

Situation professionnelle N°1 :

Monitoring proxmox et Pfsense avec
Grafana

Description :

Une entreprise me demande de mettre en place une solution pour visualiser l'utilisation de son hyperviseur (proxmox) et de son firewall (pfsense)

SOMMAIRE :

<u>Cahier des charges :</u>	Page : 3
<u>Le plan de l'infra :</u>	Page : 3
<u>Avant de commencer :</u>	Page : 4
<u>I) installation de InfluxDB :</u>	Page : 4
<u>II) configuration de Telegraf sur Pfsense :</u>	Page : 6
<u>III) configuration envoie des données depuis proxmox :</u>	Page : 8
<u>IV) VERIFICATION DE LA RÉCEPTION DES DONNÉES :</u>	Page : 8
<u>V) installation de Grafana :</u>	Page : 9
<u>VI) configuration de Grafana pour afficher les données :</u>	Page : 10

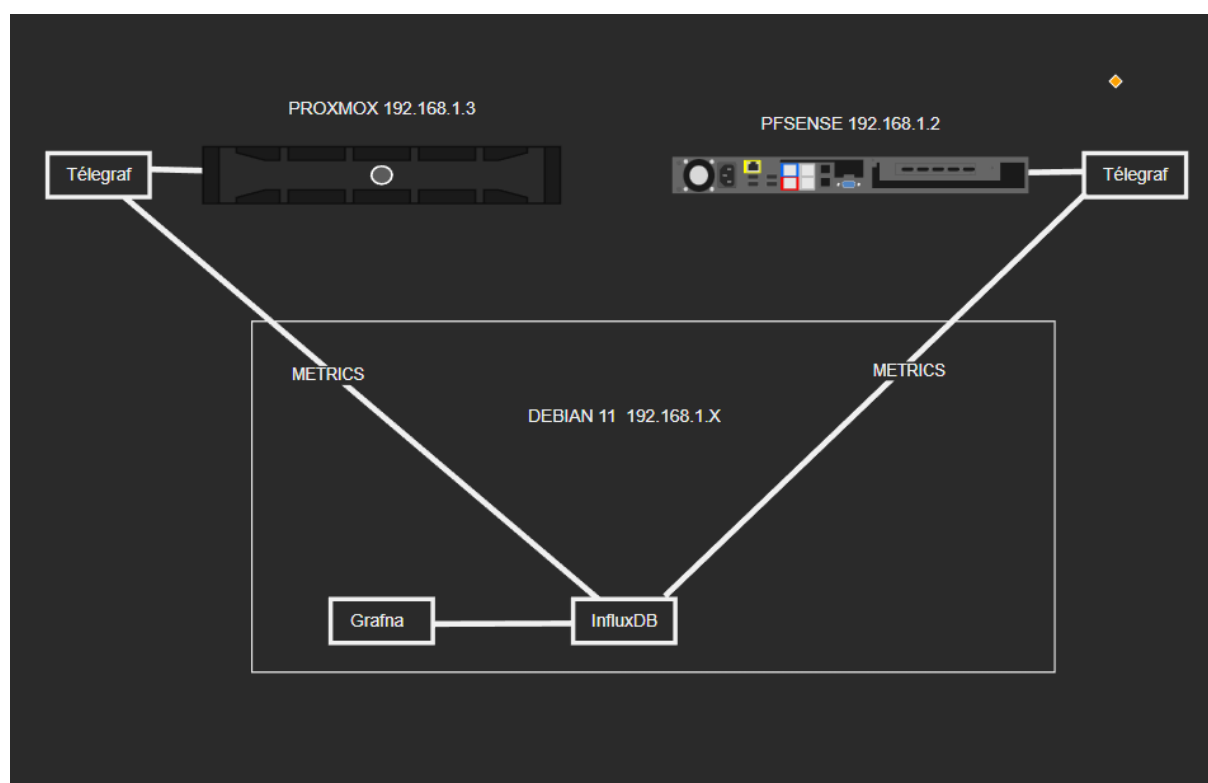
Cahier des charges :

La société info-connect souhaite visualiser son hyperviseur et son firewall

Pour permettre la visualisation des métriques des deux machines il va falloir utiliser grafana pour afficher mes donner, Télégraf pour envoyer les donner, influxDB pour stocker les donner envoyer depuis télégraf.

- Pour grafana et influxDB il seront installer sur une machine Debian 11.
- Pour telegraf il sera installé directement sur les machines concernées.

Le plan de l'infra :



Avant de commencer :

La commande sudo est à utiliser si vous n'êtes pas en root !

Il faut mettre son debian en ip static : `sudo nano /etc/network/interfaces`

Et de modifier le fichier en fonction de votre réseau !

```
GNU nano 5.4
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto ens18
iface ens18 inet static
    address 192.168.1.13
    netmask 255.255.255.0
    gateway 192.168.1.2
    dns-nameservers 192.168.1.2 8.8.8.8
```

I) INSTALLATION DE InfluxDB :

- 1) Pour commencer l'installation de InfluxDB il faut ajouter les dépôt influxDB et installer curl et wget :

La commande sudo est à utiliser si vous n'êtes pas en root !

```
sudo apt update
sudo apt install -y gnupg2 curl wget
wget -qO- https://repos.influxdata.com/influxdb.key | sudo apt-key add -
echo "deb https://repos.influxdata.com/debian $(lsb_release -cs) stable" | sudo tee
/etc/apt/sources.list.d/influxdb.list
sudo apt update
```

- 2) Après l'ajout des dépôts et installation de curl et wget on peut installer influxDB :

```
sudo apt install -y influxdb
```

3) Après avoir installer influxDB on peut démarrer et activer le service :

```
sudo systemctl enable --now influxdb
```

4) Après avoir démarré le service on peut vérifier qu'il est bien démarré avec la commande suivante :

```
systemctl status influxdb
```

```
root@Deb11-E4:~# systemctl status influxd
● influxdb.service - InfluxDB is an open-source, distributed, time series database
```

Le résultat attendu est :

```
root@Deb11-E4:~# systemctl status influxd
● influxdb.service - InfluxDB is an open-source, distributed, time series database
  Loaded: loaded (/lib/systemd/system/influxdb.service; enabled; vendor preset: enabled)
  Active: active (running) since Sun 2022-11-13 14:26:59 CET; 59min ago
    Docs: https://docs.influxdata.com/influxdb/
  Process: 12983 ExecStart=/usr/lib/influxdb/scripts/influxd-systemd-start.sh (code=exited, status=0/SUCCESS)
 Main PID: 12984 (influxd)
   Tasks: 10 (limit: 4591)
  Memory: 27.0M
    CPU: 2.484s
  CGroup: /system.slice/influxdb.service
          └─12984 /usr/bin/influxd -config /etc/influxdb/influxdb.conf
```

5) Ensuite on va créer un user et une base de données pour stocker les données :

5.1) création de l'utilisateur : `CREATE USER admin WITH PASSWORD '<password>' WITH ALL PRIVILEGES`

```
root@Deb11-E4:~# influx
Connected to http://localhost:8086 version 1.8.10
InfluxDB shell version: 1.8.10
> CREATE USER admin WITH PASSWORD '<password>' WITH ALL PRIVILEGES
```

Pour voir que la création a bien eu lieu : `SHOW USERS`

```
root@Deb11-E4:~# influx
Connected to http://localhost:8086 version 1.8.10
InfluxDB shell version: 1.8.10
> SHOW USERS
user admin
-----
admin true
>
```

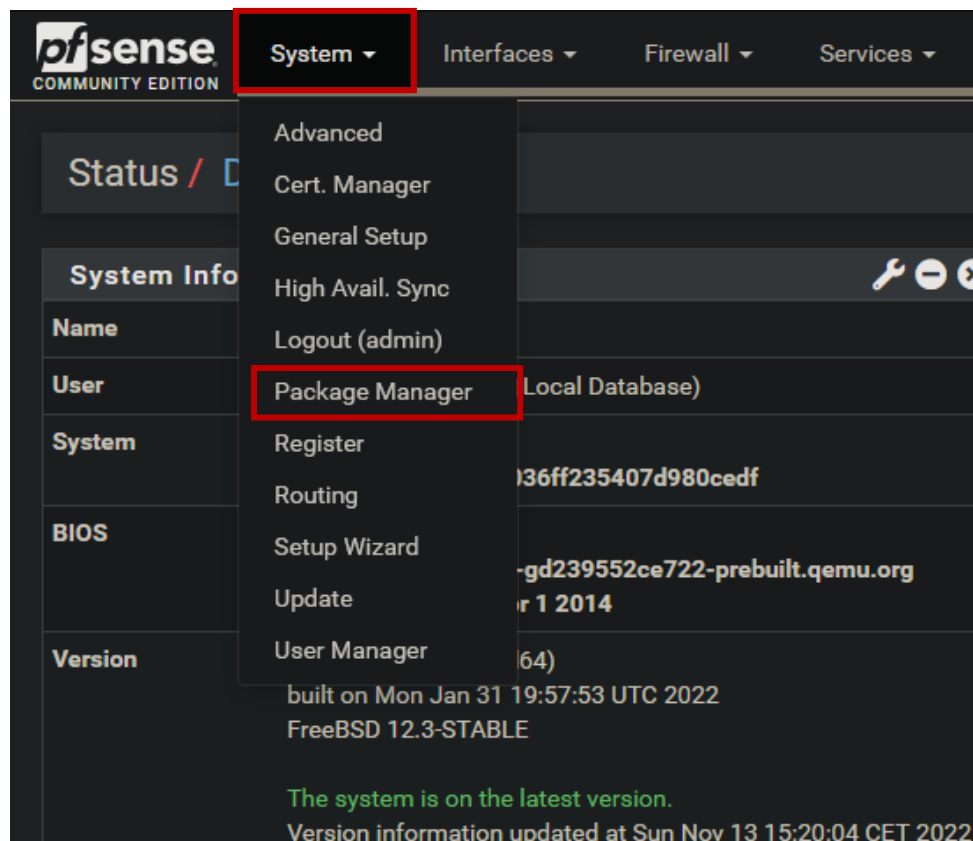
5.2) création de la base de données : `CREATE DATABASE monitoring` puis `SHOW DATABASES` pour vérifier

```
> CREATE DATABASE monitoring
> SHOW DATABASES
name: databases
name
----
 _internal
 monitoring
>
```

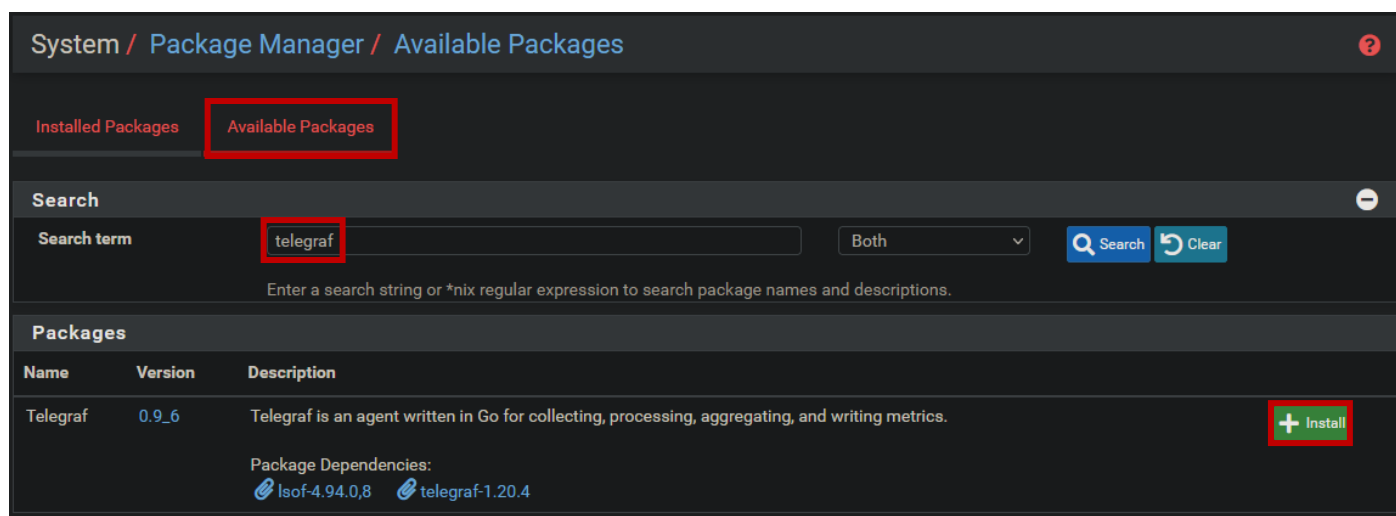
La partie installation et configuration de influx et maintenant terminée on va pouvoir passer à l'envoi des données :

II) CONFIGURATION DE TELEGRAF SUR PFSENSE :

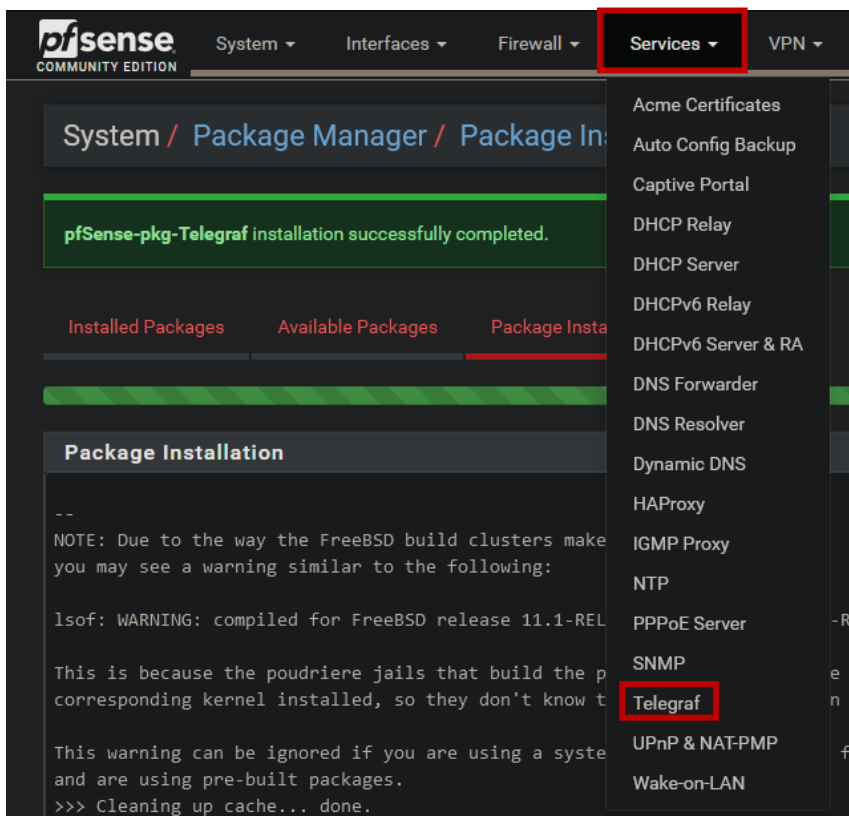
- 1) Une fois sur le Pfsense il faut installer le packet telegraf pour cela se rend dans system et gestionnaire de packet :



Puis dans packet disponible recherche telegraf et cliquer sur installer puis confirmer :



2) Une fois installer on se rend dans services puis telegraf :



3) On remplit les champs en fonction de ce que on a configuré avant : (mots de passe, username, IP etc.)
Puis tout en bas on clique sur Save :

Package / Services: Telegraf

General Options

Enable ☒ Enable Telegraf.

Update Interval: 5
Seconds. Default: 10 if not specified

Telegraf Output: InfluxDB, ElasticSearch, Graphite

InfluxDB Server: http://192.168.1.13:8086
Full HTTP or UDP endpoint URL for InfluxDB instance. E.g.: http://192.168.1.23:8086 for a default InfluxDB installation

InfluxDB Database: monitoring
Target database for metrics (created if does not exist)

InfluxDB Username: admin
Database user name if required by InfluxDB config

InfluxDB Password:
Database password if required by InfluxDB config

Skip SSL verify ☒ Use SSL but skip chain and host verification

Short Hostname ☒ Use short hostname instead of FQDN

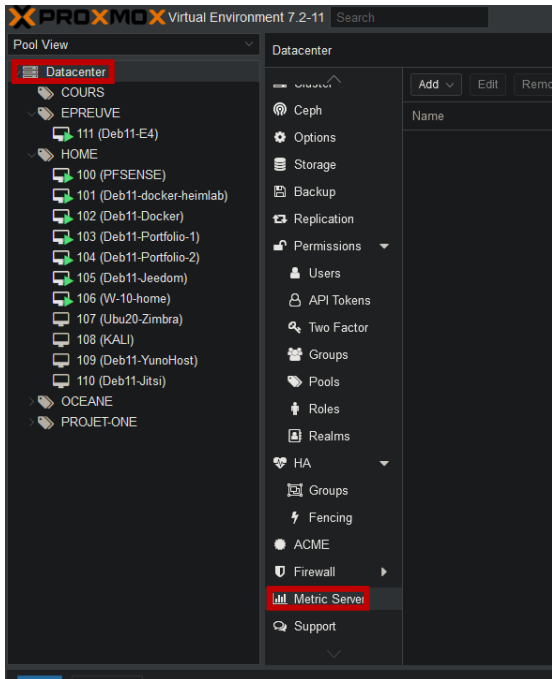
ElasticSearch Servers:
Full HTTP endpoint URL for ElasticSearch instance. E.g.: http://192.168.1.23:9200

Additional directives for telegraf.conf.

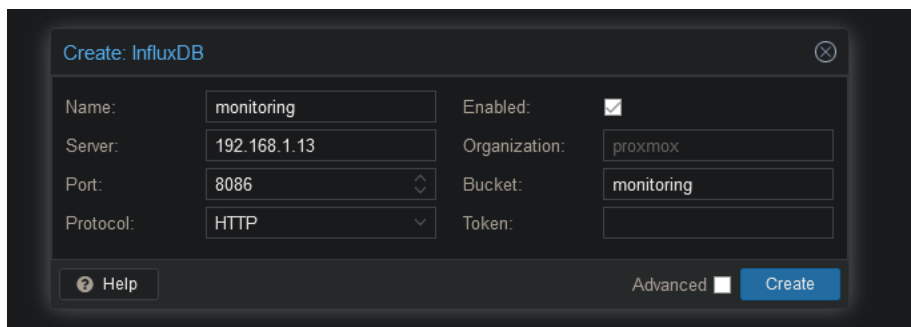
Save

III) configuration envoi des données depuis proxmox :

- 1) Une fois sur proxmox cliquer sur datacenter puis Metric Servers puis sur add influxDB :



- 2) Ensuite on va remplir les informations de notre influxDB :



IV) VERIFICATION DE LA RÉCEPTION DES DONNÉES :

- 1) Pour verifier que notre influxDB recois bien les données il suffit d'utiliser cette commande :

Systemctl status influxdb :

```
root@Debian-E4:~# systemctl status influxdb
● influxdb.service - InfluxDB is an open-source, distributed, time series database
   Loaded: loaded (/lib/systemd/system/influxdb.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2022-11-13 14:26:59 CET; 1h 10min ago
     Docs: https://docs.influxdata.com/influxdb/
   Process: 12983 ExecStart=/usr/lib/influxdb/scripts/influxd-systemd-start.sh (code=exited, status=0/SUCCESS)
   Main PID: 12984 (influxd)
     Tasks: 10 (limit: 4591)
    Memory: 43.9M
       CPU: 3.672s
    CGroup: /system.slice/influxdb.service
            └─12984 /usr/bin/influxd -config /etc/influxdb/influxdb.conf

nov. 13 15:37:13 Debian-E4 influxd-systemd-start.sh[12984]: [httpd] 192.168.1.2 - admin [13/Nov/2022:15:37:13 +0100] "POST /write?db=monitoring HTTP/1.1" 204 0 "-" "Telegraf/1.20.4 Go/1.17.4" aa08dcd2-6366b
nov. 13 15:37:23 Debian-E4 influxd-systemd-start.sh[12984]: [httpd] 192.168.1.2 - admin [13/Nov/2022:15:37:23 +0100] "POST /write?db=monitoring HTTP/1.1" 204 0 "-" "Telegraf/1.20.4 Go/1.17.4" b0009238-6366b
nov. 13 15:37:33 Debian-E4 influxd-systemd-start.sh[12984]: [httpd] 192.168.1.2 - admin [13/Nov/2022:15:37:33 +0100] "POST /write?db=monitoring HTTP/1.1" 204 0 "-" "Telegraf/1.20.4 Go/1.17.4" b5fcd1a-6366b
nov. 13 15:37:43 Debian-E4 influxd-systemd-start.sh[12984]: [httpd] 192.168.1.2 - admin [13/Nov/2022:15:37:43 +0100] "POST /write?db=monitoring HTTP/1.1" 204 0 "-" "Telegraf/1.20.4 Go/1.17.4" bbf3b092-6366b
nov. 13 15:37:49 Debian-E4 influxd-systemd-start.sh[12984]: [httpd] 192.168.1.3 - [13/Nov/2022:15:37:49 +0100] "GET /health HTTP/1.1" 200 107 "-" "libwww-perl/6.52" bf23c0ab-6366b-11ed-809d-4ef686473bb9 75
nov. 13 15:37:49 Debian-E4 influxd-systemd-start.sh[12984]: [httpd] 192.168.1.3 - [13/Nov/2022:15:37:49 +0100] "POST /api/v2/write?org=proxmox&bucket=monitoring HTTP/1.1" 400 153 "-" "libwww-perl/6.52" bf
nov. 13 15:37:49 Debian-E4 influxd-systemd-start.sh[12984]: [httpd] 192.168.1.3 - [13/Nov/2022:15:37:49 +0100] "POST /api/v2/write?org=proxmox&bucket=monitoring HTTP/1.1" 400 154 "-" "libwww-perl/6.52" bf
nov. 13 15:37:49 Debian-E4 influxd-systemd-start.sh[12984]: [httpd] 192.168.1.3 - [13/Nov/2022:15:37:49 +0100] "POST /api/v2/write?org=proxmox&bucket=monitoring HTTP/1.1" 400 153 "-" "libwww-perl/6.52" bf
nov. 13 15:37:50 Debian-E4 influxd-systemd-start.sh[12984]: [httpd] 192.168.1.3 - [13/Nov/2022:15:37:50 +0100] "POST /api/v2/write?org=proxmox&bucket=monitoring HTTP/1.1" 204 0 "-" "libwww-perl/6.52" bfb
nov. 13 15:37:54 Debian-E4 influxd-systemd-start.sh[12984]: [httpd] 192.168.1.2 - admin [13/Nov/2022:15:37:54 +0100] "POST /write?db=monitoring HTTP/1.1" 204 0 "-" "Telegraf/1.20.4 Go/1.17.4" c1ef0d71-6366b
lines 1-22/22 (END)
```

On voit bien deux IP qui envoient des données c'est que l'envoi fonctionne parfaitement :

V) INSTALLATION DE GRAFANA :

- 1) Pour commencer l'installation de Grafana il faut ajouter les dépôt Grafana et installer Apt-transport-https :

La commande sudo est à utiliser si vous n'êtes pas en root !

```
sudo apt-get install -y apt-transport-https
sudo apt-get install -y software-properties-common wget
sudo wget -q -O /usr/share/keyrings/grafana.key https://apt.grafana.com/gpg.key
echo "deb [signed-by=/usr/share/keyrings/grafana.key] https://apt.grafana.com stable
main" | sudo tee -a /etc/apt/sources.list.d/grafana.list
```

- 2) Une fois les dépôt ajouter et les paquets requis installer on peut passer à l'installation de Grafana :

```
sudo apt-get update
```

```
sudo apt-get install grafana
```

- 3) Une fois l'installation terminer on va démarrer le service et vérifier que il n'y a pas d'erreurs :

```
sudo systemctl daemon-reload
sudo systemctl start grafana-server
sudo systemctl status grafana-server
sudo systemctl enable grafana-server.service
```

```
root@Debian11-E4:~# systemctl status grafana-server.service
● grafana-server.service - Grafana instance
   Loaded: loaded (/lib/systemd/system/grafana-server.service; disabled; vendor preset: enabled)
   Active: active (running) since Sun 2022-11-13 14:23:26 CET; 4h 40min ago
     Docs: http://docs.grafana.org
   Main PID: 10081 (grafana-server)
    Tasks: 11 (limit: 4591)
   Memory: 74.7M
      CPU: 16.743s
   CGroup: /system.slice/grafana-server.service
           └─10081 /usr/sbin/grafana-server --config=/etc/grafana/grafana.ini --pidfile=/run/grafana/grafana-server.pid --packaging=deb cfg:default.paths.logs=/var/log/grafana cfg:default.paths.data=/var

nov. 13 17:33:28 Debian11-E4 grafana-server[10081]: logger=cleanup t=2022-11-13T17:33:28.192850338+01:00 level=info msg="Completed cleanup jobs" duration=100.345513ms
nov. 13 17:43:28 Debian11-E4 grafana-server[10081]: logger=cleanup t=2022-11-13T17:43:28.392724437+01:00 level=info msg="Completed cleanup jobs" duration=209.480411ms
nov. 13 17:53:28 Debian11-E4 grafana-server[10081]: logger=cleanup t=2022-11-13T17:53:28.325969761+01:00 level=info msg="Completed cleanup jobs" duration=233.441793ms
nov. 13 18:03:28 Debian11-E4 grafana-server[10081]: logger=cleanup t=2022-11-13T18:03:28.324860328+01:00 level=info msg="Completed cleanup jobs" duration=231.820807ms
nov. 13 18:13:28 Debian11-E4 grafana-server[10081]: logger=cleanup t=2022-11-13T18:13:28.191559962+01:00 level=info msg="Completed cleanup jobs" duration=99.04342ms
nov. 13 18:23:28 Debian11-E4 grafana-server[10081]: logger=cleanup t=2022-11-13T18:23:28.303037488+01:00 level=info msg="Completed cleanup jobs" duration=210.267751ms
nov. 13 18:33:28 Debian11-E4 grafana-server[10081]: logger=cleanup t=2022-11-13T18:33:28.196348984+01:00 level=info msg="Completed cleanup jobs" duration=103.289611ms
nov. 13 18:43:28 Debian11-E4 grafana-server[10081]: logger=cleanup t=2022-11-13T18:43:28.451697868+01:00 level=info msg="Completed cleanup jobs" duration=359.209325ms
nov. 13 18:53:28 Debian11-E4 grafana-server[10081]: logger=cleanup t=2022-11-13T18:53:28.465314915+01:00 level=info msg="Completed cleanup jobs" duration=371.955947ms
nov. 13 19:03:28 Debian11-E4 grafana-server[10081]: logger=cleanup t=2022-11-13T19:03:28.188269821+01:00 level=info msg="Completed cleanup jobs" duration=94.93703ms
lines 1-21/21 (END)
```

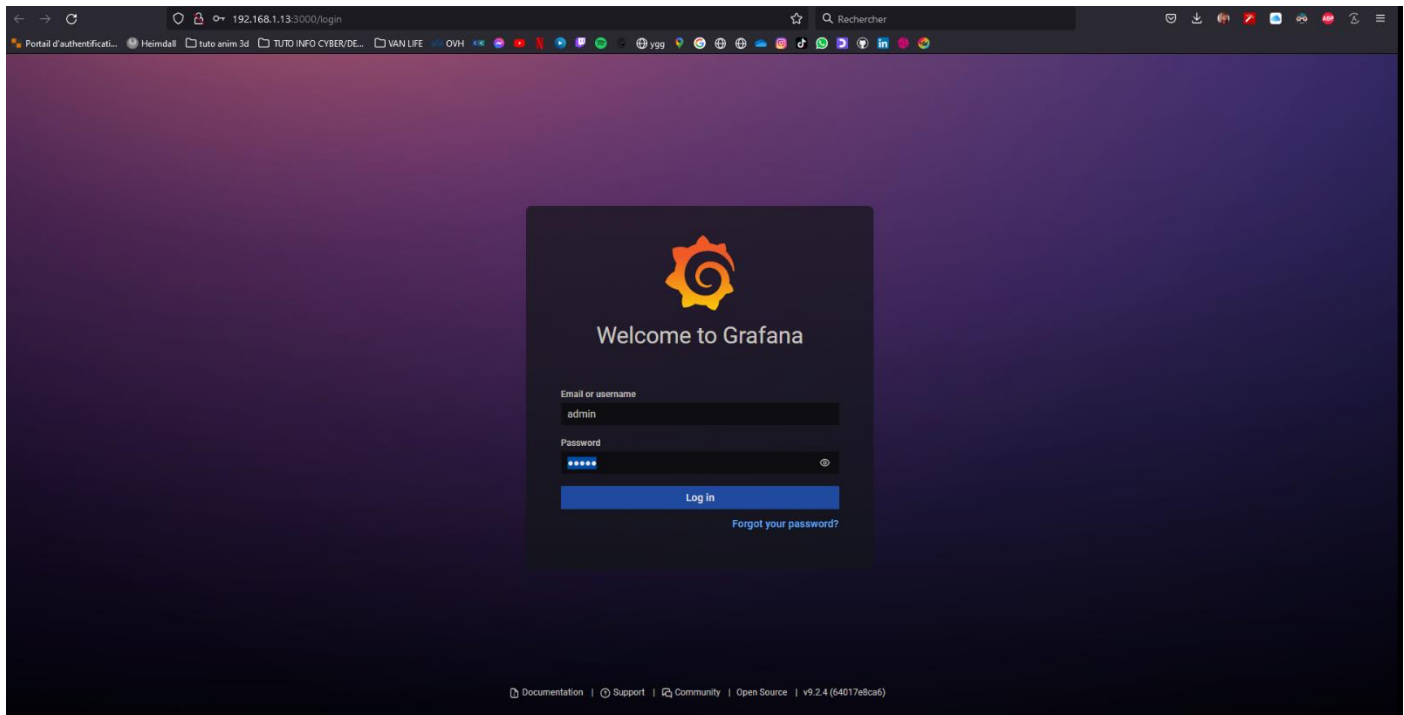
Parfait grafana est bien installer et fonctionne correctement :

On va pouvoir passer à la suite pour configurer l'affichage dans grafana des données pour cela,

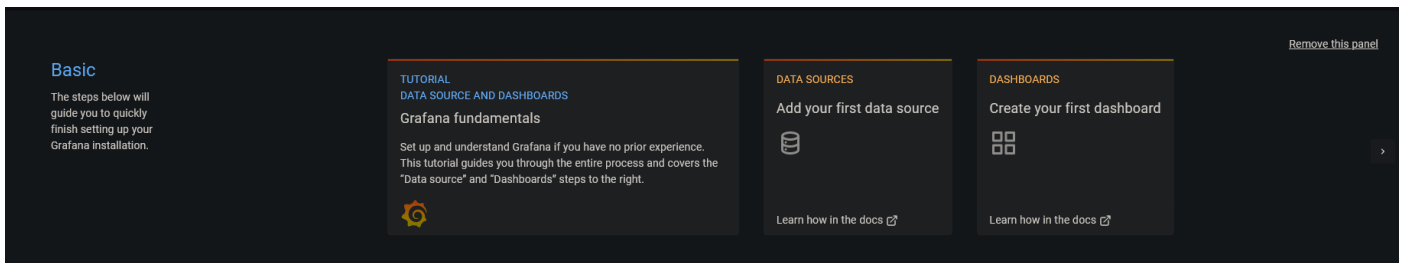
Il faut se rendre sur l'interface web de grafana <http://192.168.13:3000> (ne pas oublier le port !).

VI) CONFIGURATION DE GRAFANA POUR AFFICHER LES DONNÉES :

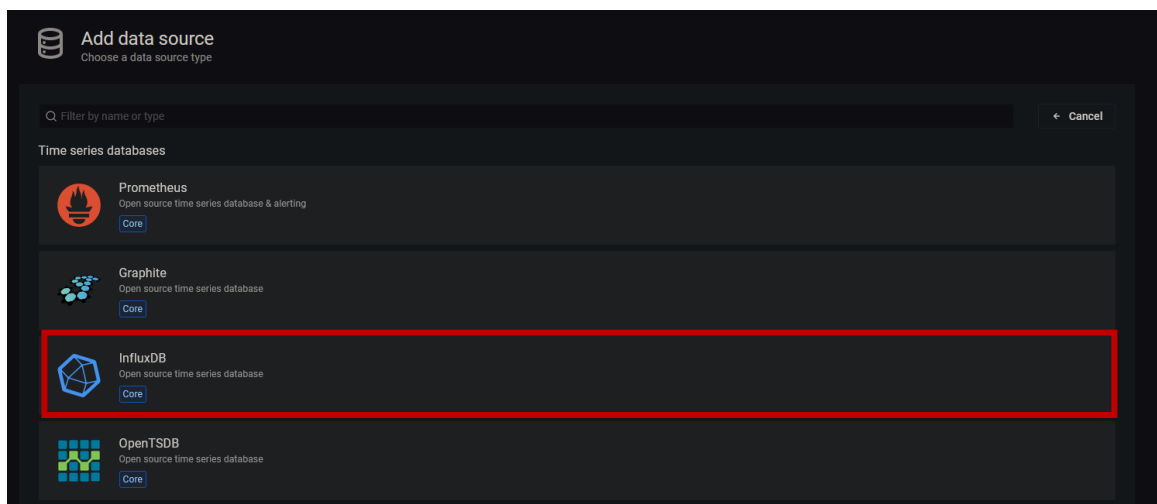
- 1) Une fois arriver sur l'interface web l'username et le mot de passe par défaut est admin / admin
(Après ça il va falloir changer le mot de passe par default)



- 2) Pour commencer on va ajouter une base de données (dans notre cas se sera influxDB)
Pour cela cliquer sur « add you first data source » :



- 3) On clique ensuite sur influxDB :



4) On donne un nom à notre base, on a choisi la bonne méthode de requête puis on remplit l'IP de notre

✓ Alerting supported

Name ⓘ

monitoring

Default

☒

Query Language

InfluxQL ▾

HTTP

URL ⓘ	http://192.168.1.13:8086
Allowed cookies ⓘ	New tag (enter key to add)
Timeout ⓘ	Timeout in seconds

Auth

Basic auth	<input type="checkbox"/>	With Credentials ⓘ	<input type="checkbox"/>
TLS Client Auth	<input type="checkbox"/>	With CA Cert ⓘ	<input type="checkbox"/>
Skip TLS Verify	<input type="checkbox"/>		
Forward OAuth Identity ⓘ	<input type="checkbox"/>		

- 5) Dans la partie base de cette page on remplit (le nom de notre database, username, mots de passe et http Method en GET) puis on clique sur Save & test et si le message si dessous apparait c'est que votre base a bien été lu par Grafana !!

InfluxDB Details

Database Access

Setting the database for this datasource does not deny access to other databases. The InfluxDB query syntax allows switching the database in the query. For example: `SHOW MEASUREMENTS ON _internal` or `SELECT * FROM "_internal".. "database" LIMIT 10`

To support data isolation and security, make sure appropriate permissions are configured in InfluxDB.

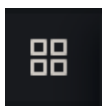
Database	monitoring	
User	admin	
Password	configured	Reset
HTTP Method	GET	
Min time interval	10s	
Max series	1000	

✓ datasource is working. 17 measurements found

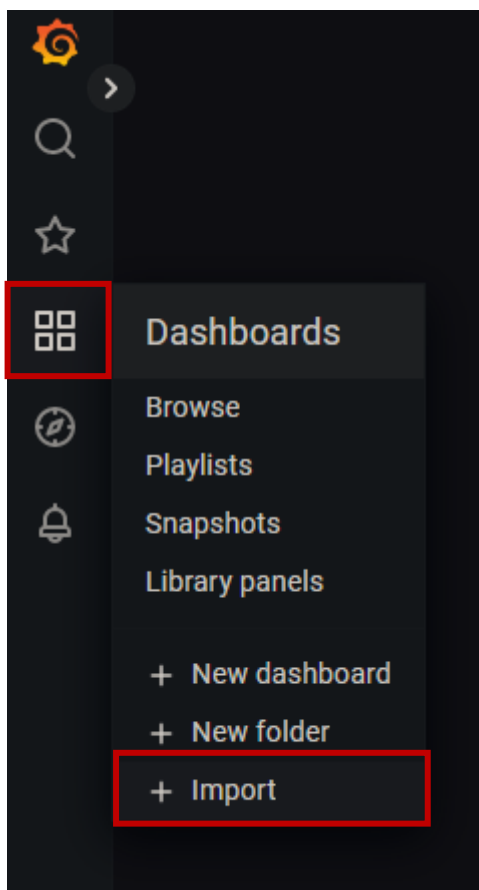
Back Explore Delete Save & test

- 6) Ensuite pour afficher les données stocker dans notre influx on va utiliser un Dashboard pour chaque machine qui va afficher toutes les valeurs.

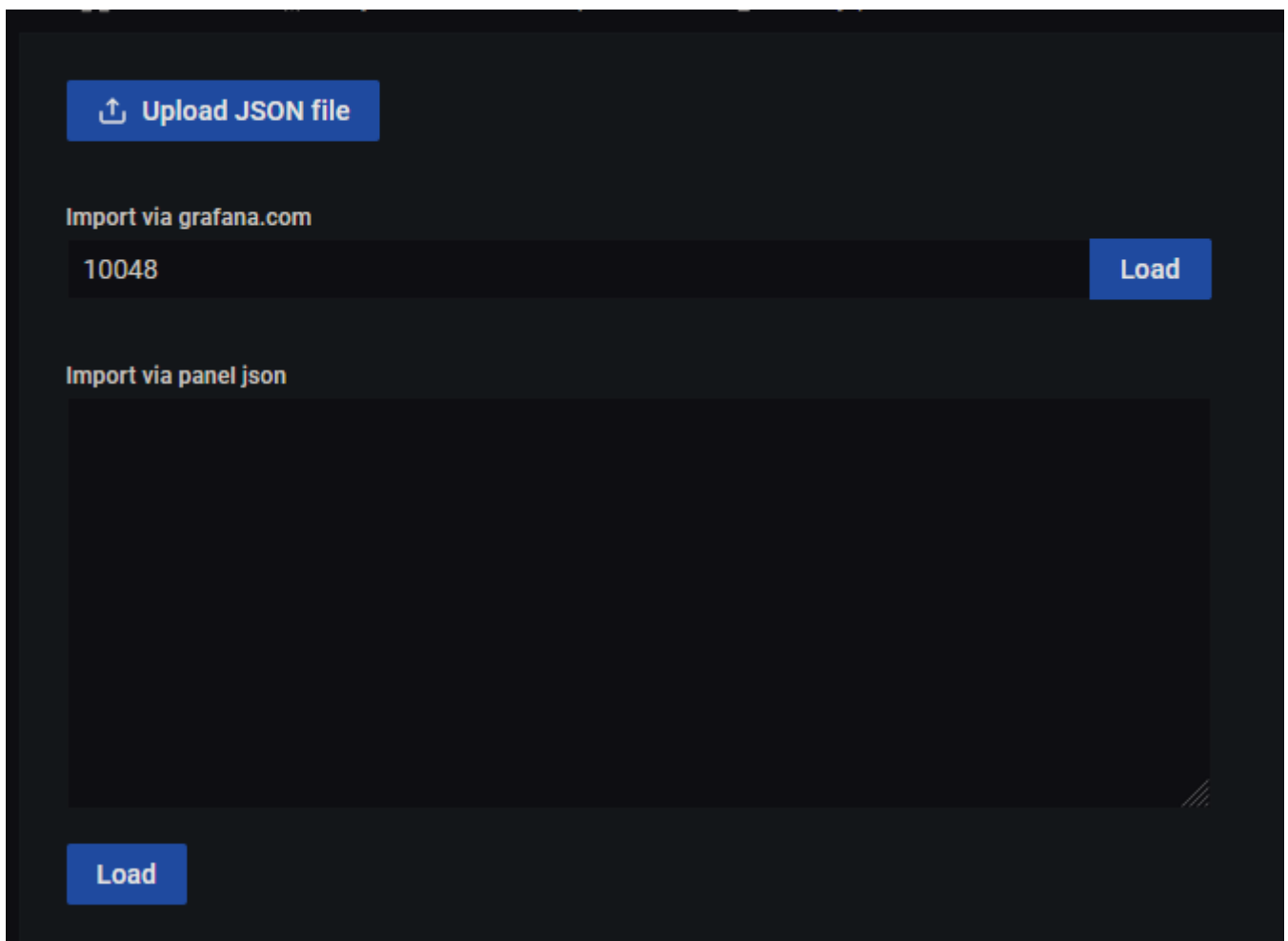
Pour importer un Dashboard il faut aller sur :



puis dans import :



- 7) Dans la page, dans le champ import via Grafana.com coller L'ID : 10048 (ce Dashboard sera utilisé pour afficher les données du proxmox) puis on clique sur Load :



Upload JSON file

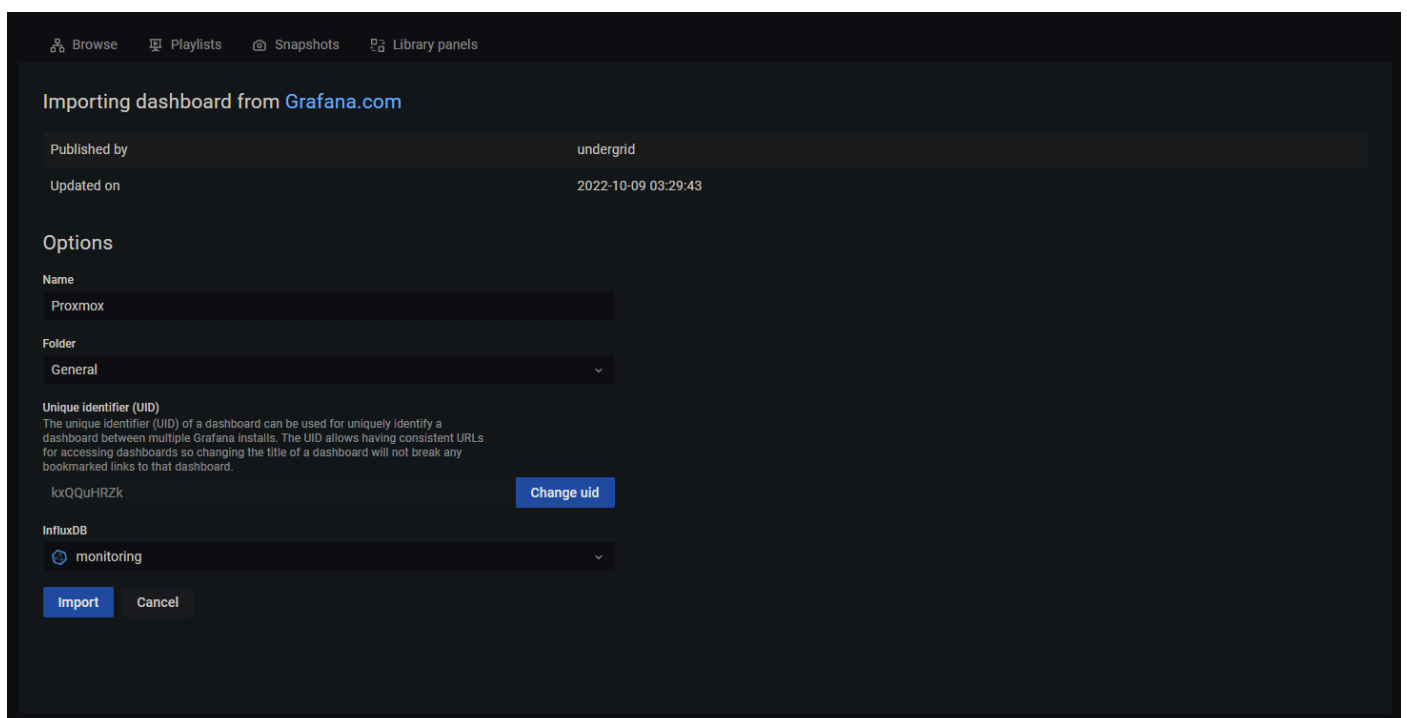
Import via grafana.com

10048 Load

Import via panel json

Load

- 8) on va ensuite donner un nom a notre Dashboard, un dossier si jamais on veut les ranger dans des dossier différents on prendra celui par défaut, puis on doit sélectionner notre base de données pour nous elle s'appelle "monitoring" pour finir on clique sur import.



Browse Playlists Snapshots Library panels

Importing dashboard from Grafana.com

Published by undergrid

Updated on 2022-10-09 03:29:43

Options

Name Proxmox

Folder General

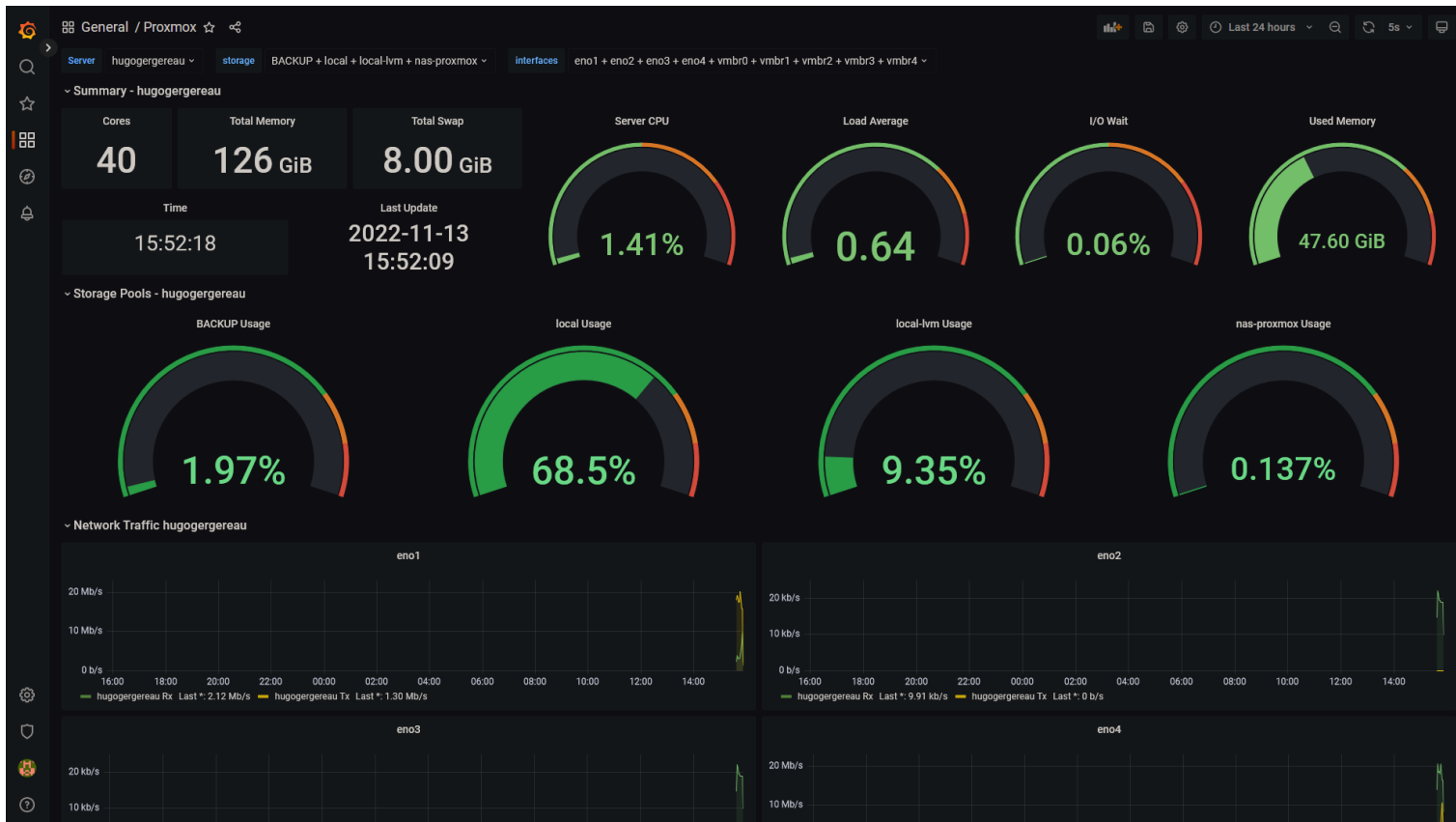
Unique identifier (UID)
The unique identifier (UID) of a dashboard can be used to uniquely identify a dashboard between multiple Grafana installs. The UID allows having consistent URLs for accessing dashboards so changing the title of a dashboard will not break any bookmarked links to that dashboard.

kxQQuHRZk Change uid

InfluxDB monitoring

Import Cancel

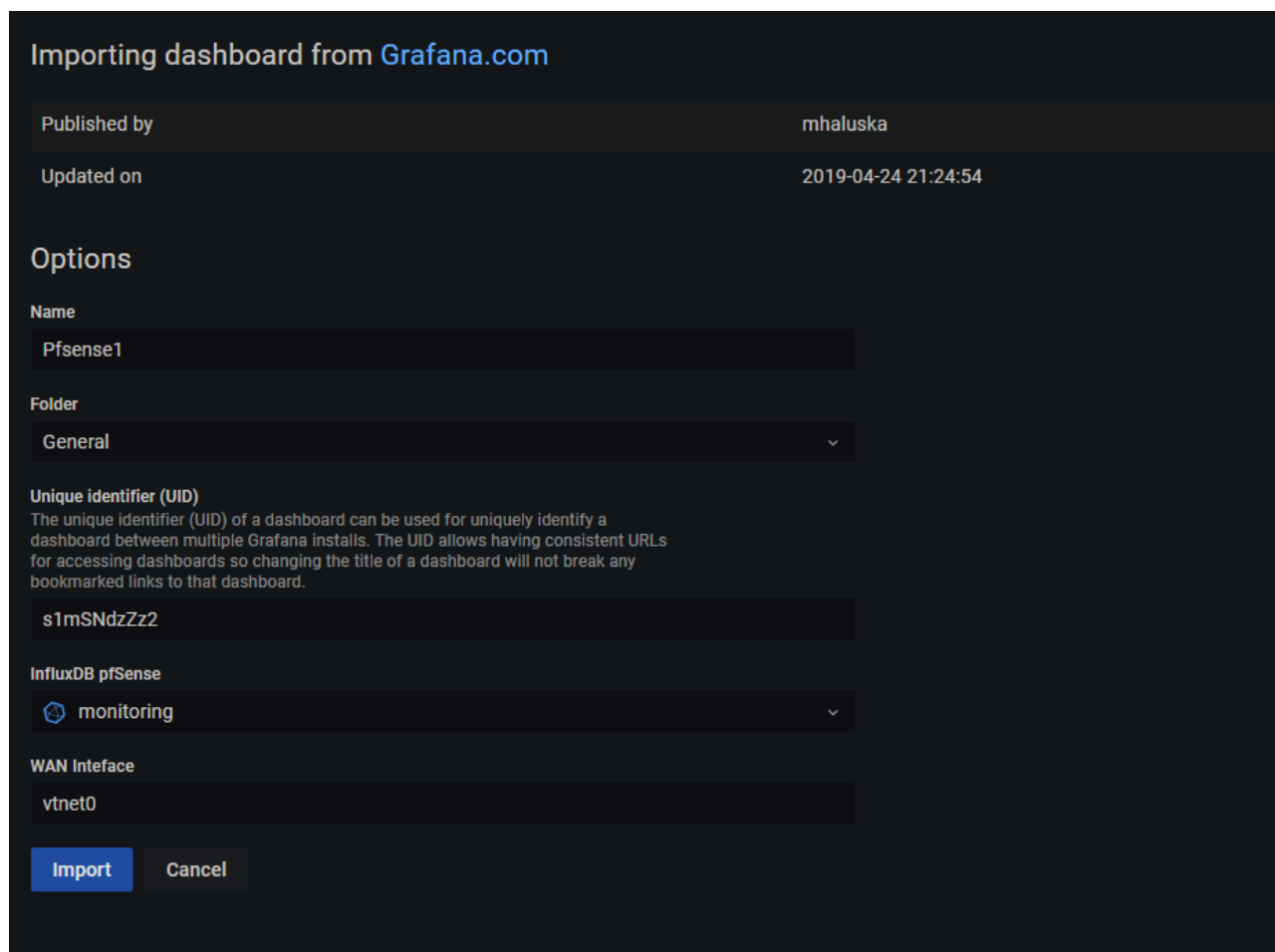
9) Après quelques secondes d'actualisation on devrait commencer à voir apparaître des informations dans le Dashboard comme si dessous :



10) après avoir fini avec proxmox nous allons afficher les données du Pfsense pour cela dans la page d'importation comme vu au pare-avant copier L'ID : 10095 puis cliquer sur Load

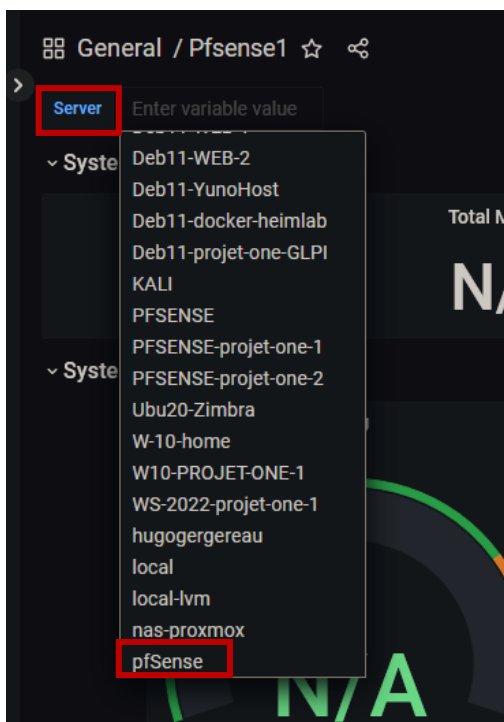
The screenshot shows the Grafana import page. At the top, there is a blue button labeled 'Upload JSON file'. Below this, the 'Import via grafana.com' section is active, featuring a text input field containing the ID '10095' and a blue 'Load' button. The 'Import via panel json' section is currently inactive.

- 11) Comme pour proxmox on ajoute un nom, un dossier, le nom de notre base, et le nom de l'interface WAN de notre Pfsense puis on clique sur import :



The screenshot shows the 'Importing dashboard from Grafana.com' interface. It includes a header with the title 'Importing dashboard from Grafana.com'. Below this, there are two rows of metadata: 'Published by' (mhaluska) and 'Updated on' (2019-04-24 21:24:54). The 'Options' section contains several fields: 'Name' (Pfsense1), 'Folder' (General), 'Unique identifier (UID)' (s1mSNdzZz2), 'InfluxDB pfSense' (monitoring), and 'WAN Interface' (vtnet0). At the bottom, there are 'Import' and 'Cancel' buttons.

- 12) Si jamais rien ne s'affiche et qu'il y a marqué NA sur tout les graph il faut bien vérifier que on a bien sélectionner le pfsense comme server sur le Dashboard pour le sélectionner il faut cliquer sur server et sélectionner notre Pfsense :



13) Apres quelques secondes d'actualisation on devrait commencer à voir apparaitre des informations dans le Dashboard comme si dessous :



VOILA NOTRE PROMOX ET PFSENSE SONT MAINTENANT EQUIPÉ D'UNE SOLUTION DE MONITORING !!!