



SECS1026

Projet de Stage CCNB

Rapport De Fiches Techniques OpenNMS + Grafana

Intervenants : Maryssa LeBlanc, Daren Thibodeau, Agnes Sanama et Mathis Cayouette

Chargés de projet : Anthony Roy, Meriem Oultache et Christian Kalla

Client : Denis Landry

Date : Juin le 6, 2025

Contents

Introduction.....	9
TRITRE I : Introduction à OpenNMS / Grafana	10
SOUS SECTION 1 : OpenNMS	10
A- Fonctionnalités principales d'OpenNMS.....	10
.....	12
B- Intégration avec Grafana via le plugin Helm.....	12
C- Exemples de visualisations.....	12
D- Ressources supplémentaires	13
SOUS SECTION 2 : Grafana	13
A-Qu'est-ce que Grafana ?	13
.....	14
B-Fonctionnalités clés de Grafana	14
.....	15
C-Exemples de visualisations Grafana	15
D-Installation de Grafana :.....	15
E-Ressources utiles.....	16
TITRE 2 : GUIDE D'INSTALLATION DE NOTRE ENVIRONNEMENT SUR PROXMOX.....	17
SOUS TITRE 1 : pfSense	17
SOUS TITRE 2 : INSTALLATION DE UBUNTU	22
Étape 1 : Télécharger l'ISO d'Ubuntu Server	22
Étape 2 : Télécharger l'ISO sur Proxmox.....	22
Étape 3 : Créer une nouvelle machine virtuelle (VM)	23
Étape 4 : Sélectionner l'ISO et configurer le système d'exploitation	23
Étape 6 : Configurer le CPU et la mémoire.....	23
Étape 7 : Réseau et options de démarrage.....	23
Étape 8 : Démarrer la VM et lancer l'installation d'Ubuntu	24
Étape 9 : Options initiales d'installation	24
Étape 10 : Configurer les paramètres réseau (optionnel – IP statique).....	24
Étape 11 : Poursuivre l'installation	25
Étape 12: Définir les identifiants utilisateur	25
Étape 13: Activer SSH.....	25
Étape 14 : Télécharger PuTTY pour l'accès SSH.....	25

Étape 15 : Terminer l'installation et redémarrer	26
Étape 16 : Tester l'accès SSH	26
Sous Titre 3 : INSTALLATION DE WINDOWS	27
Prérequis pour l'installation.....	27
A-Création de la VM Windows.....	27
B- Installation de Windows serveur	31
Sous-titre 3 : Sécurisation des accès administratifs a grafana	34
Etape 1 : Changer le mot de passe administrateur par defaut.....	34
Etape 2 : Creer des utilisateurs avec roles restreints	34
Etape 3 : Restreindre l'accès reseau a Grafana (port 3000).....	34
Etape 4 : Activer le HTTPS	34
Etape 5 : Activer la journalisation des accès	35
Etape 6 : Mise a jour reguliere de Grafana.....	35
Sous Titre 4 : comment installer la solution de surveillance OpenNMS sur Ubuntu22.04	36
A-Conditions préalables.....	36
B-Installation de Java OpenJDK.....	37
Installation et configuration de PostgreSQL Server	38
C-Installing and Configuring OpenNMS.....	39
D-Installation de Nginx en tant que proxy inverse pour OpenNMS	43
E- Configuration du pare-feu UFW	45
E-Accès à l'outil de surveillance OpenNMS	48
TRITRE 3 : INVENTAIRE DES CAPTEURS	50
Sous Titre 1 : Inventaire des capteurs	50
A-Inventaire des capteurs PRTG en production	51
B-Détails des capteurs	52
C-Processus d'alerte	53
Sous Titre 2: Méthodologie détaillée pour l'inventaire, la classification et le regroupement des capteurs pour préparer une migration vers OpenNMS	55
Étape 1: Recenser tous les capteurs existants.....	55
Étape 2: Classifier les capteurs par technologie	56
Étape 3: Regrouper par cible/équipement	57
Étape 4: Analyse et nettoyage	58
Étape 5: Priorisation pour la migration.....	58

Étape 6: Documentation finale	59
Conseils pratiques pour la réussite du projet.....	60
SOUS TITRE 3 : correspondance : PRTG → OpenNMS.....	61
1. Objectif.....	61
2. Tableau de correspondance : PRTG → OpenNMS.....	61
3- Capteurs courants dans PRTG mais pas en natif dans OpenNMS	64
4. Méthodologie de migration	65
5. Livrable final.....	66
5. Remarques Supplémentaires	67
TITRE 5 : configuration des nodes et services dans OpenNMS	68
SOUS TITRE 1 : Guide Technique : Configuration d'OpenNMS	68
1. Ajouter les hôtes	68
2. Configurer les services supervisés (ping, SNMP, etc.)	69
3. Ajouter des nœuds ("Nodes ajouté").....	70
4. Documenter la correspondance entre capteurs PRTG et OpenNMS.....	70
5. Configuration des permissions	71
6. Configuration des alertes.....	72
TITRE 5 : MISE EN PLACE DES ALERTES ET DES NOTIFICATIONS	73
SOUS TITRE 1 : Configuration pas-à-pas des alertes dans OpenNMS Horizon	73
1. Préambule : Comprendre les composants d'alerte	73
2. Configuration des seuils (thresholds)	73
3. Association des seuils aux ressources	74
4. Création de notifications	74
5. Tests et validation.....	75
6. Intégration Grafana.....	75
7. Bonnes pratiques	75
SOUS TITRE 2 : Implémentation de la notification automatique dans Grafana pour OpenNMS ...	76
1. Contexte et besoins.....	76
2. Architecture de la solution proposée.....	76
3. Étapes d'implémentation	77
4. Exemple d'implémentation pratique	78
5. Bonnes pratiques	78
6. Conclusion	78

TITRE 5 : Création structurée des utilisateurs dans Windows Server 2019 avec Active Directory et bonnes pratiques	80
SOUS TITRE 1 : Windows server 2019	80
Objectif	80
1. Installer Active Directory Domain Services (AD DS).....	80
2. Promouvoir le serveur en contrôleur de domaine	80
3. Plan de création des Unités d'Organisation (OU)	81
4. Créer les OU	81
5. Création des comptes utilisateurs AD	81
6. Appliquer une politique de mot de passe via GPO	82
6. Documentation des utilisateurs créés	82
SOUS TITRE 2 : Bonnes pratiques de sécurité Active Directory et supervision Windows (Projet OpenNMS/Grafana)	83
Objectif	83
1. Politique de verrouillage de compte (protection contre force brute)	83
2. Restriction des connexions RDP (Bureau à distance)	83
3. Activation de l'audit des connexions et accès (journalisation)	84
4. Configuration de WinRM pour la supervision OpenNMS	84
5. Création d'un compte technique pour la supervision	85
6. Bonnes pratiques complémentaires	85
TITRE 6 : Configuration Avancée des Capteurs et des tableaux de bords dans OpenNMS/Grafana .	86
SOUS TITRE 1 : Configuration des capteurs.....	86
Étape 1 : Ajouter les hôtes à superviser	86
Étape 2 : Activer les capteurs ICMP, SNMP, HTTP, SSH, etc.	87
Étape 3 : Configurer les seuils de disponibilité, alertes et SLA	90
Conclusion	93
SOUS TITRE 2 : Crédit :ation des Tableaux de Bords dans Grafana	94
1. Qu'est-ce que Grafana ?	94
2. Fonctionnement général.....	94
3. Tableaux de Bord : Définition et Structure	94
4. Crédit :ation d'un Tableau de Bord	95
7. Types de Tableaux de Bords	95
6. Cas d'usage typiques	96
7. Alertes et Notifications	97

8. Bonnes pratiques	97
SOUS titre 3 : Présentation des différents types de dashboards OpenNMS et leurs fonctionnalités	98
1.....	98
2. APC UPS Stats.....	98
3. OpenNMS Network Interfaces Report.....	99
4. OpenNMS World Map Example	99
5. OpenNMS Outage Dashboard	100
5. OpenNMS Outage Wallboard	100
7. OpenNMS ActiveMQ.....	100
8. OpenNMS JVM Metrics	101
TITRE 7 : Plan de Sécurisation du Serveur – OpenNMS + Grafana.....	103
SOUS TITRE 2 : Sécurisation du Serveur – OpenNMS + Grafana.....	103
2. Sécurisation Initiale Mise en Place	103
3. Recommandations Complémentaires	104
3.1 Mise à jour Automatisée du Système	104
3.2 Désactivation des Services Inutiles	104
3.3 Renforcement de SSH	104
3.4 Intégrité et Audit	105
3.5 Gestion des Droits et Permissions.....	105
3.6 Sécurisation HTTPS des Interfaces Web	105
3.7 Sauvegarde et Restauration	105
3.8 Contrôle des Ports Réseau.....	105
3.9 Supervision de l'Intégrité des Fichiers	105
3.10 Journalisation Centralisée.....	106
SOUS TITRE 2 : PLAN DE VÉRIFICATION STRUCTURÉ	110
Étape 1 : Vérifier la supervision des services (ICMP, HTTP,	110
SSH, SNMP...)	110
Étape 2 : Vérifier la collecte SNMP sur les équipements WiFi (AP)	110
Étape 3 : Vérifier la collecte de métriques (RRA/RRD).....	111
Étape 4 : Vérifier l'activation du module OpenNMS-Flow (Top Talkers)	111
Étape 5 : Vérifier que l'API REST est accessible à Grafana Helm.....	112
Terminal depuis la VM Grafana :.....	112

Étape 6 : (Optionnel) Activer la réception de SNMP Traps	112
Conclusion	114
Sources et références	115

Liste des tableaux

Table 1: Inventaire des capteurs.....	52
Table 2: Correspondance PRTG-OpenNMS.....	64
Table 3: capteurs courant dans PRTG mais pas natif dans OpenNMS	65
Table 4: Livrable final des capteurs configures.....	66
Table 5: Unite d'organisation.....	81
Table 6: Utilisateurs créés	82
Table 7: Checklist des tests	113

Liste des figures

Figure 1: Introduction guide d'installation pfsense sur proxmox.....	17
Figure 2: preparation et prerquis de l'installation de pfSense sur proxmox	18
Figure 3; configuration reseau initiale de pfSense	18
Figure 4: préparation de l'environnement proxmox début	19
Figure 5: préparation de l' environnement proxmox fin	19
Figure 6: creation d'une VM pfSense	19
Figure 7: installation de pfSense	20
Figure 8: configuration des interfaces reseau	20
Figure 9: configuration web de pfSense	21
Figure 10Installation de l'agent invite QEMU	21
Figure 11: Finalisation et verification de l'installation de pfSense	22
Figure 12: creation d'une VM windows	27
Figure 13: Ajout de l'iso dans la VM windows	28
Figure 14: Ajout de l'agent QEMU dans la VM windows.....	28
Figure 15: choisir l'espace de stockage	29
Figure 16: Choisir les parametre du CPU	29
Figure 17: choisir la RAM	30
Figure 18: choisir les parametre reseau de la machine.....	30
Figure 19: Ajout de l'ISO sur la VM Windows	31
Figure 20: verification des configuration final sur la VM windows.....	31
Figure 21: personalisation de windows serveur.....	32
Figure 22; choix du disque pour l'installation	32
Figure 23: choix de l'emplacement.....	32
Figure 24: windows setu	33
Figure 25: choisir une version windows	33
Figure 26: Ajout des credentiels	33
Figure 27: Ouverture du port TCP/UDP sur le pare feu	46
Figure 28: ports autorises sur le pare feu	47
Figure 29: Interface OpenNMS	48
Figure 30: Interface de configuration OPenNMS.....	49
Figure 31: modification deu mot de passe OpenNMS.....	49
Figure 32: exemple de tableau de bord	98
Figure 33: APC UPS Stats.....	99

Introduction

Ce rapport présente la démarche technique et méthodologique suivie dans le cadre du projet de remplacement de la solution PRTG par une plateforme de supervision open source. Le projet, réalisé au sein du CCNB, vise à renforcer la surveillance des infrastructures TIC, en assurant la disponibilité, la performance et la fiabilité des services critiques.

L'objectif principal est de migrer vers une solution robuste, évolutive et libre de droits, permettant la supervision de plus de 1 000 capteurs répartis sur différents services (Wi-Fi, WAN, VPN, pare-feux, serveurs, etc.). Le rapport détaille les choix technologiques effectués, les étapes d'installation, de configuration, d'intégration, ainsi que les tableaux de bord mis en place via Grafana pour faciliter la visualisation des données en temps réel.

TRITRE I : Introduction à OpenNMS / Grafana

SOUS SECTION 1 : OpenNMS

OpenNMS est une plateforme open source de supervision réseau conçue pour surveiller, visualiser et gérer des infrastructures informatiques complexes. Elle offre des fonctionnalités complètes pour la détection des pannes, la collecte de performances, la gestion des événements et des alarmes, ainsi que l'intégration avec des outils tiers comme Grafana.

A- Fonctionnalités principales d'OpenNMS

1. Gestion des événements et des alarmes

- OpenNMS utilise une architecture basée sur un bus de messages "publish and subscribe" pour gérer les événements.
- Il peut recevoir des événements sous forme de traps SNMP, messages syslog, événements TL/1 ou messages XML personnalisés.
- Les événements peuvent être configurés pour générer des alarmes, permettant une corrélation des événements et une réduction des alarmes redondantes.
- Les notifications peuvent être envoyées par e-mail, SMS, XMPP ou méthodes personnalisées.

2. Découverte et provisionnement

- OpenNMS dispose d'un système de provisionnement avancé permettant l'ajout automatique ou manuel de dispositifs à surveiller.
- La configuration peut être effectuée via l'interface web ou par des fichiers XML, facilitant l'automatisation.

- Le système est capable de gérer des réseaux de plus de 50 000 dispositifs distincts.

3. Supervision des services

- OpenNMS permet de surveiller la disponibilité des services réseau, allant des simples pings ICMP aux vérifications complexes comme la surveillance de séquences de pages ou le transport de courrier.
- Les informations sur les pannes sont stockées dans la base de données et peuvent être utilisées pour générer des rapports de disponibilité.
- Des sondeurs distants peuvent être déployés pour mesurer la disponibilité depuis des emplacements éloignés.

4. Collecte de données

- OpenNMS collecte des données de performance pour divers protocoles réseau, notamment SNMP, HTTP, JMX, WMI, XMP, XML, NSClient et JDBC.
- Les données peuvent être stockées, représentées graphiquement et vérifiées par rapport à des seuils définis.
- Le système est hautement évolutif, capable de collecter 1,2 million de points de données via SNMP toutes les cinq minutes.

5. Visualisation des données

- OpenNMS propose plusieurs outils pour visualiser les données collectées :
 - Tableaux de bord : Vue d'ensemble des performances et de l'état du réseau.
 - Vue de surveillance : Affichage des services surveillés et de leur statut.
 - Cartes thermiques : Représentation visuelle des zones problématiques.
 - Pages de tendances : Analyse des performances sur des périodes définies.

B- Intégration avec Grafana via le plugin Helm

OpenNMS peut être intégré à Grafana à l'aide du plugin Helm, permettant une visualisation avancée des données collectées :

- Création de tableaux de bord personnalisés affichant les métriques de performance, les alarmes et les tendances.
- Utilisation de filtres pour prévoir les métriques et créer des tableaux de bord dynamiques.
- Affichage de graphiques de ressources, de journaux et d'histogrammes d'alarmes.

Cette intégration facilite la surveillance en temps réel et l'analyse des performances du réseau.

C- Exemples de visualisations

Voici quelques exemples de visualisations disponibles avec OpenNMS et son intégration avec Grafana :

1. Tableau de bord principal : Affiche l'état général du réseau, les alarmes actives et les performances des services.
2. Graphiques de performance : Représentation graphique des métriques telles que l'utilisation du CPU, la mémoire, le trafic réseau, etc.
3. Cartes thermiques : Visualisation des zones du réseau avec des problèmes ou des performances dégradées.
4. Vue de surveillance : Affichage des services surveillés avec leur statut (actif, en panne, en maintenance).
5. Tableaux de bord Grafana : Intégration des données OpenNMS dans Grafana pour une visualisation avancée et personnalisée.

D- Ressources supplémentaires

- Documentation officielle OpenNMS : <https://docs.opennms.com/>
- Plugin OpenNMS pour Grafana : <https://docs.opennms.com/grafana-plugin/>
- Dépôt GitHub OpenNMS : <https://github.com/OpenNMS/opennms>

SOUS SECTION 2 : Grafana

Grafana est une plateforme open-source de visualisation et d'observabilité permettant de surveiller, analyser et présenter des métriques issues de diverses sources de données. Elle est principalement utilisée pour le monitoring des infrastructures IT, des applications, des performances réseau, et bien plus encore.

A-Qu'est-ce que Grafana ?

Définition : Grafana est une plateforme de monitoring et d'analyse de données qui permet de créer des **tableaux de bord dynamiques** en se connectant à plusieurs sources de données telles que **Prometheus, OpenNMS, InfluxDB, MySQL, Elasticsearch, PostgreSQL, AWS CloudWatch**, etc.

Objectif : Offrir une interface centralisée et personnalisable pour visualiser des métriques en temps réel et faciliter la prise de décision grâce à des graphiques détaillés.

Cas d'usage :

- Supervision des infrastructures informatiques (serveurs, réseaux, bases de données).
- Monitoring des applications et performances des microservices.
- Suivi des indicateurs clés en cybersécurité.
- Observabilité des logs et métriques des systèmes distribués.
- Surveillance des environnements IoT et industriels.

B-Fonctionnalités clés de Grafana

1. Tableaux de bord interactifs

- Interface intuitive et personnalisable.
- Graphiques dynamiques avec zoom et filtrage avancé.
- Possibilité d'ajouter des alertes visuelles.

2. Connexion à diverses sources de données

Grafana supporte plus de **50** types de bases de données et solutions de monitoring :

- **Bases de données SQL et NoSQL** : MySQL, PostgreSQL, InfluxDB.
- **Monitoring IT et Cloud** : Prometheus, OpenNMS, AWS CloudWatch.
- **Analyse des logs** : Elasticsearch, Loki.

3. Système d'alertes avancé

- Configuration de seuils d'alerte avec notifications.
- Envoi d'alertes via e-mail, Slack, Teams, Discord, webhook.
- Intégration avec des outils DevOps comme PagerDuty, Opsgenie.

4. Intégration avec OpenNMS (via Helm)

- Affichage des données de monitoring réseau en temps réel.
- Analyse des métriques de disponibilité et de performance.
- Correlation des événements et des logs.

5. Partage et collaboration

- Export des tableaux de bord en JSON.
- Partage de visualisations via des URLs publiques ou privées.
- Intégration avec des pages Web (ex. WordPress) via iframe.

C-Exemples de visualisations Grafana

1. Tableau de bord général (Infrastructure IT)

- ◆ Affiche l'état des serveurs, la consommation CPU, la mémoire et l'utilisation du réseau.

2. Monitoring des performances réseau

- ◆ Visualisation des latences, des pertes de paquets et du trafic.

3. Surveillance d'une application web

- ◆ Affichage du nombre de requêtes par seconde, des erreurs HTTP 500 et du temps de réponse.

4. Suivi des logs avec Loki

- ◆ Grafana s'intègre à **Loki** pour analyser les journaux système.

Installation de Grafana (Ubuntu/Debian)

Ajout du dépôt officiel :

- sudo apt install -y software-properties-common
- sudo add-apt-repository "deb https://packages.grafana.com/oss/deb stable main"
- wget -q -O - https://packages.grafana.com/gpg.key | sudo apt-key add -

D-Installation de Grafana :

- sudo apt update
- sudo apt install -y grafana

Démarrage du service :

- sudo systemctl enable --now grafana-server
- 💡 Interface Web : http://<IP_SERVEUR>:3000 (login : admin/admin)

Intégration avec OpenNMS et Helm

Pour connecter OpenNMS à Grafana :

1. Installer le plugin **Helm** depuis Grafana (Configuration > Plugins > OpenNMS Helm).
2. Ajouter OpenNMS comme **source de données**.
3. Configurer les métriques à afficher (latence, uptime, alertes).

E-Ressources utiles

- **Documentation officielle Grafana** : <https://grafana.com/docs/>
- **Tutoriel vidéo Grafana** : <https://www.youtube.com/watch?v=wHGDy6Ht4pA>
- **Dashboard Grafana pour OpenNMS** : <https://grafana.com/grafana/dashboards/>

TITRE 2 : GUIDE D'INSTALLATION DE NOTRE ENVIRONNEMENT SUR PROXMOX

SOUS TITRE 1 : pfSense

**Guide
d'Installation de
pfSense sur
Proxmox**

Bienvenue dans ce guide complet pour installer pfSense en tant que machine virtuelle sur Proxmox. Ce tutoriel vous guidera à travers toutes les étapes nécessaires, des prérequis jusqu'à la configuration finale de votre pare-feu pfSense.

Nous aborderons l'installation de base, la configuration des interfaces réseau, et la mise en place des fonctionnalités essentielles pour assurer une protection optimale de votre réseau. Suivez ces instructions pas à pas pour créer une solution de pare-feu robuste et personnalisée.

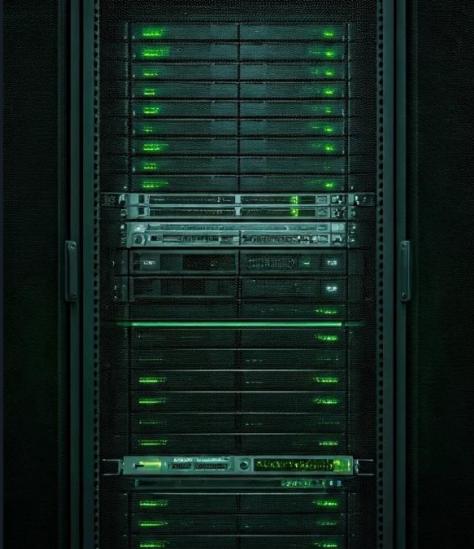


Figure 1: Introduction guide d'installation pfSense sur proxmox

Préparation et Prérequis

 Système Proxmox Assurez-vous que votre système dispose de Proxmox installé avec au moins deux ports réseau pour séparer le trafic WAN et LAN.	 Téléchargement de l'ISO Téléchargez l'ISO de pfSense depuis le site officiel : https://www.pfsense.org/download/ .	 Informations de connexion Ayez les détails de connexion de votre FAI (par exemple, identifiants PPPoE si nécessaires) à portée de main.
---	--	---

Figure 2: préparation et prérequis de l'installation de pfSense sur proxmox

Configuration Réseau Initiale

Configurer une IP statique

Connectez votre ordinateur à un port réseau de l'hôte Proxmox et le modem/routeur de votre FAI à l'autre port. Assignez une IP statique à votre ordinateur dans le même sous-réseau que votre serveur Proxmox.

Vérifier la connectivité

Si l'IP de Proxmox est 192.168.100.2, configurez votre ordinateur avec l'IP 192.168.100.11. Ouvrez le Terminal et exécutez la commande ping 192.168.100.2 pour vérifier la connectivité.

Accéder à l'interface web

Ouvrez un navigateur et accédez à l'interface web de Proxmox via <https://192.168.100.2:8006>. Acceptez les avertissements de sécurité et connectez-vous avec vos identifiants.

Figure 3; configuration reseau initiale de pfSense



Figure 4: préparation de l'environnement proxmox début



Figure 5: préparation de l'environnement proxmox fin



Figure 6: creation d'une VM pfSense



Figure 7: installation de pfSense

Configuration des Interfaces Réseau

Identifier les interfaces

pfSense détectera deux interfaces réseau. Déterminez laquelle est WAN et laquelle est LAN en comparant les adresses MAC avec les paramètres matériels de la VM dans Proxmox.

Activer le DHCP

Configurez le serveur DHCP pour distribuer des adresses IP dans la plage 192.168.100.15 à 192.168.100.150. Acceptez de revenir temporairement à HTTP pour faciliter la configuration initiale.

Assigner les interfaces

Assignez correctement les interfaces : WAN (par exemple, vtneth) pour la connexion Internet et LAN (par exemple, vtne0) pour le réseau interne. Cette étape est cruciale pour le bon fonctionnement du pare-feu.

Configurer l'interface LAN

Depuis la console pfSense, sélectionnez l'option 2 pour configurer les IPs des interfaces. Choisissez l'interface LAN et configurez-la avec l'IP statique 192.168.100.1/24.

Figure 8: configuration des interfaces réseau

Configuration Web de pfSense



Accédez à l'interface web de pfSense en ouvrant un navigateur et en vous rendant à l'adresse <http://192.168.100.1>. Connectez-vous avec les identifiants par défaut : nom d'utilisateur "admin" et mot de passe "pfSense".

Suivez l'assistant de configuration initiale en cliquant sur Next. Configurez le nom d'hôte, les serveurs DNS et le fuseau horaire. Définissez le type de connexion WAN selon votre FAI (DHCP ou PPPoE). L'IP LAN est déjà configurée. N'oubliez pas de changer le mot de passe administrateur pour renforcer la sécurité.

Figure 9: configuration web de pfSense

Installation de l'Agent Invité QEMU



Accéder au Shell

Depuis la console pfSense, sélectionnez l'option 8 pour accéder au Shell.



Installer le package

Exécutez la commande pour installer l'agent invité QEMU.



Modifier la configuration

Modifiez le fichier de configuration et ajoutez les lignes nécessaires pour activer l'agent.

Pour assurer le démarrage automatique de l'agent, installez le package Shellcmd via System > Package Manager > Available Packages. Configurez une commande "service qemu_guest_agent start" de type "early shellcmd" et sauvegardez. Cette configuration permettra à Proxmox de mieux gérer la machine virtuelle pfSense.

Figure 10 Installation de l'agent invite QEMU

Finalisation et Vérification

1

Redémarrage

Allez dans Diagnostics > Reboot et cliquez sur Submit pour redémarrer pfSense.

2

Vérification

Après le redémarrage, vérifiez si l'IP de l'invité est visible dans Proxmox.

3

Test Internet

Ouvrez un navigateur depuis le réseau LAN et visitez un site web pour vérifier l'accès Internet.

Félicitations ! Vous avez maintenant une VM pfSense entièrement fonctionnelle sur Proxmox avec les interfaces WAN et LAN correctement configurées. N'oubliez pas d'ajouter le Network device de pfSense sur vos machines virtuelles Ubuntu et Windows Server 2019 pour qu'elles puissent communiquer à travers le pare-feu.

Pour une configuration plus avancée, vous pouvez maintenant configurer les règles de pare-feu, le NAT et d'autres services comme SNMP selon vos besoins spécifiques.

Figure 11: Finalisation et vérification de l'installation de pfSense

SOUS TITRE 2 : INSTALLATION DE UBUNTU

Guide : Installer Ubuntu Server sur une machine virtuelle Proxmox

YouTube video: <https://youtu.be/i1njhiMi4dE>

Étape 1 : Télécharger l'ISO d'Ubuntu Server

- Ouvrez un onglet de navigateur et accédez à : <https://ubuntu.com/download/server>.
- Téléchargez la dernière version LTS du serveur.
- Enregistrez le fichier ISO sur votre bureau ou dans un dossier connu.

Étape 2 : Télécharger l'ISO sur Proxmox

- Connectez-vous à l'interface web de Proxmox.
- Naviguez vers : local (pve) → Images ISO → cliquez sur Upload.

- Cliquez sur **Select File**, recherchez l'emplacement où vous avez enregistré l'ISO d'Ubuntu.
- Cliquez sur **Upload** et attendez la fin du téléchargement.
- Fermez la boîte de dialogue lorsque le message **Task OK** s'affiche.

Étape 3 : Créer une nouvelle machine virtuelle (VM)

- Faites un clic droit sur votre serveur Proxmox → sélectionnez **Create VM**.
- Changez l'ID de la VM pour quelque chose d'unique (important si vous configurez des clusters plus tard).
- Nommez votre VM (par exemple, ubuntu-test).
- Cliquez sur **Next**.

Étape 4 : Sélectionner l'ISO et configurer le système d'exploitation

- Dans le menu déroulant **ISO Image**, choisissez l'ISO d'Ubuntu que vous avez téléchargé.
- Type de système d'exploitation : Linux (par défaut).
- Cliquez sur **Next**.

Étape 5 : Configurer le stockage

- Choisissez une taille de disque (par exemple, 40 Go).
- Cliquez sur **Next**.

Étape 6 : Configurer le CPU et la mémoire

- CPU : Définissez sur 2 cœurs.
- Mémoire : Définissez sur 4096 Mo (4 Go).
- Cliquez sur **Next**.

Étape 7 : Réseau et options de démarrage

- Bridge : Laissez vmbr0 (par défaut).
- Cochez la case: **Start after created**.
- Cliquez sur **Next**, puis sur **Finish**.

Étape 8 : Démarrer la VM et lancer l'installation d'Ubuntu

- La VM démarrera automatiquement.
- Cliquez sur l'onglet **Console**.
- Sélectionnez **Install Ubuntu** lorsqu'on vous le demande.

Étape 9 : Options initiales d'installation

- Langue: Sélectionnez **English**.
- Continuez sans mettre à jour.
- Utilisez-les packages d'installation par défaut (sauf si une configuration minimale est nécessaire).

Étape 10 : Configurer les paramètres réseau (optionnel – IP statique)

- Ajoutez votre interface Ethernet.
- Allez dans **Edit IPv4**:
 - Pour une IP statique, choisissez **Manual**.
 - Entrez:
 - Adresse (par exemple, 192.168.8.56/24).
 - Passerelle.
 - DNS (par exemple, 8.8.8.8 pour Google).
 - Cliquez sur **Save**.

Étape 11 : Poursuivre l'installation

- Pas de proxy → laissez vide.
- Utilisez tout le disque.
- Cliquez sur **Done**.
- Confirmez le formatage du disque.

Étape 12: Définir les identifiants utilisateur

- Choisissez :
- Nom d'utilisateur.
- Mot de passe.
- Nom du serveur.
- Cliquez sur **Done**.

Étape 13: Activer SSH

- Cochez la case pour installer le serveur OpenSSH (important pour l'accès à distance).
- Optionnel : Choisissez des packages supplémentaires (par exemple, Docker, Nextcloud) — ignorez pour l'instant.
- Continuez l'installation.

Étape 14 : Télécharger PuTTY pour l'accès SSH

- Visitez <https://putty.org>.
- Téléchargez le fichier .exe autonome ou l'installateur.
- Installez et ouvrez PuTTY.

Étape 15 : Terminer l'installation et redémarrer

- Attendez que l'installation d'Ubuntu soit terminée.
- Cliquez sur **Reboot Now** lorsque cela vous est demandé.

Étape 16 : Tester l'accès SSH

- Ouvrez PuTTY.
- Entrez l'IP statique (par exemple, 192.168.8.56).
- Cliquez sur **Open**, acceptez la clé SSH.
- Entrez le nom d'utilisateur et le mot de passe que vous avez définis.
- Vous êtes maintenant connecté à votre serveur Ubuntu !

SOUS TITRE 3 : INSTALLATION DE WINDOWS

Prérequis pour l'installation

1. Télécharger l'ISO de Windows Server 2019 depuis le site officiel de Microsoft (version d'évaluation) :

<https://www.microsoft.com/fr-fr/evalcenter/evaluatewindows-server-2019>

2. Télécharger l'ISO des pilotes VirtIO (nécessaires pour Windows) Depuis le site officiel Fedora/RedHat :

<https://fedorapeople.org/groups/virt/virtio-win/directdownloads/latest-virtio/>

A-Création de la VM Windows

Cliquez sur Create VM.

Choisir le nom et l'ID de la machine.

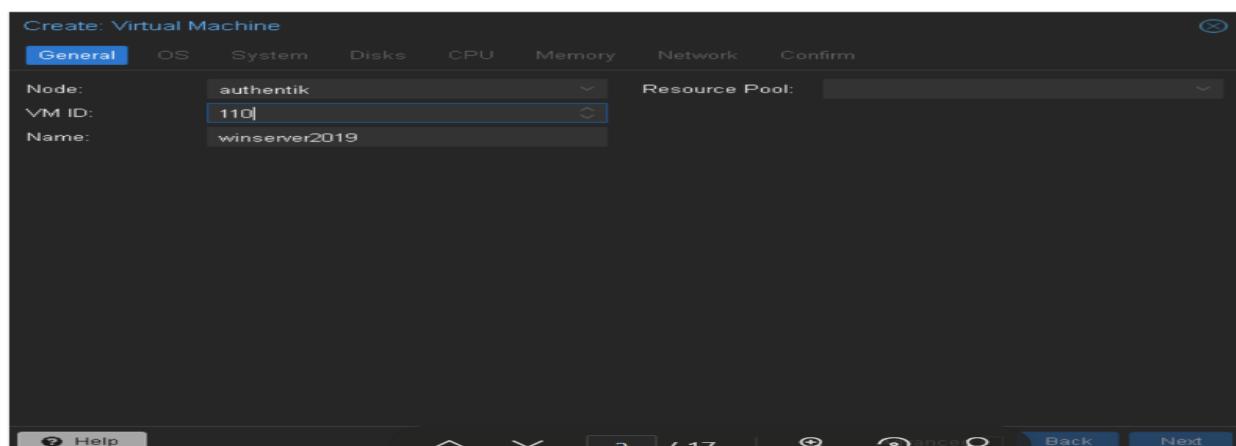


Figure 12: creation d'une VM windows

Choisir l'image ISO, le type d'OS et la version.

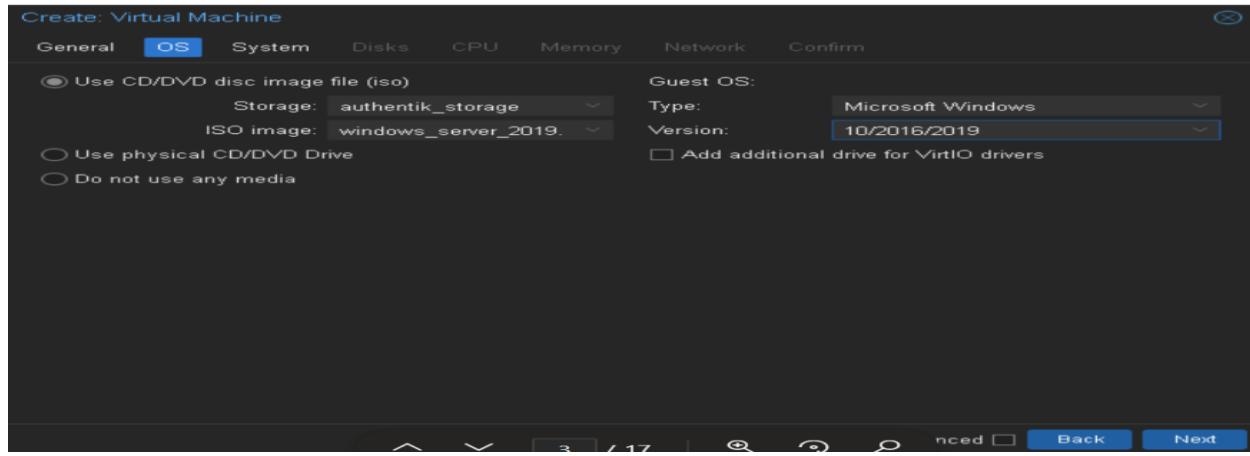


Figure 13: Ajout de l'iso dans la VM windows

Ajouté le Qemu agent qui permet un meilleur support entre l'Host (Proxmox) et le Guest (VM).

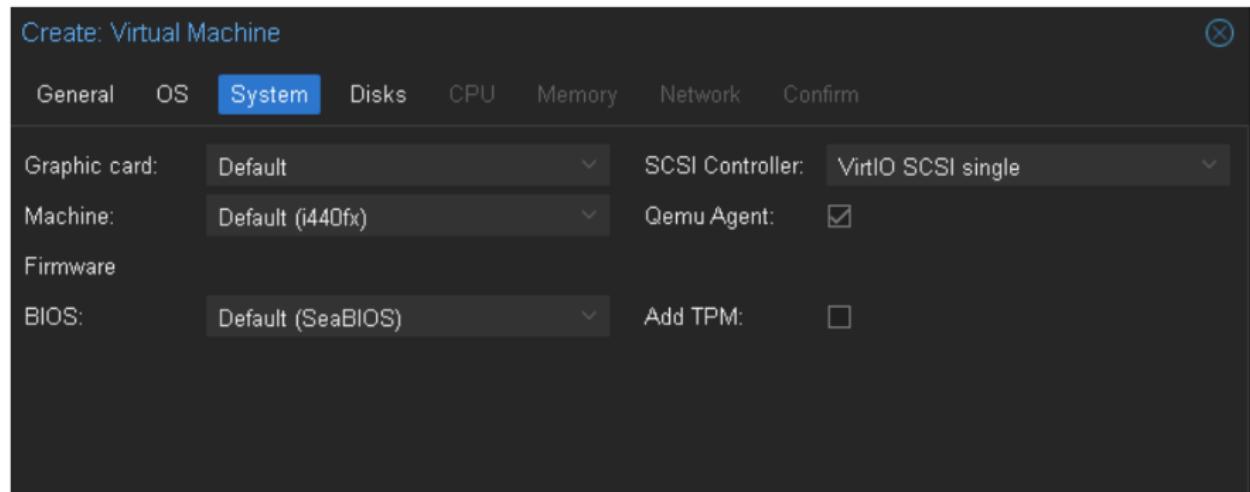


Figure 14: Ajout de l'agent QEMU dans la VM windows

Choisir l'espace de stockage de la machine.

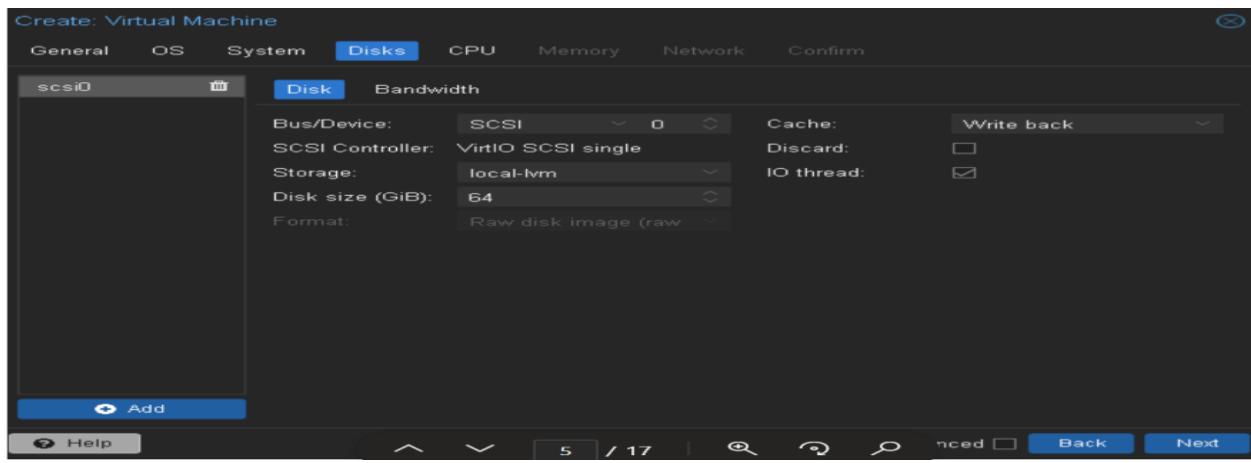


Figure 15: choisir l'espace de stockage

Choisir les paramètres du CPU.

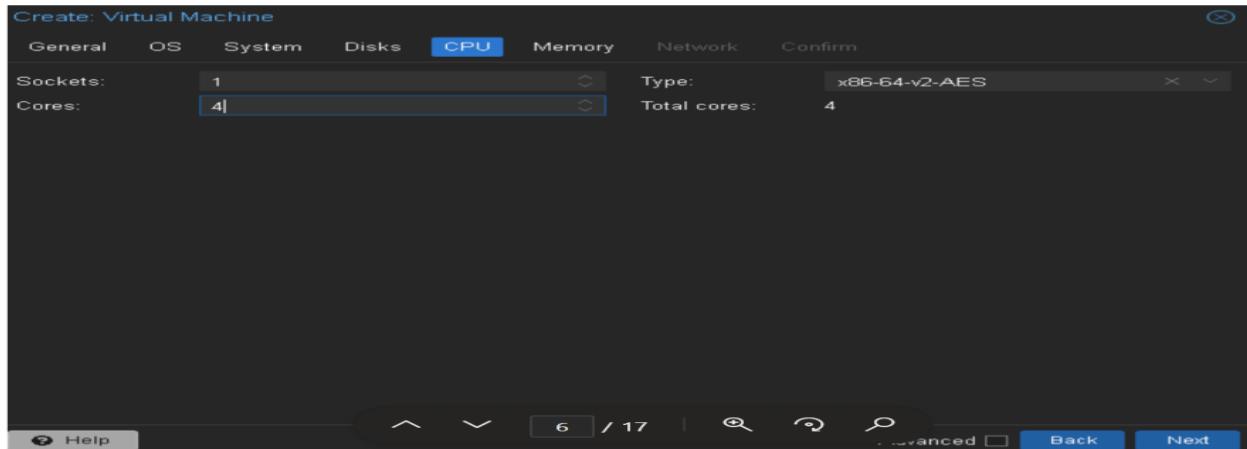


Figure 16: Choisir les parametre du CPU

Choisir la Ram de la machine.

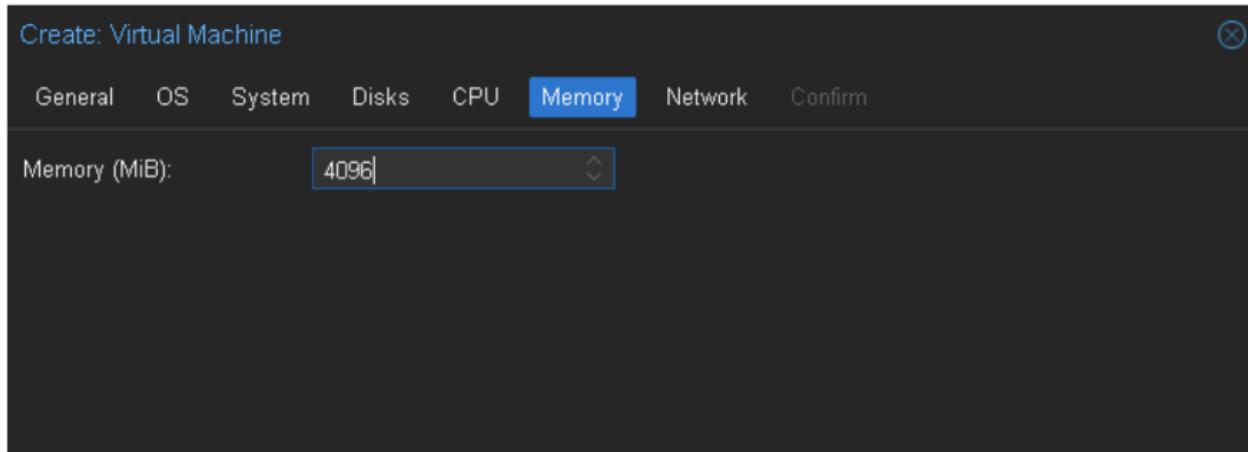


Figure 17: choisir la RAM

Choisir les paramètre réseau de la machine.

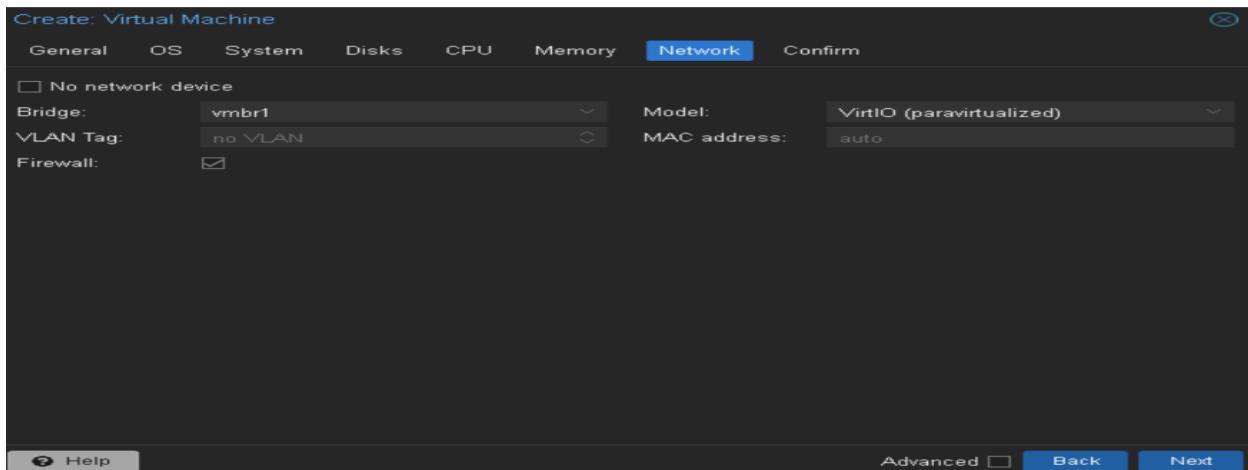


Figure 18: choisir les parametre reseau de la machine

Choisir Utiliser une image ISO.

Sélectionner virtio-win.iso et ajouter.

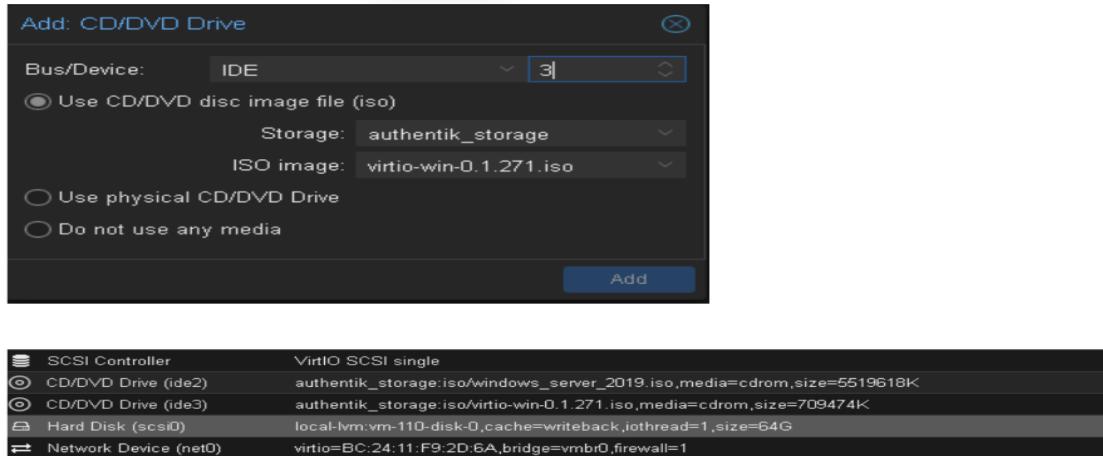


Figure 19: Ajout de l'ISO sur la VM Windows

Name	winserver2019
Start at boot	No
Start/Shutdown order	order=any
OS Type	Microsoft Windows 10/2016/2019
Boot Order	scsi0, ide2, net0, ide3
Use tablet for pointer	Yes
Hotplug	Disk, Network, USB
ACPI support	Yes
KVM hardware virtualization	Yes
Freeze CPU at startup	No
Use local time for RTC	Default (Enabled for Windows)
RTC start date	now
SMBIOS settings (type1)	uuid=8b2deefb-003b-4976-8947-fbdce6a6ee9e
QEMU Guest Agent	Enabled
Protection	No
Spice Enhancements	none
VM State storage	Automatic
AMD SEV	Default (Disabled)

Figure 20: verification des configuration final sur la VM windows

Cliquez sur démarrer et commencer l'installation de Windows Server 2019.

B- Installation de Windows serveur

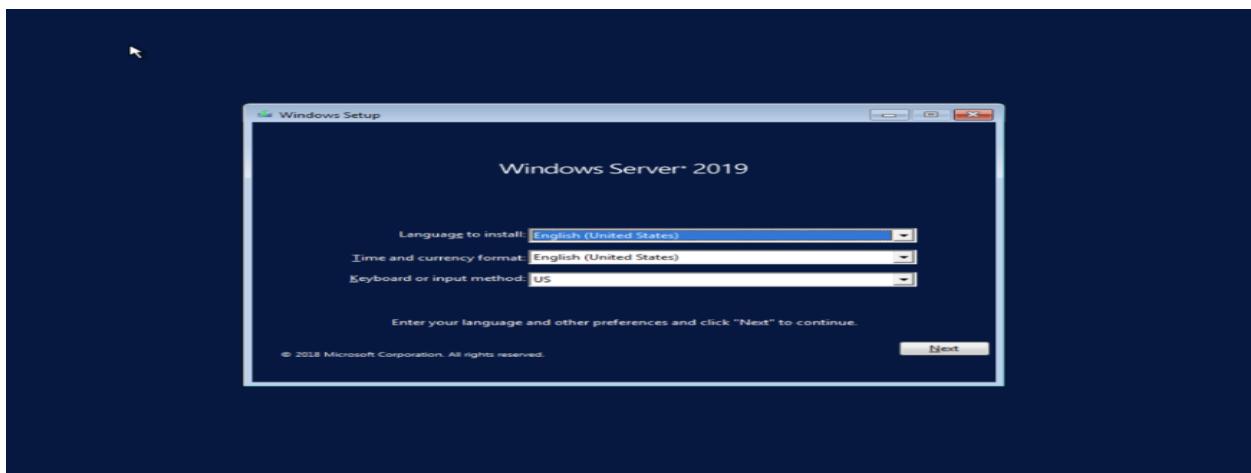


Figure 21: personnalisation de windows serveur

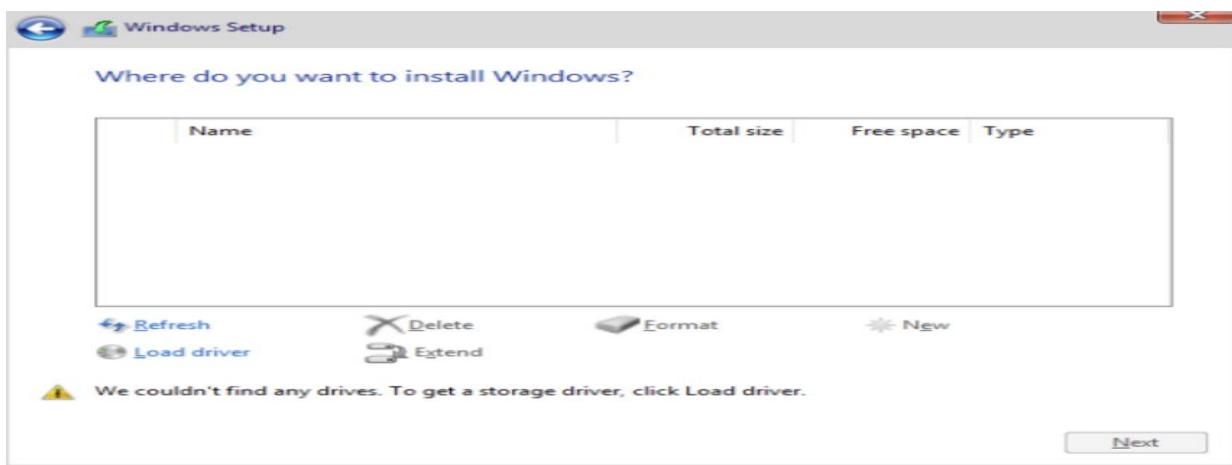


Figure 22; choix du disque pour l'installation

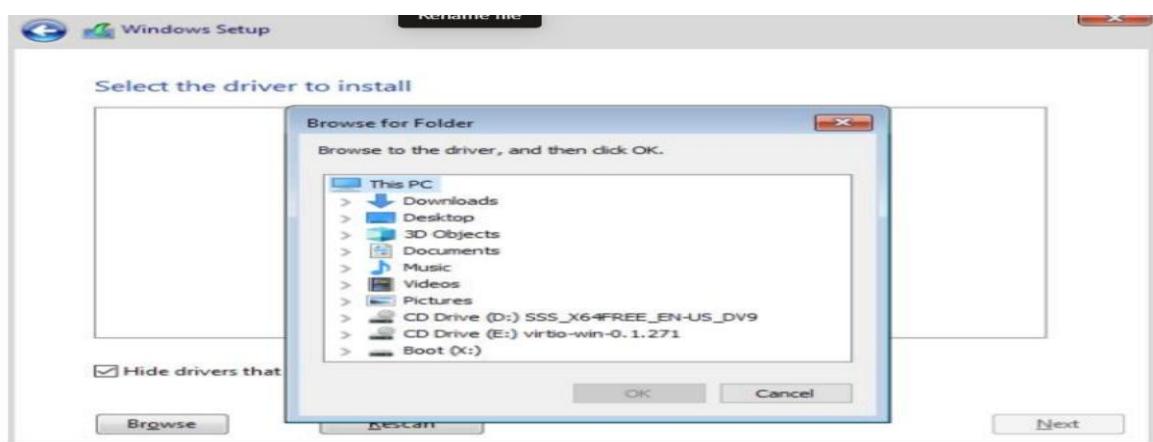


Figure 23: choix de l'emplacement

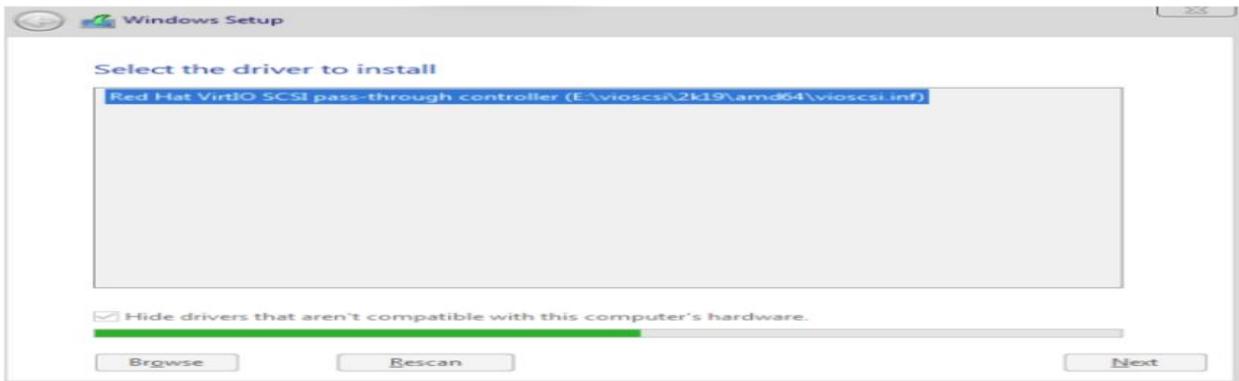


Figure 24: windows setu

Choisissez la version desktop experience de Windows

Server 2019 afin d'avoir accès au GUI.

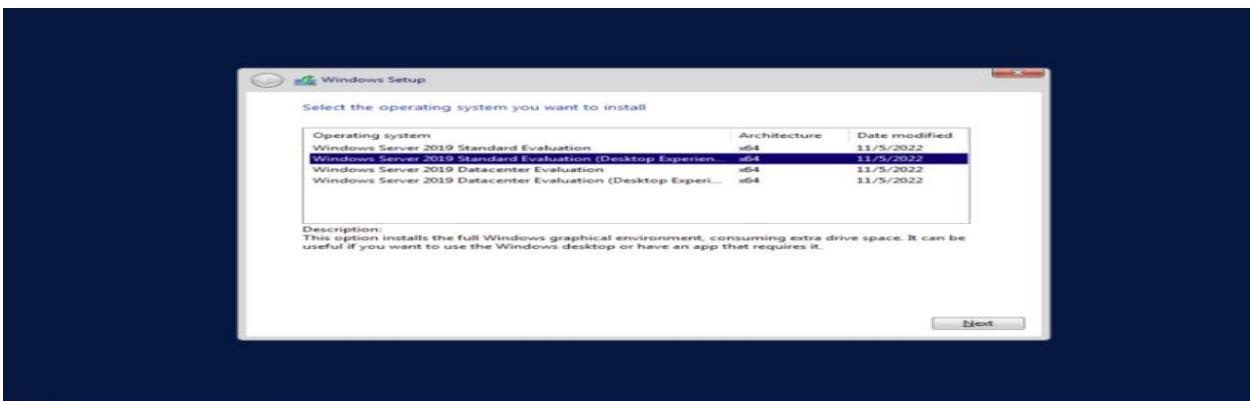


Figure 25: choisir une version windows

Entrez un nom d'utilisateur et mot de passe.

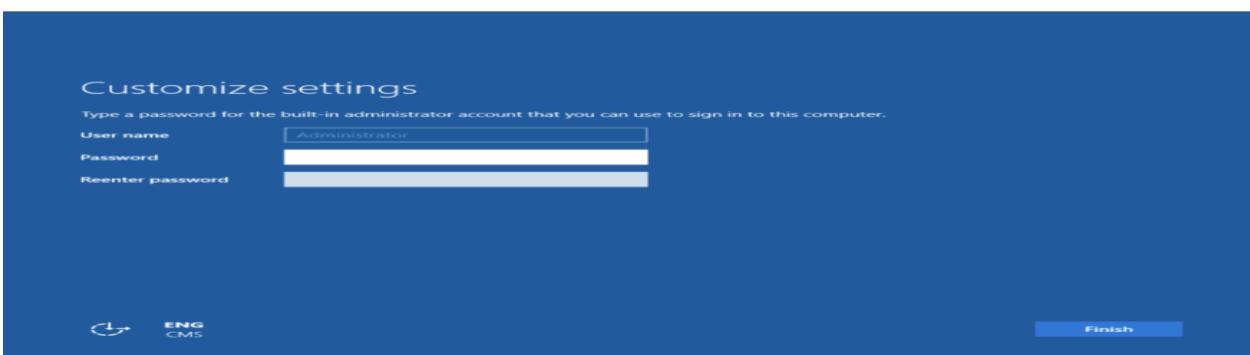


Figure 26: Ajout des credentiels

Voilà l'installation complété.

Sous-titre 3 : Sécurisation des accès administratifs à Grafana

Etape 1 : Changer le mot de passe administrateur par défaut

1. Accédez à Grafana via votre navigateur : `http://<IP_du_serveur>:3000`
2. Connectez-vous avec les identifiants par défaut : admin / admin
3. À la première connexion, changez immédiatement le mot de passe par un mot de passe complexe.

Etape 2 : Créer des utilisateurs avec rôles restreints

1. Allez dans "Configuration" > "Utilisateurs".
2. Cliquez sur "Nouveau utilisateur" et remplissez les champs nécessaires.
3. Attribuez le rôle approprié : Viewer, Editor ou Admin.

Etape 3 : Restreindre l'accès réseau à Grafana (port 3000)

Avec UFW :

- `sudo ufw enable`
- `sudo ufw allow from <ip_authorized> to any port 3000`
- `sudo ufw deny 3000` (optionnel pour bloquer les autres accès)

Etape 4 : Activer le HTTPS

Option A : Certificat auto-signé

- `sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/grafana.key -out /etc/ssl/certs/grafana.crt`
- Modifier `/etc/grafana/grafana.ini` avec les chemins vers les certificats.

Option B : Certificat Let's Encrypt

- sudo apt install certbot
- sudo certbot certonly --standalone -d votre-domaine.com
- Modifier grafana.ini avec fullchain.pem et privkey.pem

Etape 5 : Activer la journalisation des accès

- Modifier /etc/grafana/grafana.ini pour activer les logs
- Redemarrer Grafana : sudo systemctl restart grafana-server
- Consulter les logs : sudo tail -f /var/log/grafana/grafana.log

Etape 6 : Mise à jour régulière de Grafana

- sudo apt update && sudo apt list --upgradable
- sudo apt upgrade grafana
- sudo systemctl restart grafana-server

Résumé des bonnes pratiques :

- Changer mot de passe admin : éviter les identifiants par défaut
- Créer comptes utilisateurs : principe du moindre privilège
- Restreindre port 3000 : réduire surface d'attaque
- Activer HTTPS : sécuriser les communications
- Activer les logs : audit des accès
- Mises à jour régulières : corriger vulnérabilités

SOUS TITRE 4 : comment installer la solution de surveillance OpenNMS sur Ubuntu22.04

OpeNNMS est une solution gratuite et open-source de surveillance et de gestion de réseau. Il s'agit d'une plate-forme de surveillance réseau d'entreprise qui visualise et surveille tout sur les réseaux locaux et les réseaux distants. OpenNMS est une solution entièrement open-source de surveillance et de gestion de réseau, elle est publiée sous la licence AGPLv3.

OpenNMS est une plate-forme de surveillance de réseau évolutive qui vous permet de surveiller des dizaines de milliers de réseaux via des systèmes distribués et hiérarchisés. De plus,

OpenNMS est une plate-forme de surveillance flexible qui s'intègre facilement à votre activité principale et à des extensions tierces.

OpenNMS comporte plusieurs composants énumérés ci-dessous :

1. OpenNMS Horizon : offres groupées de trois composants principaux : Core (le composant principal d'Horizon), Minion (utilisé pour la surveillance distribuée à distance) et Sentinel (pour l'évolutivité).
2. Helm - tableau de bord personnalisé pour OpenNMS.
3. Architecture for Learning Enabled Correlation (ALEC) (triage des alarmes).
4. Provisioning Integration Server (PRIS) (intégration de données extraites).

Ce guide vous montre comment installer la solution de surveillance OpenNMS avec un serveur de base de données PostgreSQL et un proxy inverse Nginx sur un serveur Ubuntu 22.04. En outre, ce guide vous montrera l'installation de Java OpenJDK, la configuration de base du serveur de base de données PostgreSQL et le serveur Web Nginx.

A-Conditions préalables

Tout d'abord, vous aurez besoin des conditions suivantes pour terminer ce guide :

- Un serveur Ubuntu 22.04 : cet exemple utilise le serveur Ubuntu avec le nom *d'hôte* '*opennms-server*' et la mémoire est de 4 Go.
- Un utilisateur non root avec des priviléges d'administrateur sudo/root.\
- Un nom de domaine ou un domaine local sera utilisé pour exécuter OpenNMS.

B-Installation de Java OpenJDK

La solution de supervision OPNeNMS est un outil de supervision principalement écrit en Java. Au moment de la rédaction de cet article, la dernière version d'OpenNMS prend en charge au minimum Java 11. Le référentiel Ubuntu 22.04 par défaut fournit Java OpenJDK 11 que vous pouvez facilement installer via APT.

Avant d'installer Java, exécutez la commande apt suivante pour mettre à jour et actualiser l'index de votre package.

```
sudo apt update
```

Installez maintenant Java OpenJDK 11 via la commande apt ci-dessous. La version par défaut de Java pour le système Ubuntu 22.04 est Java OpenJDK 11, qui convient à l'installation d'OpenNMS.

```
sudo apt install default-jdk
```

Lorsque vous y êtes invité, entrez y pour confirmer et appuyez sur ENTER. L'installation de Java OpenJDK va commencer.

Une fois Java OpenJDK installé, exécutez la commande ci-dessous pour vérifier la version installée de Java. Java OpenJDK 1.11 devrait être installé sur votre système Ubuntu.

```
java -version
```

Une fois Java OpenJDK installé, passez à l'installation de la base de données PostgreSQL.

Installation et configuration de PostgreSQL Server

PostgreSQL est un RDMS (Relational Database Management System) performant. OpenNMS ne prend en charge que PostgreSQL comme backend de base de données. Au moment de la rédaction de cet article, OpenNMS prend en charge PostgreSQL v10.x-14.x.

Vous allez maintenant installer et configurer la base de données PostgreSQL v14 sur un serveur Ubuntu. Par défaut, le référentiel Ubuntu fournit plusieurs versions de PostgreSQL, et vous installerez PostgreSQL 14.x pour le déploiement d'OpenNMS.

Exécutez la commande apt ci-dessous pour installer PostgreSQL 14.

```
sudo apt install postgresql-14
```

Lorsque vous êtes invité à confirmer, entrez y et appuyez sur ENTER pour continuer.

Une fois le package PostgreSQL installé, exécutez la commande systemctl suivante pour vérifier le service PostgreSQL et vous assurer qu'il est en cours d'exécution et activé.

```
sudo systemctl is-enabled postgresql  
sudo systemctl status postgresql
```

Vous verrez alors que le service PostgreSQL est activé et qu'il sera exécuté automatiquement au démarrage. Et l'état du service PostgreSQL est en cours d'exécution.

Maintenant que la base de données PostgreSQL est en cours d'exécution, vous allez passer en revue la base de données et la création d'utilisateurs pour OpenNMS. Vous allez également configurer le mot de passe de l'utilisateur PostgreSQL par défaut '*postgres*'.

Exécutez la commande ci-dessous pour créer un nouvel utilisateur PostgreSQL '*opennms*'.

Lorsque vous êtes invité à saisir le mot de passe, entrez le nouveau mot de passe de l'utilisateur '*opennms*' et répétez-le.

```
sudo -u postgres createuser -P opennms
```

Ensuite, créez une nouvelle base de données '*opennms*' avec le propriétaire '*opennms*' via la commande suivante.

```
sudo -u postgres createdb -O opennms opennms
```

Enfin, modifiez le mot de passe de l'utilisateur '*postgres*' via la commande suivante. Et assurez-vous de le changer avec un nouveau mot de passe fort.

```
sudo -u postgres psql -c "ALTER USER postgres WITH PASSWORD '5up3rp4ssw0rd';"
```

Now that you have Java OpenJDK and PostgreSQL installed, you're ready to install OpenNMS.

C-Installing and Configuring OpenNMS

You've installed Java OpenJDK and PostgreSQL database, also you've created a new database and user for OpenNMS, and configured the default password for PostgreSQL '*postgres*' user. You'll then start installing and configuring the OpenNMS.

In this section, you will install OpenNMS via the official OpenNMS repository. Then, you will set up OpenNMS with the PostgreSQL database, set up the Java environment, initialize database schema, detect system libraries, and allow the OpenNMS to run in privileged ports.

First, run the following command to add the OpenNMS GPG key and repository.

```
sudo apt-key adv --fetch-keys https://debian.opennms.org/OPENNMS-GPG-KEY  
sudo add-apt-repository -s 'deb https://debian.opennms.org stable main'
```

When prompted, press ENTER to confirm and add the OpenNMS repository.

Installez maintenant le paquet OpenNMS avec des paquets R supplémentaires via la commande apt ci-dessous.

```
sudo apt install opennms r-recommended
```

Lorsque vous êtes invité à confirmer, entrez y pour confirmer et appuyez sur ENTER pour continuer.

Ensuite, exécutez la commande apt ci-dessous pour désactiver la mise à jour automatique du paquet OpenNMS. L'OpenNMS nécessite des étapes et des configurations manuelles lors de la mise à niveau vers une nouvelle version, vous devez donc le mettre à niveau manuellement pour éviter les erreurs pendant/après les mises à niveau.

```
sudo apt-mark hold libopennms-java |  
libopennmsdeps-java |  
opennms-common |  
opennms-db
```

Maintenant que l'OpenNMS est installé, vous pouvez vérifier le répertoire d'installation d'OpenNMS '/usr/share/opennms' via la commande ci-dessous. De plus, toutes les modifications liées à OpenNMS doivent être appliquées aux fichiers sous le répertoire '/usr/share/opennms'.

```
sudo apt install tree -y  
sudo tree /usr/share/opennms -L 1
```

You could see a list of directories and files for the OpenNMS package.

Ensuite, vous allez configurer la base de données pour OpenNMS. Ouvrez le fichier '/usr/share/opennms/etc/opennms-datasources.xml' à l'aide de la commande nano editor suivante. La commande 'sudo -u opennms..' indique que vous exécutez la commande en tant qu'utilisateur 'opennms', et non en tant qu'utilisateur root.

```
sudo -u opennms nano /usr/share/opennms/etc/opennms-datasources.xml
```

Remplacez le '*'jdbc-data-source'*' par '**'opennms'**' qui doit utiliser les détails de la base de données '*'opennms'*' et de l'utilisateur. Et pour '**'opennms-admin'**', vous devriez utiliser l'utilisateur admin *PostgreSQL* '*'postgres'*'.

```
<jdbc-data-source name="opennms"
    database-name="opennms"
    class-name="org.postgresql.Driver"
    url="jdbc:postgresql://localhost:5432/opennms"
    user-name="opennms"
    password="p4ssw0rd" />

<jdbc-data-source name="opennms-admin"
    database-name="template1"
    class-name="org.postgresql.Driver"
    url="jdbc:postgresql://localhost:5432/template1"
    user-name="postgres"
    password="5up3rp4ssw0rd" />
```

Enregistrez le fichier et quittez l'éditeur lorsque vous avez terminé.

Exécutez maintenant la commande suivante pour détecter l'environnement Java sur votre système, qui sera stocké de manière permanente dans le fichier *de configuration* '*/usr/share/opennms/etc/java.conf*'.

```
sudo -u opennms /usr/share/opennms/bin/runjava -s
```

Après cela, exécutez la commande ci-dessous pour initialiser la base de données et détecter les bibliothèques système pour OpenNMS. Les bibliothèques pour l'OpenNMS seront répertoriées dans le fichier '*/opt/opennms/etc/libraries.properties*'.

```
sudo -u opennms /usr/share/opennms/bin/install -dis
```

Ensuite, modifiez le fichier de service OpenNMS à l'aide de la commande systemctl suivante.

Vous devriez obtenir l'EDITOR par défaut sur votre système.

```
sudo systemctl edit --full opennms.service
```

Add the following configuration to the '[Service]' section. This allows the OpenNMS service to run and bind in privileged ports (ports 1-1024).

```
[Service]
...
AmbientCapabilities=CAP_NET_RAW CAP_NET_BIND_SERVICE
```

Save the file and exit the editor when you are finished.

Après avoir modifié le fichier de service OpenNMS, exécutez la commande suivante pour recharger le gestionnaire systemd, redémarrer et activer le service OpenNMS.

```
sudo systemctl daemon-reload
sudo systemctl restart opennms
sudo systemctl enable opennms
```

Maintenant que le service OpenNMS est opérationnel avec de nouvelles configurations, vous allez vérifier le service OpenNMS via la commande systemctl ci-dessous.

```
sudo systemctl is-enabled opennms
sudo systemctl status opennms
```

Le résultat - Le service OpenNMS est activé et s'exécutera automatiquement au démarrage du système. Et le service OpenNMS est actuellement en cours d'exécution.

À ce stade, vous avez terminé l'installation et la configuration d'OpenNMS. Mais, vous exécuterez l'OpenNMS avec le proxy inverse Nginx. Lisez la suite pour savoir comment configurer Nginx en tant que proxy inverse pour OpenNMS.

D-Installation de Nginx en tant que proxy inverse pour OpenNMS

Maintenant qu'OpenNMS s'exécute sur le port par défaut '8980', vous allez installer et configurer Nginx en tant que proxy inverse pour OpenNMS.

Exécutez la commande apt suivante pour installer le paquet Nginx sur votre système.

```
sudo apt install nginx
```

Entrez y lorsque vous y êtes invité, puis appuyez sur ENTER pour continuer. Et l'installation commencera.

Ensuite, vérifiez le service Nginx avec la commande systemctl suivante.

```
sudo systemctl is-enabled nginx  
sudo systemctl status nginx
```

Vous devriez voir que le service Nginx est activé et qu'il s'exécutera automatiquement au démarrage. De plus, le service Nginx est automatiquement démarré une fois l'installation terminée.

After Nginx is installed, create a new Nginx server block '/etc/nginx/sites-available/opennms.conf' using the following nano editor command.

```
sudo nano /etc/nginx/sites-available/opennms.conf
```

Add the following configuration to the file. Be sure to change the domain name with your domain.

```
server {  
    listen 80;  
    server_name opennms.howtoforge.local;  
    access_log /var/log/nginx/opennms.access.log;  
    error_log /var/log/nginx/opennms.error.log;  
  
    location / {  
        proxy_set_header Host $http_host;  
        proxy_set_header X-Forwarded-Host $host;  
        proxy_set_header X-Forwarded-Server $host;  
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;  
        proxy_set_header X-OpenNMS-Server-URL https://opennms.howtoforge.local/;  
        proxy_pass http://localhost:8980;  
    }  
}  
}
```

Enregistrez le fichier et quittez l'éditeur lorsque vous avez terminé.

Ensuite, activez le bloc de serveur '*opennms.conf*' et vérifiez la configuration de Nginx pour vous assurer que vous avez la bonne configuration.

```
sudo ln -s /etc/nginx/sites-available/opennms.conf /etc/nginx/sites-enabled/  
sudo nginx -t
```

Si vous voyez le message de sortie tel que « *test réussi - syntaxe correcte* », cela signifie que votre configuration Nginx est correcte.

Redémarrez maintenant le service Nginx pour appliquer la nouvelle configuration de bloc de serveur.

```
sudo systemctl restart nginx
```

Maintenant que le Nginx fonctionne en tant que proxy inverse pour l'OpenNMS, vous allez ensuite passer en revue la configuration du pare-feu UFW et ouvrir certains ports pour certains services.

E- Configuration du pare-feu UFW

Après avoir configuré le proxy inverse Nginx, vous allez ensuite configurer l'UFW sur votre serveur OpenNMS. Vous allez exécuter l'outil de surveillance OpenNMS avec l'UFW activé, vous devez donc ajouter des ports qui seront utilisés pour OpenNMS.

Exécutez la commande apt suivante pour installer UFW sur votre système.

```
sudo apt install ufw -y
```

Après l'installation de UFW, exécutez la commande ci-dessous pour ajouter le service OpenSSH. Ensuite, démarrez et activez le service UFW.

```
sudo ufw allow OpenSSH
```

```
sudo ufw enable
```

```
root@opennms-server:~#  
root@opennms-server:~# sudo ufw allow OpenSSH  
Rules updated  
Rules updated (v6)  
root@opennms-server:~# sudo ufw enable  
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y  
Firewall is active and enabled on system startup  
root@opennms-server:~#  
root@opennms-server:~#
```

Lorsque vous y êtes invité, entrez `y` pour confirmer et appuyez sur ENTER pour continuer.
Maintenant, l'UFW sera en cours d'exécution et il est activé et sera exécuté automatiquement au démarrage.

Ensuite, ajoutez une nouvelle règle pour autoriser les trafics vers le serveur Web Nginx.

```
sudo ufw allow "Nginx Full"
```

```
root@opennms-server:~# 
root@opennms-server:~# sudo ufw allow "Nginx Full"
Rule added
Rule added (v6)
root@opennms-server:~# sudo nano /etc/ufw/before.rules
root@opennms-server:~#
root@opennms-server:~# sudo ufw allow in 162/udp
Rule added
Rule added (v6)
root@opennms-server:~# sudo ufw allow in 10162/udp
Rule added
Rule added (v6)
root@opennms-server:~#
```

Figure 27: Ouverture du port TCP/UDP sur le pare feu

Après cela, ouvrez le fichier '`/etc/ufw/before.rules`' à l'aide de la commande nano editor suivante.

```
sudo nano /etc/ufw/before.rules
```

Ajoutez la configuration suivante avant la section '*filter'. Cela activera NAT et redirigera/transférera le trafic de *62/udp* à *10162/udp*.

```
*nat  
:PREROUTING ACCEPT [0:0]  
-A PREROUTING -p udp --dport 162 -j REDIRECT --to-port 10162  
COMMIT
```

Enregistrez le fichier et quittez l'éditeur lorsque vous avez terminé.

Ajoutez maintenant la nouvelle règle pour autoriser les deux ports *62/udp* à *10162/udp*.

```
sudo ufw allow in 162/udp  
sudo ufw allow in 10162/udp
```

Rechargez l'UFW pour appliquer les modifications et vérifier l'état de l'UFW à l'aide de la commande suivante.

```
sudo ufw reload  
sudo ufw status
```

```
root@opennms-server:~#  
root@opennms-server:~# sudo ufw reload  
Firewall reloaded  
root@opennms-server:~# sudo ufw status  
Status: active  
  
 To          Action    From  
 --          ----  
 OpenSSH      ALLOW     Anywhere  
 Nginx Full   ALLOW     Anywhere  
 162/udp     ALLOW     Anywhere  
 10162/udp   ALLOW     Anywhere  
 OpenSSH (v6) ALLOW     Anywhere (v6)  
 Nginx Full (v6) ALLOW     Anywhere (v6)  
 162/udp (v6) ALLOW     Anywhere (v6)  
 10162/udp (v6) ALLOW     Anywhere (v6)
```

Figure 28: ports autorisés sur le pare feu

Jusqu'à présent, vous avez terminé l'installation et la configuration d'OpenNMS avec les dépendances de package telles que la base de données PostgreSQL et le serveur Web Nginx, et vous avez également configuré l'UFW. Pour la dernière étape, vous accéderez à l'installation d'OpenNMS via un navigateur Web et configurerez l'utilisateur administrateur pour OpenNMS.

E-Accès à l'outil de surveillance OpenNMS

Ouvrez votre navigateur Web et visitez le nom de domaine de votre installation OpenNMS (ex : <http://opennms.howtoforge.local>). Vous devriez voir la page de connexion de l'outil de surveillance OpenNMS.

Entrez l'utilisateur/mot de passe par défaut '**admin/admin**' et cliquez sur '**Connexion**'.

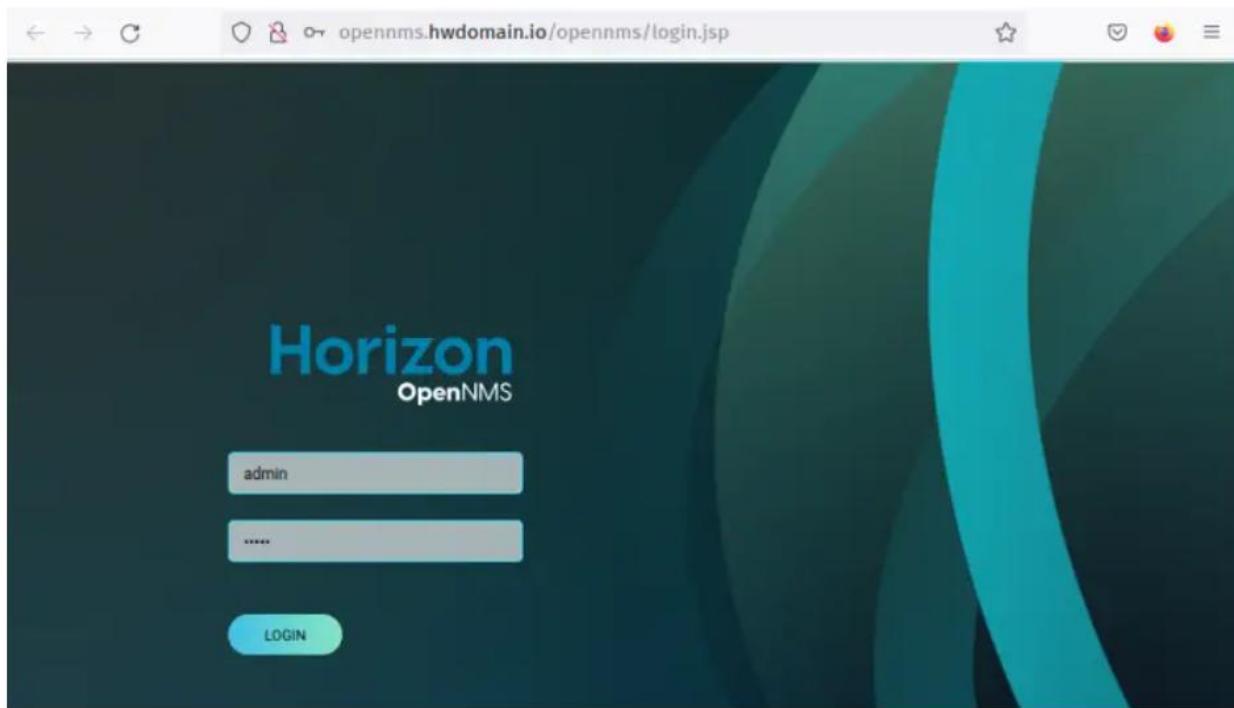


Figure 29: Interface OpenNMS

Vous verrez alors le tableau de bord d'administration d'OpenNMS.

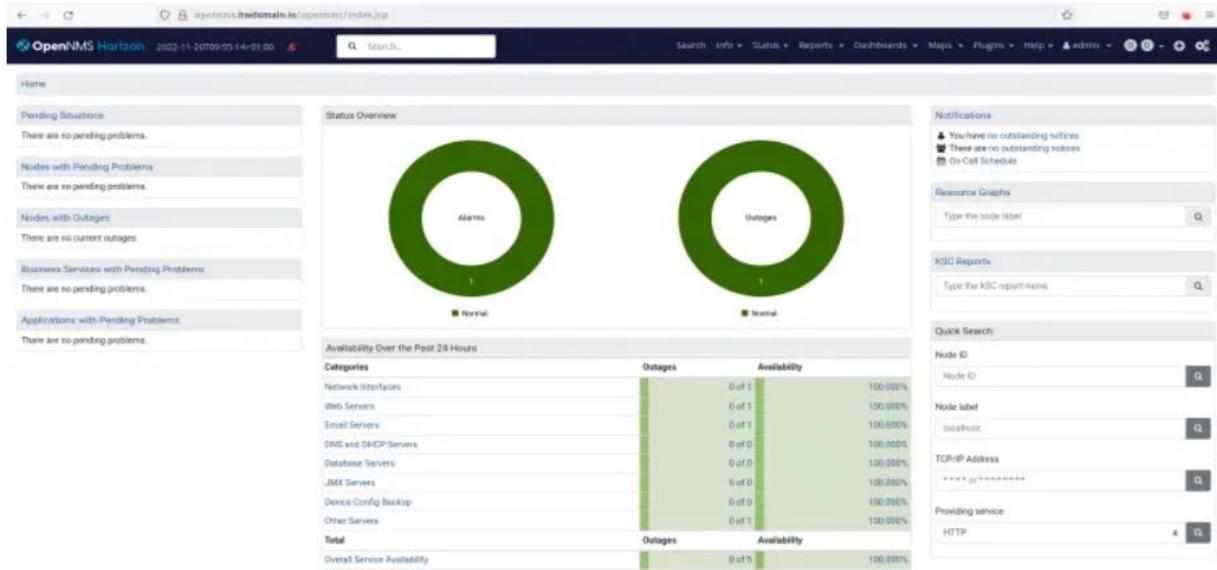


Figure 30: Interface de configuration OOpenNMS

Après vous être connecté à OpenNMS via l'utilisateur/mot de passe par défaut '**admin/admin**', vous changerez ensuite le nom d'utilisateur et le mot de passe par défaut pour votre installation OpenNMS.

Dans la barre de menu supérieure, cliquez sur le menu « **Admin** » et sélectionnez « **Modifier le mot de passe** ».

Entrez maintenant l'ancien mot de passe 'admin' et entrez le nouveau mot de passe OpenNMS et répétez le mot de passe. Ensuite, cliquez sur « **Soumettre** » pour postuler.

Please enter the old and new passwords and confirm.

Current Password

New Password

Confirm New Password

Submit **Cancel**

Figure 31: modification deu mot de passe OpenNMS

Vous avez maintenant terminé la configuration d'OpenNMS.

TRITRE 3 : INVENTAIRE DES CAPTEURS

Sous Titre 1 : Inventaire des capteurs

Dans l'environnement actuel, la majorité des capteurs utilisés dans PRTG sont de type **ping**, permettant de vérifier la disponibilité des équipements réseau. Des capteurs **SNMP** complètent cette surveillance en analysant les ports des switches et pare-feux, avec des alertes configurées en cas de dépassement de seuils. D'autres capteurs suivent l'état de santé global des équipements (mémoire, processeur, stabilité). Une attention particulière est portée à la page « **État des services TIC** », qui utilise des capteurs ping et HTTP pour valider automatiquement, via les **API de PRTG**, la disponibilité des services (comme un retour HTTP 200 pour les sites web). Les alertes sont acheminées selon les services concernés : réseau, caméras, Alertus, etc.

Dans le cadre de la migration vers une solution de supervision **open source comme OpenNMS**, il est essentiel de réaliser un **inventaire structuré des capteurs**. Cela permet de s'assurer que tous les services critiques seront bien couverts après la migration. En classant et regroupant les capteurs, on facilite la planification, on élimine les doublons et on priorise les éléments essentiels. Ce processus garantit aussi une meilleure visibilité de l'environnement supervisé et pose les bases d'une documentation claire et à jour.

La page "État des services TIC" semble afficher les services supervisés en temps réel, y compris leur état fonctionnel, intermittent ou non-fonctionnel. Voici les éléments généralement supervisés selon votre infrastructure et les informations trouvées :

1. **Accessibilité réseau** : Vérifié via des capteurs Ping ou HTTP (par exemple, pour garantir un code HTTP 200).
2. **Ressources système** : CPU, mémoire, stockage des serveurs, switches et firewalls.
3. **Applications critiques** : Par exemple, TOPdesk ou le site web du CCNB.
4. **Infrastructure Wi-Fi** : Points d'accès et leur connectivité.
5. **Intégration API** : Interaction entre PRTG et des systèmes externes, comme WordPress.

Ces services sont rapportés en temps réel sur la page pour que la communauté puisse les consulter avant de solliciter le support informatique.

<https://etatdesservicestic.cnb.ca/>

A-Inventaire des capteurs PRTG en production

- Tableau d'inventaire des capteurs (sensors) :

Type de capteur	Catégorie	Description	Critères d'alerte	Groupes d'avis
Ping	Disponibilité réseau	Détermine si l'appareil est sur le réseau et accessible.	Appareil non accessible.	Analystes réseau, Équipe technique
SNMP	Santé des équipements	Surveillance de la mémoire, du CPU, et autres paramètres de santé des switches et firewalls.	Utilisation mémoire/CPU au-dessus d'un seuil défini.	Analystes réseau, Équipe technique
HTTP	État des services TIC	Valide l'état des services TIC (ping + réponse HTTP avec code 200).	Non-réponse ou code HTTP différent de 200.	Équipe technique
CPU	Santé des équipements	Surveillance de l'utilisation du CPU des équipements.	Utilisation CPU au-dessus d'un seuil défini.	Analystes réseau, Équipe technique
RAM	Santé des équipements	Surveillance de l'utilisation de la mémoire vive (RAM) des équipements.	Utilisation mémoire vive au-dessus d'un seuil défini.	Analystes réseau, Équipe technique

Disque	Santé des équipements	Surveillance de l'utilisation du stockage disque.	Utilisation disque au-dessus d'un seuil défini.	Analystes réseau, Équipe technique
Bandé passante	Utilisation des ports	Monitoreder l'utilisation des ports sur les switches et firewalls.	Niveau de trafic au-dessus d'un seuil défini.	Analystes réseau, Équipe technique
Wi-Fi	Réseaux Wi-Fi	Surveillance des points d'accès (par ex. 50 sur 250 AP hors ligne entraîne une alerte pour perturbation).	Déconnexion d'un pourcentage défini des points d'accès.	Analystes réseau
API	Intégration API	Intégration avec WordPress pour afficher l'état des services (fonctionnel, perturbé ou non fonctionnel).	État fonctionnel avec perturbations ou non-fonctionnel détecté.	Équipe technique,

Table 1: Inventaire des capteurs

B-Détails des capteurs

- **Ping** : Ces capteurs sont majoritairement utilisés (90%) pour déterminer si les appareils sont accessibles sur le réseau.
- **SNMP** : Utilisé pour surveiller les ressources des équipements tels que la mémoire et le CPU.

- **HTTP** : Utilisé pour valider les réponses des services Web (exemple : code HTTP 200 attendu).
- **CPU** : Capteurs spécifiques pour monitorer l'utilisation du processeur.
- **RAM** : Capteurs pour surveiller l'utilisation de la mémoire vive.
- **Disque** : Capteurs pour surveiller l'espace de stockage et son utilisation.
- **Bandé passante** : Capteurs pour monitorer le trafic sur les ports des switches et firewalls.
- **Wi-Fi** : Surveillance des points d'accès et de leur disponibilité.
- **API** : Utilisé pour l'intégration avec des systèmes externes comme WordPress.

C-Processus d'alerte

Les alertes sont gérées en fonction de la classe des appareils :

- Switches : Alertes envoyées aux analystes réseau.
- Caméras : L'équipe de maintenance est avisée.
- Systèmes locaux : L'équipe technique reçoit les notifications.
- Alertus : Le DASA des campus est informé.

Ce système assure une surveillance efficace et une communication rapide avec les équipes concernées pour minimiser les interruptions de service.

Pour identifier les capteurs nécessitant une recréation manuelle, il est nécessaire de prendre en compte plusieurs facteurs, comme les types de capteurs, leurs configurations spécifiques, et les intégrations système.

Capteur nécessitant (possiblement) une recréation manuelle et leurs raisons :

1. PING - Mauvaise configuration de l'adresse ou des seuils, dépendance à des paramètres externes spécifiques
2. SNMP - Problèmes avec l'intégration des MIB, configuration manuelle des hôtes SNMP pour certains équipements.
3. HTTP - Problèmes de configuration des URL, problèmes de certificats SSL ou de ports non standards.

4. CPU - Capteurs spécifiques aux équipements qui ne migrent pas automatiquement.
5. RAM - Configurations des serveurs ou matériels qui varient d'un modèle à l'autre, nécessitant une réintégration.
6. DISQUE – Besoin de spécifications de partitionnement spécifiques ou de seils personnalisés.
7. BANDE PASSANTE - Configuration des interfaces ou des ports particuliers nécessitant une recréation des capteurs.
8. Wi-Fi - Problèmes de compatibilité avec certains points d'accès, nécessitant une configuration manuelle des capteurs.
9. API - API non documentées ou mises à jour, nécessitant des ajustements manuels pour l'intégration.

SOUS TITRE 2: Méthodologie détaillée pour l'inventaire, la classification et le regroupement des capteurs pour préparer une migration vers OpenNMS.

Je vais vous guider étape par étape dans ce processus de recensement et d'organisation des capteurs pour préparer une migration vers OpenNMS.

Étape 1: Recenser tous les capteurs existants

Commençons par extraire l'inventaire complet:

1. Extraction des données depuis PRTG:

- Connectez-vous à l'interface d'administration PRTG
- Naviguez vers "Bibliothèque" > "Gestion des capteurs"
- Utilisez la fonction d'exportation au format CSV (ou utilisez l'API si vous êtes à l'aise avec le scripting)
- Sélectionnez tous les champs pertinents dans l'export:
 - Identifiant unique
 - Nom du capteur
 - Type technique (ping, HTTP, SNMP, etc.)
 - Adresse IP ou nom d'hôte surveillé
 - Intervalle de sondage (en secondes)
 - Chemin complet dans l'arborescence PRTG
 - État actuel (actif, en pause, en erreur)
 - Seuils d'alerte configurés

2. Nettoyage initial des données:

- Importez le CSV dans Excel ou un outil similaire

- Vérifiez l'intégrité des données (caractères spéciaux, encodage)
- Créez une colonne supplémentaire pour vos notes et observations

Étape 2: Classifier les capteurs par technologie

Ajoutez une colonne "Catégorie Technique" dans votre fichier et classez chaque capteur:

1. Classification technique:

- **Réseau de base:**
 - Ping ICMP
 - Bande passante (SNMP Traffic)
 - Latence et perte de paquets
- **Infrastructure réseau:**
 - États des ports (SNMP Interface)
 - Indicateurs de performance des équipements réseau
- **Systèmes:**
 - Charge CPU (SNMP, WMI, SSH)
 - Utilisation mémoire
 - Espace disque
 - Température/ventilateurs
- **Applications:**
 - HTTP/HTTPS (disponibilité sites web)
 - Services Windows/Linux
 - Bases de données (SQL, Oracle, etc.)
 - Temps de réponse applicatifs
- **Sécurité:**

- Ports ouverts
- Certificats SSL/TLS
- Journaux d'événements sécurité

2. Vérification de la classification:

- Assurez-vous que chaque capteur est dans une seule catégorie
- Créez une catégorie "Divers" pour les cas particuliers

Étape 3: Regrouper par cible/équipement

1. Créez un second fichier pour le mapping hiérarchique:

- Structure à trois niveaux: Capteur → Équipement → Service métier
- Pour chaque capteur de l'inventaire, identifiez:
 - L'équipement physique ou virtuel associé
 - Le service métier supporté

2. Identification des équipements critiques:

- Consultez la documentation existante sur l'infrastructure
- Identifiez les serveurs critiques pour l'entreprise
- Marquez les équipements selon leur criticité (Haute/Moyenne/Basse)

3. Associez les capteurs aux services métiers:

- Web public (site internet)
- Applications internes
- Services d'infrastructure (DNS, DHCP, AD)
- Services de communication (messagerie, téléphonie)
- ERP et applications métiers

Étape 4: Analyse et nettoyage

1. Identification des doublons et capteurs inutiles:

- Appliquez des filtres pour trouver:
 - Capteurs surveillant le même paramètre sur un même équipement
 - Capteurs en erreur depuis plus de 30 jours
 - Capteurs sans alerte configurée et non consultés

2. Décision sur chaque capteur:

- Créez une colonne "Action" avec les valeurs:
 - Conserver et migrer
 - Fusionner (en cas de doublon)
 - Supprimer (obsolète ou inutile)
 - À vérifier (besoin d'investigation)

3. Validation avec les parties prenantes:

- Présentez la liste des capteurs à supprimer aux équipes techniques
- Confirmez que ces suppressions n'auront pas d'impact négatif

Étape 5: Priorisation pour la migration

1. Définition des critères de priorité:

- **Haute priorité** (Vague 1):
 - Capteurs critiques pour la production
 - Capteurs liés à la sécurité ou la disponibilité
 - Capteurs utilisés dans les tableaux de bord principaux
- **Moyenne priorité** (Vague 2):
 - Capteurs importants pour la performance

- Capteurs secondaires des systèmes critiques
- **Basse priorité** (Vague 3):
 - Capteurs informatifs non critiques
 - Capteurs de test ou de développement
 - Capteurs rarement consultés

2. **Assignez une priorité à chaque capteur:**

- Ajoutez une colonne "Priorité" (1, 2 ou 3)
- Vérifiez la cohérence des priorités par équipement

Étape 6: Documentation finale

1. **Création du tableau de suivi:**

- Fusionnez toutes les informations dans un document final avec:
 - ID unique du capteur
 - Nom et description
 - Type technique et protocole
 - Équipement et service associés
 - Vague de migration (1, 2 ou 3)
 - Commentaires et particularités

2. **Format recommandé:**

- Tableau Excel avec filtres avancés
- Colonnes colorées selon la priorité
- Feuilles séparées par catégorie technique

3. **Informations additionnelles à documenter:**

- Dépendances entre capteurs

- Notifications et alertes configurées
- Utilisateurs à notifier
- Procédures associées en cas d'alerte

Conseils pratiques pour la réussite du projet

1. Automatisez au maximum:

- Utilisez des formules Excel ou des scripts pour classer automatiquement les capteurs
- Envisagez d'utiliser l'API PRTG pour extraire des informations détaillées

2. Travaillez par échantillonnage:

- Commencez par classer un sous-ensemble représentatif
- Validez l'approche avant de traiter l'ensemble des capteurs

3. Documentez vos décisions:

- Notez les critères utilisés pour la classification
- Conservez une trace des capteurs supprimés ou fusionnés

4. Préparez la phase suivante:

- Identifiez les équivalences entre capteurs PRTG et sondes OpenNMS
- Documentez les paramètres spécifiques à configurer dans OpenNMS

SOUS TITRE 3 : correspondance : PRTG → OpenNMS

1. Objectif

Documentation détaillée de correspondance entre les anciens capteurs PRTG et les nouveaux capteurs OpenNMS, structurée en tableau et accompagnée d'explications pour chaque type de surveillance. Cela servira à migrer efficacement les capteurs lors du remplacement de PRTG par OpenNMS.

2. Tableau de correspondance : PRTG → OpenNMS

<i>Catégorie</i>	<i>Capteur PRTG</i>	<i>Capteur OpenNMS</i>	<i>Type de Surveillance</i>	<i>Remarques/Explica- tion</i>
ICMP (Ping)	Ping	ICMP	Disponibilité/Réactivité	Utilisé pour vérifier si un hôte est en ligne (temps de réponse).
HTTP/HTTPS	HTTP / HTTPS	HTTP Monitor (via http-collector ou http.xml)	Services Web	Permet de surveiller la disponibilité et le temps de réponse des sites Web.
CPU (Windows/Linux)	CPU Load	SNMP CPU Load (via snmp-graph.properties)	Ressources systèmes	Surveillance via SNMP, nécessite SNMP actif sur le périphérique.

Mémoire	Memory Usage	SNMP Memory (RAM)	Ressources systèmes	Surveillance de la RAM via SNMP.
Disques	Disk Free / Disk Usage	SNMP Disk Storage	Ressources systèmes	Surveillance de l'espace disque.
Interfaces réseau	Traffic In/Out, Errors	SNMP ifInOctets / ifOutOctets / ifErrors	Réseau / Bande passante	OpenNMS utilise les MIB SNMP standard pour les interfaces.
Services personnalisés	Port Sensor (TCP 80, 443, etc.)	TCP Monitor / Service Poller	Port TCP / service	Permet de tester l'ouverture et la réponse sur un port spécifique.
Serveurs DNS	DNS Sensor	DNS Monitor (via dns.xml)	Résolution de noms	Vérifie les réponses DNS pour un nom donné.
Serveurs DHCP	DHCP Sensor	DHCP Monitor (via dhcp.xml)	Attribution d'adresses IP	Vérifie la disponibilité d'un serveur DHCP.
SMTP/IMAP/POP3	Email Round Trip, SMTP, POP3, IMAP sensors	SMTP Monitor / Email Transport	Messagerie	Pour tester les flux de messagerie entrants et sortants.

VPN	VPN Tunnel, VPN Traffic	SNMP OID personnalisé ou Trap SNMP	Tunnel VPN	Surveillance dépend de l'équipement (pfSense, Cisco, etc.).
Traps SNMP	SNMP Trap Receiver	Trapd (OpenNMS)	Alertes SNMP	Permet de recevoir des événements SNMP envoyés par les équipements.
WiFi/AP	Number of Clients / Bandwidt h per AP	SNMP dot11StationCo unt / ifInOctets	Réseau sans fil	Utilisation des MIB SNMP pour AP (ex: Cisco, Aruba, UniFi).
Top Talkers	Top Talkers (NetFlow, sFlow)	OpenNMS Flow (via telemetryd, NetFlow v5/v9, sFlow)	Analyse de trafic réseau	Nécessite l'activation du module telemetryd.
Température	Hardware Sensor (Temp, Fan)	SNMP Sensor (Temp/Fan OIDs spécifiques)	Environnement matériel	Dépend des MIB propriétaires du fabricant.
Imprimantes	Printer Status, Toner Levels	SNMP Printer MIB	Imprimantes réseau	Utilisation de la MIB standard Printer-MIB.
Scripts/Custom	Script avancé (PowerSh	Script Monitor (via OMD/Nagios	Surveillance personnalisée	Peut être intégré via check_mk, NRPE, ou NSClient++.

	ell, Python)	plugin ou requis personnalisé)		
--	-----------------	--------------------------------------	--	--

Table 2: Correspondance PRTG-OpenNMS

3- Capteurs courants dans PRTG mais pas en natif dans OpenNMS

Capteur PRTG	Disponibilité dans OpenNMS	Commentaire / Équivalent possible
WMI Sensors (Windows Management Instrumentation)	✗ Pas en natif	OpenNMS ne supporte pas directement WMI ; il faut utiliser SNMP, NRPE ou des scripts.
VMware (SOAP/XML sensors)	⚠ Partiellement	Requiert une intégration manuelle (via VMware API, SNMP ou script REST).
Microsoft 365 Services (Teams, Outlook, OneDrive, etc.)	✗ Non disponible directement	Peut être supervisé via des scripts REST/API ou plugins Nagios.
Packet Sniffer / QoS Sensors	✗ Non pris en charge en natif	OpenNMS ne fait pas de sniffing de paquets, seulement NetFlow/sFlow avec telemetryd.
HTTP Full Web Page Sensor	✗ Pas d'équivalent complet	OpenNMS peut vérifier un HTTP mais pas toute la page avec ses composants.
Script Advanced Sensor (multi-output JSON/XML analysé automatiquement)	⚠ Possible manuellement	Nécessite l'écriture de scripts externes et parsing via collectd ou http-collector.

CloudWatch Sensor (AWS)	Pas intégré en standard	Nécessite un script ou un plugin externe via l'API AWS CloudWatch.
REST Custom Sensor	Possible	Doit être configuré via http-collector ou un script + RESTd.
Windows Updates Status	Pas en natif	Nécessite un script PowerShell + NSClient++ ou NRPE pour exporter l'état.

Table 3: capteurs courant dans PRTG mais pas natif dans OpenNMS

4. Méthodologie de migration

1. Inventaire des capteurs PRTG

- Exportez la configuration PRTG (Configuration.dat) ou utilisez l'interface pour lister les capteurs par hôte.
- Classez les capteurs par type : ICMP, SNMP, HTTP, etc.

2. Équivalence dans OpenNMS

- Identifiez les capteurs standard (ICMP, SNMP, HTTP) à migrer.
- Pour chaque type, vérifiez si OpenNMS dispose d'un monitor existant ou si une configuration XML est nécessaire (service-configuration, datacollection).

3. Ajout manuel si nécessaire

- Créez des service detectors ou modifiez les fichiers suivants :
 - /opt/opennms/etc/poller-configuration.xml
 - /opt/opennms/etc/datacollection/*.xml
 - /opt/opennms/etc/snmp-graph.properties

4. Test et validation

- Utilisez l'interface web OpenNMS pour vérifier :
 - Découverte des services sur chaque nœud.

- Graphiques de performance.
- Alertes générées (seuils).

5. Crédation de tableaux de bord

- Utilisez Grafana connecté à PostgreSQL ou opennms-performance, opennms-flow, opennms-entities :
 - Importer les panels (ICMP, CPU, Bande passante, etc.).
 - Créer des alertes visuelles (seuils rouges/verts).
 - Ajouter des variables dynamiques (\$node, \$service...).

5. Livrable final

Un fichier Excel/CSV avec les colonnes suivantes peut accompagner cette migration :

<i>Nom de l'équipement</i>	<i>Capteur PRTG</i>	<i>Capteur OpenNMS</i>	<i>Remarques techniques</i>
<i>Routeur Cisco HQ</i>	Ping, HTTP, CPU	ICMP, HTTP Monitor, SNMP	SNMP activé, template Cisco
<i>Serveur Web01</i>	HTTP, CPU, RAM	HTTP, SNMP CPU, SNMP RAM	Windows SNMP activé
<i>pfsense Firewall</i>	VPN, Traffic, Traps	SNMP VPN, Trapd	OID personnalisés, trap config

Table 4: Livrable final des capteurs configures

5. Remarques Supplémentaires

Les capteurs SNMP nécessitent que le protocole soit activé et configuré sur chaque hôte. Les configurations personnalisées peuvent être ajoutées via les fichiers XML d'OpenNMS ou via les extensions comme les scripts, les traps SNMP ou le module Flow.

TITRE 5 : configuration des nodes et services dans OpenNMS

SOUS TITRE 1 : Guide Technique : Configuration d'OpenNMS

Ce document fournit des instructions détaillées pour les différentes étapes de configuration d'OpenNMS mentionnées dans votre liste de tâches. OpenNMS est une plateforme de gestion de réseau open-source qui offre des outils pour surveiller et gérer les équipements et services réseau. Ce guide couvre les étapes suivantes : ajout des hôtes, configuration des services supervisés, ajout de nœuds, documentation des correspondances entre capteurs et configuration des permissions et alertes.

1. Ajouter les hôtes

Objectif :

Ajouter les hôtes qui ne s'affichent pas correctement dans OpenNMS après une recherche terminée.

Étapes :

1. Vérifier les hôtes non visibles :

- Accédez à l'interface utilisateur d'OpenNMS.
- Dans le menu principal, allez sur "Rechercher un hôte".
- Identifiez les hôtes qui ne sont pas affichés dans la liste des résultats.

2. Ajouter les hôtes manuellement :

- Allez dans l'onglet "Administration" > "Gérer les hôtes".
- Cliquez sur "Ajouter un nouvel hôte".
- Remplissez les informations suivantes :
 - Nom de l'hôte.

- Adresse IP.
- Services supervisés (voir section suivante).

3. Vérifications post-ajout :

- Assurez-vous que l'hôte ajouté apparaisse correctement dans la liste des nœuds.
- Effectuez un test de supervision.

2. Configurer les services supervisés (ping, SNMP, etc.)

Objectif :

Configurer la supervision des services comme le ping et SNMP pour chaque hôte.

Étapes :

1. Activer les services :

- Dans OpenNMS, allez sur "Administration" > "Gérer les services".
- Activez les services pertinents (ping, SNMP, HTTP, etc.).

2. Configurer le SNMP :

- Naviguez vers "Configuration SNMP".
- Ajoutez la communauté SNMP (par exemple, "public" ou celle configurée sur vos équipements).
- Testez la connectivité SNMP avec chaque hôte.

3. Vérifier les supervisions :

- Lancez une détection manuelle ou planifiez une détection automatique.
- Assurez-vous que les services supervisés remontent correctement dans l'interface utilisateur.

3. Ajouter des nœuds ("Nodes ajouté")

Objectif :

Ajouter de nouveaux nœuds au système de supervision.

Étapes :

1. Ajout manuel :

- Allez dans "Gérer les nœuds".
- Cliquez sur "Ajouter un nœud".
- Remplissez les informations requises :
 - Nom du nœud.
 - Adresse IP principale.
 - Groupe auquel le nœud appartient (facultatif).

2. Ajout via découverte automatique :

- Configurez une plage d'adresses IP pour la détection automatique dans "Administration" > "Paramètres de découverte".
- Laissez OpenNMS détecter et ajouter automatiquement les nouveaux nœuds.

3. Valider les nœuds :

- Vérifiez que les nœuds ajoutés apparaissent avec tous leurs services dans le tableau de bord.

4. Documenter la correspondance entre capteurs PRTG et OpenNMS

Objectif :

Documenter les correspondances entre les anciens capteurs de PRTG et les nouveaux capteurs d'OpenNMS.

Étapes :

- 1. Lister les capteurs PRTG existants :**
 - Exportez la liste des capteurs depuis l'interface de PRTG.
- 2. Identifier les équivalents OpenNMS :**
 - Comparez les capteurs avec les services offerts par OpenNMS.
 - Documentez les correspondances dans un tableau :
- 3. Mettre à jour la documentation :**
 - Ajoutez la documentation dans un fichier Excel ou dans un wiki d'entreprise.

5. Configuration des permissions

Objectif :

Configurer les permissions pour les utilisateurs et groupes dans OpenNMS.

Étapes :

- 1. Créer un utilisateur :**
 - Allez dans "Administration" > "Gérer les utilisateurs".
 - Cliquez sur "Ajouter un utilisateur".
 - Remplissez les détails (nom, e-mail, rôle).
- 2. Configurer les rôles :**
 - Définissez des rôles avec des permissions spécifiques (lecture seule, administrateur, etc.).
 - Attribuez les rôles aux utilisateurs créés.
- 3. Tester les permissions :**
 - Connectez-vous avec le nouveau compte utilisateur.

- Assurez-vous que les permissions fonctionnent comme prévu.

6. Configuration des alertes

Objectif :

Configurer les alertes pour surveiller les événements critiques.

Étapes :

1. Créer une alerte :

- Allez dans "Administration" > "Configurer les alertes".
- Créez une nouvelle alerte pour un événement spécifique (par exemple, échec du ping).

2. Configurer les destinataires :

- Définissez une liste de distribution pour les notifications.
- Ajoutez les adresses e-mail des destinataires.

3. Tester les alertes :

- Provoquez un événement pour tester l'alerte (par exemple, déconnectez un hôte supervisé).
- Vérifiez que les alertes sont correctement envoyées.

TITRE 5 : MISE EN PLACE DES ALERTES ET DES NOTIFICATIONS

SOUS TITRE 1 : Configuration pas-à-pas des alertes dans OpenNMS Horizon

1. Préambule : Comprendre les composants d'alerte

OpenNMS repose sur 4 piliers pour la gestion des alertes :

- **Événements (UEI)** : identifiants uniques d'événements (ex. perte de ping)
- **Seuils (Thresholds)** : conditions sur des métriques (CPU, mémoire, etc.)
- **Pollers** : testent la disponibilité des services (ICMP, HTTP...)
- **Notifications** : transmettent les alertes (email, SMS, webhook)

2. Configuration des seuils (thresholds)

2.1 Via l'interface Web :

- Aller dans **Admin → Configure Thresholds**
- Éditer un groupe de seuils existant (ex : netsnmp) ou créer un nouveau
- Cliquer sur **Create New Threshold**
- Remplir :
 - Type : high, low, relative...
 - Datasource : ex. hrProcessorLoad
 - Value et Rearm
 - Trigger : nb d'occurrences avant alerte

- UEI personnalisé (facultatif)
- Description
- Sauvegarder et recharger la config si besoin

2.2 Seuils avancés :

- Seuils d'expression (calculs comme taux d'utilisation disque)
- Exemple : $100 - (\$\{memAvailReal\} * 100 / \$\{memTotalReal\})$ pour % RAM utilisée

3. Association des seuils aux ressources

- Fichier **threshd-configuration.xml** : associe des groupes de seuils à des paquets (nœuds)
- Filtres au sein des seuils possibles : ex. ifName = GigabitEthernet0/1
- Les pollers (ICMP/HTTP) sont configurés dans poller-configuration.xml avec retry/timeout

4. Création de notifications

4.1 Définir les destinataires

- Menu **Admin > Configure Users/Groups**
- Créer un chemin : **Configure Destination Paths**
 - Ajouter utilisateurs/groupes
 - Choisir la commande : javaEmail, sms, snmpTrap...

4.2 Crée la notification

- Aller dans **Configure Event Notifications**
- Cliquer sur **Add New Event Notification**
- Sélectionner l'Événement (UEI)

- (Option) Ajouter une règle de filtrage
- Associer le chemin de notification
- Rédiger le message (avec macros : %nodeLabel%, %parm[value]%, etc.)
- Activer la notification

5. Tests et validation

- Provoquer une alerte (stress CPU, déconnexion)
- Observer les événements et alarmes
- Tester l'envoi de notifications
- Simulation possible via send-event.pl

6. Intégration Grafana

- Installer Grafana + plugin Helm
- Ajouter les datasources : Performance, Alarms, Entities...
- Créer des panels pour :
 - Alertes actives
 - Métriques CPU/RAM avec ligne de seuil
 - Taux de disponibilité (SLA)

7. Bonnes pratiques

- Prioriser les alertes critiques (disponibilité, sécurité, SLA)
- Documenter les seuils et actions
- Prévoir des tests réguliers et une rotation d'astreinte

- Exploiter les fichiers XML pour aller plus loin : thresholds.xml, notifications.xml, eventconf.xml

SOUS TITRE 2 : Implémentation de la notification automatique dans Grafana pour OpenNMS

Implémentation dans Grafana pour OpenNMS : Notification automatique en cas d'absence de réponse

Dans le contexte de la surveillance des infrastructures réseau, OpenNMS est une solution puissante de gestion de réseau qui, une fois intégrée avec Grafana, offre une plateforme visuelle robuste pour l'analyse et la gestion des alertes. Cependant, un enjeu majeur dans les opérations de supervision est la prise en charge automatique et rapide des alertes critiques.

L'objectif de ce document est d'expliquer comment implémenter dans Grafana une procédure de notification automatique qui, en cas d'absence de réaction à une alerte OpenNMS après un délai défini (par exemple, X minutes), déclenche l'envoi d'une notification à un superviseur.

1. Contexte et besoins

Dans un système de gestion réseau, lorsque OpenNMS détecte un problème (par exemple, un équipement en panne ou une dégradation de service), une alerte est générée. Cette alerte est visible via Grafana, qui peut aussi servir pour le suivi en temps réel. Cependant, si les équipes responsables ne répondent pas ou n'interviennent pas rapidement, le risque d'impact s'accroît.

Afin d'éviter ces situations, il est crucial de mettre en place un mécanisme de suivi temporel des alertes et d'escalade automatique. En pratique, cela revient à :

- Définir un délai de réponse maximal (par exemple, X minutes).
- Contrôler que l'alerte ait bien été prise en compte dans ce délai.
- Si aucune action ou accusé de réception n'est détecté, envoyer une notification à un niveau de supervision supérieur.

2. Architecture de la solution proposée

La solution combine trois éléments essentiels :

1. OpenNMS qui détecte et génère les alertes.
2. Grafana qui affiche les alertes sous forme de tableaux de bord interactifs.
3. Un système d'automatisation et de notification qui surveille le délai de réponse et effectue l'escalade.

Grafana, via l'utilisation des alert rules et des webhooks, peut déclencher des actions à partir de conditions spécifiques. L'idée est d'exploiter ces capacités pour détecter les alertes ouvertes depuis plus de X minutes.

3. Étapes d'implémentation

3.1. Configuration des alertes dans OpenNMS

OpenNMS génère normalement des événements qui peuvent être transformés en alertes via son moteur de règles internes. Assurez-vous que les alertes que vous souhaitez superviser soient bien configurées et remontées vers Grafana.

3.2. Intégration d'OpenNMS avec Grafana

- Utiliser un connecteur ou un plugin compatible qui expose les données d'OpenNMS vers Grafana (API REST, bases de données, etc.).
- Créer un dashboard Grafana affichant l'état des alertes en temps réel. Par exemple, un tableau listant les alertes ouvertes avec leur date/heure de création.

3.3. Mise en place d'une alerte Grafana sur le délai de réponse

- Définir une règle d'alerte Grafana qui se déclenche quand une alerte est ouverte depuis plus de X minutes sans réponse.
- Pour cela, il faut que la source de données (OpenNMS ou base intermédiaire) puisse fournir la date/heure de création et éventuellement le statut de prise en charge.
- Cette alerte Grafana sera appelée, par exemple, Alerta en attente de gestion.

3.4. Configuration de la notification et de l'escalade automatique

- Dans Grafana, la règle d'alerte précédente doit être associée à une notification, par exemple via un webhook, un email, ou via un outil de messagerie interne (Slack, Microsoft Teams, etc.).
- Ce canal de notification sera celui du supérieur hiérarchique ou du responsable escalation.

- Il est possible d'utiliser des outils d'automatisation externes (comme Zapier, n8n, ou un script personnalisé) qui reçoivent la notification webhook et déclenchent l'envoi du message au bon destinataire.

4. Exemple d'implémentation pratique

Supposons qu'une alerte OpenNMS apparaisse lorsqu'un serveur est inaccessible. Cette alerte est visible dans Grafana dans un tableau des alertes ouvertes. La date de création est stockée.

On définit dans Grafana une alerte avec la requête suivante (exemple générique) :

```
SELECT alert_id, create_time, status  
FROM alerts  
WHERE status = 'open' AND TIMESTAMPDIFF(MINUTE, create_time, NOW()) > X
```

Cette alerte devient active dès que la condition est vraie, c'est-à-dire qu'une alerte est toujours ouverte depuis plus de X minutes.

Quand cette alerte déclenche, Grafana envoie un webhook vers un serveur d'automatisation qui enverra un email ou un message instantané au supérieur.

5. Bonnes pratiques

- Définissez un délai réaliste : Le temps X doit être choisi en fonction de la criticité et des processus internes.
- Testez régulièrement vos alertes : Assurez-vous qu'elles se déclenchent correctement et que les notifications arrivent bien aux bonnes personnes.
- Prévoyez un accusé de réception : Pour un suivi optimal, intégrez une étape de confirmation de prise en charge de l'alerte par la personne notifiée.
- Documentez le processus : Tous les acteurs doivent connaître le fonctionnement du système d'escalade.

6. Conclusion

La mise en place d'une notification automatique d'escalade dans Grafana, en s'appuyant sur les alertes d'OpenNMS, permet d'améliorer significativement la réactivité dans le traitement des incidents réseau. La gestion du délai de réponse et la capacité à notifier un supérieur en cas

d'absence de réaction sont des leviers importants pour assurer la continuité et la qualité de service.

En suivant les étapes présentées, il est possible de configurer un système flexible, automatisé et adapté aux besoins opérationnels, tout en tirant parti des fonctionnalités avancées de Grafana et OpenNMS.

TITRE 5 : Création structurée des utilisateurs dans Windows Server 2019 avec Active Directory et bonnes pratiques

SOUS TITRE 1 : Windows server 2019

Objectif

Configurer un environnement Active Directory pour la gestion des utilisateurs dans le cadre du projet CCNB Groupe 2 (OpenNMS / Grafana), en respectant les bonnes pratiques :

- Préfixe des comptes utilisateurs (usr-)
- Organisation par Unités d'Organisation (OU)
- Application de politiques de mot de passe (GPO)
- Documentation traçable

1. Installer Active Directory Domain Services (AD DS)

1. Ouvrir **Server Manager > Add Roles and Features**
2. Choisir **Role-based or feature-based installation**
3. Sélectionner le serveur local
4. Cocher **Active Directory Domain Services** > Suivant jusqu'à l'installation

2. Promouvoir le serveur en contrôleur de domaine

1. Une fois AD DS installé, cliquer sur **Promote this server to a domain controller**
2. Choisir **Add a new forest** > Nom du domaine : ccnb.local

3. Configurer le mot de passe du mode restauration DSRM
4. Suivant jusqu'à **Install**
5. Redémarrer le serveur

3. Plan de création des Unités d'Organisation (OU)

Groupe projet	Nom de l'OU	Utilisateurs	Mots de passes
Monitoring	OU=OpenNMS	usr-opnms01, usr-opnms02	!@OpenNMS123, !@OpenNMS456
Analyse	OU=Grafana	usr-graf01, usr-graf02	!@Grafana123, !@Grafana456
Admin	OU=Admin	usr-admin01	!@Admin123 !@Admin456

Table 5: Unité d'organisation

4. Créer les OU

1. Aller dans **Server Manager > Tools > Active Directory Users and Computers**
2. Clic droit sur le domaine ccnb.local > **New > Organizational Unit**
3. Créer : OpenNMS, Grafana, Admin

5. Création des comptes utilisateurs AD

1. Clic droit sur une OU > **New > User**
2. Nom: usr-opnms01
3. Mot de passe : Cyber2024!@ (modifiable au 1er logon)

4. Refaire pour chaque utilisateur projet

6. Appliquer une politique de mot de passe via GPO

1. Ouvrir **Group Policy Management**
2. Créer une GPO : GPO_Password_Policy
3. Éditer :
 - o Minimum password length : 8
 - o Password complexity : Enabled
 - o Maximum password age : 30 jours
 - o Minimum password age : 1 jour
4. Lier la GPO à chaque OU :
 - o Clic droit sur l'OU > **Link an existing GPO** > Choisir GPO_Password_Policy

6. Documentation des utilisateurs créés

Nom utilisateur	OU	Rôle	Date création
usr-opnms01	OpenNMS	Superviseur	2024-05-23
usr-graf01	Grafana	Analyste	2024-05-23
usr-admin01	Admin	Admin Général	2024-05-23

Table 6: Utilisateurs créés

SOUS TITRE 2 : Bonnes pratiques de sécurité Active Directory et supervision Windows (Projet OpenNMS/Grafana)

Objectif

Mettre en place un environnement sécurisé pour l'utilisation d'Active Directory dans le cadre de la supervision Windows avec OpenNMS et Grafana. Cela inclut la configuration des GPO de sécurité, les droits d'accès, les comptes techniques, l'audit, et les paramètres de connectivité compatibles supervision (WinRM/WMI).

1. Politique de verrouillage de compte (protection contre force brute)

1. Aller dans **Group Policy Management** > Clic droit sur la GPO (ex: **GPO_Password_Policy**) > **Edit**
2. Naviguer vers :
 - o **Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Account Lockout Policy**
3. Configurer :
 - o **Account lockout threshold** : 5 tentatives
 - o **Account lockout duration** : 15 minutes
 - o **Reset account lockout counter after** : 10 minutes

2. Restriction des connexions RDP (Bureau à distance)

Empêche les utilisateurs standards d'accéder en RDP sauf autorisation explicite.

1. Aller dans la même GPO >
2. **Computer Configuration > Policies > Windows Settings > Security Settings > User Rights Assignment**

3. Modifier :
 - **Allow log on through Remote Desktop Services** : ajouter uniquement Administrators, usr-admin01, ou groupe spécifique

3. Activation de l'audit des connexions et accès (journalisation)

1. Dans GPO >
2. **Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies**
3. Activer :
 - **Logon/Logoff** > Audit logon : Success, Failure
 - **Account Logon** > Audit credential validation : Success, Failure
 - **Object Access** > Audit file share : Success, Failure

4. Configuration de WinRM pour la supervision OpenNMS

1. Sur chaque machine Windows à superviser :
2. Enable-PSRemoting -Force
3. winrm quickconfig
4. Set-Item WSMan:\localhost\Service\AllowUnencrypted -Value true
5. Set-Item WSMan:\localhost\Service\Auth\Basic -Value true
6. Ouvrir les ports sur le pare-feu Windows :
 - 7. New-NetFirewallRule -Name "WinRM_HTTP" -DisplayName "WinRM via HTTP" -Protocol TCP -LocalPort 5985 -Action Allow
 - 8. New-NetFirewallRule -Name "RPC" -DisplayName "RPC" -Protocol TCP -LocalPort 135 -Action Allow

5. Création d'un compte technique pour la supervision

1. Créer un utilisateur : **usr-opennms-agent**
2. L'ajouter aux groupes :
 - o Performance Monitor Users
 - o Distributed COM Users
3. Ne pas donner d'accès RDP à ce compte (cf. section 2)
4. Utiliser ce compte dans OpenNMS pour la supervision Windows (WMI/WinRM)

6. Bonnes pratiques complémentaires

- Renommer le compte **Administrateur** par défaut
- Désactiver le compte **Guest**
- Mettre en place un suivi **Sysmon + Wazuh** si nécessaire
- Sauvegarder régulièrement les GPO avec Backup-GPO
- Tester les GPO avec gpresult /h et rsop.msc

TITRE 6 : Configuration Avancée des Capteurs et des tableaux de bords dans OpenNMS/Grafana

Sous Titre 1 : Configuration des capteurs

Cette section détaille les étapes nécessaires pour configurer la supervision des équipements du réseau dans OpenNMS, notamment pfSense, Windows Server et d'autres hôtes. Chaque étape inclut les commandes, les justifications techniques et les bonnes pratiques à suivre.

Étape 1 : Ajouter les hôtes à superviser

Objectif : Intégrer les équipements réseau et serveurs dans OpenNMS afin d'activer leur supervision.

Hôtes cibles :

- pfSense (192.168.1.1)
- Windows Server 2019 (ex: 192.168.1.105)
- Autres VMs ou équipements selon l'inventaire

Procédure :

1. Accéder à l'interface Web d'OpenNMS via <http://192.168.1.104:8680>
2. Naviguer vers "Admin > Provisioning Requisitions"
3. Créer une nouvelle "Requisition" (ex: CCNB-LAN)
4. Ajouter un nouvel élément (node) avec les informations suivantes :
 - o Nom : pfSense / WindowsServer
 - o Adresse IP : ex. 192.168.1.1
 - o Catégories : firewall, serveur, etc.
 - o Services à détecter : cocher "Enable SNMP" si activé
5. Sauvegarder et déployer la Requisition

Justification :

- Cette méthode permet de gérer les hôtes dynamiquement par lots.
- La catégorisation aide à filtrer les équipements par type (serveur, pare-feu, etc.).

Étape 2 : Activer les capteurs ICMP, SNMP, HTTP, SSH, etc.

Objectif : Activer la détection et la surveillance des services standards sur chaque hôte.

Prérequis sur les hôtes :

A- SNMP : doit être installé et configuré (surtout sur pfSense).

1. SNMP – Installation et Configuration sur pfSense :

- Accéder à l'interface Web de pfSense (<http://192.168.1.1>)
- Aller dans : Services > SNMP
- Activer le service SNMP
- Configurer :

Community string : public (à modifier en production pour la sécurité), Contact, location : remplir selon votre environnement. Interfaces surveillées : toutes ou spécifiques (LAN/WAN)

- Sauvegarder, puis redémarrer le service SNMP

Justification : SNMP est essentiel pour collecter des métriques réseau et système (trafic, CPU, mémoire).

B- HTTP/SSH : les ports doivent être ouverts sur le pare-feu pfSense.

- Accéder à pfSense > Firewall > Rules > LAN
- Ajouter une règle pour chaque protocole à autoriser depuis OpenNMS (192.168.1.104) :

Exemple : autoriser ICMP (ping)

- Action : Pass

- Interface : LAN
- Protocol : ICMP
- Source : 192.168.1.104
- Destination : any
- Description : Autoriser ICMP depuis OpenNMS

Exemple : autoriser HTTP

- Protocol : TCP
- Destination Port : 80

Exemple : autoriser SSH

- Protocol : TCP
- Destination Port : 22

Justification :

- L'ouverture sélective améliore la sécurité tout en permettant la supervision.
- Limiter les accès au réseau local empêche des connexions externes non autorisées.

Vérification des services :

Depuis le terminal Ubuntu/OpenNMS, lancer :

`nmap -sS -sU -T4 192.168.1.1`

Cela permet d'identifier les ports/services actifs.

Dans OpenNMS :

1. Menu "Node List" > sélectionner un hôte
2. Cliquer sur "Services" > Vérifier les services détectés :
 - ICMP (ping)
 - SNMP (161/UDP)

- HTTP (80) / HTTPS (443)
- SSH (22)

3. Si absent, ajouter manuellement les services via le fichier XML

</opt/opennms/etc/serviceconfiguration.xml>

Ajout manuel des services via fichier XML

Chemin : </opt/opennms/etc/service-configuration.xml>

Étapes :

1. Ouvrir le fichier avec des privilèges administrateur :

Sudo nano /opt/opennms/etc/service-configuration.xml

2. Rechercher la balise <package name="example"> ou créer un bloc pour votre nœud.

3. Ajouter un bloc service correspondant, par exemple :

```
<service name="SSH" interval="300000" user-defined="true">  
  <filter>IPADDR != '0.0.0.0'</filter>  
  <parameter key="port" value="22"/>  
</service>
```

4. Sauvegarder et quitter

5. Redémarrer OpenNMS pour prendre en compte les changements :

sudo systemctl restart opennms

Justification :

- OpenNMS découvre automatiquement les services standards, mais une configuration manuelle permet d'ajouter des services personnalisés.
- Le monitoring multi-protocole (ICMP + SNMP + HTTP) augmente la fiabilité des alertes.

Étape 3 : Configurer les seuils de disponibilité, alertes et SLA

Objectif : Définir les seuils critiques pour déclencher des alertes et assurer la qualité de service (SLA).

Configuration des seuils :

Accéder à l'interface Web OpenNMS : <http://192.168.1.104:8680>

1. Accéder à : Admin > Thresholds
2. Choisir le type de ressource (interface, mémoire, CPU, etc.)
3. Définir un seuil d'alerte (Warning) et un seuil critique (Critical)
 - Ex : CPU > 70% = Warning / > 90% = Critical

Cliquer sur "Add New Threshold Group" pour créer un nouveau groupe.

4. Cliquer sur "Add Threshold" puis remplir les champs :

- Resource Filter : par exemple nodeLabel =~ ".*pfSense.*"
- DS (Data Source) : CPU, memUsed, etc.
- Type : High Threshold
- Value : 70 (pour Warning), puis 90 (pour Critical)
- Trigger : >= Re-arm : 60 (valeur de retour à la normale)

Justification : Cette configuration permet de détecter les anomalies de performance avant

qu'elles ne deviennent critiques, pour une action proactive.

Commande alternative (modification manuelle) : Les seuils sont configurés dans le fichier

XML :

```
sudo nano /opt/opennms/etc/thresholds.xml
```

Ajouter un bloc :

```
<group name="cpu-threshold">
```

```
<threshold type="high" ds-type="ifAlias" ds-name="cpu" value="90" rearm="60"
trigger="greaterthanorequal" />
</group>
```

Redémarrer OpenNMS :

```
sudo systemctl restart opennms
```

5. Associer le seuil à une catégorie de nœuds

Configuration SLA (Service Level Agreement) :

1. Accéder à : Admin > SLA Configurations

2. Cliquer sur "Add New SLA Configuration"

3. Remplir les champs suivants :

- Nom : SLA_pfSense
- Période de mesure : 30 jours (ou 1 an)
- Objectif : 99.5 %
- Services inclus : ICMP, HTTP, SNMP, SSH
- Nœuds concernés : sélection via label ou IP (ex. 192.168.1.1)

4. Sauvegarder la configuration

Justification : Le SLA permet de formaliser les engagements de disponibilité des services critiques, et de suivre leur conformité.

Définir les notifications :

1. Menu : Admin > Notifications > Configure Notifications

> New Notification

1. Remplir les champs :

- Name : Alerte_NodeDown
- Event UEI : uei.opennms.org/nodes/nodeDown

- Text de l'alerte : Le nœud %nodeLabel% est injoignable.
- Group : Administrateurs ou définir un contact email : admin@ccnb.ca
- Medium : Email

2. Configurer la fenêtre horaire (optionnel)

3. Sauvegarder

2. Tester la notification

3. Simuler une panne d'un nœud supervisé :

1. Éteindre ou mettre en pause une machine virtuelle supervisée (ex. Windows Server).

2. Alternativement, bloquer temporairement le trafic ICMP (ping) ou SNMP à l'aide de règles pfSense.

4. Observer les résultats dans OpenNMS :

1. Accéder au tableau de bord d'OpenNMS.

2. Vérifier que le nœud apparaît comme "Down" ou "Unavailable".

3. Aller dans "Alarms" pour voir l'alerte générée.

5. Vérifier la réception de l'alerte par courriel :

1. Confirmer que le message est bien reçu à l'adresse définie (ex. admin@ccnb.ca).

2. Vérifier le format du message, la précision de l'information (nom du nœud, heure de l'incident).

6. Réactiver le nœud ou lever la simulation :

1. Redémarrer la VM ou rétablir la connectivité réseau.

2. Observer le retour à l'état "Up" dans OpenNMS et la levée de l'alerte.

Justification :

- La configuration des seuils permet une supervision proactive avant incident critique.
- Les SLA garantissent que les équipements critiques répondent aux engagements de service.
- Les notifications assurent une réactivité rapide de l'équipe TI.

Conclusion

La configuration avancée des capteurs dans OpenNMS permet de superviser efficacement les équipements critiques comme pfSense et Windows Server. Elle offre une visibilité en temps réel sur la disponibilité des services, la performance des systèmes et les incidents réseau. Une configuration rigoureuse des seuils et des alertes garantit une réponse rapide aux pannes et renforce la fiabilité du système d'information supervisé.

SOUS TITRE 2 : Création des Tableaux de Bords dans Grafana

1. Qu'est-ce que Grafana ?

Grafana est une plateforme open source de visualisation et d'analyse de données. Elle permet de créer des tableaux de bord dynamiques et interactifs pour surveiller des métriques, des logs, et des événements issus de différentes sources de données. Utilisé massivement dans les domaines du DevOps, de la cybersécurité, de l'IoT ou encore du monitoring réseau, Grafana est un outil puissant pour centraliser les données et faciliter leur interprétation visuelle.

2. Fonctionnement général

Grafana se connecte à de nombreuses sources de données telles que :

- Prometheus
- InfluxDB
- Elasticsearch
- MySQL/PostgreSQL
- Loki (pour les logs)
- Azure Monitor, Google Cloud, AWS CloudWatch, etc.

Il interroge ces sources via des requêtes personnalisées, puis affiche les résultats sous forme de graphiques, jauge, cartes, histogrammes, tableaux ou diagrammes personnalisés.

3. Tableaux de Bord : Définition et Structure

Un tableau de bord Grafana (ou dashboard) est un ensemble de visualisations regroupées dans une interface. Chaque tableau peut contenir plusieurs panels (ou panneaux), chacun représentant un graphique ou un élément visuel spécifique.

Composants d'un tableau de bord :

Panels : visualisations (courbes, barres, jauge, etc.)

Variables : valeurs dynamiques utilisées dans les requêtes

Templates : modèles pour générer des dashboards dynamiques

Alertes : pour générer des notifications en cas de dépassement de seuils

Filtres de temps : permettent d'explorer des plages temporelles spécifiques

4. Création d'un Tableau de Bord

Étapes de base :

Connexion à une source de données dans Grafana.

Création d'un nouveau tableau de bord.

Ajout d'un panel (choix du type de visualisation).

Écriture d'une requête selon le moteur de la base de données.

Personnalisation de la visualisation (couleurs, titres, légendes).

Enregistrement et partage du tableau de bord.

7. Types de Tableaux de Bords

Dashboards techniques (Monitoring IT / DevOps)

Infrastructure Monitoring : pour surveiller des serveurs, CPU, mémoire, disque, réseau.

Application Monitoring : performance des applications, erreurs, latence.

Conteneurs et Kubernetes : état des pods, déploiements, services, etc.

Logs : pour analyser les logs centralisés.

Dashboards de performance système

Bases de données : requêtes lentes, connexions, tailles.

Web Services / API : temps de réponse, taux d'erreur, appels/minute.

Proxys : trafic, disponibilité, erreurs.

Dashboards analytiques / métier

Business Intelligence : KPIs, ventes, utilisateurs actifs, revenus, etc.

IoT / capteurs industriels : température, pression, états, événements.

Dashboards de sécurité / cybersécurité

Détection d'intrusion : alertes IDS/IPS, trafic suspect, ports scannés.

Audit d'accès : tentatives de connexions, authentifications échouées, logs système.

Dashboards temps réel

Pour afficher des données à haute fréquence (capteurs, trading, logs en direct, etc.).

6. Cas d'usage typiques

Surveillance de systèmes informatiques : CPU, mémoire, espace disque.

Monitoring de services web : temps de réponse, erreurs, charge serveur.

Visualisation des journaux d'événements (logs) : avec Loki ou Elastic.

Suivi de la sécurité : détection d'anomalies, alertes SIEM.

Analyse réseau : trafic, latence, paquets anormaux.

7. Alertes et Notifications

Grafana permet de configurer des alertes basées sur des seuils prédéfinis. Ces alertes peuvent être envoyées par :

- Courriel
- Slack
- Microsoft Teams
- Webhooks
- PagerDuty, Opsgenie, etc.

Chaque alerte est associée à une requête et peut être déclenchée si certaines conditions sont remplies.

8. Bonnes pratiques

1. Utiliser les variables pour rendre les tableaux de bord dynamiques et réutilisables.
2. Limiter le nombre de panels par tableau pour garantir la lisibilité.
3. Nommer clairement les panels et dashboards pour faciliter la maintenance.
4. Sauvegarder régulièrement les tableaux de bord ou les exporter en JSON.
5. Configurer des droits d'accès selon les rôles (lecture seule, édition).

SOUS titre 3 : Présentation des différents types de dashboards OpenNMS et leurs fonctionnalités

Cette documentation présente les différents types de dashboards issus d'OpenNMS, illustrés dans l'image fournie. Chaque dashboard a une vocation spécifique pour la supervision réseau, l'analyse de performance ou la gestion des incidents.

1. OpenNMS Basic SNMP Data

Ce dashboard affiche les métriques de performance collectées via SNMP (Simple Network Management Protocol). Il permet de visualiser des indicateurs clés tels que la bande passante, l'utilisation CPU, la mémoire, etc., sur les équipements réseau surveillés. Il est particulièrement utile pour obtenir une vue d'ensemble rapide de la santé des équipements et identifier les tendances ou anomalies de performance.

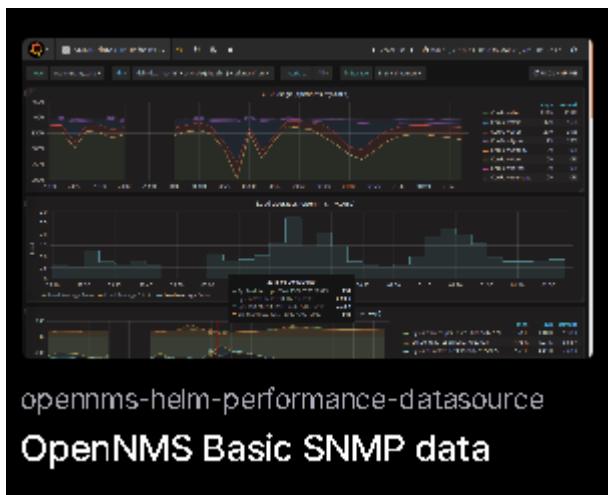


Figure 32: exemple de tableau de bord

2. APC UPS Stats

Ce dashboard est conçu pour le suivi des onduleurs APC. Il présente des statistiques détaillées comme le niveau de charge de la batterie, le temps restant, la charge supportée, l'état des unités,

la température, la tension d'entrée/sortie et la santé des batteries. Il nécessite une collecte SNMP adaptée pour récupérer ces données spécifiques.

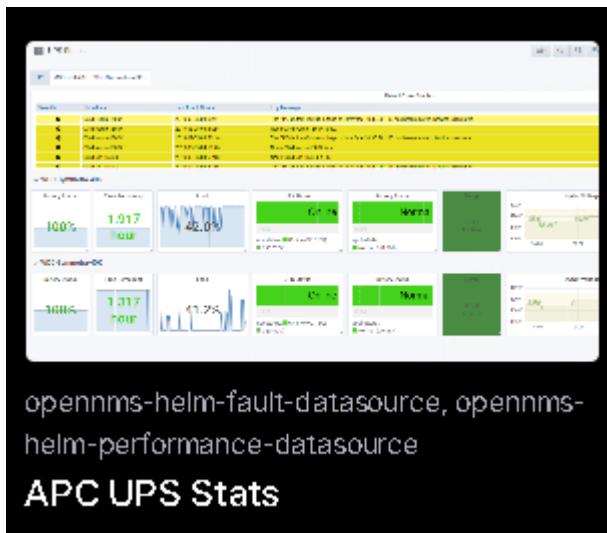


Figure 33: APC UPS Stats

3. OpenNMS Network Interfaces Report

Ce rapport propose une vue détaillée des interfaces réseau surveillées. Il affiche des métriques telles que le trafic entrant/sortant, les erreurs, les taux d'utilisation, permettant d'identifier rapidement les interfaces problématiques ou saturées.

4. OpenNMS World Map Example

Ce dashboard visualise les métriques des nœuds OpenNMS sur une carte du monde. Il utilise le plugin « Grafana Worldmap Panel » et nécessite de renseigner les coordonnées géographiques (longitude/latitude) des équipements. Cela permet de localiser visuellement les incidents ou les performances sur une base géographique, facilitant la gestion multi-sites.

5. OpenNMS Outage Dashboard

Ce dashboard synthétise les pannes en cours sur le réseau. Il affiche pour chaque nœud :

Le nom du nœud concerné

Le nombre de services impactés

La disponibilité sur les dernières 24 heures

Il permet d'avoir une vision claire des interruptions de service et de prioriser les interventions.

5. OpenNMS Outage Wallboard

Le Wallboard est une vue synthétique et visuelle des pannes et incidents, souvent utilisée sur de grands écrans en salle de supervision. Il affiche :

Le nombre total d'incidents en cours

Leur répartition par gravité ou type

Des indicateurs de performance globaux (disponibilité, nombre d'alarmes, etc.)

Cela aide les équipes à réagir rapidement aux incidents majeurs.

7. OpenNMS ActiveMQ

Ce dashboard est dédié à la surveillance des brokers ActiveMQ. Il présente des métriques telles que le nombre de messages en file d'attente, le taux de consommation, l'état des connexions, etc. Il est essentiel pour garantir la fluidité des échanges de messages dans les architectures distribuées.

8. OpenNMS JVM Metrics

Ce dashboard affiche les métriques JVM (Java Virtual Machine) pour les applications surveillées, telles que :

L'utilisation du heap

Le nombre de threads

Les temps de pause du garbage collector

Il permet de diagnostiquer les problèmes de performance ou de fuite mémoire des applications Java.

9. OpenNMS Linux Node Performance (multirow)

Ce dashboard propose une vue multi-graphique des performances d'un nœud Linux. On y retrouve généralement :

L'utilisation CPU

L'utilisation mémoire

Les I/O disques

Les métriques réseau

Il est conçu pour fournir une vue complète et rapide de la santé d'un serveur Linux.

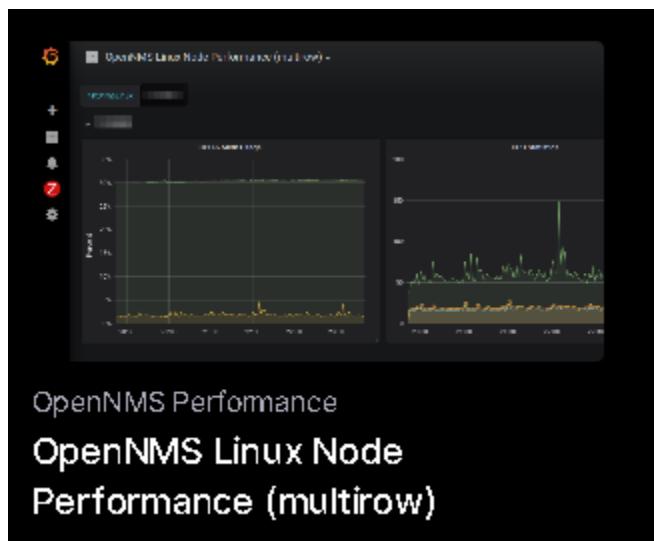


Figure 34: OpenNMS Performance

TITRE 7 : Plan de Sécurisation du Serveur – OpenNMS + Grafana

SOUS TITRE 2 : Sécurisation du Serveur – OpenNMS + Grafana

1. Introduction

Ce document détaille les mesures de sécurisation mises en œuvre ainsi que les recommandations Complémentaires pour un serveur Ubuntu 22.04 hébergeant les services OpenNMS et Grafana. L'objectif est de renforcer la sécurité selon les bonnes pratiques issues des normes reconnues Telles que CIS Benchmarks, NIST SP 800-53 et ISO/IEC 27001.

2. Sécurisation Initiale Mise en Place

2.1 Gestion des Accès Administratifs

- Modification des mots de passe par défaut sur OpenNMS et Grafana
- Création de comptes utilisateurs avec privilèges minimaux nécessaires
- Activation de mots de passe forts et suppression des comptes inactifs

2.2 Sécurisation de Grafana

Étapes appliquées pour renforcer la sécurité de l'accès à Grafana :

1. Changement du mot de passe administrateur par défaut à la première connexion
2. Création de comptes utilisateur avec rôles (Viewer, Editor, Admin) adaptés
3. Restriction du port 3000 aux IP autorisées avec UFW
4. Activation du HTTPS via certificat auto-signé ou Let's Encrypt
5. Activation de la journalisation des accès dans grafana.ini
6. Surveillance des logs via : sudo tail -f /var/log/grafana/grafana.log

2.3 Configuration du Pare-feu (UFW)

- Activation d'UFW : sudo ufw enable
- Autorisation des ports nécessaires uniquement :
 - 22/tcp : SSH (accès sécurisé)
 - 8980/tcp : OpenNMS Web
 - 3000/tcp : Grafana Web
 - ICMP, SNMP, HTTP pour supervision

GROUPE2 2

- Blocage de tous les autres ports
- Règles d'accès restrictives appliquées par IP source

2.4 Journalisation et Surveillance

- Activation des logs d'accès et tentatives d'authentification
- Configuration pour future intégration avec un IDS/IPS
- Alerte en cas d'échecs d'authentification

3. Recommandations Complémentaires

3.1 Mise à jour Automatisée du Système

- Mise à jour régulière : sudo apt update && sudo apt upgrade
- Installation d'unattended-upgrades pour automatisation

3.2 Désactivation des Services Inutiles

- Vérification des services : systemctl list-units --type=service
- Désactivation de ceux non nécessaires

3.3 Renforcement de SSH

- Changement du port par défaut (22) dans /etc/ssh/sshd_config

- Interdiction de la connexion root : PermitRootLogin no
- Authentification par clé SSH recommandée
- Installation de fail2ban pour bloquer les IPs malveillantes

3.4 Intégrité et Audit

- Installation et configuration de auditd
- Surveillance de fichiers critiques : /etc/passwd, /etc/shadow, etc.

3.5 Gestion des Droits et Permissions

- Application du principe du moindre privilège
- Supervision de l'usage de sudo avec journalisation
- Vérification des permissions systèmes avec find / -perm -2 -type f

3.6 Sécurisation HTTPS des Interfaces Web

- Forçage de l'utilisation de HTTPS
- Utilisation de certificats SSL/TLS valides
- Restriction d'accès par VPN ou par filtrage IP

GROUPE2 3

3.7 Sauvegarde et Restauration

- Mise en place de sauvegardes régulières : configurations, BDD, journaux
- Vérification périodique des procédures de restauration

3.8 Contrôle des Ports Réseau

- Scan des ports : nmap, netstat
- Fermeture des ports non utilisés via UFW

3.9 Supervision de l'Intégrité des Fichiers

- Utilisation d'AIDE pour détecter toute modification de fichiers critiques
- Comparaison régulière avec la base d'intégrité générée

3.10 Journalisation Centralisée

- Redirection des logs vers une solution SIEM (Grafana Loki, ELK, Wazuh)
- Utilisation de rsyslog pour agréger les journaux distants

Étape 1 : Mettre à jour les paquets du système

Commande : sudo apt update && sudo apt upgrade -y

Étape 2 : Installer le gestionnaire de mises à jour automatiques

Commande : sudo apt install unattended-upgrades

Étape 3 : Configurer l'exécution automatique

Commande : sudo dpkg-reconfigure --priority=low unattended-upgrades

Étape 1 : Lister les services en cours

Commande : systemctl list-units --type=service

Étape 2 : Désactiver les services inutiles

Commande : sudo systemctl disable <nom_du_service>

Sudo

Étape 2 : Redémarrer le service SSH

Commande : sudo systemctl restart ssh

GROUPE2 4

Étape 3 : Installer Fail2ban pour bloquer les IPs malveillantes

Commande : sudo apt install fail2ban

Fail2ban est un excellent outil pour renforcer la sécurité d'un serveur en bloquant automatiquement les adresses IP qui tentent d'exploiter des vulnérabilités dans des services tels que SSH, FTP, HTTP, etc. Il peut être intégré avec d'autres outils de sécurité pour fournir une couche supplémentaire de défense.

Étape 1 : Installer les outils d'audit

Commande : sudo apt install auditd audispd-plugins

Étape 2 : Activer auditd

Commande : sudo systemctl enable auditd && sudo systemctl start auditd

Étape 1 : Identifier les fichiers à permission dangereuse

Commande : sudo find / -perm -2 -type f

Étape 2 : Corriger les permissions si nécessaire

Commande : sudo chmod o-w <fichier>

Option 1 : Générer un certificat auto-signé

Commande : sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout

/etc/ssl/private/grafana.key -out /etc/ssl/certs/grafana.crt

Redémarrer Grafana : sudo systemctl restart grafana-server

Étape 1 : Scanner les ports ouverts

GROUPE2 5

Commandes :

sudo netstat -tuln

sudo nmap -sS localhost

Étape 2 : Bloquer les ports non utilisés (optionel)

Commande : sudo ufw deny <port>

Étape 1 : Installer AIDE

Commande : sudo apt install aide

Étape 2 : Initialiser la base d'intégrité

Commande : sudo aideinit

Étape 3 : Sauvegarder la base de référence

Commande : sudo cp /var/lib/aide/aide.db.new /var/lib/aide/aide.db

Étape 4 : Vérifier l'intégrité à tout moment

Commande : sudo aide --check

Étape 1 : Modifier la configuration rsyslog

Commande : sudo nano /etc/rsyslog.conf

Étape 2 : Redémarrer rsyslog

Commande : sudo systemctl restart rsyslog

2.5 Sécurisation d'OpenNMS

OpenNMS est une plateforme puissante de supervision réseau, mais elle nécessite des configurations spécifiques pour garantir sa sécurité. Voici les principales étapes mises en œuvre :

- Étape 1 : Modifier les identifiants par défaut**

Commande :

```
sudo /opt/opennms/bin/admin.pl --change-pass admin
```

GROUPE2 6

- Étape 2 : Activer l'authentification forte**

Fichier de configuration :

```
sudo nano /opt/opennms/etc/org.opennms.web.security.properties
```

- Étape 3 : Sécuriser l'interface Web avec HTTPS**

1. Générer un certificat :

```
sudo keytool -genkey -keyalg RSA -alias opennms -keystore  
/opt/opennms/etc/keystore.jks -storepass changeit -validity 365 -keysize  
2048
```

2. Modifier jetty.xml :

```
sudo nano /opt/opennms/etc/jetty.xml
```

3. Redémarrer OpenNMS :

```
sudo systemctl restart opennms
```

- **Étape 4 : Restreindre l'accès réseau à l'interface**

Commandes UFW :

```
sudo ufw allow from <ip_authorized> to any port 8980
```

```
sudo ufw deny 8980
```

- **Étape 5 : Activer la journalisation et surveiller les logs**

Répertoire des journaux : /opt/opennms/logs/

Commande pour surveillance :

```
tail -f /opt/opennms/logs/daemon.log
```

- **Étape 6 : Maintenir à jour OpenNMS**

GROUPE2 7

Commandes :

```
sudo apt update && sudo apt upgrade
```

```
sudo apt install opennms
```

- **Étape 7 : Restreindre les accès utilisateur dans l'interface OpenNMS**

Accès via l'interface Web : Admin → Users and Groups

SOUS TITRE 2 : PLAN DE VÉRIFICATION STRUCTURÉ

Étape 1 : Vérifier la supervision des services (ICMP, HTTP, SSH, SNMP...)

Interface :

OpenNMS > Admin > Requisitions

(ou Admin > Provisioning)

Actions :

1. Sélectionne un nœud supervisé (ex : Windows Server ou AP)
2. Clique sur “Edit”
3. Vérifie que les services suivants sont listés :
 - ICMP (ping)
 - HTTP / HTTPS
 - SSH
 - SNMP

Si manquant : clique sur “Add Service” et ajoute-les manuellement.

Étape 2 : Vérifier la collecte SNMP sur les équipements WiFi (AP)

Interface :

OpenNMS > Node > [Nom du Point d'accès]

Vérifie :

- Onglet **SNMP Interfaces** → Doit afficher les interfaces de l'AP
- Onglet **Resource Graphs** :

- Doit afficher ifInOctets, ifOutOctets, dot11StationCount si disponibles

Si vide :

- Assure-toi que SNMP est activé sur l'AP (vérifie via snmpwalk)

bash

```
snmpwalk -v2c -c public 192.168.1.X
```

- Si aucun résultat → AP non accessible via SNMP

Étape 3 : Vérifier la collecte de métriques (RRA/RRD)

Vérifie les fichiers :

bash

```
sudo cat /opt/opennms/etc/datacollection/*.xml | grep -i ifInOctets
```

```
sudo cat /opt/opennms/etc/datacollection/*.xml | grep -i dot11StationCount
```

Tu dois voir que les OIDs sont définis. Sinon, ajoute-les dans un fichier .xml.

Étape 4 : Vérifier l'activation du module OpenNMS-Flow (Top Talkers)

Terminal VM OpenNMS :

bash

```
sudo /opt/opennms/bin/opennms list | grep flow
```

Si non activé :

```
sudo /opt/opennms/bin/opennms enable flow
```

```
sudo systemctl restart opennms
```

Dans l'interface Web :

- Va dans Surveillance > Flows → Doit afficher les flux si le routeur envoie du NetFlow/sFlow

Étape 5 : Vérifier que l'API REST est accessible à Grafana Helm

Terminal depuis la VM Grafana :

```
bash
```

```
curl -u admin:!@CCNB2023cyse http://192.168.1.104:8980/opennms/rest/info
```

Si tu vois une réponse JSON = API REST disponible

Si tu vois “Unauthorized” ou pas de réponse → problème d'authentification ou de pare-feu.

Dans OpenNMS :

- Admin > Configure Users
- Vérifie que admin a bien le rôle ROLE_API

Étape 6 : (Optionnel) Activer la réception de SNMP Traps

Fichier de config :

```
sudo nano /opt/opennms/etc/eventd-configuration.xml
```

Vérifie que trapd est bien activé :

```
xml
```

```
<interface>0.0.0.0</interface>
```

```
<port>162</port>
```

Dans l'interface :

- Va dans Admin > SNMP Trap Configuration → active les traps que tu veux recevoir

Résumé Checklist:

Étape	Vérifié ? (✓ / ✗)
Services (ICMP/HTTP/SSH/SNMP)	
SNMP actif sur les AP	
ifIn/Out + dot11StationCount OK	
Module Flow activé	
API REST opérationnelle	
Compte admin = ROLE_API	
Traps SNMP (si utile)	

Table 7: Checklist des tests

Conclusion

Le projet de remplacement de la solution de supervision PRTG par une plateforme open source a permis d'atteindre plusieurs objectifs techniques et stratégiques. Grâce à l'implémentation d'OpenNMS, associé à Grafana pour la visualisation des métriques, le CCNB dispose désormais d'un système de supervision robuste, évolutif et conforme aux standards de l'industrie.

Les tableaux de bord personnalisés offrent une vue centralisée et dynamique sur l'état des équipements et services critiques du réseau, facilitant ainsi la détection proactive des anomalies. L'intégration avec une page publique d'état des services améliore la transparence et la communication auprès des utilisateurs finaux.

Ce projet a également permis de renforcer les compétences des participants en matière de supervision réseau, d'intégration d'outils open source, d'analyse des données et de gestion d'infrastructure TIC. Il ouvre la voie à de futures améliorations, telles que l'intégration de systèmes d'automatisation des alertes, la surveillance applicative avancée ou encore la corrélation d'événements.

En somme, ce projet constitue une avancée significative dans la modernisation des outils de supervision du CCNB, tout en favorisant une culture de surveillance proactive et de réponse rapide aux incidents.

Sources et références

- OpenNMS Documentation: <https://docs.opennms.org>
- Grafana Documentation: <https://grafana.com/docs/>
- PostgreSQL Documentation: <https://www.postgresql.org/docs/>
- PRTG vs OpenNMS – Comparative Analysis: <https://www.paessler.com/prtg> vs <https://www.opennms.org/>
- Tutoriels OpenNMS + Grafana : [YouTube] « OpenNMS & Grafana Integration Tutorial »
- Projet de statut de services : <https://etatdessimilic.ccnb.ca>
- Documentation SNMP RFC 1157: <https://datatracker.ietf.org/doc/html/rfc1157>
- CCNB Environnement TIC – Références internes