



14/0/4/2025

DEPLOIEMENT D'UN SITE WEB PUBLIQUE AVEC UNE BASE POSTGRESQL.

PERIER--PICARD VALENTIN



Table des matières

Infrastructure	2
Les serveurs :.....	2
Déploiement de Proxmox.....	2
Déploiement de OPNsense.....	3
Installation InfluxDB	3
Installation de la VM InfluxDB.....	3
Installation de InfluxDB2	4
Parametrage de InfluxDB2	5
Ajout de Proxmox dans InfluxDB2	5
Installation de Grafana	6
Création des VMs	6
Installation de Grafana	6
Configuration de Grafana.....	7
Création d'un premier Dashboard.....	8
Mise en place de Nginx.....	10
Installation de la VM Nginx.....	10
Installation de Nginx	11
Mise en place du Load Balancer	12
Installation de Fail2ban	13
Parametrage de Unbound DNS	14
Activation du service dans OPNsense	14
Monitoring de l'OPNsense.....	14
Mise en place de telegraf sur l'OPNsense	14
Ajout du Dashboard dans grafana.....	17
Test du service	18
Test avec un ordinateur client connecté sur le serveur	18

Infrastructure

Les serveurs :

L'entreprise SuperInfo possède 3 serveurs, 1 switch et 1 OPNsense.

- **Premier serveur :**
CPU: 2x Intel(R) Xeon(R) CPU E5620 8 cœurs
RAM: 16 Go DDR3
Stockage: 4 HDD de 130Go en RAID 5 physique pour un total de 400Go utilisable
- **Deuxième serveur :**
CPU: 13th Gen Intel(R) Core(TM) i7-13700 24 cœurs
RAM: 32 Go DDR5
Stockage: 1 SSD Nvme 500Go utilisable
- **Troisième serveur :**
CPU: 13th Gen Intel(R) Core(TM) i7-13700 24 cœurs
RAM: 32 Go DDR5
Stockage: 1 SSD Nvme 500Go utilisable
- **OPNsense :**
CPU: Intel® Core™ i5-6600 4 coeurs
RAM: 16 Go DDR3
Stockage: 1 HDD de 500Go utilisable

L'entreprise SuperInfo a décidé de déployer Proxmox en cluster sur le serveur 1, 2 et 3.
Elle a aussi choisi d'utiliser OPNsense comme routeur installé sur le serveur OPNsense.

Déploiement de Proxmox.

On effectue une installation de Proxmox basique.

Les serveurs étant sur le Vlan 4 « serveur » on modifie durant l'installation leurs ips :

- 192.168.4.2
- 192.168.4.3
- 192.168.4.4

Les serveurs 2 et 3 ont deux interfaces, on connecte donc la deuxième interface sur le Vlan 10 « DMZ » sans leur attribuer d'ips.

Nous pouvons ensuite les faire rejoindre un cluster.

Cluster Information			
Create Cluster Join Information Join Cluster			
Cluster Name:	main	Config Version:	3
		Number of Nodes:	3
Cluster Nodes			
Nodename	ID ↑	Votes	Link 0
pve1	1	1	192.168.4.2
pve2	2	1	192.168.4.3
pve3	3	1	192.168.4.4

Nous pouvons ensuite exécuter les script Proxmox VE Post Install de Proxmox VE Helper Scripts afin de terminer l'installation de Proxmox et désactiver les options inutiles.

Déploiement de OPNsense

OPNsense sera installé sur le serveur 4.

Le serveur OPNsense possède deux interfaces :

- Interface 1 WAN
- Interface 2 LAN

On crée dessus 3 Vlan afin de séparer les différents réseaux :

- Vlan 4 Serveurs
192.168.4.1/24
- Vlan 10 DMZ
192.168.10.1/24
- Vlan 50 Clients
192.168.50.1/24

Installation InfluxDB

Installation de la VM InfluxDB

SuperInfo a fait le choix d'utiliser Debian 12.

Le VM influxdb a 2 CPU et 4 Go de RAM et un disque de 20G.

Elle n'a accès qu'à l'interface sur le Vlan 4.

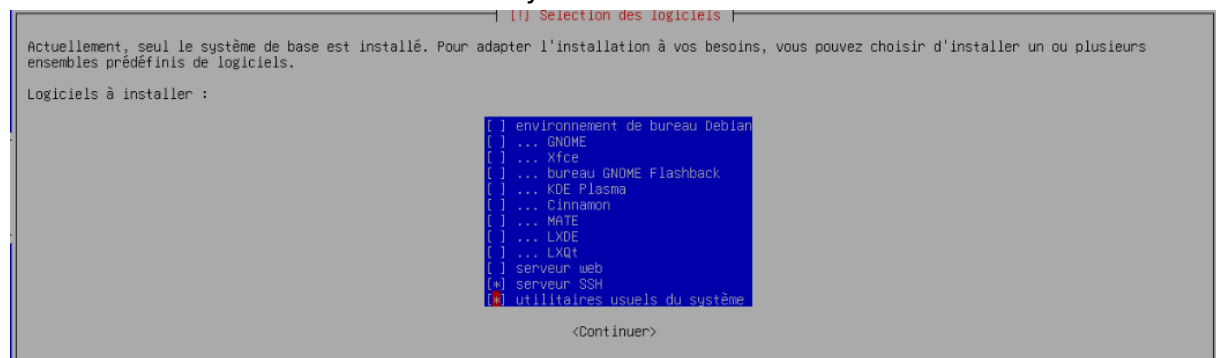
On procède à une installation Debian classique :

Installer en Français.

On a nommé la VM « influxdb »

On a effectué une installation sous LVM non chiffré avec le dossier /home séparé.

Seul un serveur SSH et les utilitaires systèmes sont installés sur la VM.



```
| [!] Selection des logiciels |  
  
Actuellement, seul le système de base est installé. Pour adapter l'installation à vos besoins, vous pouvez choisir d'installer un ou plusieurs ensembles prédéfinis de logiciels.  
  
Logiciels à installer :  
  
[ ] environnement de bureau Debian  
[ ] ... GNOME  
[ ] ... Xfce  
[ ] ... bureau GNOME Flashback  
[ ] ... KDE Plasma  
[ ] ... Cinnamon  
[ ] ... MATE  
[ ] ... LXDE  
[ ] ... LXQt  
[ ] serveur web  
[*] serveur SSH  
[*] utilitaires usuels du système  
  
<Continuer>
```

Une fois la vm installé on vérifi que qemu-guest-agent est bien installé sur la vm.

```
root@isntall:~# apt install qemu-guest-agent
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
qemu-guest-agent est déjà la version la plus récente (1:7.2+dfsg-7+deb12u12).
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.
```

Installation de InfluxDB2

Les paquets InfluxDB2 sont sur le depot de Influx, il faut donc ajouter les dépôts à la main grâce aux commande fournies dans la documentation.

```
curl --silent --location -O \
```

```
https://repos.influxdata.com/influxdata-archive.key
```

```
echo "943666881a1b8d9b849b74caebf02d3465d6beb716510d86a39f6c8e8dac7515
influxdata-archive.key" \
```

```
| sha256sum --check - && cat influxdata-archive.key \
```

```
| gpg --dearmor \
```

```
| sudo tee /etc/apt/trusted.gpg.d/influxdata-archive.gpg > /dev/null \
```

```
&& echo 'deb [signed-by=/etc/apt/trusted.gpg.d/influxdata-archive.gpg]
```

```
https://repos.influxdata.com/debian stable main' \
```

```
| sudo tee /etc/apt/sources.list.d/influxdata.list
```

```
root@isntall:~# curl --silent --location -O \
https://repos.influxdata.com/influxdata-archive.key
echo "943666881a1b8d9b849b74caebf02d3465d6beb716510d86a39f6c8e8dac7515 influxdata-archive.key" \
| sha256sum --check - && cat influxdata-archive.key \
| gpg --dearmor \
| sudo tee /etc/apt/trusted.gpg.d/influxdata-archive.gpg > /dev/null \
&& echo 'deb [signed-by=/etc/apt/trusted.gpg.d/influxdata-archive.gpg] https://repos.influxdata.com/debian stable main' \
| sudo tee /etc/apt/sources.list.d/influxdata.list
influxdata-archive.key: Réussi
deb [signed-by=/etc/apt/trusted.gpg.d/influxdata-archive.gpg] https://repos.influxdata.com/debian stable main
root@isntall:~#
```

On peut ensuite installer influxDB2 via apt :

```
root@isntall:~# sudo apt-get update && sudo apt-get install influxdb2
Atteint :1 http://deb.debian.org/debian bookworm InRelease
Atteint :2 http://deb.debian.org/debian bookworm-updates InRelease
Réception de :3 https://repos.influxdata.com/debian stable InRelease [6 907 B]
Atteint :4 http://security.debian.org/debian-security bookworm-security InRelease
Réception de :5 https://repos.influxdata.com/debian stable/main amd64 Packages [14,9 kB]
21,8 ko réceptionnés en 0s (107 ko/s)
Lecture des listes de paquets... Fait
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  influxdb2-cli
Les NOUVEAUX paquets suivants seront installés :
  influxdb2 influxdb2-cli
0 mis à jour, 2 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 61,3 Mo dans les archives.
Après cette opération, 147 Mo d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] o
Réception de :1 https://repos.influxdata.com/debian stable/main amd64 influxdb2 amd64 2.7.11-1 [49,6 MB]
23% [1 influxdb2 17,4 MB/49,6 MB 35%]
```

Parametrage de InfluxDB2

Un fois InfluxDB2 installé on peut se rendre sur le serveur web intégré et créé une Organisation.

The screenshot shows the 'Setup Initial User' page of the InfluxDB2 web interface. At the top, there are three progress indicators: 'Welcome' (completed), 'Initial User Setup' (active), and 'Complete'. The main heading is 'Setup Initial User' with a subtext: 'You will be able to create additional Users, Buckets and Organizations later'. The form contains the following fields:

- Username:** A text input field containing 'valet'.
- Password:** A password input field with masked characters '.....'.
- Confirm Password:** A password input field with masked characters '.....'.
- Initial Organization Name:** A text input field containing 'valete'.
- Initial Bucket Name:** A text input field containing 'proxmox'.

A blue 'CONTINUE' button is located at the bottom right of the form.

Ajout de Proxmox dans InfluxDB2

Tout d'abord il faut créer un clés API pour Proxmox.

Il faut aller dans la catégorie Load Data puis API TOKENS puis generate tokens->Custom

On peut ensuite l'autoriser seulement pour le bucket Proxmox

The screenshot shows the 'Edit: InfluxDB: indluxdb' configuration page. It features a table-like layout for configuration parameters:

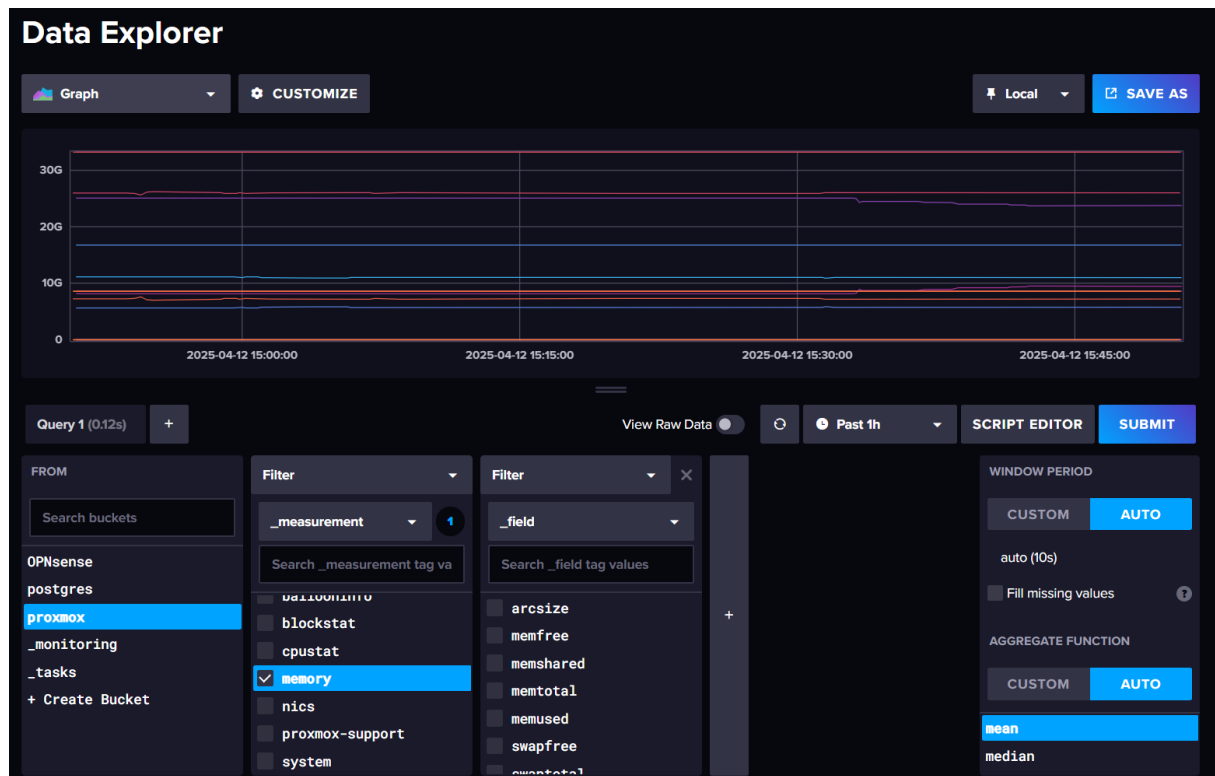
Name:	indluxdb	Enabled:	☒
Server:	192.168.4.28	Organization:	valete
Port:	8086	Bucket:	proxmox
Protocol:	HTTP	Token:	unchanged

API Path Prefix:		Batch Size (b):	25000000
Timeout (s):	1	MTU:	1500

Verify Certificate: ☒

At the bottom, there is a 'Help' button (with a question mark icon), an 'Advanced' checkbox (which is checked), and an 'OK' button.

On test dans le Data Explorer que les données sont bien présentes :



Installation de Grafana

Création des VMs

Pour les deux VMs Grafana nous allons installer des VMs sous Debian 12 comme pour InfluxDB.

Les VMs grafana ont 2 CPU et 4 Go de RAM et un disque de 10Go chacune.

Elles n'ont que accès à l'interface sur le Vlan 4.

On nomme les VMs « grafana » et « grafanaRep ».

Installation de Grafana

Les paquets Grafana sont sur leur propre dépôts comme InfluxDB il faut donc ajouter les dépôts.

```
sudo apt-get install -y apt-transport-https software-properties-common wget  
sudo mkdir -p /etc/apt/keyrings/
```

```
wget -q -O - https://apt.grafana.com/gpg.key | gpg --dearmor | sudo tee  
/etc/apt/keyrings/grafana.gpg > /dev/null
```

```
echo "deb [signed-by=/etc/apt/keyrings/grafana.gpg] https://apt.grafana.com stable  
main" | sudo tee -a /etc/apt/sources.list.d/grafana.list
```

```
echo "deb [signed-by=/etc/apt/keyrings/grafana.gpg] https://apt.grafana.com beta main"  
| sudo tee -a /etc/apt/sources.list.d/grafana.list
```

```

root@isntall:~# sudo mkdir -p /etc/apt/keyrings/
wget -q -O - https://apt.grafana.com/gpg.key | gpg --dearmor | sudo tee /etc/apt/keyrings/grafana.gpg > /dev/null
root@isntall:~# echo "deb [signed-by=/etc/apt/keyrings/grafana.gpg] https://apt.grafana.com stable main" | sudo tee -a /etc/apt/sources.list.d/grafana.list
deb [signed-by=/etc/apt/keyrings/grafana.gpg] https://apt.grafana.com stable main
root@isntall:~# echo "deb [signed-by=/etc/apt/keyrings/grafana.gpg] https://apt.grafana.com beta main" | sudo tee -a /etc/apt/sources.list.d/grafana.list
deb [signed-by=/etc/apt/keyrings/grafana.gpg] https://apt.grafana.com beta main
root@isntall:~#

```

On peut ensuite installer Grafana avec le gestionnaire de paquet apt.

```

root@isntall:~# sudo apt-get update && sudo apt-get install grafana
Atteint :1 http://deb.debian.org/debian bookworm InRelease
Atteint :2 http://deb.debian.org/debian bookworm-updates InRelease
Réception de :3 https://apt.grafana.com stable InRelease [7 661 B]
Réception de :4 https://apt.grafana.com beta InRelease [5 975 B]
Atteint :5 http://security.debian.org/debian-security bookworm-security InRelease
Réception de :6 http://deb.debian.org/debian bookworm/main amd64 DEP-11 Metadata [4 492 kB]
Atteint :7 https://repos.influxdata.com/debian stable InRelease
Réception de :8 http://deb.debian.org/debian bookworm/non-free-firmware amd64 DEP-11 Metadata [15,5 kB]
Réception de :9 https://pkgs.tailscale.com/stable/debian bookworm InRelease
Réception de :10 https://apt.grafana.com stable/main amd64 Packages [379 kB]
Réception de :11 https://apt.grafana.com beta/main amd64 Packages [1 616 B]
4 909 ko réceptionnés en 1s (4 283 ko/s)
Lecture des listes de paquets... Fait
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  musl
Les NOUVEAUX paquets suivants seront installés :
  grafana musl
0 mis à jour, 2 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 169 Mo dans les archives.
Après cette opération, 631 Mo d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] o
Réception de :1 http://deb.debian.org/debian bookworm/main amd64 musl amd64 1.2.3-1 [406 kB]
Réception de :2 https://apt.grafana.com stable/main amd64 grafana amd64 11.6.0 [169 MB]
13% [2 grafana 5 800 kB/169 MB 3%]

```

Configuration de Grafana

On crée dans un premier temps une nouvelle clé API comme fait plus haut qui a accès à tous les buckets pour Grafana.

On lit ensuite Grafana à InfluxDB en ajoutant InfluxDB2 comme Data Source :

Name ⓘ influxdb

Default ☒

Query language

Flux

ⓘ

Support for Flux in Grafana is currently in beta
Please report any issues to:
<https://github.com/grafana/grafana/issues>

HTTP

URL ⓘ http://192.168.4.28:8086

Allowed cookies ⓘ New tag (enter key to add) Add

Timeout ⓘ Timeout in seconds

InfluxDB Details

Organization valete

Token configured

Reset

Default Bucket default bucket

Min time interval ⓘ 10s

Max series ⓘ 1000

Delete

Save & test

Création d'un premier Dashboard

On va créer notre premier Dashboard dans Grafana, ce dashboard sera dédié à Proxmox.

Nous allons importer un Dashboard créé par la communauté trouvée sur le site de grafana.

<https://grafana.com/grafana/dashboards/16537-proxmox-flux/>

Import dashboard

Import dashboard from file or Grafana.com

Importing dashboard from Grafana.com

Published by

christiangursky

Updated on

2022-07-05 18:52:03

Options

Name

Proxmox 7 Flux

Folder

Dashboards

Unique identifier (UID)

The unique identifier (UID) of a dashboard can be used for 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.

lfgdXjtnkg

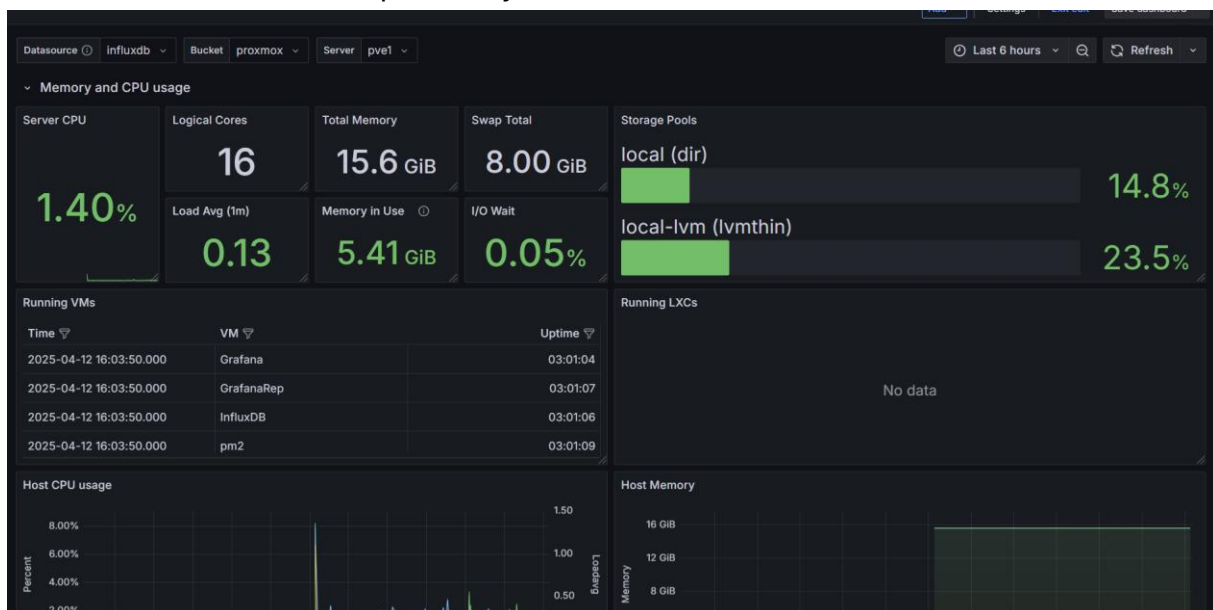
InfluxDB

influxdb

Import

Cancel

Le dashboard a bien été importé on y retrouve bien nos données Proxmox :



Mise en place de Nginx

Installation de la VM Nginx

Cette fois SuperInfo a décidé d'utiliser Alpine Linux comme système d'exploitation pour son serveur.

La VM a 1 CPU et 2 Go de RAM et un disque de 5 Go.

On procède à une installation d'Alpine classique avec la commande `setup-alpine` :

```
localhost: # setup-alpine

ALPINE LINUX INSTALL

Keymap
af  al  an  ara  at  az  ba  bd  be  bg  br  brai  by  ca  ch  cn  cn  cz  de  dk  dz  ee  epo  es  fi  fo
fr  gb  ge  gh  gr  hr  hu  id  ie  il  in  iq  ir  is  it  jp  ke  kg  kr  kz  la  latin  lk  lt  lu  na
nd  ne  nk  nl  nm  nt  nj  ny  no  nz  ph  pk  pl  pt  ro  rs  ru  se  si  sk  sy  th  tj  tn  tr
tu  ua  us  uz  on

Select keyboard layout: [none] fr

fr-afnor      fr-azerty      fr-bepo      fr-bepo_afnor      fr-bepo_latin9      fr-bre      fr-duorak
fr-ergol      fr-ergol_iso      fr-geo      fr-latin9      fr-latin9_nodeadkeys      fr-mac      fr-nodeadkeys
fr-oci        fr-oss            fr-oss_latin9      fr-oss_nodeadkeys      fr-us            fr

Select variant (or 'abort'): fr-azerty10

fr-afnor      fr-azerty      fr-bepo      fr-bepo_afnor      fr-bepo_latin9      fr-bre      fr-duorak
fr-ergol      fr-ergol_iso      fr-geo      fr-latin9      fr-latin9_nodeadkeys      fr-mac      fr-nodeadkeys
fr-oci        fr-oss            fr-oss_latin9      fr-oss_nodeadkeys      fr-us            fr

Select variant (or 'abort'): fr-azerty

* WARNING: you are stopping a boot service
* Caching service dependencies ...
* Setting keymap ...

Hostname

Enter system hostname (fully qualified form, e.g. 'foo.example.org') [localhost] pm2
```

On nomme la VM nginx.

Durant l'installation il ne faut pas oublier d'activer les dépôts communautaires.

```
APK Mirror

(f) Find and use fastest mirror
(s) Show mirrorlist
(r) Use random mirror
(e) Edit /etc/apk/repositories with text editor
(c) Community repo enable
(skip) Skip setting up apk repositories

Enter mirror number or URL: [1] c

Community repository enabled

Community repository enabled
(f) Find and use fastest mirror
(s) Show mirrorlist
(r) Use random mirror
(e) Edit /etc/apk/repositories with text editor
(c) Community repo disable
(skip) Skip setting up apk repositories

Enter mirror number or URL: [1]
```

Une fois l'installation terminée on peut redémarrer le système en enlevant le disque d'installation de la VM.

On installe ensuite `qemu-guest-agent` et on ajoute au démarrage :

```

alpine:~# apk update
fetch http://alpinelinux.mirrors.ovh.net/v3.21/main/x86_64/APKINDEX.tar.gz
fetch http://alpinelinux.mirrors.ovh.net/v3.21/community/x86_64/APKINDEX.tar.gz
v3.21.3-305-gf53b3a2c730 [http://alpinelinux.mirrors.ovh.net/v3.21/main]
v3.21.3-306-g591e6485dc1 [http://alpinelinux.mirrors.ovh.net/v3.21/community]
OK: 25395 distinct packages available
alpine:~# apk add qemu-guest-agent
(1/9) Installing libffi (3.4.7-r0)
(2/9) Installing libintl (0.22.5-r0)
(3/9) Installing libmount (2.40.4-r0)
(4/9) Installing pcre2 (10.43-r0)
(5/9) Installing glib (2.82.5-r0)
(6/9) Installing numactl (2.0.18-r0)
(7/9) Installing liburing (2.8-r0)
(8/9) Installing qemu-guest-agent (9.1.2-r1)
(9/9) Installing qemu-guest-agent-openrc (9.1.2-r1)
Executing busybox-1.37.0-r12.trigger
Executing glib-2.82.5-r0.trigger
OK: 140 MiB in 65 packages
alpine:~# rc-update add qemu-guest-agent
* service qemu-guest-agent added to runlevel default

```

Le serveur Nginx a accès aux deux interfaces Vlan 4 et Vlan 10.

Installation de Nginx

On installe Nginx sur la VM grâce au gestionnaire de paquet apk :

```

alpine:~# apk add nginx
(1/3) Installing pcre (8.45-r3)
(2/3) Installing nginx (1.26.3-r0)
Executing nginx-1.26.3-r0.pre-install
Executing nginx-1.26.3-r0.post-install
(3/3) Installing nginx-openrc (1.26.3-r0)
Executing busybox-1.37.0-r12.trigger
OK: 214 MiB in 89 packages

```

On ajoute un fichier proxy_params qui contient la configuration du reverse proxy.

```

nginx:~# ls /etc/nginx/
dhparam.pem      fastcgi_params  mime.types      nginx.conf      scgi_params
fastcgi.conf     http.d          modules         proxy_params    uwsgi_params

```

```

proxy_set_header Upgrade      $http_upgrade;
proxy_set_header Connection   "upgrade";
proxy_pass_request_headers    on;
proxy_buffering                off;
client_max_body_size          0;
proxy_connect_timeout          60s;
proxy_read_timeout             60s;
proxy_send_timeout             60s;
send_timeout                   60s;
proxy_buffer_size              4k;
proxy_buffers                   4 32k;
proxy_busy_buffers_size        64k;
proxy_temp_file_write_size     64k;
proxy_set_header Host          $host;
#proxy_set_header Host         $host:$server_port;
proxy_set_header X-Real-IP     $remote_addr;
#proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;

```

On ajoute aux scripts de démarrage :

rc-update add nginx

Mise en place du Load Balancer

On crée un fichier grafana.conf dans le dossier http.d qui contient la config du frontend et backend pour le site web.

```
upstream backend {
    server 192.168.4.31:3000;
    server 192.168.4.53:3000 backup;
}

server {
    listen 443 ssl;
    server_name grafana.lan;

    ssl_certificate /etc/ssl/certs/nginx-selfsigned.crt;
    ssl_certificate_key /etc/ssl/private/nginx-selfsigned.key;

    location / {
        include proxy_params;
        proxy_pass http://backend;
    }
}
```

On crée aussi un certificat SSL afin que le site soit accessible en SSL.

```
nginx:~# openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/nginx-selfsigned.key -out /etc/ssl/certs/nginx-selfsigned.crt
nginx:~# openssl dhparam -out /etc/nginx/dhparam.pem 4096
```

Installation de Fail2ban

On installe Fail2ban sur la machine avec le gestionnaire de paquet apk.

```
alpine: # apk add fail2ban
(1/22) Installing libbz2 (1.0.8-r6)
(2/22) Installing libexpat (2.7.0-r0)
(3/22) Installing gdbm (1.24-r0)
(4/22) Installing mpdecimal (4.0.0-r0)
(5/22) Installing libpanelw (6.5_p20241006-r3)
(6/22) Installing readline (8.2.13-r0)
(7/22) Installing python3 (3.12.10-r0)
(8/22) Installing python3-pycache-pyc0 (3.12.10-r0)
(9/22) Installing pyc (3.12.10-r0)
(10/22) Installing libnsl (1.0.5-r2)
(11/22) Installing libnftnl (1.2.8-r0)
(12/22) Installing libxtables (1.8.11-r1)
(13/22) Installing iptables (1.8.11-r1)
(14/22) Installing iptables-openrc (1.8.11-r1)
(15/22) Installing acl-libs (2.3.2-r1)
(16/22) Installing popt (1.19-r4)
(17/22) Installing logrotate (3.21.0-r1)
(18/22) Installing logrotate-openrc (3.21.0-r1)
(19/22) Installing fail2ban-pyc (1.1.0-r2)
(20/22) Installing python3-pyc (3.12.10-r0)
(21/22) Installing fail2ban (1.1.0-r2)
(22/22) Installing fail2ban-openrc (1.1.0-r2)
Executing busybox-1.37.0-r12.trigger
OK: 252 MiB in 111 packages
alpine:~#
```

On l'ajoute aux scripts de démarrage :

```
rc-update add fail2ban
```

Pour activer fail2ban on ajoute enabled = true aux jail que l'on veut activer dans le fichier jail.local de la configuration de fail2ban

```
# To use more aggressive http-auth modes set filter parameter "mode" in jail.local:
# normal (default), aggressive (combines all), auth or fallback
# See "tests/files/logs/nginx-http-auth" or "filter.d/nginx-http-auth.conf" for usage example and details.
[nginx-http-auth]
# mode = normal
enabled = true
port    = http,https
logpath = %(nginx_error_log)s

# To use 'nginx-limit-req' jail you should have `ngx_http_limit_req_module`
# and define `limit_req` and `limit_req_zone` as described in nginx documentation
# http://nginx.org/en/docs/http/ngx_http_limit_req_module.html
# or for example see in 'config/filter.d/nginx-limit-req.conf'
[nginx-limit-req]
port    = http,https
logpath = %(nginx_error_log)s

[nginx-botsearch]
enabled = true
port    = http,https
logpath = %(nginx_error_log)s

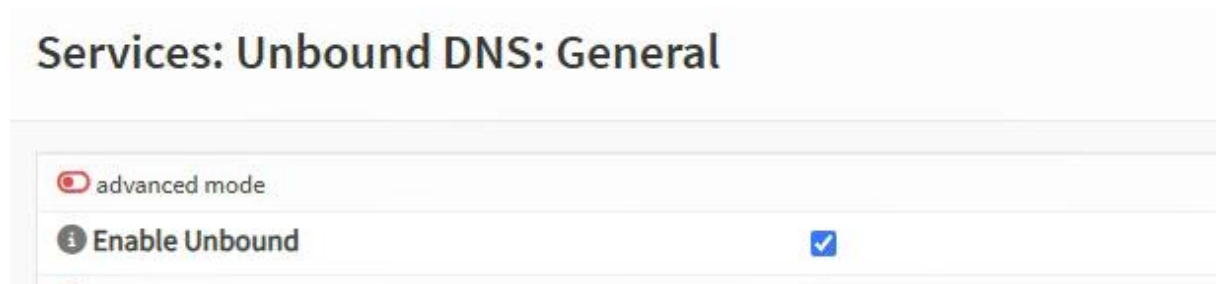
[nginx-bad-request]
enabled = true
port    = http,https
logpath = %(nginx_access_log)s

[nginx-forbidden]
enabled = true
port    = http,https
logpath = %(nginx_error_log)s
```

Parametrage de Unbound DNS

Activation du service dans OPNsense

Sur OPNsense il suffit d'aller dans Services->Unbound DNS et d'activer le service :



On ajoute ensuite les Overrides DNS pour notre serveur nginx

Edit Host Override

full help

Enabled

☒

Enable the override for this host

Host

Name of the host, without the domain part. Use "*" to create a wildcard entry.

Domain

Domain of the host, e.g. example.com

Type

A (IPv4 address)

Type of resource record, e.g. A or AAAA for IPv4 or IPv6 addresses

IP address

IP address of the host, e.g. 192.168.100.100 or fd00:abcd::1

Description

You may enter a description here for your reference (not parsed)

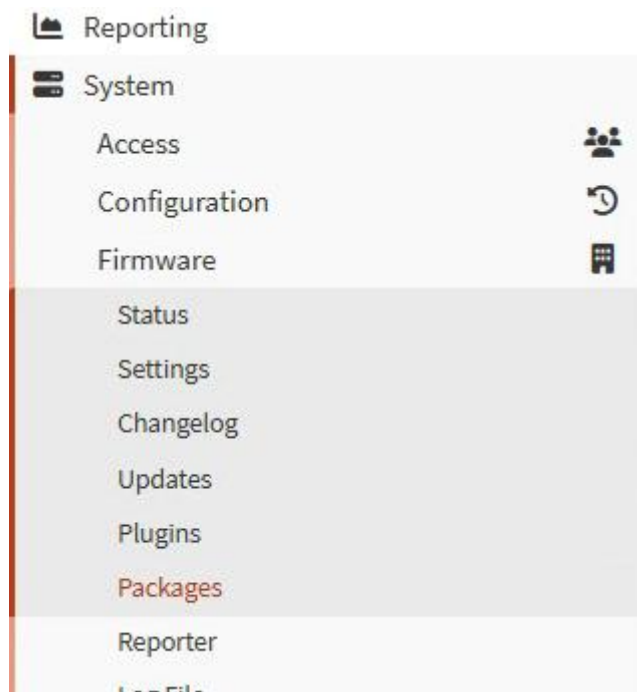
Cancel

Save

Monitoring de l'OPNsense

Mise en place de telegraf sur l'OPNsense

Il faut tout d'abord installer le plugin OPNsense dans la section system->Firmware->Plugins



System: Firmware

Status	Settings	Changelog	Updates	Plugins	Packages
telegraf	Version	Size	Tier	Repository	Comment
os-telegraf (installed)	1.12.12	99.7KiB	3	OPNsense	Agent for collecting metrics and data

Une fois installer on peut activer telegraf dans la section Services de OPNsense

Services: Telegraf: General

General

Tags

Enable Telegraf Agent

☒

Run as Root

☒

Interval

This will activate the telegraf agent.

This will start the process with wheel group and root user permission. Please use this with care, currently only needed for Unbound and Suricata.

Default data collection interval for all inputs in seconds.

Sur InfluxDB on peut maintenant créer un nouveau bucket nommé opnsense

Create Bucket ✕

Name*

opnsense ✓

Delete Data

NEVER OLDER THAN

90 days ▼

CANCEL CREATE

Puis créer un Token API avec l'accès au bucket opnsense

Generate a Custom API Token ✕

Description

opnsense

Q Filter Access Permissions...

Resources	Read	Write
▼ Buckets		
All Buckets	☐	☐
Individual Bucket Names		
OPNsense	☒	☒

Dans la partie output du service telegraf dans OPNsense on peut ensuite ajouter le

serveur InfluxDB2

▼ InfluxDB v2

Enable Influx v2 Output

☒

This will enable InfluxDB v2 as output. Format is without square brackets, just like `http://192.168.0.1:9999`.

Influx v2 URL

Set the URL where metrics should be sent to.

Influx v2 Token

Influx v2 authentication token.

Influx v2 Organization

Set the name of the organization in Influx v2.

Influx v2 Bucket

Set the name of the bucket in Influx v2.

Disable SSL verification v2

☐

This will skip chain and host verification.

Timeout

Flush timeout for the v2 Telegraf output in seconds, formatted as a string. If not provided, will default to 5. 0 means no timeout, but is not recommended. Increase if you get timeout errors.

Ajout du Dashboard dans grafana

Un fois dans grafana on peut ensuite importer un dashboard de la communauté comme fait plus haut.

<https://grafana.com/grafana/dashboards/16197-opnsense-metrics/>

Import dashboard

Import dashboard from file or Grafana.com

Importing dashboard from Grafana.com

Published by

mimirtech

Updated on

2022-05-02 07:56:02

Options

Name

Folder

Unique identifier (UID)

The unique identifier (UID) of a dashboard can be used for 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.

InfluxDB FluxQL

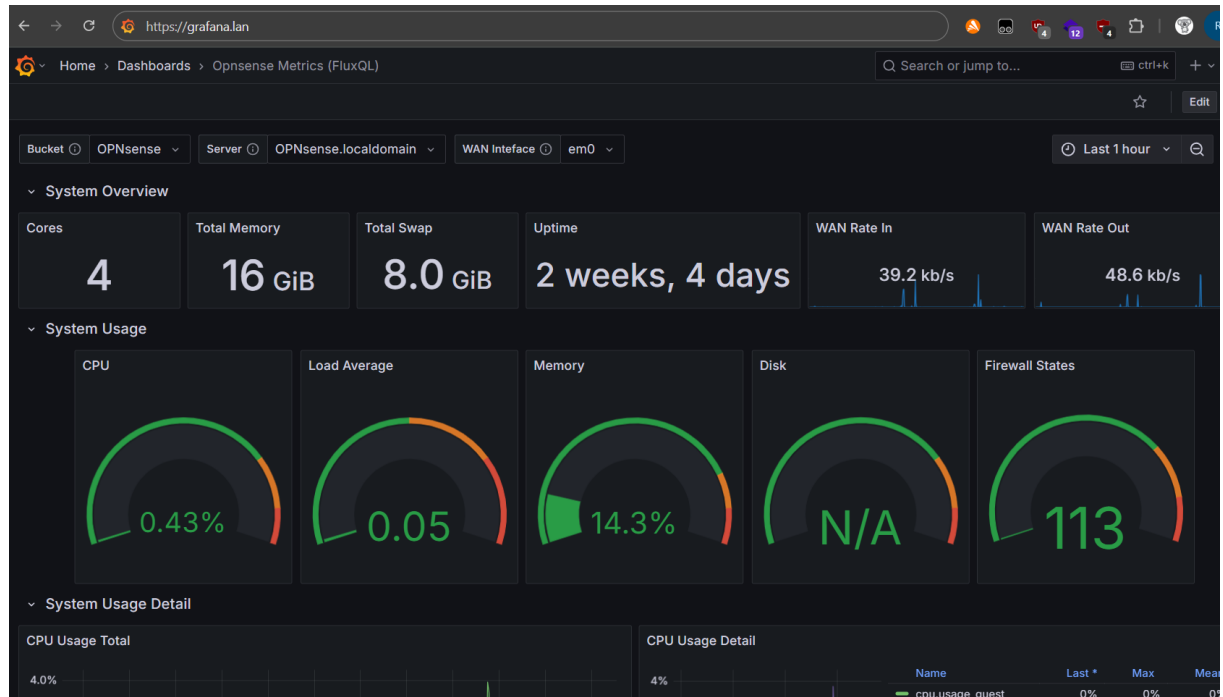
Import

Cancel

Test du service

Test avec un ordinateur client connecté sur le serveur

Il essaie d'accéder à grafana.lan via un navigateur internet



L'utilisateur accède bien au service Grafana en local.