# MONITOR YOUR INFRA

Nicolas Vadkerti Quentin Risdorfer

10 décembre 2019

https://github.com/SlaynPool/CR_MONITOR_YOUR_INFRA

## 1 Utilisation de SNMP comme vecteur de monitoring

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

Listing 1 – Installation d'un Client

```
# Pour recuperer Les OID de registry.iutbeziers.fr
snmpwalk  -v  2c -c publicbeziers registry.iutbeziers.fr
SNMPv2-MIB::sysDescr.0 = STRING: Linux registry 4.9.0-8-amd64 #1 SMP Debian 4.9.130-2
    (2018-10-27) x86_64
SNMPv2-MIB::sysObjectID.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (1320059745) 152 days, 18:49:57.45
SNMPv2-MIB::sysContact.0 = STRING: Moa  <jean-marc.pouchoulon@iutbeziers.fr>
SNMPv2-MIB::sysName.0 = STRING: registry
SNMPv2-MIB::sysLocation.0 = STRING: iutbeziers

# Pour  le switch :
[slaynpool@MiniZbeub]~$ snmpwalk  -v  2c -c publicbeziers 10.255.255.253
SNMPv2-MIB::sysDescr.0 = STRING: HP Comware Platform Software, Software Version 5.20.99
    Release 2220P09
HP A5500-24G EI Switch with 2 Interface Slots
Copyright (c) 2010-2013 Hewlett-Packard Development Company, L.P.
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.25506.11.1.24


# Pour L'ad (Oui c'est la mauvaise communate )

[slaynpool@MiniZbeub]~$ snmpwalk  -v  2c -c public 10.6.0.1
SNMPv2-MIB::sysDescr.0 = STRING: Hardware: x86 Family 15 Model 4 Stepping 3 AT/AT
    COMPATIBLE - Software: Windows Version 5.2 (Build 3790 Multiprocessor Free)
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.311.1.1.3.1.3
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (2020700073) 233 days, 21:03:20.73
SNMPv2-MIB::sysContact.0 = STRING: M. Duban
SNMPv2-MIB::sysName.0 = STRING: SERVER-RT
SNMPv2-MIB::sysLocation.0 = STRING: Salle des serveurs
SNMPv2-MIB::sysServices.0 = INTEGER: 78
IF-MIB::ifNumber.0 = INTEGER: 3
```

Listing 2 – Test d'interogation

Pour Autoriser les connections de l'exterieur, il faut :

```
#  Listen for connections from the local system only
#agentAddress  udp:127.0.0.1:161
#  Listen for connections on all interfaces (both IPv4 *and* IPv6)
agentAddress udp:161,udp6:[::1]:161



systemctl restart snmpd
```

Listing 3 – snmpd.conf

# 2 Utilisez le client SNMP afin de visualiser les informations des machineslistées dans le "terrain de jeux"

## 2.1 Interrogation via SNMP du serveur ayant pour IP 10.6.0.1.

### 2.1.1 Dumper l'ensemble des informations du serveur distant via un snmpwalk

```
[slaynpool@MiniZbeub]~$ snmpwalk  -v  2c -c public 10.6.0.1
SNMPv2-MIB::sysDescr.0 = STRING: Hardware: x86 Family 15 Model 4 Stepping 3 AT/AT
    COMPATIBLE - Software: Windows Version 5.2 (Build 3790 Multiprocessor Free)
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.311.1.1.3.1.3
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (2020868420) 233 days, 21:31:24.20
SNMPv2-MIB::sysContact.0 = STRING: M. Duban
SNMPv2-MIB::sysName.0 = STRING: SERVER-RT
SNMPv2-MIB::sysLocation.0 = STRING: Salle des serveurs
SNMPv2-MIB::sysServices.0 = INTEGER: 78
IF-MIB::ifNumber.0 = INTEGER: 3
```

Listing 4 – snmpwalk

### 2.1.2 Retrouver le système d'exploitation de la machine via un snmpget.

```
# snmpget  -v  2c -c public 10.6.0.1 sysDescr.0
SNMPv2-MIB::sysDescr.0 = STRING: Hardware: x86 Family 15 Model 4 Stepping 3 AT/AT
    COMPATIBLE - Software: Windows Version 5.2 (Build 3790 Multiprocessor Free)
```

Listing 5 – snmpget

### 2.1.3 Afficher l'arbre system de la mib à l'aide de la commande

```
[slaynpool@MiniZbeub]~$ snmptranslate -On -Tp SNMPv2-MIB::system
+--system(1)
   |
   +-- -R-- String    sysDescr(1)
   |        Textual Convention: DisplayString
   |        Size: 0..255
   +-- -R-- ObjID     sysObjectID(2)
   +-- -R-- TimeTicks sysUpTime(3)
   |  |
   |  +--sysUpTimeInstance(0)
   |
   +-- -RW- String    sysContact(4)
   |        Textual Convention: DisplayString
   |        Size: 0..255
   +-- -RW- String    sysName(5)
   |        Textual Convention: DisplayString
   |        Size: 0..255
   +-- -RW- String    sysLocation(6)
   |        Textual Convention: DisplayString
   |        Size: 0..255
   +-- -R-- INTEGER   sysServices(7)
   |        Range: 0..127
   +-- -R-- TimeTicks sysORLastChange(8)
   |        Textual Convention: TimeStamp
   |
   +--sysORTable(9)
      |
      +--sysOREntry(1)
         |  Index: sysORIndex
         |
         +-- ---- INTEGER   sysORIndex(1)
         |        Range: 1..2147483647
         +-- -R-- ObjID     sysORID(2)
         +-- -R-- String    sysORDescr(3)
         |        Textual Convention: DisplayString
         |        Size: 0..255
         +-- -R-- TimeTicks sysORUpTime(4)
                  Textual Convention: TimeStamp
```

Listing 6 – Arbre de la mib SNMPv2

### 2.1.4 Traduisez en oid SNMPv2-MIB : :system et réciproquement

```
[slaynpool@MiniZbeub]~$   snmptranslate -Ot .1.3.6.1.2.1.1
SNMPv2-MIB::system
[slaynpool@MiniZbeub]~$  snmptranslate -On -Td SNMPv2-MIB::system
.1.3.6.1.2.1.1
system OBJECT-TYPE
  -- FROM SNMPv2-MIB
::= { iso(1) org(3) dod(6) internet(1) mgmt(2) mib-2(1) 1 }
```

Listing 7 – Traduction

### 2.1.5 Retrouvez à l'aide de snmpnetstat la liste des connections TCP et UDP du serveur distant

```
[slaynpool@MiniZbeub]~$ snmpnetstat  -v  2c -c public 10.6.0.1
Active Internet (udp) Connections
Proto Local Address               Remote Address                PID
udp4  *.*                         *.*                             0
```

Listing 8 – snmpNetstat

### 2.1.6 quoi sert la commande snmpgetnext ? Utilisez la pour retrouvez SNMPv2-MIB : :sysContact.0

Source : `man_snmpgetnext`

> snmpgetnext is an SNMP application that uses the SNMP GETNEXT request to query for information on a network entity. One or more object identifiers (OIDs) may be given as arguments on the command line. Each variable name is given in the format specified in variables(5). For each one, the variable that is lexicographically "next" in the remote entity's MIB will be returned.

La commande sert donc à afficher des informations à propos du périphérique interrogé.

```
 snmpgetnext 10.6.0.1 -v 2c -c public  SNMPv2-MIB::sysContact.0
SNMPv2-MIB::sysName.0 = STRING: SERVER-RT
```

Listing 9 – snmpgetnext

# 3 Utilisation d'OMD comme logiciel de supervision SNMP

Paquets à installer :
mk-check-agent : `store.iutbeziers.fr/check-mk-agent/`
OMD : `http://clusterfrak.com/sysops/app_installs/omd_install/`

## 3.1 Supervisez avec OMD

Créer notre site avec OMD :

```
root@DebianJetable:/home/user# omd create IUTBEZIERS
Adding /omd/sites/IUTBEZIERS/tmp to /etc/fstab.
Creating temporary filesystem /omd/sites/IUTBEZIERS/tmp...OK
Restarting Apache...OK
Created new site IUTBEZIERS with version 3.20-labs-edition.

  The site can be started with omd start IUTBEZIERS.
  The default web UI is available at https://DebianJetable/IUTBEZIERS/

  The admin user for the web applications is omdadmin with password: ro4BsuaA
  (It can be changed with the 'set_admin_password' command as site user.)

  Please do a su - IUTBEZIERS for administration of this site.
```

Listing 10 – Création iutbeziers

Premiers pas :

```
OMD[IUTBEZIERS@DebianJetable]:~$ omd status
rrdcached:      stopped
npcd:           stopped
naemon:         stopped
apache:         stopped
crontab:        stopped
-----------------------
Overall state:  stopped
```

Listing 11 – Afficher status du site

```
OMD[IUTBEZIERS@DebianJetable]:~$ omd start
Starting rrdcached...OK
Starting npcd...OK
Starting naemon...OK
Starting dedicated Apache for site IUTBEZIERS...OK
Initializing Crontab...OK
OMD[IUTBEZIERS@DebianJetable]:~$ omd status
rrdcached:      running
npcd:           running
naemon:         running
apache:         running
crontab:        running
-----------------------
Overall state:  running
```

Listing 12 – Démarrer notre site IURBEZIERS

## 3.2 Quelques services Configuré

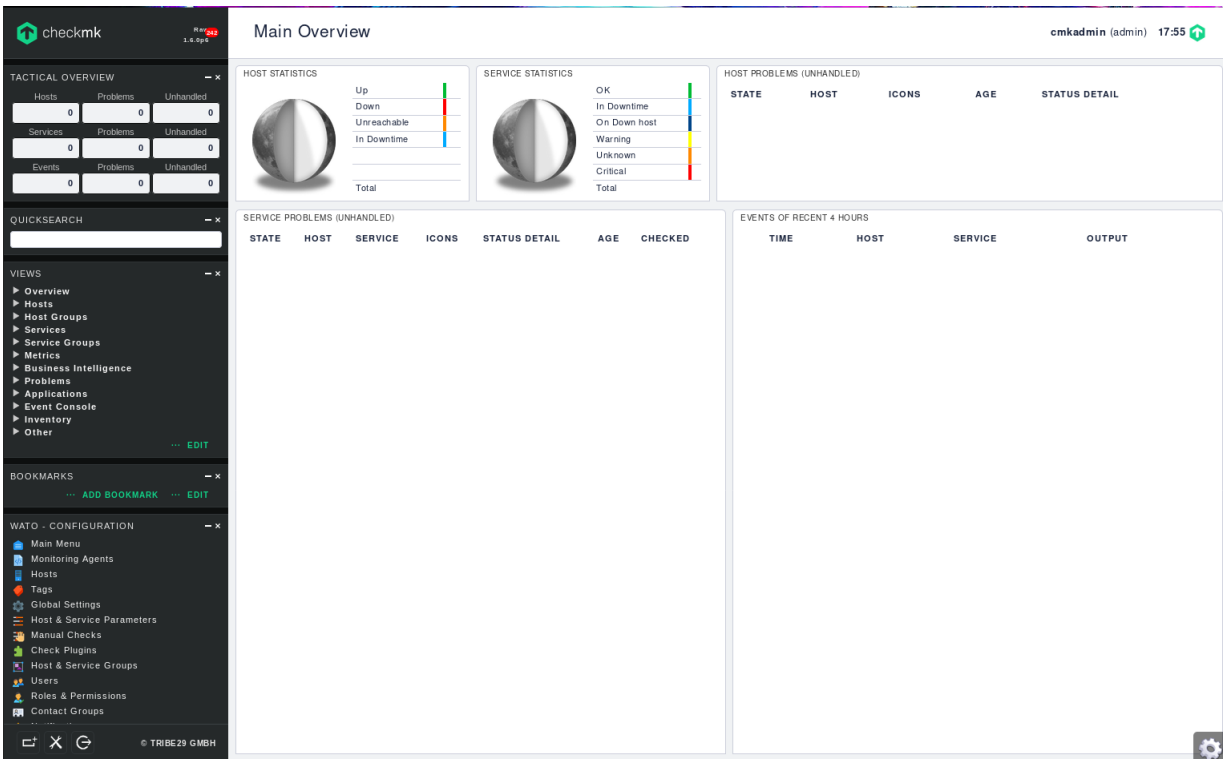


FIGURE 1 – checkmk

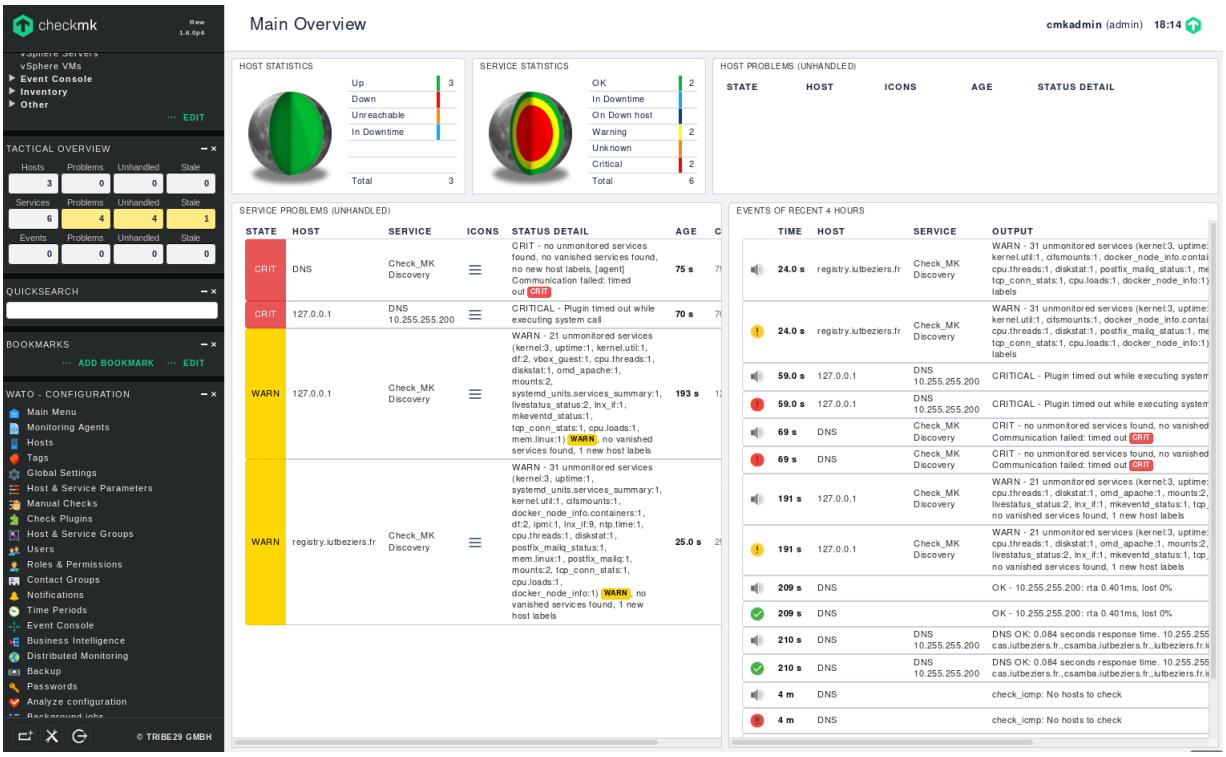


FIGURE 2 – checkmk

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

## 4.1 Installation de Grafana/influxDB côté serveur.

```
#Pour autre chose qu'une debian genre une Arch par exemple
pacman -S docker
systemctl start docker
#Pour recuperer docker-compose
```

```
git clone  https://registry.iutbeziers.fr:11443/pouchou/tp-supervision-licence-grafana.
    git
cd tp-supervision-licence-grafana
sudo docker-compose up -d
sudo docker-compose ps
                  Name                                Command            State
                                                          Ports
-------------------------------------------------------------------------------------------------------------------

tp-supervision-licence-grafana_collectd_1   /entrypoint.sh             Up
tp-supervision-licence-grafana_grafana_1    /run.sh                    Up
    0.0.0.0:3000->3000/tcp
tp-supervision-licence-grafana_influxdb_1   /entrypoint.sh influxd     Up
    0.0.0.0:25826->25826/udp, 0.0.0.0:8083->8083/tcp, 0.0.0.0:8086->8086/tcp
```

Listing 13 – Installation/Utilisation de Docker

## 4.2 Configuration de la source de données Collectd.

En suivant le sujet de TP, Nous obtenons ceci

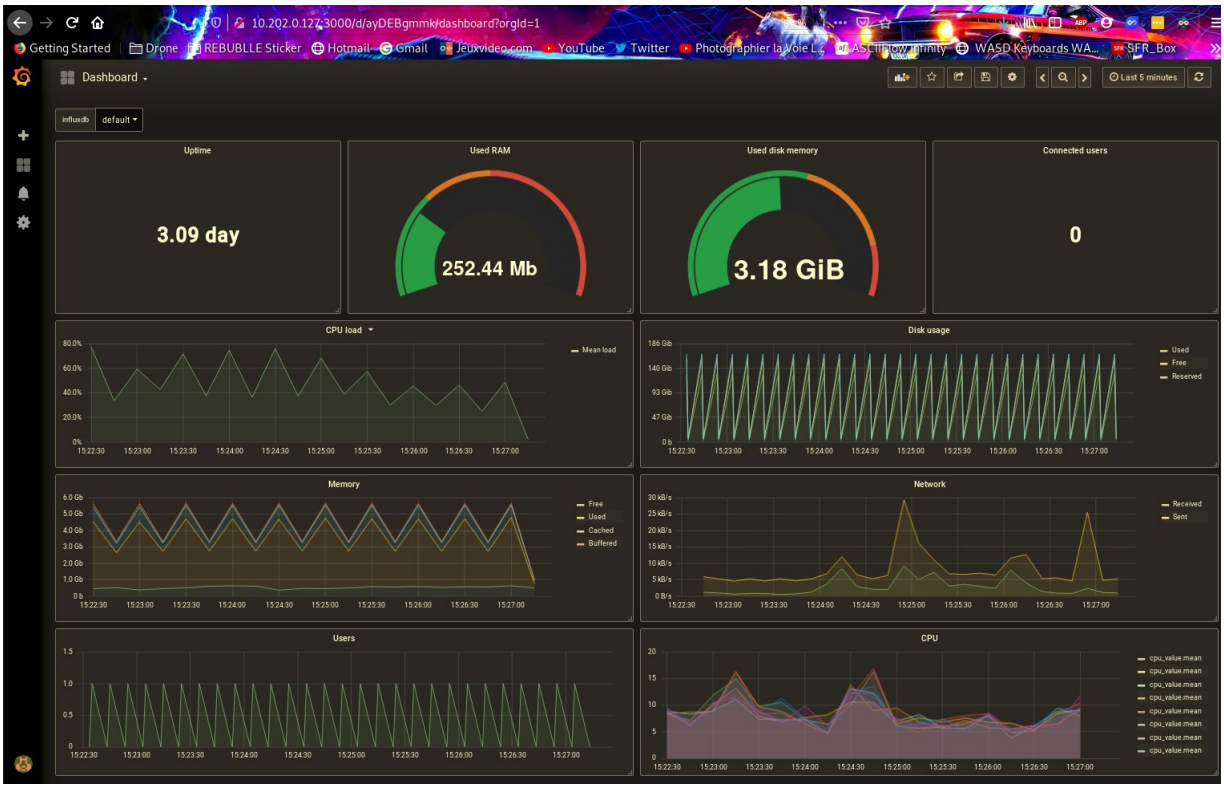


FIGURE 3 – Dashboard Graphana

## 4.3 Importation d'un dashboard pour telegraf


FIGURE 4 – Dashboard telegraf

# 5 Connexion à influxDB

## 5.1 Donnez le nom des bases

```
> SHOW DATABASES
name: databases
name
----
collectd
_internal
telegraf

# Voir la liste des tables de telegraf

> USE telegraf
Using database telegraf
> SHOW MEASUREMENTS
name: measurements
name
----
cpu
disk
diskio
kernel
mem
processes
swap
system
```

Listing 14 – Liste des Tables

## 5.2 Lister les USERS

Nous n'avons pas crée d'utilisateur dans la DB mais la commande est :

```
> SHOW USERS
user admin
---- -----
>
```

Listing 15 – Liste USERS

## 5.3 Donner la liste des "time series" par base.

```
> SHOW SERIES
key
---
cpu,cpu=cpu-total,host=DebianJetable
cpu,cpu=cpu0,host=DebianJetable
disk,device=dm-0,fstype=ext4,host=DebianJetable,mode=rw,path=/
disk,device=sda1,fstype=ext4,host=DebianJetable,mode=rw,path=/boot
diskio,host=DebianJetable,name=dm-0
diskio,host=DebianJetable,name=dm-1
diskio,host=DebianJetable,name=sda
diskio,host=DebianJetable,name=sda1
diskio,host=DebianJetable,name=sda2
kernel,host=DebianJetable
mem,host=DebianJetable
processes,host=DebianJetable
swap,host=DebianJetable
system,host=DebianJetable
>
```

Listing 16 – SHOW SERIES

## 5.4 Enregistrements groupé par tranche de 10s

```
> SELECT derivative(mean("value"), 10s) FROM "interface_rx" WHERE ("type" = 'if_octets')
     AND time >= now() - 5m GROUP BY time(10s) fill(null)
name: interface_rx
time                derivative
----                ----------
1575906750000000000 962
1575906760000000000 487
1575906770000000000 827
1575906780000000000 763
1575906790000000000 827
1575906800000000000 784
1575906810000000000 948.5
1575906820000000000 784
1575906830000000000 573
1575906840000000000 784
1575906850000000000 487
```

Listing 17 – GROUPE BY