

# INSTALLATION DE NTOPNG SOUS RASPBERRY PI

Raspberry Pi - FreeBSD  
**Configuration de base**

Tutoriel **NTOPNG** - RASPBERRY PI

David GOÏTRÉ

## Table des matières

Introduction .....	1
1. Pré requis .....	1
2. Paramétrage de connexion au serveur .....	1
3. Paramétrage du serveur .....	2
4. Installation de Ntopng.....	3
5. Configuration de connexion de Ntopng.....	4
6. Configuration avancée de Ntopng .....	4
7. Création d'un réseau.....	6
8. Paramétrage d'une plage d'@IP .....	6
9. Paramétrage de l'interface réseau .....	6
10. Création d'un Pool d'hôtes .....	7
11. Activation du monitoring .....	7
12. Visualisation du flux en direct.....	9
13. Ajout de la géolocalisation des IPs.....	9
14. Configurer les contrôles comportementaux.....	10
15. Sauvegarder les paramètres de configuration.....	11
16. Restauration des paramètres de configuration .....	11
17. Mise à jour de Ntopng.....	12
18. Désinstallation de Ntopng.....	12
19. Liens annexes .....	12
20. Commandes RaspberryPi .....	12
21. Conclusion.....	12

## Introduction

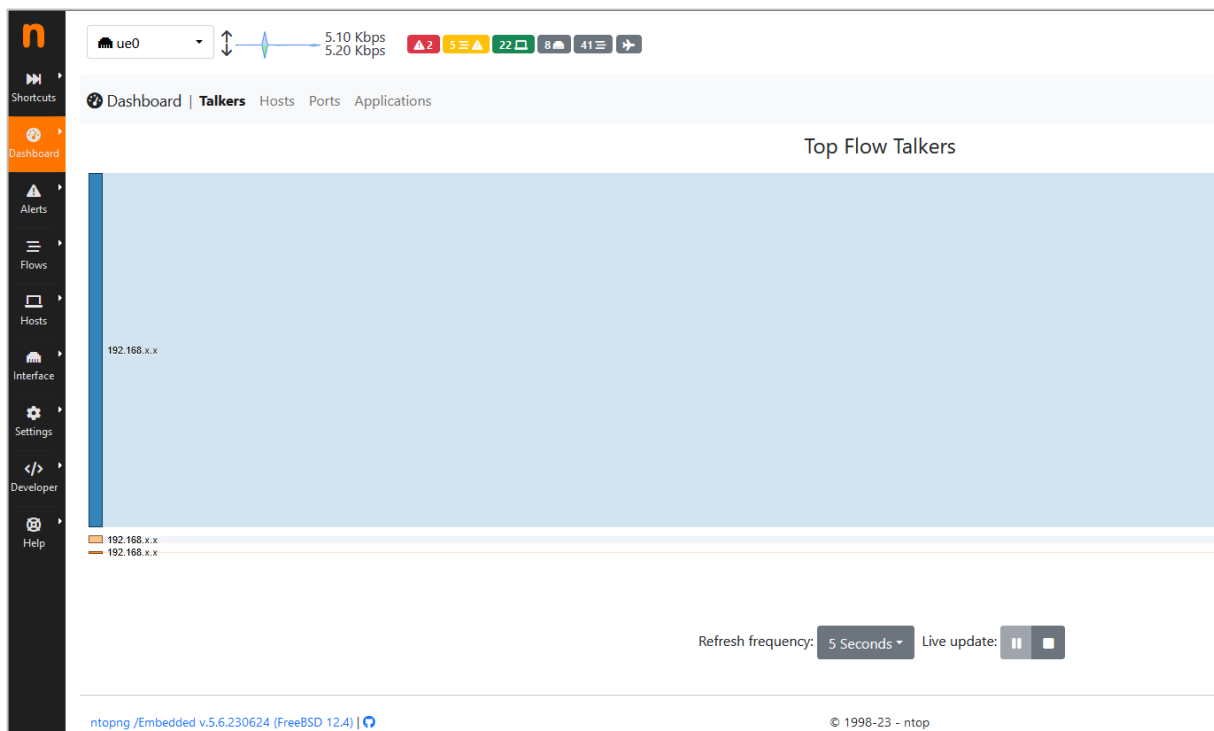
**Ntopng** (Network TOP New Generation) est un outil libre de supervision réseau. C'est une application qui produit des informations sur le trafic d'un réseau en temps réel (comme pourrait le faire la commande top avec les processus).

Il capture et analyse les trames d'une interface donnée, et permet d'observer une majeure partie des caractéristiques du trafic (entrant et sortant) et accepte pour cela, notamment deux modes de fonctionnement: Une interface web et un mode interactif.

## 1. Pré requis

On a besoin des différents matériels et logiciels pour la création d'un Serveur NTOPNG avec un RaspberryPi.

- Un ou des PC client sous Windows
  - Une Box (Free, Orange, Sfr...)
  - Un Raspberry 3B+ avec l'[OS FreeBSD 12.x](#) installé avec [Etcher](#)
  - Le logiciel [Putty](#) pour se connecter en SSH au serveur
  - Connaître l'interface réseau (eth0, br0, ens3...) via la commande : **ifconfig**
- Pour notre test c'est **l'interface ue0** qui sera utilisée



Voici un exemple d'interface que l'on doit obtenir une fois le serveur **Ntopng** mise en place

## 2. Paramétrage de connexion au serveur

a) le **SSH** est activé par défaut sur le serveur.

b) Ouvrir **Putty** et se connecter au serveur avec les identifiants (par défaut **freebsd/freebsd**)

Les identifiants d'administration sont : **root/root** (saisir **su** pour entrer en mode admin).

c) Exécuter la commande suivante pour mettre à jour et mettre à niveau les packages du système

```
# pkg update && pkg upgrade
```

### 3. Paramétrage du serveur

Avant d'aller plus loin, il nous faut connaître l'interface réseau de notre serveur **RaspberryPI** et lui attribuer une adresse IP fixe.

a) Lister les interfaces

```
# ifconfig # liste les interfaces
# ifconfig ue0 # passe la carte réseau ue0 par défaut
# grep -i ethernet /var/run/dmesg.boot # liste les propriétés de l'interface
```

b) Définir une adresse IP fixe

```
# pkg install nano # installe le logiciel nano
# nano /etc/rc.conf # ouvre le fichier des interfaces
```

c) Copier le texte ci-dessous dans le fichier **/etc/rc.conf**

```
hostname="generic" #nom de la machine
# ifconfig_DEFAULT="DHCP inet6 accept_rtadv"
ifconfig_ue0="inet 192.xxx.xxx.xxx netmask 255.255.255.0"
sshd_enable="YES"
sendmail_enable="YES"
sendmail_submit_enable="YES"
sendmail_outbound_enable="YES"
sendmail_msp_queue_enable="NO"
growfs_enable="YES"
defaultrouter="192.xxx.xxx.xxx" #@IP de la passerelle
```

d) Vérifier les DNS

```
# cat /etc/resolv.conf # affiche le contenu du fichier
```

e) Redémarrer le serveur

```
# service netif restart && service routing restart
# reboot
```

f) Modifier le mot de passe

```
$ raspi-config # ouvre l'utilitaire, sélectionner le menu System Options
```

Sélectionner le menu **S3 Password** pour modifier le mot de passe et **S4 Hostname** pour modifier le nom du serveur.

```
Raspberry Pi Software Configuration Tool (raspi-config)
1 System Options          Configure system settings
2 Display Options         Configure display settings

Raspberry Pi Software Configuration Tool (raspi-config)
S1 Wireless LAN          Enter SSID and passphrase
S2 Audio                  Select audio out through HDMI or 3.5mm jack
S3 Password              Change password for the 'pi' user
S4 Hostname               Set name for this computer on a network
```

## 4. Installation de Ntopng

Par défaut, le paquet Ntopng est disponible dans le référentiel de FreeBSD.

a) Installation de Ntopng :

```
# pkg search ntopng # vérifie la présence du paquet
# pkg install ntopng
# pkg install redis # dépendance de ntopng
```

b) Lancer les services

```
# service redis onestart
# service ntopng onestart
```

c) Modifier le fuseau horaire

```
# ln -s /usr/share/zoneinfo/Europe/Paris /etc/localtime
# ntpdate ntp.nic.fr
```

**Démarrage automatique de ntopng :**

a) Copier les lignes ci-dessous dans le fichier **/etc/rc.conf**

```
redis_enable="YES"
ntopng_enable="YES"
ntopng_flags=/usr/local/etc/ntopng.conf
```

b) Créer le fichier **/usr/local/etc/ntopng.conf** et copier les lignes ci-dessous

```
# ntopng - 1998-13 (C) ntop.org
description "ntopng: web-based traffic monitoring"

# Quand démarrer le service
start on runlevel [2345]

# Quand arrêter le service
stop on runlevel [016]

# Redémarrer automatiquement le processus en cas de plantage
respawn

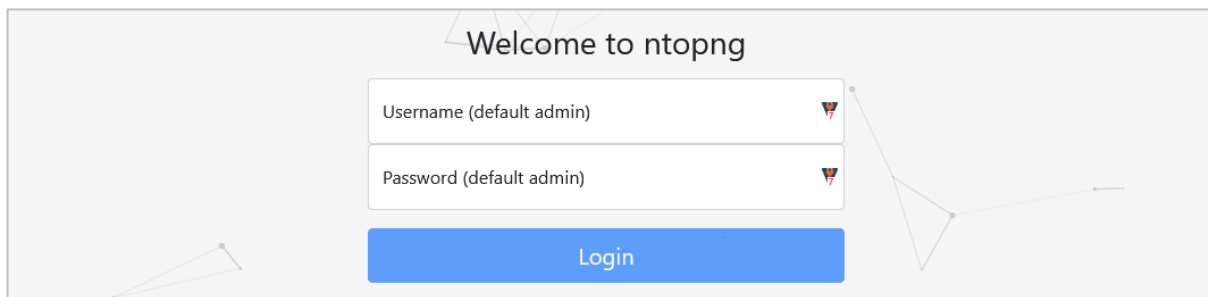
# Permet essentiellement de savoir que le processus se détachera de l'arrière-plan
expect fork
```

c) Créer le fichier **/etc/rc.local** et copier les lignes ci-dessous

```
#!/bin/bash -e
service redis onestart
service ntopng onestart
exit 0
```

## 5. Configuration de connexion de Ntopng

a) Une fois le serveur installé, **lancer-le à partir du navigateur** via **@IP:3000**, se connecter avec les identifiants **admin/admin**



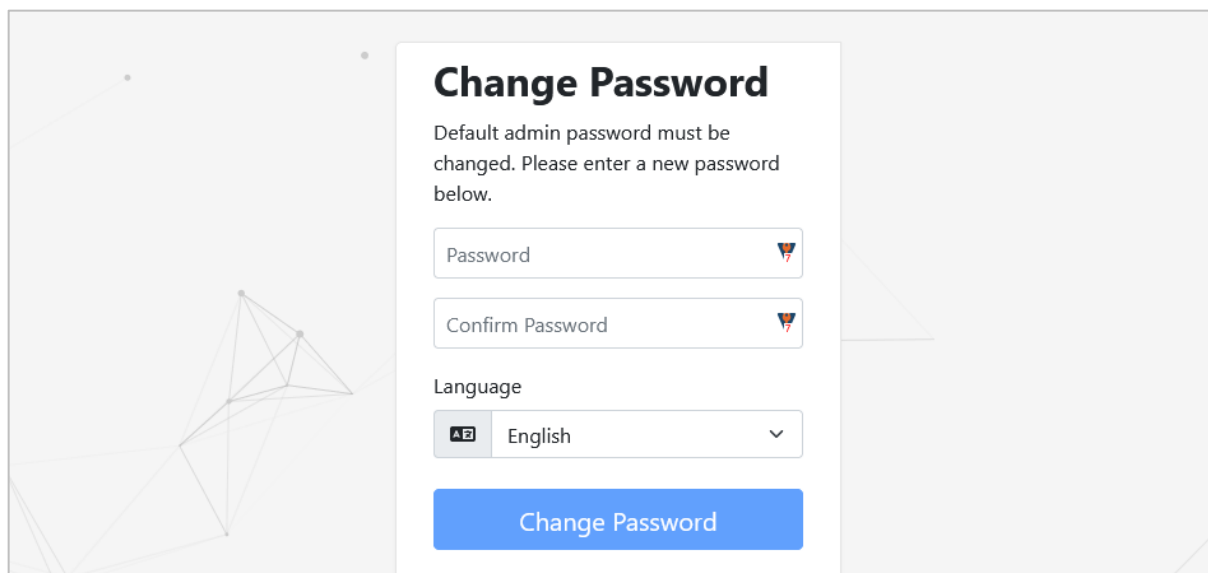
Welcome to ntopng

Username (default admin)

Password (default admin)

Login

b) Spécifier un nouveau **mot de passe** et choisir la langue



**Change Password**

Default admin password must be changed. Please enter a new password below.

Password

Confirm Password

Language

English

Change Password

## 6. Configuration avancée de Ntopng

Maintenant que notre serveur Ntopng est fonctionnel, il faut maintenant que notre Raspberry Pi reçoive l'ensemble du trafic réseau échangé vers Internet pour pouvoir analyser l'ensemble des flux réseaux.

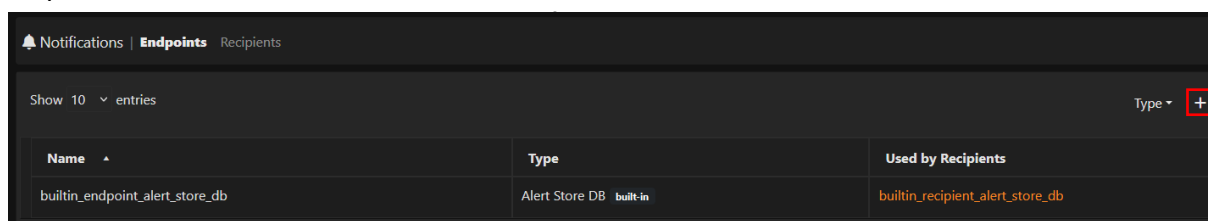
Sur un réseau Ethernet Switché l'ensemble des paquets réseau ne sont pas transmis à chaque hôte. Un filtrage est réalisé par le filtre pour ne transmettre que les paquets qui lui sont adressés.

Pour cela il faut créer un **point de terminaison** et un **récepteur** pour commencer à envoyer des alertes à l'extérieur. Le récepteur **builtin\_endpoint\_alert\_store\_dba** existant, a été créé par défaut.

**Créer un nouveau point de terminaison :**

a) Sélectionner le menu **Shortcuts/Notifications**

b) Cliquer sur le bouton +



Notifications | Endpoints | Recipients

Show 10 entries

Type +

Name	Type	Used by Recipients
builtin_endpoint_alert_store_db	Alert Store DB builtin	builtin_recipient_alert_store_db

Figure 1

- c) Dans la nouvelle fenêtre, sélectionner **Email** comme type
- d) Saisir un nom de terminaison (ex : **mail\_ntop**)
- e) Saisir votre serveur SMTP (ex : **smtp.live.fr**)
- f) Saisir le mail expéditeur (ex : **admin@live.fr**)

- g) Cliquer sur le bouton **Add**

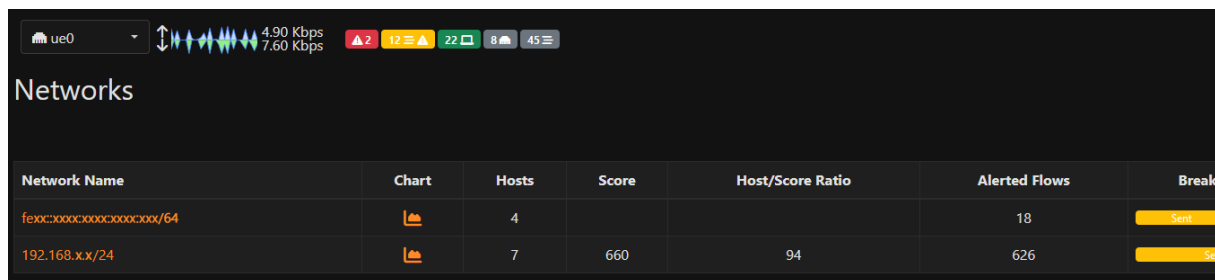
#### Créer le récipient :

- a) Cliquer sur l'onglet **Réceptiens** (voir *figure 1*)
- b) Saisir un **nom** pour le Récipient
- c) Sélectionner le **point de terminaison** créer auparavant
- d) Saisir un **email de destination** qui recevra les alertes
- e) Sélectionner le **seuil de gravité**

- d) Cliquer sur le bouton **Add**

## 7. Création d'un réseau

Dans **Ntopng**, les réseaux offrent un moyen puissant de regrouper les différents **appareils associés**. Ntopng crée par défaut le réseau de notre serveur (ex : 192.168.xxx.xxx) dans lequel on y retrouve tous les périphériques connectés.



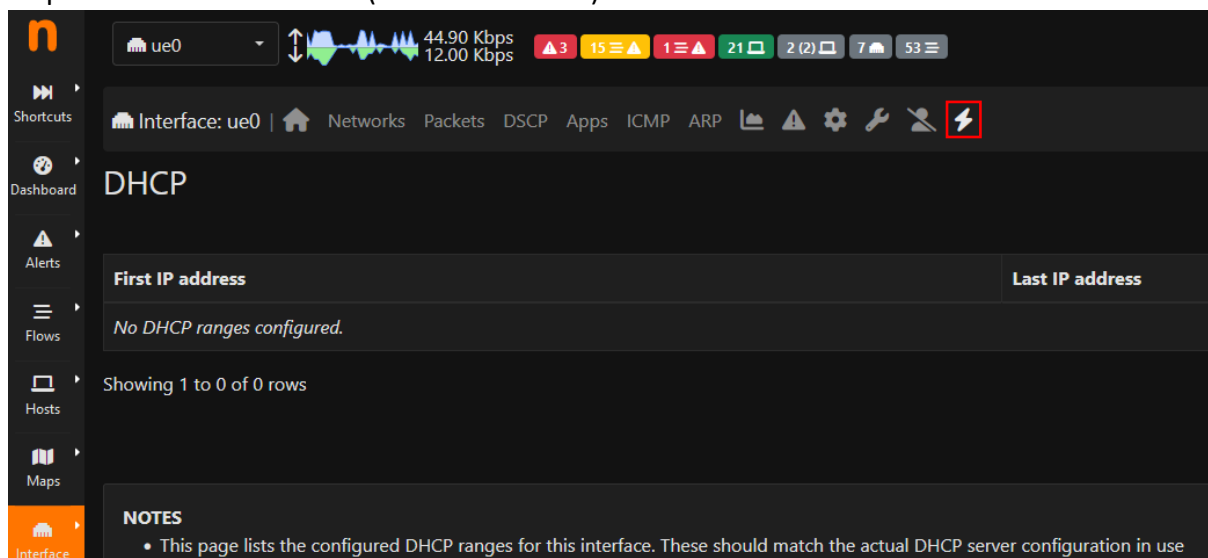
The screenshot shows the 'Networks' section of the Ntopng interface. At the top, there's a header with a dropdown menu set to 'ue0', a traffic chart, and several status indicators. Below this is a table with the following data:

Network Name	Chart	Hosts	Score	Host/Score Ratio	Alerted Flows	Break
fe8c::xxxx:xxxx:xxxx:xxxx/64		4			18	<a href="#">Send</a>
192.168.x.x/24		7	660	94	626	<a href="#">Send</a>

## 8. Paramétrage d'une plage d'@IP

Dans **Ntopng**, il faut déclarer une plage d'adresse IP et paramétrer l'interface réseau

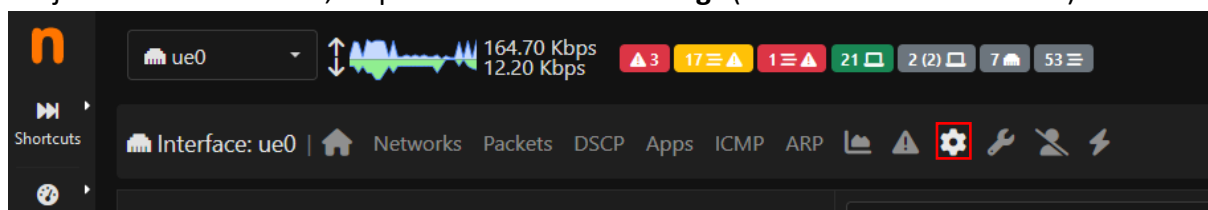
- Sélectionner le menu **Interfaces/Détails**
- Cliquer sur le bouton **DHCP** (icône d'un éclair)



- Cliquer sur le **bouton +**
- Saisir dans le champ **First IP address** une @IP de début (ex : 192.x.x.1)
- Saisir dans le champ **Last IP address** une @IP de fin (ex : 192.x.x.254)
- Cliquer sur le bouton **Save settings**

## 9. Paramétrage de l'interface réseau

- Toujours dans l'interface, cliquer sur le bouton **Settings** (icône d'une roue crantée)



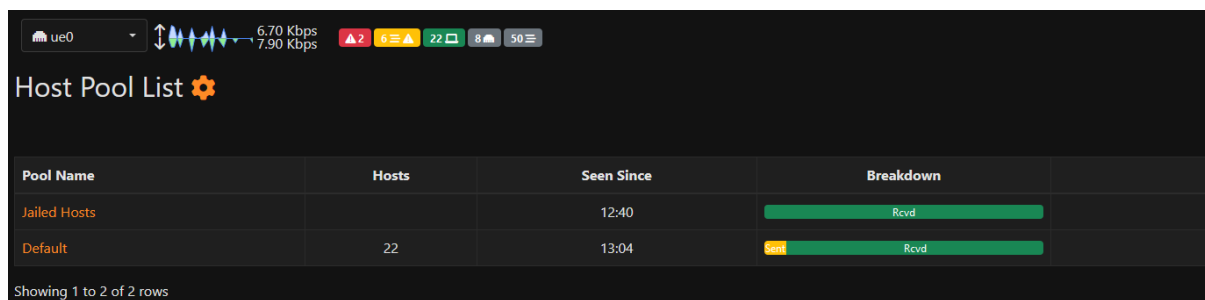
- Dans la liste **Local Broadcast Domain Hosts Identifier**, sélectionner **MAC Address**
- Cliquer sur le bouton **Save settings**



## 10. Création d'un Pool d'hôtes

Dans **Ntopng**, les **pools d'hôtes** offrent un moyen puissant de regrouper différents **hôtes**. Les pools d'hôtes sont définis sur une base d'interface réseau. Ils sont plutôt **destinés aux moyennes et grandes entreprises**.

Ntopng a créé un pool d'hôtes **default**. Pour afficher les pools d'hôtes, sélectionner le menu **Hosts/Pools**.



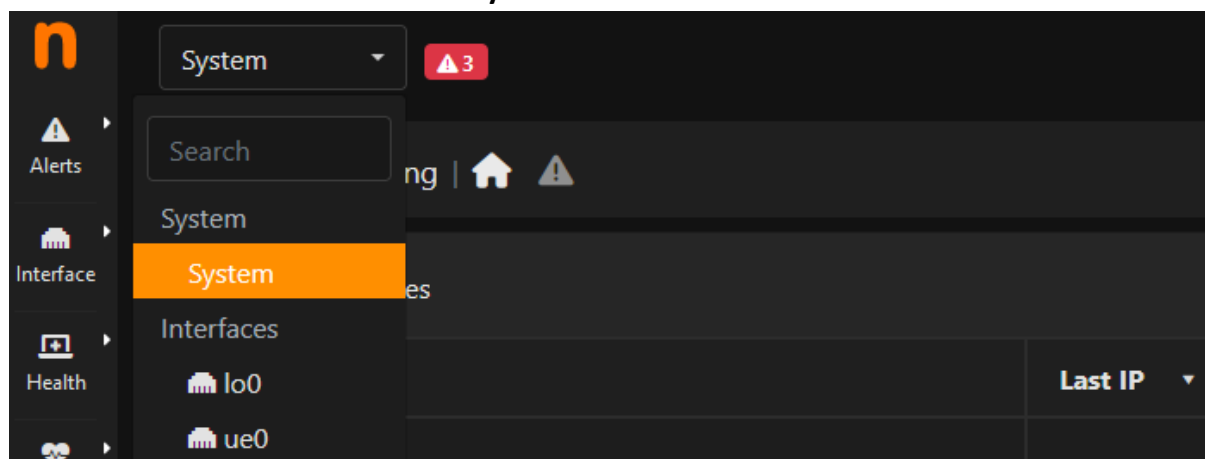
Pool Name	Hosts	Seen Since	Breakdown
Jailed Hosts		12:40	<div>Rcvd</div>
Default	22	13:04	<div>Sent Rcvd</div>

Showing 1 to 2 of 2 rows

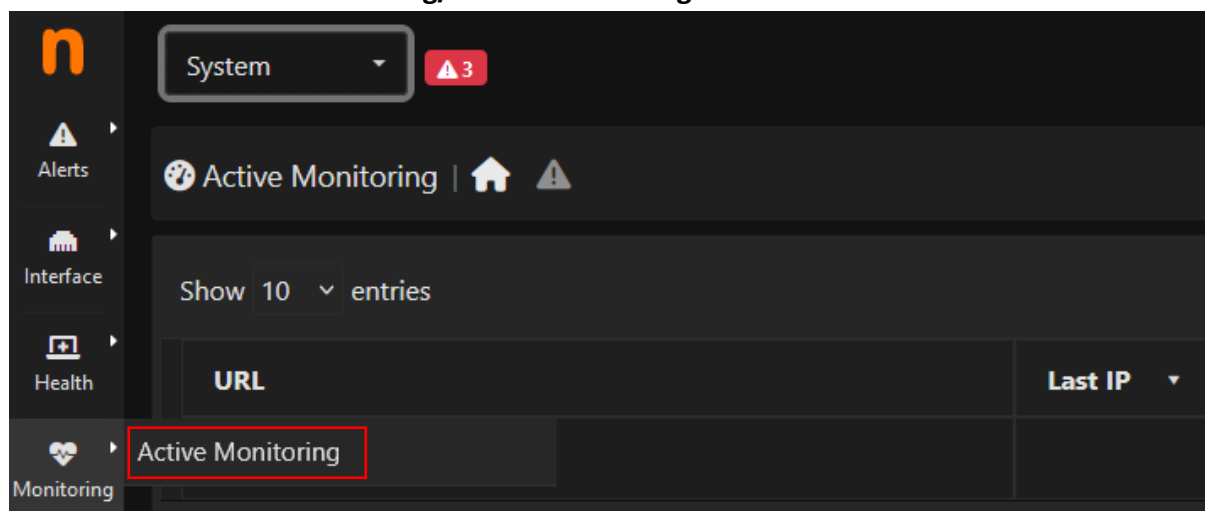
## 11. Activation du monitoring

Pour pouvoir visualiser la surveillance du réseau, il faut l'activer via l'interface **System**.

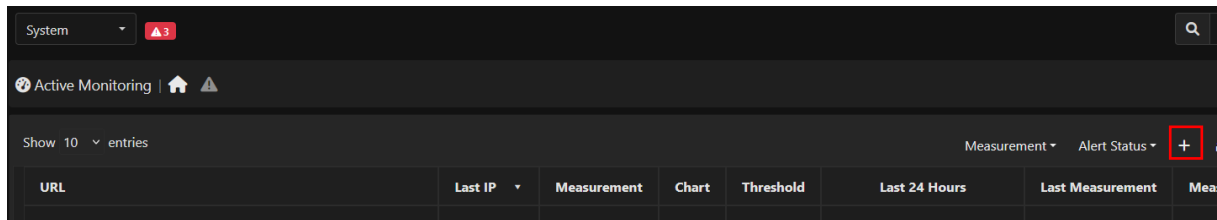
a) Sélectionner dans la liste l'interface **system**.



b) Sélectionner le menu **Monitoring/Active Monitoring**



c) Cliquer sur le **bouton +**



d) Sélectionner un **Measurement**

- > **Throughput** : mesure le débit
- > **HTTP(S)** : mesure la navigation d'un siteweb
- > **ICMP** : mesure l'envoi de données (pas disponible sous Windows)
- > **Speedtest** : mesure la rapidité

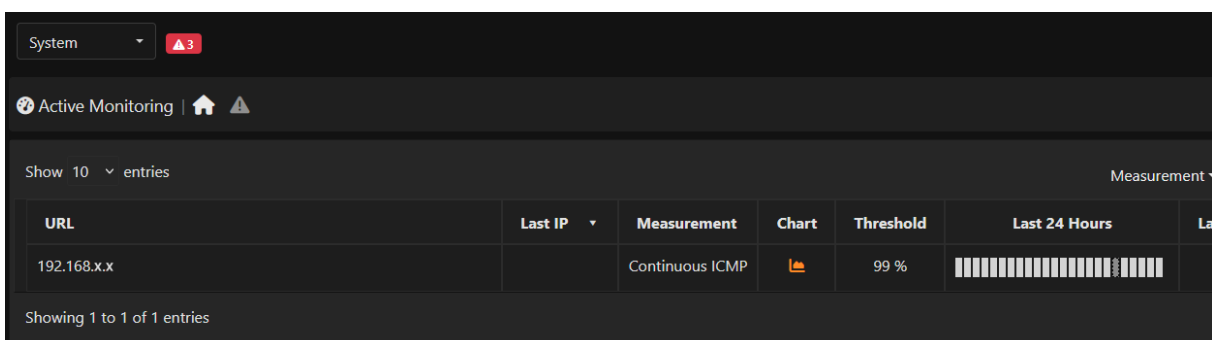
e) Saisir L'**@IP de l'hôte à surveiller**

f) Saisir un **Threshold** (un seuil de 200 minimum pour les Measurements en ms)

The screenshot shows the 'Add Active Monitoring Record' form. It has three main input fields: 'Measurement' with a dropdown menu showing 'Continuous ICMP', 'Host' with a text input showing '192.168.xxx.xxx', and 'Threshold' with a dropdown showing '<' and a text input showing '99', followed by a '%' symbol. Below these fields is a 'NOTES' section with three bullet points: 'ICMP not available on Windows.', 'Measurement HTTP(S) retrieves a web page using HTTP and HTTPS.', and 'An alert is triggered when the calculated measurement exceeds the threshold set.' At the bottom right, there is an orange 'Add' button.

g) Cliquer sur le **bouton Add**

h) Revenir sur l'interface **réseau**, puis cliquer sur le menu **shortcut/Active Monitoring**



## 12. Visualisation du flux en direct

a) Sélectionner le menu **Flows/Live**

b) Cliquer sur un **client** ou un **Server** pour voir le détail du périphérique

Recently Live Flows												Flow Idle Timeout: 60 sec
10 Hosts Status Severity Direction L7 Protocol Categories DSCP Host Pool Networks IP Version Protocol Flow Exporter												
Serial	Application	Proto	Client	Server	Duration	Score	Breakdown	Actual Thpt	Total Bytes	Info	Flow Exp	
1	TLS DPI	TCP	matteo-precision-3541 38930	185.150.190.203 https	03:51:04	10	Server	17.40 Kbps	28.46 MB			
2	TLS DPI	TCP	matteo-precision-3541 48308	ws2.bybit.com https	03:51:03	10	Server	3.80 Kbps	14.85 MB			
3	QUIC.YouTube DPI	UDP	matteo-precision-3541 51863	rr5--sn-hpa7zns6.google... https	01:07	10	Server	0 bps	9.89 MB	rr5--sn-hpa7zns6.googlevideo.com		
4	TLS DPI	TCP	matteo-precision-3541 48292	ws2.bybit.com https	03:51:02	10	Server	0 bps	3.4 MB			
5	TLS DPI	TCP	matteo-precision-3541 47622	84.16.251.31 https	03:51:04	10	Server	0 bps	2.16 MB			
6	TLS DPI	TCP	matteo-precision-3541 48322	ws2.bybit.com https	03:50:58	10	Client Server	1.30 Kbps	560.77 KB			
7	TLS DPI	TCP	matteo-precision-3541 34924	84.16.253.86 https	03:50:59	10	Client Server	0 bps	535.43 KB			

## 13. Ajout de la géolocalisation des IPs

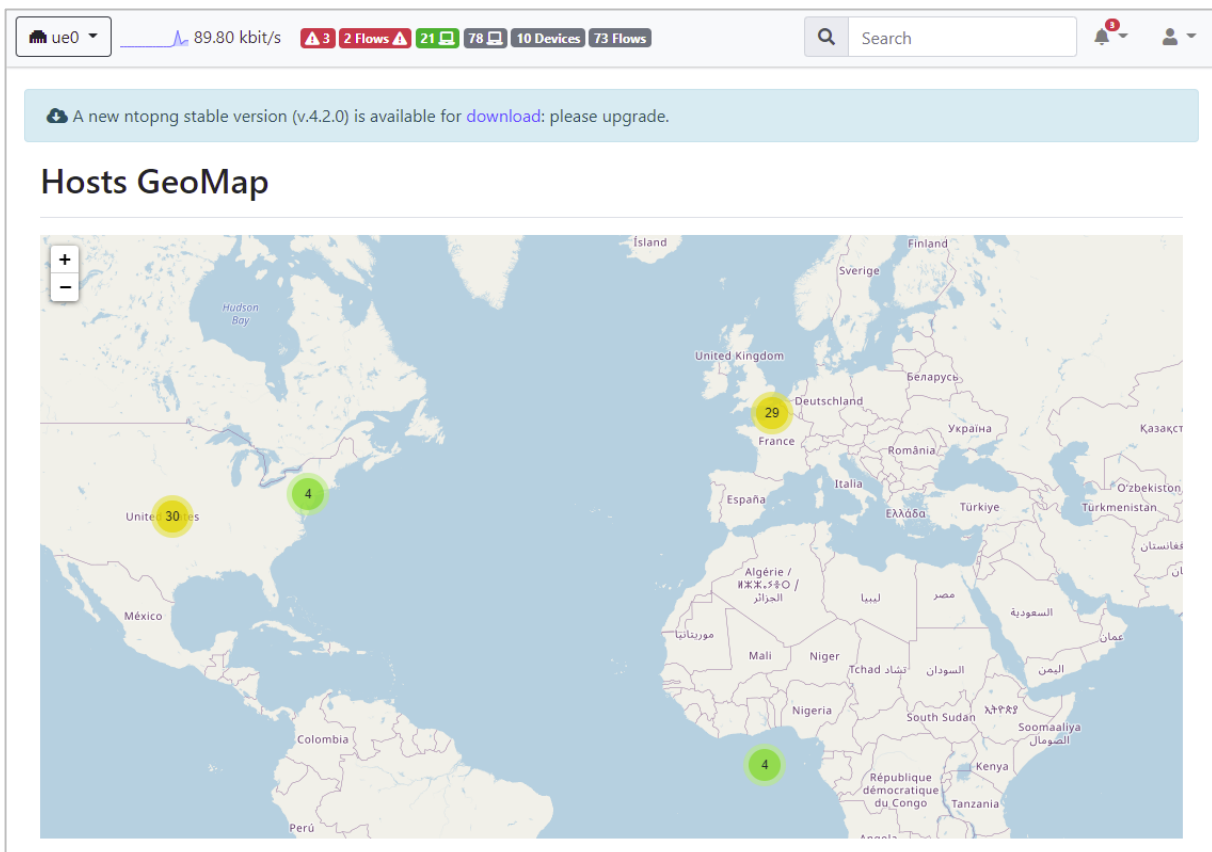
Ntopng prend en charge la géolocalisation des IPs identifiées. Pour activer cette géolocalisation :

a) Télécharger les fichiers Gzip : [GeoLite2 ASN](#), [GeoLite2 City](#) et [GeoLite2 Country](#) pour **tester uniquement**. Une version gratuite est proposée sur ce site <https://dev.maxmind.com>

b) Copier les 3 fichiers dans le répertoire `/var/lib/GeoIP/` ou `/usr/share/GeoIP/`

c) Redémarrer le serveur

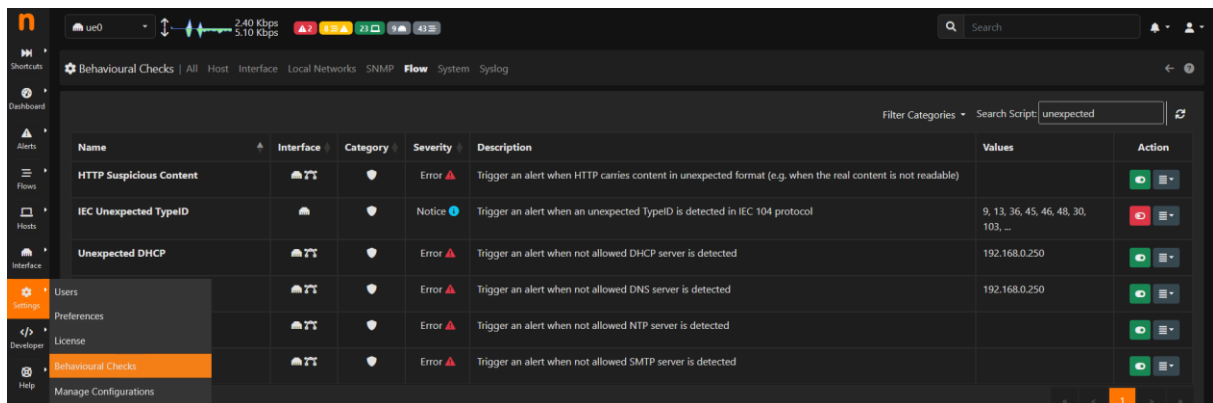
d) Sélectionner le nouveau menu **Maps/Geo Map** pour afficher la localisation des @IP



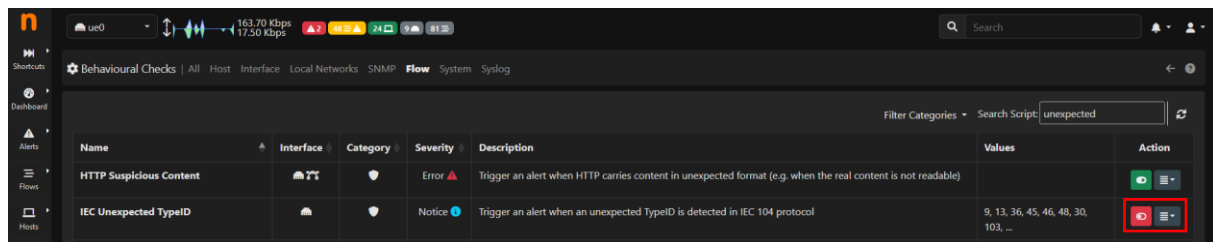
## 14. Configurer les contrôles comportementaux

Cette section permet d'envoyer des alertes sur chacun des services (DHCP, DNS, SMTP, NTP) en cas d'anomalies. Pour cela il faut les configurer.

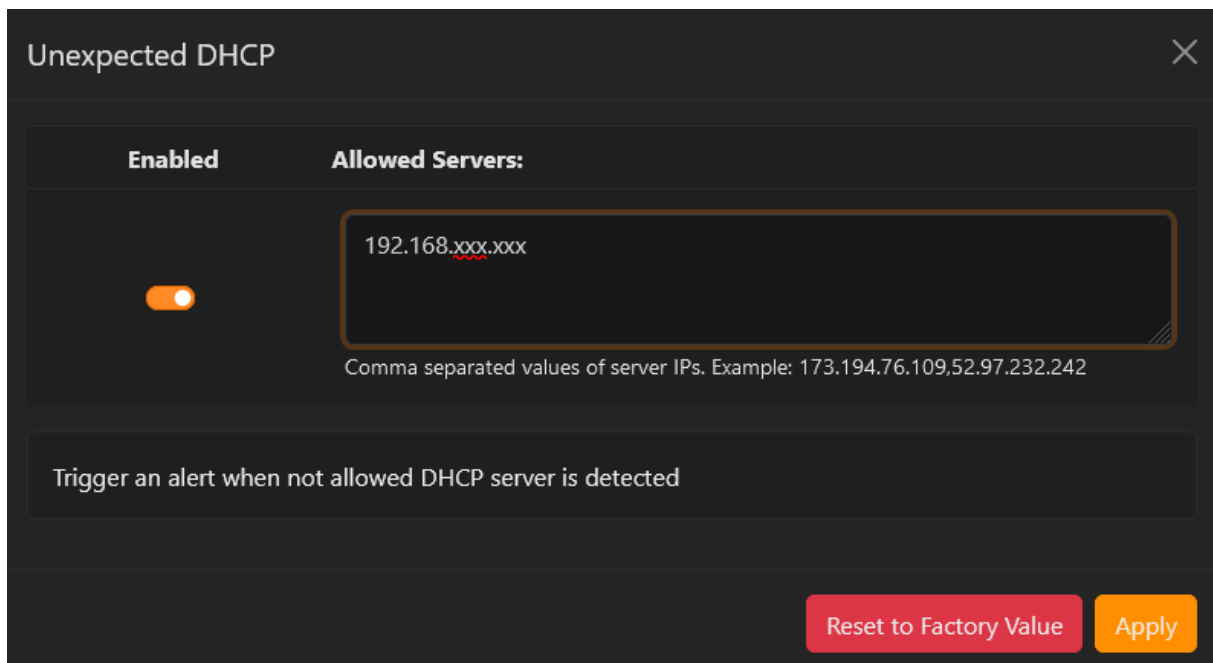
a) Cliquer sur le menu **Settings/ Behavioural Checks+**



b) Cliquer sur chaque **service** pour le configurer



c) Cliquer sur l'**interrupteur** pour activer la surveillance et **saisir l'URL** de chaque **service**

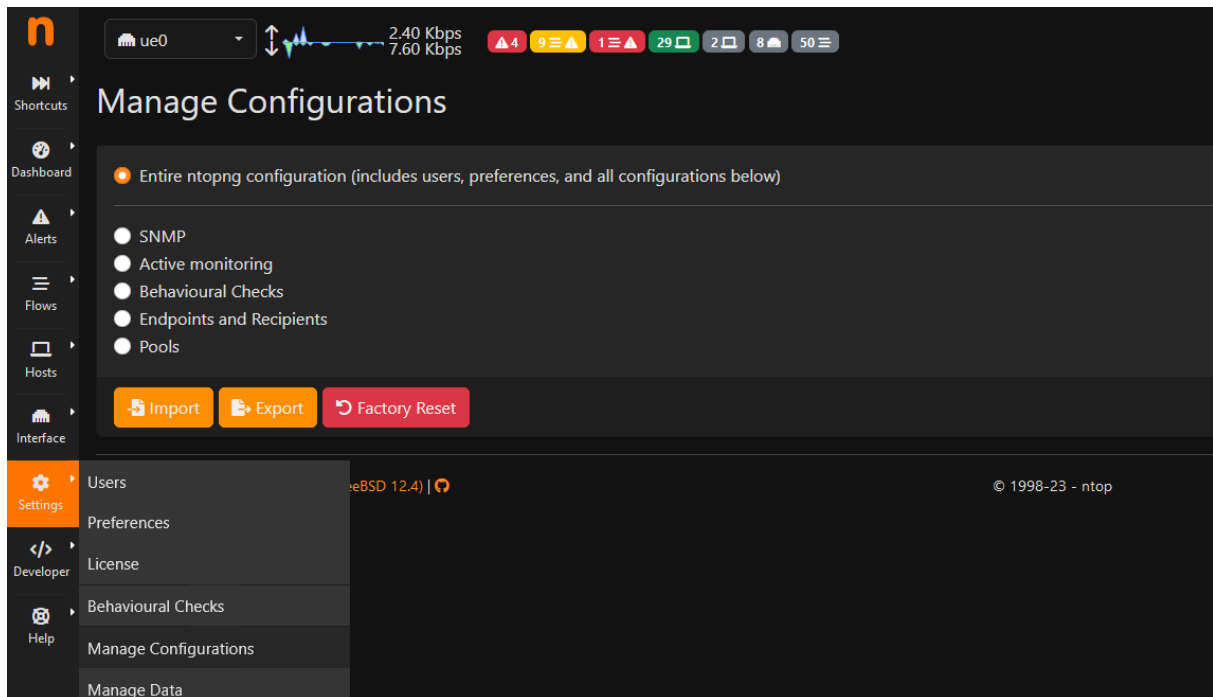


d) Cliquer sur le bouton **Apply**

## 15. Sauvegarder les paramètres de configuration

Tous les réglages effectués dans Ntopng peuvent être sauvegarder dans un fichier **.json** permettant ainsi de les réimporter en cas de besoin.

a) Cliquer sur le menu **Settings/Manage Configurations**



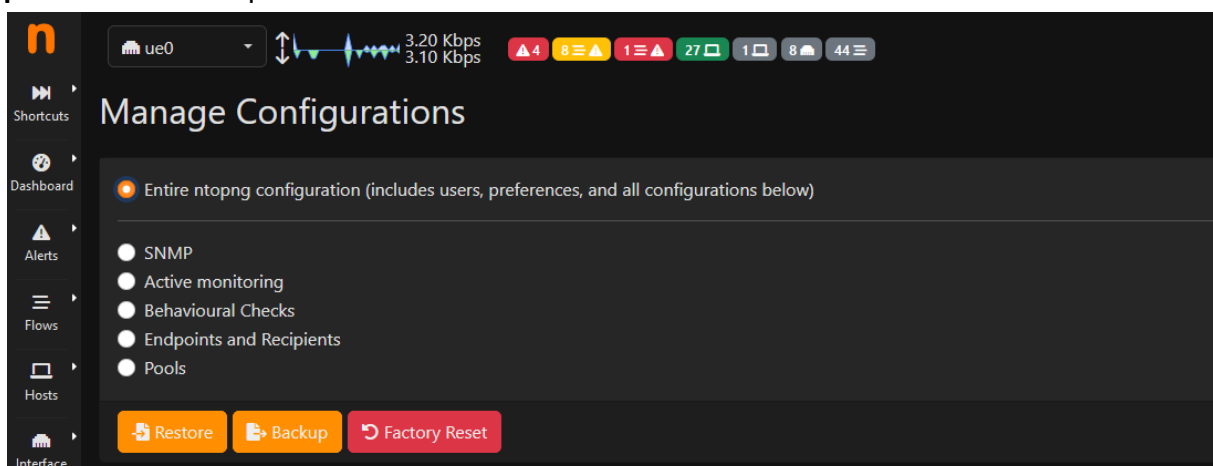
b) Sélectionner la ligne **Entire ntopng...** pour sauvegarder tous les paramètres

c) Cliquer sur le bouton **Export**

## 16. Restauration des paramètres de configuration

Tous les paramètres sauvegardés, peuvent être restaurer

a) Cliquer sur la ligne **SNMP ou une autre**, puis cliquer à nouveau sur la première ligne (le bouton **Import** sera modifier par **Restore**)



b) Cliquer sur le bouton **Restore** pour rétablir les paramètres sauvegarder

## 17. Mise à jour de Ntopng

La mise à jour de Ntopng peut se faire via le menu **admin de l'interface web**, soit en ligne de commande.

```
# pkg update  
# pkg upgrade
```

## 18. Désinstallation de Ntopng

Désinstaller Ntopng peut-être parfois nécessaire pour le réinstaller

```
# service ntopng stop  
# pkg delete redis  
# pkg delete ntopng  
# reboot
```

## 19. Liens annexes

Liste de contenu à consulter ou à télécharger pour **Ntopng**

- Ntopng Ubuntu : <https://reussirweb.com>
- Extensions : <https://github.com/P3TERX/GeoLite.mmdb>
- Monitorer son réseau : <https://www.it-connect.fr>
- Configuration FreeBSD : <https://www.cyberciti.biz>
- Documentation : <https://www.ntop.org/guides/ntopng>
- Packages Raspian : <https://packages.ntop.org/RaspberryPi>
- Geolocalisation : <https://github.com/ntop/ntopng/blob/dev/doc/README.geolocation.md>

## 20. Commandes RaspberryPi

a) Liste des commandes basique à la gestion du serveur RaspberryPi

```
# shutdown -h now # éteint le serveur en toute sécurité  
# shutdown -r now # redémarre le serveur en toute sécurité  
# pkg install xrdp # installe le bureau à distance RDP  
# nano /etc/rc.conf -> service_enable=YES # active le service au démarrage  
# pkg install wget # installe wget  
##### Désactive la mise en veille #####  
# systemctl mask sleep.target suspend.target hibernate.target hybrid-sleep.target
```

## 21. Conclusion

**Ntopng** est installé et configuré avec succès sur le serveur **RaspberryPi FreeBSD**. On peut désormais analyser son trafic réseau via les alertes.

Destiné au RaspberryPi (Raspbian), **Ntopng** fonctionne aussi parfaitement sur une distribution Debian, Windows, MacOS, Docker...

Pour Linux Ubuntu : <https://www.gamingdeputy.com/fr/guide-pratique>

Pour tout autre distribution : <https://packages.ntop.org>