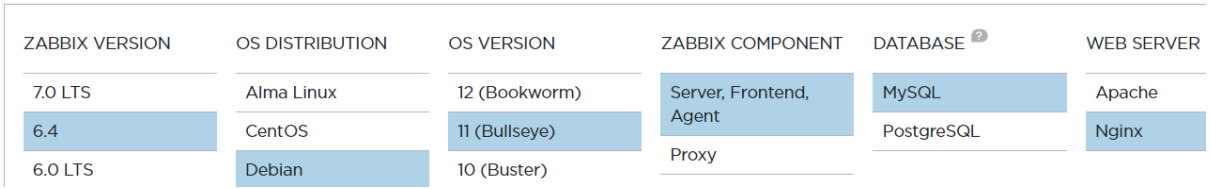
Version installée:



Install and configure Zabbix for your platform

a. Install Zabbix repository

wget https://repo.zabbix.com/zabbix/6.4/debian/pool/main/z/zabbix-release/zabbix-release_6.4-1+debian11_all.deb

```
root@debianzab:/home/renman# apt update && apt upgrade -y
Hit:1 http://security.debian.org/debian-security bullseye-security InRelease
Hit:2 http://deb.debian.org/debian bullseye InRelease
Hit:3 http://deb.debian.org/debian bullseye-updates InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@debianzab:/home/renman# wget https://repo.zabbix.com/zabbix/6.4/debian/pool/main/z/zabbix-release/zabbix-release_6.4-1+debian11_all.deb
--2024-09-01 21:53:40--  https://repo.zabbix.com/zabbix/6.4/debian/pool/main/z/zabbix-release/zabbix-release_6.4-1+debian11_all.deb
Resolving repo.zabbix.com (repo.zabbix.com)... 2604:a880:2:d0::2062:d001, 178.128.6.101
Connecting to repo.zabbix.com (repo.zabbix.com)|2604:a880:2:d0::2062:d001|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3740 (3.7K) [application/octet-stream]
Saving to: 'zabbix-release_6.4-1+debian11_all.deb'

zabbix-release_6.4-1+debian11_all.deb          100%[=========================================================================================>]   3.65K  --.-KB/s    in 0s

2024-09-01 21:53:42 (40.8 MB/s) - 'zabbix-release_6.4-1+debian11_all.deb' saved [3740/3740]
```

#CONFIGURATION du fichier (/etc/profile)pour autoriser tous les utilisateurs:
Si vous souhaitez que cette configuration s'applique à tous les utilisateurs, vous pouvez l'ajouter au fichier /etc/profile ou créer un script dans le répertoire /etc/profile.d/.

Ouvrez /etc/profile en tant que superutilisateur avec un éditeur de texte :
sudo nano /etc/profile

Ajoutez la ligne suivante à la fin du fichier :

export PATH=$PATH:/usr/local/sbin:/usr/sbin:/sbin

Sauvegardez et fermez le fichier.

Pour appliquer immédiatement les modifications, soit déconnectez-vous et reconnectez-vous, soit exécutez :
source /etc/profile

Pour vérifier que les répertoires ont bien été ajoutés au PATH, exécutez la commande suivante après avoir appliqué les modifications :
echo $PATH

```
root@debianzab:/home/renman# dpkg -i zabbix-release_6.4-1+debian11_all.deb
dpkg: warning: 'ldconfig' not found in PATH or not executable
dpkg: warning: 'start-stop-daemon' not found in PATH or not executable
dpkg: error: 2 expected programs not found in PATH or not executable
Note: root's PATH should usually contain /usr/local/sbin, /usr/sbin and /sbin
root@debianzab:/home/renman# ls /etc/ |grep profile
profile
profile.d
root@debianzab:/home/renman# nano /etc/profile
root@debianzab:/home/renman# source /etc/profile
root@debianzab:/home/renman# echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/local/sbin:/usr/sbin:/sbin
```

dpkg -i zabbix-release_6.4-1+debian11_all.deb

```
root@debianzab:/home/renman# dpkg -i zabbix-release_6.4-1+debian11_all.deb
Selecting previously unselected package zabbix-release.
(Reading database ... 172490 files and directories currently installed.)
Preparing to unpack zabbix-release_6.4-1+debian11_all.deb ...
Unpacking zabbix-release (1:6.4-1+debian11) ...
Setting up zabbix-release (1:6.4-1+debian11) ...
```

apt update

```
root@debianzab:/home/renman# apt update
Hit:1 http://deb.debian.org/debian bullseye InRelease
Hit:2 http://security.debian.org/debian-security bullseye-security InRelease
Hit:3 http://deb.debian.org/debian bullseye-updates InRelease
Get:4 https://repo.zabbix.com/zabbix/6.4/debian bullseye InRelease [2,880 B]
Get:5 https://repo.zabbix.com/zabbix/6.4/debian bullseye/main Sources [20.8 kB]
Get:6 https://repo.zabbix.com/zabbix/6.4/debian bullseye/main all Packages [11.9 kB]
Get:7 https://repo.zabbix.com/zabbix/6.4/debian bullseye/main amd64 Packages [58.0 kB]
Fetched 93.6 kB in 8s (11.1 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
```

b. Install Zabbix server, frontend, agent:

```
root@debianzab:/home/renman# apt install zabbix-server-mysql zabbix-frontend-php zabbix-nginx-conf zabbix-sql-scripts zabbix-agent
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  fping geoip-database libconfig-inifiles-perl libdbd-mariadb-perl libdbi-perl libevent-core-2.1-7 libevent-pthreads-2.1-7 libgeoip1 libmariadb3 libmodbus5 libnginx-mod-http-geoip
  libnginx-mod-http-image-filter libnginx-mod-http-xslt-filter libnginx-mod-mail libnginx-mod-stream libnginx-mod-stream-geoip libodbc1 libonig5 libopenipmi0 libssh-4 libterm-readkey-perl
  mariadb-client-10.5 mariadb-client-core-10.5 mariadb-common mysql-common nginx nginx-common nginx-core php-bcmath php-common php-fpm php-gd php-ldap php-mbstring php-mysql php-xml
  php7.4-bcmath php7.4-cli php7.4-common php7.4-fpm php7.4-gd php7.4-json php7.4-ldap php7.4-mbstring php7.4-mysql php7.4-opcache php7.4-readline php7.4-xml snmpd
Suggested packages:
  libmldbm-perl libnet-daemon-perl libsql-statement-perl geoip-bin libmyodbc odbc-postgresql tdsodbc unixodbc-bin fcgiwrap nginx-doc php-pear snmptrapd zabbix-apache-conf
  virtual-mysql-server
The following NEW packages will be installed:
  fping geoip-database libconfig-inifiles-perl libdbd-mariadb-perl libdbi-perl libevent-core-2.1-7 libevent-pthreads-2.1-7 libgeoip1 libmariadb3 libmodbus5 libnginx-mod-http-geoip
  libnginx-mod-http-image-filter libnginx-mod-http-xslt-filter libnginx-mod-mail libnginx-mod-stream libnginx-mod-stream-geoip libodbc1 libonig5 libopenipmi0 libssh-4 libterm-readkey-perl
  mariadb-client-10.5 mariadb-client-core-10.5 mariadb-common mysql-common nginx nginx-common nginx-core php-bcmath php-common php-fpm php-gd php-ldap php-mbstring php-mysql php-xml
  php7.4-bcmath php7.4-cli php7.4-common php7.4-fpm php7.4-gd php7.4-json php7.4-ldap php7.4-mbstring php7.4-mysql php7.4-opcache php7.4-readline php7.4-xml snmpd zabbix-agent
  zabbix-frontend-php zabbix-nginx-conf zabbix-server-mysql zabbix-sql-scripts
0 upgraded, 54 newly installed, 0 to remove and 0 not upgraded.
Need to get 33.7 MB of archives.
After this operation, 136 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

```
Setting up php-bcmath (2:7.4+76) ...
Setting up libnginx-mod-http-image-filter (1.18.0-6.1+deb11u3) ...
Setting up libnginx-mod-stream (1.18.0-6.1+deb11u3) ...
Setting up php7.4-mbstring (7.4.33-1+deb11u5) ...

Creating config file /etc/php/7.4/mods-available/mbstring.ini with new version
Setting up libnginx-mod-stream-geoip (1.18.0-6.1+deb11u3) ...
Setting up php7.4-cli (7.4.33-1+deb11u5) ...
update-alternatives: using /usr/bin/php7.4 to provide /usr/bin/php (php) in auto mode
update-alternatives: using /usr/bin/phar7.4 to provide /usr/bin/phar (phar) in auto mode
update-alternatives: using /usr/bin/phar.phar7.4 to provide /usr/bin/phar.phar (phar.phar) in auto mode

Creating config file /etc/php/7.4/cli/php.ini with new version
Setting up php-mbstring (2:7.4+76) ...
Setting up libdbd-mariadb-perl (1.21-3) ...
Setting up php-ldap (2:7.4+76) ...
Setting up libnginx-mod-http-geoip (1.18.0-6.1+deb11u3) ...
Setting up mariadb-client-core-10.5 (1:10.5.23-0+deb11u1) ...
Setting up zabbix-frontend-php (1:6.4.18-1+debian11) ...
update-alternatives: using /usr/share/fonts/truetype/dejavu/DejaVuSans.ttf to provide /usr/share/zabbix/assets/fonts/graphfont.ttf (zabbix-frontend-font) in auto mode
Setting up mariadb-client-10.5 (1:10.5.23-0+deb11u1) ...
Setting up php-gd (2:7.4+76) ...
Setting up nginx-core (1.18.0-6.1+deb11u3) ...
Not attempting to start NGINX, port 80 is already in use.
Setting up php-xml (2:7.4+76) ...
Setting up zabbix-server-mysql (1:6.4.18-1+debian11) ...
Setting up php7.4-fpm (7.4.33-1+deb11u5) ...

Creating config file /etc/php/7.4/fpm/php.ini with new version
NOTICE: Not enabling PHP 7.4 FPM by default.
NOTICE: To enable PHP 7.4 FPM in Apache2 do:
NOTICE: a2enmod proxy_fcgi setenvif
NOTICE: a2enconf php7.4-fpm
NOTICE: You are seeing this message because you have apache2 package installed.
Created symlink /etc/systemd/system/multi-user.target.wants/php7.4-fpm.service → /lib/systemd/system/php7.4-fpm.service.
Setting up nginx (1.18.0-6.1+deb11u3) ...
Setting up zabbix-nginx-conf (1:6.4.18-1+debian11) ...
Setting up php-fpm (2:7.4+76) ...
Processing triggers for man-db (2.9.4-2) ...
Processing triggers for libc-bin (2.31-13+deb11u11) ...
Processing triggers for php7.4-cli (7.4.33-1+deb11u5) ...
Processing triggers for php7.4-fpm (7.4.33-1+deb11u5) ...
NOTICE: Not enabling PHP 7.4 FPM by default.
NOTICE: To enable PHP 7.4 FPM in Apache2 do:
NOTICE: a2enmod proxy_fcgi setenvif
NOTICE: a2enconf php7.4-fpm
NOTICE: You are seeing this message because you have apache2 package installed.
```

c. Create initial database

Documentation

Make sure you have database server up and running.

Run the following on your database host.

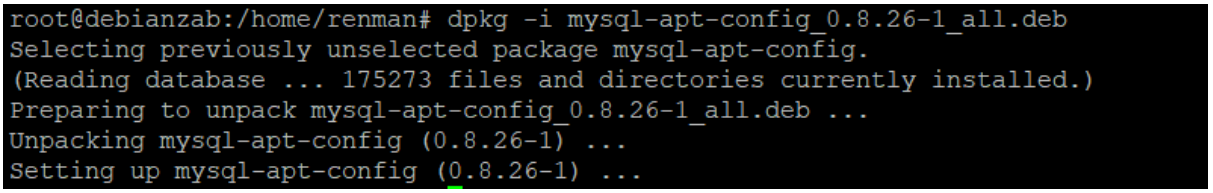
Installation de msql-server

Il est possible que mysql-server ne soit pas disponible dans les dépôts par défaut de votre distribution. Vous pouvez ajouter le dépôt officiel de MySQL à vos sources de paquets :

1. **Téléchargez et ajoutez le dépôt MySQL officiel :**

wget https://dev.mysql.com/get/mysql-apt-config_0.8.26-1_all.deb

sudo dpkg -i mysql-apt-config_0.8.26-1_all.deb



1. Ajouter la clé publique manquante pour le dépôt MySQL
Comme la commande apt-key est désormais dépréciée sur les systèmes plus récents, y compris Debian 11, la méthode recommandée consiste à ajouter la clé directement à /usr/share/keyrings/ et à l'associer au dépôt.

a. Télécharger et ajouter la clé GPG
Téléchargez la clé publique du dépôt MySQL :
wget https://repo.mysql.com/RPM-GPG-KEY-mysql-2022

Convertissez-la en un format utilisable par apt et déplacez-la dans le répertoire des clés :
sudo gpg --dearmor -o /usr/share/keyrings/mysql.gpg RPM-GPG-KEY-mysql-2022

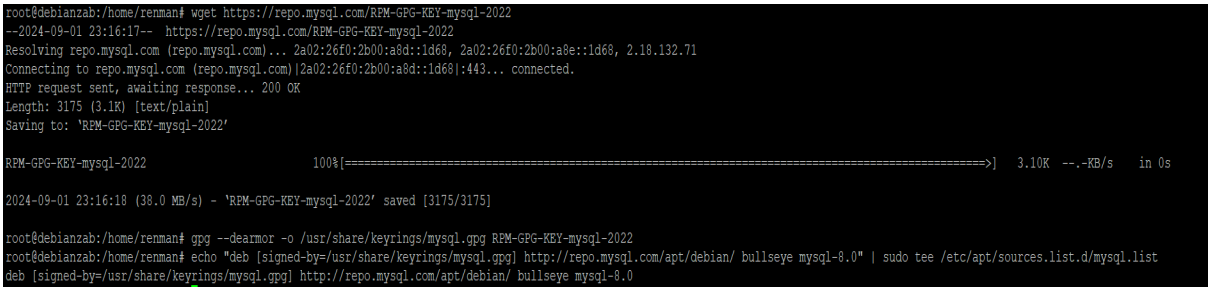
b. Configurer le dépôt MySQL avec la clé GPG

1. **Modifiez le fichier de configuration du dépôt MySQL pour qu'il utilise la clé que vous avez ajoutée. Si vous avez déjà ajouté le dépôt, modifiez-le pour utiliser l'option signed-by :**

echo "deb [signed-by=/usr/share/keyrings/mysql.gpg] http://repo.mysql.com/apt/debian/ bullseye mysql-8.0" | sudo tee /etc/apt/sources.list.d/mysql.list

Cette commande ajoute ou modifie la configuration du dépôt pour Debian 11 en spécifiant la clé GPG à utiliser pour vérifier les paquets.

Après avoir configuré le dépôt avec la clé correcte, mettez à jour la liste des paquets :



sudo apt install mysql-server

On Zabbix server host import initial schema and data. You will be prompted to enter your newly created password.
 # zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql --default-character-set=utf8mb4 -uzabbix -p zabbix

c. Create initial database
Documentation
Make sure you have database server up and running.

Run the following on your database host.

 # mysql -uroot -p
password
mysql> create database zabbix character set utf8mb4 collate utf8mb4_bin;
mysql> create user zabbix@localhost identified by 'password';
mysql> grant all privileges on zabbix.* to zabbix@localhost;
mysql> set global log_bin_trust_function_creators = 1;
mysql> quit;
On Zabbix server host import initial schema and data. You will be prompted to enter your newly created password.

 # zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql --default-character-set=utf8mb4 -uzabbix -p zabbix
Disable log_bin_trust_function_creators option after importing database schema.

```
# mysql -uroot -p
password
mysql> set global log_bin_trust_function_creators = 0;
mysql> quit;
```

d. Configure the database for Zabbix server

Edit file /etc/zabbix/zabbix_server.conf

```
DBPassword=password
```

e. Configure PHP for Zabbix frontend

Edit file /etc/zabbix/nginx.conf uncomment and set 'listen' and 'server_name' directives.

```
# listen 8080;
# server_name example.com;
```

f. Start Zabbix server and agent processes

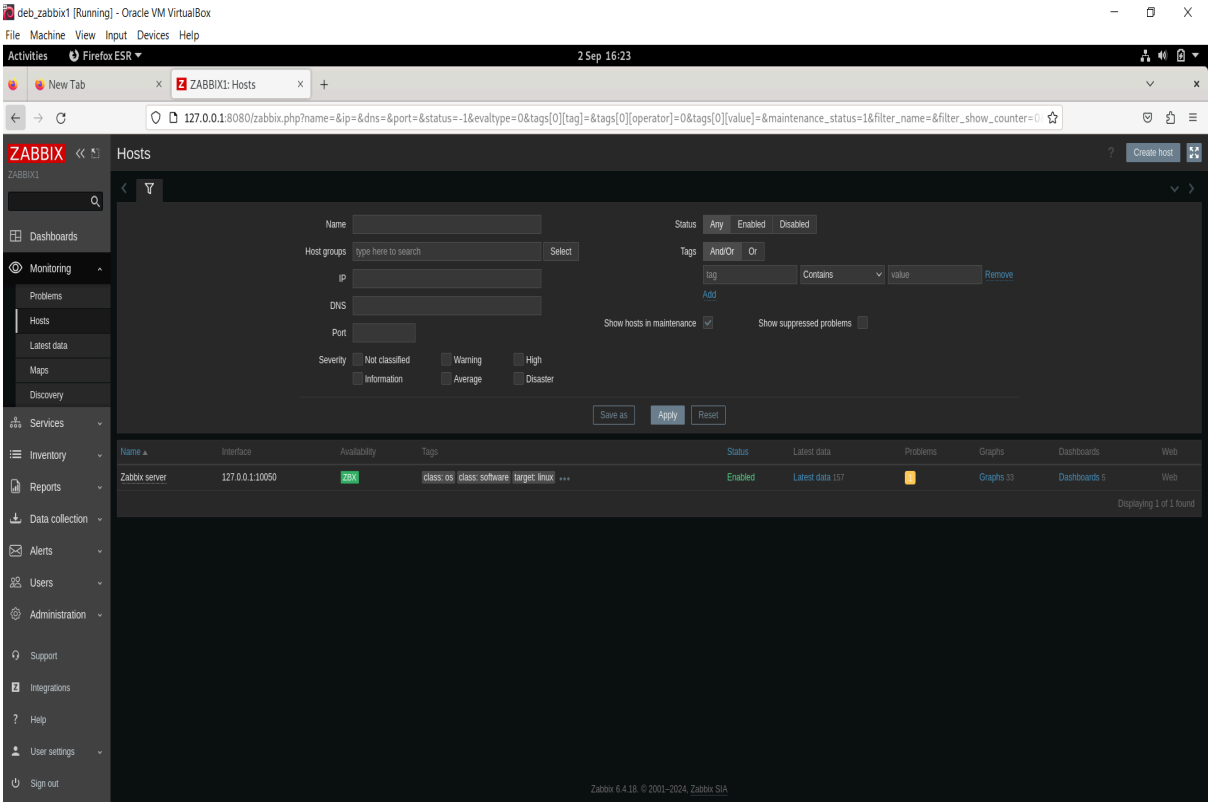
Start Zabbix server and agent processes and make it start at system boot.

```
# systemctl restart zabbix-server zabbix-agent nginx php7.4-fpm
# systemctl enable zabbix-server zabbix-agent nginx php7.4-fpm
```

g. Open Zabbix UI web page

The URL for Zabbix UI when using Nginx depends on the configuration changes you should have made.

#interface graphique de zabbix:



Installation de zabbix agent:

wget
https://repo.zabbix.com/zabbix/6.4/debian/pool/main/z/zabbix-release/zabbix-release_6.4-1+debian12_all.deb

```
root@debian3:/home/renman# wget https://repo.zabbix.com/zabbix/6.4/debian/pool/main/z/zabbix-release/zabbix-release_6.4-1+debian12_all.deb
--2024-09-02 16:16:28--  https://repo.zabbix.com/zabbix/6.4/debian/pool/main/z/zabbix-release/zabbix-release_6.4-1+debian12_all.deb
Resolving repo.zabbix.com (repo.zabbix.com)... 178.128.6.101, 2604:a880:2:d0::2062:d001
Connecting to repo.zabbix.com (repo.zabbix.com)|178.128.6.101|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3540 (3.5K) [application/octet-stream]
Saving to: 'zabbix-release_6.4-1+debian12_all.deb'

zabbix-release_6.4-1+debian12_all.deb          100%[=========================================================================================>]   3.46K  --.-KB/s    in 0s

2024-09-02 16:16:29 (23.3 MB/s) - 'zabbix-release_6.4-1+debian12_all.deb' saved [3540/3540]

root@debian3:/home/renman# ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos  zabbix-release_6.4-1+debian12_all.deb
```

sudo dpkg -i zabbix-release_6.4-1+debian12_all.deb

```
root@debian3:/home/renman# dpkg -i zabbix-release_6.4-1+debian12_all.deb
Selecting previously unselected package zabbix-release.
(Reading database ... 177518 files and directories currently installed.)
Preparing to unpack zabbix-release_6.4-1+debian12_all.deb ...
Unpacking zabbix-release (1:6.4-1+debian12) ...
Setting up zabbix-release (1:6.4-1+debian12) ...
```

sudo apt update

```
root@debian3:/home/renman# apt update
Get:1 http://security.debian.org/debian-security bookworm-security InRelease [48.0 kB]
Hit:2 http://deb.debian.org/debian bookworm InRelease
Hit:3 http://deb.debian.org/debian bookworm-updates InRelease
Get:4 https://repo.zabbix.com/zabbix/6.4/debian bookworm InRelease [2,880 B]
Get:5 https://repo.zabbix.com/zabbix/6.4/debian bookworm/main Sources [18.7 kB]
Get:6 https://repo.zabbix.com/zabbix/6.4/debian bookworm/main amd64 Packages [49.7 kB]
Get:7 https://repo.zabbix.com/zabbix/6.4/debian bookworm/main all Packages [10.3 kB]
Fetched 129 kB in 3s (39.8 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
114 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

2. Installer Zabbix Agent
Ensuite, installez Zabbix Agent à l'aide du gestionnaire de paquets apt :

```
root@debian3:/home/renman# apt install zabbix-agent
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libmodbus5
The following NEW packages will be installed:
  libmodbus5 zabbix-agent
0 upgraded, 2 newly installed, 0 to remove and 114 not upgraded.
Need to get 723 kB of archives.
After this operation, 1,226 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://deb.debian.org/debian bookworm/main amd64 libmodbus5 amd64 3.1.6-2.1 [31.3 kB]
Get:2 https://repo.zabbix.com/zabbix/6.4/debian bookworm/main amd64 zabbix-agent amd64 1:6.4.18-1+debian12 [691 kB]
Fetched 723 kB in 2s (404 kB/s)
Selecting previously unselected package libmodbus5:amd64.
(Reading database ... 177524 files and directories currently installed.)
Preparing to unpack .../libmodbus5_3.1.6-2.1_amd64.deb ...
Unpacking libmodbus5:amd64 (3.1.6-2.1) ...
Selecting previously unselected package zabbix-agent.
Preparing to unpack .../zabbix-agent_1%3a6.4.18-1+debian12_amd64.deb ...
Unpacking zabbix-agent (1:6.4.18-1+debian12) ...
Setting up libmodbus5:amd64 (3.1.6-2.1) ...
Setting up zabbix-agent (1:6.4.18-1+debian12) ...
Created symlink /etc/systemd/system/multi-user.target.wants/zabbix-agent.service → /lib/systemd/system/zabbix-agent.service.
Processing triggers for man-db (2.11.2-2) ...
Processing triggers for libc-bin (2.36-9+deb12u7) ...
```

```
root@debian3:/home/renman# systemctl status zabbix-agent
● zabbix-agent.service - Zabbix Agent
     Loaded: loaded (/lib/systemd/system/zabbix-agent.service; enabled; preset: enabled)
     Active: active (running) since Mon 2024-09-02 16:30:34 CEST; 5min ago
    Process: 4871 ExecStart=/usr/sbin/zabbix_agentd -c $CONFFILE (code=exited, status=0/SUCCESS)
   Main PID: 4873 (zabbix_agentd)
      Tasks: 6 (limit: 1074)
     Memory: 5.8M
        CPU: 148ms
     CGroup: /system.slice/zabbix-agent.service
             ├─4873 /usr/sbin/zabbix_agentd -c /etc/zabbix/zabbix_agentd.conf
             ├─4874 "/usr/sbin/zabbix_agentd: collector [idle 1 sec]"
             ├─4875 "/usr/sbin/zabbix_agentd: listener #1 [waiting for connection]"
             ├─4876 "/usr/sbin/zabbix_agentd: listener #2 [waiting for connection]"
             ├─4877 "/usr/sbin/zabbix_agentd: listener #3 [waiting for connection]"
             └─4878 "/usr/sbin/zabbix_agentd: active checks #1 [idle 1 sec]"

Sep 02 16:30:33 debian3 systemd[1]: Starting zabbix-agent.service - Zabbix Agent...
Sep 02 16:30:34 debian3 systemd[1]: Started zabbix-agent.service - Zabbix Agent.
```

3. Configurer Zabbix Agent
Une fois installé, vous devez configurer Zabbix Agent pour qu'il puisse communiquer avec le serveur Zabbix.

Éditez le fichier de configuration /etc/zabbix/zabbix_agentd.conf :

sudo nano /etc/zabbix/zabbix_agentd.conf

Trouvez et modifiez les lignes suivantes selon votre environnement :

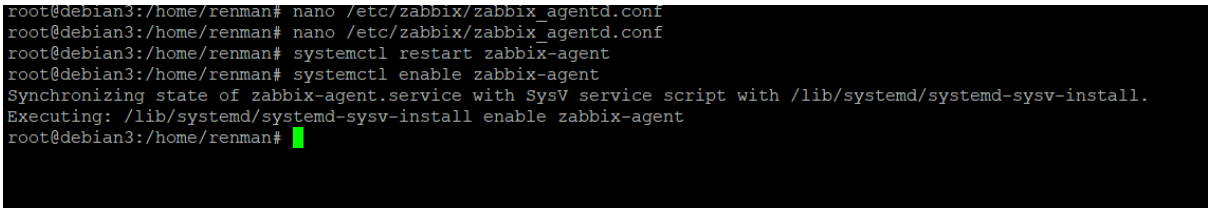
Server= : Remplacez 127.0.0.1 par l'adresse IP ou le nom de domaine de votre serveur Zabbix.

Server=IP_DU_SERVEUR_ZABBIX
ServerActive= : Mettez l'adresse IP ou le nom de domaine de votre serveur Zabbix, pour que l'agent puisse envoyer des données au serveur.

ServerActive=IP_DU_SERVEUR_ZABBIX
Hostname= : Remplacez Zabbix server par le nom d'hôte unique de votre machine (doit correspondre au nom configuré sur le serveur Zabbix).

Hostname=nom_du_client
4. Démarrer et activer le service Zabbix Agent
Après avoir configuré l'agent, démarrez le service et assurez-vous qu'il s'exécute au démarrage du système :

sudo systemctl restart zabbix-agent
sudo systemctl enable zabbix-agent



5. Vérifier le statut du service
Pour vous assurer que l'agent fonctionne correctement, vous pouvez vérifier l'état du service :

sudo systemctl status zabbix-agent

Vous devriez voir quelque chose comme "active (running)".

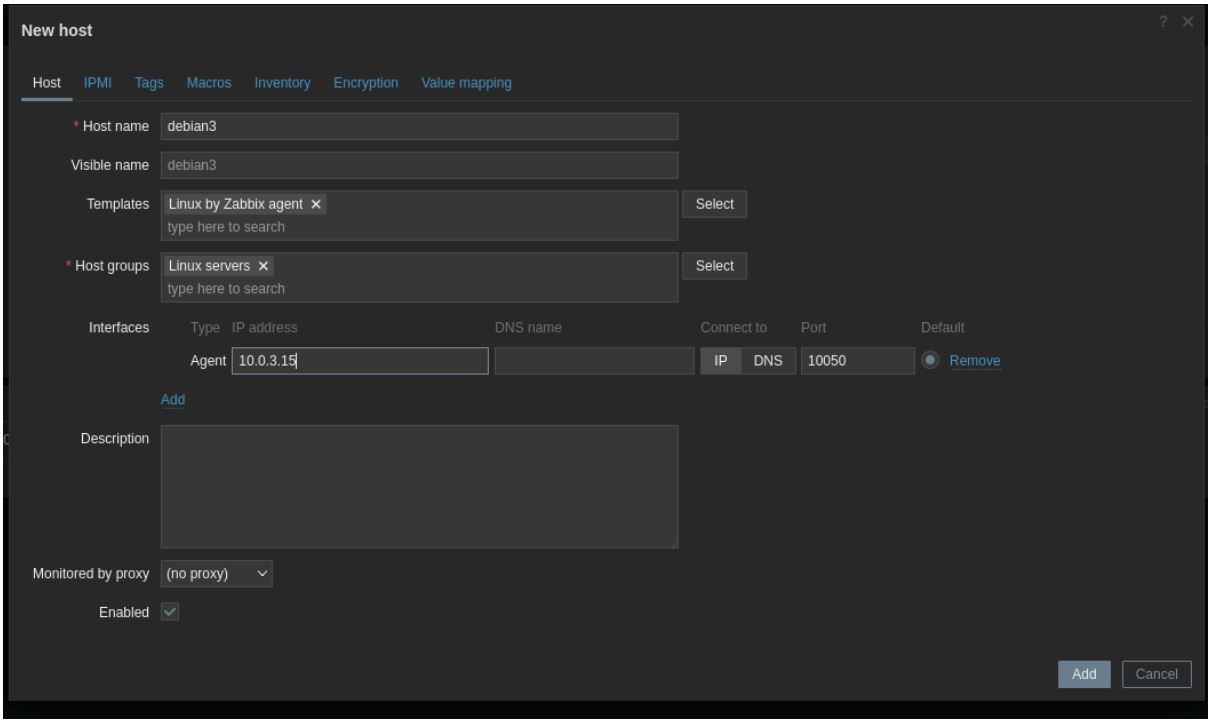
```
root@debian3:/home/renman# systemctl status zabbix-agent
● zabbix-agent.service - Zabbix Agent
     Loaded: loaded (/lib/systemd/system/zabbix-agent.service; enabled; preset: enabled)
     Active: active (running) since Mon 2024-09-02 17:13:10 CEST; 1min 51s ago
   Main PID: 6216 (zabbix_agentd)
      Tasks: 5 (limit: 1074)
     Memory: 4.1M
        CPU: 83ms
     CGroup: /system.slice/zabbix-agent.service
             ├─6216 /usr/sbin/zabbix_agentd -c /etc/zabbix/zabbix_agentd.conf
             ├─6217 "/usr/sbin/zabbix_agentd: collector [idle 1 sec]"
             ├─6218 "/usr/sbin/zabbix_agentd: listener #1 [waiting for connection]"
             ├─6219 "/usr/sbin/zabbix_agentd: listener #2 [waiting for connection]"
             └─6220 "/usr/sbin/zabbix_agentd: listener #3 [waiting for connection]"

Sep 02 17:13:10 debian3 systemd[1]: Starting zabbix-agent.service - Zabbix Agent...
Sep 02 17:13:10 debian3 systemd[1]: Started zabbix-agent.service - Zabbix Agent.
root@debian3:/home/renman#
```

Consultation des logs:

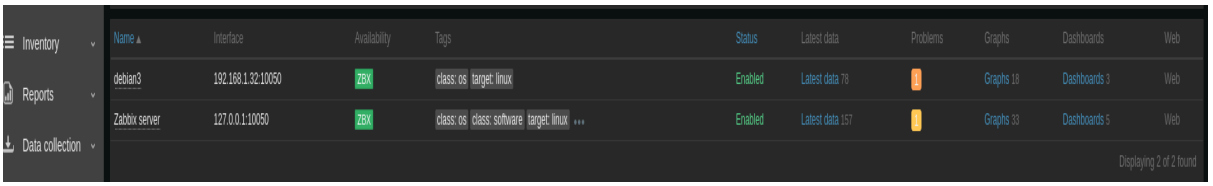
tail -f /var/log/zabbix/zabbix_agentd.conf

```
root@debian3:/home/renman# tail -f /var/log/zabbix/zabbix_agentd.log
  6216:20240902:171310.636 **** Enabled features ****
  6216:20240902:171310.636 IPv6 support:          YES
  6216:20240902:171310.636 TLS support:           YES
  6216:20240902:171310.636 **************************
  6216:20240902:171310.636 using configuration file: /etc/zabbix/zabbix_agentd.conf
  6216:20240902:171310.659 agent #0 started [main process]
  6218:20240902:171310.663 agent #2 started [listener #1]
  6217:20240902:171310.666 agent #1 started [collector]
  6219:20240902:171310.666 agent #3 started [listener #2]
  6220:20240902:171310.670 agent #4 started [listener #3]
```

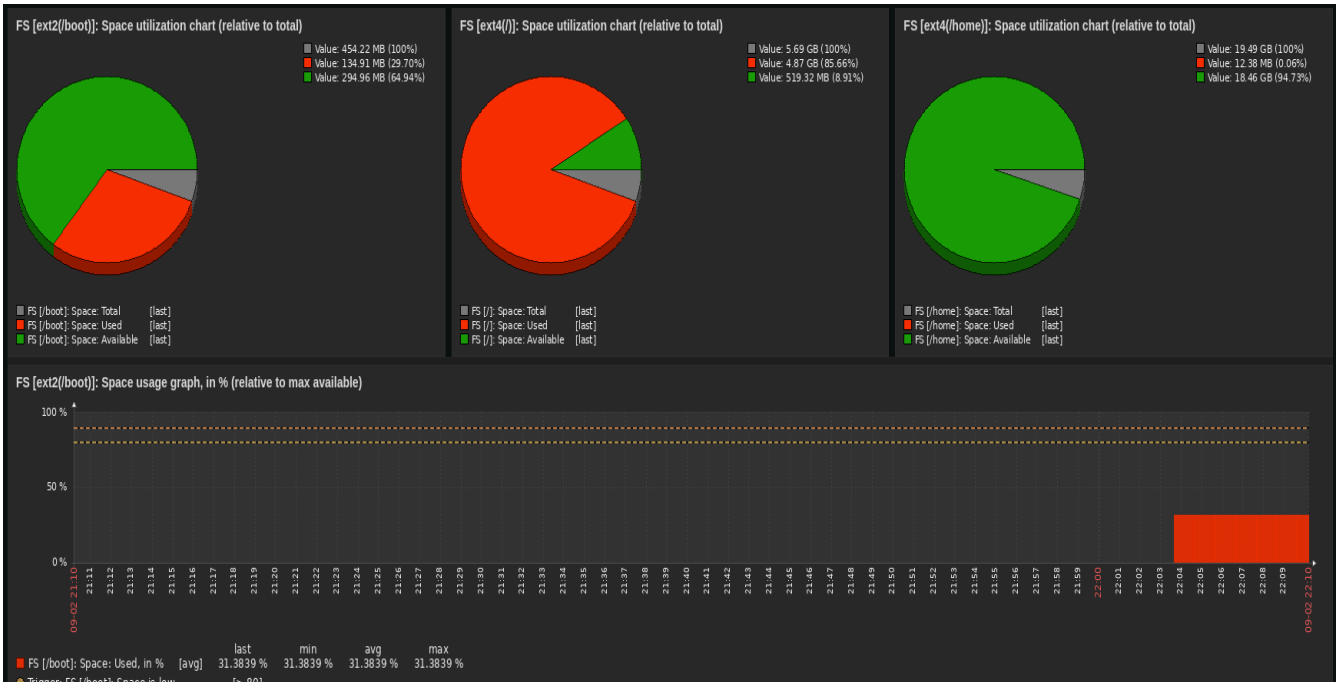
Configurer l'hôte sur le serveur Zabbix:



Affichage des agents zabbix sur l'interface graphique de zabbix:



Affichage des systemes de fichiers



INSTALLATION DE PROMETHEUS SUR DEBIAN11

1. Add a new system user
add a group called Prometheus:

groupadd --system prometheus

add a user and assign it to the group created above with no login rights.

useradd -s /sbin/nologin --system -g prometheus prometheus

```
root@debianzab:/home/renman# groupadd --system prometheus
root@debianzab:/home/renman# useradd -s /sbin/nologin --system -g prometheus prometheus
root@debianzab:/home/renman#
```

2. Create a user directory for Prometheus

mkdir /etc/prometheus

mkdir /var/lib/prometheus

```
root@debianzab:/home/renman# mkdir /etc/prometheus
root@debianzab:/home/renman# mkdir /var/lib/prometheus
root@debianzab:/home/renman#
```

3. Download Prometheus Monitoring

For the latest version, you can visit its website download page. or use the command line method:
wget
https://github.com/prometheus/prometheus/releases/download/v2.54.1/prometheus-2.54.1.linux-amd64.tar.gz

```
root@debianzab:/tmp# wget https://github.com/prometheus/prometheus/releases/download/v2.54.1/prometheus-2.54.1.linux-amd64.tar.gz
--2024-09-03 01:48:06--  https://github.com/prometheus/prometheus/releases/download/v2.54.1/prometheus-2.54.1.linux-amd64.tar.gz
Resolving github.com (github.com)... 140.82.121.4
Connecting to github.com (github.com)|140.82.121.4|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://objects.githubusercontent.com/github-production-release-asset-2e65be/6838921/04e495b6-6719-4ec2-b374-4f31fac8dd23?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=releaseassetproduction%2F20240902%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20240902T234806Z&X-Amz-Expires=300&X-Amz-Signature=03192b4f551ce9b57f47ef587cbe654cfac3228be0a03e5027d5d8d0322cc621&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=6838921&response-content-disposition=attachment%3B%20filename%3Dprometheus-2.54.1.linux-amd64.tar.gz&response-content-type=application%2Foctet-stream [following]
--2024-09-03 01:48:07--  https://objects.githubusercontent.com/github-production-release-asset-2e65be/6838921/04e495b6-6719-4ec2-b374-4f31fac8dd23?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=releaseassetproduction%2F20240902%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20240902T234806Z&X-Amz-Expires=300&X-Amz-Signature=03192b4f551ce9b57f47ef587cbe654cfac3228be0a03e5027d5d8d0322cc621&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=6838921&response-content-disposition=attachment%3B%20filename%3Dprometheus-2.54.1.linux-amd64.tar.gz&response-content-type=application%2Foctet-stream
Resolving objects.githubusercontent.com (objects.githubusercontent.com)... 185.199.109.133, 185.199.108.133, 185.199.111.133, ...
Connecting to objects.githubusercontent.com (objects.githubusercontent.com)|185.199.109.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 105689699 (101M) [application/octet-stream]
Saving to: 'prometheus-2.54.1.linux-amd64.tar.gz'

prometheus-2.54.1.linux-amd64.tar.gz          100%[=============================================================================================>] 100.79M  20.0MB/s    in 7.0s

2024-09-03 01:48:14 (14.4 MB/s) - 'prometheus-2.54.1.linux-amd64.tar.gz' saved [105689699/105689699]
```

3. Extraire l'archive
Extrayez le contenu du fichier tar.gz téléchargé.

tar -xvf prometheus-2.54.1.linux-amd64.tar.gz
cd prometheus-2.54.1.linux-amd64

```
root@debianzab:/tmp# tar -xvf prometheus-*.linux-amd64.tar.gz
prometheus-2.54.1.linux-amd64/
prometheus-2.54.1.linux-amd64/NOTICE
prometheus-2.54.1.linux-amd64/LICENSE
prometheus-2.54.1.linux-amd64/prometheus.yml
prometheus-2.54.1.linux-amd64/prometheus
prometheus-2.54.1.linux-amd64/consoles/
prometheus-2.54.1.linux-amd64/consoles/prometheus-overview.html
prometheus-2.54.1.linux-amd64/consoles/node-overview.html
prometheus-2.54.1.linux-amd64/consoles/index.html.example
prometheus-2.54.1.linux-amd64/consoles/node.html
prometheus-2.54.1.linux-amd64/consoles/node-disk.html
prometheus-2.54.1.linux-amd64/consoles/prometheus.html
prometheus-2.54.1.linux-amd64/consoles/node-cpu.html
prometheus-2.54.1.linux-amd64/promtool
prometheus-2.54.1.linux-amd64/console_libraries/
prometheus-2.54.1.linux-amd64/console_libraries/menu.lib
prometheus-2.54.1.linux-amd64/console_libraries/prom.lib
root@debianzab:/tmp# cd prometheus-*.linux-amd64
root@debianzab:/tmp/prometheus-2.54.1.linux-amd64#
```

4. Déplacer les fichiers binaires

Déplacez les fichiers binaires Prometheus et promtool dans le répertoire **/usr/local/bin** pour les rendre accessibles globalement:

sudo mv prometheus /usr/local/bin/
sudo mv promtool /usr/local/bin/

```
root@debianzab:/tmp/prometheus-2.54.1.linux-amd64/prometheus-2.54.1.linux-amd64# mv prometheus /usr/local/bin/
root@debianzab:/tmp/prometheus-2.54.1.linux-amd64/prometheus-2.54.1.linux-amd64# mv promtool /usr/local/bin/
root@debianzab:/tmp/prometheus-2.54.1.linux-amd64/prometheus-2.54.1.linux-amd64#
```

5. Configurer les répertoires et permissions

Créez les répertoires nécessaires pour les fichiers de configuration et de données de Prometheus, puis ajustez les permissions:

sudo chown prometheus:prometheus /var/lib/prometheus

sudo mv consoles /etc/prometheus/

sudo mv console_libraries /etc/prometheus/

sudo mv prometheus.yml /etc/prometheus/

sudo chown -R prometheus:prometheus /etc/prometheus/

```
root@debianzab:/tmp/prometheus-2.54.1.linux-amd64/prometheus-2.54.1.linux-amd64# chown prometheus:prometheus /var/lib/prometheus
root@debianzab:/tmp/prometheus-2.54.1.linux-amd64/prometheus-2.54.1.linux-amd64# mv consoles /etc/prometheus/
root@debianzab:/tmp/prometheus-2.54.1.linux-amd64/prometheus-2.54.1.linux-amd64# mv console_libraries /etc/prometheus/
root@debianzab:/tmp/prometheus-2.54.1.linux-amd64/prometheus-2.54.1.linux-amd64# mv prometheus.yml /etc/prometheus/
root@debianzab:/tmp/prometheus-2.54.1.linux-amd64/prometheus-2.54.1.linux-amd64# chown -R prometheus:prometheus /etc/prometheus/
root@debianzab:/tmp/prometheus-2.54.1.linux-amd64/prometheus-2.54.1.linux-amd64#
```

6. Créer un fichier de service systemd

Pour gérer Prometheus via systemd, créez un fichier de service:

sudo nano /etc/systemd/system/prometheus.service

contenu de ce fichier:

```
[Unit]
Description=Prometheus
Wants=network-online.target
After=network-online.target

[Service]
User=prometheus
Group=prometheus
Type=simple
ExecStart=/usr/local/bin/prometheus \
  --config.file /etc/prometheus/prometheus.yml \
  --storage.tsdb.path /var/lib/prometheus/ \
  --web.console.templates=/etc/prometheus/consoles \
  --web.console.libraries=/etc/prometheus/console_libraries

[Install]
WantedBy=multi-user.target
```

```
[Unit]
Description=Prometheus
Wants=network-online.target
After=network-online.target

[Service]
User=prometheus
Group=prometheus
Type=simple
ExecStart=/usr/local/bin/prometheus \
  --config.file /etc/prometheus/prometheus.yml \
  --storage.tsdb.path /var/lib/prometheus/ \
  --web.console.templates=/etc/prometheus/consoles \
  --web.console.libraries=/etc/prometheus/console_libraries

[Install]
WantedBy=multi-user.target
```

7. Démarrer et activer Prometheus

Rechargez systemd pour prendre en compte le nouveau service, puis démarrez Prometheus et configurez-le pour qu'il démarre automatiquement au démarrage du système:

sudo systemctl daemon-reload

sudo systemctl start prometheus

sudo systemctl enable prometheus

8. Vérifier l'installation

Pour vérifier que Prometheus fonctionne correctement, utilisez la commande suivante :

sudo systemctl status prometheus

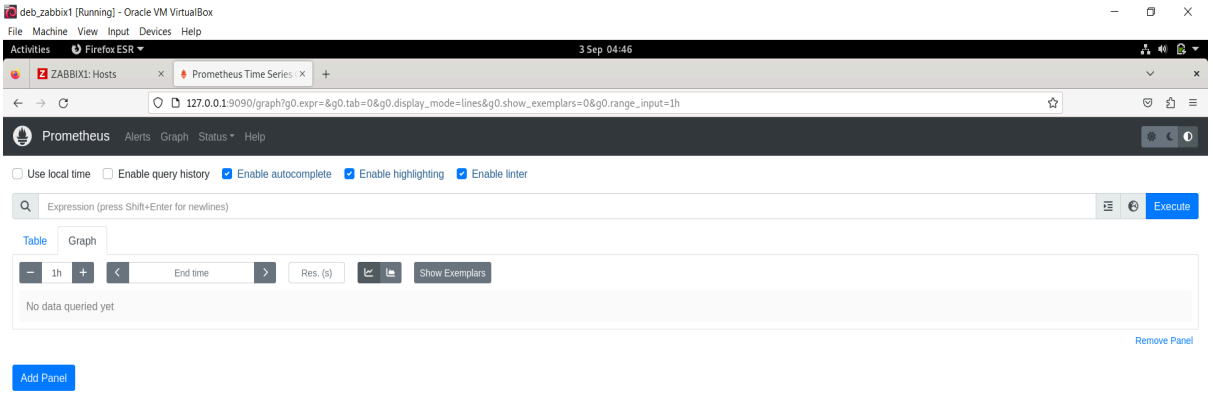
```
root@debianzab:/tmp/prometheus-2.54.1.linux-amd64/prometheus-2.54.1.linux-amd64# systemctl daemon-reload
root@debianzab:/tmp/prometheus-2.54.1.linux-amd64/prometheus-2.54.1.linux-amd64# systemctl start prometheus
root@debianzab:/tmp/prometheus-2.54.1.linux-amd64/prometheus-2.54.1.linux-amd64# systemctl enable prometheus
Created symlink /etc/systemd/system/multi-user.target.wants/prometheus.service → /etc/systemd/system/prometheus.service.
root@debianzab:/tmp/prometheus-2.54.1.linux-amd64/prometheus-2.54.1.linux-amd64# systemctl status prometheus
● prometheus.service - Prometheus
     Loaded: loaded (/etc/systemd/system/prometheus.service; enabled; vendor preset: enabled)
     Active: active (running) since Tue 2024-09-03 04:33:18 CEST; 31s ago
   Main PID: 6920 (prometheus)
      Tasks: 8 (limit: 4641)
     Memory: 20.7M
        CPU: 229ms
     CGroup: /system.slice/prometheus.service
             └─6920 /usr/local/bin/prometheus --config.file /etc/prometheus/prometheus.yml --storage.tsdb.path /var/lib/prometheus/ --web.console.templates=/etc/prometheus/consoles --web.c>

Sep 03 04:33:18 debianzab prometheus[6920]: ts=2024-09-03T02:33:18.314Z caller=head.go:721 level=info component=tsdb msg="Replaying WAL, this may take a while"
Sep 03 04:33:18 debianzab prometheus[6920]: ts=2024-09-03T02:33:18.314Z caller=head.go:793 level=info component=tsdb msg="WAL segment loaded" segment=0 maxSegment=0
Sep 03 04:33:18 debianzab prometheus[6920]: ts=2024-09-03T02:33:18.314Z caller=head.go:830 level=info component=tsdb msg="WAL replay completed" checkpoint_replay_duration=87.092µs wal_repl>
Sep 03 04:33:18 debianzab prometheus[6920]: ts=2024-09-03T02:33:18.323Z caller=main.go:1181 level=info fs_type=EXT4_SUPER_MAGIC
Sep 03 04:33:18 debianzab prometheus[6920]: ts=2024-09-03T02:33:18.323Z caller=main.go:1184 level=info msg="TSDB started"
Sep 03 04:33:18 debianzab prometheus[6920]: ts=2024-09-03T02:33:18.324Z caller=main.go:1367 level=info msg="Loading configuration file" filename=/etc/prometheus/prometheus.yml
Sep 03 04:33:18 debianzab prometheus[6920]: ts=2024-09-03T02:33:18.325Z caller=main.go:1404 level=info msg="updated GOGC" old=100 new=75
Sep 03 04:33:18 debianzab prometheus[6920]: ts=2024-09-03T02:33:18.325Z caller=main.go:1415 level=info msg="Completed loading of configuration file" filename=/etc/prometheus/prometheus.yml>
Sep 03 04:33:18 debianzab prometheus[6920]: ts=2024-09-03T02:33:18.325Z caller=main.go:1145 level=info msg="Server is ready to receive web requests."
Sep 03 04:33:18 debianzab prometheus[6920]: ts=2024-09-03T02:33:18.325Z caller=manager.go:164 level=info component="rule manager" msg="Starting rule manager..."
lines 1-20/20 (END)
```

7. Access web interface

Point to http://server-ip-address:9090

Note: Replace, server-ip-addresswith the actual Ip-address of your Server. Also, make sure the 9090 is open in the firewall:

sudo ufw allow 9090



Étape 1: Installation de Grafana sur Debian

1.1. Ajouter le dépôt APT de Grafana

Ajoutez le dépôt officiel de Grafana à votre système pour que vous puissiez installer la dernière version stable.

sudo apt-get install -y software-properties-common

sudo add-apt-repository "deb https://packages.grafana.com/oss/deb stable main"

```
root@debianzab:/home/renman# apt-get install -y software-properties-common
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
software-properties-common is already the newest version (0.96.20.2-2.1).
software-properties-common set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 14 not upgraded.
root@debianzab:/home/renman# add-apt-repository "deb https://packages.grafana.com/oss/deb stable main"
root@debianzab:/home/renman#
```

Ajoutez la clé GPG pour le dépôt :

wget -q -O - https://packages.grafana.com/gpg.key | sudo apt-key add -

```
root@debianzab:/home/renman# wget -q -O - https://packages.grafana.com/gpg.key | sudo apt-key add -
Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).
OK
root@debianzab:/home/renman#
```

1.2. Mettre à jour les dépôts et installer Grafana

Mettez à jour votre liste de paquets et installez Grafana :

sudo apt-get update

sudo apt-get install grafana

```
root@debianzab:/home/renman# apt-get install grafana
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  musl
The following NEW packages will be installed:
  grafana musl
0 upgraded, 2 newly installed, 0 to remove and 14 not upgraded.
Need to get 123 MB of archives.
After this operation, 464 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://deb.debian.org/debian bullseye/main amd64 musl amd64 1.2.2-1 [418 kB]
Get:2 https://packages.grafana.com/oss/deb stable/main amd64 grafana amd64 11.2.0 [123 MB]
Fetched 123 MB in 17s (7,111 kB/s)
Selecting previously unselected package musl:amd64.
(Reading database ... 181556 files and directories currently installed.)
Preparing to unpack .../musl_1.2.2-1_amd64.deb ...
Unpacking musl:amd64 (1.2.2-1) ...
Selecting previously unselected package grafana.
Preparing to unpack .../grafana_11.2.0_amd64.deb ...
Unpacking grafana (11.2.0) ...
Setting up musl:amd64 (1.2.2-1) ...
Setting up grafana (11.2.0) ...
Adding system user `grafana' (UID 121) ...
Adding new user `grafana' (UID 121) with group `grafana' ...
Not creating home directory `/usr/share/grafana'.
### NOT starting on installation, please execute the following statements to configure grafana to start automatically using systemd
 sudo /bin/systemctl daemon-reload
 sudo /bin/systemctl enable grafana-server
### You can start grafana-server by executing
 sudo /bin/systemctl start grafana-server
Processing triggers for man-db (2.9.4-2) ...
root@debianzab:/home/renman#
```

1.3. Démarrer et activer le service Grafana

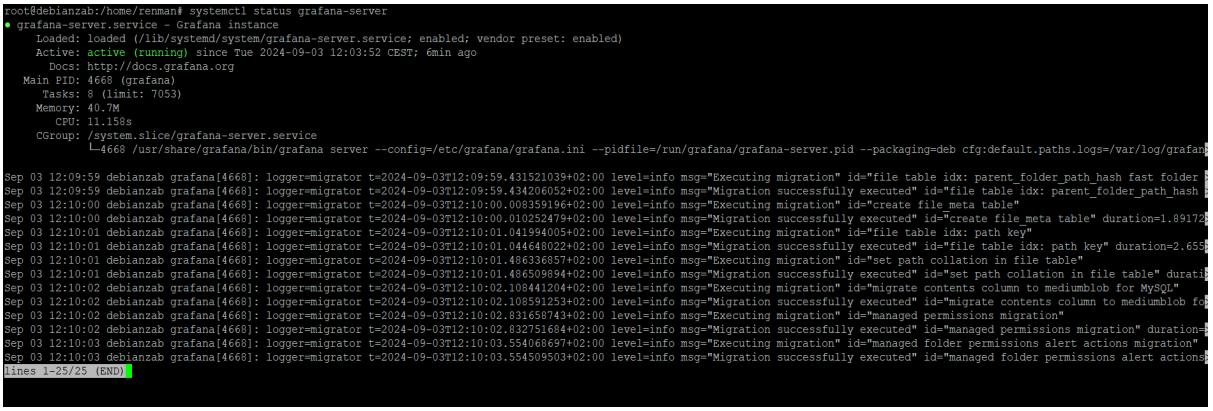
Démarrez Grafana et configurez-le pour qu'il démarre automatiquement au démarrage du système :

sudo systemctl start grafana-server

sudo systemctl enable grafana-server

```
root@debianzab:/home/renman# systemctl start grafana-server
root@debianzab:/home/renman# systemctl enable grafana-server
Synchronizing state of grafana-server.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable grafana-server
Created symlink /etc/systemd/system/multi-user.target.wants/grafana-server.service → /lib/systemd/system/grafana-server.service.
root@debianzab:/home/renman#
```

Affichage de l’Etat de grafana



1.4. Accéder à l'interface web de Grafana

Ouvrez un navigateur et accédez à Grafana à l'adresse http://<IP_DE_VOTRE_SERVEUR>:3000. Par défaut, le port est 3000.

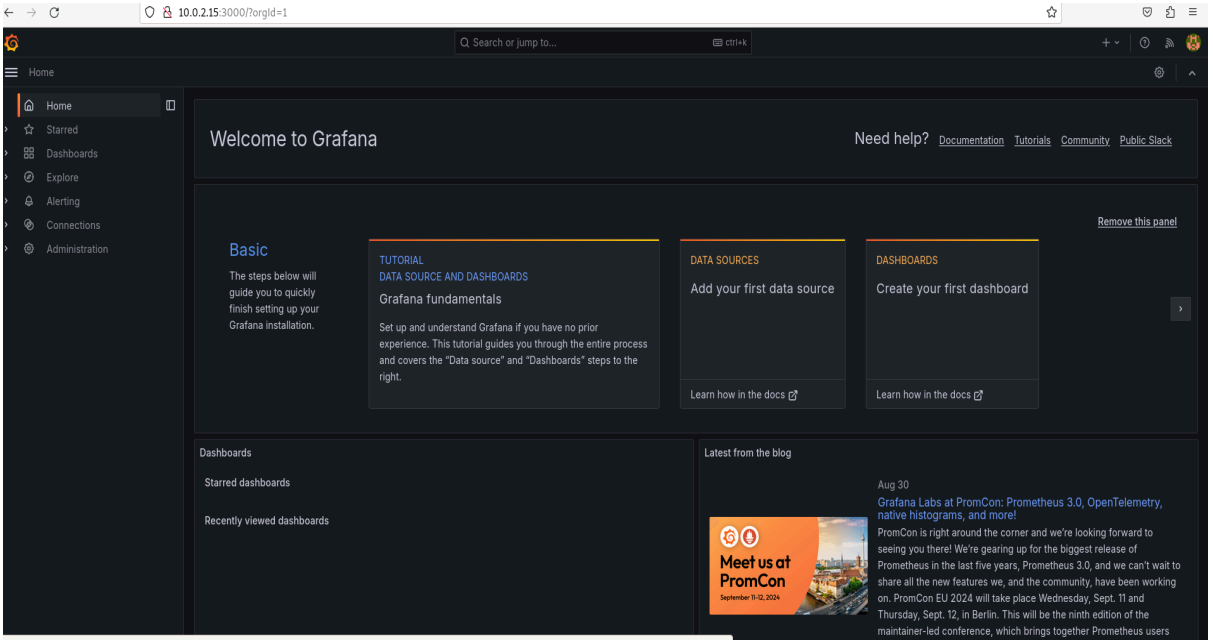
Identifiants par défaut :

Nom d'utilisateur: admin

Mot de passe: admin

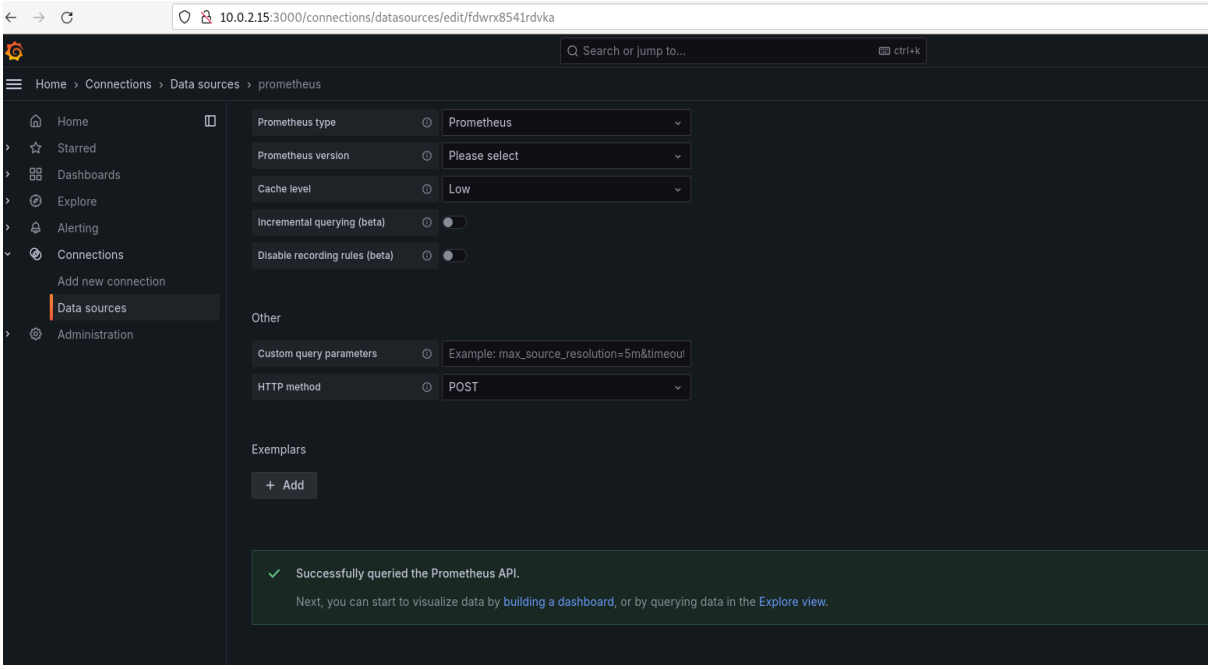
Lors de votre première connexion, Grafana vous demandera de changer le mot de passe administrateur.

Affichage graphique de grafana



Étape 2: Intégration Prometheus-Grafana
2.1. Ajouter Prometheus comme source de données dans Grafana
Connectez-vous à Grafana.
Cliquez sur l'icône de configuration (engrenage) dans la barre latérale, puis sur "Data Sources".
Cliquez sur "Add data source".
Dans la liste des sources de données disponibles, sélectionnez "Prometheus".
Configurez Prometheus :
URL : Entrez l'URL de votre instance Prometheus. Si Prometheus est sur le même serveur que Grafana, l'URL est souvent http://localhost:9090.
Laissez les autres paramètres par défaut.
Cliquez sur "Save & Test" pour vérifier que Grafana peut se connecter à Prometheus.

Si la connexion est réussie, vous verrez un message confirmant que Grafana est bien connecté à Prometheus.



Étape 3: Créer des tableaux de bord pour visualiser les données de Prometheus
3.1. Créer un nouveau tableau de bord
Cliquez sur l'icône "+" dans la barre latérale, puis sur "Create Dashboard".
Cliquez sur "Add new panel" pour ajouter un panneau à votre tableau de bord.
3.2. Configurer un panneau avec des données Prometheus
Dans l'éditeur de panneau, sélectionnez votre source de données Prometheus.

Construisez votre requête PromQL dans le champ "Query". Par exemple, pour surveiller l'utilisation du CPU, vous pouvez utiliser une requête comme :

prometheus
Copy code
rate(node_cpu_seconds_total{mode!="idle"}[5m])
Personnalisez l'affichage :

Choisissez le type de visualisation : graphique, jauge, etc.
Ajustez les axes, légendes et autres paramètres d'affichage pour que les données soient bien représentées.
Enregistrez le panneau et donnez un nom à votre tableau de bord.

3.3. Ajouter des panneaux supplémentaires
Répétez le processus pour ajouter d'autres panneaux au tableau de bord, chacun représentant différentes métriques (RAM, disque, réseau, etc.) en fonction des requêtes PromQL que vous utilisez.

3.4. Sauvegarder le tableau de bord
Une fois que vous avez terminé d'ajouter des panneaux, cliquez sur "Save Dashboard" pour sauvegarder votre tableau de bord. Donnez-lui un nom descriptif.

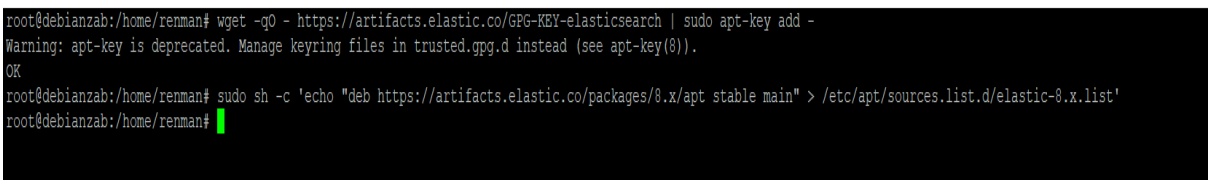
Étape 4: Personnalisation et partage
Personnalisez vos tableaux de bord en fonction de vos besoins, en ajustant les couleurs, les intervalles de temps, etc.
Partagez vos tableaux de bord avec d'autres utilisateurs via des liens partagés ou en configurant des comptes utilisateurs dans Grafana.
Conclusion
En suivant ces étapes, vous avez installé Grafana, intégré Prometheus comme source de données et créé des tableaux de bord pour visualiser les données collectées par Prometheus. Ces tableaux de bord vous permettront de surveiller efficacement l'état de vos systèmes et services en temps réel.

Installation de l'ELK Stack
1.1. Installer Elasticsearch
Ajouter la clé GPG d'Elasticsearch :

```
wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
```

Ajouter le dépôt Elasticsearch :

```
sudo sh -c 'echo "deb https://artifacts.elastic.co/packages/8.x/apt stable main" > /etc/apt/sources.list.d/elastic-8.x.list'
```



Mettre à jour les dépôts et installer Elasticsearch :

sudo apt-get update
sudo apt-get install elasticsearch

```
root@debianzab:/home/renman# apt install elasticsearch
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  elasticsearch
0 upgraded, 1 newly installed, 0 to remove and 15 not upgraded.
Need to get 606 MB of archives.
After this operation, 1,168 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 elasticsearch amd64 8.15.0 [606 MB]
Fetched 606 MB in 60s (10.1 MB/s)
Selecting previously unselected package elasticsearch.
(Reading database ... 191285 files and directories currently installed.)
Preparing to unpack .../elasticsearch_8.15.0_amd64.deb ...
Creating elasticsearch group... OK
Creating elasticsearch user... OK
Unpacking elasticsearch (8.15.0) ...
Setting up elasticsearch (8.15.0) ...
--------------------------- Security autoconfiguration information ------------------------------

Authentication and authorization are enabled.
TLS for the transport and HTTP layers is enabled and configured.

The generated password for the elastic built-in superuser is : W_P4q8tmaA8aBl-0ibqQ

If this node should join an existing cluster, you can reconfigure this with
'/usr/share/elasticsearch/bin/elasticsearch-reconfigure-node --enrollment-token <token-here>'
after creating an enrollment token on your existing cluster.

You can complete the following actions at any time:

Reset the password of the elastic built-in superuser with
'/usr/share/elasticsearch/bin/elasticsearch-reset-password -u elastic'.

Generate an enrollment token for Kibana instances with
 '/usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s kibana'.

Generate an enrollment token for Elasticsearch nodes with
'/usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s node'.

-------------------------------------------------------------------------------------------------
### NOT starting on installation, please execute the following statements to configure elasticsearch service to start automatically using systemd
 sudo systemctl daemon-reload
 sudo systemctl enable elasticsearch.service
### You can start elasticsearch service by executing
 sudo systemctl start elasticsearch.service
```

Démarrer et activer Elasticsearch :

sudo systemctl start elasticsearch
sudo systemctl enable elasticsearch

```
root@debianzab:/home/renman#  systemctl start elasticsearch.service
root@debianzab:/home/renman#  systemctl enable elasticsearch.service
Created symlink /etc/systemd/system/multi-user.target.wants/elasticsearch.service → /lib/systemd/system/elasticsearch.service.
root@debianzab:/home/renman#  systemctl enable elasticsearch
root@debianzab:/home/renman#
```

Vérifier qu'Elasticsearch fonctionne :

Accédez à **http://localhost:9200** dans votre navigateur ou utilisez curl pour vérifier :

curl -X GET "localhost:9200/"

```
root@debianzab:/home/renman# systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
     Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; vendor preset: enabled)
     Active: active (running) since Tue 2024-09-03 22:21:02 CEST; 4min 19s ago
       Docs: https://www.elastic.co
   Main PID: 4984 (java)
      Tasks: 82 (limit: 7053)
     Memory: 3.4G
        CPU: 3min 8.789s
     CGroup: /system.slice/elasticsearch.service
             ├─4984 /usr/share/elasticsearch/jdk/bin/java -Xms4m -Xmx64m -XX:+UseSerialGC -Dcli.name=server -Dcli.script=/usr/share/elasticsearch/bin/elasticsearch -Dcli.libs=lib/tools/ser>
             ├─5042 /usr/share/elasticsearch/jdk/bin/java -Des.networkaddress.cache.ttl=60 -Des.networkaddress.cache.negative.ttl=10 -Djava.security.manager=allow -XX:+AlwaysPreTouch -Xss1>
             └─5064 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/bin/controller

Sep 03 22:19:08 debianzab systemd[1]: Starting Elasticsearch...
Sep 03 22:19:24 debianzab systemd-entrypoint[4984]: Sep 03, 2024 10:19:24 PM sun.util.locale.provider.LocaleProviderAdapter <clinit>
Sep 03 22:19:24 debianzab systemd-entrypoint[4984]: WARNING: COMPAT locale provider will be removed in a future release
Sep 03 22:21:02 debianzab systemd[1]: Started Elasticsearch.
lines 1-17/17 (END)
```

.2. Installer Logstash

1. Installer Logstash :

sudo apt-get install logstash

Démarrer et activer Logstash :

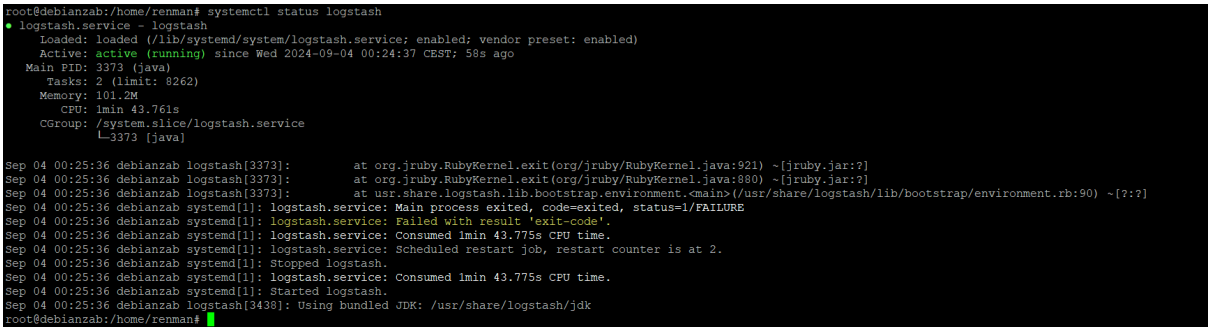
sudo systemctl start logstash

sudo systemctl enable logstash

```
root@debianzab:/home/renman# apt-get install logstash
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  logstash
0 upgraded, 1 newly installed, 0 to remove and 15 not upgraded.
Need to get 421 MB of archives.
After this operation, 698 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 logstash amd64 1:8.15.0-1 [421 MB]
Fetched 421 MB in 56s (7,575 kB/s)
Selecting previously unselected package logstash.
(Reading database ... 192800 files and directories currently installed.)
Preparing to unpack .../logstash_1%3a8.15.0-1_amd64.deb ...
Unpacking logstash (1:8.15.0-1) ...
Setting up logstash (1:8.15.0-1) ...
root@debianzab:/home/renman# systemctl start logstash
root@debianzab:/home/renman# systemctl enable logstash
Created symlink /etc/systemd/system/multi-user.target.wants/logstash.service → /lib/systemd/system/logstash.service.
root@debianzab:/home/renman#
```

Verification de l'état de logstash

systemctl status logstash



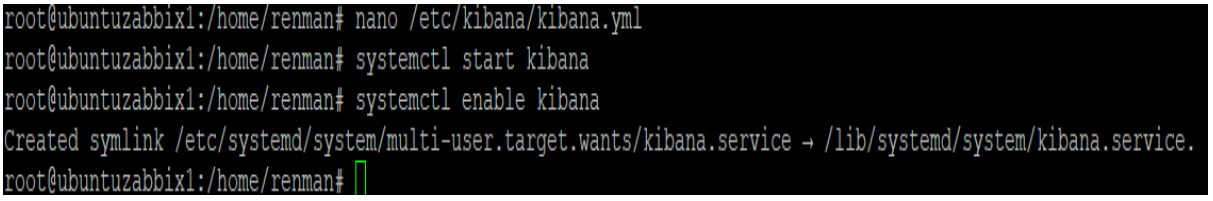
Installer Kibana :

sudo apt-get install kibana

Démarrer et activer Kibana :

sudo systemctl start kibana

sudo systemctl enable kibana



Sources:

https://play.grafana.org/d/bdnahipisghdsa/getting-started-with-grafana-play

modeles de graphes telechargeables:

https://grafana.com/grafana/dashboards/

Tuto

https://www.youtube.com/watch?v=dTjzkxuG20Y

analyse avec kibana:

https://www.youtube.com/watch?v=ULtlDOs0mAs

elasticsearch+logstash=kibana

elasticsearch: base de données nosql bien scalable et flexible dans le stockage,analyse et recherche en utilisant des index des mots de fichiers de données et de logs

Logstash: interface entre source des données et elasticsearch,logstash joue le rôle de gestion de source de données(twitter,tcp,syslog,Redis,Logs apache,etc..).Logstash va se connecter à une source de données,récupère en temps réel des informations et les injecter dans elasticsearch.

Kibana: outil de dashboarding en temps réel,il récupère des données dans elasticsearch ,on n'a pas besoin de savoir coder ,il est très puissant au niveau de filtrage.Kibana gère aussi la géolocalisation comme des adresse ip par exemple.avec kibana, on peut générer des sparklines et des tendances,suivi de codes retour,suivi de conversions,recherche dans les données brutes

1. Installation de TheHive

TheHive est une plateforme d'analyse et de réponse aux incidents de sécurité.

1.1. Prérequis

Un serveur sous Ubuntu/Debian ou une machine virtuelle pour installer TheHive.

Java installé sur le serveur, car TheHive est basé sur Java.

1.2. Installer Java

TheHive requiert une version de Java, installez-la en exécutant les commandes suivantes :

sudo apt update

sudo apt install openjdk-11-jdk -y

1.3. Installer TheHive

Ajouter le dépôt officiel de TheHive :

echo "deb https://dl.bintray.com/thehive-project/deb stable main" | sudo tee -a /etc/apt/sources.list.d/thehive-project.list

Importer la clé GPG et mettre à jour les paquets :

sudo apt install apt-transport-https

sudo apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv-keys 562CBC1C3B89D402

sudo apt update

Installer TheHive :

script

https://docs.strangebee.com/thehive/installation/automated-installation-script/

steps by steps

```
apt install wget gnupg apt-transport-https git ca-certificates
ca-certificates-java curl software-properties-common python3-pip lsb-release
```