

Monitor your infra || die("No check=>No prod=>No job");

Jean-Marc Pouchoulon

Décembre 2021

1 Objectifs du TP et organisation.

1.1 Les compétences à acquérir à la fin de cette séance sont les suivantes :

- Utilisez le protocole SNMP et un agent pour superviser et obtenir des éléments de métrologie.
- Monitorisez l'infrastructure de l'IUT à l'aide d'un logiciel standard de supervision (OMD).
- Mettre en place de la métrologie sur votre poste Linux (Grafana, influxDB, Telegraf, collectd).

1.2 Organisation, recommandations et notation du TP.

Vous travaillerez par groupe de deux en vous répartissant le travail du TP. Il vous explicitement demandé de faire valider votre travail par l'enseignant. Ces "checks" permettront de vous noter. Un compte rendu succinct (fichiers de configuration , copie d'écran montrant la réussite de la construction ...) est demandé et à rendre sur Moodle Didex.

2 Utilisation de SNMP comme vecteur de monitoring.

2.1 Installez le client SNMP sous Linux

```
apt-get update
apt-get install snmp snmp-mibs-downloader

#Remplacez la ligne dans /etc/snmp/snmp.conf par
mibs +ALL

# Remplacer la mib qui génère une erreur ( dangereux ne pas faire en prod ) :
wget http://pastebin.com/raw.php?i=p3QyuXzZ -O /usr/share/snmp/mibs/ietf/SNMPv2-PDU
```

2.2 Description du terrain de jeu.

La liste des équipements interrogeables par SNMP sur l'IUT est la suivante :

- Le serveur windows AD (10.6.0.1 communauté snmp public).
- Configurez aussi un switch cisco 2950/2960 comme serveur SNMP avec une communauté RW *privatebeziens* et une communauté RO *publicbeziens* . Vous pouvez vous inspirer de <http://wiki.monitoring-fr.org/supervision/snmp-install>
- Installez aussi serveur SNMP sur vos machines Linux.

```
apt-get install snmp snmpd snmp-mibs-downloader libsnmp-dev

#Remplace la ligne dans /etc/snmp/snmp.conf par:
mibs +ALL

# Remplacer la mib qui génère une erreur ( dangereux ne pas faire en prod) :
wget http://pastebin.com/raw.php?i=p3QyuXzZ -O /usr/share/snmp/mibs/ietf/SNMPv2-PDU
```

Il faut modifier snmpd.conf pour autoriser un client SNMP à accéder à la totalité de la mib.

Vous travaillerez en version 2c de SNMP.

2.3 Utilisez le client SNMP afin de visualiser les informations des machines listées dans le "terrain de jeux".

1. Interrogation via SNMP du serveur ayant pour IP 10.6.0.1.
 - a) Dumper l'ensemble des informations du serveur distant via un snmpwalk.
 - b) Retrouver le système d'exploitation de la machine via un snmpget.
 - c) Retrouvez l'uptime de la machine via un snmpget.
 - d) Afficher l'arbre system de la mib à l'aide de la commande :
`snmptranslate -On -Tp SNMPv2-MIB::system`
 - e) Traduisez en oid SNMPv2-MIB : :system et réciproquement.
 - f) Retrouvez à l'aide de snmpnetstat la liste des connections TCP et UDP du serveur distant.
 - g) A quoi sert la commande snmpgetnext ? Utilisez la pour retrouver SNMPv2-MIB : :sysContact.0

3 Utilisation d'OMD comme logiciel de supervision SNMP

OMD est une distribution qui permet une installation très rapide d'un environnement de supervision et qui va contenir entre autres les briques nagios et check_mk . Vous pourrez l'installer (voir <https://checkmk.com/download.php?edition=cre&version=stable>). Prenez l'édition "raw" En suivant https://labs.consol.de/omd/getting_started.html. Vous paramétrez une instance OMD appelée IUTBEZIERS. Vous utiliserez le frontal de supervision de check_mk et wato afin de créer vos hôtes.

3.1 Supervisez avec OMD

En plus de la liste des machines listées précédemment dans le terrain de jeux vous superviserez avec OMD aussi :

- Le serveur registry.iutbeziers.fr (communauté snmp publicbeziers en ro et agent check_mk).
- Votre machine Linux sur laquelle vous installerez l'agent check-mk (téléchargeable sur store.iutbeziers.fr)
- Les services web de www.iutbeziers.fr (Vérifiez la durée du certificat pour les services SSL).
- L'annuaire de l'IUT. (Utilisez votre compte IUT ou demandez-en un à l'enseignant). Pensez à désactiver sur le serveur OMD l'obligation d'avoir un certificat pour le client LDAP en rajoutant dans le fichier /etc/ldap/ldap.conf la ligne "TLS_REQCERT never").
- Le service DNS de l'IUT.
- Le service ldap de l'IUT.
- Les services de messagerie de l'université.
- Le temps de réponse http de www.iutbeziers.fr.
- La validité du certificat ssl de www.iutbeziers.fr.
- le temps de réponse ICMP de google.fr.

4 Métrologie de vos serveurs et postes de travail avec Grafana.

4.1 Schéma de l'infrastructure de métrologie à mettre en place.

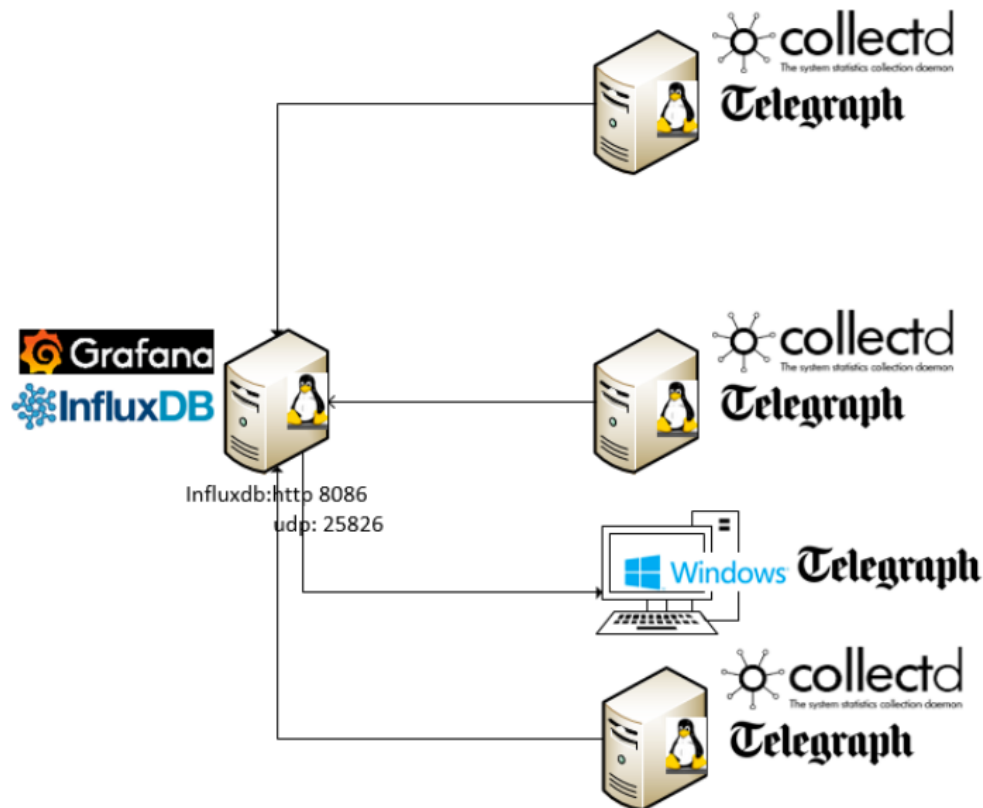


FIGURE 1 – Schéma de l'infrastructure à mettre en place.

4.2 Installation de Grafana/influxDB côté serveur.

Vous devez avoir docker et docker-compose installés sur votre machine (physique ou VM). Le mieux est d'utiliser une VM debian téléchargée depuis <http://store.iutbeziers.fr> Mais vous pouvez aussi installer docker-compose avec la commande curl voir :

<https://docs.docker.com/compose/install/> .

Clonez le fichier d'installation de l'environnement du TP via Git.

```
git clone https://registry.iutbeziers.fr:11443/pouchou/tp-supervision-licence-grafana1.git
```

Vous récupérerez ainsi le fichier docker-compose.yml.

Lancez la création des containers à l'aide de la commande suivante :

```
docker-compose up -d
```

Vérifiez que tout se passe bien avec les commandes suivantes (en vous plaçant dans le directory ou se trouve le fichier docker-compose.yml)

```
docker-compose ps
docker-compose logs -f
```

Vous pouvez réinitialiser le container en tapant la commande suivante :

```
docker-compose stop && docker-compose rm -f
```

L'application Grafana est accessible via `http://votreip:3000`. Un dashboard est préchargé par défaut par le container grafana et qui est alimenté par un container collectd qui récupère les informations de l'hôte du container.

Vous pouvez accéder à un des containers via la commande :

```
docker-compose exec grafana bash
```

4.3 Installation de Collectd/Telegraf sur les clients à monitorer.

Ces deux clients vont recueillir des données systèmes et réseaux qui vont alimenter les bases de données influxDB. Télégraf est le collecteur officiel de Grafana. Collectd s'installe via :

```
apt-get install collectd
```

Sa configuration se fait dans `/etc/collectd/collectd.conf`. Vous activez le plugin network qui est chargé d'envoyer les données recueillies vers la base de données influxDB.

```
LoadPlugin network
<Plugin network>
  <Server "ip de votre serveur influxDB" "25826">
</Plugin>
```

Installez et paramétrez Telegraf en suivant les articles suivants :

- Installation ;
- Configuration

Sa configuration se fait dans `/etc/telegraf/telegraf.conf`. Modifiez :

```
[[outputs.influxDB]]
# The full HTTP or UDP endpoint URL for your influxDB instance.
# Multiple urls can be specified but it is assumed that they are part of the same
# cluster, this means that only ONE of the urls will be written to each interval.
# urls = ["udp://localhost:8089"] # UDP endpoint example
urls = ["http://ip de votre serveur:8086"] # required
```

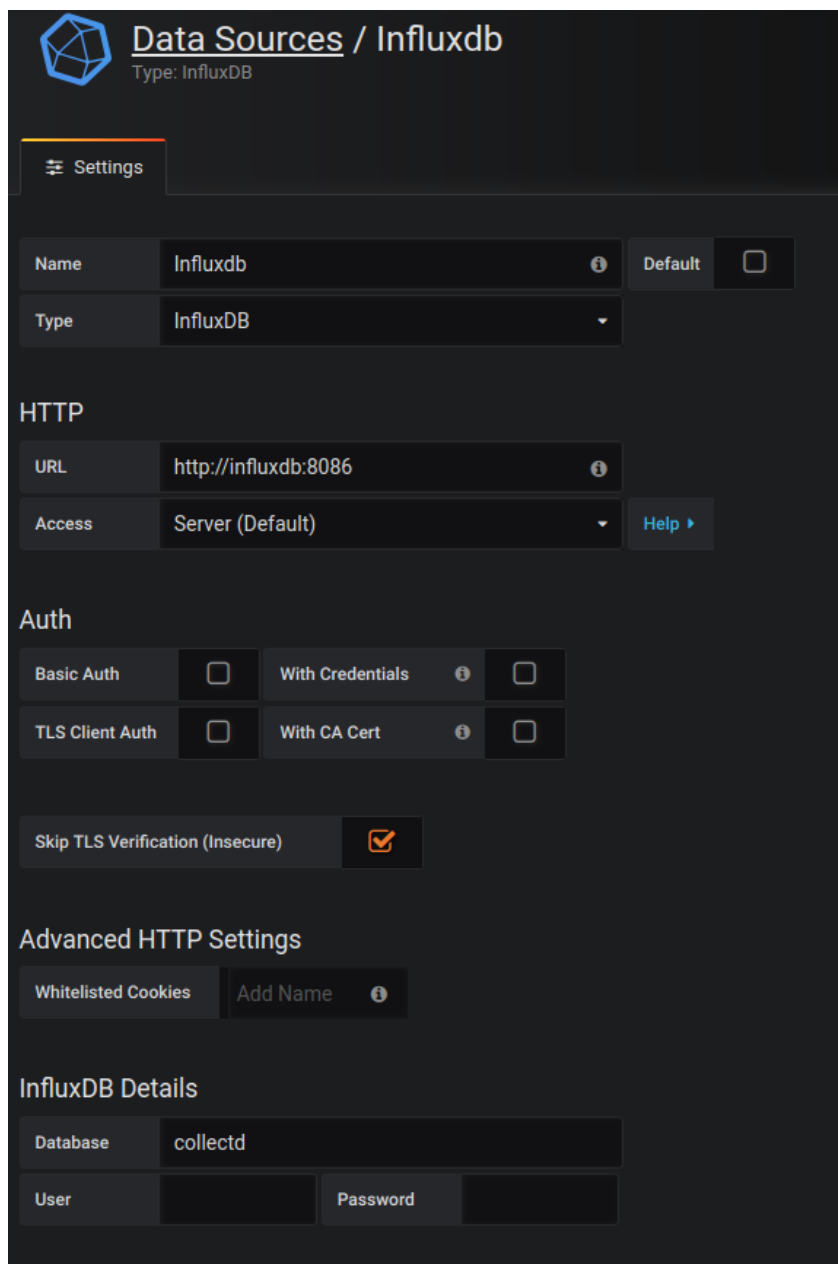
telegraf se débogue via :

```
/usr/bin/telegraf -config /etc/telegraf/telegraf.conf
```

4.4 Configuration des sources de données Telegraf et InfluxDB dans Grafana.

Ces sources permettent à Grafana de récupérer les enregistrements dans la base influxDB.

4.5 Configuration de la source de données Collectd.



The screenshot shows the 'Data Sources / Influxdb' configuration page. The page has a dark theme. At the top, there's a header with the InfluxDB logo and the title 'Data Sources / Influxdb' with a subtitle 'Type: InfluxDB'. Below the header, there's a 'Settings' tab. The main configuration area is divided into several sections: 'Name' (Influxdb), 'Type' (InfluxDB), 'HTTP' (URL: http://influxdb:8086, Access: Server (Default)), 'Auth' (Basic Auth, TLS Client Auth, Skip TLS Verification (Insecure)), 'Advanced HTTP Settings' (Whitelisted Cookies), and 'InfluxDB Details' (Database: collectd, User and Password fields).

Data Sources / Influxdb
Type: InfluxDB

Settings

Name Influxdb **Default** ☐

Type InfluxDB

HTTP

URL http://influxdb:8086

Access Server (Default) **Help**

Auth

Basic Auth ☐ **With Credentials** ☐

TLS Client Auth ☐ **With CA Cert** ☐

Skip TLS Verification (Insecure) ☒

Advanced HTTP Settings

Whitelisted Cookies **Add Name**

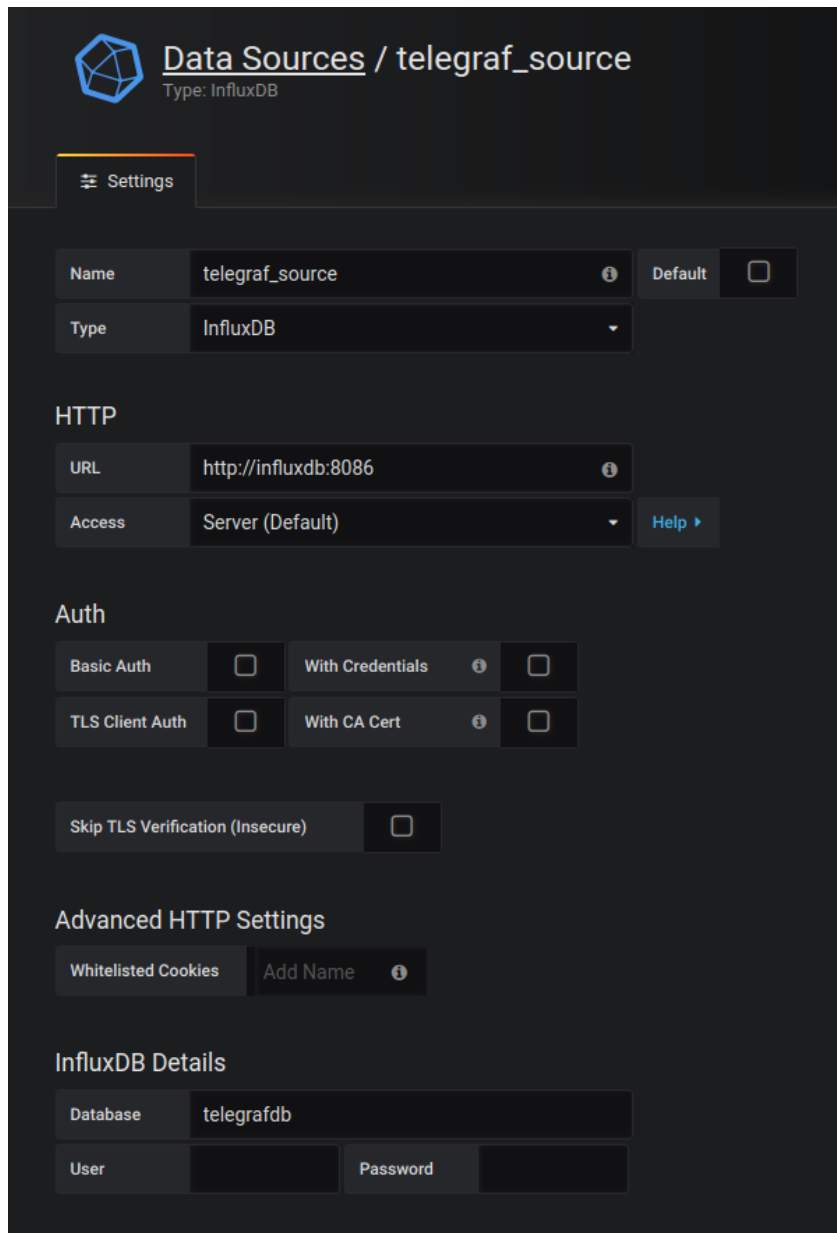
InfluxDB Details

Database collectd

User **Password**

FIGURE 2 – Configuration de la source de données collectd.

4.6 Configuration de la source de données telegraf.



The screenshot shows the 'Data Sources / telegraf_source' configuration page in Grafana. The page has a dark theme. At the top, there's a 'Settings' tab. Below it, the 'Name' is 'telegraf_source' and the 'Type' is 'InfluxDB'. The 'HTTP' section shows the 'URL' as 'http://influxdb:8086' and 'Access' as 'Server (Default)'. The 'Auth' section has checkboxes for 'Basic Auth', 'With Credentials', 'TLS Client Auth', and 'With CA Cert', all of which are currently unchecked. There is also a 'Skip TLS Verification (Insecure)' checkbox which is unchecked. The 'Advanced HTTP Settings' section has a 'Whitelisted Cookies' field with an 'Add Name' button. The 'InfluxDB Details' section has a 'Database' field set to 'telegrafdb', and 'User' and 'Password' fields which are empty.

Data Sources / telegraf_source
Type: InfluxDB

Settings

Name: telegraf_source ⓘ Default ☐

Type: InfluxDB ▼

HTTP

URL: http://influxdb:8086 ⓘ

Access: Server (Default) ▼ [Help ▶](#)

Auth

Basic Auth ☐ With Credentials ⓘ ☐

TLS Client Auth ☐ With CA Cert ⓘ ☐

Skip TLS Verification (Insecure) ☐

Advanced HTTP Settings

Whitelisted Cookies Add Name ⓘ

InfluxDB Details

Database: telegrafdb

User: Password:

FIGURE 3 – Configuration de la source de données Telegraf.

4.7 Importation d'un dashboard pour telegraf

Importez dans l'application Grafana le dashboard suivant pour télégraf :

<https://grafana.com/dashboards/5955>

4.8 Tips Grafana

Il faut configurer la timezone à UTC dans les préférences de Grafana sous peine d'avoir une heure de retard dans l'affichage des données.

Influxdb supporte des requêtes avec la time zone et en affichant la date dans un format "human readable".

Pour l'activer :

```
precision rfc3339
SELECT derivative(mean("bytes_sent"), 10s) FROM "net" WHERE time > now() - 1h GROUP BY time(10s) tz('Europe/Paris');
```

4.9 Réalisation d'un mini Dashboard.

1. Interrogez un de vos serveurs afin d'obtenir ce graphe des CPUs pour un de vos serveurs :

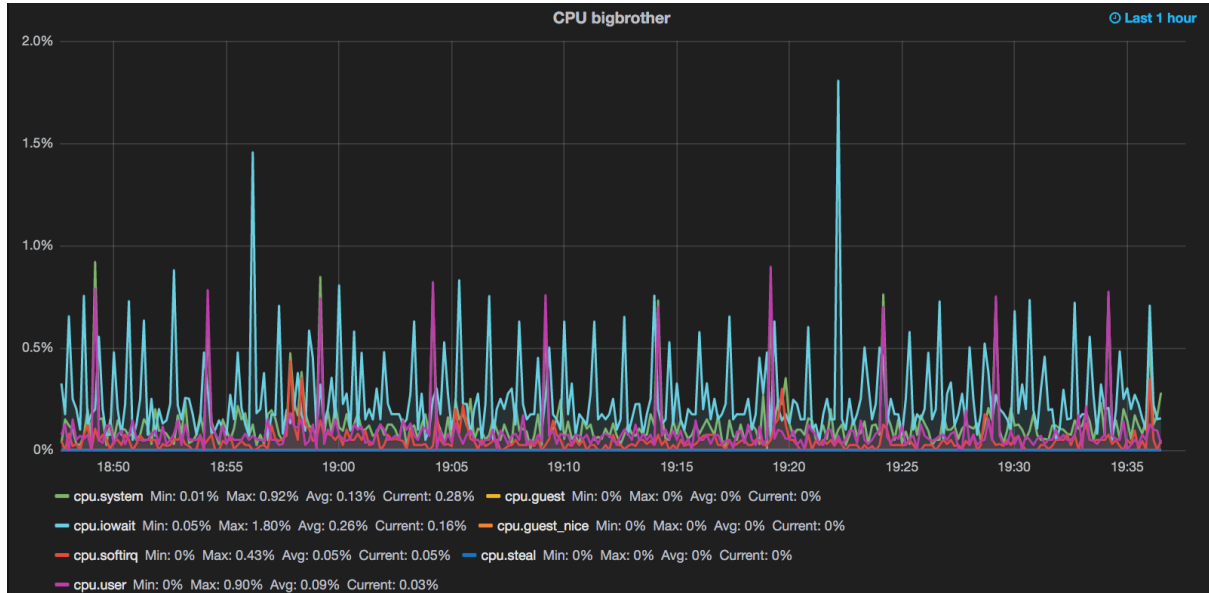


FIGURE 4 – Graphe des cpu.

2. Interrogez un de vos serveurs afin d'obtenir ce graphe du réseau :

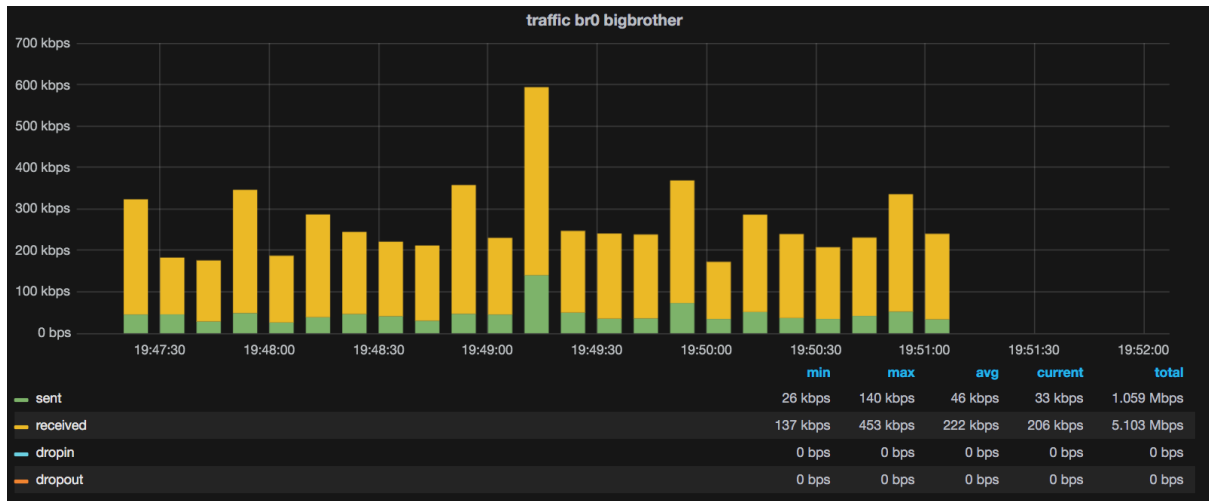


FIGURE 5 – Graphe bande passante.

4.10 Connexion à influxDB.

On va accéder au container docker afin de requêter la base infludb :

```
docker-compose exec influxdb bash -c "/usr/bin/influx -username '' -password ''"
Visit https://enterprise.influxdata.com to register for updates, influxDB server management, and monitoring.
Connected to http://localhost:8086 version 0.10.2
influxDB shell 0.10.2
```

influxDB s'interroge dans un langage très proche du SQL. Voir : <https://docs.influxdata.com/influxdb>

1. Donnez le nom des bases.
2. Donnez la liste des users.
3. Donner la liste des "time series" par base.
4. Lister via une requête SQL les enregistrements "bytes_recv" groupés par tranche de 10 seconde pour l'interface eth0 d'un de vos serveurs.