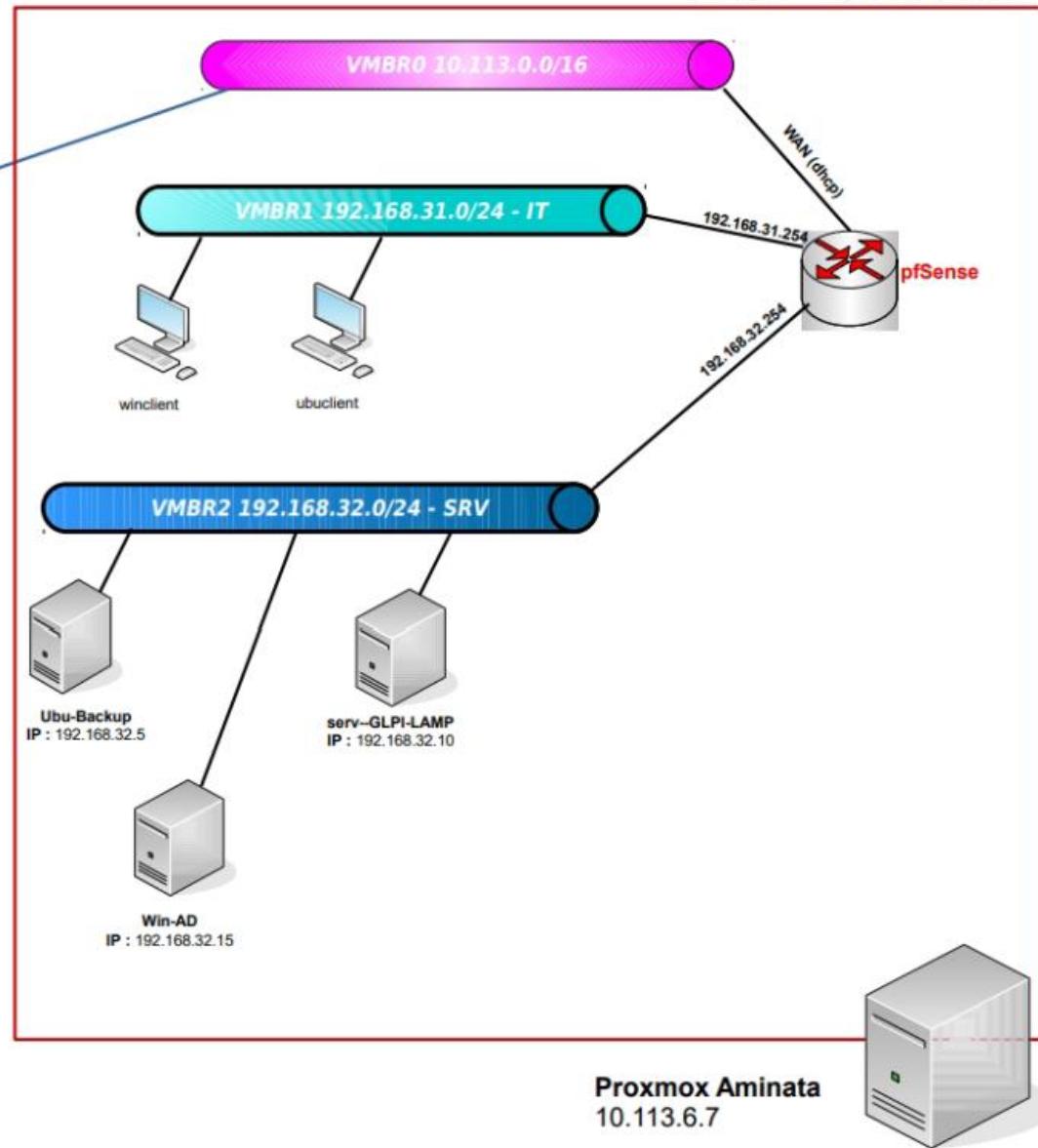
| Nom | ID | OS | Comptes | Stockage | RAM | CPU | NIC @MAC | Réseau | Services/Remarques |
|--|-------|-------------------|----------------------------|----------|-----|--------------------------|---|------------------------------------|--|
| Ubu-Backup 192.168.32.5 | MV100 | Ubuntu 24.04 | User Labo-113 | 32Go | 2Go | 1 processeur 1 cœur | BC:24:11:F9:ED:90 | VMBR2 | |
| winclient | MV101 | Windows 10 | | 36Go | 2Go | 1 processeur 1 cœur | BC:24:11:EC:12:7E | VMBR1 | |
| Serv-GLPI-LAMP 192.168.32.10 | MV102 | Ubuntu 24.04 | Root Labo-113 | 32Go | 2Go | 1 processeur 1 cœur | BC:24:11:50:29:13 | VMBR2 | |
| Ubuclient | MV103 | Ubuntu 24.04 | Root Labo-113 | 20Go | 2Go | 1 processeur 1 cœur | BC:24:11:C4:50:FB | VMBR1 | |
| Win-AD 192.168.32.15 | MV104 | Windows server 22 | Administrateur labo-113 | 32Go | 4Go | 2 processeurs 2 cœurs | BC:24:11:13:96:F6 | VMBR2 | |
| pfSense | MV105 | Pfsense 7.2.0 | Admin Labo-113 | 20Go | 1Go | 1 processeur 1 cœur | BC:24:11:EC:7C:0F BC:24:11:A0:D0:5D BC:24:11:CE:76:66 | VMBR0 VMBR1 - IT VMBR2 - SRV | DHCP 192.168.31.254/16 192.168.32.254/16 |



Schéma de l'infrastructure virtuelle



PLOT – 6 Aminata





3. Planning

3.1. Trello et la méthode Kanban

Trello est un outil de gestion de projet en ligne basé sur la méthode **Kanban**, qui permet d'organiser et de suivre les tâches de manière visuelle. Il fonctionne sous forme de **tableaux**, contenant des **listes** dans lesquelles on déplace des **cartes** représentant les différentes tâches à accomplir.

The screenshot shows a Trello board titled "PLOT 6" with the following columns:

- Backlog**: Contains tasks like "Fail2ban" (0/11), "architecture personnel de votre proxmox" (0/1), and "Wireguard" (0/14).
- TO DO**: Contains tasks like "GLPI" (0/4) and "Assemblage des livrables" (85/88).
- Work in progress**: Contains tasks like "Prometheus + grafana" (14/23) and "BackupManager" (14/14).
- Verify**: Contains tasks like "Snort" (11/11), "Nessus" (10/10), and "BackupManager" (14/14).
- Done**: Contains tasks like "PfSense" (15/15), "Veracrypt" (11/11), "LAMP" (13/13), and "GLPI" (13/13).

The "Verify" column is expanded to show the details of the "Veracrypt" task. The right-hand panel shows the task details for "Veracrypt" with the following checklist:

- Installation**: Progress 100% (green bar). Items: "Masquer les tâches cochées", "Supprimer".
- Livrable**: Progress 100% (green bar). Items: "Masquer les tâches cochées", "Supprimer".

Below these, there is a "Power-Ups" section with items like "Ajouter des Power-ups", "Automatisation", and "Actions".



3.2. Méthode Kanban (ou Kanboard) :

C'est une approche **agile** qui vise à optimiser le flux de travail en visualisant les tâches et en limitant le travail en cours. Elle repose sur trois principes :

1. **Visualiser le travail** – Grâce aux cartes et aux colonnes, on voit en un coup d'œil l'état d'avancement des tâches.
2. **Limiter le travail en cours** – Pour éviter la surcharge, on définit un nombre maximum de tâches en cours par colonne.
3. **Optimiser le flux** – On identifie et élimine les blocages pour fluidifier le processus.

3.3. Mise au point - Discord

Dans notre équipe, nous avons instauré un rythme de **mises au point régulières** pour assurer un bon suivi de notre projet. Chaque **lundi, mercredi et vendredi à 20h**, nous nous retrouvions sur **Discord** pour faire le point sur l'avancement des tâches, discuter des éventuels blocages et ajuster nos priorités. Ces réunions nous permettaient de **coordonner nos efforts**, de clarifier les objectifs et de garantir une progression fluide et efficace. Grâce à cet échange fréquent, nous avons pu maintenir une bonne dynamique de travail et favoriser la collaboration entre les membres de l'équipe.

3.4. Délais et Planning

- **Phase 1 :** Analyse des besoins et étude de faisabilité (3 jours)
- **Phase 2 :** Installation et configuration des solutions (5 mois)
- **Phase 3 :** Tests et validation (1 mois)
- **Phase 4 :** Déploiement et mise en production (1 mois)
- **Phase 5 :** Maintenance et optimisation continue



4. Outils

1. GLPI (Gestionnaire libre de parc informatique)

- **Description** : GLPI est un logiciel de gestion de parc informatique et de gestion de services. Il permet de gérer les équipements informatiques, les demandes d'assistance (helpdesk), les incidents, ainsi que la gestion des licences et des contrats.
- **Utilisation** : Il est utilisé par les équipes IT pour suivre l'inventaire matériel, gérer les tickets de support et les demandes des utilisateurs, ainsi que pour la gestion de la maintenance.

2. GLPI Agent

- **Description** : L'agent GLPI est un logiciel qui s'installe sur les machines pour permettre à GLPI de collecter des informations détaillées sur le matériel et le logiciel des machines distantes.
- **Utilisation** : Il est utilisé pour l'inventaire automatique des équipements et la gestion des informations système à distance, facilitant la mise à jour de l'inventaire dans GLPI.

3. VeraCrypt

- **Description** : VeraCrypt est un logiciel de chiffrement de disque open source qui permet de créer des volumes cryptés ou de chiffrer des partitions et disques entiers.
- **Utilisation** : Utilisé pour sécuriser les données sensibles en les chiffrant, VeraCrypt est souvent utilisé pour protéger les informations personnelles ou professionnelles sur des supports de stockage.

4. pfSense

- **Description** : pfSense est un système d'exploitation open source basé sur FreeBSD qui transforme une machine en un pare-feu et routeur très puissant et configurable.
- **Utilisation** : Utilisé principalement pour sécuriser les réseaux, pfSense permet de mettre en place des VPN, de gérer des règles de pare-feu, de faire du routage et de la surveillance de trafic.

5. Portail Captif

- **Description** : Un portail captif est une page web qui apparaît lorsqu'un utilisateur tente d'accéder à un réseau Wi-Fi public ou privé. Avant de pouvoir naviguer, l'utilisateur doit s'authentifier ou accepter des conditions.
- **Utilisation** : Utilisé dans les hôtels, aéroports, et autres lieux publics pour contrôler l'accès au réseau Wi-Fi, souvent en demandant une authentification ou en affichant un message d'avertissement.



6. Prometheus

- **Description :** Prometheus est un système open source de surveillance et d'alerte, principalement utilisé pour collecter et stocker des métriques sous forme de séries temporelles.
- **Utilisation :** Principalement utilisé pour surveiller des systèmes et des applications. Il récupère des métriques via des "exporters" et peut alerter en cas de seuils critiques dépassés.

7. Grafana

- **Description :** Grafana est un outil de visualisation de données open source qui se connecte à diverses bases de données et sources de métriques pour créer des dashboards interactifs et visuellement attractifs.
- **Utilisation :** Utilisé pour visualiser les données collectées par des outils comme Prometheus, afin de mieux comprendre l'état des systèmes et applications.

8. Node Exporter

- **Description :** Node Exporter est un exportateur de métriques système pour Prometheus. Il collecte des métriques sur le système d'exploitation comme l'utilisation du CPU, de la mémoire, du disque, etc.
- **Utilisation :** Il est utilisé pour collecter des informations détaillées sur les machines qui seront ensuite utilisées par Prometheus pour le monitoring.

9. Alertmanager

- **Description :** Alertmanager est un composant de Prometheus qui gère les alertes. Il prend les alertes envoyées par Prometheus et les dirige vers les destinataires (email, Slack, etc.), les regroupant et les envoyant de manière ordonnée.
- **Utilisation :** Utilisé pour gérer les alertes et les notifications, permettant aux équipes de répondre rapidement aux incidents.

10. Nessus

- **Description :** Nessus est un scanner de vulnérabilité. Il permet d'identifier les failles de sécurité dans les systèmes, les applications et les réseaux.
- **Utilisation :** Il est utilisé pour effectuer des audits de sécurité, détecter des vulnérabilités et assurer la conformité des systèmes.



11. Snort

- **Description** : Snort est un système de détection et de prévention d'intrusion (IDS/IPS) open source, qui analyse le trafic réseau pour détecter des attaques potentielles.
- **Utilisation** : Utilisé pour surveiller et analyser les flux réseau en temps réel afin de détecter des comportements suspects ou des attaques.

12. Fail2ban

- **Description** : Fail2ban est un logiciel qui protège les serveurs en bloquant les adresses IP après plusieurs tentatives de connexion échouées.
- **Utilisation** : Utilisé principalement pour se défendre contre les attaques par force brute, notamment sur des services comme SSH, FTP, etc.

13. BackupManager

- **Description** : BackupManager est un outil de gestion des sauvegardes qui permet de planifier, exécuter et restaurer des sauvegardes de données.
- **Utilisation** : Utilisé pour assurer la sécurité des données en créant des copies de sauvegarde régulières, permettant la récupération en cas de perte de données.

14. LAMP (Linux, Apache, MySQL, PHP)

- **Description** : LAMP est une pile logicielle open source composée de Linux (système d'exploitation), Apache (serveur web), MySQL (base de données) et PHP (langage de script).
- **Utilisation** : Utilisée pour héberger des applications web et des sites dynamiques. C'est une des configurations les plus courantes pour le développement web.

15. WireGuard

- **Description** : WireGuard est un protocole VPN moderne et rapide qui utilise des clés publiques et privées pour sécuriser les communications entre les clients et les serveurs.
- **Utilisation** : Utilisé pour établir des connexions VPN sécurisées et rapides entre des utilisateurs ou des serveurs, tout en étant simple à configurer par rapport aux autres solutions VPN.



1. Inventaire avec GLPI + GLPI agent

1.1. Cahier des charges

1.1.1. Contexte et Objectifs

Contexte

Dans le cadre de l'amélioration de la gestion des services informatiques de l'entreprise, nous avons pour objectif de déployer GLPI et son agent sur l'ensemble des équipements. Cette initiative vise à centraliser la gestion des actifs, des incidents et des demandes, tout en assurant un suivi efficace et une optimisation des ressources IT. Ce projet contribuera à renforcer la transparence, la traçabilité et la performance des processus informatiques.

Objectif

- Centraliser la gestion des équipements informatiques.
- Suivre efficacement les incidents et les demandes.
- Optimiser les ressources IT.
- Faciliter la coordination entre les équipes.
- Améliorer la traçabilité des processus.

1.1.2. Descriptions fonctionnelles des besoins

- Server Proxmox pour mettre en place notre projet
- Appel tous les jours à partir de 21h30
- Intégration agent avec server GLPI
- Documentation Technique
- Gérer les incidents et les demandes de manière centralisée.
- Planifier et suivre les opérations de maintenance.

1.1.3. Cahier des charges technique

- Installation du server GLPI
- Installation d'un client GLPI sur lequel on pourra envoyer des inventaires à notre server.
- Installation de pfSense et configuration des connexion réseau avec notre server et nos clients

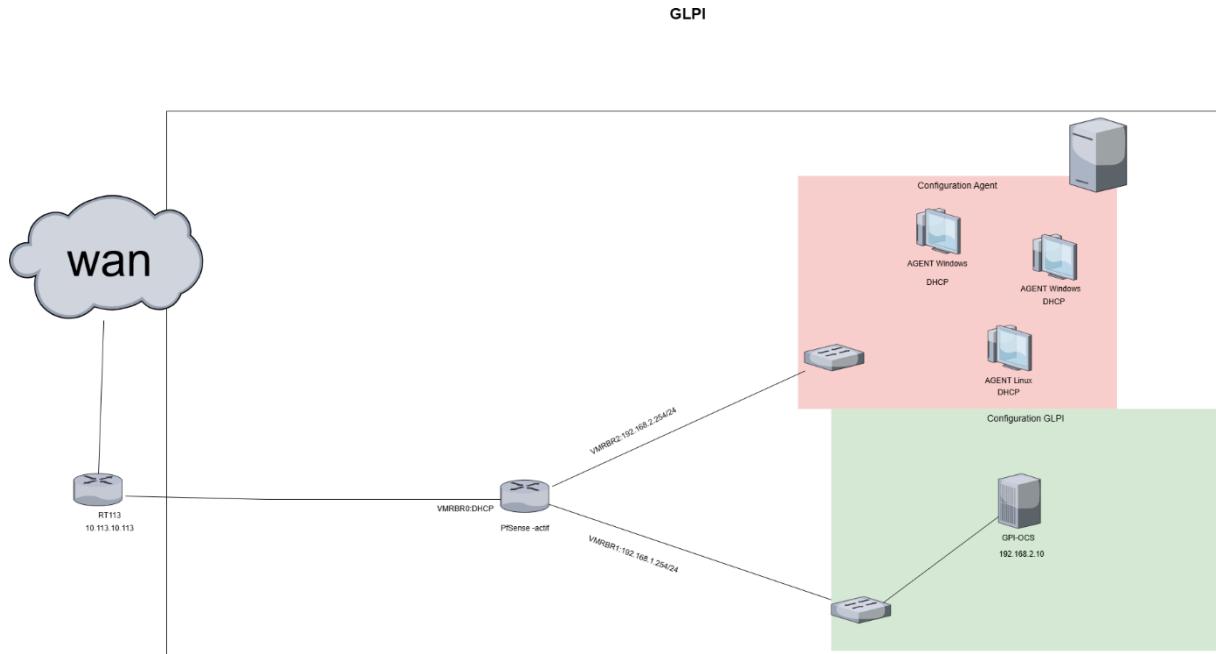
1.1.4. Planning prévisionnel

| Tâche | Durée |
|--|---------|
| Installation Lamp(Linux, Apache,Mariadb,Php) | 1 jour |
| Installation server GLPI | 1 jour |
| Installation agent GLPI | 2 jours |
| Installation Pfsense | 2 jours |

1.2. Plan d'adressage

| @réseau | @passerelle | NIC | Machine/rôle | Config plage (DHCP) |
|----------------|--------------------|-------|----------------------------|---------------------|
| 10.113.6.0/16 | 10.113.6.10 | VMBR0 | WAN accès vers l'extérieur | Pas de config DHCP |
| 192.168.1.0/24 | 192.168.1.254/24 | VMBR1 | Server GLPI :192.168.2.10 | Config DHCP |
| 192.168.2.0/24 | 192.168.2.254/24 | VMBR2 | Agent GLPI : DHCP | Config DHCP |

1.3. Schéma réseau





1.4. Documentation technique

Mise à jour du système

Avant d'installer tout logiciel, il est recommandé de mettre à jour les paquets du système :
sudo apt update && sudo apt upgrade -y

Installer les paquets du socle LAMP : Linux Apache2 MariaDB PHP. Sous Debian 12, qui est la dernière version stable de Debian, PHP 8.2

sudo apt-get install apache2 php mariadb-server

Installer toutes les extensions nécessaires au bon fonctionnement de GLPI.

sudo apt-get install php-xml php-common php-json php-mysql php-mbstring php-curl php-gd
php-intl php-zip php-bz2 php-imap php-apcu

Si vous envisagez d'associer GLPI avec un annuaire LDAP comme l'Active Directory, vous devez installer l'extension LDAP de PHP.

sudo apt-get install php-ldap

1.4.1. Installation en ligne de commande

Préparer une base de données pour GLPI

Préparer MariaDB pour qu'il puisse héberger la base de données de GLPI

sudo mysql_secure_installation

```
Setting the root password or using the unix_socket ensures that nobody
can log into the MariaDB root user without the proper authorisation.
You already have your root account protected, so you can safely answer 'n'.
Switch to unix_socket authentication [Y/n] n
... skipping.

You already have your root account protected, so you can safely answer 'n'.
Change the root password? [Y/n] y
New password:
Re-enter new password:
Password updated successfully!
Reloading privilege tables...
... Success!

By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them. This is intended only for testing, and should be removed
before moving into a
production environment.
Remove anonymous users? [Y/n] y
... Success!

Normally, root should only be allowed to connect from 'localhost'. This
ensures that someone cannot guess at the root password from the network.
Disallow root login remotely? [Y/n] y
... Success!

By default, MariaDB comes with a database named 'test' that anyone can
access. This is also intended only for testing, and should be removed
before moving into a production environment.
Remove test database and access to it? [Y/n] y
... Success!
- Removing privileges on test database...
... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.
Reload privilege tables now? [Y/n] y
... Success!

Cleaning up...

All done! If you've completed all of the above steps, your MariaDB
installation should now be secure.

Thanks for using MariaDB!
```

Créer une base de données dédiée pour GLPI et celle-ci sera accessible par un utilisateur dédié.

sudo mysql -u root -p



Puis, nous allons exécuter les requêtes SQL ci-dessous pour créer la base de données "db23_glpi" ainsi que l'utilisateur "glpi_adm" avec le mot de passe "Labo-113"

```
CREATE DATABASE db23_glpi;
GRANT ALL PRIVILEGES ON db23_glpi.* TO glpi_adm@localhost IDENTIFIED BY "Labo-113";
FLUSH PRIVILEGES;
EXIT
```

Télécharger GLPI et préparer son installation

La prochaine étape consiste à télécharger l'archive ".tgz" qui contient les sources d'installation de GLPI. A partir du GitHub de GLPI, récupérez le lien vers la dernière version. Ici, c'est la version GLPI 10.0.10 qui est installée.

[GitHub de GLPI](#)

L'archive sera téléchargée dans le répertoire "/tmp" :

```
cd /tmp
wget https://github.com/glpi-project/glpi/releases/download/10.0.10/glpi-10.0.10.tgz
```

Exécuter la commande ci-dessous pour décompresser l'archive .tgz dans le répertoire "/var/www/", ce qui donnera le chemin d'accès "/var/www/glpi" pour GLPI.

```
sudo tar -xvf glpi-10.0.10.tgz -C /var/www/
Nous allons définir l'utilisateur "www-data" correspondant à Apache2, en tant que propriétaire sur les fichiers GLPI.
```

```
sudo chown www-data /var/www/glpi/ -R
```

Créer plusieurs dossiers et sortir des données de la racine Web (/var/www/glpi) de manière à les stocker dans les nouveaux dossiers que nous allons créer. Ceci va permettre de faire une installation sécurisée de GLPI, qui suit les recommandations de l'éditeur.

Le répertoire /etc/glpi

Créer le répertoire "/etc/glpi" qui va recevoir les fichiers de configuration de GLPI. Nous donnons des autorisations à www-data sur ce répertoire car il a besoin de pouvoir y accéder.

```
sudo mkdir /etc/glpi
sudo chown www-data /etc/glpi/
```

Déplacer le répertoire "config" de GLPI vers ce nouveau dossier :

```
sudo mv /var/www/glpi/config /etc/glpi
```

Le répertoire /var/lib/glpi

Répétons la même opération avec la création du répertoire "/var/lib/glpi" :



```
sudo mkdir /var/lib/glpi
sudo chown www-data /var/lib/glpi/
```

Dans lequel nous déplaçons également le dossier "files" qui contient la majorité des fichiers de GLPI : CSS, plugins, etc.

```
sudo mv /var/www/glpi/files /var/lib/glpi
Le répertoire /var/log/glpi
```

Terminons par la création du répertoire "/var/log/glpi" destiné à stocker les journaux de GLPI. Toujours sur le même principe :

```
sudo mkdir /var/log/glpi
sudo chown www-data /var/log/glpi
!!Nous n'avons rien à déplacer dans ce répertoire !!
```

Créer les fichiers de configuration

Nous devons configurer GLPI pour qu'il sache où aller chercher les données. Autrement dit, nous allons déclarer les nouveaux répertoires fraîchement créés.

```
sudo nano /var/www/glpi/inc/downstream.php
```

Afin d'ajouter le contenu ci-dessous qui indique le chemin vers le répertoire de configuration :

```
<?php
define('GLPI_CONFIG_DIR', '/etc/glpi/');
if (file_exists(GLPI_CONFIG_DIR . '/local_define.php')) {
require_once GLPI_CONFIG_DIR . '/local_define.php';
}
```

Ensuite, nous allons créer ce second fichier :

```
sudo nano /etc/glpi/local_define.php
```

Pour déclarer deux variables qui spécifient les chemins vers les répertoires 'files' et 'log' que nous avons préparés précédemment, ajoutez le contenu suivant.

```
<?php
define('GLPI_VAR_DIR', '/var/lib/glpi/files');
define('GLPI_LOG_DIR', '/var/log/glpi');
```

Préparer la configuration Apache2

Pour configurer le serveur web Apache2 en vue d'installer GLPI, vous devez créer un fichier de configuration spécifique pour un VirtualHost. Dans cet exemple, le fichier est nommé "support.it-connect.tech.conf", en référence au domaine choisi pour accéder à GLPI : support.it-connect.tech.. Idéalement, il est préférable d'utiliser un nom de domaine (même interne) pour accéder à GLPI, ce qui permettra ensuite d'installer un certificat SSL pour sécuriser la connexion. Cela garantit une configuration optimale et sécurisée pour l'accès à l'application GLPI.



```
sudo nano /etc/apache2/sites-available/support.it-connect.tech.conf
```

```
<VirtualHost *:80>
    ServerName support.it-connect.tech
    DocumentRoot /var/www/glpi/public
    # If you want to place GLPI in a subfolder of your site (e.g. your virtual host is serving multiple
    # applications),
    # you can use an Alias directive. If you do this, the DocumentRoot directive MUST NOT target the
    # GLPI directory itself.
    # Alias "/glpi" "/var/www/glpi/public"

    <Directory /var/www/glpi/public>
        Require all granted
        RewriteEngine On # Redirect
        all requests to GLPI router, unless file exists.
        RewriteCond %{REQUEST_FILENAME} !-f
        RewriteRule ^(.*)$ index.php [QSA,L]
    </Directory>

</VirtualHost>
```

Puis, nous allons **activer ce nouveau site dans Apache2** :

```
sudo a2ensite support.it-connect.tech.conf
```

Désactiver le site par défaut car il est inutile :

```
sudo a2dissite 000-default.conf
```

Activer le module "rewrite" (pour les règles de réécriture) car on l'a utilisé dans le fichier de configuration du VirtualHost (*RewriteCond / RewriteRule*).

```
sudo a2enmod rewrite
```

Redémarrer le service Apache2 :

```
sudo systemctl restart apache2
```

Utilisation de PHP8.2-FPM avec Apache2

Pour utiliser PHP avec Apache2, deux options sont possibles : intégrer PHP directement avec le module Apache2 (libapache2-mod-php8.2) ou opter pour PHP-FPM. Ce dernier est recommandé pour ses meilleures performances et son fonctionnement en tant que service indépendant, contrairement à l'exécution par chaque processus Apache2 dans l'autre mode. Si vous choisissez PHP-FPM, commencez par installer PHP8.2-FPM. Sinon, assurez-vous de configurer l'option "session.cookie_httponly".

Installer PHP8.2-FPM avec la commande suivante :

```
sudo apt-get install php8.2-fpm
```



Nous allons activer deux modules dans Apache et la configuration de PHP-FPM, avant de recharger Apache2 :

```
sudo a2enmod proxy_fcgi setenvif
sudo a2enconf php8.2-fpm
sudo systemctl reload apache2
```

Configurer PHP-FPM pour Apache2, nous n'allons pas éditer le fichier "/etc/php/8.2/apache2/php.ini" mais plutôt ce fichier :

```
sudo nano /etc/php/8.2/fpm/php.ini
```

Recherchez l'option "**session.cookie_httponly**" et indiquez la valeur "on" pour l'activer, afin de protéger les cookies de GLPI (Faites ctrl W et copier-coller le début du script pour être plus rapide).

```
; Whether or not to add the httpOnly flag to the cookie, which makes it
; inaccessible to browser scripting languages such as JavaScript.
; https://php.net/session.cookie-httponly
session.cookie_httponly = on
```

Pour appliquer les modifications, nous devons redémarrer PHP-FPM :

```
sudo systemctl restart php8.2-fpm.service
```

Nous devons modifier notre VirtualHost pour préciser à Apache2 que PHP-FPM doit être utilisé pour les fichiers PHP :

```
sudo nano /etc/apache2/sites-available/support.it-connect.tech.conf
```

Puis mettre en bas de directory

```
<FilesMatch \.php$> SetHandler "proxy:unix:/run/php/php8.2-fpm.sock|fcgi://localhost/"
</FilesMatch>
```

On redemare

```
sudo systemctl restart apache2
```

1.4.2. Installation graphique de GLPI

Placer notre addressee ip dans un navigateur



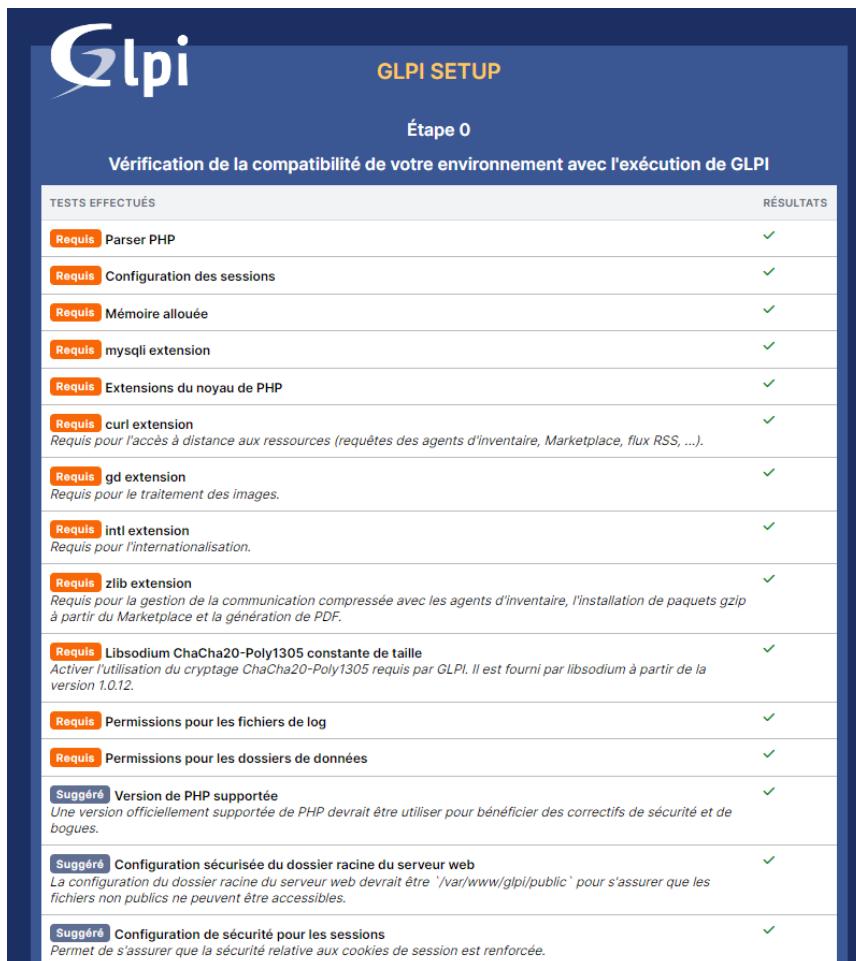


Mettre français



Nouvelle Installation donc Installer

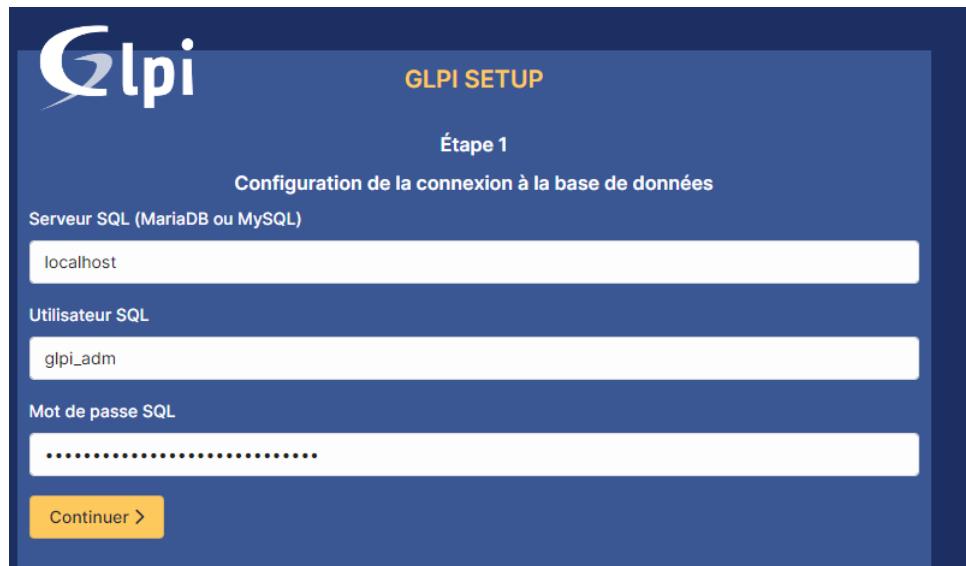
GLPI vérifie la configuration de notre serveur pour déterminer si tous les prérequis sont respectés. Tout est bon, donc nous pouvons continuer.



A l'étape suivante, nous devons renseigner les informations pour se connecter à la base de données. Nous indiquons "**localhost**" en tant que serveur SQL puisque MariaDB est installé en



local, sur le même serveur que GLPI. Puis, nous indiquons notre utilisateur "glpi_adm" et le mot de passe **Labo-113**.



GLPI SETUP

Étape 1

Configuration de la connexion à la base de données

Serveur SQL (MariaDB ou MySQL)

localhost

Utilisateur SQL

glpi_adm

Mot de passe SQL

.....

Continuer >

This screenshot shows the first step of the GLPI setup process, titled 'Étape 1 Configuration de la connexion à la base de données'. It asks for the database connection details: the server is set to 'localhost', the user is 'glpi_adm', and the password is masked as '.....'. A yellow 'Continuer >' button is at the bottom.

Après avoir cliqué sur "**Continuer**", nous devons choisir la base de données "**db23_glpi**" créée précédemment.



GLPI SETUP

Étape 2

Test de connexion à la base de données

✓ Connexion à la base de données réussie

Veuillez sélectionner une base de données :

Créer une nouvelle base ou utiliser une base existante :

db23_glpi

Continuer >

This screenshot shows the second step of the GLPI setup process, titled 'Étape 2 Test de connexion à la base de données'. It shows a success message 'Connexion à la base de données réussie'. It then asks to select a database, with 'db23_glpi' selected. A yellow 'Continuer >' button is at the bottom.

Suivez les dernières étapes



GLPI SETUP

Étape 3

Initialisation de la base de données.

OK - La base a bien été initialisée

Continuer >

This screenshot shows the third step of the GLPI setup process, titled 'Étape 3 Initialisation de la base de données'. It displays the message 'OK - La base a bien été initialisée'. A yellow 'Continuer >' button is at the bottom.



Cliquer sur Continuez



Tous est bon GLPI est installée 😊😊



Connexion à votre compte

Identifiant

Mot de passe

Source de connexion

 Se souvenir de moi

GLPI Copyright (C) 2015-2023 Teclib' and contributors

Mettre : glpi et encore glpi

The dashboard displays the following key statistics:

- Central:
 - Logiciel: 0
 - Ordinateur: 0
 - Matériel réseau: 0
 - Téléphone: 0
 - Licence: 0
 - Moniteur: 0
 - Bâle: 0
 - Imprimante: 0
- Autres données trouvées (Empty):
 - Autre donnée trouvée (Empty)
 - Autre donnée trouvée (Empty)
 - Autre donnée trouvée (Empty)
- Statuts des tickets par mois:
 - Ticket: 0
 - Tickets en retard: 0
 - Problème: 0
 - Changement: 0

Left sidebar menu:

- Chercher dans le menu
- Parc
- Assistance
- Gestion
- Outils
- Administration
- Configuration

Top right corner:

- Rechercher
- Super-Admin
- Entité racine (Arborescence)



1.4.3. Installation Agent GLPI

Installer le Setup Windows sur notre machine cliente Windows

GLPI Agent v1.13 (Latest)

Here you can download GLPI-Agent v1.13 packages.

Don't forget to follow our [installation documentation](#).

Windows

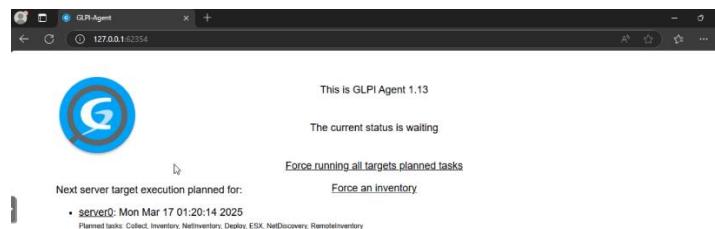
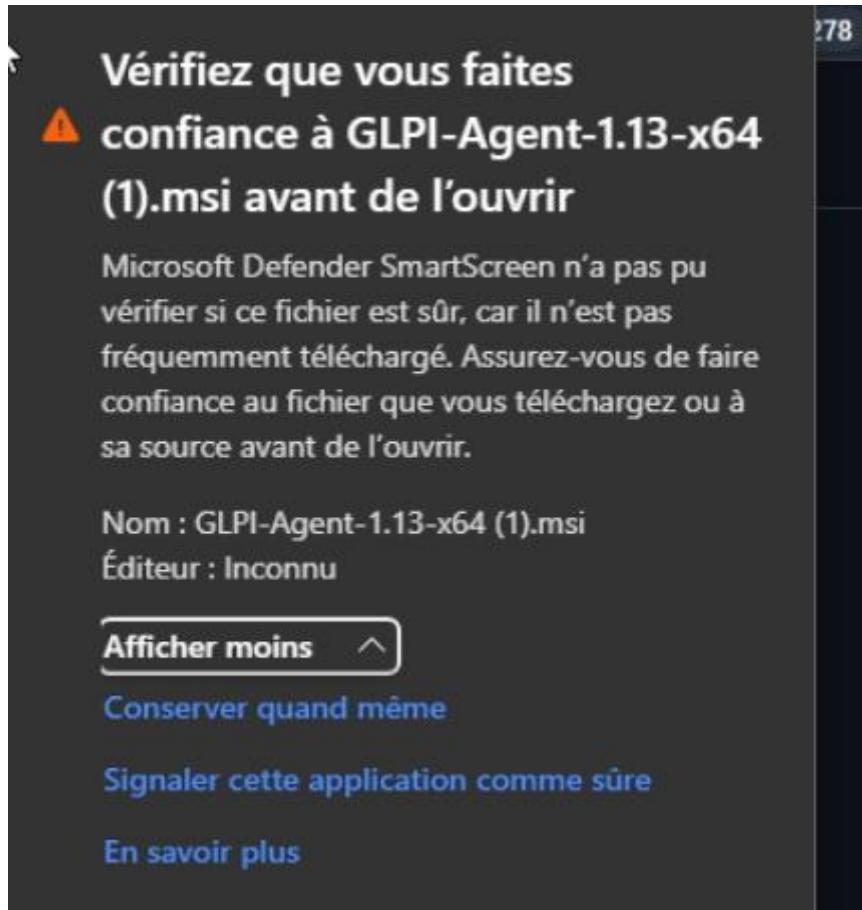
| Arch | Windows installer | Windows portable archive |
|---------|---|---|
| 64 bits | GLPI-Agent-1.13-x64.msi | GLPI-Agent-1.13-x64.zip |

MacOSX

Un Message d'Erreur apparait ne vous inquiéter pas c'est normal cliquer sur Conserver



Cliquer sur Conserver



Pour tester envoyer un inventaire aux server GLPI



ACTIVER L'INVENTAIRE AVANT PUIS CLIQUER SUR SAVE EN BAS

Attendre quelques minutes et voilà notre agent prêt.

| | | |
|--|---|-----------|
| | Hariharani THEIVENDRAM, Aminata THIAM, Omar SISSOKO | |
| | Livrable - intégrale | 2024-2025 |

1.5. Fiche procédure - utilisateur

Objet : Gestion des utilisateurs et des sessions sur GLPI.

1. Accès à l'interface GLPI

Ouvrir un navigateur web (Chrome ou Firefox).

Saisir l'adresse IP de GLP Dans la barre d'adresse : <https://192.168.2.10/>

Entrer les identifiants fournis :

| |
|--------------------------|
| Nom d'utilisateur : glpi |
| Mot de passe : glpi |

2. Gestion des Utilisateurs

2.1. Envoyer un inventaire

Accéder via 127.0.0.1 :62354

Cliquer sur send inventory.

Puis vérifier si le server a bien reçu l'inventaire

2.2. Envoyer un ticket

Accéder à **System > User Manager**.

Selectionner l'utilisateur concerné.

Modifier le champ Mot de passe.

Enregistrer les modifications.

3. Bonnes Pratiques

- **Organiser les tickets** : Demandez aux utilisateurs de bien classifier et prioriser leurs tickets. Cela permet de traiter les demandes selon leur importance et de s'assurer qu'aucun problème urgent ne passe inaperçu.
- **Rédaction claire** : Insistez sur la rédaction de descriptions précises et détaillées pour chaque ticket. Plus les informations sont complètes, plus la résolution sera rapide et pertinente.
- **Suivi régulier des tickets** : Encouragez les utilisateurs à consulter régulièrement l'état de leurs tickets et à répondre rapidement aux mises à jour ou aux demandes d'informations supplémentaires. Cela accélère le processus de résolution.



1.6. Cahier de recettes

Fonctionnalités principales

- Server GLPI opérationnel.
- Client (AGENT) GLPI opérationnelles
- Gestion des agents.

Validation des Tests

- Tous les tests fonctionnels concernant la réception d'inventaire de l'agent.

1.7. Cahier de test

| Test | OK | Remarque |
|---|----|----------|
| Vérifier l'état des services de GLPI server et de son agent | Ok | |
| Tester la détection de l'agent en envoyant un inventaire | Ok | |
| Visualiser l'inventaire sur GLPI server | Ok | |
| Checker l'inventaire, envoyer des tickets | Ok | |



2. Chiffrement des données - VeraCrypt

2.1. Cahier des charges

2.1.1. Contexte et Objectifs

Contexte

Déployer VeraCrypt, un logiciel de chiffrement de disque, afin de protéger les données sensibles contre tout accès non autorisé

Objectif

- Sécuriser les données sensibles de *DataSecurePro*.
- Chiffrer les disques durs avec VeraCrypt.
- Prévenir les fuites de données.
- Respecter les normes de sécurité.

2.1.2. Descriptions fonctionnelles des besoins

- Trello pour la gestion de projet
- Server Proxmox pour mettre en place notre projet
- Appel tous les jours à partir de 21h30
- Documentation Technique
- Chiffrement des disques dur de manière sécurisée.
- Planifier et suivre les opérations de maintenance.

2.1.3. Cahier des charges technique

Systèmes d'exploitation :

- Ubuntu 24.10
- VeraCrypt 1.26.20

Création de volume :

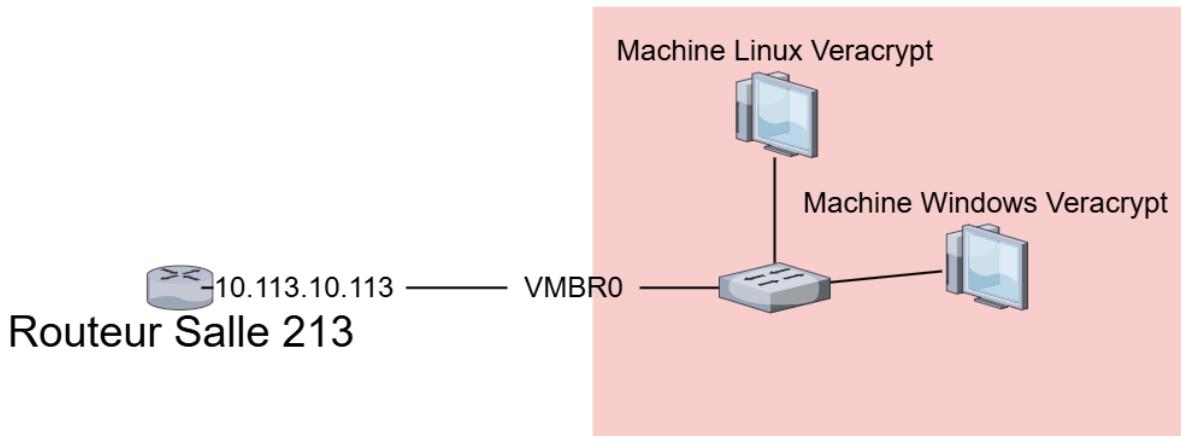
- Clé de chiffrement
- Mots de passe établi



2.1.4. Planning prévisionnel

| Tâche | Durée |
|--|--------|
| Trouver La bonne version | 1 jour |
| Installer le GUI | 1 jour |
| Crée un disque | 1 jour |
| Crée une clé de déchiffrement ex: photo de chat | 1 jour |
| Tester la mise en conformité du disque en testant avec une clé de déchiffrement fausse et avec la vrai | 1 jour |

2.2. Schéma réseau



2.3. Documentation technique

Tout D'abord écrire Veracrypt dans le navigateur

La capture d'écran montre une recherche Google pour "veracrypt". Les résultats sont listés :

- VeraCrypt** (<https://www.veracrypt.fr>)
- Download VeraCrypt** : Aucune information n'est disponible pour cette page. Découvrir pourquoi
- Les Numériques** (<https://www.lesnumeriques.com>)
- Télécharger VeraCrypt - Sécurité** : 5 févr. 2025 — VeraCrypt est un logiciel de chiffrement de disque open source et gratuit qui se distingue par sa capacité à protéger efficacement les données ...
- Autres questions :**

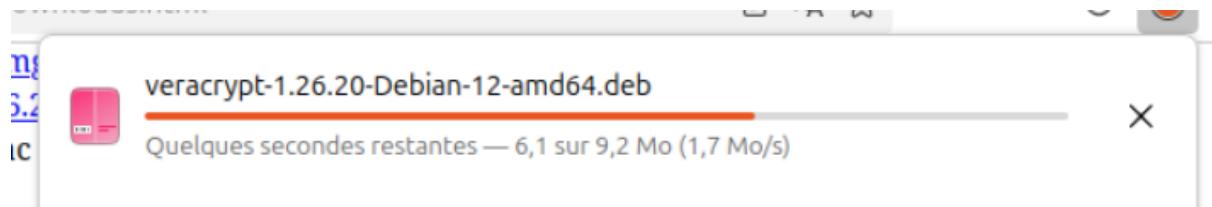
À droite de la liste de résultats, une fenêtre supplémentaire affiche une présentation de VeraCrypt, y compris son logo et des captures d'écran de son interface utilisateur.

Partir dans la rubrique "download"



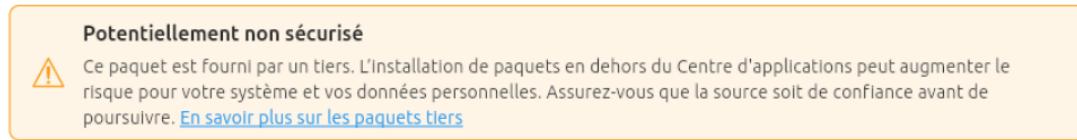
Installer le GUI

- **Linux:**
 - Generic Installers: [veracrypt-1.26.20-setup.tar.bz2](#) (PGP Signature)
 - Linux Legacy installer for 32-bit CPU with no SSE2: [veracrypt-1.26.20-x86-legacy-setup.tar.bz2](#) (PGP Signature)
 - Debian/Ubuntu packages:
 - Debian 12:
 - GUI: [veracrypt-1.26.20-Debian-12-amd64.deb](#) (PGP Signature) and [veracrypt-1.26.20-Debian-12-i386.deb](#) (PGP Signature)

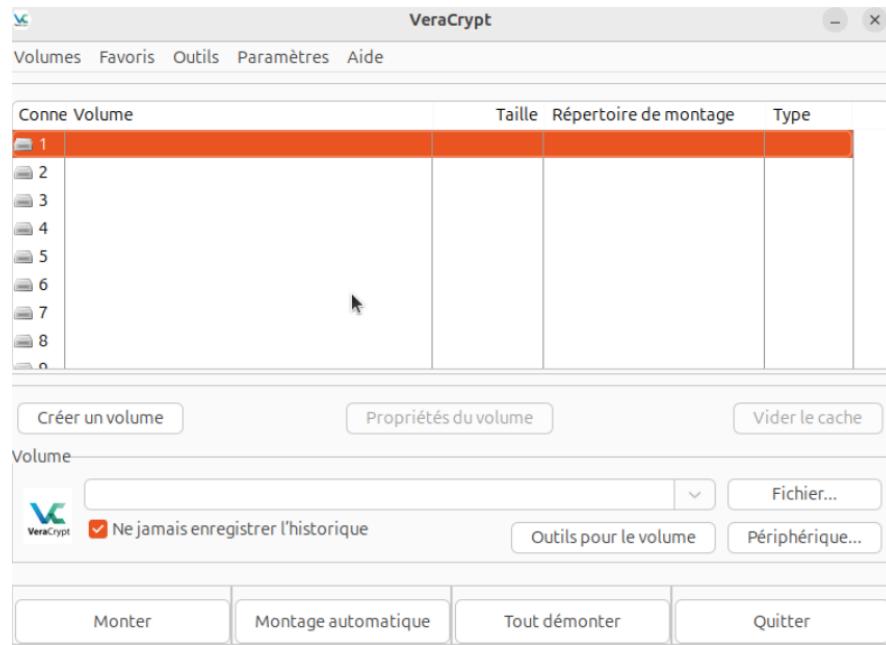


Après L'installation double cliquez

veracrypt



Pas d'inquiétude cliquer sur Installer



Double cliquez et Veracrypt est installée 😊



2.4. Fiche procédure - utilisateur

Objet : Création d'un disque chiffrée .

Accès à l'interface Veracrypt

Ouvrir dans un post Veracrypt.

Crée un Volume

Cliquez sur Assistant de Création de volume.

Choisir son emplacement .

Puis vérifier son option de chiffrement prendre Aes ou NTFS en cas de gros fichier

Choisir la taille du Volume

Par la suite mettre son Mdp et ajouter un fichier clés (exemple photo de chat)

Puis nous le formatons en bougeant la souris

Le volume est créé !!

Nous choisissons un disque puis mettons notre volume dedans et pour l'ouvrir nous devons avoir notre clé (exemple photo de chat) et de notre mdp

Après cela nous pouvons formater notre disque

Bonnes Pratiques

Utilisez un mot de passe long et complexe : Choisissez un: Choisissez un mot de passe d'au moins 20 caractères, combinant lettres, chiffres et symboles.

Activez un volume caché : Util: Utilisez cette fonction pour camoufler des données sensibles, ce qui permet de cacher des informations cruciales si quelqu'un vous force à fournir votre mot de passe.

Sauvegardez vos clés et mots de passe en toute sécurité :: Ne les stockez jamais en clair sur votre ordinateur. Utilisez un gestionnaire de mots de passe ou une clé USB sécurisée.



2.5. Cahier de recettes

Fonctionnalités principales

- Veracrypt opérationnel.
- Machine Windows et Ubuntu opérationnel

Validation des Tests

- Tous les tests fonctionnels concernant la réception d'inventaire de l'agent.

2.6. Cahier de test

| Test | OK | Remarque |
|--|----|----------|
| Vérifier l'installation la sécurité et le bon fonctionnement de VeraCrypt. | Ok | |
| Tester la création d'un volume chiffré, l'accès avec un mot de passe correct | Ok | |
| Tester la création et le montage d'un volume chiffré. | Ok | |
| Tester VeraCrypt sur différents systèmes (Windows, macOS, Linux). | Ok | |



3. OpenVPN

3.1. Cahier des charges

3.1.1. Contexte et Objectifs

Contexte

Dans le cadre de l'amélioration de la sécurité et de la connectivité des services informatiques de l'entreprise, nous avons pour objectif de déployer OpenVPN pour assurer un accès distant sécurisé aux ressources internes. Cette initiative permettra de protéger les communications, d'améliorer la productivité des équipes travaillant à distance et de garantir la confidentialité des données. Le projet vise également à simplifier la gestion des connexions VPN tout en renforçant les standards de sécurité réseau.

Objectif

- Assurer un accès distant sécurisé aux ressources internes.
- Protéger les communications entre les utilisateurs et les serveurs.
- Renforcer la sécurité du réseau de l'entreprise.
- Améliorer la connectivité et la productivité des équipes distantes.
- Faciliter la gestion des connexions VPN.

3.1.2. Descriptions fonctionnelles des besoins

- Serveur dédié pour l'installation d'OpenVPN.
- Certification SSL pour sécuriser les connexions.
- Planification quotidienne des tests de connectivité à partir de 21h30.
- Documentation technique complète pour l'installation et l'administration d'OpenVPN.
- Création et gestion centralisée des utilisateurs et des autorisations d'accès.
- Intégration avec les outils de supervision existants pour un suivi des performances et des incidents.

3.1.3. Cahier des charges technique

Système d'exploitation :Glpi version 10.0 7

Interface graphiques Pfsense:192.168.2.254

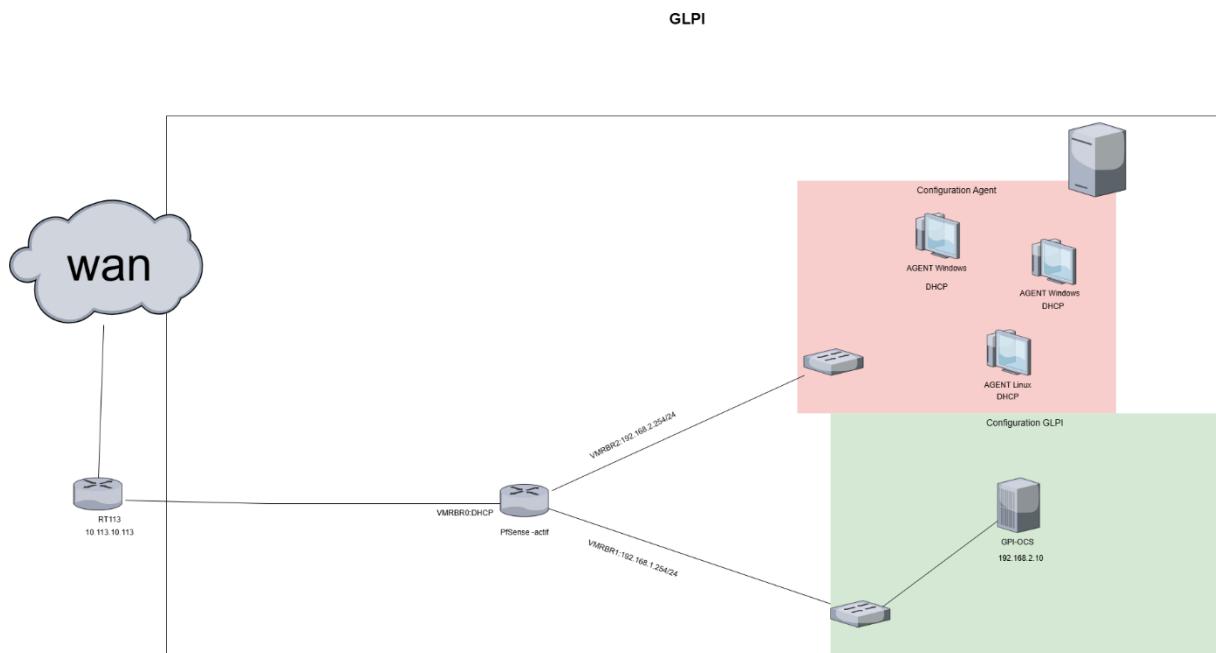
3.1.4. Planning prévisionnel

| Tâche | Durée |
|---|-------|
| Créé Le Certificat | 1jour |
| Certificat Serveur | 1jour |
| Utilisateur du VPN | 1jour |
| Installation du package « OpenVPN-Client-Export | 1jour |
| Configurer OpenVPN | 1jour |

3.2. Plan d'adressage

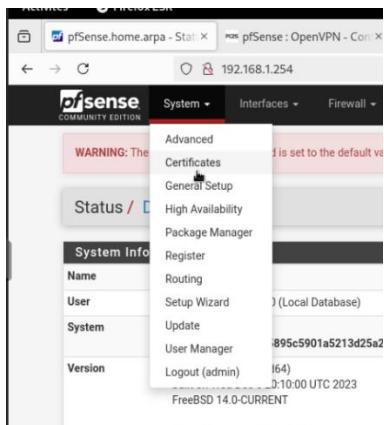
| @réseau | @passerelle | NIC | Machine/rôle | Config plage (DHCP) |
|----------------|--------------------|-------|----------------------------|---------------------|
| 10.113.6.0/16 | 10.113.6.10 | VMBR0 | WAN accès vers l'extérieur | Pas de config DHCP |
| 192.168.1.0/24 | 192.168.1.254/24 | VMBR1 | Server GLPI :192.168.2.10 | Config DHCP |
| 192.168.2.0/24 | 192.168.2.254/24 | VMBR2 | Agent GLPI : DHCP | Config DHCP |

3.3. Schéma réseau





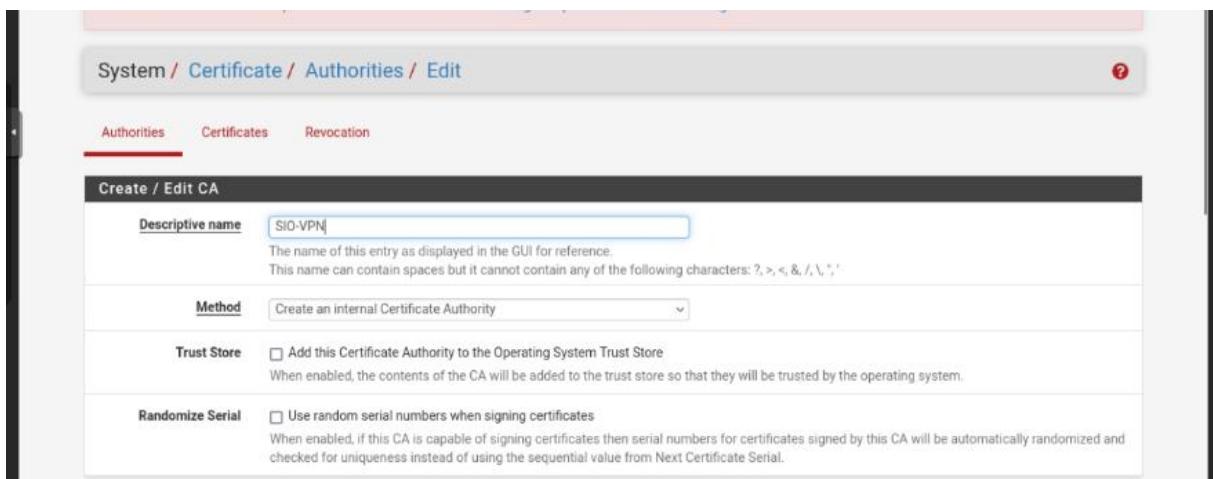
3.4. Documentation technique



Selectioner system >certificates

Cliquer sur "+ Add"

Donner un "**Nom**", sans espace. Exemple : "sio-vpn" , laisser le reste par défaut et cliquez sur "**Save**"





Note: « **Common Name** » : le nom du certificat sans espaces, ni caractères spéciaux. Ce nom doit être unique.

The screenshot shows the 'Internal Certificate Authority' configuration page. The 'Common Name' field is highlighted with the value 'SIO-OMAR'. Other fields include 'Key type: RSA', 'Key Length: 2048', 'Digest Algorithm: sha256', 'Lifetime (days): 3650', and 'Country Code: None'.

Le Certificat est créé

Création du Certificat Serveur

Selectionner : « **Certificates** » et cliquer sur « **+ Add/Sign** »

The screenshot shows the 'Add/Sign a New Certificate' configuration page. The 'Method' is set to 'Create an internal Certificate', 'Descriptive name' is 'VPN-113', 'Certificate authority' is 'SIO-VPN', and 'Key type' is 'RSA'.

Définir « **Method** » sur « **Create an Internal Certificate** », donner un Nom « **VPN-113** » et sélectionner l'autorité de certification « **Certificate authority** » créée précédemment « **SIO-VPN** »

Note: « **Common Name** » : le nom du certificat sans espaces, ni caractères spéciaux. Ce nom doit être unique.



Digest Algorithm sha256
The digest method used when the certificate is signed.
The best practice is to use SHA256 or higher. Some services and platforms, such as the GUI web server and OpenVPN, consider weaker digest algorithms invalid.

Lifetime (days) 3650
The length of time the signed certificate will be valid, in days.
Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.

Common Name SIO-OMAR
The following certificate subject components are optional and may be left blank.

Certificate Attributes

Attribute Notes The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode.
For Internal Certificates, these attributes are added directly to the certificate as shown.

Certificate Type Server Certificate
Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.

Alternative Names FQDN or Hostname
Type Value
Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate as an Alternative Name. The

Selectionner le type de certificat (Certificate Type) : « Server Certificate » puis cliquer sur « Save »

Le Certificat est créé.

Authorities **Certificates** **Certificate Revocation**

Search
Search term Both

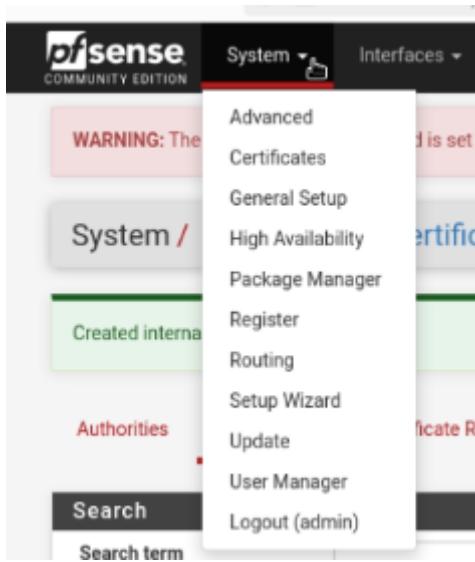
Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificates

| Name | Issuer | Distinguished Name | In Use | Actions |
|--|---------|--------------------|--------|---------|
| VPN-113 Server Certificate CA: No Server: Yes | SIO-VPN | CN=SIO-OMAR | | |

Valid From: Thu, 03 Apr 2025 21:47:50 +0000
Valid Until: Sun, 01 Apr 2035 21:47:50 +0000

Add/Sign



Sélectionner : System > **User Manager**

| Username | Full name | Status | Groups | Actions |
|----------|----------------------|--------|--------|---------|
| admin | System Administrator | ✓ | admins | |

Cliquer sur “+ Add”

User Properties

Defined by: USER

Disabled: This user cannot login

Username: User-SIO

Password:

Full name: User's full name, for administrative information only

Expiration date: Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY

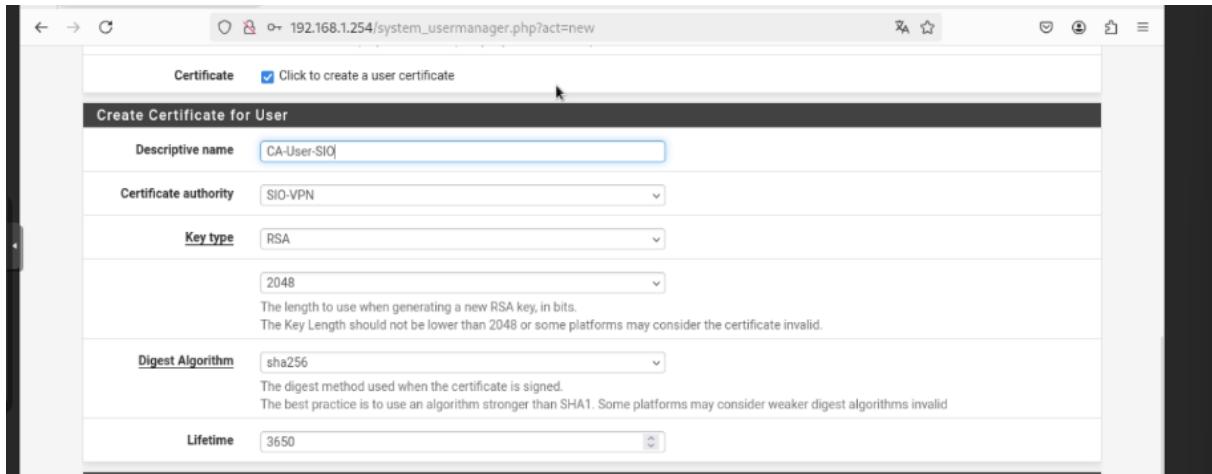
Custom Settings: Use individual customized GUI options and dashboard layout for this user.

Entrer un **Nom d'Utilisateur** “User-SIO” et son **mot de passe**. « labo » > **Cocher** « **Click to create a user certificate** »



Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Certificate Click to create a user certificate



Descriptive name: CA-User-SIO

Certificate authority: SIO-VPN

Key type: RSA

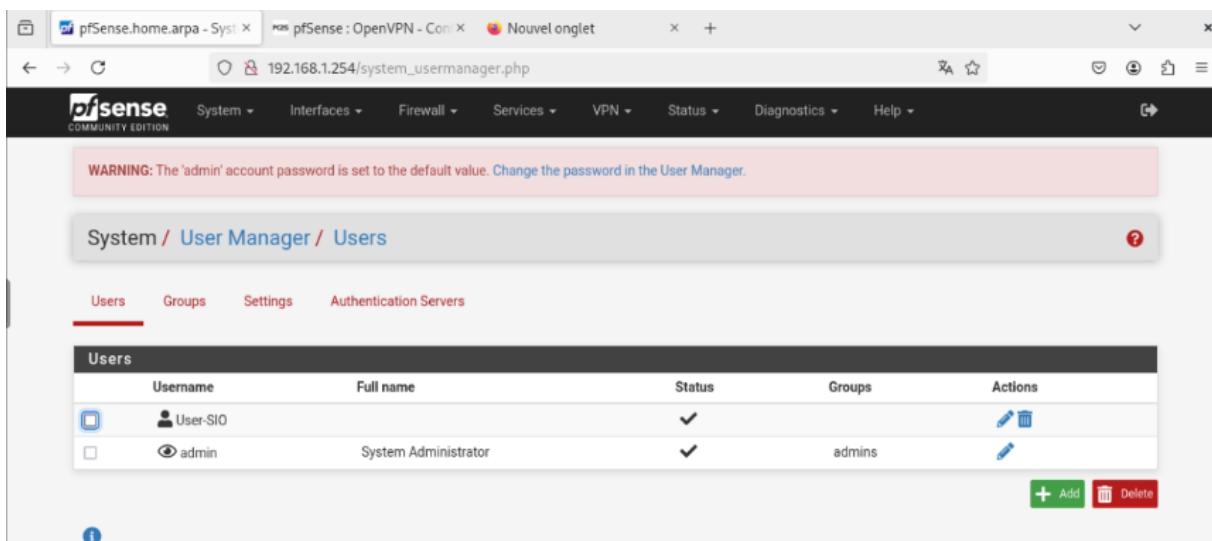
Key Length: 2048

Digest Algorithm: sha256

Lifetime: 3650

Entrer le **Nom du Certificat de l'Utilisateur** « CA-User-SIO » et sélectionner le « Certificate authority » « SIO-VPN » puis cliquer sur « **Save** »

L'Utilisateur du VPN est créé.



| Username | Full name | Status | Groups | Actions |
|----------|----------------------|--------|--------|---------|
| User-SIO | | ✓ | | |
| admin | System Administrator | ✓ | admins | |

Actions:



WARNING: The password for the root user is set to the default value. Change the password in the User Manager.

| Full name | Status | Groups | Actions |
|----------------------|--------|--------|---------|
| System Administrator | ✓ | admins | |

Installation du package « OpenVPN-Client-Export » (Utilitaire pour exporter la configuration Client au format .ovpn)

Sélectionner : System > Package Manager

WARNING: The password for the root user is set to the default value. Change the password in the User Manager.

| Installed Packages |
|----------------------------------|
| There are no packages installed. |



Activities Firefox ESR 4 avril 00:02

192.168.1.254/system_usermanager.php

pfSense COMMUNITY EDITION

System /

WARNING: The password for the root user is set to the default value. Change the password in the User Manager.

Users

Authentication Servers

| Full name | Status | Groups | Actions |
|----------------------|--------|--------|---------|
| System Administrator | ✓ | admins | |

Add Delete

Sélectionner « Available Packages », rechercher « **openvpn** » et installer « **openvpn-client-export** »

System / Package Manager / Available Packages

Installed Packages Available Packages

Search

Search term: openvpn

Both

Search Clear

Enter a search string or *nix regular expression to search package names and descriptions.

Packages

| Name | Version | Description |
|-----------------------|---------|---|
| openvpn-client-export | 1.5_6 | Allows a pre-configured OpenVPN Windows Client or Mac OS X's Viscosity configuration bundle to be exported directly from pfSense. |

Package Dependencies:

openvpn-client-export-2.5.0 openvpn-2.5.0 zip-3.0_1 p7zip-16.02_3

Sélectionner « Available Packages », rechercher « **openvpn** » et installer « **openvpn-client-export** »



Installed Packages Available Packages

Search term: openvpn Both

Enter a search string or *nix regular expression to search package names and descriptions.

Packages

| Name | Version | Description |
|-----------------------|---------|--|
| openvpn-client-export | 1.9.2 | Exports pre-configured OpenVPN Client configurations directly from pfSense software. |

Package Dependencies: openvpn-client-export-2.6.7 openvpn-2.6.8_1 zip-3.0_1 7-zip-23.01

+ Install

Configurer OpenVPN

Sélectionner « VPN » > « OpenVPN » et cliquer sur « + Add »

pfSense.home.arpa - Système 192.168.1.254/pkg_mgr_install.php

pfSense COMMUNITY EDITION

VPN - Status - Diagnostics - Help -

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

System / Package Manager / Package Installer

pfSense-pkg-openvpn-client-export installation successfully completed.

Installed Packages Available Packages Package Installer

Package Installation

```
[4/5] Installing 7-zip-23.01...
[4/5] Extracting 7-zip-23.01: .... done
[5/5] Installing pfSense-pkg-openvpn-client-export-1.9.2...
[5/5] Extracting pfSense-pkg-openvpn-client-export-1.9.2: .... done
Saving updated package information...
done.
Loading package configuration... done.
Configuring package components...
Loading package instructions...
Custom commands...
Executing custom_php_install_command()...done.
Writing configuration... done.
```

Activités 4 avril 00:06

pfSense.home.arpa - VPN 192.168.1.254/vpn_openvpn_server.php

pfSense COMMUNITY EDITION

VPN - Status - Diagnostics - Help -

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

VPN / OpenVPN / Servers

Servers Clients Client Specific Overrides Wizards Client Export

OpenVPN Servers

| Interface | Protocol / Port | Tunnel Network | Mode / Crypto | Description | Actions |
|-----------|-----------------|----------------|---------------|-------------|---------|
|-----------|-----------------|----------------|---------------|-------------|---------|

+ Add



- Server mode : « **Remote Access (SSL/TLS)**»
- Local port : **1194** (Port par Défaut)
- Description : « **Open-VPN -SIO** » (Nom du Tunnel VPN)

The screenshot shows the configuration interface for an OpenVPN server. The 'General Information' section includes a 'Description' field set to 'Open-VPN-SIO'. The 'Mode Configuration' section shows 'Server mode' as 'Remote Access (SSL/TLS)' and 'Device mode' as 'tun - Layer 3 Tunnel Mode'. The 'Endpoint Configuration' section sets 'Protocol' to 'UDP on IPv4 only', 'Interface' to 'WAN', and 'Local port' to '1194'. The 'Cryptographic Settings' section has a 'TLS Configuration' checkbox checked.

The screenshot shows the 'Cryptographic Settings' and 'Data Encryption' sections. In 'Cryptographic Settings', 'Peer Certificate Authority' is set to 'SIO-VPN', 'Server certificate' is set to 'VPN-113 (Server: Yes, CA: SIO-VPN)', and 'Data Encryption' lists 'AES-128-CBC (128 bit key, 128 bit block)' and 'AES-256-GCM (128 bit key, 128 bit block)'.

Sélectionner votre autorité de certification « vpn-113 » dans « Peer Certificate Authority » et le certificat Server « **VPN-PC2S** » dans « Server certificate ».

- IPv4 Tunnel Network : **10.210.10.0/24** (Adresse du réseau VPN au format CIDR)
- **Cocher « Redirect IPv4 Gateway »** pour passer en mode full tunnel
- **Concurrent connections** : Nombre de connexions VPN simultanées



Tunnel Settings

IPv4 Tunnel Network This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.

A tunnel network of /30 or smaller puts OpenVPN into a special peer-to-peer mode which cannot push settings to clients. This mode is not compatible with several options, including Exit Notify, and Inactive.

IPv6 Tunnel Network This is the IPv6 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.

Redirect IPv4 Gateway Force all client-generated IPv4 traffic through the tunnel.

Redirect IPv6 Gateway Force all client-generated IPv6 traffic through the tunnel.

IPv6 Local network(s) IP6 networks that will be accessible from the remote endpoint. Enter each as a comma-separated list of one or more IP/PREFIX or host/network tune

Cocher « Dynamic IP » et laisser « Topology » sur « Subnet – One IP address per client... »

Client Settings

Dynamic IP Allow connected clients to retain their connections if their IP address changes.

Advanced Configuration

Custom options Enter any additional options to add to the OpenVPN server configuration here, separated by semicolon.
EXAMPLE: push "route 10.0.0.0 255.255.255.0"

Indiquez « **auth-nocache** » dans « **Custom options** ». (Pas de mise en cache des identifiants)

Cliquer sur « **Save** ». Le Serveur VPN est créé.

Menu « **Client Export** », Sélectionner « **Other** » pour « **Host Name Resolution** » et renseigner **votre IP WAN Publique** dans « **Host Name** » (Exemple : 217.178.212.123)

OpenVPN Server

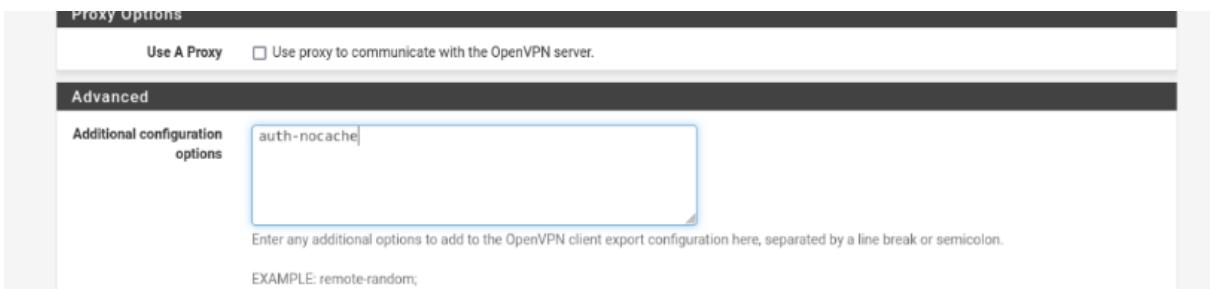
Remote Access Server Open-VPN-SIO UDP4:1194

Client Connection Behavior

Host Name Resolution Other

Host Name 192.168.2.10/24

Enter the hostname or IP address the client will use to connect to this server.



Indiquez « **auth-nocache** » dans « **Additional configuration options** » . (Pas de mise en cache des identifiants)

Cliquer sur « **Save as default** »

| OpenVPN Servers | | | | | | |
|-----------------|-------------------|----------------|--|--------------|---------|--|
| Interface | Protocol / Port | Tunnel Network | Mode / Crypto | Description | Actions | |
| WAN | UDP4 / 1194 (TUN) | 10.210.10.0/24 | Mode: Remote Access (SSL/TLS) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA256 D-H Params: 2048 bits | Open-VPN-SIO | | |

Votre VPN est créée



3.5. Cahier de recettes

OpenVPN:

Installation et configuration pour le routage réseau et la sécurité avancée.

Interface graphique :

Développement ou configuration d'un tableau de bord intuitif pour l'installation est la configuration.

Machine GLPI :

Connexion à l'interface graphique de pfSense sur cette machine.

3.6. Cahier de test

| Test | OK | Remarque |
|----------------------------------|----|----------|
| Création du certificat | Ok | |
| Création du certificat server | Ok | |
| Création de l'utilisateur | Ok | |
| Installation du Packages OpenVPN | Ok | |



4. Portail captif avec pfSense

4.1. Cahier des charges

4.1.1. Contexte et Objectifs

Contexte

Dans une entreprise, la gestion de l'accès à Internet est essentielle pour garantir la **sécurité des données**, éviter les **usages abusifs** et assurer une **bonne répartition de la bande passante**. Un **portail captif** est une solution efficace permettant de contrôler et authentifier les utilisateurs avant qu'ils ne puissent accéder au réseau.

Objectif

L'objectif principal est de mettre en place un **système de portail captif** permettant :

- **D'authentifier les utilisateurs** avant d'accéder à Internet.
- **De sécuriser les accès au réseau** en limitant l'utilisation aux personnes autorisées.
- **De tracer les connexions** pour respecter la réglementation en vigueur.
- **De gérer les droits d'accès** en fonction des profils d'utilisateurs (employés, visiteurs, prestataires).
- **De contrôler la bande passante** pour éviter les saturations et garantir une bonne qualité de service.

4.1.2. Descriptions fonctionnelles des besoins

Le portail captif devra répondre aux besoins suivants :

Authentification et gestion des utilisateurs

- Authentification via **nom d'utilisateur / mot de passe**.
- Connexion pour les **visiteurs avec génération de codes d'accès temporaires**.
- Déconnexion automatique après une période d'inactivité configurable.

Gestion et administration

- Accès administrateur pour la gestion des comptes et la consultation des logs.
- Tableau de bord pour suivre en temps réel les utilisateurs connectés.
- Possibilité d'exporter des rapports d'utilisation.

4.1.3. Cahier des charges technique

- Installation de pfSense et configuration des interface réseau.
- Installation d'un client sur lequel on aura accès à l'interface Web de pfSense.
- Configurer le portail captif.

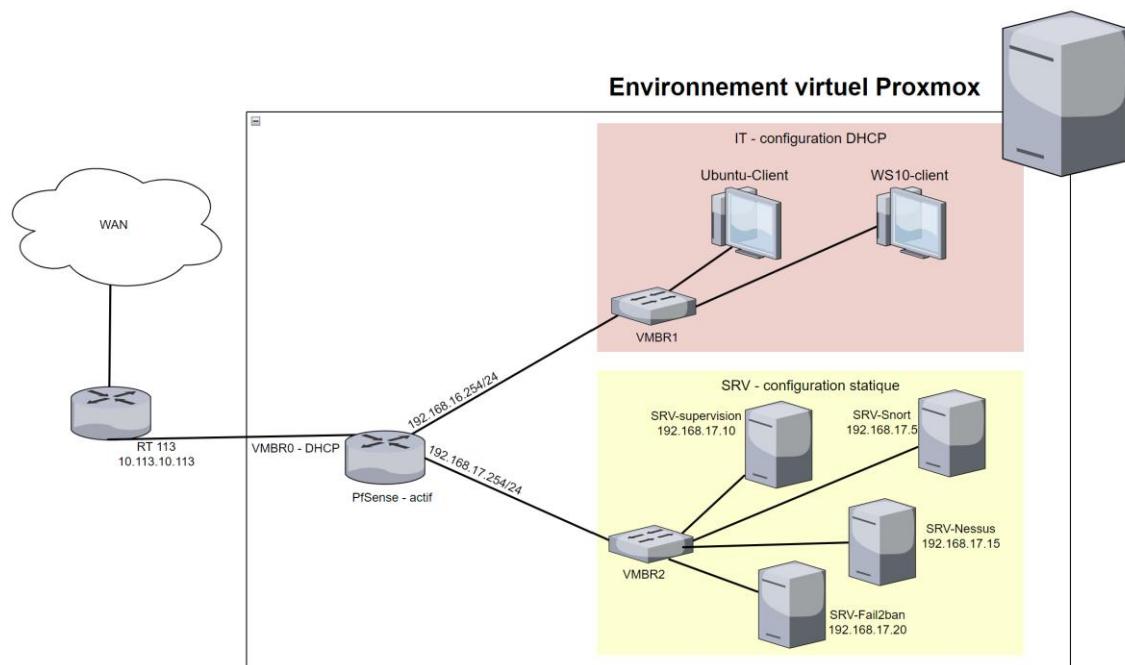
4.1.4. Planning prévisionnel

| Tâche | Durée |
|---|--------|
| Déploiement de pfSense et configuration du portail captif | 1 jour |
| Tests de charge, validation de l'authentification et de la sécurité | 1 jour |
| Documentation et formation à l'utilisation du portail captif | 1 jour |

4.2. Plan d'adressage

| @réseau | @passerelle | NIC | Machine/rôle | DHCP ? |
|-----------------|----------------|-------|--|-------------|
| 10.113.0.0/16 | DHCP | VMBR0 | pfSense : WAN accès vers l'extérieur | Config DHCP |
| 192.168.16.0/24 | 192.168.16.254 | VMBR1 | Ubuntu-client/WS10-client Interface graphique : http://192.168.16.254/ | Config DHCP |

4.3. Schéma réseau





4.4. Documentation technique

4.4.1. Pfsense - actif

Installation de Pfsense

Etape 1 : Créer la VM, avec les configurations ci-dessous.

| Nom | ID | OS | Mémoire | RAM | CPU | Réseau | Services/Remarques |
|-----------------|-------|---------------|---------|-----|------------------------|-------------------------|--|
| Pfsense - actif | MV200 | Pfsense 2.7.2 | 20Go | 1Go | 1 processor 1 cœurs | VMBR0 VMBR1 VMBR2 | Em0 : 10.113.0.81/16 Em1 : 192.168.16.254/24 Em2 : 192.168.17.254/24 |

Configuration réseau

Etape 2 : Configurer les interfaces dans pfsense, via la console et attribuer leurs passerelles.

Em0 : DHCPv4

Em1 : 192.168.16.254/24

Em2 : 192.168.17.254/24

```
WAN (wan)      -> vtnet0      -> v4/DHCP4: 10.113.113.26/16
IT (lan)        -> vtnet1      -> v4: 192.168.16.254/24
SRV (opt1)      -> vtnet2      -> v4: 192.168.17.254/24
```

4.4.2. Ubuntu - client

Installation de Ubuntu

| Nom | ID | OS | Mémoire | RAM | CPU | Réseau | @IP |
|---------------|-------|--------------|---------|-----|------------------------|--------|-------------------|
| Ubuntu-client | MV120 | Ubuntu 24.04 | 32Go | 2Go | 1 processor 1 cœurs | VMBR1 | Attribué via DHCP |

Interface graphique Pfsense

Accéder à l'interface graphique de Pfsense avec : <http://192.168.17.254/>

Modifier le nom des interfaces :

Em0 : WAN

Em1 : IT

Em2 : SRV

Activation des logs sur les interfaces



Créer des règles en autorisant tout et activer les logs.

Configuration du portail captif – Gestion d'utilisateurs

PfSense dispose d'un portail captif. Le portail captif force les clients d'un réseau à afficher une page Web d'authentification avant de pouvoir se connecter à Internet.

Il est utilisé dans des réseaux qui assurent un accès public tels que les espaces d'accueil, établissements scolaires.

Important : Ne pas modifier le langage de l'interface en Français avant la configuration du portail car il y a un Bug lors de la sauvegarde des modifications dans certaines versions.

En revanche, une fois la configuration terminée et validée, vous pouvez modifier la langue de l'interface en Français.

Cliquer sur « + Add »

Renseigner le Nom du portail captif et sa description.



Services / Captive Portal / Add Zone

Add Captive Portal Zone

Zone name: PORTAIL

Zone description: Portail Captif

Save & Continue

- Activer « **Enable Captive Portal** ».
- Sélectionner l'interface « **IT** ».
- Maximum concurrent connections : **1** (Limite le nombre de connexions simultanées d'un même utilisateur).
- Idle timeout (Minutes) : Choisir entre **1 à 5** (Les clients seront déconnectés après cette période d'inactivité).

Services / Captive Portal / PORTAIL / Configuration

Configuration MACs Allowed IP Addresses Allowed Hostnames Vouchers High Availability File Manager

Captive Portal Configuration

Enable: Enable Captive Portal

Description: portail captif

Interfaces: IT

Maximum concurrent connections: 1

Idle timeout (Minutes): 5

- Activer « **Enable logout popup window** » (une fenêtre popup permet aux clients de se déconnecter).
- Définir « **Pre-authentication Redirect URL** » (*URL HTTP de redirection par défaut. Les visiteurs ne seront redirigés vers cette URL après authentification que si le portail captif ne sait pas où les rediriger*).
- Définir « **After authentication Redirection URL** » (*URL HTTP de redirection forcée. Les clients seront redirigés vers cette URL au lieu de celle à laquelle ils ont initialement tenté d'accéder après s'être authentifiés*).
- Activer « **Disable Concurrent user logins** » (seule la connexion la plus récente par nom d'utilisateur sera active).
- Activer « **Disable MAC filtering** » (nécessaire lorsque l'adresse MAC du client ne peut pas être déterminée).



| | |
|---|--|
| Logout popup window | <input checked="" type="checkbox"/> Enable logout popup window If enabled, a popup window will appear when clients are allowed through the captive portal. This allows clients to explicitly disconnect themselves before the idle or hard timeout occurs. |
| Pre-authentication redirect URL | <input type="text" value="http://www.google.fr/"/> Set a default redirection URL. Visitors will be redirected to this URL after authentication only if the captive portal doesn't know where to redirect them. This field will be accessible through \$PORTAL_REDIRURL\$ variable in captiveportal's HTML pages. |
| After authentication Redirection URL | <input type="text" value="http://www.google.fr"/> Set a forced redirection URL. Clients will be redirected to this URL instead of the one they initially tried to access after they've authenticated. |
| Blocked MAC address redirect URL | <input type="text"/> Blocked MAC addresses will be redirected to this URL when attempting access. |
| Concurrent user logins | <input checked="" type="checkbox"/> Disable Concurrent user logins If enabled only the most recent login per username will be active. Subsequent logins will cause machines previously logged in with the same username to be disconnected. |
| MAC filtering | <input checked="" type="checkbox"/> Disable MAC filtering If enabled no attempts will be made to ensure that the MAC address of clients stays the same while they are logged in. This is required when the MAC address of the client cannot be determined (usually because there are routers between pfSense and the clients). If this is enabled, RADIUS MAC authentication cannot be used. |

- Sélectionner « **Use an Authentication backend** ».
- Sélectionner « **Local Database** » pour « **Authentication Server** ».
- **Attention** : Ne pas sélectionner « **Local Database** » pour « **Secondary Authentication Server** ».
- Activer « **Local Authentication Privileges** » (Autoriser uniquement les utilisateurs avec les droits de « Connexion au portail captif »).

Puis cliquer « **Save** »

| | |
|--|--|
| Authentication | |
| Authentication Method | <input type="text" value="Use an Authentication backend"/> Select an Authentication Method to use for this zone. One method must be selected. - "Authentication backend" will force the login page to be displayed and will authenticate users using their login and password, or using vouchers. - "None" method will force the login page to be displayed but will accept any visitor that clicks the "submit" button. - "RADIUS MAC Authentication" method will try to authenticate devices automatically with their MAC address without displaying any login page. |
| Authentication Server | <input type="text" value="Local Database"/> You can add a remote authentication server in the User Manager . Vouchers could also be used, please go to the Vouchers Page to enable them. |
| Secondary authentication Server | <input type="text" value="Local Database"/> You can optionally select a second set of servers to authenticate users. Users will then be able to login using separated HTML inputs. This setting is useful if you want to provide multiple authentication method to your users. If you don't need multiple authentication method, then leave this setting empty. |
| Reauthenticate Users | <input type="checkbox"/> Reauthenticate connected users every minute If reauthentication is enabled, request are made to the server for each user that is logged in every minute. If an access denied is received for a user, that user is disconnected from the captive portal immediately. Reauthentication requires user credentials to be cached in the captive portal database while a user is logged in; The cached credentials are necessary for the portal to perform automatic reauthentication requests. |
| Local Authentication Privileges | <input checked="" type="checkbox"/> Allow only users/groups with "Captive portal login" privilege set |

| | |
|----------------------|--|
| HTTPS Options | |
| Login | <input type="checkbox"/> Enable HTTPS login When enabled, the username and password will be transmitted over an HTTPS connection to protect against eavesdroppers. A server name and certificate must also be specified below. |
| Save | |

Résultat



Configuration du Groupe et des Utilisateurs pour la délégation du Portail Captif

Création d'un groupe et utilisateur qui aura pour fonction de créer des Utilisateurs autorisés à se connecter au Portail Captif. Ce groupe et utilisateurs associés auront seulement le droit de créer des Utilisateurs du Portail Captif.

Sélectionner : System – User Manager

Onglet 'Groups », cliquer sur « + Add »

Renseigner le Nom du groupe « Utilisateurs »



System / User Manager / Groups / Edit

Users Groups Settings Authentication Servers

Group Properties

| | |
|---|--------------|
| Group name | Utilisateurs |
| Scope | Local |
| Warning: Changing this setting may affect the local groups file, in which case a reboot may be required for the changes to take effect. | |
| Description | |
| Group description, for administrative information only | |
| Group membership | admin |
| Not members | Members |
| Move to "Members" Move to "Not members" | |
| Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items. | |

Dans le menu « Actions », modifier le groupe créé en cliquant sur le stylo

System / User Manager / Groups

Users Groups Settings Authentication Servers

Groups

| Group name | Description | Member Count | Actions |
|--------------|-----------------------|--------------|---------|
| Utilisateurs | | 0 | |
| admins | System Administrators | 1 | |
| all | All Users | 1 | |

+ Add

Cliquez sur « + Add » rubrique « Assigned Privileges ».

Group Properties

| | |
|---|--|
| Group name | Agent |
| Scope | Local |
| Warning: Changing this setting may affect the local groups file, in which case a reboot may be required for the changes to take effect. | |
| Description | Delegation Creation Utilisateurs Portail |
| Group description, for administrative information only | |
| Group membership | admin |
| Not members | Members |
| Move to "Members" Move to "Not members" | |
| Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items. | |

Assigned Privileges

| Name | Description | Action |
|--------------|-------------|--------|
| + Add | | |

Sélectionnez dans la liste « WebCfg – System: User Manager » (Accès à la page de gestion des utilisateurs « User Manager »)



Puis cliquez sur « **Save** »

Group Privileges

Group Utilisateurs

Assigned privileges

- WebCfg - System: Static Routes
- WebCfg - System: Static Routes: Edit route
- WebCfg - System: Update: Settings
- WebCfg - System: User Manager**
- WebCfg - System: User Manager: Add Privileges
- WebCfg - System: User Manager: Settings
- WebCfg - System: User Password Manager
- WebCfg - System: User Settings
- WebCfg - VPN: IPsec
- WebCfg - VPN: IPsec: Edit Phase 1
- WebCfg - VPN: IPsec: Edit Phase 2
- WebCfg - VPN: IPsec: Edit Pre-Shared Keys
- WebCfg - VPN: IPsec: Mobile
- WebCfg - VPN: IPsec: Pre-Shared Keys List
- WebCfg - VPN: IPsec: Settings
- WebCfg - VPN: L2TP
- WebCfg - VPN: L2TP: Users
- WebCfg - VPN: L2TP: Users: Edit
- WebCfg - XMLRPC Interface Stats
- WebCfg - XMLRPC Library

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Revenir à la rubrique « **Assigned Privileges** » en cliquant sur « **+ Add** »

Selectionnez dans la liste « **WebCfg – Status: Captive Portal** » (Voir le Status des utilisateurs connectés)

System / User Manager / Groups / Edit / Add Privileges

Users Groups Settings Authentication Servers

Group Privileges

Group Utilisateurs

Assigned privileges

- WebCfg - Services: Wake-on-LAN
- WebCfg - Services: Wake-on-LAN: Edit
- WebCfg - Status: Captive Portal**
- WebCfg - Status: Captive Portal Voucher Rolls
- WebCfg - Status: Captive Portal Vouchers
- WebCfg - Status: Captive Portal: Expire Vouchers
- WebCfg - Status: Captive Portal: Test Vouchers
- WebCfg - Status: CARP
- WebCfg - Status: CPU load
- WebCfg - Status: DHCP leases
- WebCfg - Status: DHCPv6 leases
- WebCfg - Status: DNS Resolver
- WebCfg - Status: Filter Reload Status
- WebCfg - Status: Gateway Groups
- WebCfg - Status: Gateways
- WebCfg - Status: Interfaces
- WebCfg - Status: IPsec
- WebCfg - Status: IPsec: Leases

Puis cliquez sur « **Save** »

Vérifier les droits, puis cliquez sur « **Save** »



Assigned Privileges

| Name | Description | Action |
|---------------------------------|--|--------|
| WebCfg - System: User Manager | Allow access to the 'System: User Manager' page. (admin privilege) | |
| WebCfg - Status: Captive Portal | Allow access to the 'Status: Captive Portal' page. | |

Security notice: Users in this group effectively have administrator-level access

+ Add

Save

Création des Utilisateurs

Onglet « **Users** », cliquez sur « **+ Add** »

System / User Manager / Users

Users Groups Settings Authentication Servers

| Users | | | | | |
|----------|----------------------|--------|--------|---------|--|
| Username | Full name | Status | Groups | Actions | |
| admin | System Administrator | ✓ | admins | | |

+ Add Delete

Entrer un **Nom d'Utilisateur** « osissoko », son **mot de passe** et sa **description** (Agent autorisé à créer des utilisateurs du Portail Captif).

Selectionner dans « **Group membership** » le groupe « **Agents** » précédemment créé. Cliquez sur « **Move to Member of list** » puis « **Save** »

User Properties

| | | | | | |
|------------------|--|---------------|----------------------------|-----------|---------------------------------|
| Defined by | USER | | | | |
| Disabled | <input type="checkbox"/> This user cannot login | | | | |
| Username | osissoko | | | | |
| Password | ***** | | | | |
| Full name | Omar SISSOKO User's full name, for administrative information only | | | | |
| Expiration date | Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY | | | | |
| Custom Settings | <input type="checkbox"/> Use individual customized GUI options and dashboard layout for this user. | | | | |
| Group membership | <table border="1"><tr><td>Not member of</td><td> » Move to "Member of" list</td></tr><tr><td>Member of</td><td> << Move to "Not member of" list</td></tr></table> <p>Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.</p> | Not member of | » Move to "Member of" list | Member of | << Move to "Not member of" list |
| Not member of | » Move to "Member of" list | | | | |
| Member of | << Move to "Not member of" list | | | | |
| Certificate | No private CAs found. A private CA is required to create a new user certificate. Save the user first to import an external certificate. | | | | |



System / User Manager / Users

Users Groups Settings Authentication Servers

| Username | Full name | Status | Groups | Actions |
|----------|----------------------|--------|--------------|---------|
| admin | System Administrator | ✓ | admins | |
| osissoko | Omar SISSOKO | ✓ | Utilisateurs | |

Add Delete

Configuration du groupe et des utilisateurs autorisés à se connecter au Portail Captif

Ce groupe et utilisateurs associés auront seulement le droit d'utiliser le Portail Captif.

Onglet « Groups », cliquez sur « + Add »

System / User Manager / Groups

Users Groups Settings Authentication Servers

| Group name | Description | Member Count | Actions |
|--------------|-----------------------|--------------|---------|
| Utilisateurs | | 1 | |
| admins | System Administrators | 1 | |
| all | All Users | 2 | |

Add

Renseigner le **Nom du Groupe** « Portail – user management » et sa **description** « Utilisateurs du Portail ». Cliquez « Save »

Group Properties

| | | | | | |
|---|---|-------------|---------|-------|----------|
| Group name | Portail | | | | |
| Scope | Local | | | | |
| Warning: Changing this setting may affect the local groups file, in which case a reboot may be required for the changes to take effect. | | | | | |
| Description | Group description, for administrative information only | | | | |
| Group membership | <table border="1"><tr><td>Not members</td><td>Members</td></tr><tr><td>admin</td><td>osissoko</td></tr></table> <p> </p> <p>Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.</p> | Not members | Members | admin | osissoko |
| Not members | Members | | | | |
| admin | osissoko | | | | |

Dans le menu « Actions », **modifier** le groupe créé en cliquant sur le stylo.



| Groups | | | |
|--------------|---|--------------|---------|
| Group name | Description | Member Count | Actions |
| Portail | utilisateurs du portail captif | 3 | |
| admins | System Administrators | 2 | |
| all | All Users | 4 | |
| utilisateurs | délégation création utilisateurs portail captif | 3 | |

Add

Cliquez sur « + Add » rubrique « **Assigned Privileges** » .

Group Properties

Group name: Portail

Scope: Local

Description: Group description, for administrative information only

Group membership:

| | |
|------------------------------|------------------|
| Not members: admin, osissoko | Members: (empty) |
|------------------------------|------------------|

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Sélectionnez dans la liste « **User – Services: Captive Portal login** » (Autorisé seulement à se connecter au Portail Captif)

Puis cliquez sur « **Save** »

Group Privileges

Group: Portail

Assigned privileges:

- System - HA node sync
- User - Config: Deny Config Write
- User - Notices: View
- User - Notices: View and Clear
- User - Services: Captive Portal login**
- User - System: Copy files (scp)
- User - System: Copy files to home directory (chrooted scp)
- User - System: Shell account access
- User - System: SSH tunneling
- User - VPN: IPsec xauth Dialin
- User - VPN: L2TP Dialin
- User - VPN: PPPOE Dialin
- WebCfg - AJAX: Get Service Providers
- WebCfg - AJAX: Get Stats
- WebCfg - All pages
- WebCfg - Crash reporter
- WebCfg - Dashboard (all)
- WebCfg - Dashboard widgets (direct access)
- WebCfg - Diagnostics: ARP Table
- WebCfg - Diagnostics: Authentication

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Vérifier les droits, puis cliquez sur « **Save** »



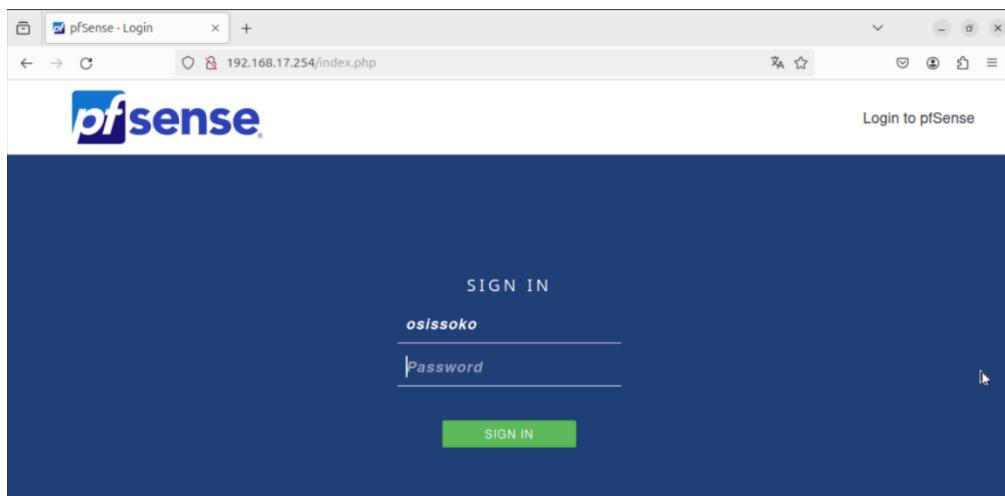
Assigned Privileges

| Name | Description | Action |
|---------------------------------------|--|--------|
| User - Services: Captive Portal login | Indicates whether the user is able to login on the captive portal. | |

Save

Connexion avec le compte « osissoko »

Cet utilisateur a seulement le droit de créer des Utilisateurs du Portail Captif par délégation et de voir le Statut des utilisateurs connectés.



pfSense COMMUNITY EDITION

System / User Manager / Users

Users

| Username | Full name | Status | Groups | Actions |
|-----------------------------------|----------------------|--------|----------------------|---------|
| <input type="checkbox"/> admin | System Administrator | ✓ | admins | |
| <input type="checkbox"/> osissoko | Omar SISSOKO | ✓ | Portail.Utilisateurs | |

Tableau de bord restreint. Seulement les fonctions de création d'utilisateur et de Statut du Portail Captif sont disponibles.

Le « Statut du Portail Captif » permet de voir les utilisateurs connectés et de les déconnecter si besoin ...



Créer un compte depuis le compte « osissoko »

| Username | Full name | Status | Groups | Actions |
|----------|----------------------|--------|-----------------------|---------|
| admin | System Administrator | ✓ | admins | |
| osissoko | Omar SISSOKO | ✓ | Portail, Utilisateurs | |

Cliquer sur “+ Add”

Defined by: USER

Disabled: This user cannot login

Username: test

Password: *****

Full name: TEST
User's full name, for administrative information only

Expiration date: Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY

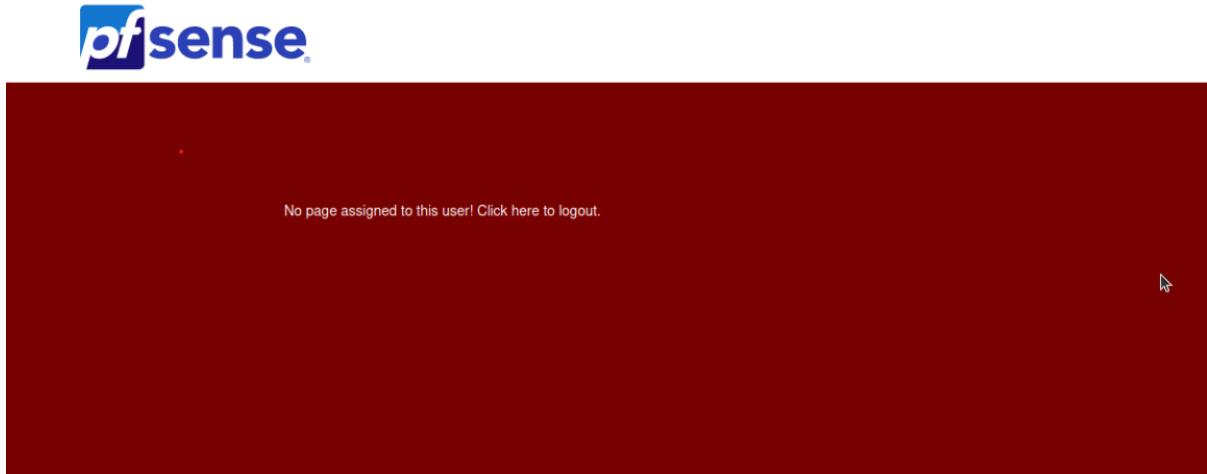
Custom Settings: Use individual customized GUI options and dashboard layout for this user.

Group membership: Utilisateurs
 admins

Not member of: Portail

| Username | Full name | Status | Groups | Actions |
|----------|----------------------|--------|-----------------------|---------|
| admin | System Administrator | ✓ | admins | |
| osissoko | Omar SISSOKO | ✓ | Portail, Utilisateurs | |
| test | TEST | ✓ | Portail | |

Test en se connectant au compte “Test”



On a assigné aucune fonctionnalité mais la session est bien connectée.



4.5. Fiche procédure - utilisateur

Objet : Gestion des utilisateurs et des sessions sur le portail captif de pfSense.

4. Accès à l'interface pfSense

Ouvrir un navigateur web (Chrome ou Firefox).

Saisir l'adresse IP de pfSense dans la barre d'adresse : <https://192.168.17.254/>

Entrer les identifiants fournis :

| |
|------------------------------|
| Nom d'utilisateur : osissoko |
| Mot de passe : Labo-113 |

5. Gestion des Utilisateurs

2.1. Créer un utilisateur

Accéder à **System > User Manager**.

Cliquer sur **Add**.

Remplir les champs :

 Nom d'utilisateur

 Mot de passe

 Privilèges : accès au portail captif uniquement.

Enregistrer les modifications.

2.2. Modifier un mot de passe

Accéder à **System > User Manager**.

Sélectionner l'utilisateur concerné.

Modifier le champ Mot de passe.

Enregistrer les modifications.

2.3. Supprimer un utilisateur

Accéder à **System > User Manager**.

Cocher la case à côté de l'utilisateur à supprimer.

Cliquer sur **Delete**.

Confirmer la suppression.

6. Surveillance des Sessions

Accéder à **Status > Captive Portal**.

Consulter la liste des sessions actives.

Pour déconnecter un utilisateur :

 Sélectionner la session.

 Cliquer sur **Disconnect**.



4.6. Cahier de recettes

Fonctionnalités principales

- Portail captif opérationnel.
- Gestion des comptes utilisateurs fonctionnelle.
- Accès restreint pour Omar.

Validation des Tests

- Tous les tests fonctionnels et de sécurité réussis.
- Conformité avec les politiques de sécurité.

4.7. Cahier de test

| Test | OK | Remarque |
|--|----|----------|
| Vérification de l'accès via l'interface web pfsense | X | |
| Authentification avec différents comptes utilisateurs | X | |
| Création, modification et suppression des comptes utilisateurs | X | |
| Changement de mot de passe | X | |
| Visualisation des sessions actives | X | |
| Déconnexion manuelle d'un utilisateur | X | |
| Test de l'accès restreint pour Omar | X | |



5. Supervision de l'espace disque avec Prometheus

5.1. Cahier des charges

5.1.1. Contexte et Objectifs

Contexte

Dans le cadre de l'optimisation de la gestion des infrastructures IT, l'entreprise souhaite mettre en place un **système de surveillance et d'alertes** pour garantir la **disponibilité, la stabilité et la performance** de ses serveurs et applications.

Pour répondre à ce besoin, nous allons déployer **Prometheus, Grafana, Node Exporter et Alertmanager**, trois outils open-source permettant de **collecter, analyser et alerter** en cas d'incident.

Objectifs

- Superviser l'état des serveurs et applications** (CPU, RAM, disque, réseau).
- Visualiser en temps réel** les métriques via un tableau de bord intuitif.
- Déetecter les anomalies** et déclencher des alertes automatisées.
- Envoyer des notifications aux équipes IT** par email, Slack ou Telegram.

5.1.2. Descriptions fonctionnelles des besoins

Fonctionnalités Principales

| Fonctionnalité | Description |
|----------------------------|---|
| Collecte des métriques | Prometheus récupère les données système (CPU, RAM, disque, etc.) via Node Exporter. |
| Visualisation des données | Grafana affiche les métriques sous forme de graphiques interactifs. |
| Détection des anomalies | Définition de règles d'alerte basées sur des seuils critiques. |
| Notifications automatisées | Alertmanager envoie des alertes aux équipes IT via email ou autres canaux. |

Exemples d'Alertes Configurées

| Type d'alerte | Condition | Action |
|----------------------|----------------------|-----------------------------|
| Espace disque faible | < 20% d'espace libre | Envoi un mail à l'équipe IT |



5.1.3. Cahier des charges technique

Architecture du Système

- Prometheus** : Collecte les métriques via des exporters (Node Exporter, cAdvisor...).
- Grafana** : Interface pour visualiser les métriques.
- Alertmanager** : Gère et envoie les notifications d'alerte.

Technologies Utilisées

| Composant | Technologie |
|-------------------------|---------------|
| Monitoring | Prometheus |
| Visualisation | Grafana |
| Alertes | AlertManager |
| Collectes des métriques | Node Exporter |
| Notifications | Gmail |

Configuration Requise

- Serveur Ubuntu**
- Installation des packages nécessaires** (prometheus, grafana, alertmanager).
- Accès réseau pour les notifications externes (SMTP)**

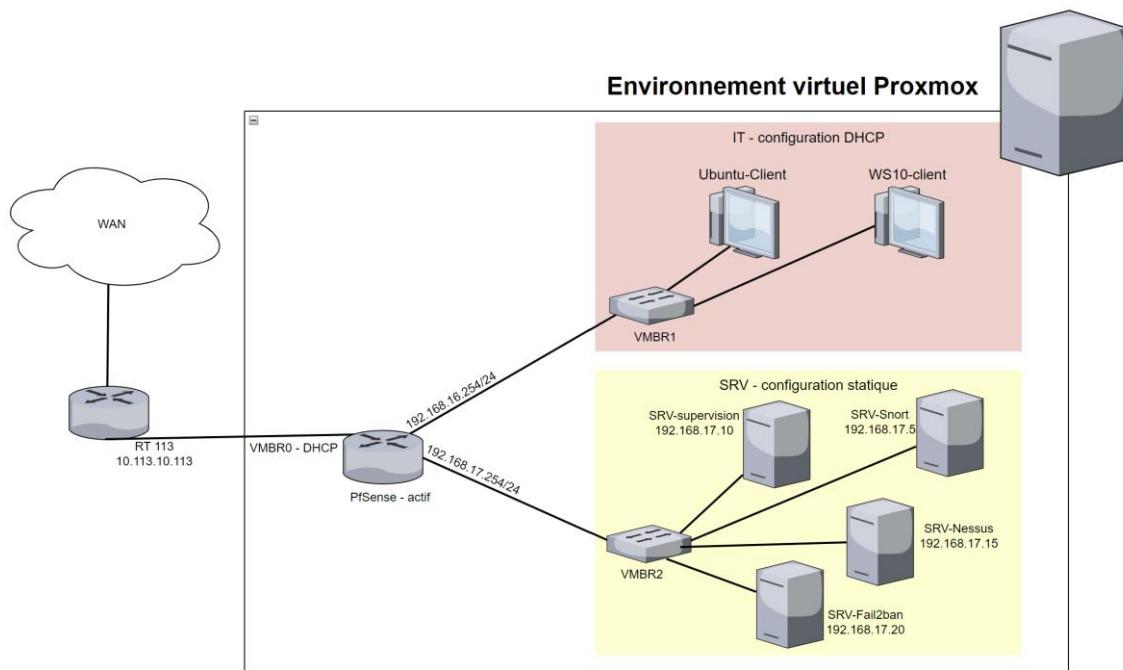
5.1.4. Planning prévisionnel

| Tâche | Durée |
|-------------------------------|--------|
| Installation des outils | 1 jour |
| Configuration des métriques | 1 jour |
| Création des tableaux de bord | 1 jour |
| Mis en place des alertes | 1 jour |
| Test et validation | 1 jour |

5.2. Plan d'adressage

| @réseau | @passerelle | NIC | Machine/rôle | DHCP ? |
|-----------------|----------------|-------|--|-------------|
| 10.113.6.0/16 | 10.113.6.11 | VMBR0 | WAN accès vers l'extérieur | Config DHCP |
| 192.168.16.0/24 | 192.168.16.254 | VMBR1 | Interface graphique : http://192.168.16.254/ | Config DHCP |
| 192.168.17.0/24 | 192.168.17.254 | VMBR2 | Interface graphique : http://192.168.17.254/ SRV-Snort: 197.168.17.5 SRV-Prometheus : 192.168.17.10 SRV-Nessus: 197.168.17.15 SRV-Fail2ban : 192.168.17.20 | Config DHCP |

5.3. Schéma réseau



5.4. Documentation technique

5.4.1. Pré-requis

Sources

Lien utile :

Page officiel Prometheus : <https://prometheus.io/download/>

Page officiel Grafana : <https://grafana.com/docs/grafana/latest/setup-grafana/installation/debian/>

Dépôt Github :

Prometheus : <https://github.com/prometheus/prometheus/releases>

Node exporter : https://github.com/prometheus/node_exporter/releases

Email

Mail : plot.6.turgot@gmail.com | Mdp : Labo-113

VM

Etape 1 : Créer la VM, avec les configurations ci-dessous.

| Nom | ID | OS | Stockage | RAM | CPU | Réseau | Services/Remarques |
|----------------|-------|--------------|----------|-----|------------------------|--------|--------------------|
| SRV-Prometheus | MV202 | Ubuntu 24.04 | 20Go | 4Go | 1 processor 1 cœurs | VVMBR2 | 192.168.17.10/24 |

Configuration réseau de la machine SRV-Prometheus

Annuler
Filaire
Appliquer

Détails
Identité
IPv4
IPv6
Sécurité

Méthode IPv4

 Automatique (DHCP)
 Manuel
 Partagée avec d'autres ordinateurs

 Réseau local seulement
 Désactiver

Adresses

Adresse
Masque de réseau
Passerelle

DNS
Automatique
8.26.56.26

Séparer les adresses IP avec des virgules

MAJ du système

```
user@srv-Prometheus:~$ sudo apt update && sudo apt upgrade -y
```

Créer un utilisateur pour Prometheus

```
user@srv-Prometheus:~$ sudo useradd --no-create-home --shell /bin/false prometheus
```

5.4.2. Prometheus

Télécharger, extraire et déplacer Prometheus

```
user@srv-Prometheus:~$ cd /tmp
```

Remplacez la version par la plus récente si nécessaire :

```
user@srv-Prometheus:~/tmp $ wget
```

<https://github.com/prometheus/prometheus/releases/download/v2.37.0/prometheus-2.37.0.linux-amd64.tar.gz>

```
user@srv-Prometheus:~/tmp $ tar xvf prometheus-2.37.0.linux-amd64.tar.gz
```



Déplacer les fichiers

```
user@srv-Prometheus:~/tmp $ cd prometheus-*/
user@srv-Prometheus:~/tmp/prometheus-2.37.0.linux-amd64$ sudo mv prometheus
/usr/local/bin/
user@srv-Prometheus:~/tmp/prometheus-2.37.0.linux-amd64$ sudo mv promtool
/usr/local/bin/
user@srv-Prometheus:~/tmp/prometheus-2.37.0.linux-amd64$ sudo mkdir /etc/prometheus
/var/lib/prometheus
user@srv-Prometheus:~/tmp/prometheus-2.37.0.linux-amd64$ sudo mv consoles/
console_libraries/ prometheus.yml /etc/prometheus/
```

Changement de propriétaire

```
user@srv-Prometheus:~/tmp/prometheus-2.37.0.linux-amd64$ sudo chown -R
prometheus:prometheus /etc/prometheus/ /var/lib/prometheus
user@srv-Prometheus:~/tmp/prometheus-2.37.0.linux-amd64$ sudo chown
prometheus:prometheus /usr/local/bin/Prometheus /usr/local/bin/promtool
```

Vérification de la version

```
hari@srv-supervision:~$ prometheus --version
prometheus, version 2.37.0 (branch: HEAD, revision: b41e0750abf5cc18d8233161560731de05199330)
  build user:      root@0ebb6827e27f
  build date:    20220714-15:13:18
  go version:    go1.18.4
  platform:      linux/amd64
```

Prometheus.service

```
user@srv-Prometheus:~/tmp/prometheus-2.37.0.linux-amd64$ sudo nano
/etc/systemd/system/prometheus.service
```

Ajoutez le contenu suivant :

```
[Unit]
Description=Prometheus
Wants=network-online.target
After=network-online.target

StartLimitIntervalSec=500
StartLimitBurst=5

[Service]
User=prometheus
Group=prometheus
Type=simple
Restart=on-failure
RestartSec=5s
ExecStart=/usr/local/bin/prometheus \
  --config.file=/etc/prometheus/prometheus.yml \
  --storage.tsdb.path=/var/lib/prometheus \
  --web.console.templates=/etc/prometheus/consoles \
  --web.console.libraries=/etc/prometheus/console_libraries \
  --web.listen-address=0.0.0.0:9090
  --web.enable-lifecycle

[Install]
WantedBy=multi-user.target
```



Recharger systemd et démarrer Prometheus

```
user@srv-Prometheus:~/tmp/prometheus-2.37.0.linux-amd64$ sudo systemctl daemon-reload
user@srv-Prometheus:~/tmp/prometheus-2.37.0.linux-amd64$ sudo systemctl enable
prometheus
user@srv-Prometheus:~/tmp/prometheus-2.37.0.linux-amd64$ sudo systemctl start prometheus
user@srv-Prometheus:~/tmp/prometheus-2.37.0.linux-amd64:~$ sudo systemctl status
prometheus
```

```
harani@srv-supervision:~$ sudo systemctl enable prometheus
Synchronizing state of prometheus.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable prometheus
harani@srv-supervision:~$ sudo systemctl start prometheus
harani@srv-supervision:~$ sudo systemctl status prometheus
● prometheus.service - Prometheus
   Loaded: loaded (/etc/systemd/system/prometheus.service; enabled; preset: enabled)
   Active: active (running) since Sun 2025-03-16 00:01:53 CET; 9s ago
     Main PID: 8701 (prometheus)
        Tasks: 6 (limit: 4610)
       Memory: 15.1M (peak: 15.4M)
          CPU: 37ms
         CGroup: /system.slice/prometheus.service
                  └─8701 /usr/local/bin/prometheus --config.file=/etc/prometheus/prometheus.yml --storage.tsdb.path=/data -->
```

Interface graphique de Prometheus

http://<Adresse_IP_server>:9090 soit ici : <http://192.168.17.10:9090>

The screenshot shows the Prometheus web interface with a dark theme. At the top, there is a navigation bar with links for Prometheus, Alerts, Graph, Status, and Help. Below the navigation bar, there are several configuration checkboxes: 'Use local time', 'Enable query history', 'Enable autocomplete' (checked), 'Enable highlighting' (checked), and 'Enable linter' (checked). A search bar with a magnifying glass icon and a placeholder 'Expression (press Shift+Enter for newlines)' is followed by a 'Execute' button. Below the search bar, there are two tabs: 'Table' (selected) and 'Graph'. A 'Evaluation time' selector with arrows is positioned between the tabs. A large text area below displays the message 'No data queried yet'. At the bottom, there are buttons for 'Add Panel' and 'Remove Panel'.

Aller dans **Status > Targets** et on peut visualiser que notre serveur est bien active.

The screenshot shows the 'Targets' page of the Prometheus web interface. The title 'Targets' is at the top. Below it, there are buttons for 'All', 'Unhealthy', and 'Collapse All', and a search bar with a placeholder 'Filter by endpoint or labels'. A table titled 'prometheus (1/1 up)' shows one active endpoint. The table has columns: Endpoint, State, Labels, Last Scrape, Duration, and Error. The single entry is: Endpoint 'http://localhost:9090/metrics', State 'UP', Labels 'instance="localhost:9090"', 'job="prometheus"', Last Scrape '7.778s ago', Duration '2.332ms', and Error is empty.

| Endpoint | State | Labels | Last Scrape | Duration | Error |
|-------------------------------|-------|--|-------------|----------|-------|
| http://localhost:9090/metrics | UP | instance="localhost:9090",job="prometheus" | 7.778s ago | 2.332ms | |



5.4.3. Node Exporter (client Linux)

Installer sur tous les machines Linux de l'infrastructure virtuel.

Créer un utilisateur pour Node Exporter

```
user@srv-Prometheus:~$ sudo useradd --no-create-home --shell /bin/false node_exporter
user@srv-Prometheus:~$ cd /tmp
```

Télécharger, extraire et déplacer Node Exporter

```
user@srv-Prometheus:~/tmp $ wget
https://github.com/prometheus/node_exporter/releases/download/v.1.9.1/node_exporter-
1.9.1.linux-amd64.tar.gz

user@srv-Prometheus:~/tmp $ tar -xvf node_exporter-1.9.0.linx-amd64.tar.gz
user@srv-Prometheus:~/tmp $ cd node_exporter-*/
```

```
user@srv-Prometheus:~/tmp/node_exporter-1.9.1.linux-amd64 $ sudo mv node_exporter
/usr/local/bin/
```

```
user@srv-Prometheus:~/tmp/node_exporter-1.9.1.linux-amd64 $ sudo chown
node_exporter:node_exporter /usr/local/bin/node_exporter
```

Création du fichier node_exporter.service

```
user@srv-Prometheus:~$ sudo nano /etc/systemd/system/node_exporter.service
```

```
GNU nano 7.2                               /etc/systemd/system/node_exporter.service *
[Unit]
Description=Node Exporter
Wants=network-online.target
After=network-online.target

StartLimitIntervalSec=500
StartLimitBurst=5

[Service]
User=node_exporter
Group=node_exporter
Type=simple
Restart=on-failure
RestartSec=5s
ExecStart=/usr/local/bin/node_exporter \
--collector.logind

[Install]
WantedBy=multi-user.target
```

Démarrer le Node Exporter

```
user@srv-Prometheus:~$ sudo systemctl daemon-reload
```

```
user@srv-Prometheus:~$ sudo systemctl enable node_exporter
```

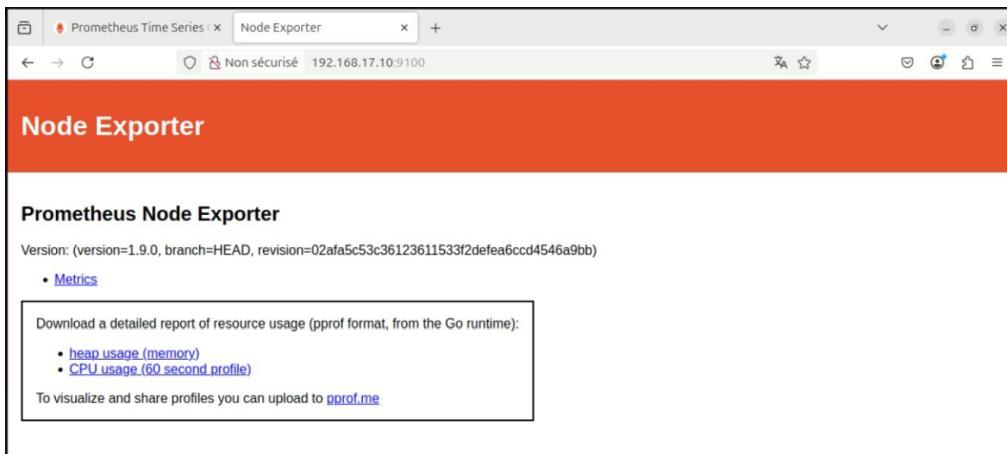


```
user@srv-Prometheus:~$ sudo systemctl start node_exporter
```

```
user@srv-Prometheus:~$ sudo systemctl status node_exporter
```

```
hariharani@srv-supervision:~$ sudo systemctl status node_exporter
● node_exporter.service - Node Exporter
   Loaded: loaded (/etc/systemd/system/node_exporter.service; enabled; preset: enabled)
   Active: active (running) since Sun 2025-03-16 01:03:50 CET; 9s ago
     Main PID: 11133 (node_exporter)
        Tasks: 3 (limit: 4610)
       Memory: 2.0M (peak: 2.2M)
          CPU: 5ms
        CGroup: /system.slice/node_exporter.service
                  └─11133 /usr/local/bin/node_exporter --collector.logind
```

Sur le navigateur taper : 192.168.17.10:9100



Modification du fichier de configuration Prometheus.yml

```
user@srv-Prometheus:~$ sudo nano /etc/prometheus/prometheus.yml
```

Ajouter cette section sous **scrape_configs** :

```
scrape_configs:
  # The job name is added as a label `job=<job_name>` to any timeseries scraped from this config.
  - job_name: "prometheus"

    # metrics_path defaults to '/metrics'
    # scheme defaults to 'http'.
    static_configs:
      - targets: ["localhost:9090"]

  - job_name: "node_exporter"
    static_configs:
      - targets: ["localhost:9100"]
```

Le localhost peut-être remplacer par l'adresse IP des hôtes aussi.

**Redémarrer le service prometheus :**

```
user@srv-Prometheus:~$:~$ sudo systemctl restart Prometheus
```

Vérifier l'interface graphique de Prometheus. Vous devrez trouver comme ci-dessous dans **Status > Targets** :

The screenshot shows the Prometheus Targets page. At the top, there are buttons for 'All', 'Unhealthy', and 'Collapse All', along with a search bar and a filter for 'Labels'. Below this, there are two sections: 'node_exporter (1/1 up)' and 'prometheus (1/1 up)'. Each section contains a table with columns: Endpoint, State, Labels, Last Scrape, Scrape Duration, and Error. For the 'node_exporter' section, the table shows:

| Endpoint | State | Labels | Last Scrape | Scrape Duration | Error |
|-------------------------------|-------|---|-------------|-----------------|-------|
| http://localhost:9100/metrics | UP | instance="localhost:9100",job="node_exporter" | 12.323s ago | 23.972ms | |

For the 'prometheus' section, the table shows:

| Endpoint | State | Labels | Last Scrape | Scrape Duration | Error |
|-------------------------------|-------|--|-------------|-----------------|-------|
| http://localhost:9090/metrics | UP | instance="localhost:9090",job="prometheus" | 9.526s ago | 2.274ms | |



5.4.4. Windows Exporter (client Windows)

Installation de Windows Exporter

Dépôt Github : https://github.com/prometheus-community/windows_exporter/releases

Ici, je vais choisir la version 0.19.0 et télécharger le .exe

| Asset | Size | Published |
|-----------------------------------|-----------|--------------|
| sha256sums.txt | 396 Bytes | Jul 23, 2022 |
| windows_exporter-0.19.0-386.exe | 18.3 MB | Jul 23, 2022 |
| windows_exporter-0.19.0-386.msi | 9.5 MB | Jul 23, 2022 |
| windows_exporter-0.19.0-amd64.exe | 18.3 MB | Jul 23, 2022 |
| windows_exporter-0.19.0-amd64.msi | 9.39 MB | Jul 23, 2022 |
| Source code (zip) | | Jul 23, 2022 |
| Source code (tar.gz) | | Jul 23, 2022 |

Lancer le fichier, une fois téléchargé.

Lancer Windows Exporter en arrière-plan au démarrage

Pour éviter de le lancer à chaque fois on va le lancer en tant que service en arrière-plan au démarrage :

Clic droit > créer un raccourci

Win + R > shell:startup déplacer le raccourci dedans.

Ou

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

Et copier le fichier .exe



5.4.4. Grafana

Installation de Grafana

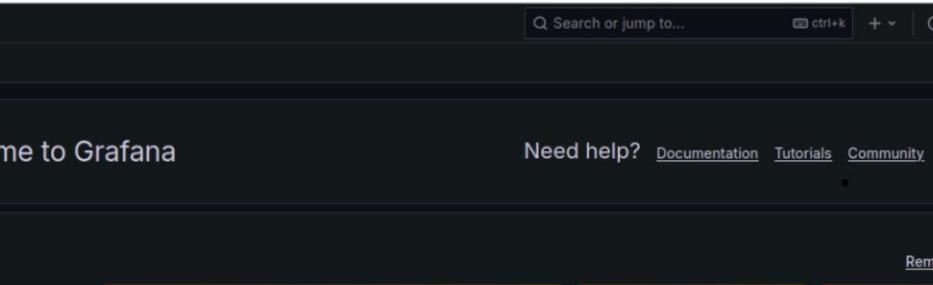
```
user@srv-Prometheus:~$ sudo apt-get install -y apt-transport-https software-properties-common wget
user@srv-Prometheus:~$ sudo mkdir -p /etc/apt/keyrings/
user@srv-Prometheus:~$ wget -q -O - https://apt.grafana.com/gpg.key | gpg --dearmor | sudo tee /etc/apt/keyrings/grafana.gpg > /dev/null
user@srv-Prometheus:~$ echo "deb [signed-by=/etc/apt/keyrings/grafana.gpg] https://apt.grafana.com stable main" | sudo tee -a /etc/apt/sources.list.d/grafana.list
user@srv-Prometheus:~$ sudo apt-get update
```

```
user@srv-Prometheus:~$ sudo apt-get install grafana
user@srv-Prometheus:~$ sudo /bin/systemctl start grafana-server
user@srv-Prometheus:~$ sudo /bin/systemctl status grafana-server
```

```
● grafana-server.service - Grafana instance
  Loaded: loaded (/usr/lib/systemd/system/grafana-server.service; disabled; preset: enabled)
  Active: active (running) since Sun 2025-03-16 21:35:49 CET; 1min 25s ago
    Docs: http://docs.grafana.org
  Main PID: 4841 (grafana)
    Tasks: 7 (limit: 4610)
   Memory: 106.5M (peak: 110.9M)
      CPU: 2.576s
     CGroup: /system.slice/grafana-server.service
             └─4841 /usr/share/grafana/bin/grafana server --config=/etc/grafana/grafana.ini --pidfile=/run/grafana/grafan...
```

Vérifier en accédant l'interface Web avec : <http://localhost:3000>

Changer le mot de passe par défaut et vous tomberez sur cette page :

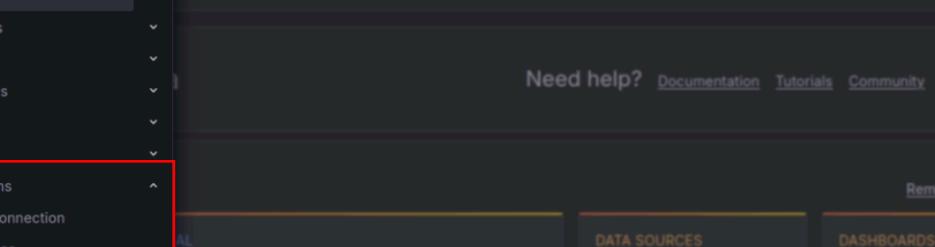


The screenshot shows the Grafana landing page. At the top, there are three tabs: "Prometheus Time Series" (active), "Node Exporter", and "Install Grafana on Debian". Below the tabs, the URL is "localhost:3000/?orgId=1&from=now-6h&to=now&timezone=browser". The main content area has a dark background. On the left, a "Basic" section is shown with a "TUTORIAL" card. The card contains "DATA SOURCE AND DASHBOARDS" and "Grafana fundamentals" sections. The "Grafana fundamentals" section describes setting up and understanding Grafana. On the right, there are three cards: "DATA SOURCES" (with "Add your first data source" and "Learn how in the docs" buttons), "DASHBOARDS" (with "Create your first dashboard" and "Learn how in the docs" buttons), and a "Remove this panel" button. At the bottom, there are links for "Dashboards", "Starred dashboards", and "Recently viewed dashboards". The "Latest from the blog" section is also visible.

Par défaut : id : admin | mdp : admin

Liées les sources de données

Allez dans **Connections > Data sources**



The screenshot shows the Grafana interface. The left sidebar is open, displaying navigation options: Home, Bookmarks, Starred, Dashboards, Explore, Alerting, Connections, Add new connection, Data sources, and Administration. The 'Alerting' option is highlighted with a red box. The main content area features a search bar at the top right. Below the search bar, a 'Need help?' section includes links to Documentation, Tutorials, Community, and Public Slack. The main content area is divided into several sections: 'AL' (with a 'Get started' button), 'SOURCE AND DASHBOARDS' (with 'Grafana fundamentals' and a 'Tutorial' button), 'DATA SOURCES' (with 'Add your first data source' and a 'Tutorial' button), and 'DASHBOARDS' (with 'Create your first dashboard' and a 'Tutorial' button). At the bottom, there are sections for 'Latest from the blog' and 'Grafana Cloud'.

Cliquer sur « **Add data source** » :

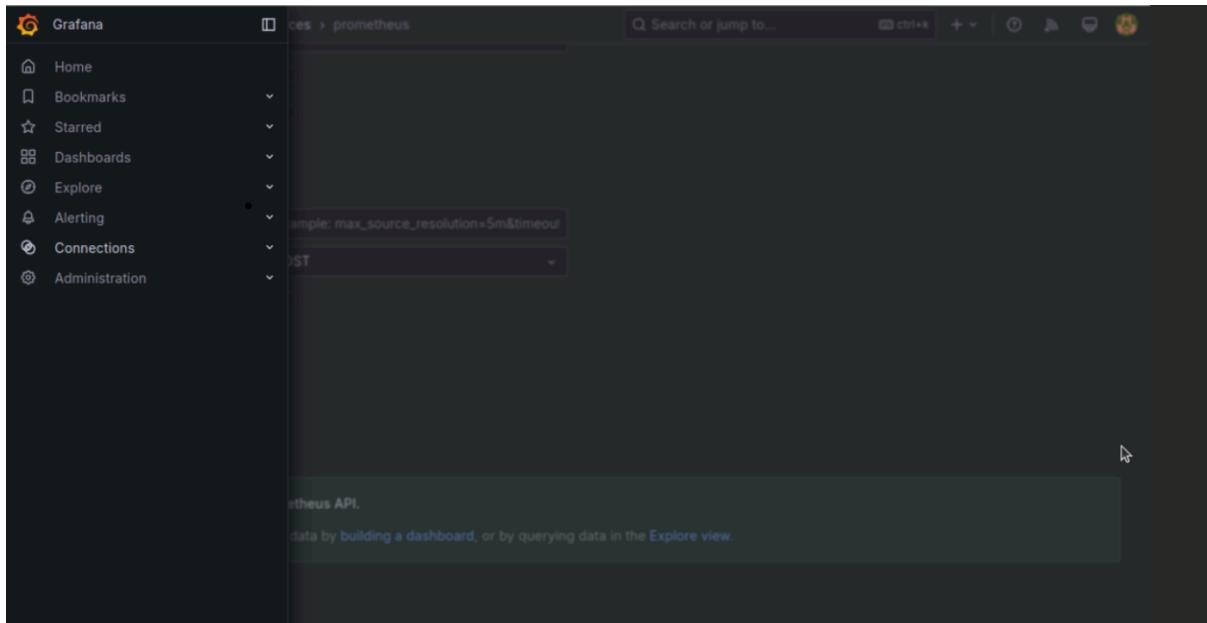


Sélectionner Prometheus et renseigner l'URL : <http://localhost:9090> oui bien l'adresse du serveur :

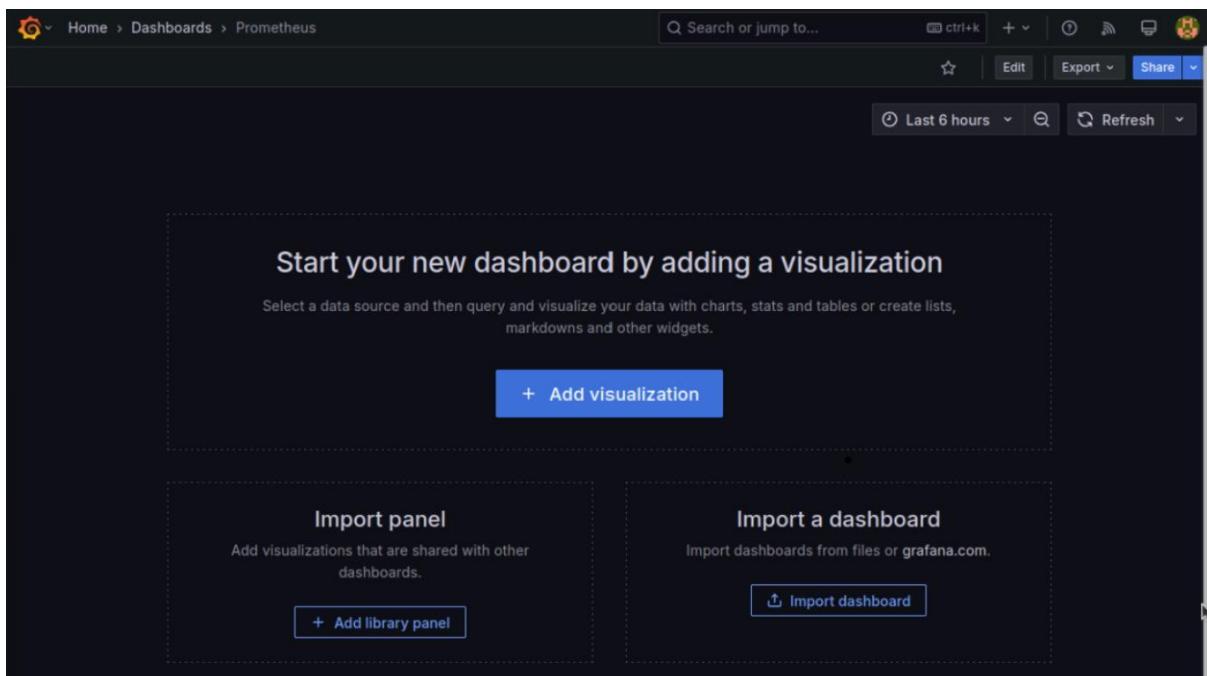
Aller tout en bas et cliquer sur Valider & Test :

Création du Dashboard

Cliquer dans Dashboard



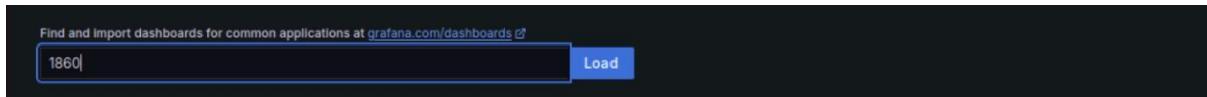
Cliquer à droite dans New > New Dashboard > Import Dashboard et nommé le Dashboard Prometheus.



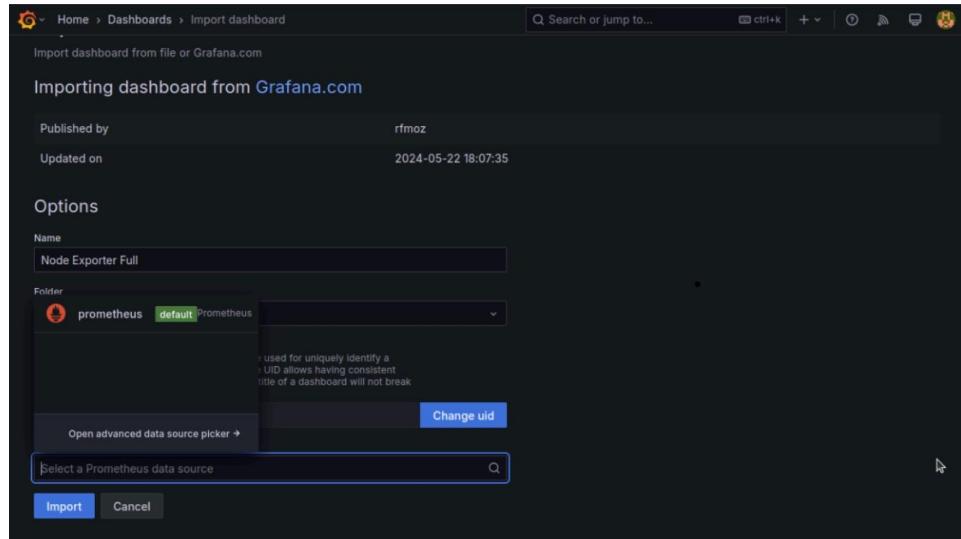
Importation d'un modèle de Dashboard :

Grafana propose des dashboards prêts à l'emploi sur **Grafana.com**. dans notre contexte :

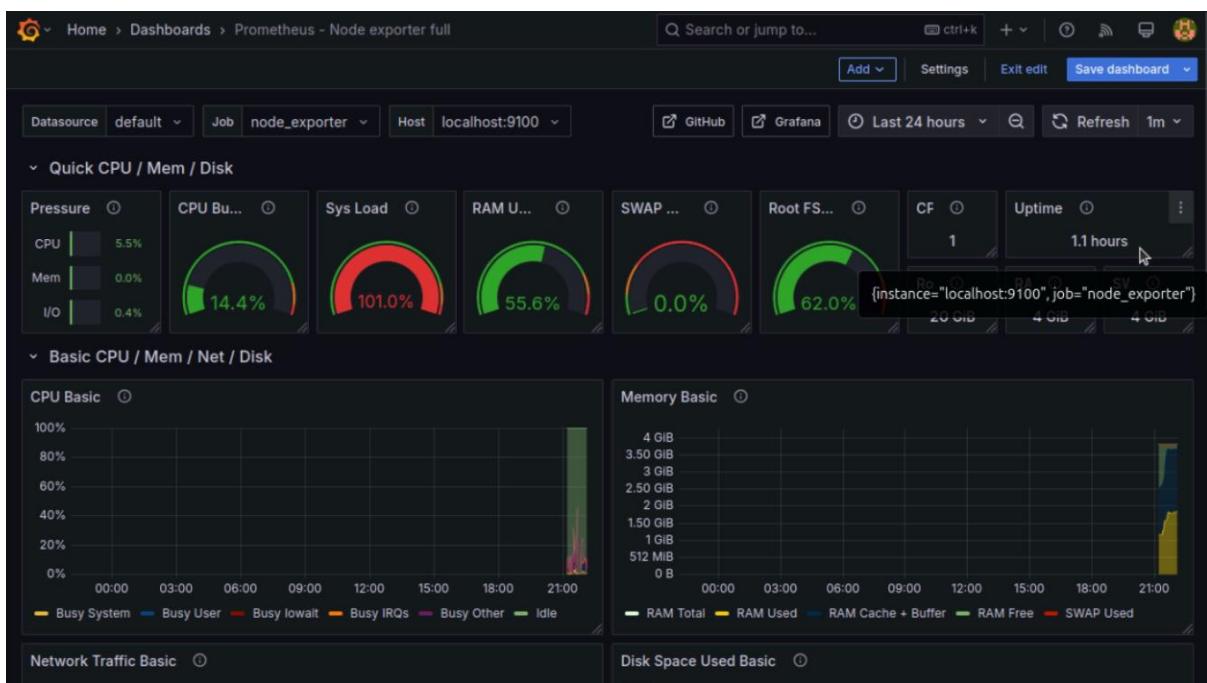
1. Chercher **Node Exporter Full** (ID 1860), cliquer sur "Import", puis entre l'ID du dashboard et cliquer sur **load**



Sélectionner Prometheus pour les données de sources et importer le :



Résultat obtenu du Dashboard :





5.4.5. Alertmanager

Créer les dossiers nécessaires

```
user@srv-Prometheus:~$ sudo useradd --no-create-home --shell /bin/false alertmanager
user@srv-Prometheus:~$ sudo mkdir -p /etc/alertmanager /var/lib/alertmanager
user@srv-Prometheus:~$ sudo chown -R alertmanager:alertmanager /etc/alertmanager
/var/lib/alertmanager
```

Télécharger Alertmanager

```
user@srv-Prometheus:~$ cd /tmp
user@srv-Prometheus:~/tmp $ wget
https://github.com/prometheus/alertmanager/releases/download/v0.28.0/alertmanager-
0.28.0.linux-amd64.tar.gz
user@srv-Prometheus:~/tmp $ tar xvf alertmanager-*
user@srv-Prometheus:~/tmp $ cd alertmanager-*/
user@srv-Prometheus:~/tmp/alertmanager-0.28.0.linux-amd64 $ sudo cp alertmanager amtool
/usr/local/bin/
user@srv-Prometheus:~/tmp/alertmanager-0.28.0.linux-amd64 $ sudo chown
alertmanager:alertmanager /usr/local/bin/alertmanager /usr/local/bin/amtool
```

Créer un mot de passe applicative pour alertmanager

On ne peut pas utiliser le mot de passe Gmail classique ici. Il faut créer un mot de passe d'application.

Étapes :

1. Aller sur : <https://myaccount.google.com/security>
2. Activer la **validation en deux étapes**
3. Ensuite, tu verras une option “**Mots de passe des applications**”
4. Générer un mot de passe pour l'application (ex : “Alertmanager”)
5. Noter ce mot de passe



Créer le fichier de configuration

```
user@srv-Prometheus:~/tmp/alertmanager-0.28.0.linux-amd64 $ sudo nano  
/etc/alertmanager/alertmanager.yml
```

```
global:  
  smtp_smarthost: 'smtp.gmail.com:587'  
  smtp_from: 'plot.6.turgot@gmail.com'  
  smtp_auth_username: 'plot.6.turgot@gmail.com'  
  smtp_auth_password: 'gmgeoijtbdxwahxb'  
  smtp_require_tls: true  
  resolve_timeout: 5m  
  
route:  
  receiver: 'default'  
  
receivers:  
  - name: 'default'  
    email_configs:  
      - to: 'plot.6.turgot@gmail.com'
```

Dans smtp_auth_password, entrer le mot de passe générer par Google sans espace.

Créer le service systemd

```
user@srv-Prometheus:~/tmp/alertmanager-0.28.0.linux-amd64 $ sudo nano  
/etc/systemd/system/alertmanager.service
```

```
[Unit]  
Description=Alertmanager  
Wants=network-online.target  
After=network-online.target  
  
[Service]  
User=alertmanager  
Group=alertmanager  
Type=simple  
ExecStart=/usr/local/bin/alertmanager \  
  --config.file=/etc/alertmanager/alertmanager.yml \  
  --storage.path=/var/lib/alertmanager  
Restart=always  
  
[Install]  
WantedBy=multi-user.target
```

```
user@srv-Prometheus:~/tmp/alertmanager-0.28.0.linux-amd64 $ sudo systemctl daemon-  
reexec  
user@srv-Prometheus:~/tmp/alertmanager-0.28.0.linux-amd64 $ sudo systemctl daemon-  
reload  
user@srv-Prometheus:~/tmp/alertmanager-0.28.0.linux-amd64 $ sudo systemctl start  
alertmanager  
user@srv-Prometheus:~/tmp/alertmanager-0.28.0.linux-amd64 $ sudo systemctl enable  
alertmanager  
user@srv-Prometheus:~/tmp/alertmanager-0.28.0.linux-amd64 $ sudo systemctl status  
alertmanager
```



```
user@srv-prometheus:/tmp/alertmanager-0.28.0.linux-amd64$ sudo systemctl status alertmanager
● alertmanager.service - Alertmanager
   Loaded: loaded (/etc/systemd/system/alertmanager.service; enabled; preset: enabled)
   Active: active (running) since Sun 2025-04-06 19:56:47 CEST; 7s ago
     Main PID: 46833 (alertmanager)
        Tasks: 6 (limit: 4610)
       Memory: 13.7M (peak: 13.9M)
          CPU: 45ms
        CGroup: /system.slice/alertmanager.service
                  └─46833 /usr/local/bin/alertmanager --config.file=/etc/alertmanager/alertmanager.yml --storage.path=/var/lib/alertmanager

avr 06 19:56:47 srv-prometheus systemd[1]: Started alertmanager.service - Alertmanager.
avr 06 19:56:47 srv-prometheus alertmanager[46833]: time=2025-04-06T17:56:47.514Z level=INFO source=main.go:191 msg=">
avr 06 19:56:47 srv-prometheus alertmanager[46833]: time=2025-04-06T17:56:47.515Z level=INFO source=main.go:192 msg=">
avr 06 19:56:47 srv-prometheus alertmanager[46833]: time=2025-04-06T17:56:47.515Z level=INFO source=cluster.go:185 ms>
avr 06 19:56:47 srv-prometheus alertmanager[46833]: time=2025-04-06T17:56:47.532Z level=INFO source=cluster.go:674 ms>
avr 06 19:56:47 srv-prometheus alertmanager[46833]: time=2025-04-06T17:56:47.553Z level=INFO source=coordinator.go:11>
avr 06 19:56:47 srv-prometheus alertmanager[46833]: time=2025-04-06T17:56:47.554Z level=INFO source=coordinator.go:12>
avr 06 19:56:47 srv-prometheus alertmanager[46833]: time=2025-04-06T17:56:47.555Z level=INFO source=tls_config.go:347>
avr 06 19:56:47 srv-prometheus alertmanager[46833]: time=2025-04-06T17:56:47.555Z level=INFO source=tls_config.go:350>
avr 06 19:56:49 srv-prometheus alertmanager[46833]: time=2025-04-06T17:56:49.532Z level=INFO source=cluster.go:699 ms>
lines 1-20/20 (END)
```

Configurer les règles d'alerte dans Prometheus

```
user@srv-Prometheus:~$ sudo nano /etc/prometheus/alert_rules.yml
```

Configurer une règle d'alerte dans Prometheus pour envoyer une alerte lorsque l'espace disque est inférieur à 20%.

```
groups:
- name: alert_rules
  rules:
  - alert: LowDiskSpace
    expr: (node_filesystem_avail_bytes{fstype=~"ext4|xfs"} / node_filesystem_size_bytes{fstype=~"ext4|xfs"}) < 0.2
    for: 5m
    labels:
      severity: critical
    annotations:
      summary: "Espace disque faible sur {{ $labels.instance }}"
      description: "L'espace disque est inférieur à 20% sur {{ $labels.instance }}"
```

Explication :

La capture montre la configuration d'une règle d'alerte dans un fichier YAML utilisé pour un système de surveillance. Voici l'explication des lignes principales :

- **Groups** : Crée un groupe de règles, ici nommé alert_rules.
- **Rules** : Contient une liste de règles d'alerte spécifiques.
- **Alert**: LowDiskSpace : Nom de l'alerte, qui est déclenchée en cas de faible espace disque.
- **expr** :
(node_filesystem_avail_bytes{fstype=~"ext4|xfs"} / node_filesystem_size_bytes{fstype=~"ext4|xfs"}) < 0.2
 - Vérifie si l'espace disponible (en octets) est inférieur à 20 % de la taille totale sur des systèmes de fichiers de type ext4 ou xfs.
- **for**: 5m : La condition doit durer 5 minutes avant que l'alerte soit déclenchée.
- **labels**: severity: critical : Indique que l'alerte a un niveau de gravité critical.
- **Annotations** :
 - **summary** : Résume l'alerte (ici, espace disque faible).
 - **Description** : Fournit un message détaillé en français, précisant l'instance et le point de montage concernés.



Configurer Prometheus pour envoyer des alertes

```
user@srv-Prometheus:~/alertmanager-0.28.0.linux-amd64$ sudo nano
/etc/prometheus/prometheus.yml
```

Modifier les parties comme ci-dessous :

```
# Alertmanager configuration
alerting:
  alertmanagers:
    - static_configs:
      - targets:
          - 'localhost:9093'

# Load rules once and periodically from disk
rule_files:
  - "alert_rules.yml"
```

Redémarrer tout les services

```
user@srv-Prometheus:~$ sudo systemctl restart prometheus
user@srv-Prometheus:~$ sudo systemctl restart alertmanager
```

Vérification

Aller sur l'interface web de Prometheus :

http://localhost:9090

- Menu Alerts
- Tu devrais voir "LowDiskSpace"
- Déclenche-la manuellement en réduisant ton espace disque (ou en modifiant la règle pour tester : < 0.95 par exemple).

The screenshot shows the Prometheus Alerting interface. At the top, there are buttons for 'Inactive (1)', 'Pending (0)', and 'Firing (0)'. A search bar is labeled 'Filter by name or labels'. Below the buttons, a list of alert rules is shown. One rule is expanded, revealing its configuration:

```
name: LowDiskSpace
expr: (node_filesystem_avail_bytes{fstype=~"ext4|xfs"} / node_filesystem_size_bytes{fstype=~"ext4|xfs"}) < 0.2
for: 10m
labels:
  severity: critical
annotations:
  description: L'espace disque est inférieur à 20% sur {{ $labels.instance }}
  summary: Espace disque faible sur {{ $labels.instance }}
```



5.5. Simulation d'espace disque faible

1. Installer Node Exporter sur les machines Linux et Windows Exporter sur Windows.

2. SRV-Prometheus :

Ajouter les IP des serveurs dans le fichier de configuration (*par rapport à mon environnement virtuel*)

```
user@srv-Prometheus:~$ sudo nano /etc/prometheus/prometheus.yml
```

```
- job_name: "node_exporter"

  # metrics_path defaults to '/metrics'
  # scheme defaults to 'http'.

  static_configs:
    - targets: ["localhost:9100"]
      labels:
        instance: 'SRV-Prometheus'

    - targets: ["192.168.17.5:9100"]
      labels:
        instance: 'SRV-Snort'

    - targets: ["192.168.17.15:9100"]
      labels:
        instance: 'SRV-Nessus'

    - targets: ["192.168.17.20:9100"]
      labels:
        instance: 'SRV-Fail2Ban'

    - targets: ["192.168.17.25:9100"]
      labels:
        instance: 'SRV-LAMP-GLPI-BackupManager'
```

```
user@srv-Prometheus:~$ sudo systemctl restart prometheus
```

3. Accéder à l'interface graphique de Prometheus : <http://192.168.17.10:9090> Status > Targets



Remarque :

Si certaines machine sont en DOWN, activer le port 9100 :

```
user@srv-Prometheus:~$ sudo ufw allow 9100
```

| Endpoint | State | Labels | Last Scrape | Scrape Duration | Error |
|-----------------------------------|-------|--|-------------|-----------------|-------|
| http://192.168.17.10:9100/metrics | UP | instances="192.168.17.10:9100" job="node exporter" | 3.297s ago | 15.131ms | |
| http://192.168.17.15:9100/metrics | UP | instances="192.168.17.15:9100" job="node exporter" | 11.293s ago | 16.286ms | |
| http://192.168.17.20:9100/metrics | UP | instances="192.168.17.20:9100" job="node exporter" | 12.198s ago | 14.508ms | |
| http://192.168.17.25:9100/metrics | UP | instances="192.168.17.25:9100" job="node exporter" | 8.393s ago | 12.730ms | |
| http://localhost:9100/metrics | UP | instances="localhost:9100" job="node exporter" | 13.455s ago | 15.204ms | |
| http://192.168.17.5:9100/metrics | UP | instances="192.168.17.5:9100" job="node exporter" | 11.742s ago | 20.433ms | |

| Endpoint | State | Labels | Last Scrape | Scrape Duration | Error |
|-------------------------------|-------|--|-------------|-----------------|-------|
| http://localhost:9090/metrics | UP | instance="localhost:9090" job="prometheus" | 7.844s ago | 3.203ms | |

4. SRV-Fail2Ban

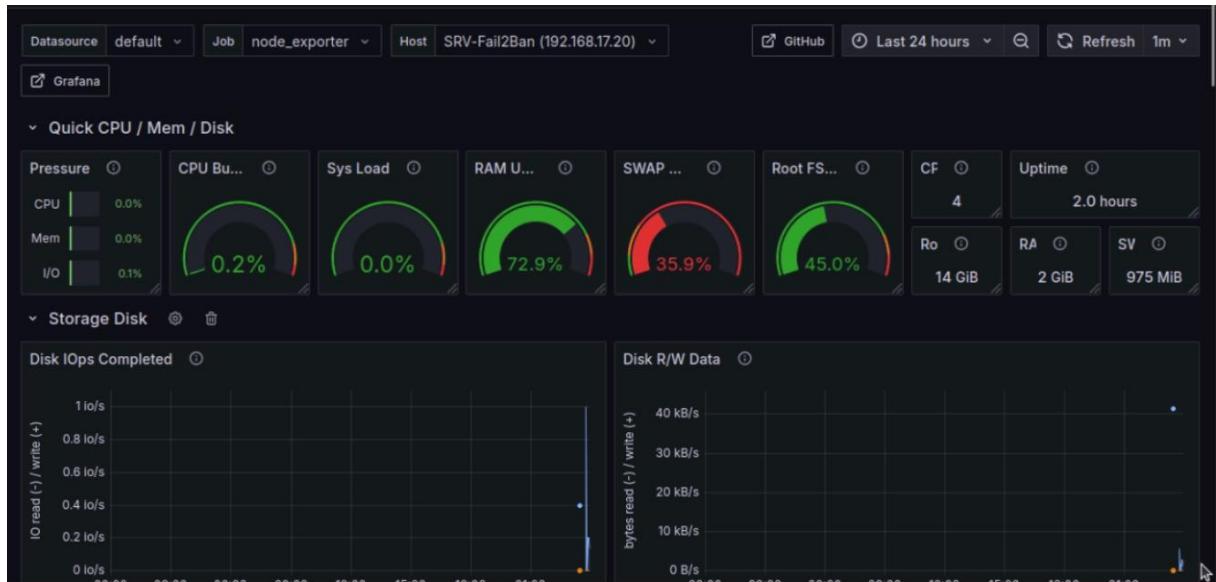
Cette machine l'a 15Go de stockage. On va installer des fichiers de 1Go pour utiliser un maximum d'espace disque et voir si l'alerte est bien déclenché.

Au départ :

| Statut | running |
|--------------------------------|------------|
| Etat de la haute disponibilité | aucun |
| Nœud | turgot-sio |

| Utilisation processeur | 0.80 % de 4 Processeur(s) |
|-----------------------------|-------------------------------|
| Utilisation mémoire | 86.81 % (1.74 Gi sur 2.00 Gi) |
| Taille du disque d'amorçage | 15.00 Gi |

Utilisation processeur



```
root@SRV-Fail2ban:~# df -h
Sys. de fichiers Taille Utilisé Dispo Utile% Monté sur
udev          951M      0  951M  0% /dev
tmpfs         197M  1,2M  196M  1% /run
/dev/sda1     14G  7,5G  5,7G  57% /
tmpfs         984M      0  984M  0% /dev/shm
tmpfs         5,0M      0  5,0M  0% /run/lock
tmpfs         197M  108K  197M  1% /run/user/1000
root@SRV-Fail2ban:~# dd if=/dev/zero of=~/test_file1 bs=M count=2000
2000+0 enregistrements lus
2000+0 enregistrements écrits
2097152000 octets (2,1 GB, 2,0 GiB) copiés, 2,22593 s, 942 MB/s
```

5. Remplir l'espace disque (pour tester)

5.1. Vérifier l'utilisation de l'espace disque

Tu peux vérifier l'espace disque pour voir si tu as bien réduit l'espace libre à moins de 20 % en utilisant la commande suivante :

```
user@srv-fail2ban:~$ df -h
```

Créer un fichier de grande taille (2Go)

```
user@srv-fail2ban:~$ dd if=/dev/zero of=~/test_file1 bs=1M count=2000
```

Une fois avoir créer plusieurs fichiers :



```
root@SRV-Fail2ban:~# df -h
Sys. de fichiers Taille Utilisé Dispo Utile% Monté sur
udev              951M      0  951M  0% /dev
tmpfs             197M  1,2M  196M  1% /run
/dev/sda1          14G   12G  1,7G  87% /
tmpfs             984M      0  984M  0% /dev/shm
tmpfs              5,0M      0  5,0M  0% /run/lock
tmpfs             197M   112K  197M  1% /run/user/1000
root@SRV-Fail2ban:~#
```

6. Vérifier si l'alerte se déclenche dans Prometheus

Une fois l'espace disque réduit sous les 20 %, vérifie que l'alerte est bien déclenchée dans **Prometheus**. Consulter les alertes actives dans Prometheus avec la commande suivante :

- Accéder à l'interface web de Prometheus (<http://192.168.17.10:9090>).
- Aller dans l'onglet **Alerts** pour voir les alertes actives. Si l'alerte est bien configurée, tu devrais la voir apparaître une fois que l'espace disque tombe sous les 20 %.

The screenshot shows the Prometheus Alert Rules interface. The URL is /etc/prometheus/alert_rules.yml > alert_rules. There is 1 active alert named 'LowDiskSpace'. The alert configuration is as follows:

```
name: LowDiskSpace
expr: (node_filesystem_avail_bytes{fstype=="ext4|xfs"} / node_filesystem_size_bytes{fstype=="ext4|xfs"}) < 0.2
for: 5m
labels:
  severity: critical
annotations:
  description: L'espace disque est inférieur à 20% sur {{ $labels.instance }}
  summary: Espace disque faible sur {{ $labels.instance }}
```

Below the configuration, a table shows the active alert details:

| Labels | State | Active Since | Value |
|--|---------|--------------------------------|---------------------|
| alarmname:LowDiskSpace device:/dev/sda1 fstype:ext4 instance:SRV-Fail2Ban (192.168.17.20) job:node_exporter mountpoint:/ severity:critical | PENDING | 2025-04-06T22:16:15.551272403Z | 0.12337509263938719 |

📌 Résumé de la situation dans Prometheus

- **🔔 Alerte détectée** : LowDiskSpace est en état **PENDING**.
- **⌚ Depuis** : le 6 avril 2025 à 22:05 UTC.
- **☒ Valeur actuelle** : 0.123 → soit **12.3 % d'espace libre**.
- **💻 Instance concernée** : SRV-Fail2Ban (192.168.17.20).
- **⌚ Périphérique** : /dev/sda1, monté sur /.

🔍 Que signifie le statut PENDING ?

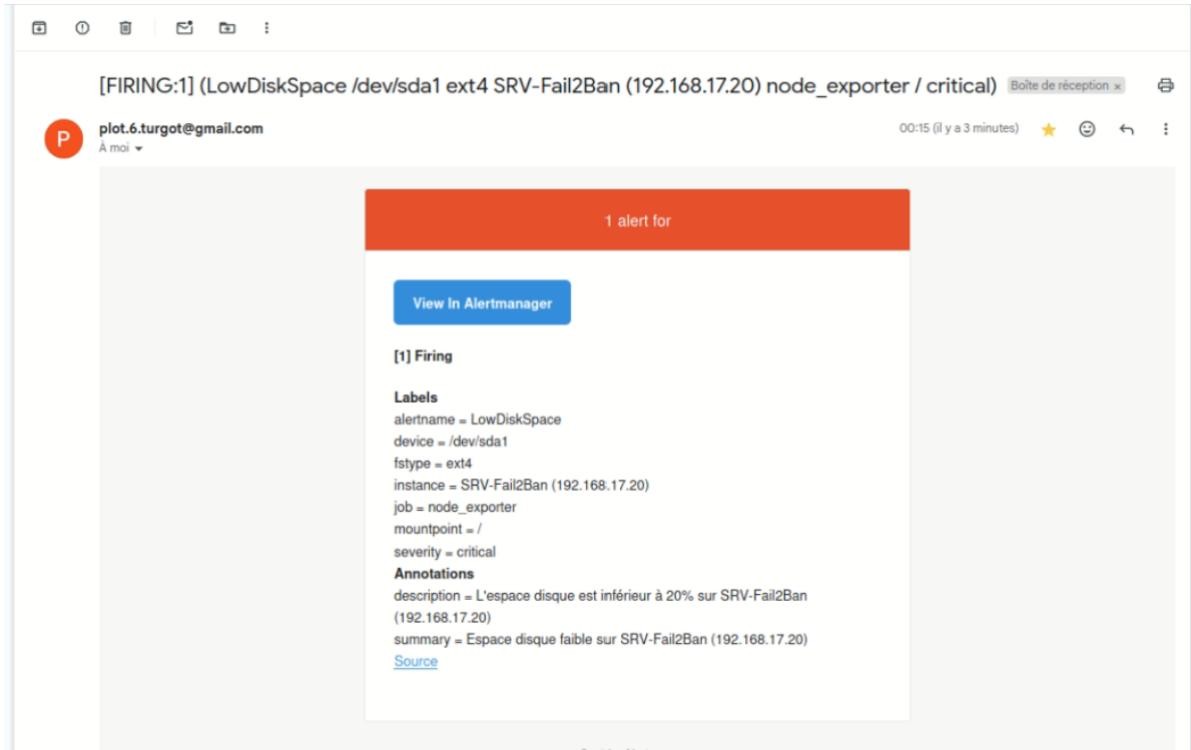
L'état PENDING dans Prometheus signifie que :

- ⌚ La condition de l'alerte est **vraie** maintenant, mais elle doit rester vraie **pendant 5 minutes** (comme spécifié dans for: 5m) **avant de passer à l'état FIRING**, qui déclenche Alertmanager.



👉 Donc actuellement, **l'alerte attend** de voir si le disque reste sous 20 % de libre **pendant 5 minutes complètes** avant de t'envoyer une alerte via Alertmanager.

7. Notification par mail





5.6. Cahier de recettes

1. Installation et configuration de Prometheus

- Installation de Prometheus
- Configuration du fichier prometheus.yml
- Ajout de Node Exporter pour collecter les métriques système
- Vérification du bon fonctionnement

2. Installation et configuration de Grafana

- Installation de Grafana
- Configuration de la source de données (Prometheus)
- Création d'un tableau de bord avec les métriques principales

3. Installation et configuration d'Alertmanager

- Installation d'Alertmanager
- Configuration du fichier alertmanager.yml
- Ajout des règles d'alerte dans alert_rules.yml
- Test des alertes

4. Mise en place d'une alerte sur l'espace disque

- Création d'une règle d'alerte pour détecter un disque plein
- Configuration de l'alerte dans Alertmanager
- Test et validation

5.7. Cahier de test

| Test | OK | Remarque |
|---|----|----------|
| Vérifier l'état des services Prometheus, Node Exporter, Grafana et Alertmanager | Ok | |
| Installer Node Exporter sur tous les serveurs | Ok | |
| Rendre l'espace disque d'une machine supérieur à 80% de libre. | Ok | |
| Tester la détection d'une faible disponibilité d'espace disque. | Ok | |
| Visualiser l'alerte sur Prometheus et Grafana. | Ok | |
| Recevoir la notification via mail. | Ok | |



6. Analyse de vulnérabilités : Nessus

6.1. Cahier des charges

6.1.1. Contexte et Objectifs

Contexte

Nessus est une solution de gestion des vulnérabilités permettant d'analyser et d'identifier les failles de sécurité au sein d'un réseau informatique. Son déploiement vise à renforcer la cybersécurité de l'infrastructure et à prévenir les risques d'attaques.

Objectif

- Installer et configurer Nessus sur le réseau interne.
- Assurer la sécurisation et la mise à jour de l'outil.
- Former les administrateurs à l'utilisation de Nessus.

6.1.2. Descriptions fonctionnelles des besoins

- Scanner le réseau et identifier les vulnérabilités.
- Automatiser les audits de sécurité.

6.1.3. Cahier des charges technique

- Serveur dédié ou machine virtuelle compatible, OS Linux.
- Configuration réseau permettant la communication avec les équipements à auditer.

6.1.4. Planning prévisionnel

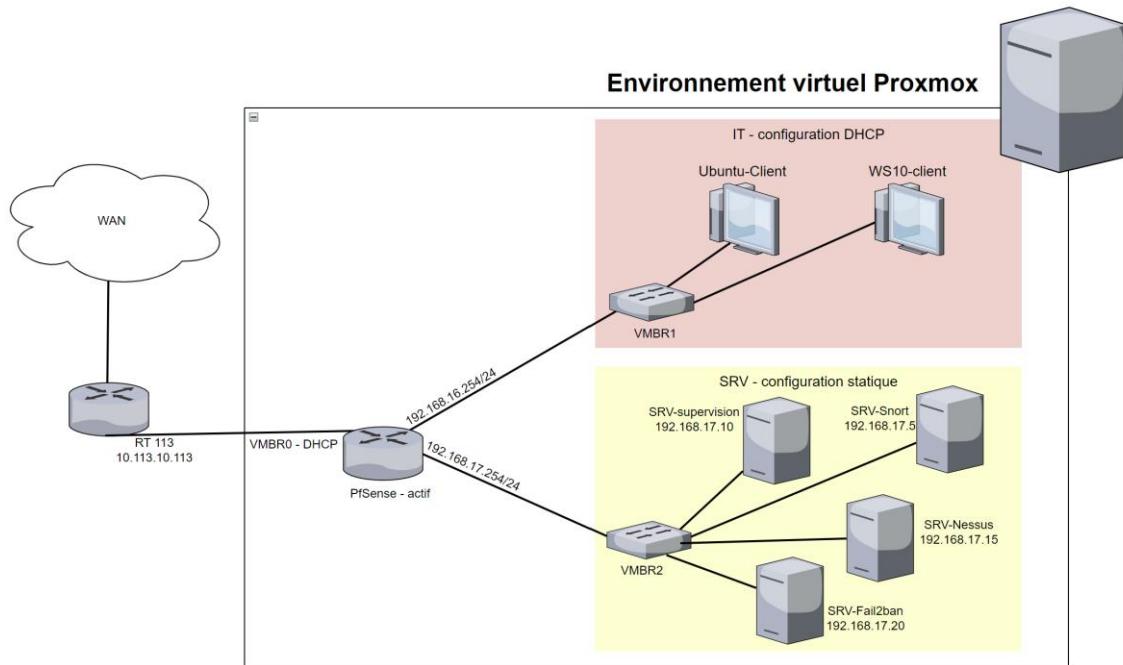
| Tâche | Durée |
|--------------------------------|--------|
| Installation du serveur Nessus | 1 jour |
| Configuration initiale | 1 jour |
| Test et validation | 1 jour |
| Formation des utilisateurs | 1 jour |

6.2. Plan d'adressage

| @réseau | @passerelle | NIC | Machine/rôle | DHCP ? |
|-----------------|----------------|-------|---|-------------|
| 10.113.6.0/16 | 10.113.6.11 | VMBR0 | WAN accès vers l'extérieur | Config DHCP |
| 192.168.16.0/24 | 192.168.16.254 | VMBR1 | Interface graphique : http://192.168.16.254/ | Config DHCP |
| 192.168.17.0/24 | 192.168.17.254 | VMBR2 | Interface graphique : http://192.168.17.254/ SRV-Snort: 197.168.17.5 SRV-supervision : 192.168.17.10 SRV-Nessus: 197.168.17.15 | Config DHCP |

| | | | | |
|--|--|--|------------------------------|--|
| | | | SRV-Fail2ban : 192.168.17.20 | |
|--|--|--|------------------------------|--|

6.3. Schéma réseau



6.4. Documentation technique

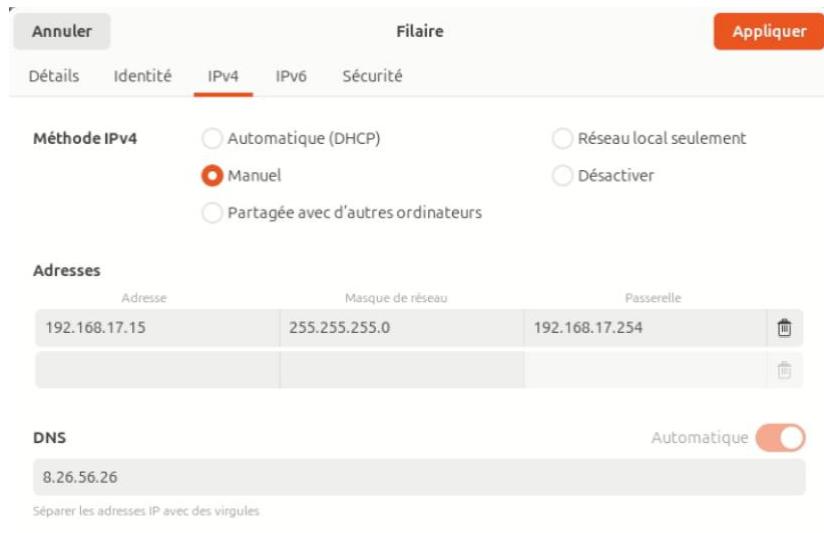
6.4.1. Prérequis

VM

| Nom | ID | OS | Mémoire | RAM | CPU | Réseau | Services/Remarques |
|------------|-------|---------------|---------|-----|--------------------------|--------|--------------------|
| SRV-Nessus | MV203 | Debian 12.7.0 | 50Go | 4Go | 2 processeurs 2 cœurs | VMBR2 | 192.168.17.15/24 |



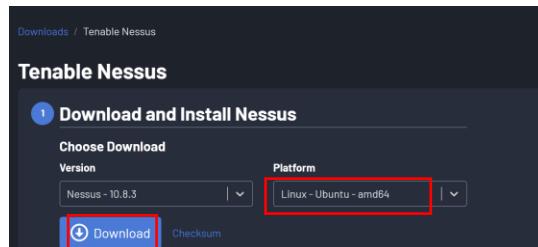
Configuration réseau de la machine SRV-Nessus



6.4.2. Choix de l'installation

Page officiel : <https://www.tenable.com/downloads/nessus>

Version : Nessus Essentials (gratuit pour usage personnel)



Télécharger le contenu.

6.4.3. Installation du package

user@srv-snort-nessus:~\$ cd ~/Téléchargements

user@srv-snort-nessus:~/Téléchargements\$ sudo dpkg -i Nessus-*.deb

Activation de Nessus

user@srv-snort-nessus:~/Téléchargements\$ sudo systemctl enable nessusd

Démarrer Nessus

user@srv-snort-nessus:~/Téléchargements\$ sudo systemctl start nessusd

user@srv-snort-nessus:~/Téléchargements\$ sudo systemctl status nessusd



6.4.4. Configuration initiale

Accéder à l'interface Web

Ouvrir un navigateur et aller sur :

<https://localhost:8834>

Accepter l'exception de sécurité (le certificat auto-signé).

Création du compte administrateur

Entrer un nom d'utilisateur et un mot de passe.

Selectionner la version : **Nessus Essentials** (clé d'activation gratuite).

Get an activation code
To register for a free Nessus Essentials activation code, enter your information.

First Name: user Last Name: PLOT-6
Email: plot.6.turgot@gmail.com

Already have activation code? Skip this step to enter it manually.

Back Skip Register

© 2025 Tenable®, Inc.

2

Welcome to Nessus
Choose how you want to deploy Nessus. Select an option to get started.

- Set up a purchased instance of Nessus
- Start a trial of Nessus Expert
- Start a trial of Nessus Professional
- Register for Nessus Essentials
- Link Nessus to another Tenable product

Continue

License Information
Activation Code: NZ26-QZU6-BZ3A-88DA-AKWT

Continue

© 2025 Tenable®, Inc.

1

3

Télécharger et installer les plugins (cela peut prendre plusieurs minutes).

Create a user account
Create a Nessus administrator user account. Use this username and password to log in to Nessus.

Username *: user
Password *: Labo-113

Back Submit

© 2025 Tenable®, Inc.

4

Initializing
Please wait while Nessus is initializing.

Downloading plugins...

Continue

© 2025 Tenable®, Inc.

5



6.4.5. Optimisation et sécurisation

Ajouter Nessus aux exceptions du pare-feu

```
user@srv-snort-nessus:~/Téléchargements$ sudo ufw allow 8834/tcp
```

```
user@srv-snort-nessus:~/Téléchargements$ sudo ufw enable
```

Mise à jour des plugins Nessus

```
user@srv-snort-nessus:~/Téléchargements$ sudo /opt/nessus/sbin/nessuscli update --all
```

```
user@srv-snort-nessus:~/Téléchargements$ sudo systemctl restart nessusd
```

```
user@srv-snort-nessus:~/Téléchargements$ sudo systemctl status nessusd
```

6.4.6. Configuration du scanner

Une fois connecté à votre session, entrer les adresses IP des machines cibles ou l'adresse réseau cible.

The screenshot shows two windows side-by-side. The left window is titled 'Welcome to Nessus Essentials' and contains instructions for launching a host discovery scan. It has a text input field labeled 'Targets' containing '192.168.17.0/24'. The right window is titled 'My Host Discovery Scan Results' and lists discovered hosts: 192.168.17.15, 192.168.17.5, 192.168.17.10, and 192.168.17.254. Both windows have 'Close' and 'Submit' buttons at the bottom.

Il va lancer un scan sur ce réseau-là.

Sélectionner les machines que vous voulez scanner et cliquer sur « **Run Scan** »



Download Tenable Nessus X Nessus Essentials / Fold X +

https://localhost:8834/#/scans/reports/11/hosts

Tenable Nessus Essentials Scans Settings

My Basic Network Scan

Back to My Scans

Hosts 4 Vulnerabilities 54 History 1

Filter Search Hosts 4 Hosts

| Host | Vulnerabilities | % |
|----------------|-----------------|------|
| 192.168.17.15 | 59 | 100% |
| 192.168.17.10 | 21 | 98% |
| 192.168.17.254 | 5 | 3% |
| 192.168.17.5 | 3 | 99% |

Scan Details

Policy: Basic Network Scan
Status: Running (green circle)
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 10:37 PM

Vulnerabilities

● Critical
● High
● Medium
● Low
● Info

Tenable News

What Is Exposure Management and Why Does It Matter...

Read More



6.5. Fiche procédure - utilisateur

Ouvrir l'interface web

1. Ouvrir un navigateur web.
2. Saisir l'URL suivante : <https://localhost:8834>
3. Accepter l'exception de sécurité si demandée.
4. Se connecter avec les identifiants créés lors de l'installation.

Lancer un Scan de Vulnérabilités

Créer un nouveau scan

1. Aller dans l'onglet **Scans**.
2. Cliquer sur **New Scan**.
3. Sélectionner **Basic Network Scan**.
4. Renseigner les informations :
 - o **Nom du scan** : Choisir un nom descriptif.
 - o **Cibles** : Entrer l'adresse IP ou le sous-réseau à scanner (ex: 192.168.17.0/24).
5. Cliquer sur **Save**, puis **Launch** pour démarrer le scan.

Surveiller l'état du scan

- Aller dans l'onglet **Scans**.
- Vérifier la progression du scan en cours.
- Attendre la fin du scan (peut prendre plusieurs minutes à plusieurs heures selon la taille du réseau).

Analyser les Résultats

Consulter les vulnérabilités

1. Une fois le scan terminé, cliquer sur le scan effectué.
2. Examiner les vulnérabilités détectées (classées par criticité) :
 - o ● **Critique**
 - o ● **Élevée**
 - o ● **Moyenne**
 - o ● **Faible**
3. Cliquer sur une vulnérabilité pour voir :
 - o La description du problème.
 - o Le score CVSS (indicateur de gravité).
 - o Les systèmes affectés.
 - o La solution recommandée.

Générer un rapport

1. Dans l'onglet **Scans**, ouvrir le scan terminé.
2. Cliquer sur **Export** et choisir un format :
 - o **PDF** (présentation claire).
 - o **CSV** (analyse sous Excel).
 - o **HTML** (rapport interactif).
3. Enregistrer et partager avec l'équipe de sécurité si nécessaire.



Appliquer les Correctifs

Prioriser les actions

| Gravité | Action Corrective |
|------------|---|
| ● Critique | Mise à jour immédiate, restriction d'accès, désactivation des services vulnérables. |
| ● Élevée | Vérification et correction rapide (mises à jour, configurations). |
| ● Moyenne | Application des correctifs recommandés. |
| ● Faible | Surveiller et corriger progressivement. |

Appliquer les solutions

- **Mettre à jour** les logiciels et systèmes vulnérables.
- **Modifier les configurations** (désactiver services inutiles, restreindre accès).
- **Appliquer les règles de pare-feu** pour sécuriser les ports ouverts.

Vérification et Suivi

Re-scanner après correction

1. Après avoir appliqué les correctifs, relancer un scan pour vérifier la suppression des vulnérabilités.
2. Comparer les résultats avec le scan précédent.
3. Répéter l'opération si des failles persistent.

Planifier des scans réguliers

1. Aller dans **Scans > New Scan**.
2. Dans l'onglet **Schedule**, définir :
 - **Fréquence** : Quotidienne / Hebdomadaire / Mensuelle.
 - **Heure d'exécution**.
3. Enregistrer pour automatiser la surveillance de la sécurité.

Sécurisation de Nessus

Mise à jour des plugins Nessus

```
sudo /opt/nessus/sbin/nessuscli update --all
```

```
sudo systemctl restart nessusd
```

Restreindre l'accès à Nessus

```
sudo ufw allow 8834/tcp
```

```
sudo ufw enable
```



6.6. Cahier de recettes

- Vérification de l'installation.
- Validation des accès réseau.
- Test des fonctionnalités principales.

6.7. Cahier de test

| Test | OK | Remarque |
|----------------------------|----|----------|
| Accès à l'interface Nessus | Ok | |
| Scan d'un sous-réseau | Ok | |
| Génération d'un rapport | Ok | |



7. Snort

7.1. Cahier des charges

7.1.1. Contexte et Objectifs

Contexte

Snort est un système de détection d'intrusion (IDS) open source permettant d'analyser le trafic réseau en temps réel afin d'identifier des activités suspectes ou malveillantes. Il est couramment utilisé pour renforcer la sécurité des réseaux d'entreprise et prévenir les cyberattaques.

Objectif

L'objectif de ce projet est d'installer, configurer et tester Snort sur un réseau afin de surveiller le trafic, détecter les intrusions et fournir une documentation complète pour son utilisation et sa maintenance.

7.1.2. Descriptions fonctionnelles des besoins

- Déploiement de Snort sur un serveur dédié ou une machine virtuelle.
- Configuration des règles de détection et mise à jour automatique des signatures.
- Intégration avec des outils de gestion des journaux et d'analyse.
- Génération d'alertes en cas d'activité suspecte.
- Mise en place d'un tableau de bord pour la visualisation des événements.
- Documentation détaillée pour l'administration et l'utilisation de Snort.

7.1.3. Cahier des charges technique

Système d'exploitation : Ubuntu 24.04

Base de données : MySQL/PostgreSQL (optionnel, pour stockage des logs)

Interface de gestion : Snorby

Protocole supporté : IPv4, IPv6

Logs et monitoring : Intégration avec SIEM (ex : Splunk, ELK Stack)

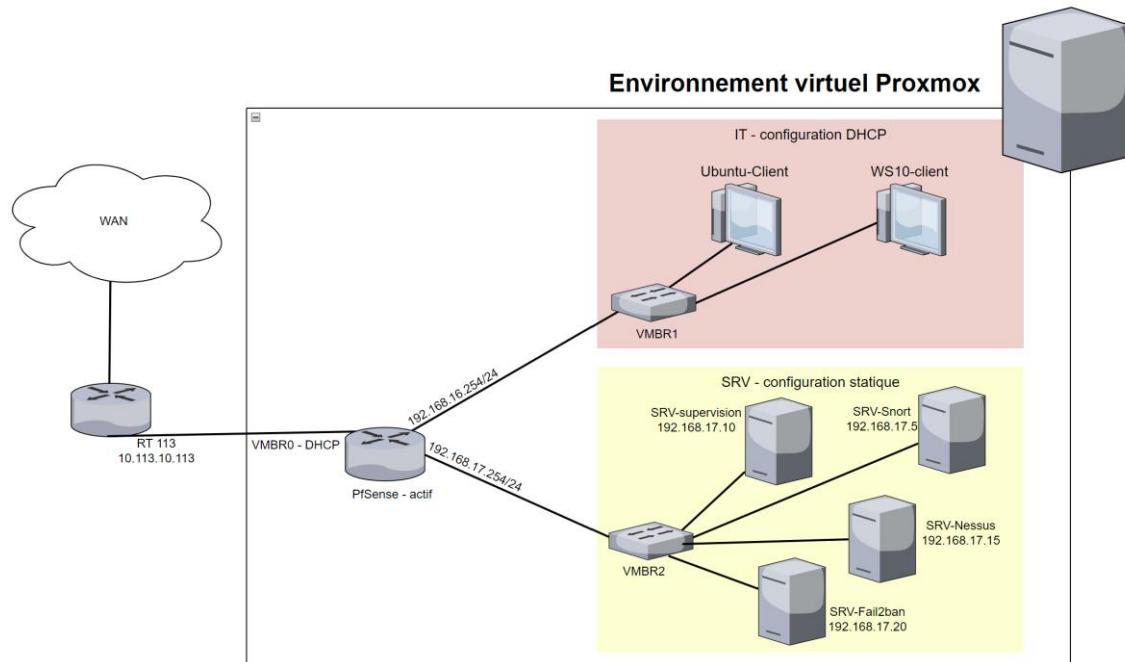
7.1.4. Planning prévisionnel

| Tâche | Durée |
|----------------------------|---------|
| Installation de Snort | 2 jours |
| Configuration des règles | 2 jours |
| Tests et validation | 1 jour |
| Documentation et formation | 2 jours |

7.2. Plan d'adressage

| @réseau | @passerelle | NIC | Machine/rôle | DHCP ? |
|-----------------|--------------------|-------|---|-------------|
| 10.113.6.0/16 | 10.113.6.11 | VMBR0 | WAN accès vers l'extérieur | Config DHCP |
| 192.168.16.0/24 | 192.168.16.254 | VMBR1 | Interface graphique : http://192.168.16.254/ | Config DHCP |
| 192.168.17.0/24 | 192.168.17.254 | VMBR2 | Interface graphique : http://192.168.17.254/ SRV-Snort: 197.168.17.5 SRV-supervision : 192.168.17.10 SRV-Nessus: 197.168.17.15 SRV-Fail2ban : 192.168.17.20 | Config DHCP |

7.3. Schéma réseau



7.4. Documentation technique

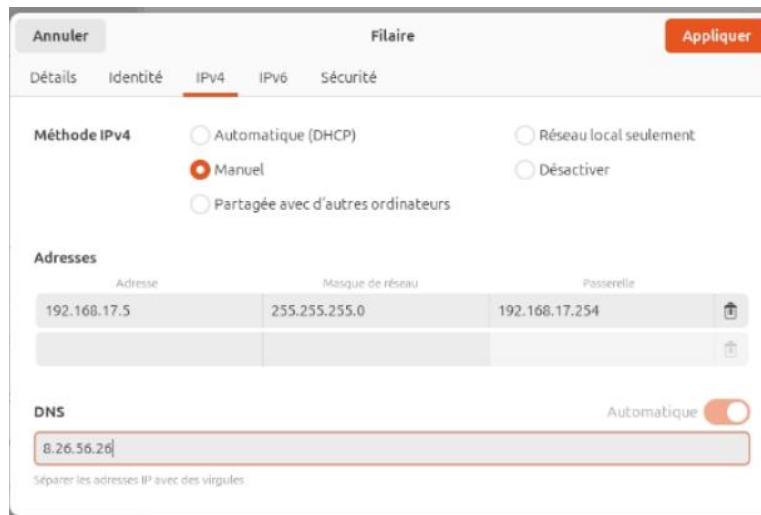
7.4.1. Prérequis

VM

| Nom | ID | OS | Mémoire | RAM | CPU | Réseau | Services/Remarques |
|-----------|-------|--------------|---------|-----|------------------------|--------|--------------------|
| SRV-Snort | MV201 | Ubuntu 24.04 | 20Go | 2Go | 1 processeur 1 cœur | VMBR2 | 192.168.17.5/24 |



Configuration réseau de la machine SRV-Snort



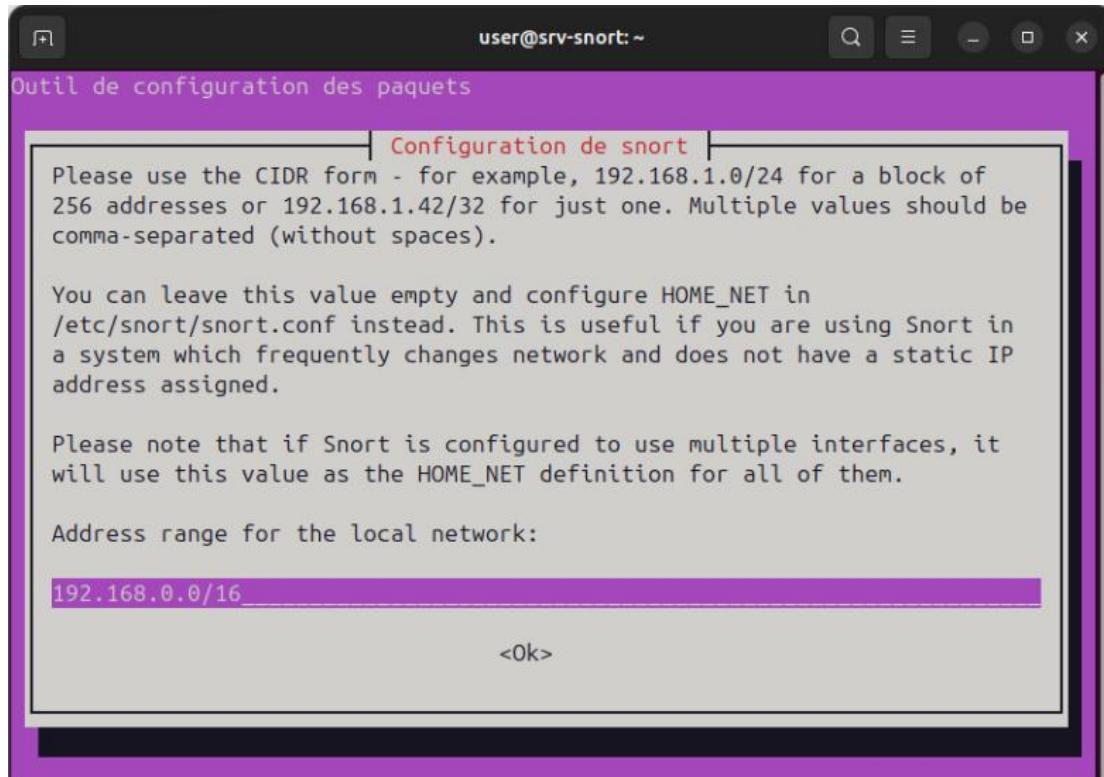
MAJ du système

```
user@srv-snort:~$ sudo apt update && sudo apt upgrade -y
```

7.4.2. Installation

Installer les dépendances requises

```
user@srv-snort:~$ sudo apt install -y snort
```





Configuration de Snort

```
user@srv-snort:~$ sudo nano /etc/snort/snort.conf
```

Définir l'adresse du réseau à surveiller :

Trouvez la ligne contenant `ipvar HOME_NET any` et modifiez-la en fonction de votre réseau local, ici :

```
ipvar HOME_NET 192.168.17.0/24
```

```
#  
ipvar HOME_NET 192.168.17.0/24
```

Lancer Snort en mode écoute

Pour obtenir le nom de l'interface :

```
user@srv-snort:~$ ip a
```

```
user@srv-snort:~$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    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_codel state UP group default qlen 1000  
    link/ether bc:24:11:8f:c7:3b brd ff:ff:ff:ff:ff:ff  
    altname enp0s18  
    inet 192.168.17.5/24 brd 192.168.17.255 scope global noprefixroute ens18  
        valid_lft forever preferred_lft forever  
user@srv-snort:~$
```

```
user@srv-snort:~$ sudo snort -i vtnet2 -A console -c /etc/snort/snort.conf
```

```
4057 Snort rules read  
  3383 detection rules  
    0 decoder rules  
    0 preprocessor rules  
3383 Option Chains linked into 949 Chain Headers  
+++++  
-----[Rule Port Counts]-----  
|      tcp      udp      icmp      ip  
|  src    151      18       0       0  
|  dst    3306     126       0       0  
|  any    383      48      52      22  
|  nc     27       8       15      20  
|  s+d    12       5       0       0  
+-----  
-----[detection-filter-config]-----  
| memory-cap : 1048576 bytes  
+-----[detection-filter-rules]-----  
| none  
-----  
-----[rate-filter-config]-----  
| memory-cap : 1048576 bytes  
+-----[rate-filter-rules]-----  
| none  
-----  
-----[event-filter-config]-----  
| memory-cap : 1048576 bytes  
+-----[event-filter-global]-----  
| none  
  event_filter_global
```



Cela affichera les alertes directement dans le terminal.

Tester Snort

```
user@srv-snort:~$ sudo apt install nmap
user@srv-snort:~$ sudo nmap -V -sS 192.168.17.5
```

7.4.3. Détection des attaques

```
user@srv-snort:~$ sudo snort -i vtnet2 -A console -c /etc/snort/snort.conf
user@srv-snort:~$ sudo nmap -v -sS 192.168.17.5
```

Ici l'IP du serveur Snort.

7.4.4. Configurer une règle de test

Les règles de Snort se trouvent dans /etc/snort/rules/. Ajoutez une règle de test :

```
user@srv-snort:~$ echo 'alert icmp any any -> any any (msg:"Ping détecté"; sid:1000001; rev:1;)' | sudo tee -a /etc/snort/rules/local.rules
```

Puis, assurez-vous que le fichier de configuration inclut local.rules :

```
user@srv-snort:~$ sudo nano /etc/snort/snort.conf
```

Vérifiez que cette ligne n'est pas commentée (# à enlever si présent) :

```
include $RULE_PATH/local.rules
```

```
# site specific rules
include $RULE_PATH/local.rules
```

7.4.5. Tester la configuration de Snort

```
user@srv-snort:~$ sudo snort -T -c /etc/snort/snort.conf
```

```
.-> Snort! <-
o'`--> Version 2.9.20 GRE (Build 82)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.10.4 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.3

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.2 <Build 1>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_DCRPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_SNTP Version 1.1 <Build 9>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_S7COMMPLUS Version 1.0 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_SDP Version 1.1 <Build 1>
Preprocessor Object: apid Version 1.1 <Build 5>

Total snort Fixed Memory Cost - MaxRss:104612
Snort successfully validated the configuration!
Snort exiting
user@srv-snort:~$
```



Lancer Snort en mode écoute

```
user@srv-snort:~$ ip a
```

```
user@srv-snort:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    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_codel state UP group default qlen 1000
    link/ether bc:24:11:8f:c7:3b brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet 192.168.17.5/24 brd 192.168.17.255 scope global noprefixroute ens18
        valid_lft forever preferred_lft forever
user@srv-snort:~$
```

```
user@srv-snort:~$ sudo snort -i ens18 -A console -c /etc/snort/snort.conf
```

Redémarrage du service

Redémarrez Snort pour appliquer la modification :

```
user@srv-snort:~$ sudo systemctl restart snort
```

```
user@srv-snort:~$ sudo systemctl status snort
```

```
user@srv-snort:~$ sudo systemctl status snort
● snort.service - LSB: Lightweight network intrusion detection system
  Loaded: loaded (/etc/init.d/snort; generated)
  Active: active (running) since Tue 2025-03-25 23:42:58 CET; 46s ago
    Docs: man:systemd-sysv-generator(8)
  Process: 3309 ExecStart=/etc/init.d/snort start (code=exited, status=0/SUCCESS)
    Tasks: 2 (limit: 2272)
   Memory: 80.1M (peak: 96.1M)
     CPU: 239ms
    CGroup: /system.slice/snort.service
            └─3330 /usr/sbin/snort -m 027 -D -d -l /var/log/snort -u snort -g snort --p
```

7.4.6. Tester Snort avec un ping

Testez avec un **ping** depuis une autre machine :

```
user@srv-snort:~$ ping -c 4 192.168.17.5
```

Si tout fonctionne, Snort devrait générer une alerte.

7.4.7. Démarrer Snort en tant que service

```
user@srv-snort:~$ sudo systemctl enable snort
```

```
user@srv-snort:~$ sudo systemctl start snort
```

```
user@srv-snort:~$ sudo systemctl status snort
```



7.5. Cahier de recettes

- Analyse du trafic réseau en temps réel.
- Détection des attaques basées sur des signatures (règles personnalisables)
- Enregistrement des alertes dans `/var/log/snort/`.
- Inspection des paquets pour détecter les comportements anormaux.
- Détection des scans de ports et des tentatives d'exploitation.

7.6. Cahier de test

| Test | OK | Remarque |
|--|----|----------|
| Vérification de la version de Snort | Ok | |
| Vérification des fichiers de configuration | Ok | |
| Validation de la configuration Snort | Ok | |
| Vérification du chargement des règles | Ok | |
| Test de détection de ping | Ok | |



8. Fail2ban

8.1. Cahier des charges

8.1.1. Contexte et Objectifs

Contexte

L'augmentation des attaques par force brute et des tentatives d'intrusion sur les serveurs expose les infrastructures informatiques à des risques de sécurité. Afin de renforcer la sécurité d'un serveur sous Ubuntu, il est nécessaire d'implémenter une solution de protection contre ces attaques, notamment sur les services critiques comme SSH, Apache, et Postfix.

Objectif

L'objectif est d'installer et de configurer **Fail2Ban** sur une machine virtuelle Ubuntu afin de :

- Prévenir les tentatives d'intrusion répétées.
- Bloquer temporairement ou définitivement les adresses IP malveillantes.
- Améliorer la sécurité des services exposés.
- Générer des logs et statistiques pour le suivi des attaques.

8.1.2. Descriptions fonctionnelles des besoins

- Surveillance des logs des services critiques.
- Détection automatique des tentatives de connexion répétées.
- Application de règles de bannissement selon la configuration définie.
- Possibilité de personnalisation des règles de détection et de bannissement.
- Notification des bannissements via e-mail (optionnel).

8.1.3. Cahier des charges technique

- SSH (`/var/log/auth.log`)
- Apache/Nginx (`/var/log/apache2/access.log` ou `/var/log/nginx/access.log`)

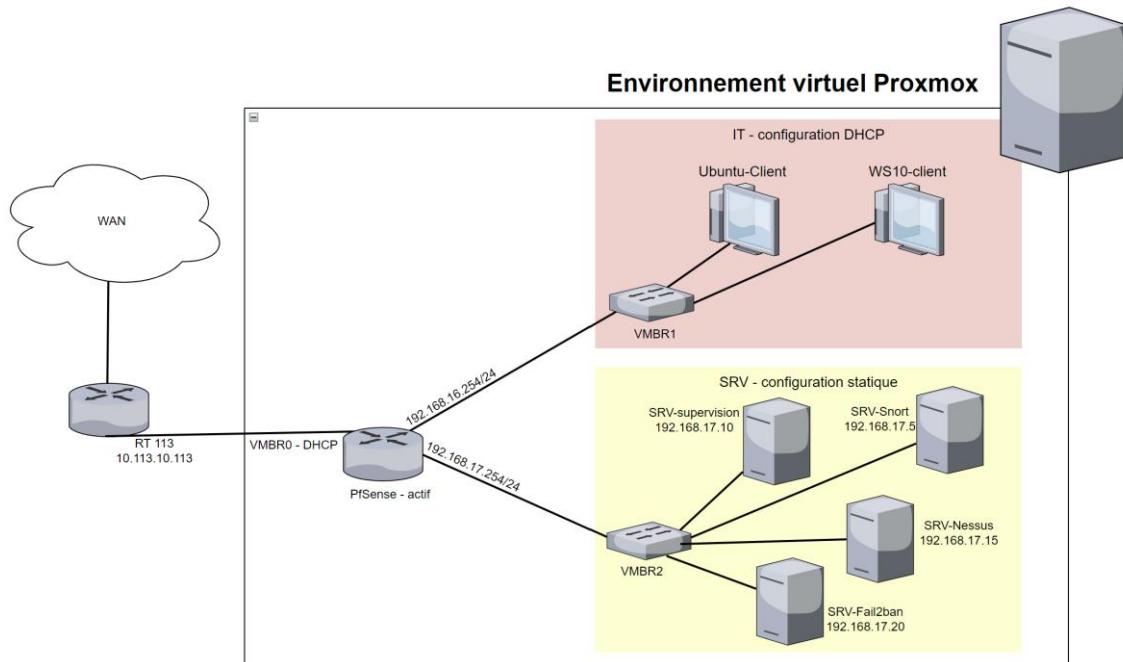
8.1.4. Planning prévisionnel

| Tâche | Durée |
|-------------------------------------|---------|
| Préparation de la VM | 1 jour |
| Installation de Fail2ban | 1 jour |
| Configuration et personnalisation | 2 jours |
| Test et validation | 2 jours |
| Documentation et mise en production | 2 jours |

8.2. Plan d'adressage

| @réseau | @passerelle | NIC | Machine/rôle | DHCP ? |
|-----------------|--------------------|-------|---|-------------|
| 10.113.6.0/16 | 10.113.6.11 | VMBR0 | WAN accès vers l'extérieur | Config DHCP |
| 192.168.16.0/24 | 192.168.16.254 | VMBR1 | Interface graphique : http://192.168.16.254/ | Config DHCP |
| 192.168.17.0/24 | 192.168.17.254 | VMBR2 | Interface graphique : http://192.168.17.254/ SRV-Snort: 197.168.17.5 SRV-supervision : 192.168.17.10 SRV-Nessus: 197.168.17.15 SRV-Fail2ban : 192.168.17.20 | Config DHCP |

8.3. Schéma réseau



8.4. Documentation technique

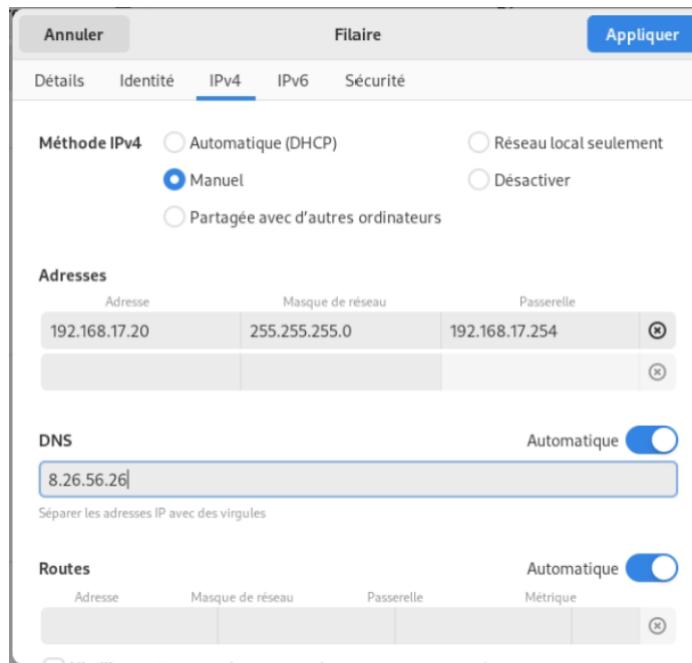
8.4.1. Prérequis

VM

| Nom | ID | OS | Mémoire | RAM | CPU | Réseau | Services/Remarques |
|--------------|-------|---------------|---------|-----|--------------------------|--------|--------------------|
| SRV-Fail2ban | MV204 | Debian 12.7.0 | 15Go | 2Go | 2 processeurs 2 cœurs | VMBR2 | 192.168.17.20/24 |



Configuration réseau de la machine SRV-Fail2ban



MAJ du système

```
root@srv-fail2ban:/home/harani# apt update && apt upgrade -y
```

8.4.2. Installation de Fail2Ban

```
root@srv-fail2ban:/home/harani# apt install fail2ban -y
root@srv-fail2ban:/home/harani# fail2ban-client -V
```

5.4.3. Configuration de Fail2Ban

Création du fichier de configuration local

Copiez le fichier par défaut pour éviter qu'il ne soit écrasé lors des mises à jour :

```
root@srv-fail2ban:/home/harani# cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
```

Configuration des paramètres généraux

Éditez le fichier de configuration :

```
root@srv-fail2ban:/home/harani# nano /etc/fail2ban/jail.local
```

Ajouter/modifier les paramètres suivants :

[DEFAULT]

```
bantime = 10m # Durée du bannissement
findtime = 10m # Fenêtre de temps pour détecter les échecs
maxretry = 5 # Nombre d'échecs avant bannissement
backend = systemd # Gestionnaire des logs
```



Configuration de la protection SSH

Ajouter/modifier les paramètres suivants /etc/fail2ban/jail.local :

[sshd]

```
enabled = true
port = ssh
filter = sshd
logpath = /var/log/auth.log
maxretry = 3
bantime = 1h
```

Configuration de la protection Apache/Nginx

Ajoutez ou modifiez les sections suivantes selon le serveur web utilisé :

Apache :

[apache-auth]

```
enabled = true
port = http,https
logpath = /var/log/apache2/error.log
maxretry = 5
```

Nginx :

[nginx-http-auth]

```
enabled = true
port = http,https
logpath = /var/log/nginx/error.log
maxretry = 5
```

5.4.5. Activation et vérification

Redémarrer Fail2ban

```
root@srv-fail2ban:/home/harani# systemctl restart fail2ban
```

```
root@srv-fail2ban:/home/harani# systemctl enable fail2ban
```

Vérifier le statut

```
root@srv-fail2ban:/home/harani# systemctl status fail2ban
```

```
root@SRV-Fail2ban:/home/harani# systemctl status fail2ban
● fail2ban.service - Fail2Ban Service
  Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; preset: enabled)
  Active: active (running) since Wed 2025-03-26 21:58:44 CET; 22s ago
    Docs: man:fail2ban(1)
    Main PID: 3275 (fail2ban-server)
       Tasks: 9 (limit: 2282)
      Memory: 15.8M
         CPU: 121ms
      CGroup: /system.slice/fail2ban.service
              └─3275 /usr/bin/python3 /usr/bin/fail2ban-server -xf start
```



Vérifier les services surveillés

```
root@srv-fail2ban:/home/harani# fail2ban-client status
root@srv-fail2ban:/home/harani# fail2ban-client status sshd
```

5.4.6. Installer OpenSSH

```
root@srv-fail2ban:/home/harani# apt install openssh-server -y
root@srv-fail2ban:/home/harani# systemctl enable ssh
root@srv-fail2ban:/home/harani# systemctl start ssh
root@srv-fail2ban:/home/harani# systemctl status ssh
```

Vérifier le port d'écoute SSH

```
root@srv-fail2ban:/home/harani# netstat -tulnp | grep ssh
root@SRV-Fail2ban:~# netstat -tulnp | grep ssh
tcp      0      0 0.0.0.0:22          0.0.0.0:*
                                              LISTEN      3710/sshd: /usr/sbi
```

```
root@srv-fail2ban:/home/harani# systemctl restart ssh
```

Vérification du pare-feu

```
root@srv-fail2ban:/home/harani# apt install ufw
root@srv-fail2ban:/home/harani# sudo ufw status
root@srv-fail2ban:/home/harani# sudo ufw allow ssh
root@srv-fail2ban:/home/harani# sudo ufw enable
root@SRV-Fail2ban:~# sudo ufw status
Status: inactive
root@SRV-Fail2ban:~# sudo ufw allow ssh
Rules updated
Rules updated (v6)
root@SRV-Fail2ban:~# sudo ufw enable
Firewall is active and enabled on system startup
root@SRV-Fail2ban:~#
```

5.4.6. Simuler un bannissement

⌚ Objectif :

Nous allons provoquer un bannissement en générant plusieurs tentatives de connexion SSH échouées.

Vérifier la configuration actuelle de Fail2ban

Assurer que Fail2Ban surveille bien SSH :

```
root@srv-fail2ban:/home/harani# fail2ban-client status sshd
```

Tu devrais voir une section **"Banned IP list"**, qui est vide pour l'instant.



Trouver l'adresse IP de la machine

Avant de tester, trouver l'IP de la machine qui va être bannie (celle d'où tu vas tester). Sur ta machine locale (celle avec laquelle tu vas tester la connexion SSH).

On va utiliser la machine SRV-Prometheus : 192.168.17.10

Provoquer le bannissement

Tu dois maintenant générer plusieurs erreurs de connexion SSH.

Depuis **une autre machine** (ou un autre terminal si tu es en local), essaie de te connecter à ton serveur avec un faux mot de passe :

ssh utilisateur@<IP_server_fail2ban>

SRV-Prometheus

```
harani@srv-prometheus:~$ ssh harani@192.168.17.20
```

Quand on te demande le mot de passe, entre un mot de passe incorrect volontairement.

```
harani@srv-supervision:~$ ssh harani@192.168.17.20
The authenticity of host '192.168.17.20 (192.168.17.20)' can't be established.
ED25519 key fingerprint is SHA256:69HZ3/HfZ6XoPAD1TpuK9QGbMagGwWbdFqb4FTHlKR8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.17.20' (ED25519) to the list of known hosts.
harani@192.168.17.20's password:
Connection closed by 192.168.17.20 port 22
harani@srv-supervision:~$
```

Répète cette action 3 à 5 fois de suite (selon la valeur de maxretry définie dans /etc/fail2ban/jail.local).

On va tester ici 6 fois.

```
harani@srv-supervision:~$ ssh harani@192.168.17.20
harani@192.168.17.20's password:
Permission denied, please try again.
harani@192.168.17.20's password:
Permission denied, please try again.
harani@192.168.17.20's password:
harani@192.168.17.20: Permission denied (publickey,password).
harani@srv-supervision:~$
```

Vérifier si l'IP de la machine de test est bannie

Après plusieurs tentatives échouées, aller sur le serveur **192.168.17.20** et vérifie si l'IP **192.168.17.10** a été bannie par Fail2Ban.



Pour cela, utilise la commande suivante sur **SRV-Fail2ban** :

```
root@srv-fail2ban:/home/harani# fail2ban-client status sshd
```

```
root@SRV-Fail2ban:~# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed: 3
| |- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
`- Actions
  |- Currently banned: 1
  |- Total banned: 1
  |- Banned IP list: 192.168.17.10
root@SRV-Fail2ban:~#
```

Si l'**IP 192.168.17.10** apparaît dans la liste des IP bannies, cela signifie que **Fail2Ban a bien bloqué l'IP** après les échecs de connexion.

5.4.7. Débannir une IP manuellement

```
root@srv-fail2ban:/home/harani# fail2ban-client unban 192.168.17.10
```

```
root@SRV-Fail2ban:~# fail2ban-client unban 192.168.17.10
1
root@SRV-Fail2ban:~# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed: 3
| |- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
`- Actions
  |- Currently banned: 0
  |- Total banned: 1
  |- Banned IP list:
root@SRV-Fail2ban:~#
```

5.4.8. Vérification des logs

Vérifier les logs avec journalctl

```
root@srv-fail2ban:/home/harani# journalctl -u fail2ban --no-pager
```

```
root@srv-fail2ban:/home/harani# journalctl -u fail2ban | grep sshd
```



```
root@SRV-Fail2ban:~# journalctl -u fail2ban -no-pager
mars 26 21:36:21 SRV-Fail2ban systemd[1]: Started fail2ban.service - Fail2Ban Service.
mars 26 21:36:21 SRV-Fail2ban fail2ban-server[3215]: 2025-03-26 21:36:21,241 fail2ban.configreader [3215]: WARNING 'allowipv
5' not defined in 'Definition'. Using default one: 'auto'
mars 26 21:36:21 SRV-Fail2ban fail2ban-server[3215]: 2025-03-26 21:36:21,248 fail2ban [3215]: ERROR Failed du
ring configuration: Have not found any log file for sshd jail
mars 26 21:36:21 SRV-Fail2ban fail2ban-server[3215]: 2025-03-26 21:36:21,252 fail2ban [3215]: ERROR Async con
figuration of server failed
mars 26 21:36:21 SRV-Fail2ban systemd[1]: fail2ban.service: Main process exited, code=exited, status=255/EXCEPTION
mars 26 21:36:21 SRV-Fail2ban systemd[1]: fail2ban.service: Failed with result 'exit-code'.
mars 26 21:58:44 SRV-Fail2ban systemd[1]: Started fail2ban.service - Fail2Ban Service.
mars 26 21:58:44 SRV-Fail2ban fail2ban-server[3275]: 2025-03-26 21:58:44,829 fail2ban.configreader [3275]: WARNING 'allowipv
5' not defined in 'Definition'. Using default one: 'auto'
mars 26 21:58:44 SRV-Fail2ban fail2ban-server[3275]: Server ready
root@SRV-Fail2ban:~# journalctl -u fail2ban | grep sshd
mars 26 21:36:21 SRV-Fail2ban fail2ban-server[3215]: 2025-03-26 21:36:21,248 fail2ban [3215]: ERROR Failed du
ring configuration: Have not found any log file for sshd jail
```

Vérifier les logs de Fail2ban dans le fichier /var/log/fail2ban.log

```
root@srv-fail2ban:/home/harani# tail -f /var/log/fail2ban.log
```

```
root@SRV-Fail2ban:~# tail -f /var/log/fail2ban.log
2025-03-26 21:58:44,882 fail2ban.filtersystemd [3275]: NOTICE [apache-auth] Jail started without 'journalmatch' set. Jail re
gexes will be checked against all journal entries, which is not advised for performance reasons.
2025-03-26 21:58:44,883 fail2ban.jail [3275]: INFO Jail 'apache-auth' started
2025-03-26 21:58:44,883 fail2ban.filtersystemd [3275]: INFO [nginx-http-auth] Jail is in operation now (process new journa
l entries)
2025-03-26 21:58:44,883 fail2ban.filtersystemd [3275]: INFO [apache-auth] Jail is in operation now (process new journal en
tries)
2025-03-26 21:58:44,884 fail2ban.jail [3275]: INFO Jail 'nginx-http-auth' started
2025-03-26 23:24:14,091 fail2ban.filter [3275]: INFO [sshd] Found 192.168.17.10 - 2025-03-26 23:24:13
2025-03-26 23:24:26,088 fail2ban.filter [3275]: INFO [sshd] Found 192.168.17.10 - 2025-03-26 23:24:25
2025-03-26 23:24:32,088 fail2ban.filter [3275]: INFO [sshd] Found 192.168.17.10 - 2025-03-26 23:24:31
2025-03-26 23:24:32,861 fail2ban.actions [3275]: NOTICE [sshd] Ban 192.168.17.10
2025-03-26 23:30:04,455 fail2ban.actions [3275]: NOTICE [sshd] Unban 192.168.17.10
```



8.5. Fiche procédure - utilisateur

Vérification de la connexion réseau

Avant de se connecter, assurez-vous que le serveur et la machine cliente sont sur le même réseau et peuvent se joindre :

- Vérifiez l'adresse IP du serveur 192.168.17.20.
- Testez la connexion avec la commande ping : **ping 192.168.17.20**

Si la réponse est positive, le serveur est accessible.

Connexion au serveur via SSH

Depuis la machine cliente (par exemple, 192.168.17.10), ouvrez un terminal et exécutez la commande suivante pour vous connecter au serveur : **ssh admin@192.168.17.20**

Remplacez utilisateur par le nom d'utilisateur valide sur le serveur.

Saisie du mot de passe

Une fois la commande exécutée, vous serez invité à entrer le mot de passe de l'utilisateur spécifié sur le serveur → **Labo-113**

- **Si le mot de passe est correct**, vous serez connecté au serveur.
- **Si le mot de passe est incorrect**, vous recevrez un message d'erreur. Si plusieurs tentatives échouées se produisent, Fail2Ban peut bannir votre IP temporairement.



8.6. Cahier de recettes

1. Test : Provoquer un bannissement SSH

- Ouvrir un terminal sur la machine cliente.
- Tenter de se connecter au serveur (192.168.17.20) via SSH avec un mot de passe incorrect.
- Répète l'opération 3 à 5 fois.
- Vérifie que l'IP de la machine cliente est bannie.

2. Test : Vérification du bannissement dans Fail2Ban

- Sur le serveur (192.168.17.20), utilise la commande suivante :
sudo fail2ban-client status sshd
- Vérifie que l'IP de la machine cliente apparaît dans la liste des IP bannies.

3. Test : Vérification de la réception de l'e-mail de notification

- Vérifie l'adresse e-mail configurée pour recevoir les notifications.
- Assure-toi qu'un e-mail a été envoyé lorsqu'une IP a été bannie (si la notification par e-mail est configurée).

4. Test : Vérification des logs de Fail2Ban

- Utilise la commande suivante pour voir les logs de Fail2Ban :
sudo tail -f /var/log/fail2ban.log
- Vérifie qu'un log d'interdiction apparaît lorsque l'IP est bannie après plusieurs tentatives échouées.

5. Test : Débannir une IP

- Exécute la commande suivante pour débannir une IP :
sudo fail2ban-client unban <IP_bannie>
- Vérifie que l'IP n'est plus présente dans la liste des IP bannies.

6. Test : Vérification après redémarrage

- Redémarre Fail2Ban avec la commande suivante :
sudo systemctl restart fail2ban
- Vérifie que les protections SSH sont toujours actives.

8.7. Cahier de test

| Test | OK | Remarque |
|--|----|----------|
| Détection d'une tentative de brute-force sur SSH | Ok | |
| Bannissement d'une IP après X échecs | Ok | |
| Débannissement manuel d'une IP | Ok | |
| Vérification des logs | Ok | |



Aminata THIAM

9. BackupManager

9.1. Cahier des charges

9.1.1. Contexte et Objectifs

Contexte

Le projet a pour objectif de mettre en place une solution de **sauvegarde et restauration de fichiers**. La solution doit permettre à un utilisateur de sauvegarder des fichiers ou des répertoires, puis de les restaurer en cas de besoin. Cette solution doit être automatisée et sécurisée, avec une interface en ligne de commande pour le gestionnaire du système.

Objectif

- Mettre en place un système de sauvegarde fiable.
- Permettre la restauration des fichiers en cas de besoin.
- Automatiser les sauvegardes pour éviter les pertes de données.

9.1.2. Descriptions fonctionnelles des besoins

L'utilisateur souhaite disposer d'un système de sauvegarde automatique et manuel pour sécuriser des fichiers spécifiques présents sur une machine Ubuntu.

Fonctionnalités attendues :

Sauvegarde

- Pouvoir sauvegarder un dossier déterminé.
- Stocker les archives dans un répertoire de destination spécifique.

Restauration

- Permettre la restauration de l'archive dans un dossier choisi par l'utilisateur.
- La restauration doit être simple via une commande terminale.

9.1.3. Cahier des charges technique

| Outil / Technologie | Usage |
|---------------------|---|
| Backup Manager | Outil principal pour la sauvegarde/restauration |
| tar (Unix) | Format de compression (.tar.gz) utilisé |
| nano | Éditeurs de texte pour la configuration |
| bash | Exécution des commandes système Linux |



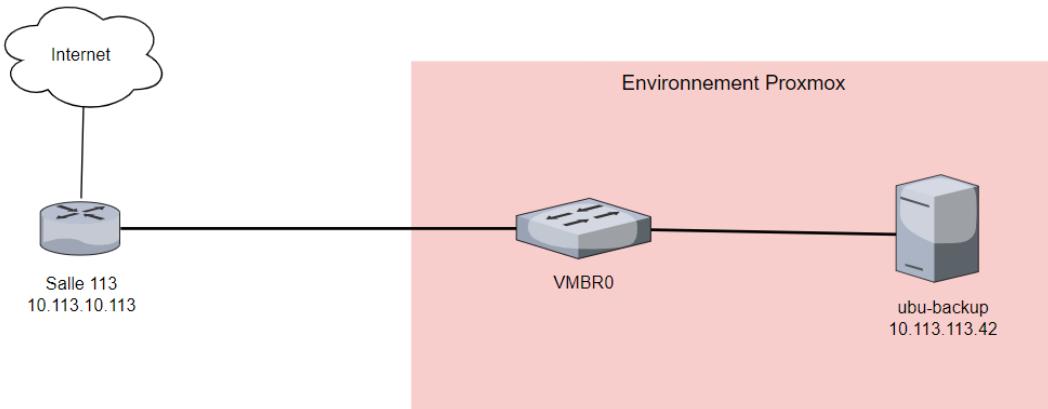
9.1.4. Planning prévisionnel

| Tâche | Durée |
|---|--------|
| Installation de Backup manager et des dépendances | 1 jour |
| Configuration de Backup manager | 1 jour |
| Test de sauvegarde et de restauration manuels | 1 jour |

9.2. Plan d'adressage

| @réseau | @passerelle | NIC | Machine/rôle | DHCP ? |
|---------------|---------------|-------|------------------------------------|-------------|
| 10.113.6.0/16 | 10.113.10.113 | VMBR0 | Backup -Manager : 10.113.113.42 | Config DHCP |

9.3. Schéma réseau



9.4. Documentation technique

9.4.1. Installation du système d'exploitation Ubuntu

Créer la VM, avec les configurations ci-dessous.

| Nom | ID | OS | Mémoire | RAM | CPU | Réseau | Services/Remarques |
|------------|-------|--------------|---------|-----|--------------------------|-------------------|--------------------|
| ubu-backup | MV105 | Ubuntu 24.04 | 32Go | 2Go | 1 processeur 2 coeurs | bc:24:11:bb:fa:71 | 10.113.113.42 |

9.4.2. Installation de backup-manager

Mise à jour du système

Avant d'installer tout logiciel, il est recommandé de mettre à jour les paquets du système :

```
sudo apt update
```

Installation du paquet Backup Manager



Si Backup Manager est disponible dans le **repository officiel d'Ubuntu**, tu peux l'installer en utilisant la commande apt :

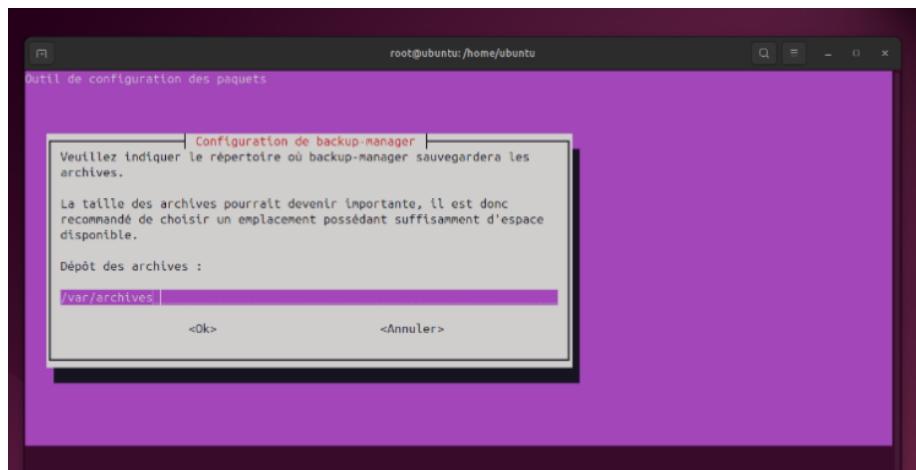
```
sudo apt install backup-manager
```

9.4.3. Configuration du répertoire de sauvegarde

Après l'installation de **Backup Manager**, il est nécessaire de configurer le répertoire où les sauvegardes seront stockées.

Ouverture du fichier de configuration avec un éditeur de texte comme nano :

```
sudo nano /etc/backup-manager.conf
```



Modifier la ligne concernant le répertoire de destination de la sauvegarde. Par exemple, pour stocker les sauvegardes dans /home/sio/Sauvegardes :

```
# Where to store the archives
export BM_REPOSITORY_ROOT="/home/sio/Sauvegardes"
```

Définir les répertoires qui seront archivés

```
# Paths without spaces in their name:
export BM_TARBALL_DIRECTORIES="/etc /home /var/www /var/log /etc/apache2 /etc/letsencrypt/ /var/lib /home/sio/packages"
```

Sauvegarder et quitter l'éditeur (Ctrl+X, puis appuie sur Y pour sauvegarder et Enter pour quitter).



9.4.4. Test de la Configuration

Lancer une première sauvegarde manuelle

Après avoir configuré Backup Manager, lance une sauvegarde manuelle pour tester la configuration :

```
sudo backup-manager
```

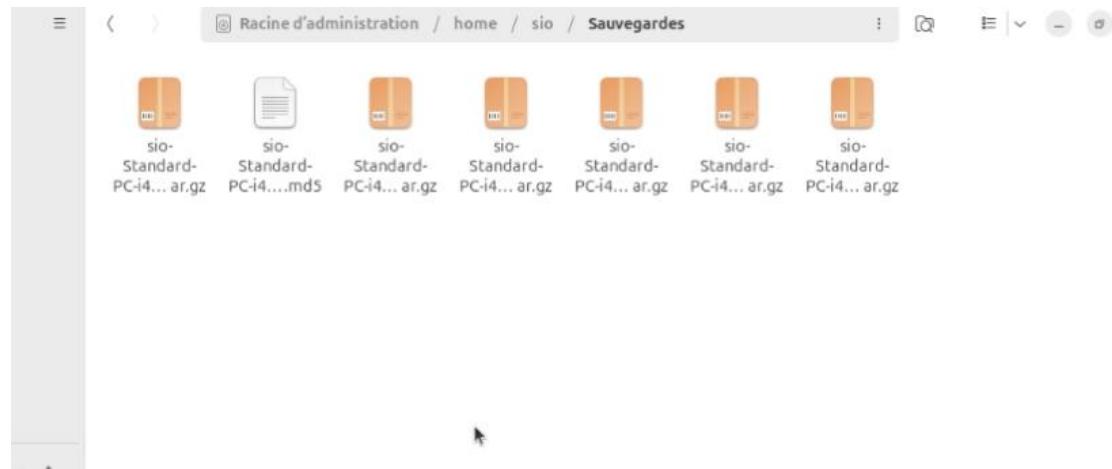
Cela va créer une sauvegarde des répertoires définis dans le fichier de configuration.

Vérifier la sauvegarde

```
ls /home/sio/Sauvegardes
```

```
sio@sio-Standard-PC-i440FX-PIIX-1996: $ sudo ls /home/sio/Sauvegardes
restauration
sio-Standard-PC-i440FX-PIIX-1996-etc.20250315.master
sio-Standard-PC-i440FX-PIIX-1996-etc.20250315.master.tar.gz
sio-Standard-PC-i440FX-PIIX-1996-hashes.md5
sio-Standard-PC-i440FX-PIIX-1996-home.20250315.master.tar.gz
sio-Standard-PC-i440FX-PIIX-1996-home-sio.20250315.master.tar.gz
sio-Standard-PC-i440FX-PIIX-1996-home-sio-packages.list.20250315.master.tar.gz
sio-Standard-PC-i440FX-PIIX-1996-var-lib.20250315.master.tar.gz
sio-Standard-PC-i440FX-PIIX-1996-var-log.20250315.master.tar.gz
```

Tu devrais voir une archive (fichier .tar.gz) qui contient tes fichiers sauvegardés.



9.4.5. Restauration de la Sauvegarde

Créer une sauvegarde préventive dans un nouveau répertoire

```
sio@sio-Standard-PC-i440FX-PIIX-1996: $ sudo cp -a /home/sio/Sauvegardes/sio-Standard-PC-i440FX-PIIX-1996-var-log.20250315.master/var/log/ /home/sio/Sauvegardes/restauration
```



Vérifier que les fichiers ont bien été restaurés

```
sio@sio-Standard-PC-i440FX-PIIX-1996:~$ sudo ls /home/sio/Sauvegardes/restauration
log  'restore.var [log.20250315.tar.gz']'
```





9.5. Cahier de recettes

Étape 1: Installation de Backup Manager

- **Action :** Installer Backup Manager avec la commande `sudo apt install backup-manager`
- **Validation :**
 - L'outil est installé sans erreur
 - La commande `backup-manager --version` fonctionne correctement

Étape 2 : Configuration de Backup Manager

- **Action :** Modifier le fichier de configuration `/etc/backup-manager.conf`
 - Définir le répertoire source à sauvegarder : `/home/sio /var/lib /var/log /etc/apache2 /var/www /etc /home`
 - Définir le répertoire de destination : `/home/sio/Sauvegardes`
 - Choisir le format d'archive : `tar.gz`
- **Validation :**
 - Les chemins sont corrects dans le fichier de configuration
 - Le format d'archive est bien configuré

Étape 3 : Lancement de la sauvegarde

- **Action :** Exécuter la commande `sudo backup-manager` pour créer une archive
- **Validation :**
 - Le fichier de sauvegarde (ex. `/home/sio/Sauvegardes/sio-Standard-PC-i440FX-PIIX-1996-var-lib.20250315.master.tar.gz`) est bien généré
 - L'archive n'est pas vide et ne présente pas d'erreur lors de la création

Étape 4 : Vérification de l'archive

- **Action :**
 - Vérifier la taille de l'archive et l'ouvrir avec la commande `sudo tar -tvf /home/sio/Sauvegardes/sio-Standard-PC-i440FX-PIIX-1996-var-log.20250315.master.tar.gz`
- **Validation :**
 - Tous les fichiers et sous-dossiers d'origine sont bien présents dans l'archive



Étape 5 : Restauration des fichiers

- **Action :**
- Extraire l'archive avec la commande `cp -a /home/sio/Sauvegardes/sio- Standard-PC-i440FX-PIIX-1996-var-log.20250315.master.tar.gz /home/sio/Sauvegardes/restauration`
- **Validation :**
 - Tous les fichiers sont correctement restaurés dans le dossier cible.
 - Les permissions des fichiers sont conservées après extraction.

9.6. Cahier de test

| Test | OK | Remarque |
|--------------------------------------|----|----------|
| Installation de BackupManager | OK | |
| Configuration correcte | OK | |
| Sauvegarde générée avec succès | OK | |
| Vérification du contenu de l'archive | OK | |
| Restauration | OK | |



10. Serveur LAMP

10.1. Cahier des charges

10.1.1. Contexte et Objectifs

Contexte

Dans le cadre d'un projet pédagogique ou professionnel, nous souhaitons installer et configurer un serveur LAMP (Linux, Apache, MySQL, PHP) sur une machine virtuelle Ubuntu 24.04 afin d'héberger des applications web.

Objectif

- Déployer un serveur Ubuntu 24.04.
- Installer et configurer Apache 2 comme serveur web.
- Installer MySQL pour la gestion des bases de données.
- Configurer PHP pour l'exécution des scripts côté serveur.
- Sécuriser le serveur MySQL.
- Tester la bonne communication entre Apache, MySQL et PHP.

10.1.2. Descriptions fonctionnelles des besoins

- Un serveur web Apache pour héberger les sites.
- Un moteur de base de données MySQL.
- PHP pour exécuter les scripts côté serveur.
- Sécurisation de MySQL avec la création d'un utilisateur non-root.
- Vérification que tous les services sont fonctionnels et démarrent automatiquement.

10.1.3. Cahier des charges technique

Environnement technologique :

- OS : Ubuntu Server 24.04
- VM : 1 CPU, 2 cœurs, 2 Go RAM, IP fixe : 10.113.6.57
- Réseau : Bridge VMBR0 sur Proxmox VE

Outils et technologies :

- Apache2 (serveur web)
- MySQL Server (base de données)
- PHP + modules nécessaires (php-mysql, libapache2-mod-php)
- Nano (éditeur)



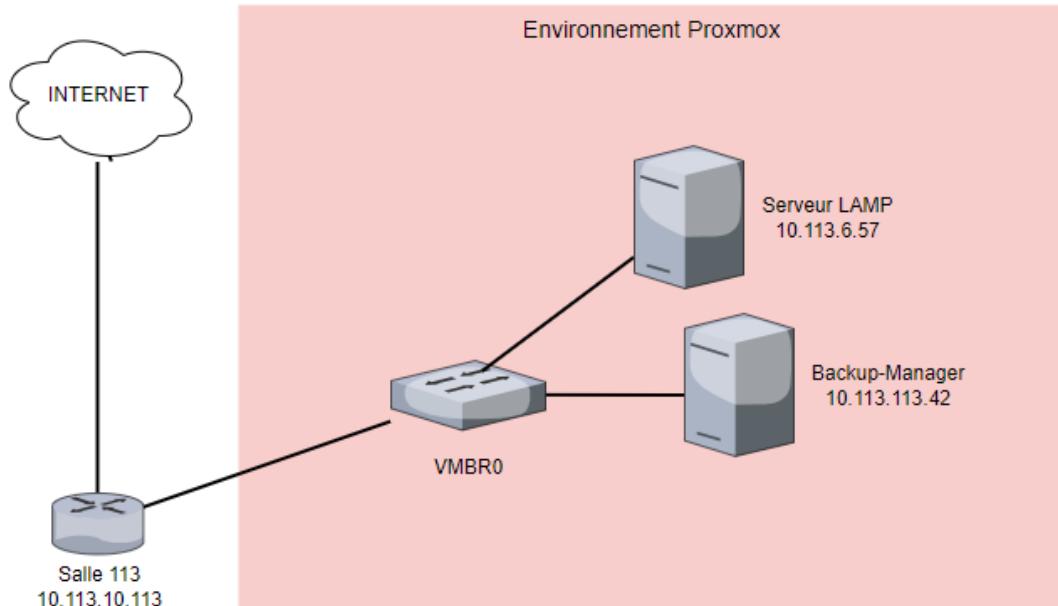
10.1.4. Planning prévisionnel

| Tâche | Durée |
|--|----------|
| Installation de la VM Ubuntu | 1 jour |
| Installation Apache, Mysql et PHP | 1 jour |
| Configuration et sécurisation de Mysql | 1 jour |
| Création de l'utilisateur Mysql non root | 0,5 jour |
| Test de fonctionnalité et finalisation | 1 jour |

10.2. Plan d'adressage

| @réseau | @passerelle | NIC | Machine/rôle | DHCP ? |
|---------------|-------------|-------|--|-----------------------|
| 10.113.6.0/16 | 10.113.6.12 | VMBR0 | BackupManager : 10.113.113.42/16 LAMP : 10.113.6.57/16 | Pas de config DHCP |

10. Schéma réseau



10.3. Documentation technique

10.3.1. Installation et configuration d'une machine virtuelle Ubuntu sous Linux

Créer une machine virtuelle Ubuntu sous Linux avec les configurations suivantes :

| Nom | ID | OS | Mémoire | RAM | Réseau |
|----------|-------|--------------|--------------------------|-------|-------------|
| ubu-LAMP | VM107 | Ubuntu 24.04 | 1 processeur 2 coeurs | VMBR0 | 10.113.6.57 |

Identifiant administrateur : Sio



Mot de passe administrateur : labo-113

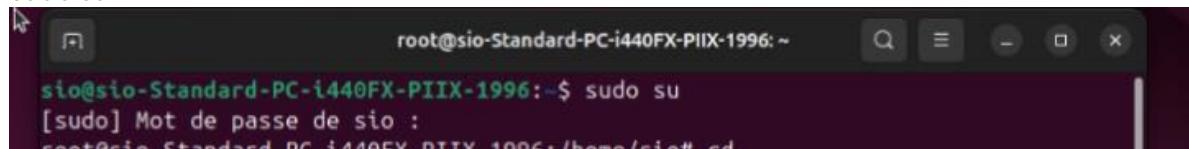
10.3.2. Mise à jour des paquets

Ouvrir le terminal de commande de la machine Ubuntu sous Linux



Accéder aux droits administrateurs avec la commande :

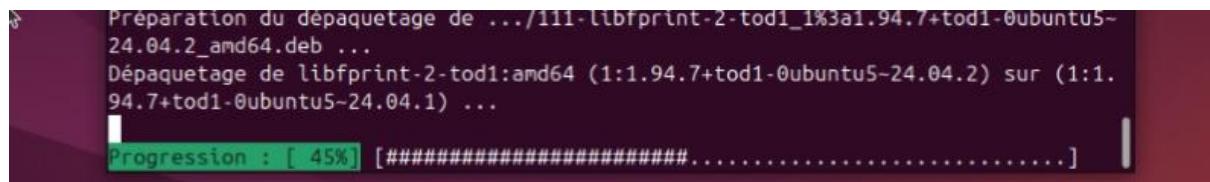
`sudo su`



```
root@sio-Standard-PC-i440FX-PIIX-1996:~$ sudo su
[sudo] Mot de passe de sio :
```

Se connecter avec le mot de passe de l'administrateur "labo-113"

Les commandes "`sudo apt update`" et "`sudo apt upgrade -y`" mettent à jour la liste des paquets disponibles, garantissant que les dernières versions des logiciels sont installées.



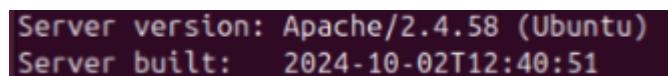
```
Préparation du dépaquetage de .../libfprint-2-tod1_1%3a1.94.7+tod1-0ubuntu5-24.04.2_amd64.deb ...
Dépaquetage de libfprint-2-tod1:amd64 (1:1.94.7+tod1-0ubuntu5-24.04.2) sur (1:1.94.7+tod1-0ubuntu5-24.04.1) ...
Progression : [ 45%] [#####.....]
```

10.3.3. Installation des composants de LAMP

Installation de Apache 2

`Sudo apt install apache2`

Après avoir installé Apache2 avec la commande ci-dessus, nous pouvons vérifier son installation avec `apache2 -v`, qui affiche la version installée.



```
Server version: Apache/2.4.58 (Ubuntu)
Server built:   2024-10-02T12:40:51
```

S'assurer que le service Apache2 fonctionne :

`sudo systemctl status apache2`



```
root@stio-Standard-PC-i440FX-PIIX-1996:~# systemctl status apache2
● apache2.service - The Apache HTTP Server
  Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: >
  Active: active (running) since Thu 2025-03-20 23:21:17 CET; 4min 49s ago
    Docs: https://httpd.apache.org/docs/2.4/
```

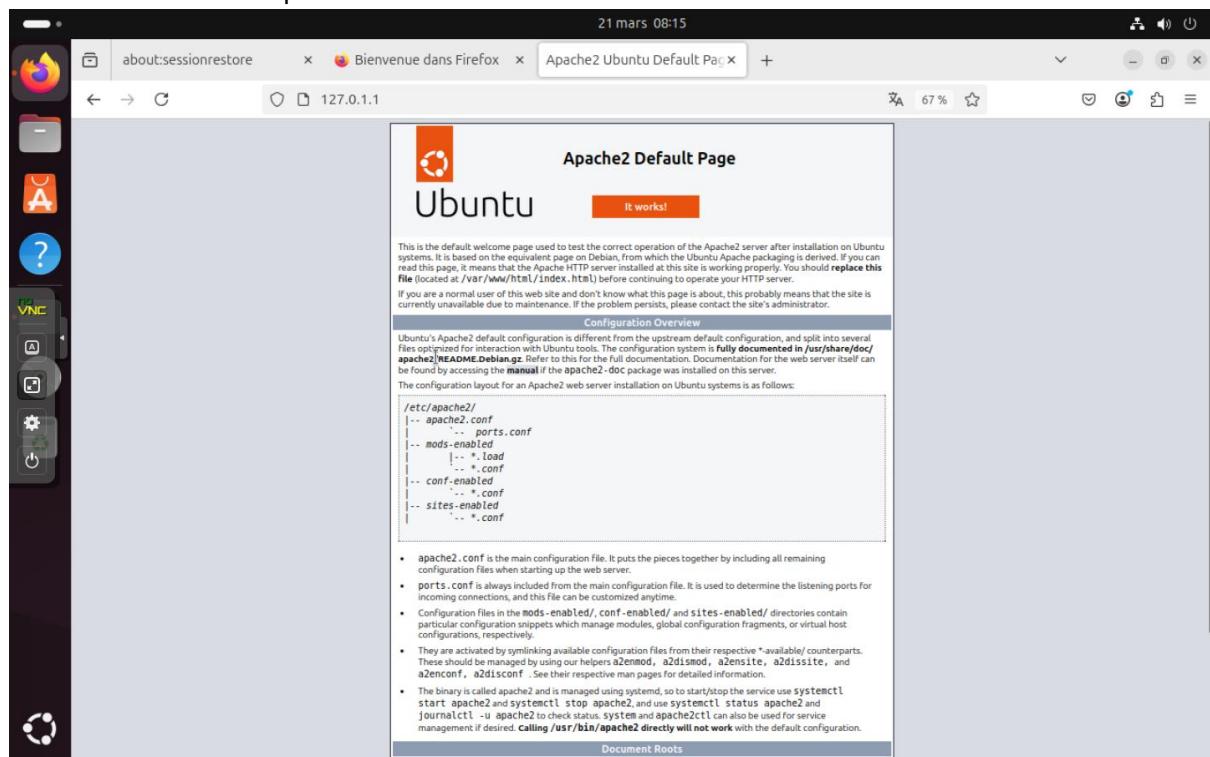
On peut vérifier que le Apache2 fonctionne bien avec l'adresse ip du serveur ou le lien URL <http://localhost>

Retrouver l'adresse ip du serveur Apache 2 :

hostname -i

```
bio@stio-Standard-PC-i440FX-PIIX-1996:~$ hostname -i
127.0.1.1
```

Entrer l'adresse ip dans un moteur de recherche comme Mozilla Firefox

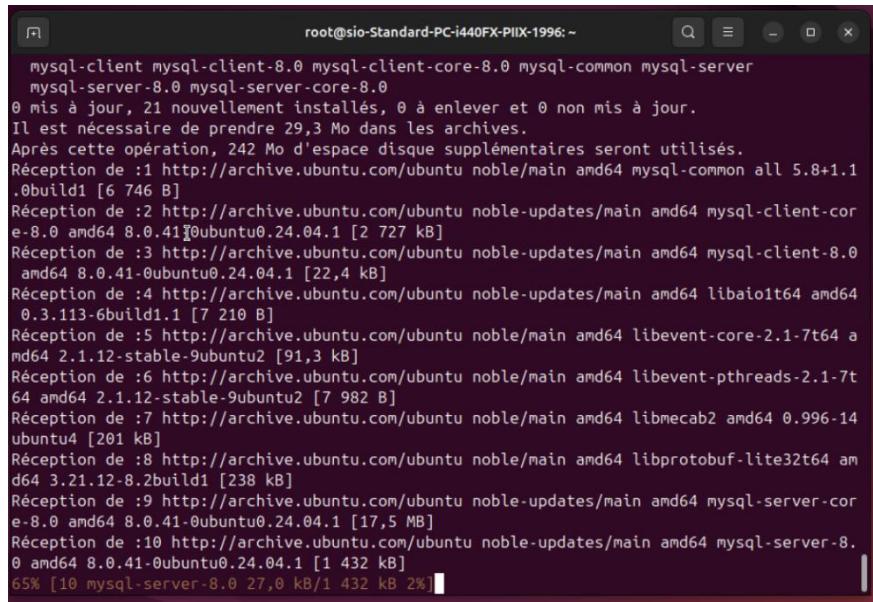


Si cette page apparaît ça veut dire que le serveur Apache2 fonctionne bien.

Installation de Mysql

Pour gérer les bases de données utilisées par les applications web :

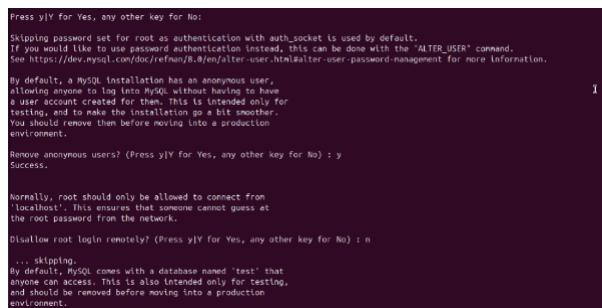
```
sudo apt install mysql-server mysql-client -y
```



```
root@sio-Standard-PC-i440FX-PIIX-1996: ~
mysql-client mysql-client-8.0 mysql-client-core-8.0 mysql-common mysql-server
mysql-server-8.0 mysql-server-core-8.0
0 mis à jour, 21 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 29,3 Mo dans les archives.
Après cette opération, 242 Mo d'espace disque supplémentaires seront utilisés.
Réception de :1 http://archive.ubuntu.com/ubuntu noble/main amd64 mysql-common all 5.8+1.1
..0build1 [6 746 B]
Réception de :2 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 mysql-client-cor
e-8.0 amd64 8.0.41-0ubuntu0.24.04.1 [2 727 kB]
Réception de :3 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 mysql-client-8.0
amd64 8.0.41-0ubuntu0.24.04.1 [22,4 kB]
Réception de :4 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 libaio1t64 amd64
0.3.113-6build1.1 [7 210 B]
Réception de :5 http://archive.ubuntu.com/ubuntu noble/main amd64 libevent-core-2.1-7t64 a
md64 2.1.12-stable-9ubuntu2 [91,3 kB]
Réception de :6 http://archive.ubuntu.com/ubuntu noble/main amd64 libevent-pthreads-2.1-7t
64 amd64 2.1.12-stable-9ubuntu2 [7 982 B]
Réception de :7 http://archive.ubuntu.com/ubuntu noble/main amd64 libmecab2 amd64 0.996-14
ubuntu4 [201 kB]
Réception de :8 http://archive.ubuntu.com/ubuntu noble/main amd64 libprotobuf-lite32t64 am
d64 3.21.12-8.2build1 [238 kB]
Réception de :9 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 mysql-server-cor
e-8.0 amd64 8.0.41-0ubuntu0.24.04.1 [17,5 MB]
Réception de :10 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 mysql-server-8.
0 amd64 8.0.41-0ubuntu0.24.04.1 [1 432 kB]
65% |10 mysql-server-8.0 27,0 kB/1 432 kB 2%
```

Installer la sécurisation de la base de données :

`sudo mysql_secure_installation`



```
Press y|Y for Yes, any other key for No:
Skipping password set for root as authentication with auth_socket is used by default.
If you would like to use password authentication instead, this can be done with the 'ALTER_USER' command.
See https://dev.mysql.com/doc/refman/8.0/en/alter-user.html#alter-user-password-management for more information.

By default, a MySQL installation has an anonymous user,
allowing anyone to log into MySQL without having to have
a user account created for them. This is intended only for
testing, and to make the installation go a bit smoother.
You should remove them before moving into a production
environment.

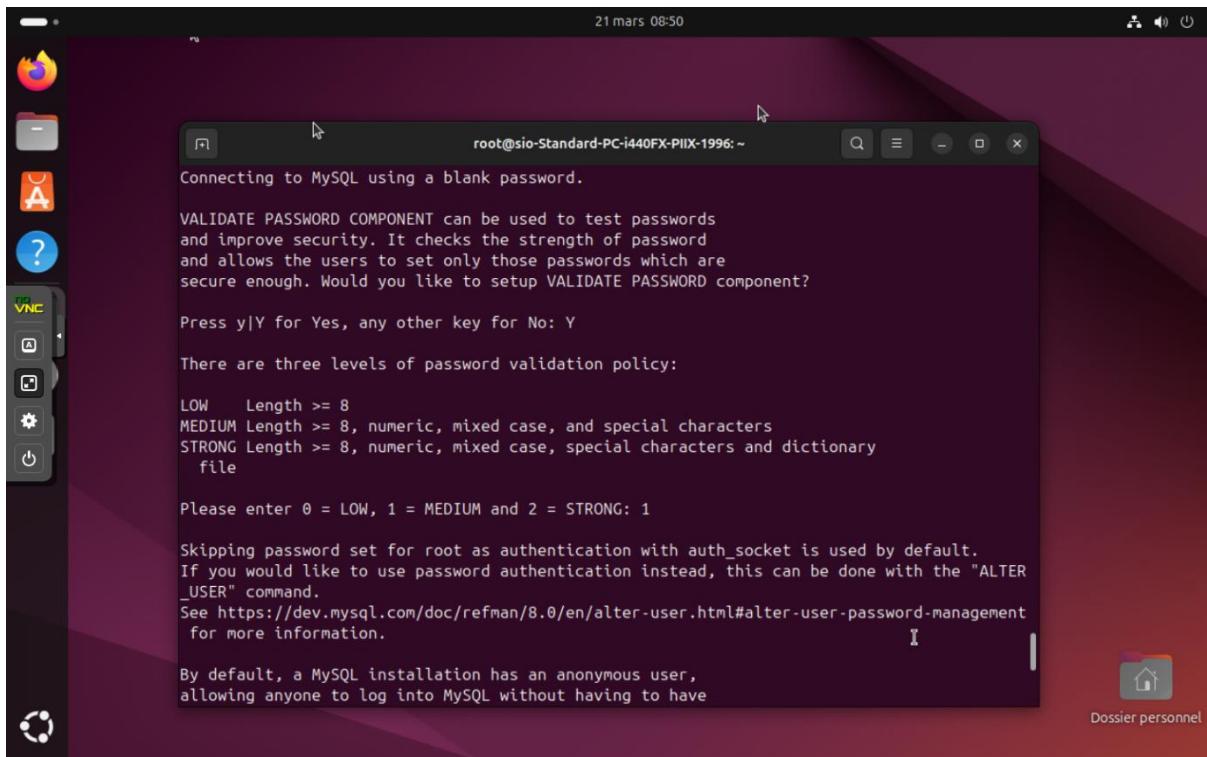
Remove anonymous users? (Press y|Y for Yes, any other key for No) : y
Success.

Normally, root should only be allowed to connect from
'localhost'. This ensures that someone cannot guess at
the root password from the network.

Disallow root login remotely? (Press y|Y for Yes, any other key for No) : n
.... skipping.

By default, MySQL comes with a database named 'test' that
anyone can access. This is also intended only for testing,
and should be removed before moving into a production
environment.
```

Determiner le niveau de sécurité 1, 2 ou 3 :



```
21 mars 08:50
root@sio-Standard-PC-i440FX-PIIX-1996: ~
Connecting to MySQL using a blank password.

VALIDATE PASSWORD COMPONENT can be used to test passwords
and improve security. It checks the strength of password
and allows the users to set only those passwords which are
secure enough. Would you like to setup VALIDATE PASSWORD component?

Press y|Y for Yes, any other key for No: Y

There are three levels of password validation policy:

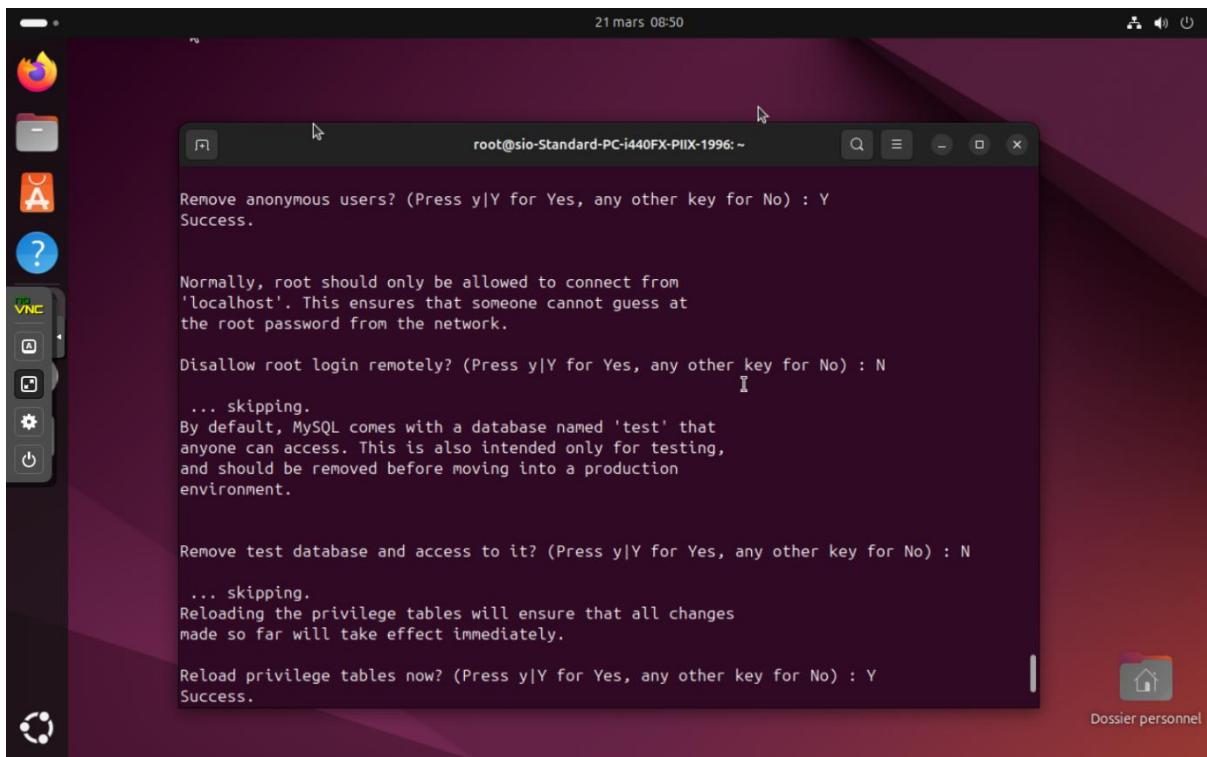
LOW    Length >= 8
MEDIUM Length >= 8, numeric, mixed case, and special characters
STRONG Length >= 8, numeric, mixed case, special characters and dictionary
      file

Please enter 0 = LOW, 1 = MEDIUM and 2 = STRONG: 1

Skipping password set for root as authentication with auth_socket is used by default.
If you would like to use password authentication instead, this can be done with the "ALTER
_USER" command.
See https://dev.mysql.com/doc/refman/8.0/en/alter-user.html#alter-user-password-management
      for more information.

By default, a MySQL installation has an anonymous user,
allowing anyone to log into MySQL without having to have
```

Ici on a choisi le niveau 1 qui donne l'obligation de créer un mot de passe de 8 caractères, de chiffres et de caractères spéciaux.



```
21 mars 08:50
root@sio-Standard-PC-i440FX-PIIX-1996: ~
Remove anonymous users? (Press y|Y for Yes, any other key for No) : Y
Success.

Normally, root should only be allowed to connect from
'localhost'. This ensures that someone cannot guess at
the root password from the network.

Disallow root login remotely? (Press y|Y for Yes, any other key for No) : N
... skipping.

By default, MySQL comes with a database named 'test' that
anyone can access. This is also intended only for testing,
and should be removed before moving into a production
environment.

Remove test database and access to it? (Press y|Y for Yes, any other key for No) : N
... skipping.

Reloading the privilege tables will ensure that all changes
made so far will take effect immediately.

Reload privilege tables now? (Press y|Y for Yes, any other key for No) : Y
Success.
```

Supprimer ou pas les utilisateurs anonymes

“ Reload privileges tables – Y”Appliquer immédiatement toutes les modifications faites, comme :



- Suppression des utilisateurs anonymes
- Désactivation des connexions root distantes
- Suppression de la base de test
- Changements de mot de passe pour root

Vérifier que le serveur MySQL est bien installé et opérationnel

```
All done!
root@sio-Standard-PC-i440FX-PIIX-1996:~# sudo systemctl status mysql
● mysql.service - MySQL Community Server
  Loaded: loaded (/usr/lib/systemd/system/mysql.service; enabled; preset: enabled)
  Active: active (running) since Fri 2025-03-21 08:34:25 CET; 12min ago
    Process: 7381 ExecStartPre=/usr/share/mysql/mysql-systemd-start pre (code=exited, sta>
  Main PID: 7390 (mysqld)
    Status: "Server is operational"
   Tasks: 38 (limit: 2985)
  Memory: 364.5M (peak: 378.0M)
    CPU: 4.445s
   CGroup: /system.slice/mysql.service
           └─7390 /usr/sbin/mysqld

mars 21 08:34:25 sio-Standard-PC-i440FX-PIIX-1996 systemd[1]: Starting mysql.service - My>
mars 21 08:34:25 sio-Standard-PC-i440FX-PIIX-1996 systemd[1]: Started mysql.service - MyS>
lines 1-14/14 (END)
```

Pour utiliser mysql avec le rôle “administrateur”

```
sudo mysql -u root -p
```

Entrer le mot de passe administrateur : labo-113

```
Main PID: 7390 (mysqld)
Status: "Server is operational"
Tasks: 38 (limit: 2985)
Memory: 364.5M (peak: 378.0M)
CPU: 4.445s
CGroup: /system.slice/mysql.service
        └─7390 /usr/sbin/mysqld

mars 21 08:34:25 sio-Standard-PC-i440FX-PIIX-1996 systemd[1]: Starting mysql.service - My>
mars 21 08:34:25 sio-Standard-PC-i440FX-PIIX-1996 systemd[1]: Started mysql.service - MyS>
lines 1-14/14 (END)
root@sio-Standard-PC-i440FX-PIIX-1996:~# sudo mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 10
Server version: 8.0.41-0ubuntu0.24.04.1 (Ubuntu)

Copyright (c) 2000, 2025, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> 
```

Lister la liste des bases existantes “`show databases;`”

ATTENTION à ne pas oublier de mettre un point-virgule “;” à la fin de chaque commande dans la base de données



```
-> /c
-> ^C
mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| sys |
+-----+
4 rows in set (0,00 sec)

mysql>
```

Affiche le statut du serveur “show status;”

```
21 mars 09:09
root@sio-Standard-PC-i440FX-PIIX-1996: ~
| Max_execution_time_set | 0
| Max_execution_time_set_failed | 0
| Max_used_connections | 1
| Max_used_connections_time | 2025-03-21 08:35:09
| Mysqlx_aborted_clients | 0
| Mysqlx_address | 127.0.0.1
| Mysqlx_bytes_received | 0
```



| Performance Schema Component | Lost Events |
|---|-------------|
| Performance_schema_nested_statement_lost | 0 |
| Performance_schema_prepared_statements_lost | 0 |
| Performance_schema_program_lost | 0 |
| Performance_schema_rwlock_classes_lost | 0 |
| Performance_schema_rwlock_instances_lost | 0 |
| Performance_schema_session_connect_attrs_longest_seen | 131 |

Sélectionner la base de données par défaut “`use mysql;`” Notre base de données par défaut est “`mysql`”

Afficher les tables de notre base courante mysql “`show tables;`”

```
mysql> create database lamp
-> ^C
mysql> show tables;
+-----+
| Tables_in_mysql |
+-----+
| columns_priv
| component
| db
| default_roles
| engine_cost
| func
| general_log
| global_grants
| gtid_executed
| help_category
| help_keyword
| help_relation
| help_topic
| innodb_index_stats
| innodb_table_stats
| password_history
| plugin
| procs_priv
| proxies_priv
| replication_asynchronous_connection_failover
| replication_asynchronous_connection_failover_managed
| replication_group_configuration_version
| replication_group_member_actions
| role_edges
| server_cost
| servers
```

Créer une nouvelle base de données avec la commande “`create database lamp`”

Vérifier que la base de données a bien été installée “`show databases`”



```
mysql> create database lamp;
Query OK, 1 row affected (0,02 sec)

mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| lamp |
| mysql |
| performance_schema |
| sys |
+-----+
5 rows in set (0,00 sec)

mysql>
```

Pour initialiser l'authentification du client root avec un mot de passe, utilisez l'instruction **ALTER USER** pour définir le plugin "**mysql_native_password**".

ALTER USER 'root'@'localhost' IDENTIFIED WITH mysql_native_password BY 'password';

Enregistrer les modifications ci-dessus comme suit :

FLUSH PRIVILEGES;

```
mysql> ALTER USER 'root'@'localhost' IDENTIFIED WITH mysql_native_password BY 'Labo-113';
Query OK, 0 rows affected (0,02 sec)

mysql> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0,01 sec)

mysql>
```

L'instruction [MySQL](#) "FLUSH PRIVILEGES" enregistre les modifications apportées aux tables de la base de données par les clauses ALTER, INSERT, UPDATE et DELETE.

Créez un nouveau compte et accordez tous les priviléges pour attribuer un contrôle de niveau administratif au nouvel utilisateur. Ensuite, quittez l'invite MySQL. Exécutez les requêtes SQL suivantes une par une pour y parvenir :

```
CREATE USER 'ubuntu'@'localhost' IDENTIFIED BY 'labO-113';
GRANT ALL PRIVILEGES ON *.* TO 'ubuntu'@'localhost' WITH GRANT OPTION;
```

```
mysql> CREATE USER 'ubuntu'@'localhost' IDENTIFIED BY 'labO-113';
Query OK, 0 rows affected (0,02 sec)

mysql> GRANT ALL PRIVILEGES ON *.* TO 'ubuntu'@'localhost' WITH GRANT OPTION;
Query OK, 0 rows affected (0,02 sec)

mysql> exit
Bye
root@sio-Standard-PC-i440FX-PIIX-1996:~#
```

"exit" Pour quitter la base de données

Configurez le service pour qu'il s'exécute au démarrage du serveur Ubuntu en utilisant la commande **systemctl enable** comme suit :

```
sudo systemctl enable mysql
```



De plus, vous pouvez tester le serveur pour qu'il soit opérationnel en tapant :

```
sudo systemctl status mysql
```

```
root@sio-Standard-PC-i440FX-PIIX-1996:~# sudo systemctl enable mysql
Synchronizing state of mysql.service with SysV service script with /usr/lib/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/lib/systemd/systemd-sysv-install enable mysql
root@sio-Standard-PC-i440FX-PIIX-1996:~# sudo systemctl status mysql
● mysql.service - MySQL Community Server
    Loaded: loaded (/usr/lib/lib/systemd/system/mysql.service; enabled; preset: enabled)
    Active: active (running) since Fri 2025-03-21 08:34:25 CET; 1h 5min ago
      Main PID: 7390 (mysqld)
        Status: "Server is operational"
          Tasks: 38 (limit: 2985)
        Memory: 391.5M (peak: 392.0M)
          CPU: 32.81s
        CGroup: /system.slice/mysql.service
                └─7390 /usr/sbin/mysqld

mars 21 08:34:25 sio-Standard-PC-i440FX-PIIX-1996 systemd[1]: Starting mysql.service - MySQL Community Server...
mars 21 08:34:25 sio-Standard-PC-i440FX-PIIX-1996 systemd[1]: Started mysql.service - MySQL Community Server.
root@sio-Standard-PC-i440FX-PIIX-1996:~#
```

Installation de PHP

PHP permet d'exécuter des scripts côté serveur.

```
Sudo apt install php libapache2-mod-php php-mysql -y
```

```
sio@sio-Standard-PC-i440FX-PIIX-1996:~ Paramétrage de php8.3-readline (8.3.19-1+ubuntu24.04.1+deb.sury.org+1) ...
Creating config file /etc/php/8.3/mods-available/readline.ini with new version
Paramétrage de php8.3-opcache (8.3.19-1+ubuntu24.04.1+deb.sury.org+1) ...
Creating config file /etc/php/8.3/mods-available/opcache.ini with new version
Paramétrage de php8.3-cli (8.3.19-1+ubuntu24.04.1+deb.sury.org+1) ...
Creating config file /etc/php/8.3/cli/php.ini with new version
Paramétrage de libapache2-mod-php8.3 (8.3.19-1+ubuntu24.04.1+deb.sury.org+1) ...
Creating config file /etc/php/8.3/apache2/php.ini with new version
libapache2-mod-php8.3: php8.1 module already enabled, not enabling PHP 8.3
Paramétrage de php8.3 (8.3.19-1+ubuntu24.04.1+deb.sury.org+1) ...
Paramétrage de libapache2-mod-php (2:8.3+95+ubuntu24.04.1+deb.sury.org+2) ...
Paramétrage de php (2:8.3+95+ubuntu24.04.1+deb.sury.org+2) ...
Traitement des actions différées (« triggers ») pour man-db (2.12.0-4build2) ...
Traitement des actions différées (« triggers ») pour php8.3-cli (8.3.19-1+ubuntu24.04.1+deb.sury.org+1) ...
Traitement des actions différées (« triggers ») pour libapache2-mod-php8.3 (8.3.19-1+ubuntu24.04.1+deb.sury.org+1) ...
sio@sio-Standard-PC-i440FX-PIIX-1996:~$
```

```
Php -v
```

```
sio@sio-Standard-PC-i440FX-PIIX-1996:~$ php -v
PHP 8.4.5 (cli) (built: Mar 13 2025 15:36:20) (NTS)
Copyright (c) The PHP Group
Zend Engine v4.4.5, Copyright (c) Zend Technologies
    with Zend OPcache v8.4.5, Copyright (c), by Zend Technologies
```

```
sudo nano /var/www/html/phpinfo.php
```



root@srv-LAMP:/home/user
/var/www/html//phpinfo.php: 4

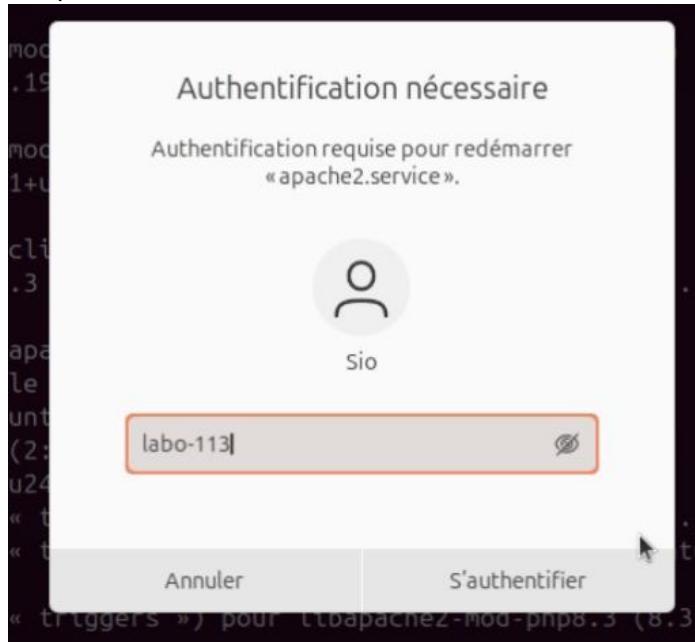
GNU nano 7.2

... (Terminal menu bar: Aide, Quitter, Ecrire Fich., Chercher, Remplacer, Couper, Coler, Exécuter, Emplacement, Annuler, Marquer, > Crochet, Lire Fich., Remplacer, Couper, Coler, Justifier, Emplacement, Annuler, Marquer, > Crochet, Retrouver)

```
<?php phpinfo(); ?>
```

Redémarrer apache 2 et mysql afin de prendre en compte PHP :

Sudo systemctl restart apache2



Sudo systemctl restart mysql

10.4. Cahier de recettes

L'objectif de ce cahier des recettes est de valider l'installation et la configuration d'un serveur LAMP (Linux, Apache, MySQL, PHP) sur une machine virtuelle Ubuntu 24.04. La recette a pour but de s'assurer que :

- Chaque composant du stack LAMP est correctement installé et opérationnel.
- Le serveur respecte les normes de sécurité de base (ex : sécurisation MySQL).
- Les services Apache, MySQL et PHP sont fonctionnels et interconnectés.
- Le serveur est accessible via son adresse IP locale et les tests d'intégration sont validés.



10.5. Cahier de test

| Test | OK | Remarque |
|--|----|--------------------------|
| Apache est installé et la page par défaut est visible | Ok | |
| MySQL est installé et sécurisé avec mot de passe root | Ok | Labo-113 en mot de passe |
| Création de l'utilisateur MySQL "ubuntu" réussie | Ok | |
| PHP est installé et fonctionne avec Apache | Ok | |
| La page <code>phpinfo()</code> affiche bien la configuration PHP | Ok | |
| Redémarrage automatique des services Apache et MySQL | Ok | |
| Le serveur est accessible via <code>http://10.113.6.57</code> | Ok | |



11. GLPI + agent

11.1. Cahier des charges

11.1.1. Contexte et Objectifs

Contexte

Dans le cadre de l'amélioration de la gestion du parc informatique, il est nécessaire d'installer une solution de gestion centralisée. Le choix s'est porté sur **GLPI**, un outil open source permettant la gestion des tickets, des équipements, des utilisateurs, et l'inventaire automatique.

Objectif

- Installer un serveur GLPI sur Ubuntu (192.168.32.10)
- Connecter des postes via l'agent GLPI (Linux & Windows)
- Permettre l'inventaire automatique et la gestion des tickets

11.1.2. Descriptions fonctionnelles des besoins

| Besoin | Description |
|----------------------------------|--|
| Gestion des tickets | Création et suivi de demandes utilisateurs |
| Inventaire automatique | Collecte des infos matérielles/logicielles |
| Interface Web centralisée | Accessible depuis le réseau interne |
| Création de profils utilisateurs | Technicien, administrateur, utilisateurs standards |
| Historique des interventions | Traçabilité des actions effectuées |
| Notifications par mail | Pour les tickets ouverts/fermés/affectés |

11.1.3. Cahier des charges technique

| Élément | Spécification |
|---------------------|--------------------------------|
| Système serveur | Ubuntu 24.04 LTS |
| IP serveur GLPI | 192.168.32.10 |
| Services installés | Apache2, MariaDB, PHP 8+, GLPI |
| Base de données | glpidb (user: glpiuser) |
| Agents GLPI | Version 1.13 (Linux & Windows) |
| Communication agent | HTTP ou HTTPS vers /glpi |
| Port agent local | 62354 |

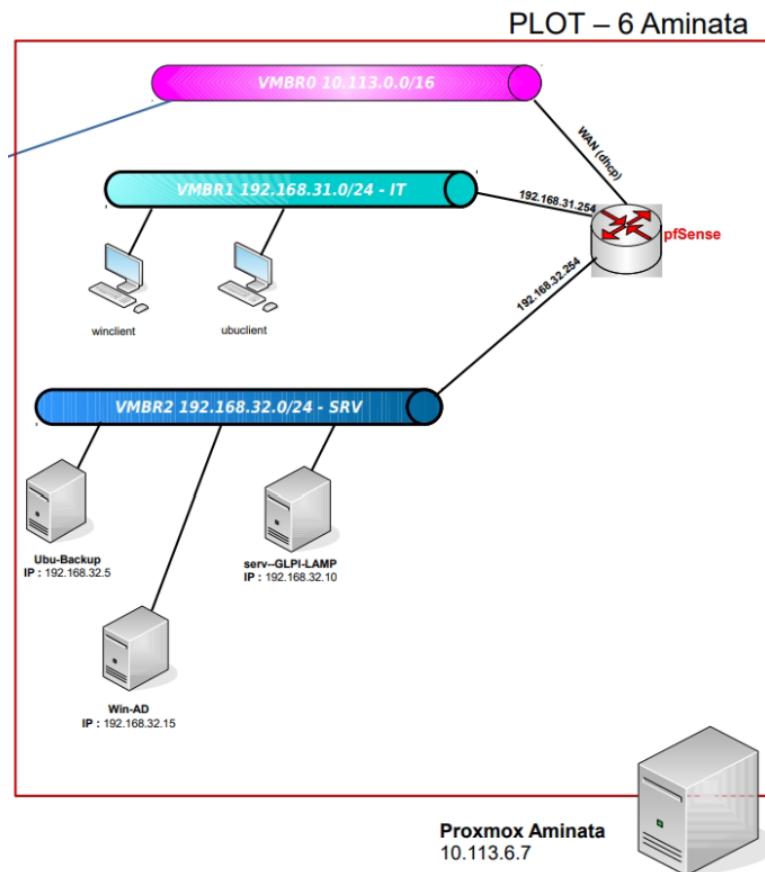
11.1.4. Planning prévisionnel

| Tâche | Durée |
|-------------------------------------|----------|
| Mise en place du serveur Ubuntu | 0,5 jour |
| Installation de GLPI | 1 jour |
| Configuration base de données | 0,5 jour |
| Installation agent GLPI (Linux) | 0,5 jour |
| Installation agent GLPI (Windows) | 0,5 jour |
| Tests de remontée d'inventaire | 0,5 jour |
| Rédaction documentation utilisateur | 0,5 jour |

11.2. Plan d'adressage

| @réseau | @passerelle | NIC | Machine/rôle | Plages d'adresses attribuables (DHCP) |
|------------------|----------------|------------|---|---------------------------------------|
| 192.168.3.1.0/24 | 192.168.31.254 | VMB R1 IT | Machine cliente ubuntu et windows | DHCP 192.168.31.1 à 192.168.31.253 |
| 192.168.3.2.0/24 | 192.168.32.254 | VMB R2 SRV | Ubu-Backup : 192.168.32.5 Serv-GLPI-LAMP : 192.168.32.10 Win-AD : 192.168.32.15 | DHCP 192.168.32.1 à 192.168.32.253 |

11.3. Schéma réseau





11.4. Documentation technique

11.4.1. Installation d'un serveur GLPI sous Linux (ubuntu)

Prérequis :

- Machine virtuelle Ubuntu (24.04 LTS)
- IP statique : 192.168.32.10
- Droits administrateur (sudo)

Mise à jour du système

```
sudo apt update && sudo apt upgrade -y
```

```
Installation des paquets nécessaires : sudo apt install apache2 mariadb-server php php-mysql  
php-curl php-gd php-imap php-mbstring php-xml php-cli php-ldap php-zip php-bz2 php-intl  
unzip -y
```

Sécurisation de la base de données mariadb :

```
sudo mysql_secure_installation
```

```
Connexion à mariadb : sudo mysql -u root -p
```

Commandes SQL à exécuter :

```
CREATE DATABASE glpidb;  
CREATE USER 'glpiuser'@'localhost' IDENTIFIED BY 'Labo-113';  
GRANT ALL PRIVILEGES ON glpidb.* TO 'glpiuser'@'localhost';  
FLUSH PRIVILEGES;  
EXIT;
```

Téléchargement et installation de la nouvelle version de glpi

(sans oublier de donner les bons droits) :

```
cd /tmp  
wget https://github.com/glpi-project/glpi/releases/download/10.0.18/glpi-10.0.18.tgz  
tar -xvzf glpi-10.0.18.tgz  
sudo mv glpi /var/www/html/  
sudo chown -R www-data:www-data /var/www/html/glpi  
sudo chmod -R 755 /var/www/html/glpi
```



Création d'un fichier de configuration pour GLPI :

```
sudo nano /etc/apache2/sites-available/glpi.conf
```

Voici le script à insérer dans la page de configuration :

```
<VirtualHost *:80>
ServerAdmin admin@glpi.local
DocumentRoot /var/www/html/glpi
ServerName glpi.local
<Directory /var/www/html/glpi>
    Options FollowSymlinks
    AllowOverride All
    Require all granted
</Directory>
ErrorLog ${APACHE_LOG_DIR}/glpi_error.log
CustomLog ${APACHE_LOG_DIR}/glpi_access.log combined
</VirtualHost>
```

Activation du site et redémarrage d'Apache :

```
sudo a2ensite glpi.conf
sudo a2enmod rewrite
sudo systemctl restart apache2
```

Accès à GLPI via navigateur :

<http://192.168.32.10> C'est l'adresse à entrer dans le navigateur pour accéder à l'interface glpi

Dans l'interface il faut :

- Se connecter à la base avec :
 - Host : localhost
 - Base : glpidb
 - Utilisateur : glpiuser
 - Mot de passe : Labo-113

Après installation, les comptes par défaut sont :

| Utilisateur | Mot de passe |
|-------------|--------------|
| glpi | glpi |
| tech | tech |
| normal | normal |
| post-only | postonly |

Dans l'interface, aller dans "Administration" puis "Inventaire" et activer l'inventaire.



11.4.2. Agent GLPI sous Linux (ubuntu)

Prérequis :

- Système Ubuntu
- Accès root (sudo)
- Accès internet pour télécharger l'agent
- Le port **62354** (interface agent) est facultatif mais utile pour tester

Mise à jour du système :

```
sudo apt update && sudo apt upgrade -y
```

Installation de perl :

```
root@backupmanager:/home/user# sudo apt install perl
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
perl est déjà la version la plus récente (5.38.2-3.2build2.1).
perl passé en « installé manuellement ».
Les paquets suivants ont été installés automatiquement et ne sont plus nécessaires :
  libllvm17t64 python3-netifaces
Veuillez utiliser « sudo apt autoremove » pour les supprimer.
0 mis à jour, 0 nouvellement installés, 0 à enlever et 1 non mis à jour.
```

Téléchargement de la dernière version de l'agent glpi depuis la page officielle de github :

```
wget https://github.com/glpi-project/glpi-agent/releases/download/1.13/glpi-agent_1.13-1_all.deb
```

Installation du paquet : Sudo dpkg -i glpi-agent_1.13-1_all.deb

```
Dépaquetage de glpi-agent (1:1.13-1) ...
dpkg: des problèmes de dépendances empêchent la configuration de glpi-agent :
  glpi-agent dépend de libnet-cups-perl; cependant :
```

Vérification de l'installation de l'agent glpi : dpkg -l | grep glpi-agent

```
root@backupmanager:/home/user# dpkg -l | grep glpi-agent
ii  glpi-agent                         1:1.13-1                               all          hardware and so
```

Installation des dépendances nécessaires : Sudo apt-get install -f

```
root@backupmanager:/home/user# sudo apt-get install -f
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
```

Configuration de l'agent : Sudo nano /etc/glpi-agent/agent.cfg

La page de configuration doit contenir les lignes suivantes :

```
# send tasks results to a GLPI server
server = http://192.168.32.10/glpi
```



Activation et démarrage de l'agent glpi :

```
user@user-Standard-PC-i440FX-PIIX-1996:~$ sudo systemctl enable glpi-agent
user@user-Standard-PC-i440FX-PIIX-1996:~$ sudo systemctl start glpi-agent
```

Vérification du fonctionnement de l'agent glpi :

```
user@user-Standard-PC-i440FX-PIIX-1996:~$ sudo systemctl status glpi-agent
● glpi-agent.service - GLPI agent
  Loaded: loaded (/usr/lib/systemd/system/glpi-agent.service; enabled; preset: enabled)
  Active: active (running) since Sun 2025-04-06 00:24:29 CEST; 12s ago
    Docs: man:glpi-agent
   Main PID: 38033 (glpi-agent: wai)
      Tasks: 1 (limit: 2278)
     Memory: 65.6M (peak: 67.6M)
        CPU: 320ms
       CGroup: /system.slice/glpi-agent.service
               └─38033 "glpi-agent: waiting"

avril 06 00:24:29 user-Standard-PC-i440FX-PIIX-1996 systemd[1]: Started glpi-agent.service - GLPI agent.
avril 06 00:24:29 user-Standard-PC-i440FX-PIIX-1996 (pi-agent)[38033]: glpi-agent.service: Referenced but unset environment variable evaluates to an empty string: OPTIONS
avril 06 00:24:29 user-Standard-PC-i440FX-PIIX-1996 glpi-agent[38033]: [info] GLPI Agent starting
avril 06 00:24:29 user-Standard-PC-i440FX-PIIX-1996 glpi-agent[38033]: [info] [http server] HTTPD service started on port 62354
avril 06 00:24:29 user-Standard-PC-i440FX-PIIX-1996 glpi-agent[38033]: [info] target server0: next run: Sun Apr 6 01:15:00 2025
```

Désormais, l'agent fonctionne !

```
user@user-Standard-PC-i440FX-PIIX-1996:~$ sudo journalctl -u glpi-agent -f
avril 06 00:19:19 user-Standard-PC-i440FX-PIIX-1996 systemd[1]: Started glpi-agent.service - GLPI agent.
avril 06 00:19:19 user-Standard-PC-i440FX-PIIX-1996 glpi-agent[36905]: Execution failure:.
avril 06 00:19:19 user-Standard-PC-i440FX-PIIX-1996 glpi-agent[36905]: Config: non-existing file /etc/glpi-agent/agent.cfg
avril 06 00:19:19 user-Standard-PC-i440FX-PIIX-1996 systemd[1]: glpi-agent.service: Main process exited, code=exited, status=1/FAILURE
avril 06 00:19:19 user-Standard-PC-i440FX-PIIX-1996 systemd[1]: glpi-agent.service: Failed with result 'exit-code'.
avril 06 00:24:29 user-Standard-PC-i440FX-PIIX-1996 systemd[1]: Started glpi-agent.service - GLPI agent.
avril 06 00:24:29 user-Standard-PC-i440FX-PIIX-1996 (pi-agent)[38033]: glpi-agent.service: Referenced but unset environment variable evaluates to an empty string: OPTIONS
avril 06 00:24:29 user-Standard-PC-i440FX-PIIX-1996 glpi-agent[38033]: [info] GLPI Agent starting
avril 06 00:24:29 user-Standard-PC-i440FX-PIIX-1996 glpi-agent[38033]: [info] [http server] HTTPD service started on port 62354
avril 06 00:24:29 user-Standard-PC-i440FX-PIIX-1996 glpi-agent[38033]: [info] target server0: next run: Sun Apr 6 01:15:00 2025 - http://192.168.32.10/glpi
^C
```

Lancement manuel d'un inventaire :

```
user@user-Standard-PC-i440FX-PIIX-1996:~$ sudo glpi-agent --server http://192.168.32.10/glpi
[info] target server0: server http://192.168.32.10/glpi
[info] sending prolog request to server0
[info] server0 answer shows it supports GLPI Agent protocol
[info] running task Inventory
[info] New inventory from user-Standard-PC-i440FX-PIIX-1996-2025-04-06-00-24-29 for server0
```

Vérification de l'inventaire sur le serveur GLPI dans 'Parc' -> 'Ordinateurs' :



Informations d'inventaire

| | | |
|-----------------------------------|------------------------|--------------------------------------|
| Agent | UserAgent | Tag d'inventaire |
| backupmanager-2025-04-06-15-12-45 | GLPI-Agent_v1.13-1 | |
| Adresse publique de contact | Dernier contact | Dernière mise à jour de l'inventaire |
| 192.168.32.5 | 2025-04-06 13:29 | 2025-04-06 13:29 |
| Statut de l'agent | Demander un inventaire | |
| Inconnu | Inconnu | |

Voici notre machine, on la reconnaît par son adresse ip : 192.168.32.5 et par le nom de l'agent "backupmanager-2025-04-06-15-12-45". L'inventaire a été effectué sans erreur !

11.4.3. Installation de l'agent GLPI sous Windows

Prérequis :

- Windows 10, 11 ou Server (2016+)
- Droits administrateurs pour l'installation
- Accès au serveur GLPI (HTTP ou HTTPS)
- Accès au service Windows pour démarrer/redémarrer l'agent
- Accès à l'interface agent via : <http://localhost:62354>

Téléchargement :

Télécharger l'agent depuis :

<https://github.com/glpi-project/glpi-agent/releases>

Voici le lien de la dernière version à télécharger :

Windows

| Arch | Windows installer | Windows portable archive |
|---------|---|---|
| 64 bits | GLPI-Agent-1.13-x64.msi | GLPI-Agent-1.13-x64.zip |

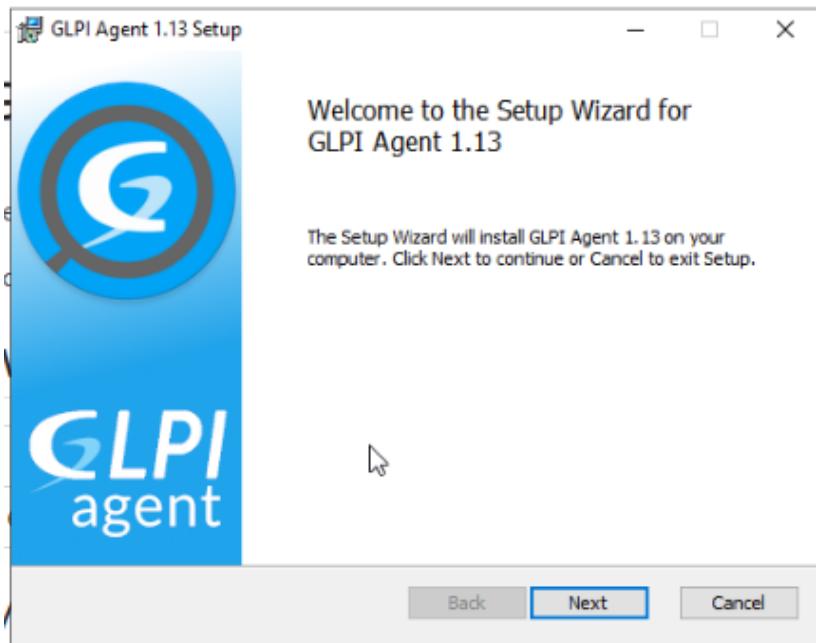


La nouvelle version est téléchargée :

Téléchargements

GLPI-Agent-1.13-x64.msi
[Ouvrir un fichier](#)

Exécuter le fichier .exe :



Installation :

Choisir installation complète

Indiquer l'URL du serveur GLPI :

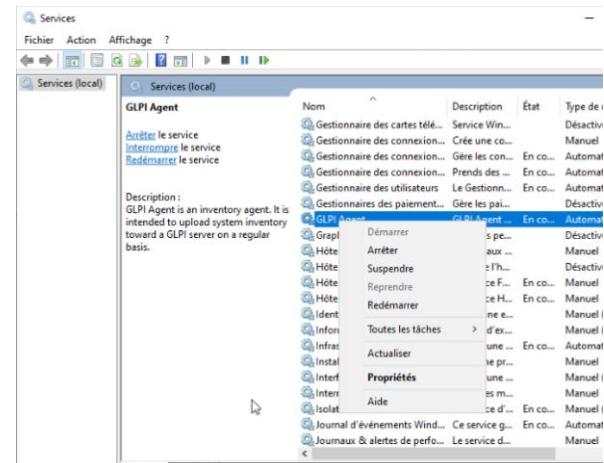
<http://192.168.32.10/glpi>

Activation de l'agent :

Ouvrir le menu Services

Rechercher GLPI Agent

Clic droit → Redémarrer



Interface Web de l'agent:

Ouvrir l'agent dans un navigateur à l'adresse : <http://127.0.0.1:62354> ou <http://localhost:62354>



This is GLPI Agent 1.13

The current status is waiting

[Force running all targets planned tasks](#)

Next server target execution planned for: [Force an inventory](#)

- server0: Sun Apr 6 18:23:44 2025

Planned tasks: Inventory, RemoteInventory

Cliquer sur **Force an inventory**

Vérification sur le serveur GLPI :

Accéder à GLPI → Parc → Ordinateurs

Le poste Windows apparaît après synchronisation.

| WIN-RT5CL9J39V9 | BOCHS_ | QEMU BXPC | Microsoft Windows Server 2022 Standard Evaluation | 2025-04-06 16:11 | QEMU Virtual CPU version 2.5+ |
|-------------------------------------|------------------------|--------------------------------------|---|------------------|-------------------------------|
| Agent | UserAgent | Tag d'inventaire | | | |
| WIN-RT5CL9J39V9-2025-04-06-18-08-42 | GLPI-Agent_v1.13 | | | | |
| Adresse publique de contact | Dernier contact | Dernière mise à jour de l'inventaire | | | |
| 192.168.32.7 | 2025-04-06 16:11 | 2025-04-06 16:11 | | | |
| Statut de l'agent | Demander un inventaire | | | | |
| Inconnu | Inconnu | | | | |



11.5. Fiche procédure - utilisateur

Accès GLPI :

<http://192.168.32.10>

Comptes disponibles :

- glpi / glpi
- tech / tech
- normal / normal

Créer un ticket :

1. Connexion avec son compte
2. Onglet **Assistance > Créer un ticket**
3. Renseigner le problème et valider

Suivre l'inventaire :

- Onglet **Parc > Ordinateurs**

11.6. Cahier de recettes

Fonctionnalités principales

- Server GLPI opérationnel.
- Client (AGENT) GLPI opérationnelles
- Gestion des agents.

Validation des Tests

- Tous les tests fonctionnels concernant la réception d'inventaire de l'agent.

11.7. Cahier de test

| Test | OK | Remarque |
|---|----|---|
| Accès à l'interface GLPI | OK | http://192.168.32.10/glpi |
| Connexion à la base de données | OK | |
| Ajout d'un ticket test | OK | Ticket appelé "Test" |
| Vérifier que l'agent est bien installé sur la machine Ubuntu | OK | |
| Forcer une remontée de l'inventaire vers GLPI sur la machine Ubuntu | OK | |
| S'assurer que l'agent est bien installé sur la machine Windows | OK | |
| S'assurer que le service tourne sur la machine Windows | OK | |
| Accéder à l'interface locale de l'agent | OK | http://localhost:62354 |
| S'assurer que l'agent sous Windows peut envoyer un inventaire | OK | |
| Confirmer que les postes (Linux & Windows) apparaissent | OK | |



12. Règles de filtrage (pfSense)

12.1. Cahier des charges

12.1.1. Contexte et Objectifs

Contexte

L'entreprise, spécialisée dans des services numériques, utilise un pare-feu pfSense pour sécuriser son réseau interne. Le réseau comprend deux segments principaux :

- **LAN1 (192.168.31.254/24)** : utilisé par les employés pour les postes de travail.
- **LAN2 (192.168.32.254/24)** : dédié à l'infrastructure interne et aux services comme les serveurs locaux. L'interface WAN est connectée à Internet et assure l'accès externe pour les utilisateurs et les services.

Objectif

1. **Diagnostic réseau fiable** : Permettre aux utilisateurs des réseaux internes de vérifier la connectivité vers l'extérieur à l'aide de requêtes ICMP (ping).
2. **Renforcement de la sécurité** : Interdire l'accès à l'interface Web d'administration de pfSense depuis l'extérieur (interface WAN), afin de protéger contre les intrusions non autorisées.
3. **Optimisation des ressources réseau** : Limiter la bande passante pour un utilisateur ou un périphérique spécifique afin d'assurer une répartition équitable des ressources réseau.

Ces objectifs visent à améliorer la sécurité et l'efficacité du réseau tout en offrant un outil de diagnostic de base aux utilisateurs internes.

12.1.2. Descriptions fonctionnelles des besoins

Besoin 1 : Les utilisateurs des réseaux LAN1 et LAN2 doivent pouvoir tester la connectivité Internet en utilisant des pings.

Besoin 2 : Aucun utilisateur externe (hors réseaux LAN1 et LAN2) ne doit avoir accès à l'interface Web d'administration (généralement sur le port TCP/HTTPS 443).

Besoin 3 : Définir une règle de QoS pour restreindre la bande passante attribuée à un utilisateur ou à un périphérique donné (par exemple, basé sur l'adresse IP ou MAC).

12.1.3. Cahier des charges technique

Infrastructure actuelle :

- Interface WAN connectée à Internet.
- LAN1 : Adresse IP 192.168.31.254/24.
- LAN2 : Adresse IP 192.168.32.254/24.

**Configurations à mettre en place :**

1. Ajouter une règle de pare-feu pour autoriser le protocole ICMP (type "echo request" et "reply") vers l'extérieur.
2. Ajouter une règle pour bloquer tout accès à l'interface Web de pfSense depuis l'interface WAN.
3. Configurer une file d'attente ou une limitation de bande passante (par exemple via le Limiteur de pfSense ou une file HFSC).

Outils nécessaires :

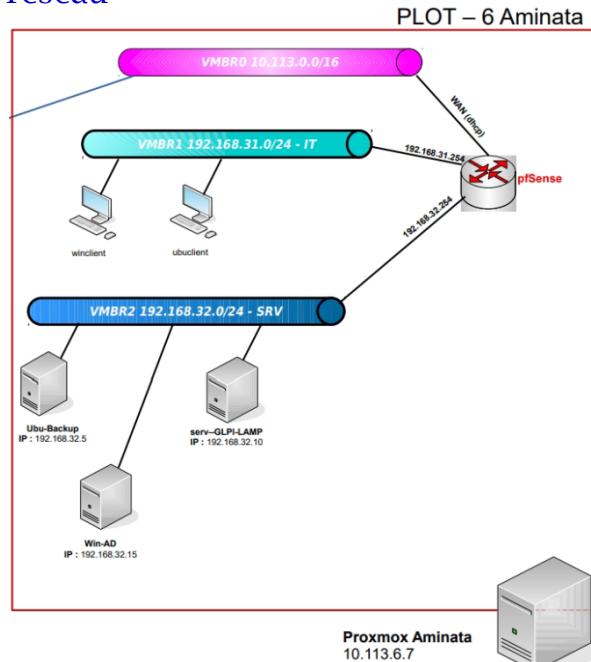
- Accès administrateur à pfSense.
- Connaissances sur la configuration des règles de pare-feu et des files QoS sur pfSense.

12.1.4. Planning prévisionnel

| Tâche | Durée |
|---|--------|
| Analyse des besoins et validation des prérequis | 1 jour |
| Configuration des règles de pare-feu | 1 jour |
| Test de connectivité et validation des règles | 1 jour |
| Mise en production et documentation | 1 jour |

12.2. Plan d'adressage

| @réseau | @passerelle | NIC | Machine/rôle | DHCP ? |
|-----------------|--------------------|--------------|---|---------------------------------------|
| 10.113.6.0/16 | 10.113.6.12 | VMBR0 | WAN accès vers l'extérieur | Pas de config DHCP |
| 192.168.31.0/24 | 192.168.31.254 | VMBR1 IT | Machine cliente | DHCP 192.168.31.1 à 192.168.31.253 |
| 192.168.32.0/24 | 192.168.32.254 | VMBR2 SRV | Ubu-Backup : 192.168.32.5 Serv-GLPI-LAMP : 192.168.32.10 Win-AD : 192.168.32.15 | DHCP 192.168.32.1 à 192.168.32.253 |

12.3. Schéma réseau



12.4. Documentation technique

Prérequis

- Machine pfSense
- Machine cliente (VMBR0)
- Machine cliente Windows connecté à l'interface 192.168.31.254 (VMBR1)
- Machine cliente Ubuntu connecté à l'interface 192.168.32.254 (VMBR2)

12.4.1. Activer le NAT

1. Accéder à l'interface Web de pfSense

- Connectez-vous à l'interface Web via l'adresse IP de l'interface LAN (par exemple : <https://192.168.31.254>).

2. Configurer le NAT

1. Naviguer vers les paramètres NAT :

- Allez dans Firewall > NAT.
- Vous verrez plusieurs onglets, tels que Port Forward, 1:1, et Outbound.

2. Configurer le NAT sortant (Outbound NAT) :

- Cliquez sur l'onglet Outbound.
- Sélectionnez le mode Manual Outbound NAT pour avoir un contrôle total sur les règles.
- Cliquez sur Save et ensuite sur Apply Changes.

3. Créer une règle NAT :

- Cliquez sur Add pour ajouter une nouvelle règle.
- Configurez les paramètres comme suit :
 - Interface : WAN (car le NAT est utilisé pour le trafic sortant vers Internet).
 - Source : Sélectionnez le réseau local LAN.
 - Destination : any (pour autoriser le trafic vers n'importe quelle adresse externe).
 - Translation : Laissez l'option par défaut pour utiliser l'adresse IP WAN comme adresse source.

4. Sauvegarder et appliquer les modifications :

- Cliquez sur Save pour enregistrer la règle.
- Cliquez sur Apply Changes pour appliquer les modifications.

3. Tester la configuration



- Depuis un poste connecté au réseau local (LAN1 ou LAN2), essayez d'accéder à Internet ou d'effectuer un ping vers une adresse externe (exemple : 8.8.8.8).
- Vérifiez que le trafic est correctement traduit et que la connectivité fonctionne.

12.4.2. Autoriser le ping vers le WAN

Accéder à l'interface Web de pfSense :

- Connectez-vous à l'interface Web de pfSense via l'adresse IP de l'interface LAN (exemple : <https://192.168.31.254>).

Naviguer vers les règles de pare-feu :

- Allez dans le menu **Firewall > Rules**.
- Sélectionnez l'onglet correspondant à l'interface LAN.

Créer une nouvelle règle :

- Cliquez sur le bouton **Add** pour ajouter une nouvelle règle.
- Configurez les paramètres suivants :
 - Action** : Pass (autoriser le trafic).
 - Interface** : Sélectionnez l'interface LAN1 ou LAN2.
 - Protocol** : ICMP (protocole utilisé pour les pings).
 - Source** : LAN subnet (pour autoriser les pings depuis le réseau local).
 - Destination** : any (pour autoriser les pings vers n'importe quelle adresse externe).
- Ajoutez une description (exemple : "Autoriser les pings vers l'extérieur").

Sauvegarder et appliquer les modifications :

- Cliquez sur **Save** pour enregistrer la règle.
- Cliquez sur **Apply Changes** pour appliquer les modifications.

| Rules (Drag to Change Order) | | | | | | | | | | | Actions |
|-------------------------------------|------------|-----------|-------------|------|-------------|------|---------|-------|----------|--------------------------------------|---------|
| | States | Protocol | Source | Port | Destination | Port | Gateway | Queue | Schedule | Description | Actions |
| <input checked="" type="checkbox"/> | 1/751 KiB | * | * | * | LAN Address | 80 | * | * | | Anti-Lockout Rule | |
| <input type="checkbox"/> | 0/0 B | IPv4 ICMP | LAN subnets | * | * | * | * | none | | Autoriser les pings vers l'extérieur | |
| <input checked="" type="checkbox"/> | 9/1.73 GiB | IPv4 * | LAN subnets | * | * | * | * | none | | Default allow LAN to any rule | |
| <input checked="" type="checkbox"/> | 0/0 B | IPv6 * | LAN subnets | * | * | * | * | none | | Default allow LAN IPv6 to any rule | |

Tester la configuration :

- Depuis un poste connecté à LAN, exécutez une commande ping vers une adresse externe (exemple : ping 8.8.8.8).



- Vérifiez que les pings reçoivent une réponse.

```
user@user-Standard-PC-i440FX-PIIX-1996:~$ 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=3.88 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=114 time=4.38 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=114 time=3.99 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=114 time=3.67 ms
^C
... 8.8.8.8 ping statistics ...
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 3.674/3.980/4.382/0.257 ms
user@user-Standard-PC-i440FX-PIIX-1996:~$
```

12.4.3. Bloquer l'accès à l'interface Web de pfSense depuis Internet

1. Accéder à l'interface Web de pfSense

- Connectez-vous à l'interface Web via l'adresse IP de l'interface LAN (par exemple : <https://192.168.31.254>).

2. Naviguer vers les règles de pare-feu

- Allez dans **Firewall > Rules**.
- Sélectionnez l'onglet **WAN** (car l'accès indésirable proviendrait de l'extérieur via cette interface).

3. Ajouter une nouvelle règle pour bloquer l'accès

- Cliquez sur **Add** pour ajouter une règle.
- Configurez les paramètres comme suit :
 - **Action** : Block (bloquer le trafic).
 - **Interface** : WAN.
 - **Protocol** : TCP (puisque l'interface Web utilise HTTPS, qui fonctionne avec TCP).
 - **Source** : any (pour bloquer tout accès provenant de l'extérieur).
 - **Destination** :
 - **Address** : Sélectionnez l'adresse WAN de pfSense (souvent This Firewall (self)).
 - **Port** : Spécifiez le port utilisé par l'interface Web (par défaut : HTTPS sur le port 443).
- Ajoutez une description, par exemple : "Bloquer l'accès à l'interface Web depuis WAN".

4. Sauvegarder et appliquer les changements

- Cliquez sur **Save** pour enregistrer la règle.

- Cliquez sur **Apply Changes** pour la rendre effective.

| Rules (Drag to Change Order) | | | | | | | | | | | |
|-------------------------------------|-------------|----------|-------------------------------------|------|----------------|------|---------|-------|----------|--|---|
| | States | Protocol | Source | Port | Destination | Port | Gateway | Queue | Schedule | Description | Actions |
| <input checked="" type="checkbox"/> | 0/20.40 MiB | * | RFC 1918 networks | * | * | * | * | * | | Block private networks |  |
| <input checked="" type="checkbox"/> | 0/17.94 MiB | * | Reserved Not assigned by IANA | * | * | * | * | * | | Block bogon networks |  |
| <input checked="" type="checkbox"/> | 0/0 B | IPv4 | * | * | 192.168.31.254 | * | * | none | | Bloquer l'accès à l'interface web depuis WAN |      |

5. Vérification

- Testez depuis un appareil extérieur (connecté à VMBR0) en essayant d'accéder à l'adresse IP publique de l'interface WAN via HTTPS.
 - L'accès doit être bloqué.

12.4.4.Limiter la bande passante d'un client

1. Accéder à l'interface Web de pfSense

- Connectez-vous à l'interface Web via l'adresse IP de l'interface LAN (par exemple : <https://192.168.31.254>).

2. Configurer un Limiteur de bande passante

1. Allez dans **Firewall > Traffic Shaper > Limiter**.
 2. Cliquez sur **Add** pour créer un nouveau limiteur.
 3. Configurez les paramètres pour la limite de téléchargement (**Download**):
 - o **Name** : Donnez un nom au limiteur (exemple : "Download_Limiter").
 - o **Bandwidth** : Spécifiez la bande passante à appliquer (par exemple : 1 Mbps).
 - o **Queue Length** : Laissez la valeur par défaut (exemple : 50).
 - o Cliquez sur **Save**.
 4. Répétez la même opération pour la limite d'upload (**Upload**):
 - o **Name** : Donnez un nom au limiteur (exemple : "Upload_Limiter").
 - o **Bandwidth** : Spécifiez la bande passante (par exemple : 512 Kbps).
 - o **Queue Length** : Laissez par défaut (exemple : 50).
 - o Cliquez sur **Save**.

3. Associer le Limiteur à une règle de pare-feu

1. Allez dans **Firewall > Rules**.
 2. Accédez à l'onglet correspondant à l'interface du client (par exemple, OPT1).
 3. Cliquez sur **Add** pour créer une règle.



4. Configurez les paramètres comme suit :

- **Action** : Pass.
- **Interface** : OPT1
- **Protocol** : any (tous les protocoles).
- **Source** : Adresse IP ou MAC du client cible (par exemple : 192.168.32.10).
- **Destination** : any (pour appliquer la limite à tout le trafic).
- **In/Out** :
 - **In** : Associez le limiteur de téléchargement créé ("Download_Limiter").
 - **Out** : Associez le limiteur d'upload ("Upload_Limiter").

5. Ajoutez une description (exemple : "Limiter la bande passante du client 192.168.32.10").

6. Cliquez sur **Save** et ensuite sur **Apply Changes**.

4. Vérification

- Depuis le client cible, effectuez un test de bande passante (par exemple via speedtest.net ou en téléchargeant un fichier).

1. Ouvrez un terminal sur votre machine Ubuntu.

2. Installez speedtest-cli (si non installé) :

```
sudo apt update
```

```
sudo apt install speedtest-cli
```

3. Exécutez un test de bande passante :

```
speedtest
```

- **Résultat attendu** : Si la règle pfSense est correctement configurée, les vitesses mesurées (téléchargement et upload) doivent être limitées à ce qui est défini dans pfSense.

2. Tester en téléchargeant un fichier avec wget

Vous pouvez également télécharger un fichier depuis Internet et observer la vitesse.



Commande wget :

1. Téléchargez un fichier exemple :

```
wget http://speedtest.tele2.net/1MB.zip
```

2. Pendant le téléchargement, la vitesse sera affichée dans le terminal.

- o **Résultat attendu :** La vitesse doit respecter la limitation de bande passante configurée dans pfSense.

```
user@serv-GLPI-LAMP: ~ wget http://speedtest.tele2.net/1MB.zip
--2025-04-07 23:08:56-- http://speedtest.tele2.net/1MB.zip
Résolution de speedtest.tele2.net (speedtest.tele2.net)... 90.130.70.73, 2a00:800:1010::1
Connexion à speedtest.tele2.net (speedtest.tele2.net)|90.130.70.73|:80... connecté.
requête HTTP transmise, en attente de la réponse... 200 OK
Taille : 1048576 (1,0M) [application/zip]
Enregistre : '1MB.zip'

1MB.zip          100%[=====] 1,00M 76,9KB/s  ds 17s

2025-04-07 23:09:13 (60,4 KB/s) - '1MB.zip' enregistré [1048576/1048576]
```

12.5. Cahier de recettes

Tests prévus :

1. Vérification que les pings sortants fonctionnent depuis LAN1 et LAN2.
2. Vérification qu'il est impossible d'accéder à l'interface Web depuis l'interface WAN.
3. Vérification que la bande passante du client cible est bien limitée.

Critères de validation :

- Ping externe réussi.
- Blocage effectif de l'accès externe à l'interface Web.
- Bande passante respectant les limites configurées.

12.6. Cahier de test

| Test | OK | Remarque |
|--|----|---|
| Les pings vers des adresses externes fonctionnent | Ok | Tests effectués depuis LAN1 et LAN2. |
| L'accès à l'interface Web de pfSense depuis Internet est bloqué | Ok | Interface inaccessible depuis WAN. |
| Limitation de la bande passante pour un client est fonctionnelle | Ok | Bandes passante limitée selon les paramètres. |
| Toutes les règles coexistantes fonctionnent sans conflit | Ok | Tests d'interaction entre les règles réussis. |