RÉPUBLIQUE DU BÉNIN
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR
ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITÉ D'ABOMEY-CALAVI

INSTITUT DE FORMATION ET DE RECHERCHE EN INFORMATIQUE

BP 526 Cotonou Tel : +229 21 14 19 88
http://www.ifri-uac.bj Courriel : contact@ifri.uac.bj

MÉMOIRE

pour l'obtention du

Diplôme de Licence en Informatique

Option : Sécurité Informatique

Présenté par :
Mahoumin Judith **HOUINSOU**

Mise en place d'un système de Monitoring: Cas du VPS de Jilmonde

Sous la supervision :
A. Tidjani **SANDA MAHAMA**

Membres du jury :

M. Emery ASSOGBA	Docteur	IFRI	Président
Mme. Miranda GNONLONFOUN	Ingénieur	IFRI	Examinatrice
M. Tidjani A. SANDA MAHAMA	Docteur	IFRI	Rapporteur

Année Académique : **2023-2024**

Sommaire

Dédicace ii

Remerciements iii

Résumé iv

Abstract v

List of Figures vi

List of Tables vii

Liste des acronymes viii

Glossaire ix

1 Etat de l'Art 4

2 Conception et choix technique 11

3 Résultats et Discussion 18

Bibliographie 33

Webographie 34

Table des matières 35

Dédicace

À ma famille aimante,

Ce travail est dédié à :

Mes très chers Parents pour leurs sacrifices, amour, tendresse, soutiens et prières tout au long de mes études. **A**vec toute ma gratitude, je vous remercie.

Remerciements

Je remercie sincèrement notre Dieu tout puissant, qui nous a permis d'arriver à cette étape, car sans lui rien n'est possible. J'adresse également mes remerciements à tous ceux qui d'une manière ou d'une autre ont contribués à la réalisation de ce document. Particulièrement mes sincères remerciements vont à l'endroit de :

- **Professeur EZIN C. Eugène**, Directeur de IFRI-UAC pour ces conseils et cette formation qu'il nous a accordé ;
- **membres du corps professoral** de l'Institut de Formation et de Recherche en Informatiques de l'Université d'Abomey-Calavi, je tiens à exprimer ma profonde gratitude envers vous. Vos connaissances partagées, vos défis intellectuels ont nourri ma soif d'apprendre.
- **Docteur AMADOU SANDA MAHAMA TIDJANI** mon maitre de mémoire, pour son encadrement, son suivi et ses conseils tout au long de la réalisation de ce mémoire ;
- **Directeur Général de Jilmonde Consulting, Monsieur Jildas NOUMONZOUNDE** pour m'avoir accepter comme stagiaire dans son entreprise.
- **Monsieur Pio ADJAKOTAN** Et **Monsieur Joel DJOSSOU** pour le suivi rigoureux tout au long du stage.
- **l'équipe informatique de Jilmonde Consulting** pour le soutien et les différents apports.
- **membres du jury** pour leur précieux temps accordé à l'évaluation de notre mémoire.

Résumé

La rapide évolution du monde numérique a entraîné une augmentation significative de l'utilisation des serveurs privés virtuels (VPS). Un VPS est une machine virtuelle hébergée sur un serveur physique chez un fournisseur. Les VPS permettent d'héberger des sites web, de sauvegarder et stocker des données, entre autres. Il est essentiel de prêter une attention particulière aux ressources des VPS, d'où l'importance du monitoring. Dans ce document, nous proposons la mise en place d'un système de monitoring utilisant les outils Prometheus, Grafana et Ntopng au sein de l'entreprise Jilmonde Consulting.

Dans un premier temps, nous avons réalisé une revue de littérature approfondie des VPS, mettant en évidence divers cas d'utilisation de Prometheus, Ntopng et Grafana comme outils de monitoring. Ensuite, nous avoons examiné les caractéristiques de chaque outil, puis choisi d'adopter Prometheus, Grafana et Ntopng en raison de leurs capacités à répondre aux besoins spécifiques et aux réalités de l'entreprise. Enfin, nous avons procédé au déploiement et aux tests de fonctionnalités pour assurer une intégration réussie de ces outils dans l'environnement de Jilmonde Consulting.

Mots clés : Sécurité, Virtual Private Server, Monitoring, Prometheus, Grafana.

Abstract

The rapid evolution of the digital world has led to a significant increase in the use of virtual private servers (VPS). A VPS is a virtual machine hosted on a physical server at a provider. VPS allows you to host websites, backup and store data, among other things. It is essential to pay particular attention to VPS resources, hence the importance of monitoring. In this document, we propose the implementation of a monitoring system using the Prometheus, Grafana and Ntopng tools within the company Jilmonde Consulting.

First, we carried out an in-depth literature review of VPS, highlighting various use cases of Prometheus, Ntopng and Grafana as monitoring tools. Next, we examined the characteristics of each tool, then chose to adopt Prometheus, Grafana and Ntopng because of their abilities to meet the specific needs and realities of the business. Finally, we carried out the deployment and testing of functionalities to ensure successful integration of these tools into the Jilmonde Consulting environment.

Key words: Prometheus,Monitoring, Grafana, Virtual Private Server.

List of Figures

1.1 Architecture des VPS 5

2.1 Architecture du Couple Prometheus Grafana 14
2.2 Architecture de Prometheus 15
2.3 Architecture de Prometheus 16

3.1 Statut Prometheus 19
3.2 Statut Prometheus 20
3.3 Targets Prometheus 20
3.4 Node Exporter 21
3.5 Blackbox Exporter 21
3.6 Blackbox Exporter Status 22
3.7 Blackbox Exporter Config 22
3.8 affichage des exporters dans Prometheus 23
3.9 installation de ntopng 24
3.10 configuration ntopng.conf 24
3.11 Interface Web ntopng 25
3.12 Onglets Flows 25
3.13 Récupération des Flows 26
3.14 Grafana 27
3.15 Sources Grafana 27
3.16 Node Exporter1 28
3.17 Node Exporter2 28
3.18 Blackbox Exporter 29
3.19 Ajout Ntopng 29
3.20 Ajout Ntopng 30
3.21 Node Exporter Interpretation 30

List of Tables

1.1 Serveurs locaux 7
1.2 Serveurs Virtuel Privé 8

2.1 Tableau Comparatifs 12

Liste des acronymes

EXPORTER :

Exporter *:* EXPORTER

GPL :

General Public License *:* GPL

GRAFANA :

Grafana *:* GRAFANA

JOB :

job *:* JOB

METRICS :

Metrics *:* METRICS

NTOPNG :

Network Top Next Generation *:* NTOPNG

OPEN SOURCE :

Open Source *:* OPEN SOURCE

OSI :

Open Systems Interconnection *:* OSI

PROMETHEUS :

Prometheus *:* PROMETHEUS

SCRAPING :

Scraping *:* SCRAPING

TSDB :

Time Series Database *:* TSDB

VPS :

Virtual Private Server *:* VPS

Glossaire

EXPORTER : un processus ou un composant qui expose les métriques dans un format compréhensible par Prometheus. Les exporters permettent de récupérer des métriques à partir de systèmes tiers et de les rendre disponibles pour la collecte par Prometheus. viii

GPL : est une licence de logiciel libre qui a été créée pour promouvoir la liberté et l'ouverture dans la distribution et l'utilisation des logiciels. Elle a été développée par la Free Software Foundation (FSF) et existe en différentes versions, dont la plus courante est la GPL version 3 (GPLv3). viii

GRAFANA : un outil de visualisation open-source populaire utilisé en combinaison avec Prometheus pour créer des tableaux de bord et des graphiques pour l'analyse et la surveillance des métriques. viii

JOB : un job dans Prometheus fait référence à un ensemble d'endpoints que le serveur de métriques scrute pour récupérer les données de performance. Chaque job est configuré pour collecter des métriques spécifiques auprès d'un service ou d'une application. viii

METRICS : une mesure quantitative qui représente une valeur spécifique d'une performance ou d'un état donné. Les métriques dans Prometheus sont généralement enregistrées sous forme de paires clé-valeur. viii

NTOPNG : est un outil de surveillance du trafic réseau et un logiciel qui fournit des informations détaillées en temps réel sur le trafic réseau, l'utilisation et la consommation de la bande passante. C'est une version améliorée de l'outil ntop d'origine, conçue pour offrir des fonctionnalités et des capacités plus avancées aux administrateurs réseau, aux analystes de sécurité et aux professionnels de l'informatique. viii

OPEN SOURCE : fait référence à des logiciels dont le code source est mis à la disposition du public de manière libre et ouverte. Les utilisateurs ont la liberté d'accéder, de visualiser, de modifier et de redistribuer le code source du logiciel selon les termes d'une licence open source spécifique. viii

OSI : est un modèle conceptuel créé par l'Organisation internationale de normalisation qui permet à divers systèmes de communication de communiquer à l'aide de protocoles standards. viii

PROMETHEUS : prométhée est une figure de la mythologie grecque, principalement connue pour son rôle dans le vol du feu aux dieux et pour l'avoir donné à l'humanité. Il est souvent représenté comme bienfaiteur de l'humanité et ses actions ont une signification symbolique dans différents contextes culturels et philosophiques. viii

SCRAPING : le processus par lequel le serveur Prometheus récupère les métriques des cibles configurées (jobs) en effectuant des requêtes HTTP régulières sur les endpoints d'exposition de ces cibles. viii

TSDB : le moteur de stockage de données en temps réel utilisé par Prometheus pour enregistrer les métriques de performance sur une base de données en temps réel. viii

VPS : Un serveur privé virtuel (VPS) est un serveur virtualisé qui fonctionne au sein d'un serveur physique plus grand. C'est une solution d'hébergement populaire qui offre plus de contrôle et de flexibilité par rapport à l'hébergement mutualisé tout en étant plus économique que les serveurs dédiés. viii

Introduction

Le progrès lié à l'utilisation massive des services **cloud** devient de plus en plus remarquable dans nos entreprises. L'utilisation du cloud envahit notre quotidien aussi bien professionnel que personnel. Il faut souligner que les services cloud sont souvent conçus et développés très rapidement, ce qui rend difficile la garantie de disponibilité totale de ses ressources.

Contexte et justification

Le Cabinet Jilmonde Consulting SARL, situé à Abomey-Calavi, offre des services d'assistance en création d'entreprise, en analyses financières, en management d'organisation, en organisations administratives et en conception de logiciels de gestion. Il dispose à son actif d'un Virtual Private Server sur lequel sont hébergées les différentes solutions WEB des clients ainsi que celles utilisées en interne. L'espace CLOUD a été acquis chez OPEN DIGITAL SOLUTION avec les caractéristiques suivantes :

- Random Access Memory : 64 Go
- Processeur : 10 cœurs, 3.0 GHz, 100 Mo/s
- Disque dur : 800 Go SSD (Solid State Drive)

JILMONDE Consulting dispose en son sein d'un ERP (Enterprise Resource Planning) lui permettant la gestion des ressources humaines, la gestion des Paies, la gestion des courriers et la gestion du personnel. L'Enterprise Resource Planning de Jilmonde est hébergé sur le Virtual Private Server.

Problématique

La gestion d'un serveur nécessite une réactivité constante, d'autant plus lorsque ce serveur n'ai pas physique. Le système informatique de l'entreprise Jilmonde Consulting est constitué d'un VPS sur lequel est héberger les solutions web de leurs différents clients. Il est alors capital de se poser ces questions : Comment assurer la disponibilité continue des solutions web des clients , surveiller les performances du VPS, le flux réseau , dimunier le temps de réponse en cas de pannes? Il devient nécessaire de mettre en place une solution de monitoring pour simplifier le travail et répondre aux besoins. Notre problématique est donc d'identifier un outil de supervision informatique qui répondra aux attentes de l'entreprise et tout en nécessitant moins de ressources financières.

Objectifs

Objectif Principal

L'objectif principal est de proposer une solution de monitoring pour assurer la disponibilité continue des ressources applicatives du VPS de Jilmonde Consulting.

Objectifs spécifiques

Les objectifs spécifiques se déclinent comme suit :

- Faire un état de l'art sur les solutions existante et les VPS ;
- Proposer une solution de monitoring en prenant en compte l'architecture du système informatique de jilmonde et les ressources financière ;
- mettre en place un outil de monitoring pour la surveillance des ressources physiques ;
- mettre en place un outil de monitoring pour la surveillance du flux réseau;
- mettre en place un outil de monitoring pour la surveillance des ressources applicatives;
- rendre la supervision des ressources plus flexible;

Organisation du mémoire

Le présent travail s'articule autour de trois grands chapitres.
Le premier concerne l'état de l'art. Après une clarification conceptuelle de certains termes relatifs à notre sujet d'étude, il expose les différentes entreprises béninoises qui offrent des services de vente de VPS (Virtual Private Server) en faisant une étude comparative des mesures de sécurité proposées par lesdites entreprises. Le deuxième chapitre présente le choix de la solution et explique le fonctionnement et l'architecture des différentes solutions choisies pour le système de monitoring. Le troisième chapitre est consacré à la mise en place du système de monitoring.

Chapitre 1

Etat de l'Art

Introduction

Le serveur virtuel privé (VPS) est une solution d'hébergement qui permet de créer plusieurs serveurs virtuels sur un seul serveur physique. Les VPS sont utilisés pour héberger des sites web, des applications et des services en ligne, garantissant des performances élevées et une sécurité renforcée.

1.1 Clarification Conceptuelle

1.1.1 Architecture des VPS

Les VPS reposent sur la virtualisation, avec un hyperviseur qui divise un serveur physique en plusieurs serveurs virtuels. Chaque VPS a ses propres ressources, système d'exploitation et logiciels, offrant ainsi une isolation, une flexibilité et un contrôle complets.

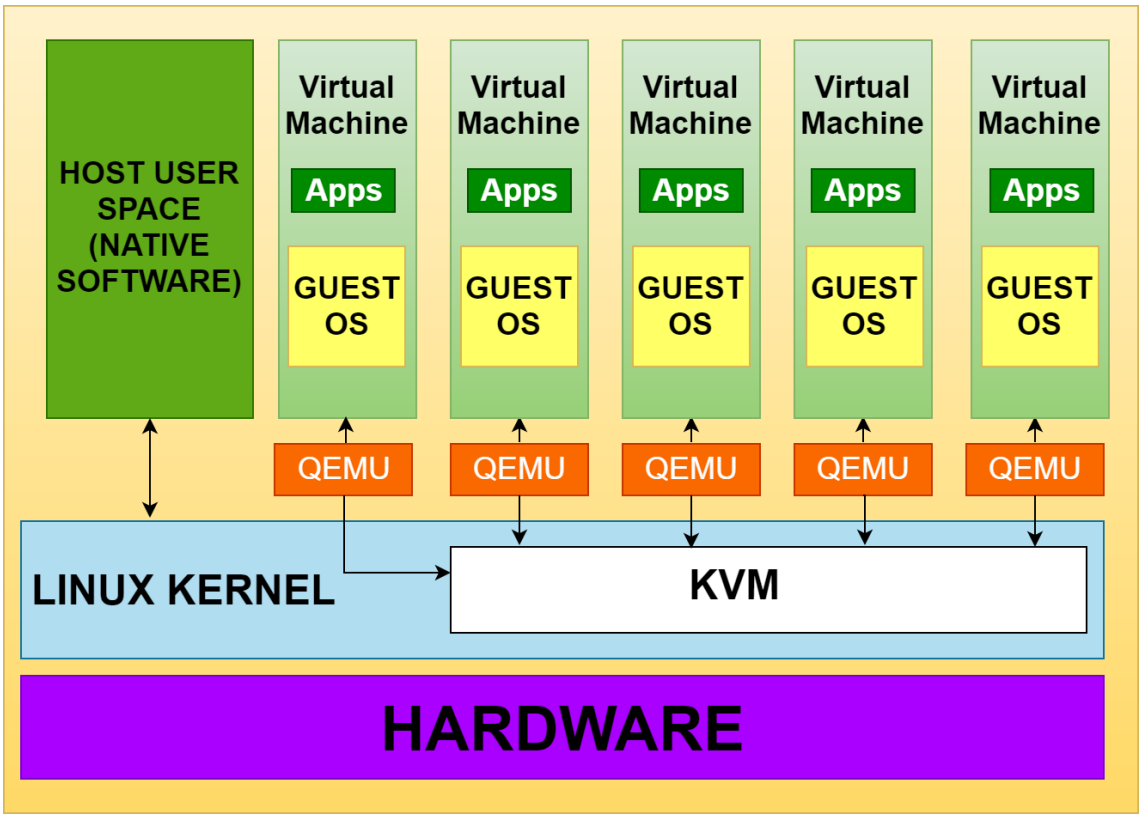


FIGURE 1.1 : Architecture des VPS

VMware Server : c'est une plateforme de virtualisation permettant de créer et de gérer des machines virtuelles sur un serveur physique. Il a été développé par VMware, une société spécialisée dans les solutions de virtualisation.

Système d'exploitation : Il s'agit d'un ensemble de logiciels qui gère les ressources d'un ordinateur, permet à l'utilisateur d'interagir avec l'ordinateur, coordonne les tâches et processus, gère la mémoire, facilite le stockage des fichiers, assure la communication avec les périphériques et offre une interface utilisateur pour interagir avec l'ordinateur. Les systèmes d'exploitation courants incluent Windows, MacOS, Linux, Android, iOS, etc.

Matériel : Ceci représente la machine physique ou le serveur réel.

Applications : Il s'agit des différentes solutions logicielles que nous pouvons héberger ou installer sur notre serveur virtuel privé.

1.1.2 Fonctionnement des VPS

Les serveurs virtuels privés (VPS) fonctionnent en utilisant la virtualisation pour diviser un serveur physique en plusieurs serveurs virtuels indépendants. Chaque VPS possède ses propres ressources, système d'exploitation et logiciels. L'hyperviseur gère la création, l'allocation des ressources et l'isolation entre les VPS. Les VPS offrent une personnalisation et un contrôle plus importants que l'hébergement partagé, ce qui permet une flexibilité pour les besoins spécifiques des utilisateurs. Les VPS peuvent héberger des sites web, des applications et des services, garantissant des performances élevées et une sécurité accrue. Les utilisateurs peuvent gérer leurs VPS via un panneau de contrôle, accéder aux ressources et configurer les paramètres selon leurs besoins.

1.1.3 Les défis liés aux serveurs virtuels privés (VPS)

Les serveurs virtuels privés (VPS) présentent certains défis. La configuration et la gestion peuvent être complexes, nécessitant des connaissances techniques. Les ressources sont limitées, avec un partage potentiel des performances entre les VPS sur le même serveur physique. La sécurité reste un défi, car une vulnérabilité dans une VM peut compromettre l'ensemble du serveur. L'évolutivité peut être limitée par les ressources physiques, nécessitant éventuellement une migration ou une mise à niveau.

1.1.4 Les enjeux de sécurité liés aux VPS

Les serveurs virtuels privés (VPS) présentent des enjeux de sécurité importants. Les principales préoccupations comprennent l'isolation des ressources pour éviter les compromissions, la gestion des vulnérabilités du système d'exploitation, la protection contre l'accès non autorisé et la sécurisation des identifiants, la défense contre les menaces externes telles que les attaques DDoS, les logiciels malveillants et les tentatives d'intrusion, ainsi que la mise en place de sauvegardes pour éviter la perte de données.

1.1.5 Les différentes options d'hébergements pour les serveurs d'entreprise

Il existe plusieurs moyens d'obtenir un serveur pour une entreprise, en fonction de ses besoins spécifiques. Voici quelques-unes des options courantes :

- Serveur sur site : L'entreprise peut acheter, installer et gérer physiquement un serveur dans ses propres locaux. Cela offre un contrôle total sur le matériel et les logiciels, mais nécessite des ressources internes pour la gestion, la maintenance et la sécurité.
- Hébergement dédié : L'entreprise peut louer un serveur dédié auprès d'un fournisseur d'hébergement. Le serveur est dédié exclusivement à l'entreprise, offrant ainsi de meilleures performances et une plus grande flexibilité. Le fournisseur gère généralement l'infrastructure matérielle, tandis que l'entreprise est responsable de la configuration et de la gestion logicielle.
- Hébergement cloud : L'entreprise peut opter pour des services de cloud computing tels que les serveurs cloud ou les instances virtuelles. Les ressources informatiques sont fournies par un fournisseur de services cloud, offrant une évolutivité, une flexibilité et une gestion simplifiée. L'entreprise paie généralement en fonction de l'utilisation.
- Colocation : L'entreprise peut posséder son propre serveur et le placer dans un centre de données tiers. Le centre de données fournit l'infrastructure physique, telle que l'alimentation électrique, la connectivité réseau et la sécurité, tandis que l'entreprise est responsable de la maintenance du serveur.
- Serveur virtuel privé (VPS) : L'entreprise peut opter pour un VPS, qui est un serveur virtuel qu'on peut partagé avec d'autres utilisateurs. Chaque VPS fonctionne de manière indépendante, offrant une isolation et une personnalisation plus importantes que l'hébergement partagé, à un coût relativement abordable.

1.1.6 Comparaison entre un serveur local et un serveur virtuel privé (VPS)

Voici une comparaison entre un serveur local et un serveur virtuel privé (VPS) en termes de limites, d'inconvénients, d'avantages, d'exemples d'infrastructures et de comparaison des architectures :

Types de serveur	Risques	Limites	Avantages	Inconvénients	Exemple d'infra-structures
Héberger en local	Pannes de courant Pannes matérielles Accès non autorisé Catas-trophes naturelles Menaces internes (les em-ployés)	• Capacité phy-sique limitée : L'espace phy-sique disponible dans vos locaux peut limiter le nombre de ser-veurs que vous pouvez héberger. • Évolutivité limitée. • Dispo-nibilité limitée	• Contrôle total : Vous avez un contrôle total sur l'infrastructure, les logiciels et les configurations. • Confidentialité et sécurité des données : Vous avez un niveau de contrôle plus élevé sur la confi-dentialité et la sécurité • Accès direct et contrôle des données : vous avez un accès direct et un contrôle total sur vos données.	• Limitations de capacité et d'évolutivité • Temps de mise en œuvre : L'ins-tallation et la configuration initiales d'un serveur en local peuvent prendre du temps • Coûts initiaux élevés : L'ins-tallation d'un serveur en local nécessite plus d'investissement. • Limitations géographiques et accès à distance	HP Pro-Liant, IBM System x, Lenovo ThinkSys-tem, Dell PowerEdge R740

TABLE 1.1 : Serveurs locaux

Types de serveur	Risques	Limites	Avantages	Inconvénients	Exemple d'infrastructures
Héberger sur un cloud : VPS (Virtual Private Server)	Performance insuffisante : Si l'hébergeur surcharge ses serveurs physiques. Perte de données : En cas de défaillance matérielle ou de panne du système chez l'hébergeur Sécurité : votre serveur virtuel peut être vulnérable aux attaques informatiques, aux piratages ou aux logiciels malveillants	Ressources matérielles limitées ; Bande passante limitée ; Limitations logicielles : Certains hébergeurs peuvent imposer des restrictions sur les logiciels que vous pouvez installer sur votre VPS ; Administration limitée : Certains hébergeurs peuvent restreindre l'accès à certaines fonctionnalités ou fichiers système pour des raisons de sécurité ou de maintien de la stabilité de leur infrastructure.	Support technique spécialisé : L'hébergeur met à votre disponibilité des experts pour vous aider à résoudre les éventuels soucis techniques, répondre à vos questions Évolutivité et flexibilité : Vous pouvez augmenter ou réduire la capacité de votre VPS en termes de CPU, de mémoire, de stockage et de bande passante, généralement de manière flexible et rapide. Sécurité renforcée : Les hébergeurs mettent en place des mesures de sécurité avancées pour protéger votre VPS et vos données. . Coûts réduits : Vous évitez les coûts initiaux élevés liés à l'achat de matériel, ainsi que les dépenses continues pour la maintenance, la connectivité Internet, l'électricité, etc.	Besoin de compétences techniques :l'utilisation d'un VPS chez un hébergeur peut nécessiter une certaine connaissance technique pour configurer, gérer et maintenir efficacement votre serveur virtuel. Limitations géographiques : Selon l'emplacement géographique de l'hébergeur, il peut y avoir des limitations en termes de latence réseau, d'accès à certaines régions ou de conformité réglementaire spécifique à un pays. Partage des ressources : vous partagez les ressources physiques avec d'autres utilisateurs sur le même serveur physique.	Amazon Web Services ; Microsoft Azure ; Google Cloud Platform (GCP) ; IT-NUM, DigitalSiteWeb ; Truehost Africa,etc. . . .

TABLE 1.2 : Serveurs Virtuel Privé

1.2 Analyse et étude de l'existant

1.2.1 Quelques entreprises offrant des services de VPS au Bénin

1.2.1.1 IT-NUM

[5] IT-NUM lancé en 2011 est une entreprise Béninoise qui offre des services numériques de vente de nom de domaine, d'hébergement mutualisé, de VPS (virtual Private Server), de certificat SSL, de solution e-commerce, de conception d'application web ou mobile, d'ingénierie informatique et d'IWE.

1.2.1.2 DigitalSiteWeb

[3] c'est une entreprise informatique au Bénin qui offrent des services d'hébergement de site web, d'applications web, des mails pro sur des serveurs rapides et sécurisés, de vente de serveur Virtuel Privé, d'enregistrements de nom de domaine, de serveur dédié. Il offre une protection contre les attaques DDOS

1.2.1.3 BENIN HOSTING

[1] c'est une filiale d'EBURNY HOSTING GROUP qui offre des services d'hébergement web (VPS, application web ou logiciel, mutualisé, serveurs dédié, cloud), d'enregistrement de nom de domaine, de conception de site web.

1.2.1.4 Wanekoo

[10] Wanekoo Group SAS est une société béninoise d'hébergement web et fournisseur de service internet tel que la vente de nom de domaine, les certificats SSL, les Emails professionnels, les hébergements, les VPS, les cloud, les serveurs. Il offre une sauvegarde régulière des données, utilise des firewalls physique pour le filtrage du trafic.Une surveillance constante de la charge et regroupement des VPS est effectués sur les différents modèles utilisés. Wanekoo utilise aussi des composants neufs de haute qualité provenant de sociétés comme Intel, AMD et Samsung.

1.2.1.5 Afriregister

[2] Afriregister est une entreprise Béninoise qui offre des solutions d'hébergement de site web, d'achat de nom de domaine, de certificat SSL.

1.2.2 Solutions de monitoring existantes

Dans [1] **Odjohoundé Salomon ATCHOBA** a proposer une solution de monitoring des ressources physique avec Prometheus et Grafana .
Enrique Gómez dans ses travaux [9] intitulé **How to Monitor an Ubuntu Server with Grafana and Prometheus** a également proposé grafana et Prometheus pour la supervision des ressources physique. Dans cet article [7]l'auteur propose la surveillance des machines virtuelle Azure à l'aide de Grafana.

Dans son article [6] l'auteur propose la surveillance d'une base de donnée Postgresql à l'aide de Grafana et Kibana.
Jonathan Mukendi dans son mémoire [2] a proposer l'utilisation de Prometheus et Grafana pour le monitoring des conteneurs Docker.
Dans l'article [8] l'auteur propose la surveillance des ressources physique d'une machine virtuelle à l'aide de prometheus et grafana.

1.2.3 Analyse

Les entreprises au Bénin proposent des services de VPS (serveurs privés virtuels) aux petites, moyennes et grandes entreprises qui en ont besoin. Cependant, en me basant sur le VPS de Jilmonde les mesures de sécurité fondamentales indiqué pour les infrastructure critique dans la Politique de Sécurité des Systèmes d'Information de l'Etat [3] ne sont pas respecté, laissant ainsi les ressources exposés à des risques potentiels. Les ressources applicatives des clients sont déployés de plusieurs manière soit à l'aide de conteneurs docker , soit directement sur un cloud public ou un cloud privé(Cas de Jilmonde Consulting). Les choix d'outils de monitoring dépendent étroitement du type de déploiement effectué. Si les ressources de l'infrastructure sont déployées sur un cloud privé, une gamme d'outils tels que Prometheus, Grafana, ELK Stack (Elasticsearch, Logstash, Kibana), Nagios, Zabbix, Ntopng, etc., peut être utilisée pour surveiller et analyser les performances. En revanche, si le déploiement s'effectue à l'aide de conteneurs Docker, des solutions de monitoring comme cAdvisor (Container Advisor), Prometheus, Grafana, Docker Swarm Visualizer, Jaeger, etc., sont plus adaptées pour la surveillance.

1.2.4 Problématiques

La non sécurisation des VPS peut affecté leurs performances ainsi que la disponibilité des services et ressources qui y figure. Il est donc impératif de mettre en place un outil de supervision des activités des VPS afin de prévenir et réduire le temps de réponses aux incidents.

Conclusion

Somme toute, ce chapitre nous présente un éta de l'art sur les Serveurs virtuel privés, quelques cas de mise en place d'une solution de monitoring et une comparaison entre les serveurs virtuels privé et d'autre types de serveur.

Chapitre 2

Conception et choix technique

Introduction

Ce chapitre expose non seulement, le choix de solution et la méthodologie adoptée pour atteindre nos résultats, conformément aux différents objectifs élaborés mais aussi présente les différents outils utilisés et leurs caractéristiques.

2.1 Etudes comparatives des solutions existantes

Plusieurs solutions sont disponibles pour la surveillance d'un système d'information, et parmi tant d'autre, voici un petit résumé de quelques-uns :

- Prometheus : Prometheus est un système de surveillance et d'alerte open source qui collecte et stocke les métriques, permettant ainsi de suivre les performances, la disponibilité et l'état des applications.
- ELK Stack : Elasticsearch, Logstash, Kibana est une pile d'outils qui permet de collecter, analyser et visualiser les logs, fournissant ainsi une surveillance efficace pour la détection des problèmes , l'investigation des incidents et la surveillance.
- Grafana est une plateforme open-source de visualisation de données et de surveillance utilisée pour analyser et afficher des données de séries temporelles. Il permet aux utilisateurs de créer des tableaux de bord avec des panneaux interactifs et dynamiques, facilitant ainsi la compréhension et la surveillance des données
- Zeek est un outil open-source d'analyse de réseau spécialisé dans la surveillance. Il est principalement utilisé pour examiner le trafic réseau en temps réel, détecter les anomalies, les menaces et les vulnérabilités potentielles, et générer des journaux de trafic détaillés pour l'analyse ultérieure.

2.1.1 Tableau Comparatifs

Le tableau ci-dessous présente une comparaison de ses différents outils en fonction de plusieurs critères.

Solutions/Critères	Prometheus	ELK Stack	Zeek (bro)	Grafana
Installation et configuration	Simple	Complexe	Complexe	Simple
Évolutivité	Facile	Possible, mais complexes	Possible mais complexes	Possible
Alertes et notifications	Possible	Nécessite une configuration avancée	Nécessite une configuration avancée	Possible
Sécurité	Nécessite une configuration supplémentaire pour être vraiment sécurisé	Sécurité de base	Disponible mais de base	Nécessite une configuration supplémentaire pour être vraiment sécurisé.
Suivi des performances réseau	Possible	Possible	Possible	Possible mais nécessite l'installation d'autre outils
Surveillance des événements système	Nécessite l'utilisation d'autres outils	Offre une gestion avancée des journaux	Nécessite l'utilisation d'autre outils	Possible mais nécessite l'installation d'autre outils
Support communautaire	Communauté active	Grande communauté	Communauté restreindre	Communauté active
Gestion des journaux (logs)	Nécessite l'utilisation d'autres outils pour la gestion des journaux	Offre une gestion avancée des journaux	Offre une gestion avancée des journaux	Nécessite l'utilisation d'autres outils pour la gestion des journaux
Flexibilité du déploiement	Peut être déployé avant le projet en tant qu'outil de monitoring préventif ou pendant le projet	Peut être déployé à différents stades du projet, avant, pendant ou après, en fonction des exigences de monitoring spécifiques	Il peut être configuré et déployé de différentes manières en fonction des besoins spécifiques de votre environnement et de vos objectifs de surveillance	Il peut être adapter à différents environnements et personnaliser aux besoins.
Portabilité en OS	Disponible sous Linux, MacOS et Windows	Disponible sous Linux, MacOS et Windows	Linux, MacOS, Open BSD, FreeBSD	Disponible sous Linux, MacOS et Windows
Licence et prix	Gratuit, Licence GPL	DGratuit, Licence GPL	Gratuit	Gratuit

TABLE 2.1 : Tableau Comparatifs

2.2 choix de l'outil

Prometheus offre une installation et une configuration simple, une évolutivité robuste, et des fonctionnalités d'alertes et de notifications. Sa communauté active et son support solide en font de lui une solution fiable. Grafana permet une visualisation parfaite des différentes cibles de prometheus, on peut facilement le personnaliser en fonction des besoins et objectifs. De plus, Prometheus et grafana sont distribué sous une licence gratuite, ce qui permet à Jilmonde Consulting de l'utiliser sans frais supplémentaires. En choisissant Prometheus et grafana comme outil de surveillance des différentes ressources de leurs VPS, nous bénéficierons d'une solution puissante et flexible pour collecter, analyser et visualiser les métriques, ce qui nous permettra ainsi d'atteindre les objectifs de sécurité, de fiabilité et de disponibilité des solutions web héberger sur le VPS. Prometheus et Grafana sont le couple idéal pour Jilmonde Consulting. Mais pour surveillance réseau avec Prometheus il doit être configuré pour collecter des métriques à partir des différentes cibles du réseau, telles que les équipements réseau (routeurs, commutateurs). Disposant d'un VPS hébergé chez un fournisseur la collecte des métriques réseau avec prometheus devient impossible car nous n'avons pas accès aux équipement réseau permettant la communication entre les différents clients et le VPS. Pour compenser cela nous avions choisi l'utilisateur d'une solution Open source de surveillance réseau **ntopng** afin d'effectuer la surveillance en temps réel du réseau.
Ntopng est un outil open source de surveillance réseau en temps réel il analyse le trafic, détecte les anomalies, gère la bande passante et permet de surveiller son réseau. De plus il peut être intégrer directement à grafana afin d'améliorer la visualisation des données et dispose d'une version Community qui est sous une licence GPL.

2.3 Description de la solution choisie ou retenue

2.3.1 Prometheus

Prometheus est un outil open source de surveillance et d'alerte. Il permet de collecter, stocker et traiter les métriques provenant de diverses sources, tels que les applications ,les systèmes d'exploitation. etc... En utilisant une approche basée sur les séries temporelles, Prometheus permet de stocker les données collectées de manière flexible, facilitant ainsi l'analyse et la visualisation ultérieures. Il se distingue également par sa compatibilité avec les infrastructures Cloud, ce qui en fait une plateforme de surveillance polyvalente pour les environnements modernes. L'univers de Prometheus est composé de plusieurs éléments, dont beaucoup sont optionnels :

- Le cœur du système est constitué du serveur principal Prometheus, responsable de la collecte et du stockage des données en séries chronologiques.
- Des bibliothèques clientes sont également disponibles pour instrumenter le code des applications.
- Une passerelle de type "push" est prévue pour soutenir les tâches éphémères.
- Des exportateurs spécialisés sont disponibles

- Un gestionnaire d'alertes (alertmanager) est intégré pour gérer les alertes émises par le système.
- On trouve également divers outils d'assistance.

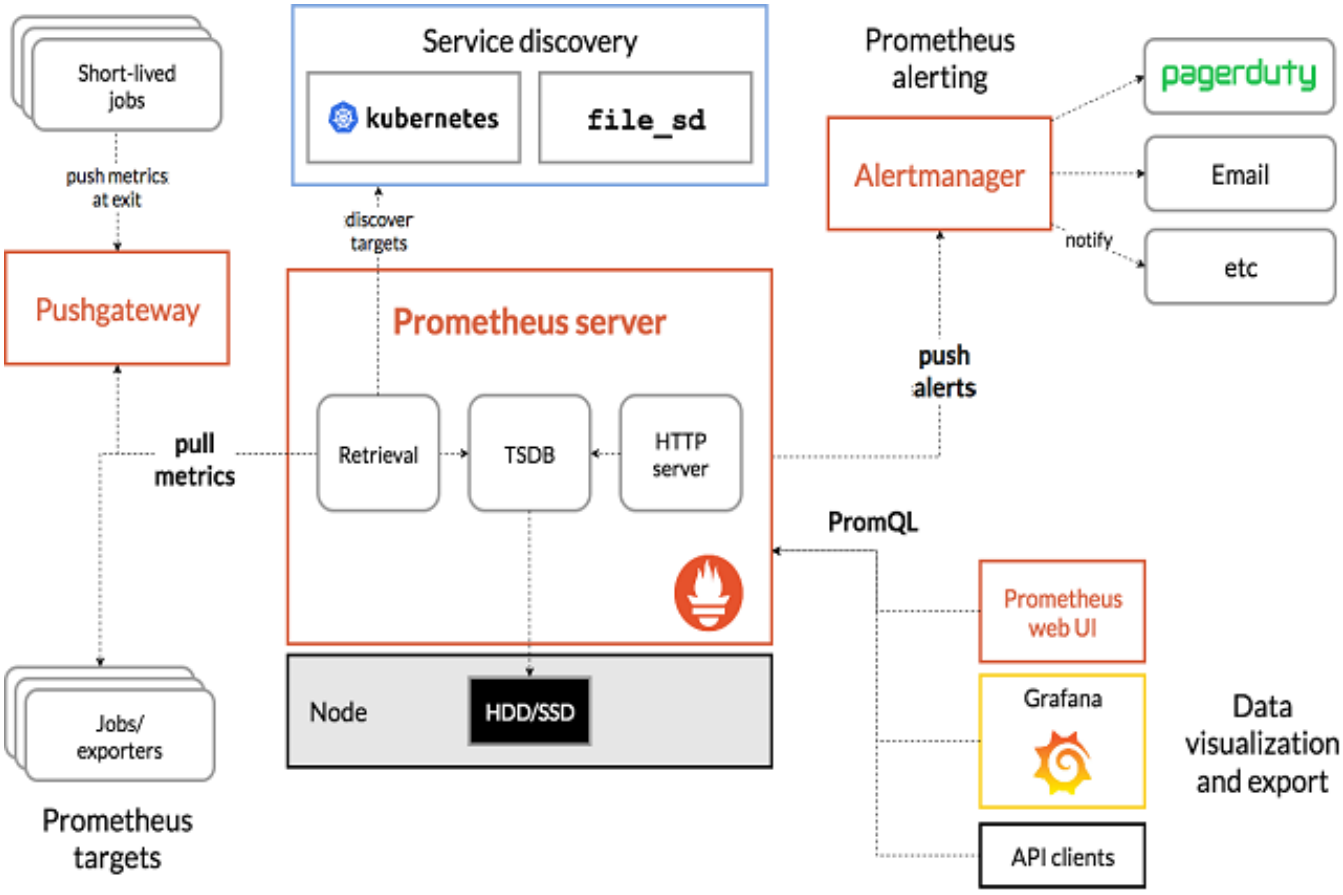


FIGURE 2.1 : Architecture du Couple Prometheus Grafana

De ce diagramme, nous devons comprendre que :

- Prometheus Server : Il s'agit du cœur du système, responsable du stockage des métriques collectées.
- **Exporteurs (Job Exporters) :** Ce sont des agents qui collectent les métriques spécifiques et les exposent à Prometheus.
- **Interface utilisateur Web (Web UI)** : C'est l'interface graphique qui permet aux utilisateurs de visualiser les métriques collectées et de créer des tableaux de bord personnalisés.
- **Alertmanager :** C'est le composant qui gère l'envoi des alertes aux utilisateurs en cas de conditions anormales ou de dépassement de seuils définis.

2.3.2 Fonctionnements de prometheus :

Prometheus surveille ses différentes cibles via les exporteurs installé afin de collecter des informations sur ses différents applications en cours d'exécution. Il interroge périodiquement les exporteurs respectives pour récupérer les métriques telles que l'utilisation des ressources et l'état des applications. Ces métriques sont stockées dans la base de données de séries chronologiques de Prometheus.

2.3.3 GRAFANA

Grafana est une interface Web de graphes multi-sources qui est notamment capable d'afficher des données issues de Prometheus. Il dispose des capacités de présentation très grandes, notamment via ses Dashboard, paramétrables.

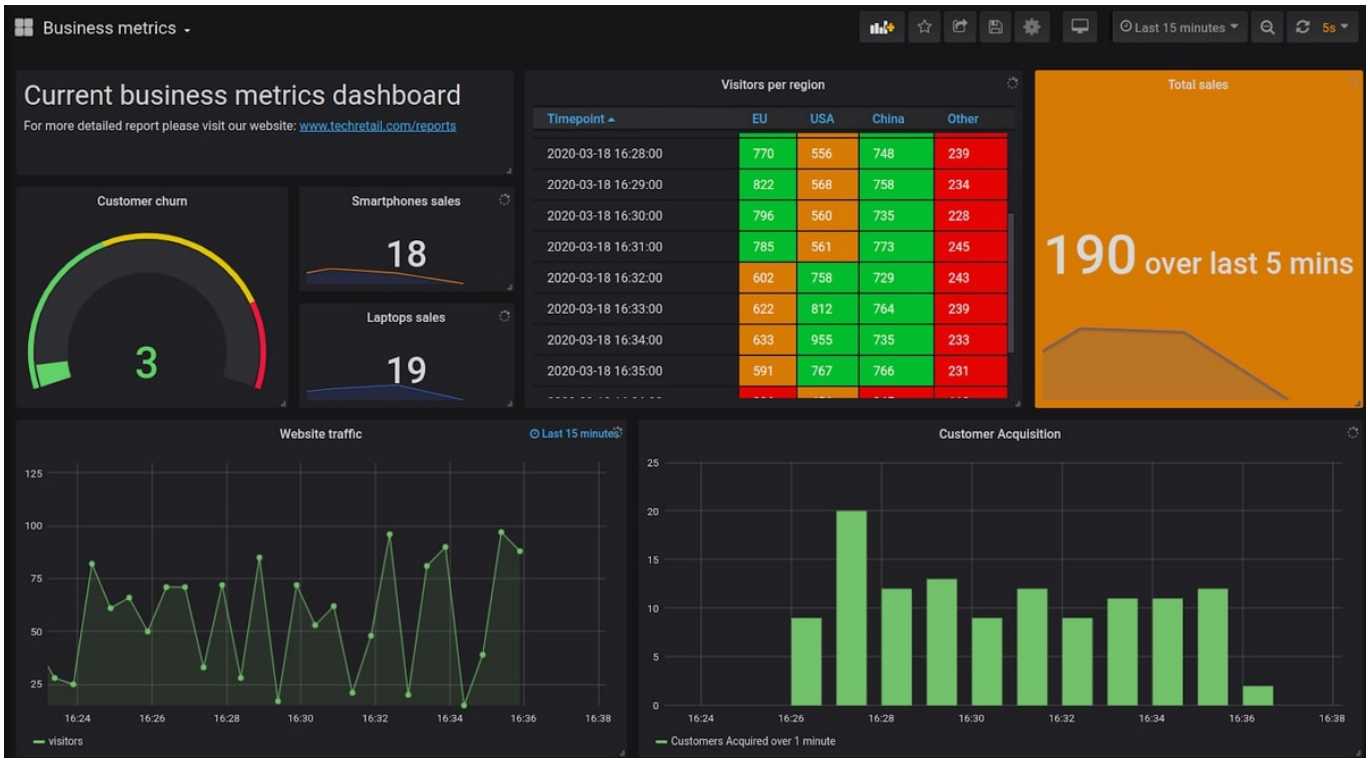


FIGURE 2.2 : Architecture de Prometheus

2.3.4 Principales caractéristiques de Grafana :

- **Prise en charge des sources de données :** Grafana peut se connecter à une large gamme de sources de données, y compris des bases de données de séries temporelles populaires telles que Prometheus, Influx DB, Graphite et Elasticsearch, ainsi que des bases de données relationnelles comme MySQL et PostgreSQL.
- **Création des tableaux de bord :** Les utilisateurs peuvent construire des tableaux de bord personnalisés en ajoutant différents panneaux, tels que des graphiques, des tableaux, des affichages de statistiques uniques, des cartes de chaleur, et plus encore. Ces panneaux peuvent visualiser des données provenant d'une ou de plusieurs sources de données.
- **Modèles :** Grafana prend en charge les variables de modèle qui permettent aux utilisateurs de créer des tableaux de bord dynamiques et flexibles. Le modèle permet aux utilisateurs de basculer facilement entre différentes sources de données, plages de temps ou autres paramètres.
- **Alertes :** Grafana offre des fonctionnalités d'alerte qui permettent aux utilisateurs de configurer des alertes en fonction des seuils définis. Lorsque les données dépassent ou tombent en dessous de ces seuils, Grafana peut envoyer des notifications par le biais de différents canaux tels que l'e-mail, Slack ou d'autres webhooks.

- **Plugins et intégrations :** Grafana dispose d'un vaste écosystème de plugins qui permet aux utilisateurs d'étendre ses fonctionnalités. Les utilisateurs peuvent créer des panneaux personnalisés, des sources de données et des intégrations avec des systèmes tiers.
- **Équipes et autorisations :** Grafana permet la gestion des utilisateurs, la collaboration en équipe et le contrôle d'accès basé sur les autorisations. Cela permet aux organisations de limiter l'accès à des tableaux de bord et à des fonctionnalités spécifiques en fonction des rôles des utilisateurs.
- **Communauté et support :** Grafana dispose d'une communauté importante et active d'utilisateurs et de développeurs, fournissant une documentation complète, des forums et des ressources contribuées par la communauté.

2.3.5 NTOPNG(Network Top Next Generation)

Ntopng : c'est un outil open-source de surveillance du trafic réseau qui offre une visibilité en temps réel sur le trafic réseau et les statistiques d'utilisation du réseau.

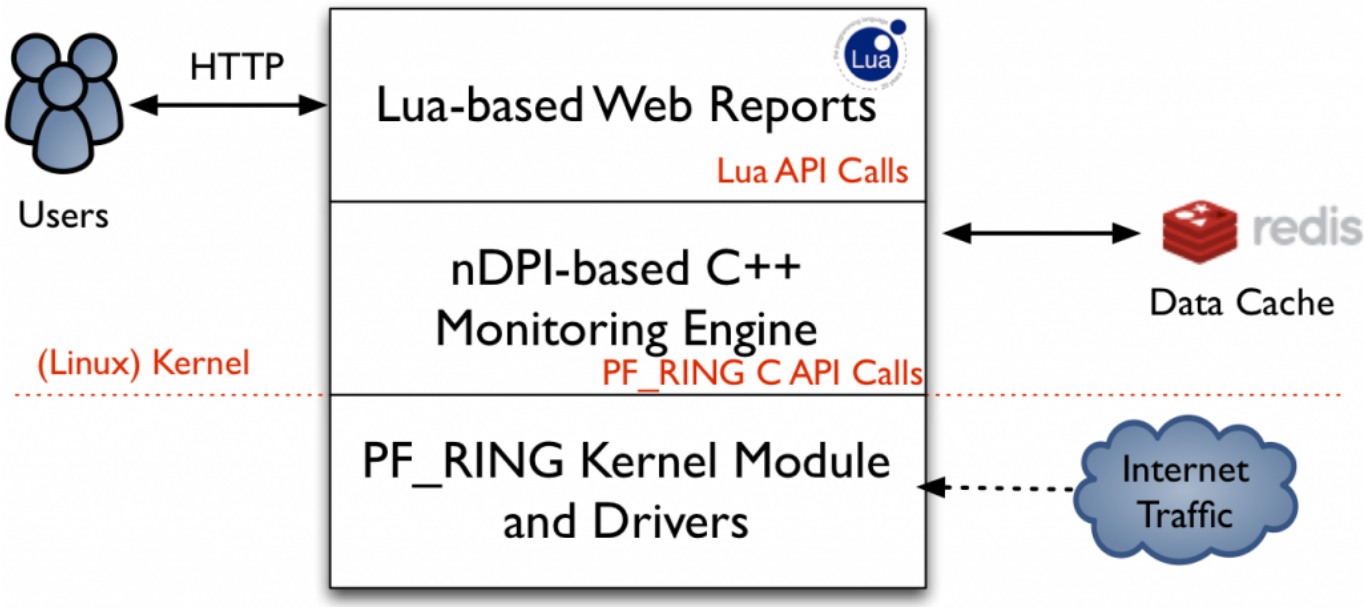


FIGURE 2.3 : Architecture de Prometheus

- **Lua-based :** permet d'utiliser le langage de programmation Lua pour personnaliser et générer des rapports personnalisés à partir des données de trafic collectées par ntopng.
- **Lua :** est un langage de script léger et extensible souvent utilisé pour ajouter des fonctionnalités personnalisées à des applications
- **nDPI-based (Network Data and Protocol Identification)** : permet d'identifier et de catégoriser différentes applications et protocoles de réseau en analysant les données de trafic.
- **PFRING kernel (Packet Filtering Ring) :** est utilisé pour améliorer les performances de la capture et de l'analyse du trafic réseau à haute vitesse. Il est utilisé ici pour faire l'analyse du trafic internet.
- **Data cache :** est une zone de stockage temporaire utilisée pour stocker des copies de données fréquemment utilisées afin d'accélérer l'accès à ces données et d'améliorer les performances.

Conclusion

Le choix de solution et la méthodologie de validation que nous avons employés ainsi que les caractéristiques matérielles et logicielles de notre environnement de travail ont été détaillées dans cette section. La section suivante expose les différents résultats obtenus.

Chapitre 3

Résultats et Discussion

Introduction

Dans ce chapitre, nous allons exposer les résultats issus de notre travail et produire une discussion.

3.1 Architecture

Pour démontrer l'importance de notre travail, l'image ci-dessous présente l'architecture interne du VPS de Jilmonde Consulting avant le déploiement du système de monitoring.

3.2 Mise en place du système de monitoring

Notre système de monitoring est composé de trois outils à savoir prometheus, grafana, ntopng

3.2.1 Installation de Prometheus

wgethttps ://github.com/prometheus/prometheus/releases/download/v2.18.1/prometheus-2.18.1.linux-amd64.tar.gz : permet de télécharger le dossier zipper de Prometheus **tar -xzf prometheus-2.18.1.linux-amd64.tar.gz** :permet de dézipper le dossier de Prometheus télécharger précédemment. **sudo useradd -s /sbin/false prometheus** :permet de créer l'utilisateur prometheus. Cet utilisateur sera utilisé lorsqu'on veut effectuer des modifications au niveau du fichier de configuration de prometheus. **cd /etc** : permet d'accéder au dossier etc du système d'exploitation. **mkdir prometheus** : crée le dossier prometheus **cp -r prometheus-2.18.1.linux-amd64 /etc/prometheus** : permet de copier le contenu du dossier de prometheus télécharger vers le nouveau dossier prometheus créer. **sudo chmod 755 /etc/prometheus -R** : permet de donner d'exécution sur ce dossier à l'utilisateur Prometheus. **sudo chown prometheus :prometheus /etc/prometheus -R** : ajout de l'utilisateur aux groupes prometheus. Dans le dossier de prometheus nous avons le fichier prometheus.yml Prometheus.yml est le fichier de configuration de prometheus. **sudo nano /etc/systemd/system/prometheus.service** : cette commande permet de créer le fichier système de prometheus. **sudo systemctl daemon-reload** : permet d'appliquer les differentes modifications apporter au fichier Unit.

sudo systemctl start prometheus.service : permet de démarrer le fichier de systemd préconfiguré pour prometheus.
sudo systemctl enable prometheus.service :active le fichier de démarrage.
sudo systemctl status prometheus.service -l : donne l'état du service .

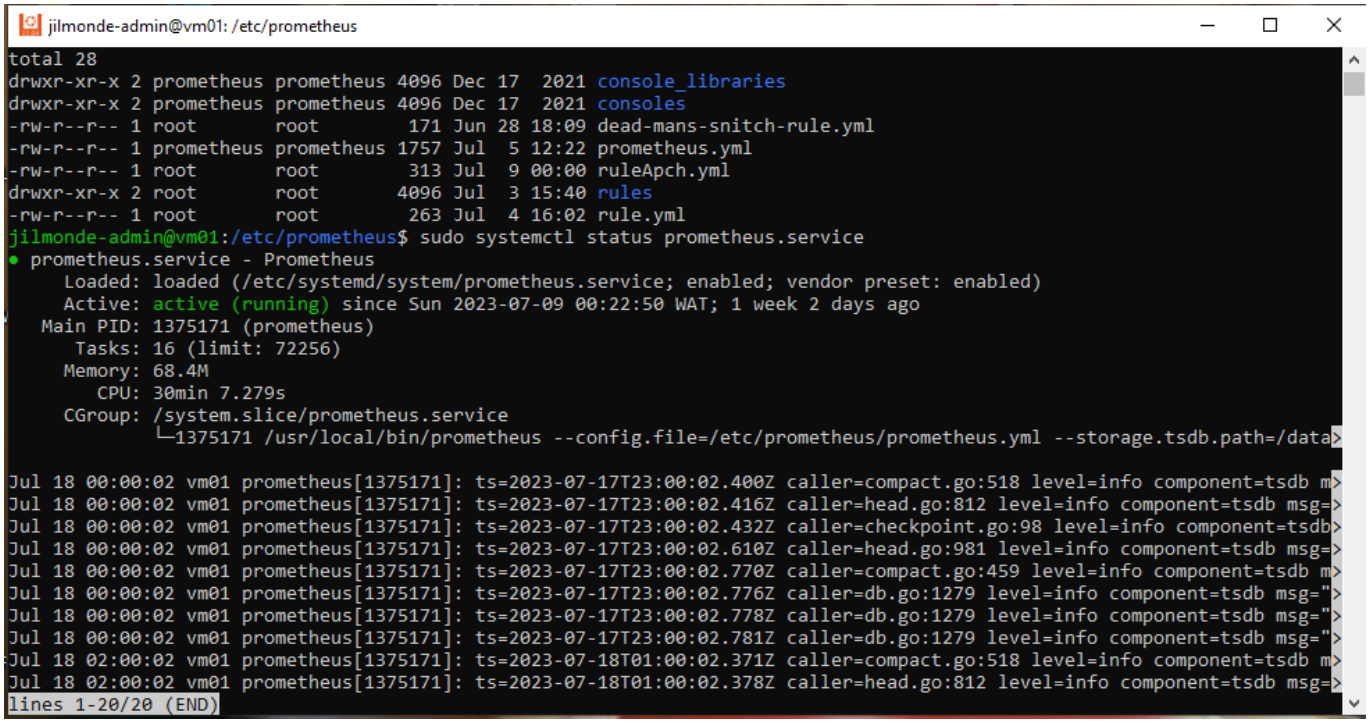


FIGURE 3.1 : Statut Prometheus

Avec l'état « **running** » nous savons que notre fichier systemd a été bien configuré et fonctionne correctement.
Prometheus fonctionne sur le port 9090 par défaut
Avec **sudo ufw allow 9090** : on alloue le port 9090 à Prometheus. Ensuite nous pouvons accéder à Prometheus via le navigateur en tapant l'adresse IP et le port.

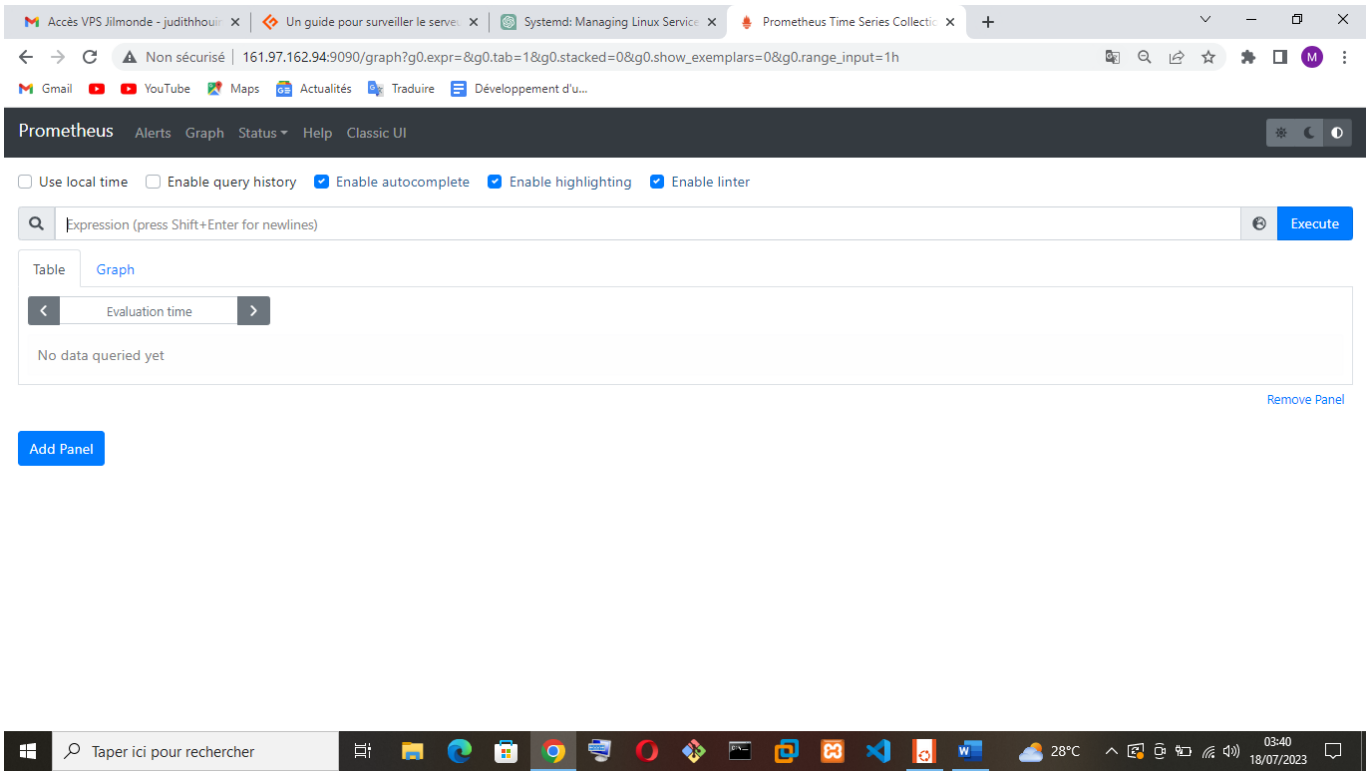


FIGURE 3.2 : Statut Prometheus

Nous pouvons maintenant afficher prometheus dans le navigateur Pour voir les différentes cibles de prometheus nous irons sur l'onglet « **statut** » et choisir « **targets** »

Sur la page des targets nous aurons les différentes cibles que surveille prometheus ainsi que prometheus lui-même. Lorsqu'on installe prometheus par défaut c'est lui seul qui s'affiche sur la page targets. Notons que dans notre cas nous avons déjà ajouter d'autre cible, ne prenez pas en compte cela.

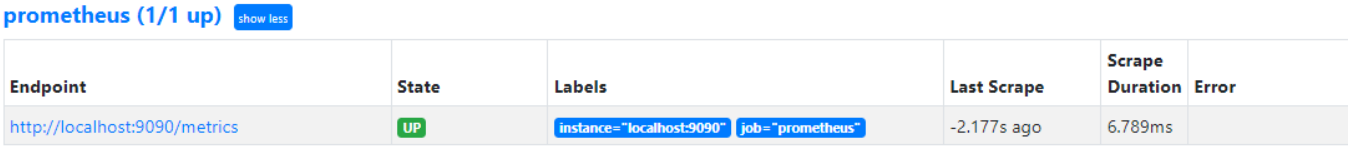


FIGURE 3.3 : Targets Prometheus

3.2.1.1 Configuration des métriques au niveau de prometheus en utilisant les exporteurs

. Pour collecter les métriques d'une application ou d'un service prometheus a besoin d'une « passerelle ». Les passerelles dans le cas de prometheus se nomment les exporteurs.
Il existe de nombreux types d'exportateurs pour Prometheus, chacun étant spécialement conçu pour collecter des métriques à partir de sources spécifiques.
Nous avons : **node exporter, MySQL Exporter, Redis Exporter, PostgreSQL Exporter, Apache Exporter, Blackbox Exporter, etc. ...**

Dans notre cas nous avons installé en premier lieu node exporter et après Blackbox exporter.
Node exporter permet la collecte des métriques système telles que l'utilisation du CPU, de la mémoire, de l'espace disque, etc. Il surveille les performances de l'hôte où il est installé.
Blackbox Exporter permet de sonder et de surveiller des services externes, tels que des services web,

des serveurs de messagerie,etc., en vérifiant qu'ils sont disponibles et en collectant des métriques sur leur état.

3.2.1.2 Installation de node exporter et de blackbox exporter

Téléchager le dossier de node exporter et de blackbox exporter depuis leurs site github avec wget
Dézipper les deux dossiers node exporter et blackbox exporter téléchargés.
Création d'un dossier node exporter et blackbox exporter au niveau du dossier **/usr/local/bin**
Copie du contenu des dossiers dézipper node exporter et blackbox exporter vers le nouveau dossier de node exporter dans **/usr/local/bin** et donner les droits d'exécution à ses dossiers.

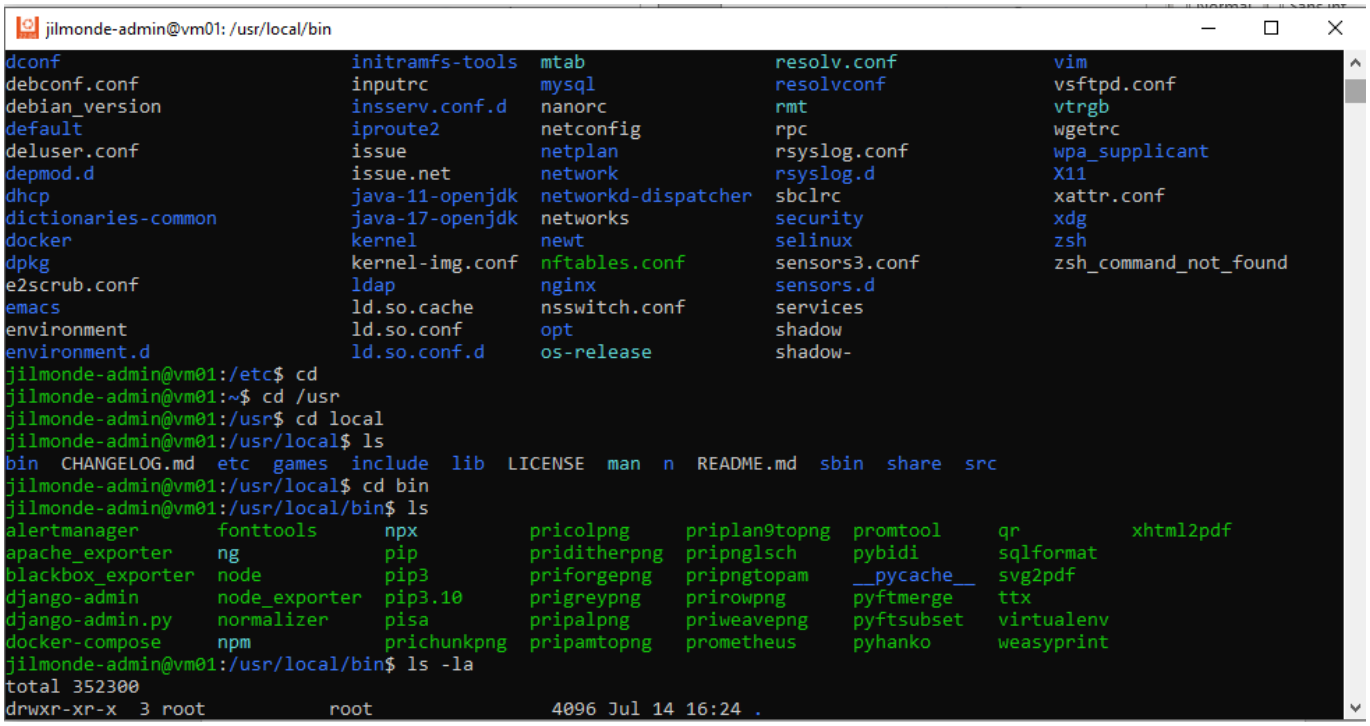


FIGURE 3.4 : Node Exporter

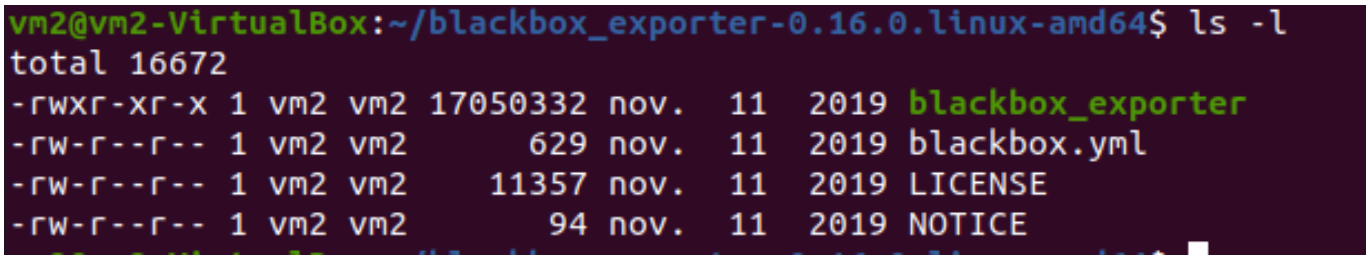


FIGURE 3.5 : Blackbox Exporter

Ensuite création du fichier systemd de node exporter afin de configurer le démarrage automatique lorsque le système d'exploitation est allumé. **sudo systemctl daemon-reload** : redémarre le systemd afin d'appliquer les dernières modifications.
sudo systemctl start node exporter : démarre le fichier systemd de node exporter.
sudo systemctl status node exporter : vérifie si le service a bien démarré et qu'il n'y est pas d'erreur de configuration.

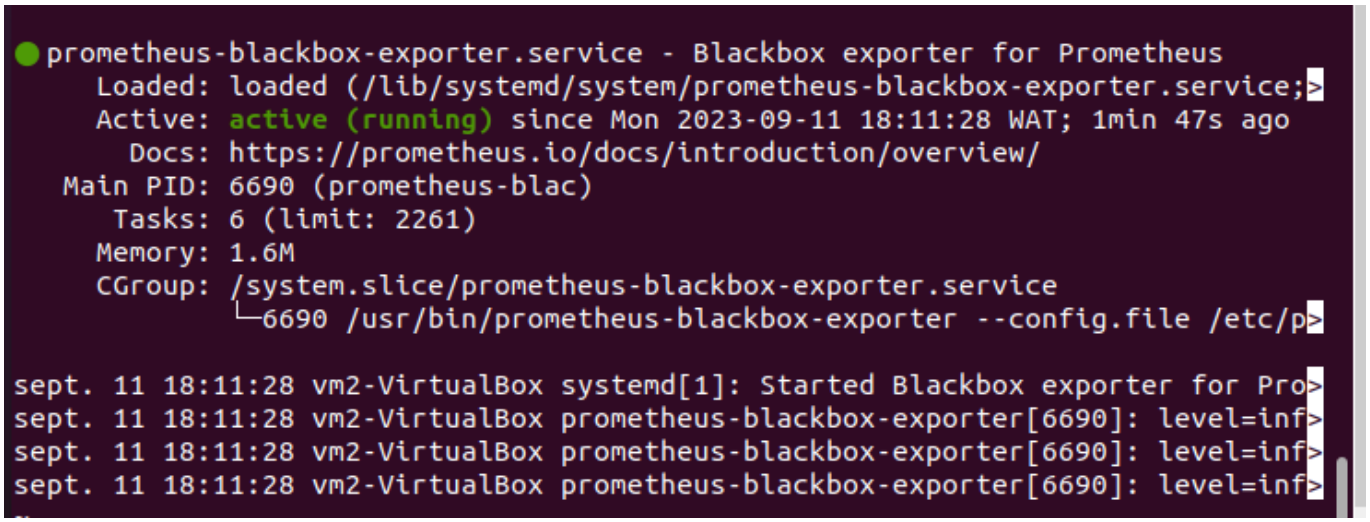


FIGURE 3.6 : Blackbox Exporter Status

La capture d'écran ci-dessus nous indique que node exporter et blackbox exporter sont bien installés et qu'il n'a pas d'erreur de configuration d'où l'état « **active** » affiché. Nous devons ajouter un nouveau travail dans le fichier prometheus.yml afin que node exporter et blackbox exporter deviennent des cibles de prometheus. Accéder au dossier de prometheus situé dans **/etc** avec la commande cd Fait un **sudo nano prometheus.yml** pour pouvoir effectuer des modifications.

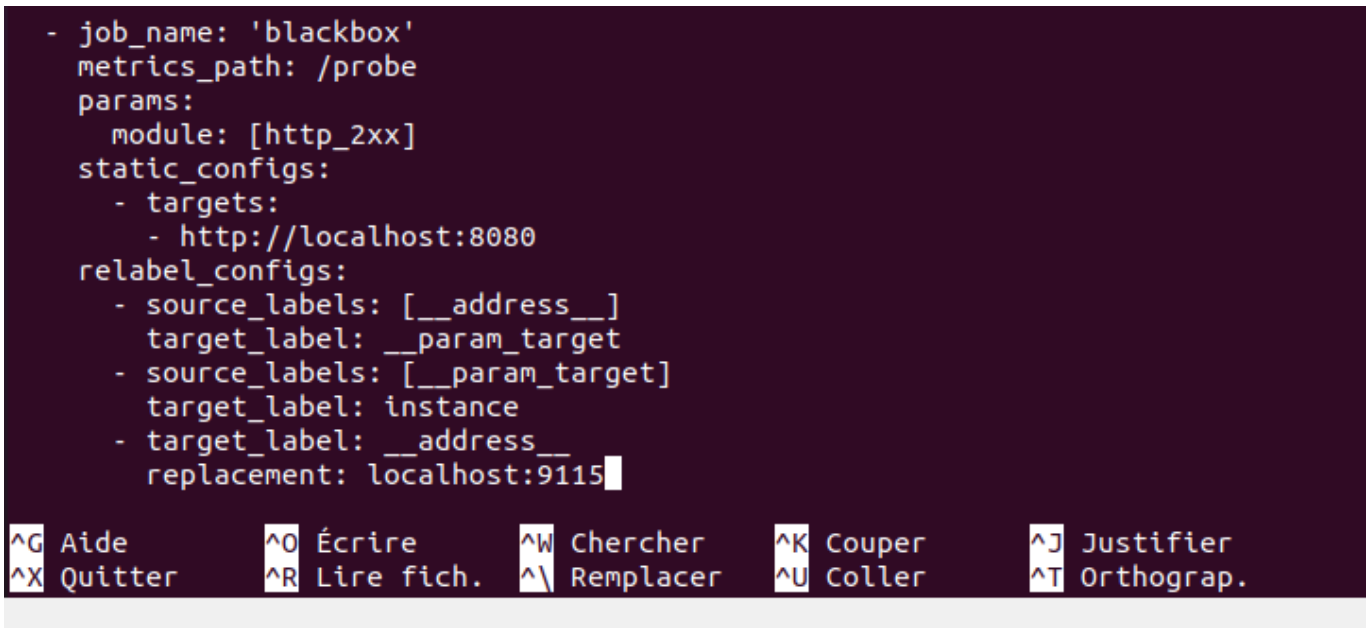


FIGURE 3.7 : Blackbox Exporter Config

Après la configuration, arretez et démarrez Prometheus à nouveau afin qu'il ne prenne en compte les différentes modifications.

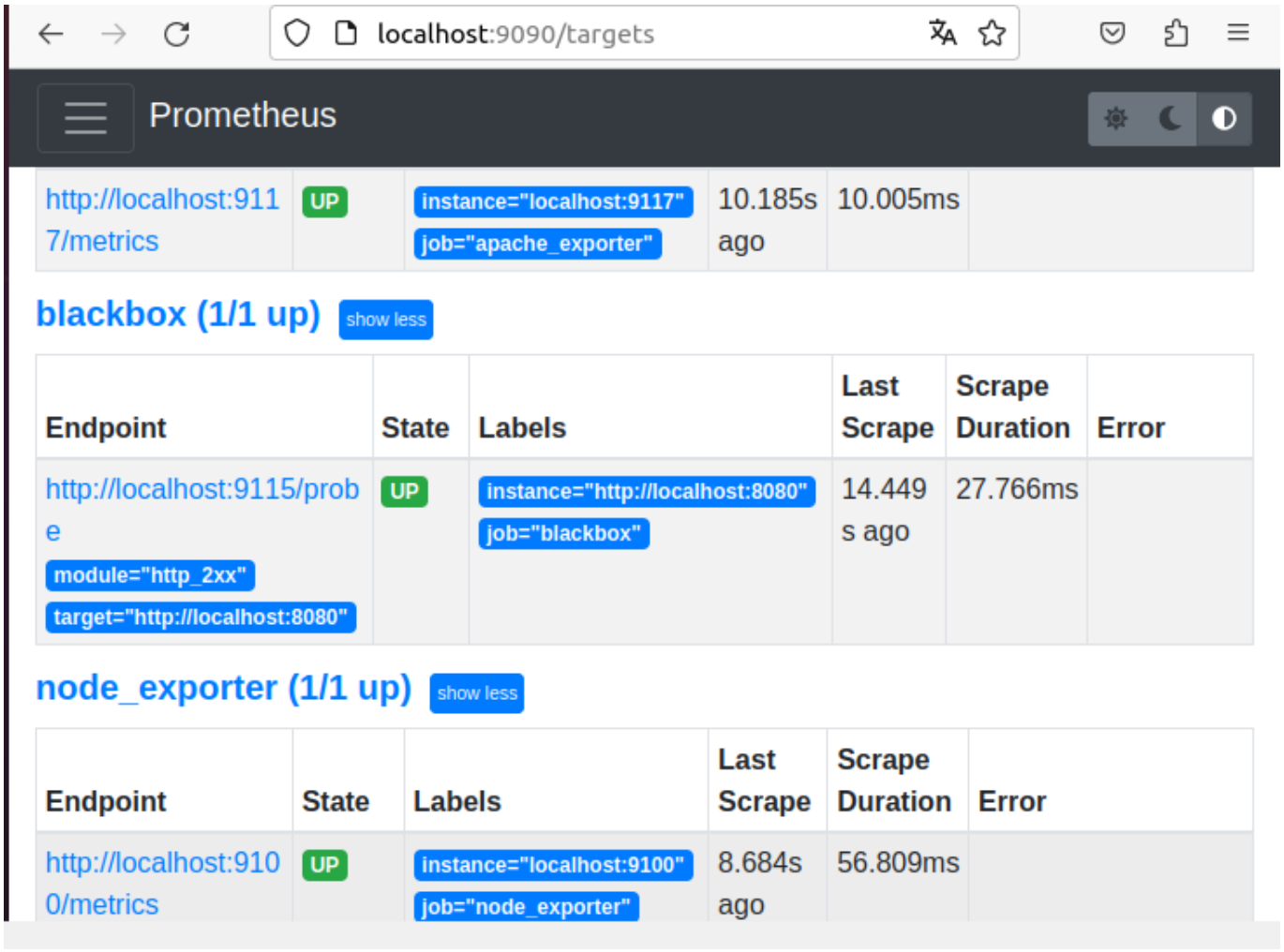


FIGURE 3.8 : affichage des exporters dans Prometheus

3.2.2 Installation de Ntopng

sudo apt install ntopng : cette commande permet d'installer ntopng.

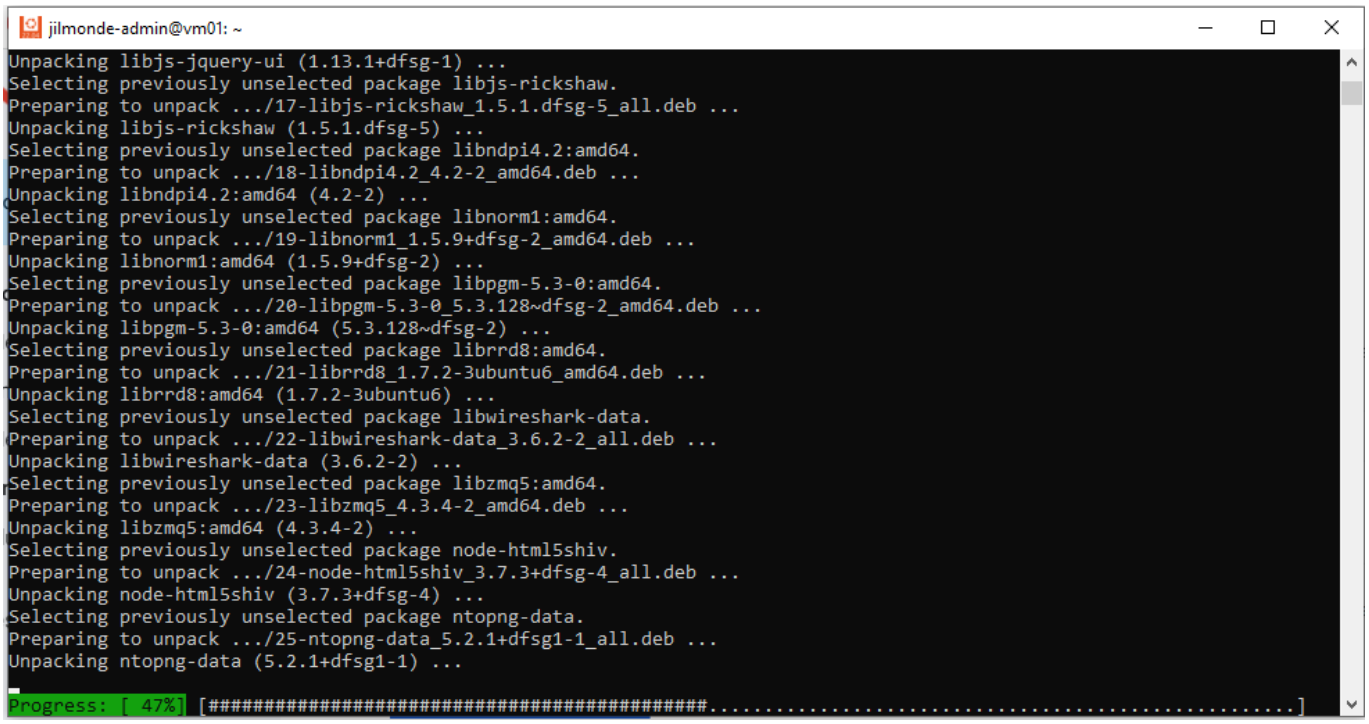


FIGURE 3.9 : installation de ntopng

Après l'installation de ntopng nous sommes passé à la vérification des différentes interfaces réseaux.
Nous constatons que l'adresse publique du serveur se situe au niveau de l'interface eth0. Pour effectuer l'analyse du trafic il faut ajouter l'interface réseau de l'adresse IP qui est utilisée pour fournir les services. Le fichier de configuration de ntopng se situe dans le dossier**/etc**. **-i=eth0 :**avec cette option nous demandons à ntopng de surveiller le trafic sur cette interface.
-w=3001 :permet d'ajouter à la configuration le port sur lequel ntopng doit démarrer.

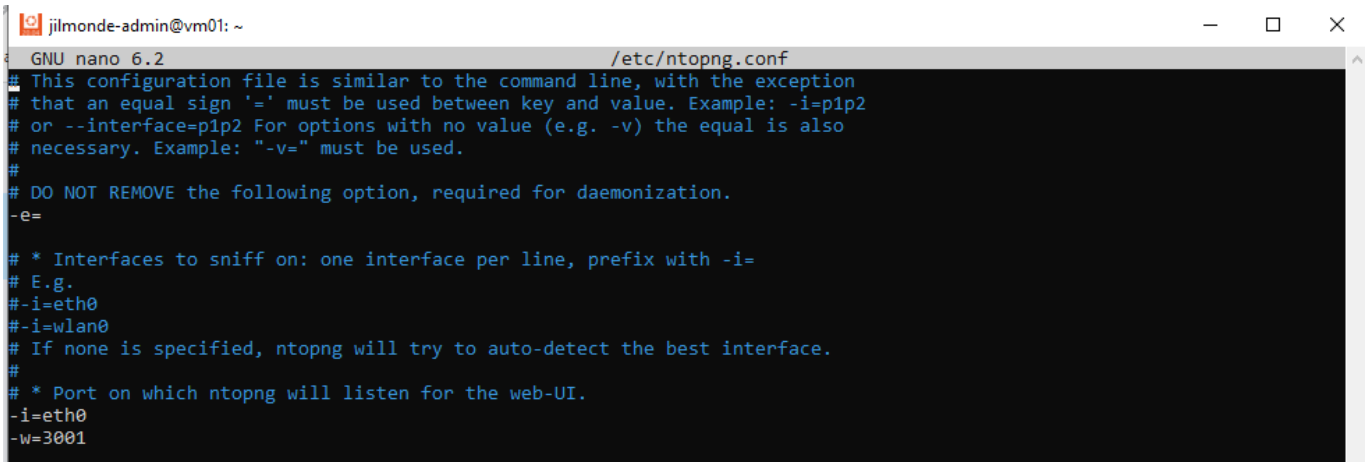


FIGURE 3.10 : configuration ntopng.conf

Nous avons ensuite activer le service ntopng avec la commande sudo systemctl enable ntopng et démarrer ntopng avec sudo systemctl start ntopng . Le service ntopng a bien démarré sans erreur. L'état « **running** » nous démontre que ntopng a été bien installé et bien démarré. Nous pouvons maintenant accéder à l'interface graphique via le navigateur en utilisant l'adresse IP et le port que nous avions configuré dans ntopng.conf

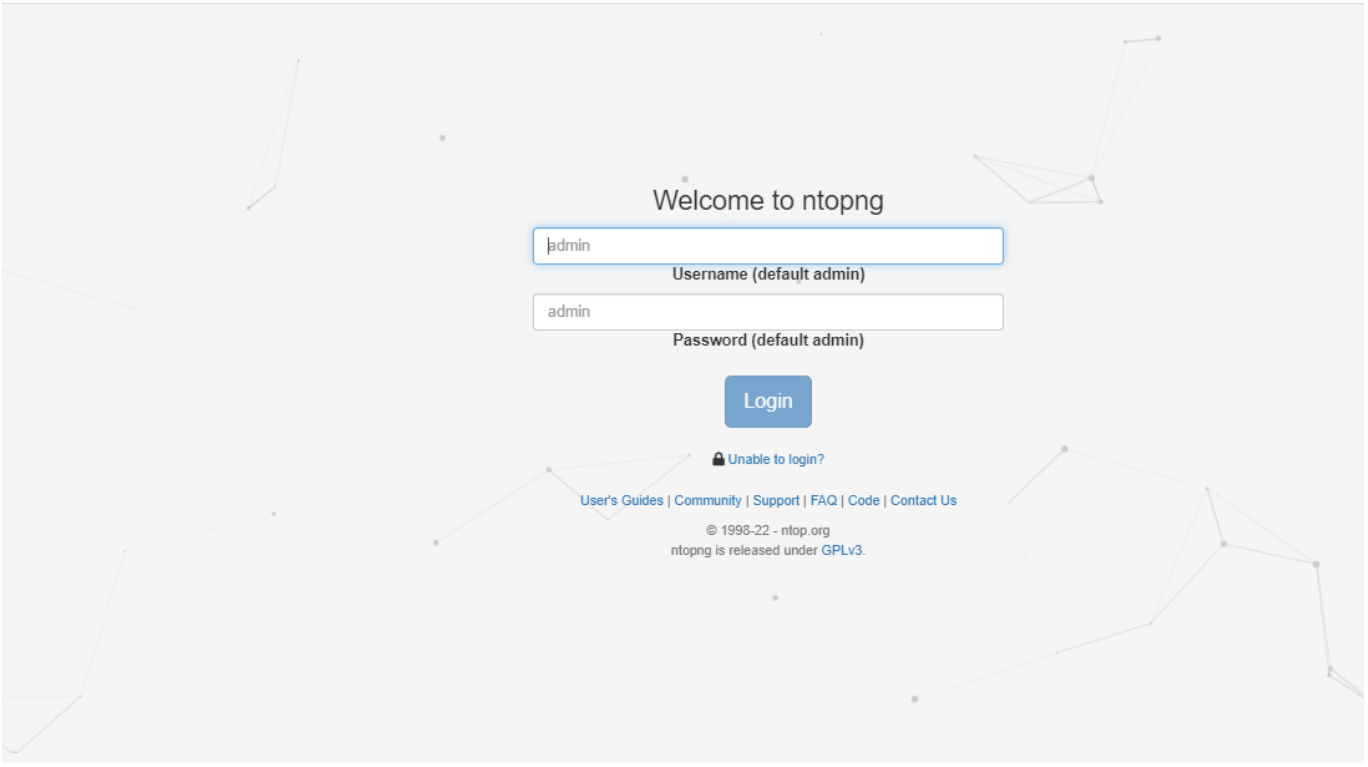


FIGURE 3.11 : Interface Web ntopng

Les identifiants par défaut sont admin comme username et password. Après nous avons ajouté un nouveau mot de passe La partie de ntopng qui permet de récuperer les informations sur le trafic est l'onglet flows. L'onglets Flows permet de voir en temps réel les flux du trafic qui passent par notre interface réseau. Cela peut nous aider à identifier les connexions actives, les destinations, les protocoles utilisés, et plus encores.

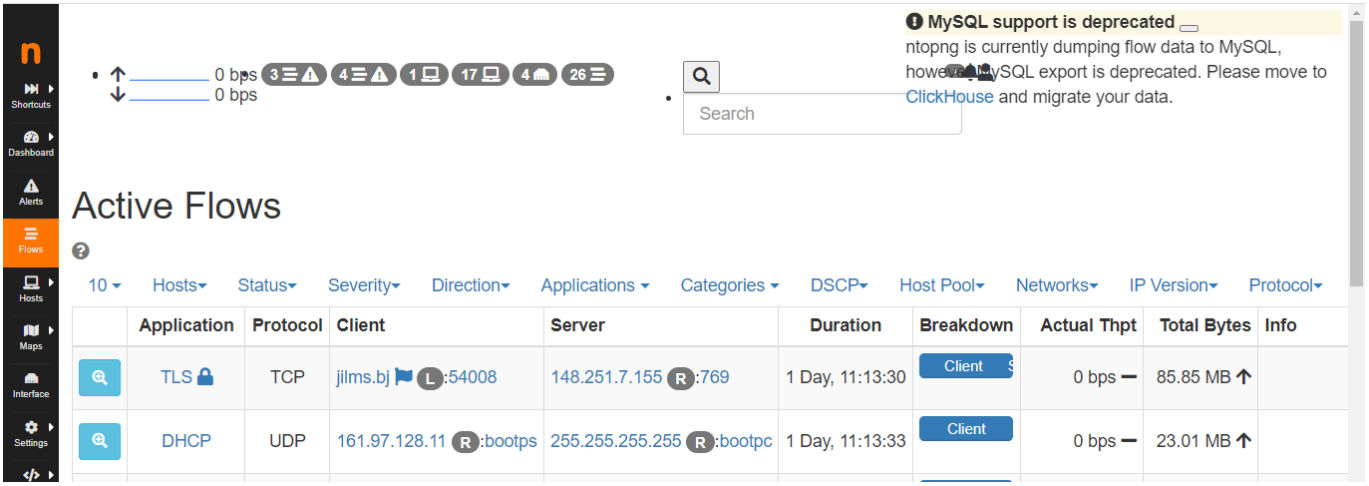


FIGURE 3.12 : Onglets Flows

Pour récupérer les informations collectées par ntopng nous allons créer une base de données Mysql où nous allons stocker ces différentes informations.Un utilisateur ntopng a été créé avec mot de passe ntopng. Après nous allons récupérer les informations en direct avec la commande dump de Mysql.

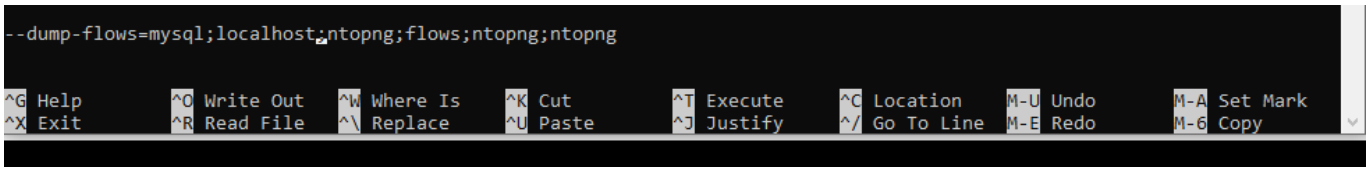


FIGURE 3.13 : Récupération des Flows

Deux autres tables ont été ajoutés de manière automatique, c'est deux tables flowsv4 et flowsv6 contiennent le flux lorsqu'on utilise IPv4 et IPV6. Nous devons ajouter la table flowsv4 au niveau de la configuration de ntopng

3.2.3 Installation de Grafana

Grafana est une plateforme open-source de visualisation et d'analyse de données conçue pour créer des tableaux de bord interactifs et des graphiques pour la surveillance et l'analyse des métriques.

- sudo apt-get install -y apt-transport-https software-properties-common : permet d'installer les packages nécessaires pour le bon fonctionnement de grafana serveur.

- wget -q -O - https ://packages.grafana.com/gpg.key | sudo apt-key add - : ajout de la clé GPG

- echo "deb https ://packages.grafana.com/oss/deb stable main" |
- sudo tee -a /etc/apt/sources.list.d/grafana.list : permet d'ajouter cette version de grafana à la liste des versions stables.

- sudo apt-get update : permet la mise à jour du système et des packages installés précédemment.

- sudo apt-get -y install grafana : permet d'installer grafana depuis le dépôt APT.

- sudo systemctl enable grafana-server : permet d'activer le fichier de grafana qui se situe dans /lib/systemd/system.
  Par défaut le fichier systemd d'un service se crée dans lib/systemd/system lorsqu'on utilise apt.

- sudo systemctl start grafana-server : permet de démarrer le fichier systemd de grafana qui est grafana-server.service.
- sudo systemctl status grafana-server : permet de connaitre l'état de grafana. Grafana utilise par défaut le port 3000 donc il faut autoriser ce port au niveau de son pare feu cela permettra d'afficher grafana dans le navigateur en utilisant l'adresse IP et le port.

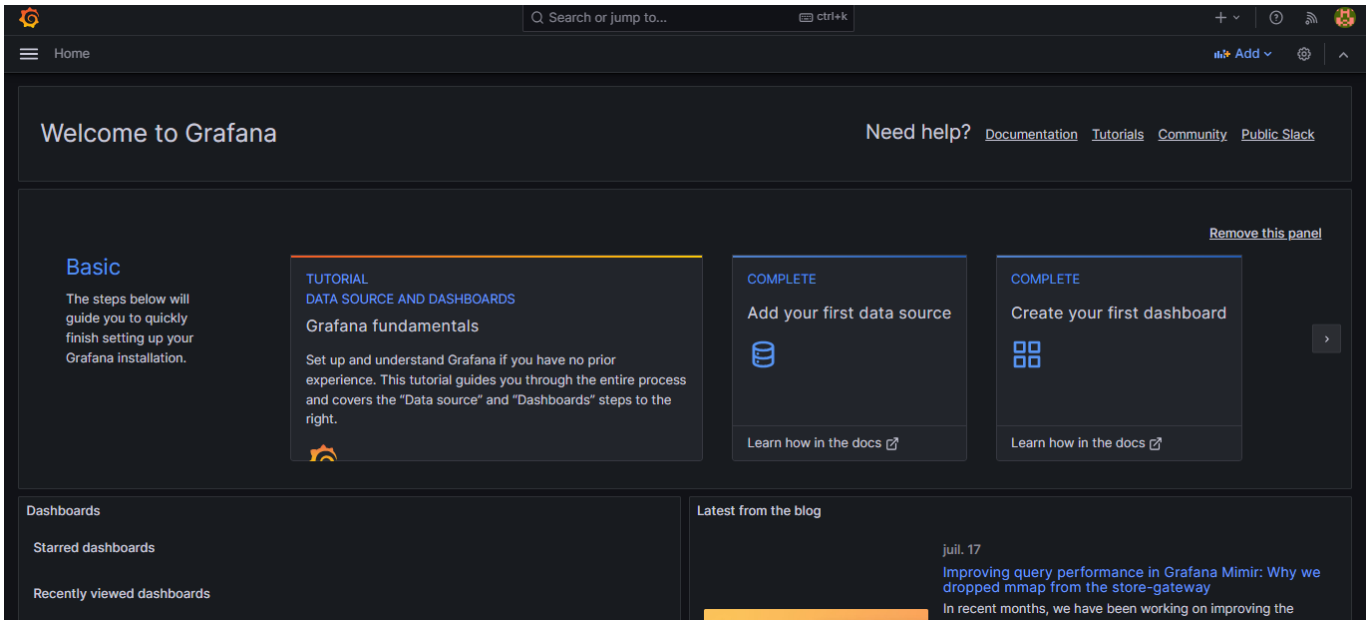


FIGURE 3.14 : Grafana

Le mot de passe par défaut est admin et le nom d'utilisateur aussi ;

3.2.3.1 Intégration des exporters de prometheus à grafana

Sur Grafana cliquez sur le signe de réglage sur la gauche. Cliquez ensuite sur « **Sources de données** ». Cliquez sur Ajouter une source de données et sélectionnez Prometheus.

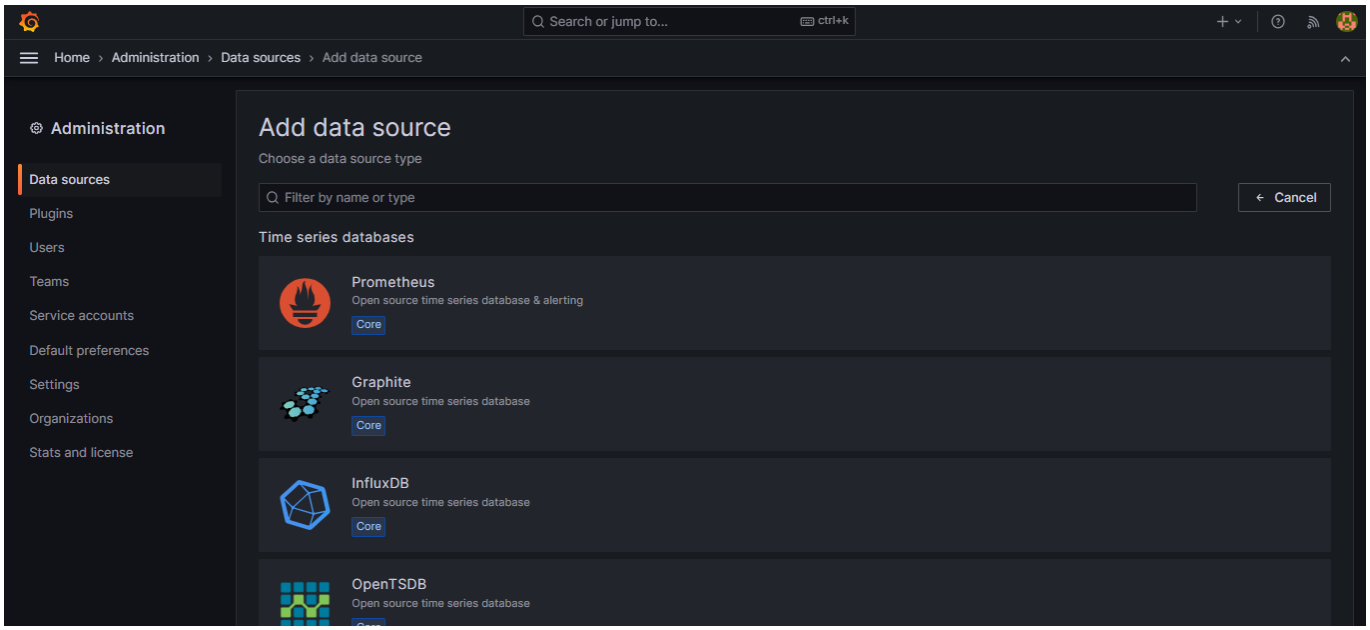


FIGURE 3.15 : Sources Grafana

Définissez l'URL comme IP du serveur Prometheus (161.97.162.94) avec le port 9090 ou localhost : 9090 si Prometheus est installer sur le même serveur que grafana.
Cliquez sur Enregistrer et tester. Vous recevrez un message de réussite de l'ajout de la source de données. (Une notification de couleur verte)

Grafana est connecté avec succès à Prometheus. Il est temps de créer un tableau de bord. Pour vous faciliter la tâche, j'utiliserai des tableaux de bord existants, qui sont présents sur le site officiel de Grafana pour surveiller les métriques du serveur Linux.
Accédez au tableau de bord d'accueil Grafana, cliquez sur le signe + et cliquez sur Importer.
Dans Importer via grafana.com, mettez l'ID du tableau de bord 1860 et cliquez sur Charger.
Sélectionnez ensuite la source de données Prometheus et cliquez sur Importer.
Le tableau de bord complet de Node Exporter est importé.
Nous pouvons voir toutes les mesures telles que la charge du système, la RAM utilisée, l'occupation du processeur, etc qui sont surveillées avec succès sur Grafana.
C'est le meme processus qui a été utilisé pour importer le tableau de bord de blackbox Exporter[4].



FIGURE 3.16 : Node Exporter1

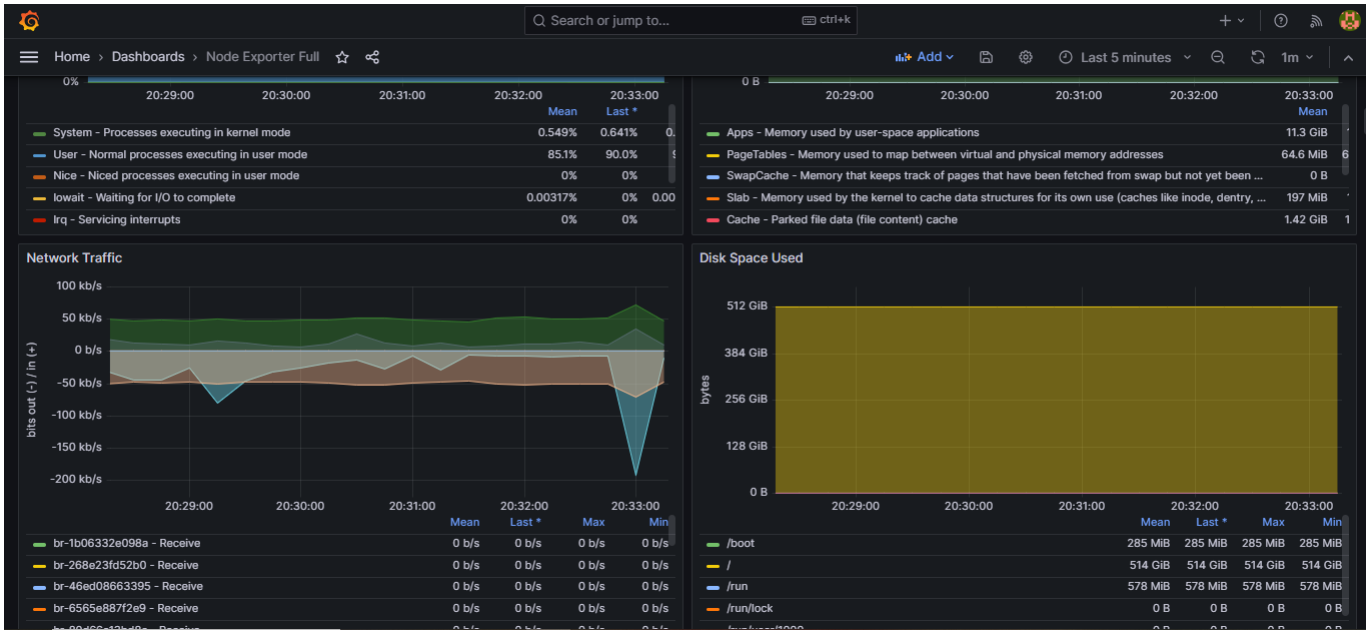


FIGURE 3.17 : Node Exporter2

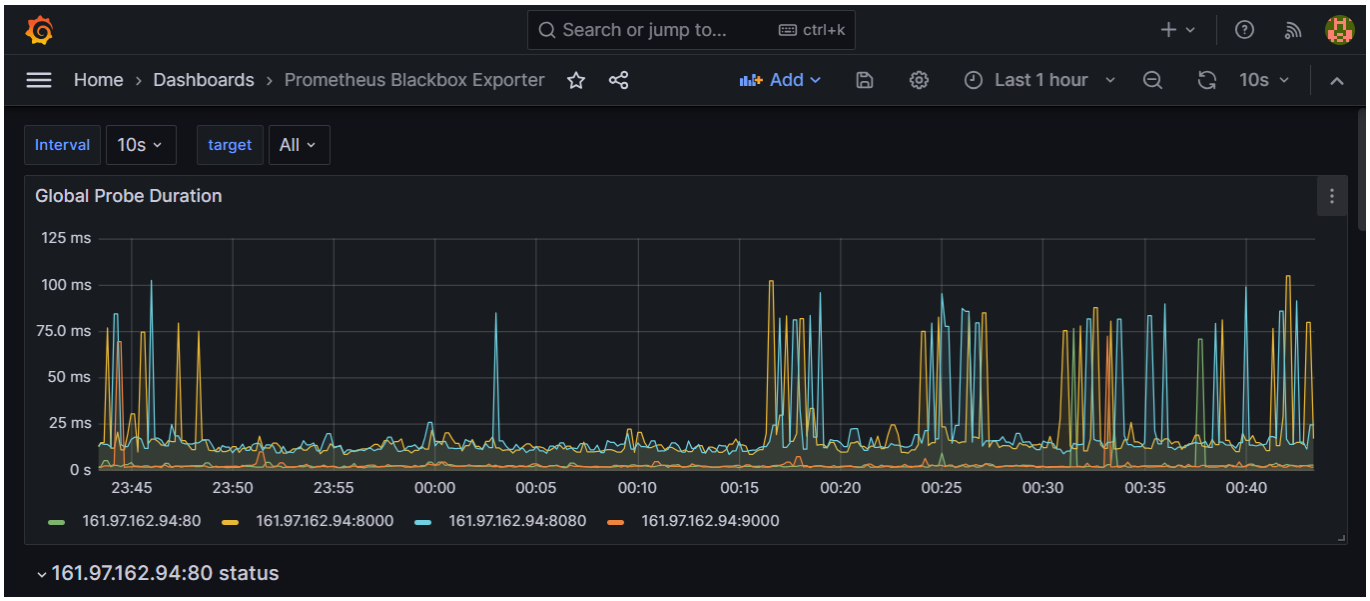


FIGURE 3.18 : Blackbox Exporter

Pour ntopng nos données sont situé dans notre base de donnée MySQl donc nous allons ajouter comme source de donnée Mysql. Le port d'écoute de Mysql est par défaut est 3306, au niveau de database nous avions inséré le nom de la base de donnée ntopng qui est **ntopng** dans notre cas. Le « user » correspond au nom d'utilisateur ayant les droits sur notre base données et le mot de passe correspond à son mot de passe.

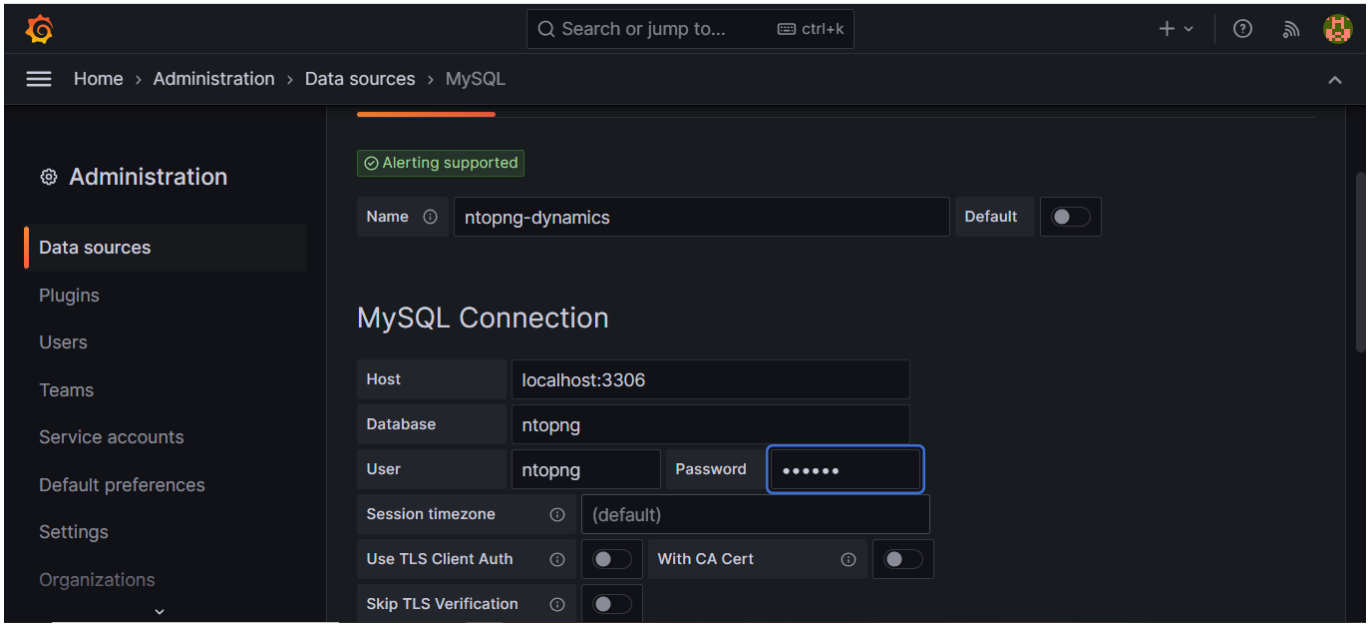


FIGURE 3.19 : Ajout Ntopng

Ensuite cliquer sur « save et test » pour ajouter la base de données comme source de donnée à grafana.
Il existe un dashboard développé par l'équipe de grafana qui répond à notre besoin donc nous allons l'importer. L'identifiant de cette base de données est **14357**.
Vous importez ce dashbord pour afficher les informations de la base de donnée ntopng.

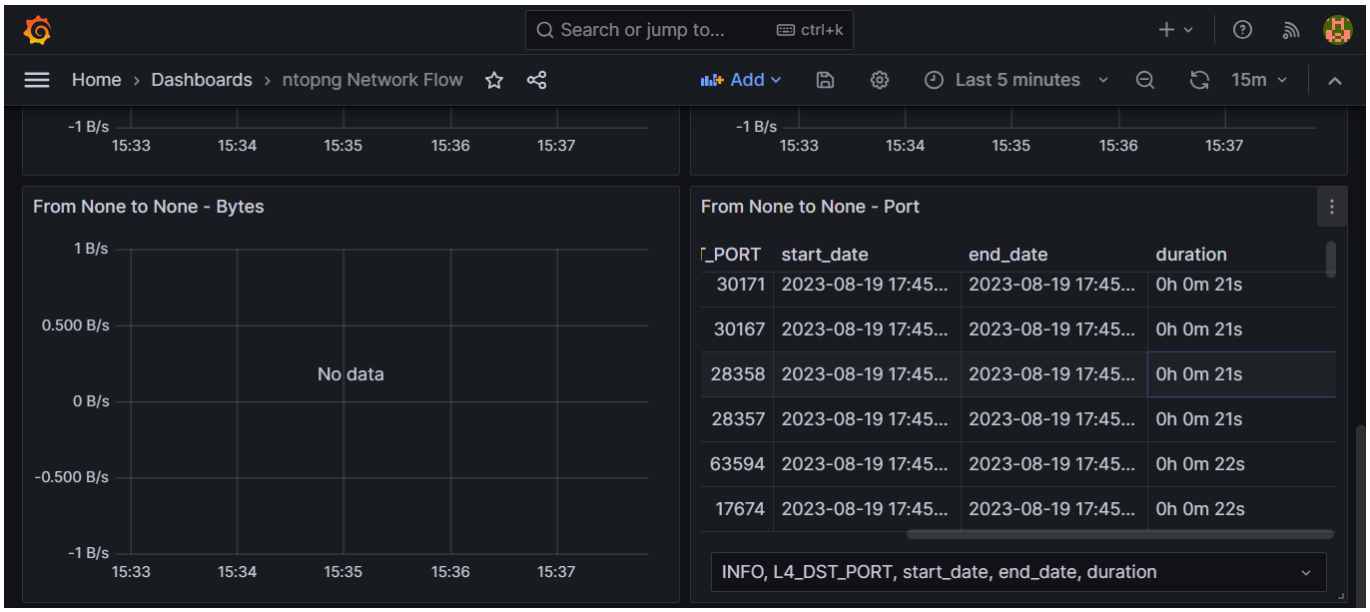


FIGURE 3.20 : Ajout Ntopng

Vous pouvez aussi trouver notre travail sur github : https ://github.com/HPJM3018/M-moire-Licence

3.3 Interpretation

Dans cette partie, nous allons effectuer une interprétation de l'état affiché par Grafana.

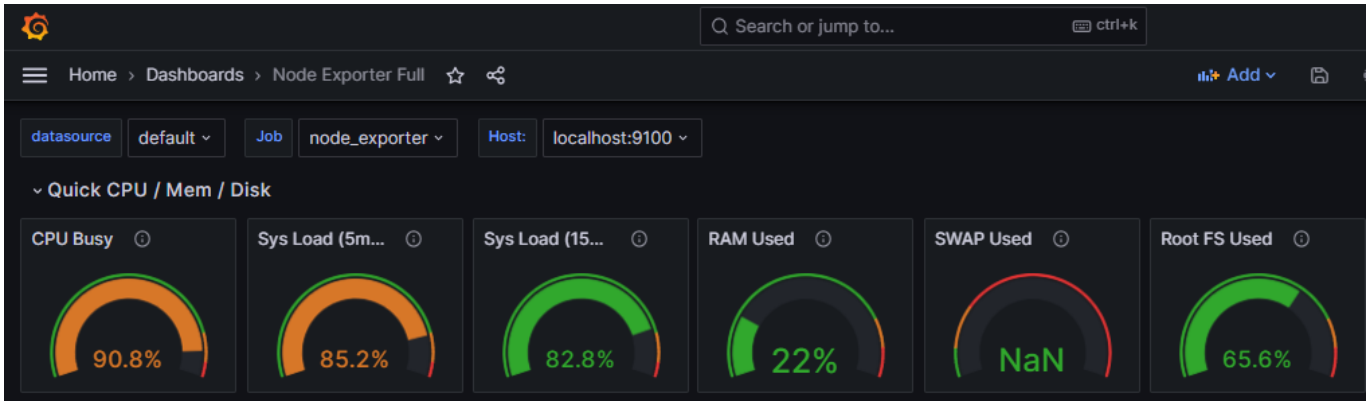


FIGURE 3.21 : Node Exporter Interpretation

L'image ci-dessus nous indique :

- Le taux d'utilisation du processeur de la machine est de 90,8/100 ;
- Le taux d'utilisation de la RAM (Random Access Memory) de la machine est de 22/100 ;
- Le SWAP n'est pas utilisé ;
- Le "Root FS used" à 65,6/100 signifie l'espace disque utilisé sur la partition racine du système de fichiers (File System) de la machine ;

– Le "Sys load" à 82,0/100 et 85,2/100 représente le nombre moyen de processus en cours d'exécution sur mon système. Ces informations permettent de mesurer l'activité du système.

3.4 Discussion

En analysant les résultats obtenus, nous pouvons affirmer que nous avons atteint nos objectifs (surveillance du flux réseau, surveillance des ressources physique, surveillance des ressource applicatives) dans la réalisation de notre projet mise en place d'un système de monitoring sur le VPS de Jilmonde Consulting. Notre système de monitoring permet à Jilmonde fournisseurs de service critique à l'état de veiller à la sécurité des données , d'assurer la défense de leurs réseaux comme le stipule les codes cy-09 et cy-11 de la Politique de Sécurité des Systèmes d'Information de l'État[3].
Cependant, en comparaison avec les solutions de monitoring existantes, notre solution présente certaines lacunes. Il convient de noter que :

– Notre solution ne comporte pas de système d'alerte.

– La surveillance du flux réseau est restreinte aux adresses IPv4.

Conclusion

Ce chapitre a fait l'objet d'un exposé des résultats obtenus à travers l'installation des différents outils de surveillance et la procédure de configuration de ces différents outils. Les pespectives ont été énnumérées afin de veiller à la disponibilité des ressources.

Conclusion

Notre objectif principal est de mettre en place un système de monitoring pour veiller à la disponibilité des ressources de Jilmonde Consulting.

Pour atteindre notre objectif, nous avons utilisé plusieurs outils tels que ntopng pour la surveillance du flux réseau, Blackbox Exporter pour la surveillance des services, et Node Exporter pour la surveillance des ressources physiques. Blackbox Exporter et Node Exporter constituent des exportateurs de Prometheus.

Afin de visualiser les différents éléments surveillés, nous avons installé Grafana, qui est un excellent outil de visualisation récent. Depuis Grafana, nous pouvons visualiser le flux réseau, la disponibilité des sites web et des ressources matérielles telles que le CPU, le SWAP et l'utilisation de la RAM.

Nous avons également détaillé l'environnement utilisé dans notre travail. Notre travail a été effectué sur le cloud, plus précisément sur le VPS de Jilmonde Consulting. Le système de monitoring étant fonctionnel, la mise en place d'un système d'alerte avec Alertmanager fait partie intégrante de nos perspectives, afin que tout comportement anormal du système soit notifié. Ceci permettra de réduire le temps de réponse aux incidents et d'assurer une disponibilité continue.

Bibliographie

[1] Mémoire : '' Mise en place d'une solution de monitoring avec Prometheus-Grafana dans l'entreprise BATI-RENOV'' présenté par Odjohoundé Salomon ATCHOBA, IFRI, 2020-2021.

[2] Mémoire : '' Conception d'une solution de monitoring des conteneurs docker.'' présenté par Jonathan Mukendi,Ecole Supérieure d'Informatique Salama - Diplôme d'ingénieur technicien en réseaux, 2018.

[3] PSSIE : ''regles-de-politique-de-protection-des-infrastructures-dinformation-critiques-en-republique-du-benin, ANSSI, 22 FEVRIER 2023.

Webographie

[1] It-num. https://001.africa/store/vps.

[2] Afriregister. https://www.afriregister.bj/hosting.php?type=9, 2023.

[3] Beninhosting. https://www.beninhosting.com/hebergement-vps-benin/, 2023.

[4] Blackbox. devconnected.com/how-to-install-and-configure-blackbox-exporter-for-prometheus/, 2023.

[5] Digitalsiteweb. https://www.digitalsiteweb.com/serveur-dedie-et-vps.php, 2023.

[6] Magit. https://www.lemagit.fr/conseil/Grafana-vs-Kibana-le-match-des-outils-de-visualisation-IT, 2023.

[7] Medium. https://medium.com/globant/monitoring-azure-vms-using-grafana-6b6636582bdd, 2023.

[8] Medium2. https://medium.com/@MetricFire/monitoring-virtual-machines-with-prometheus-vs-graphite-9f86fb7eb3f2, 2023.

[9] Oastic. https://oastic.com/posts/how-to-monitor-an-ubuntu-server-with-grafana-and-prometheus/, 2023.

[10] Wanekoo. https://wanekoo.bj/serveur-prive-virtuel-vps/, 2023.

Table des matières

Dédicace **ii**

Remerciements **iii**

Résumé **iv**

. iv

Abstract **v**

. v

List of Figures **vi**

List of Tables **vii**

Liste des acronymes **viii**

Glossaire **ix**

1 Etat de l'Art **4**

Introduction 4

1.1 Clarification Conceptuelle 4

1.1.1 Architecture des VPS 4

1.1.2 Fonctionnement des VPS 5

1.1.3 Les défis liés aux serveurs virtuels privés (VPS) 6

1.1.4 Les enjeux de sécurité liés aux VPS 6

1.1.5 Les différentes options d'hébergements pour les serveurs d'entreprise . . 6

1.1.6 Comparaison entre un serveur local et un serveur virtuel privé (VPS) . . . 6

1.2 Analyse et étude de l'existant 9

1.2.1 Quelques entreprises offrant des services de VPS au Bénin 9

1.2.1.1 IT-NUM 9

1.2.1.2 DigitalSiteWeb 9

1.2.1.3 BENIN HOSTING 9

1.2.1.4 Wanekoo 9

1.2.1.5 Afriregister 9

1.2.2 Solutions de monitoring existantes 9

1.2.3 Analyse 10

1.2.4 Problématiques 10

Conclusion 10

2 Conception et choix technique **11**
Introduction . . . 11
2.1 Etudes comparatives des solutions existantes . . . 11
2.1.1 Tableau Comparatifs . . . 11
2.2 choix de l'outil . . . 13
2.3 Description de la solution choisie ou retenue . . . 13
2.3.1 Prometheus . . . 13
2.3.2 Fonctionnements de prometheus : . . . 14
2.3.3 GRAFANA . . . 15
2.3.4 Principales caractéristiques de Grafana : . . . 15
2.3.5 NTOPNG(Network Top Next Generation) . . . 16
Conclusion . . . 16

3 Résultats et Discussion **18**
Introduction . . . 18
3.1 Architecture . . . 18
3.2 Mise en place du système de monitoring . . . 18
3.2.1 Installation de Prometheus . . . 18
3.2.1.1 Configuration des métriques au niveau de prometheus en utilisant les exporteurs . . . 20
3.2.1.2 Installation de node exporter et de blackbox exporter . . . 21
3.2.2 Installation de Ntopng . . . 23
3.2.3 Installation de Grafana . . . 26
3.2.3.1 Intégration des exporters de prometheus à grafana . . . 27
3.3 Interpretation . . . 30
3.4 Discussion . . . 31
Conclusion . . . 31

Bibliographie **33**

Webographie **34**

Table des matières **35**