Pourquoi installer du monitoring

- vision d'ensemble de son infrastructure.
- récupération d'information de santé de ses actifs.
- mise en place d'alerte pour réduire le temps de réaction et par conséquent d'intervention.

I. Étapes importantes de l'installation

Du fait que nous soyons sur une distribution arch linux, l'installation de zabbix ne ce fait pas aussi simplement que sur d'autres distributions.
Voici les étapes clés pour que l'installation se passe au mieux.

Dans un premier temps, pour l'installation de la base de données :

1. Installation de mariadb

```
sudo pacman -S mariadb
```

Initialisation de la base de donnée :

```
sudo mariadb-install-db --user=mysql --basedir=/usr --datadir=/var/lib/mysql
```

Sans ça, la base de données ne démarre pas.

2. Installation de php :

Extension à activer dans php.ini :

```
extension=bcmath
;extension=bz2
;extension=calendar
extension=curl
;extension=dba
;extension=enchant
;extension=exif
;extension=ffi
;extension=ftp
extension=gd
extension=gettext
;extension=gmp
;extension=iconv
;extension=intl
;extension=ldap
extension=mysqli
;extension=odbc
;zend_extension=opcache
;extension=pdo_dblib
;extension=pdo_mysql
;extension=pdo_odbc
;extension=pdo_pgsql
;extension=pdo_sqlite
;extension=pgsql
;extension=shmop
;extension=snmp
;extension=soap
extension=sockets
;extension=sodium
;extension=sqlite3
;extension=sysvmsg
;extension=sysvsem
;extension=sysvshm
;extension=tidy
;extension=xsl
```

3. Configuration du serveur web :

Configuration à ajouter dans nginx.conf :

```
server {
listen 80;
server_name 192.168.10.8;

root /srv/http;
index index.php index.html index.htm;

location / {
    try_files $uri $uri/ =404;
}

location /zabbix {
    alias /srv/http/zabbix/;
    index index.php;
}

location ~ \.php$ {
    fastcgi_pass unix:/run/php-fpm/php-fpm.sock;
    fastcgi_index index.php;
    include fastcgi.conf;
    fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
}
```

Une fois les changements effectués, vous devriez pouvoir poursuivre l'installation de votre outil zabbix.

ATTENTION : En étant sur arch linux, si vous installez le paquet php, la version installées sera trop récente et donc incompatible avec zabbix. (voir ci dessous).

De ce fait, vous devez installer une version plus ancienne de php.

Ici, je fais l'exemple avec php7.4 mais il est important de noter que les versions les plus récentes de zabbix acceptent au minimum une version 8.0 de php.

Remplacement de php8.4 par php7.4 :

```
sudo ln -sf /usr/bin/php74 /usr/bin/php
```

```
[localadm@zabbix php74]$ sudo systemctl disable php-fpm
Removed '/etc/systemd/system/multi-user.target.wants/php-fpm.servi
ce'.
```

Changement de nginx.conf

```
location ~ \.php$ {
    fastcgi_pass unix:/run/php74-fpm/php-fpm.sock;
```

Vérification :

```
[localadm@zabbix php74]$ sudo -u zabbix-server php -v
PHP 7.4.33 (cli) (built: Feb 28 2025 10:59:28) ( NTS )
Copyright (c) The PHP Group
Zend Engine v3.4.0, Copyright (c) Zend Technologies
    with Zend OPcache v7.4.33, Copyright (c), by Zend Technologies
```

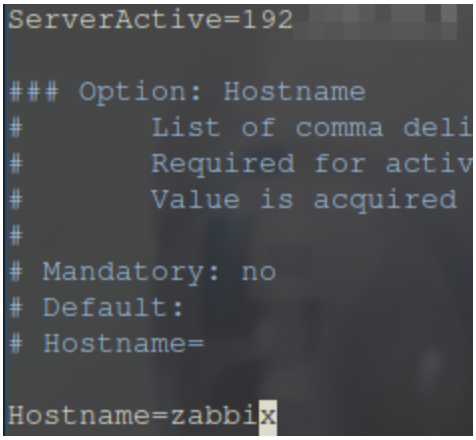
II. Installation d'un agent

Installation de l'agent

`bash sudo pacman -S zabbix-agent`

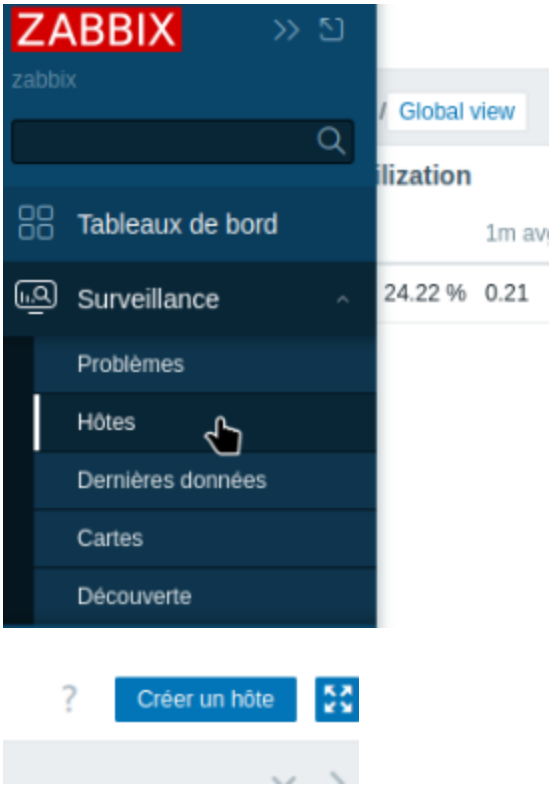
Configuration :

```
vim /etc/zabbix/zabbix_agentd.conf
```

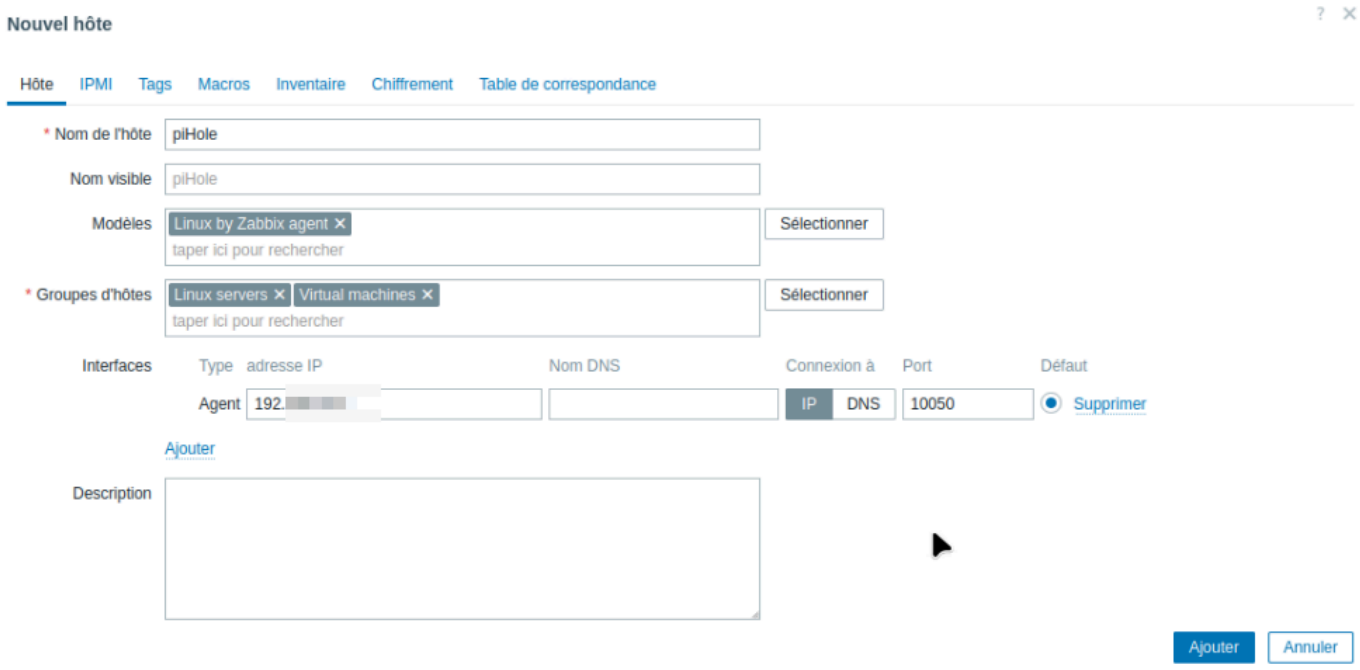


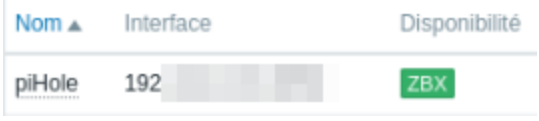
III. Ajout d'un hôte

Sur la page hôte :



Configuration de l'hôte :





IV. Activation du SSL

Il est important de chiffrer ses flux de données, peu importe l'importance du service au sein d'une infrastructure.

Création du dossier de certificat :

```
mkdir -p /etc/ssl/private
chmod 0750 /etc/ssl/private
```

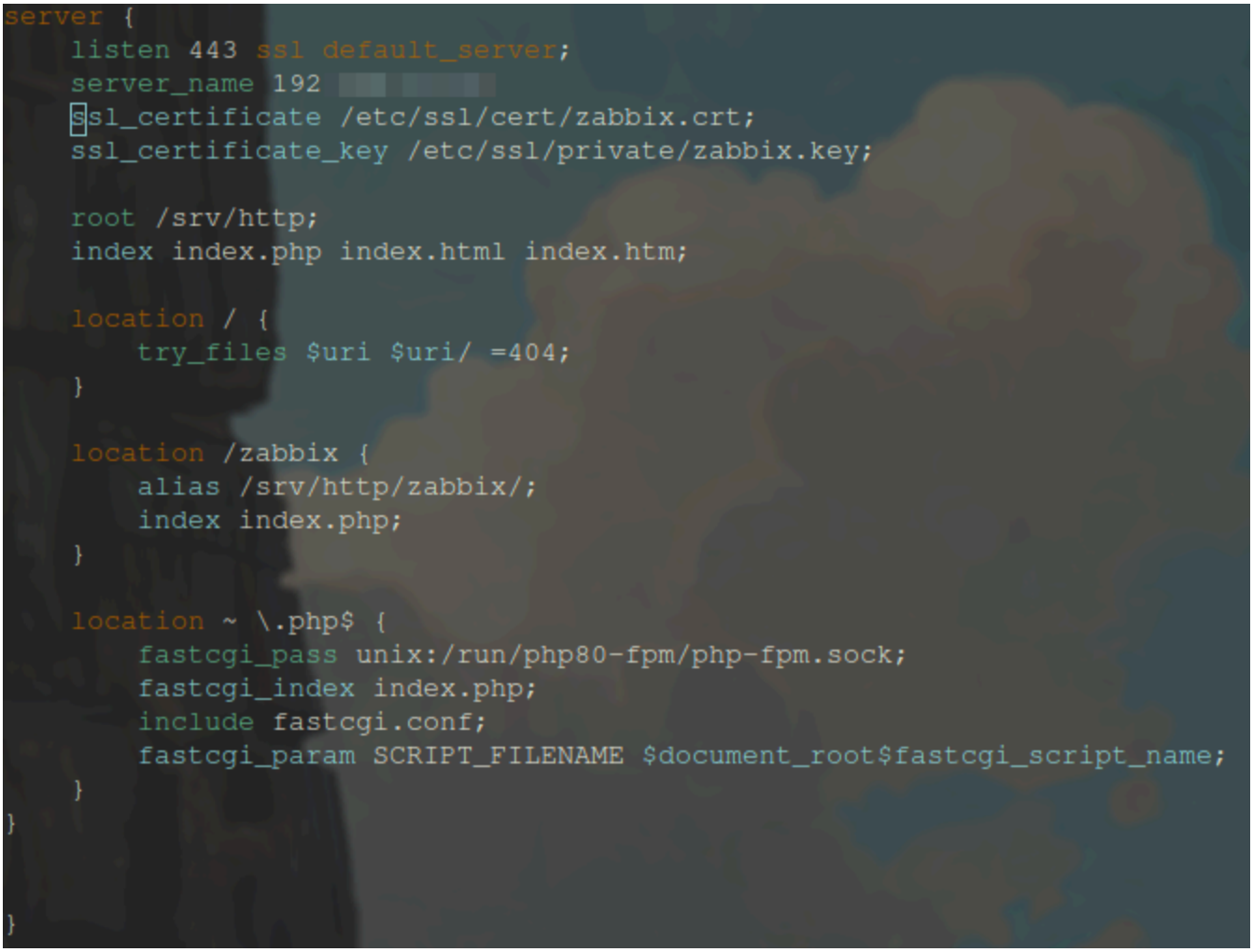
Génération du certificat (autosigné) :
A NOTER : On utilise aujourd'hui l'algorithme RSA pour le chiffrement, cependant l'évolution des ordinateurs quantiques est assez importante de nos jours pour que l'on commence à s'interroger sur l'utilisation de chiffrement post quantique **CRYSTALS-KYBER** ou **Dilithium**.

```
sudo openssl -req -newkey rsa:2048 -nodes -keyout
/etc/ssl/private/zabbix.key -x509 -days 1825 -out /etc/ssl/certs/zabbix.crt
```

Permission des certificats :

```
chmod 0400 /etc/ssl/certs/zabbix.crt
chmod 0400 /etc/ssl/private/zabbix.key;
```

Création du fichier zabbix-ssl.conf pour la configuration nginx :



```
server {
    listen 443 ssl default_server;
    server_name 192 [redacted]
    ssl_certificate /etc/ssl/cert/zabbix.crt;
    ssl_certificate_key /etc/ssl/private/zabbix.key;

    root /srv/http;
    index index.php index.html index.htm;

    location / {
        try_files $uri $uri/ =404;
    }

    location /zabbix {
        alias /srv/http/zabbix/;
        index index.php;
    }

    location ~ \.php$ {
        fastcgi_pass unix:/run/php80-fpm/php-fpm.sock;
        fastcgi_index index.php;
        include fastcgi.conf;
        fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
    }
}


}
```

On redémarre le service.

Notre site web est bien passé en ssl avec notre certificat :