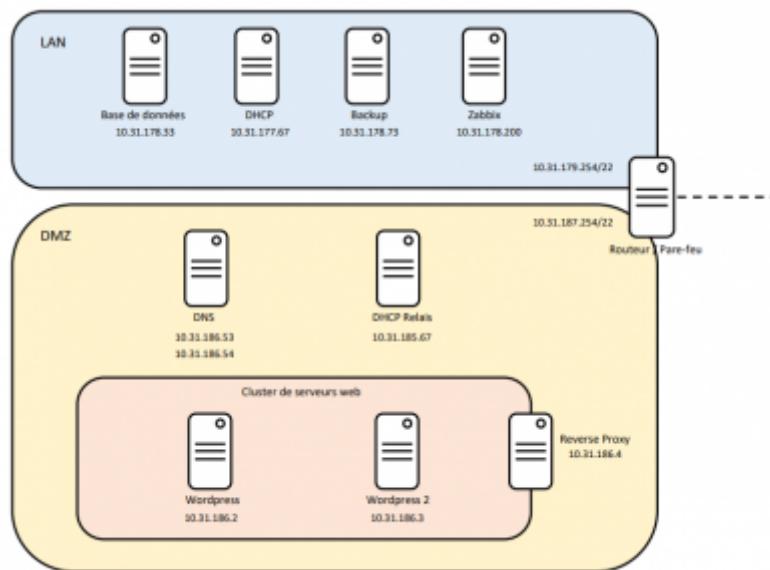


- Accueil
- Situation Professionnelle 1 Lucie
- Situation Professionnelle 2 Lucie

# I) Introduction et Contexte

La société GSB souhaite sécuriser le nouveau site internet de la filiale japonaise. Pour ce faire, un second serveur web ainsi qu'un reverse proxy seront créés afin de mettre en place le load balancing. La solution IPS Fail2ban sera mise en place afin de protéger les serveurs web. Enfin, la solution de supervision Zabbix sera mise en place afin de monitorer le cluster de serveurs web.

Voici le schéma du réseau comprenant chaque machine utilisée pour cette situation professionnelle :



## I) HAProxy

### A) Création du reverse proxy et du second serveur web

Nous clonons dans un premier temps la VM template et lui attribuons une nouvelle adresse IP (10.31.186.4 (haproxy)) et un nouveau nom d'hôte dans le DHCP :

```
dhclient -r && dhclient -v
```

```
# Change le nom d'hôte à l'aide d'une commande
hostnamectl set-hostname srv-web1-1 # Ou srv-web2-1
```

```
# Change le nom d'hôte directement depuis le fichier de configuration  
nano /etc/hosts
```

Nous modifions dans le fichier /etc/hosts le nom d'hôte de la machine et nous nous déconnectons pour actualiser l'affichage du nom.

Nous clonons ensuite notre serveur web pour créer notre second serveur web identique qui aura pour IP 10.31.186.3 et pour nom d'hôte wordpress-sp2.

## B) Configuration du reverse proxy

Nous installons les paquets nécessaires :

```
apt update && apt upgrade  
apt install haproxy
```

Nous démarrons le service haproxy :

```
systemctl start haproxy  
systemctl enable haproxy
```

Nous modifions le fichier de configuration. Nous ferons en sorte que le reverse proxy soit configuré en mode transparent, c'est-à-dire qu'il laissera passer les requêtes HTTP afin que le serveur web fasse lui-même la redirection HTTPS. Nous gèrerons également les cookies de sorte que lorsqu'une session est ouverte, nous ne soyons pas changé de serveur web à l'envoie d'une autre requête. Nous configurerons également le load balancing de sorte que le serveur ayant reçu le moins de requêtes reçoive la requête.

```
frontend http-in  
    bind *:80  
    mode http  
    #http-request redirect scheme https code 301 unless { ssl_fc }  
    default_backend http-servers

frontend https-in  
    bind *:443  
    mode tcp  
    default_backend https-servers

backend http-servers  
    mode http  
    cookie SERVERID insert indirect nocache
```

```

# Redirige les requêtes sur le serveur ayant le moins reçu de
requêtes
    balance leastconn
        # L'argument check permet de vérifier l'état d'un serveur et de le
sortir du load balancing en cas de problème
        server wordpress-sp1 10.31.186.2:80 check
        server wordpress-sp2 10.31.186.3:80 check

backend https-servers
    mode tcp
    cookie SERVERID insert indirect nocache
    balance leastconn
    server wordpress-sp1 10.31.186.2:443 check
    server wordpress-sp2 10.31.186.3:443 check

```

Nous redémarrons le service :

```
systemctl restart haproxy
```

## C) Modification DNS

Pour permettre à notre reverse proxy d'effectuer la balance des charges, nous devons rediriger les requêtes du DNS vers ce dernier. Nous changeons donc dans nos DNS le fichier db.japon.gsb.org :

```

$TTL      604800;
@ IN SOA ns2-1-pub.gsb.org. root.gsb.org. (
    2023101701;
    43200;
    3600;
    3600000;
    172800 );

; Adresse de la zone (le ping japon.gsb.org pinguera cette adresse)
@ IN A 10.31.186.4;

; DNS Server (on définit les DNS d'autorité pour cette zone)
@ IN NS ns2-1-pub.gsb.org. ;
@ IN NS ns2-2-pub.gsb.org. ;

; Association adresse IP des DNS avec leurs noms (si on ping ces noms on
pinguera ces adresses)
ns2-1-pub IN A 10.31.186.53;
ns2-2-pub IN A 10.31.186.54;

```

```
; Association adresse IP du cluster de serveurs avec www (le ping
www.japon.gsb.org pinguera ces adresses)
www IN A 10.31.186.4;
```

nous redémarrons notre service :

```
systemctl restart bind9
```

Pour vérifier que le load balancing soit bien opérationnel, nous modifions les pages d'accueil d'Nginx. Nous nous rendons ensuite sur notre navigateur pour rentrer l'adresse IP de notre reverse proxy :

web-1 (10.31.186.2) :



## Welcome to nginx 2!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to [nginx.org](http://nginx.org). Commercial support is available at [nginx.com](http://nginx.com).

*Thank you for using nginx.*

web-2 (10.31.186.3) :



## Welcome to nginx 3!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to [nginx.org](http://nginx.org). Commercial support is available at [nginx.com](http://nginx.com).

*Thank you for using nginx.*

## II) Fail2ban

Afin de sécuriser notre nouveau cluster de serveurs web, nous mettrons en place la solution IPS Fail2Ban, permettant de bannir des adresses IP après un certain nombre de tentatives de connexion échouées. Nous commençons par installer le paquet nécessaire :

```
apt install fail2ban
```

Nous dupliquons son fichier de configuration pour créer une copie sur laquelle on effectuera nos changements. En effet, le fichier de configuration par défaut risque d'être écrasé lors de mises à jour.

```
cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
```

Nous modifions notre nouveau fichier de configuration pour l'adapter à notre besoin :

```
# "bantime" is the number of seconds that a host is banned.  
bantime = 10m  
  
# A host is banned if it has generated "maxretry" during the last "findtime"  
# seconds.  
findtime = 10m  
  
# "maxretry" is the number of failures before a host get banned.  
maxretry = 5
```

Testons d'échouer une connexion avec un client :

```
std@10.31.186.2's password:  
Permission denied, please try again.  
std@10.31.186.2's password:  
Permission denied, please try again.  
std@10.31.186.2's password:  
std@10.31.186.2: Permission denied (publickey,password).  
root@glpi-itil:~# ssh std@10.31.186.2  
std@10.31.186.2's password:  
Permission denied, please try again.  
std@10.31.186.2's password:  
Permission denied, please try again.  
std@10.31.186.2's password:  
Connection closed by 10.31.186.2 port 22
```

Nous affichons la liste des IP bannies :

```
fail2ban-client status sshd
```

```
root@wordpress-spl:~# sudo fail2ban-client status sshd  
Status for the jail: sshd  
|- Filter  
| |- Currently failed: 0  
| |- Total failed: 5  
| '- File list: /var/log/auth.log  
'- Actions  
| |- Currently banned: 1  
| |- Total banned: 1  
| '- Banned IP list: 10.31.179.26
```

Nous pouvons débannir notre IP à l'aide de la commande suivante et vérifier la liste des IP bannies :

```
fail2ban-client set sshd unbanip <IP>
fail2ban-client status sshd
```

```
root@wordpress-spl:~# sudo fail2ban-client set sshd unbanip 10.31.179.26
1
root@wordpress-spl:~# sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed: 5
| '-- File list: /var/log/auth.log
`- Actions
  |- Currently banned: 0
  |- Total banned: 1
  '-- Banned IP list:
```

## III) Zabbix

### A) Installation du serveur

Nous clonons dans un premier temps la VM template et lui attribuons une nouvelle adresse IP (10.31.178.200) et un nouveau nom d'hôte dans le DHCP :

```
dhclient -r && dhclient -v
```

```
# Change le nom d'hôte à l'aide d'une commande
hostnamectl set-hostname zabbix-sp2

# Change le nom d'hôte directement depuis le fichier de configuration
nano /etc/hosts
```

Nous modifions dans le fichier /etc/hosts le nom d'hôte de la machine et nous nous déconnectons pour actualiser l'affichage du nom.

### B) Configuration du serveur

Dans un premier temps, nous devons installer le dépôt officiel de Zabbix. En effet, ce dernier n'est pas par défaut sur les machines Debian et les paquets téléchargeables sont des paquets obsolètes. Nous entrons donc les commandes ci-dessous :

```
wget
```

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

```
root@zabbix-srv2:~# wget https://repo.zabbix.com/zabbix/6.4/debian/pool/main/z/zabbix-release/zabbix-release_6.4-1+debia
n12_all.deb
--2023-12-15 10:11:22--  https://repo.zabbix.com/zabbix/6.4/debian/pool/main/z/zabbix-release/zabbix-release_6.4-1+debia
n12_all.deb
Résolution de repo.zabbix.com (repo.zabbix.com)... 178.128.6.101, 2604:a880:2:d0::2062:d001
Connexion à repo.zabbix.com (repo.zabbix.com)|178.128.6.101|:443... connecté.
requête HTTP transmise, en attente de la réponse... 200 OK
Taille : 3540 (3,5K) [application/octet-stream]
Sauvegarde en : « zabbix-release_6.4-1+debian12_all.deb »

zabbix-release_6.4-1+debian12 100%[=====] 3,46K --.-KB/s   ds 0s
2023-12-15 10:11:23 (94,3 MB/s) - « zabbix-release_6.4-1+debian12_all.deb » sauvegardé [3540/3540]
```

```
root@zabbix-srv2:~# dpkg -i zabbix-release_6.4-1+debian12_all.deb
dpkg: avertissement: dégradation (« downgrade ») de zabbix-release depuis 1:6.4-1+ubuntu22.04 vers 1:6.4-1+debian12
(Lecture de la base de données... 42652 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de zabbix-release_6.4-1+debian12_all.deb ...
Dépaquetage de zabbix-release (1:6.4-1+debian12) sur (1:6.4-1+ubuntu22.04) ...
Paramétrage de zabbix-release (1:6.4-1+debian12) ...
Installation de la nouvelle version du fichier de configuration /etc/apt/sources.list.d/zabbix.list ...
```

Nous installons ensuite les paquets nécessaires à l'utilisation de Zabbix. Notons que Zabbix a besoin d'un serveur web :

```
apt update && apt upgrade
apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf
zabbix-sql-scripts zabbix-agent apache2 php php-mysql php-mysqlnd php-ldap
php-bcmath php-mbstring php-gd php-pdo php-xml libapache2-mod-php
```

L'outil de supervision Zabbix a besoin de fonctionner avec une base de données. Nous utiliserons la base de données présente sur le réseau LAN. Il n'y a donc pas besoin d'ouvrir de flux dans notre pare-feu étant donné que les machines sont sur le même réseau et peuvent communiquer entre elles. Nous créons donc sur notre serveur de bases de données notre nouvelle base de données :

```
mysql -u root -p
```

```
create database zabbix_sp1 character set utf8mb4 collate utf8mb4_bin;
create user zabbix_sp1@'%' identified by 'password';
grant all privileges on zabbix_sp1.* to zabbix_sp1@'%';
# Cette commande nous permettra d'obtenir les droits pour remplir la base de
données à distance via la commande zcat
set global log_bin_trust_function_creators = 1;
```

```
MariaDB [(none)]> create database zabbix_sp1 character set utf8mb4 collate utf8mb4_bin;
Query OK, 1 row affected (0,000 sec)

MariaDB [(none)]> create user zabbix_sp1@'%' identified by 'password';
Query OK, 0 rows affected (0,001 sec)

MariaDB [(none)]> grant all privileges on zabbix_sp1.* to zabbix_sp1@'%';
Query OK, 0 rows affected (0,001 sec)

MariaDB [(none)]> set global log_bin_trust_function_creators = 1;
Query OK, 0 rows affected (0,000 sec)
```

Nous vérifions que notre base de données soit créée. Pour l'instant, aucune table n'est créée. Notre base de données est vide :

```
use zabbix_sp1
show tables;
```

```
MariaDB [(none)]> use zabbix_sp1
Database changed
MariaDB [zabbix_sp1]> show tables;
Empty set (0,000 sec)
```

Nous retournons sur le serveur Zabbix et entrons la commande zcat. Cette commande permet de remplir la base de données que nous avons créé précédemment

```
zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql --default-character-set=utf8mb4 -h 10.31.178.33 -uzabbix_sp1 -ppassword zabbix_sp1
```

Nous retournons sur notre serveur de bases de données pour vérifier que notre nouvelle base soit bien complétée :

```
use zabbix_sp1
show tables
```

```
MariaDB [zabbix_sp1]> show tables;
+-----+
| Tables_in_zabbix_sp1 |
+-----+
| acknowledges
| actions
| alerts
| auditlog
| autoreg_host
| changelog
| conditions
| config
| config_autoreg_tls
| connector
| connector_tag
| corr_condition
| corr_condition_group
| corr_condition_tag
| corr_condition_tagpair
| corr_condition_tagvalue |
```

```
| valuemap
| valuemap_mapping
| widget
| widget_field
+-----+
186 rows in set (0,001 sec)
```

Nous devons maintenant désactiver la variable globale MariaDB permettant d'obtenir des privilèges spécifiques :

```
set global log_bin_trust_function_creators = 0;
```

```
MariaDB [(none)]> set global log_bin_trust_function_creators = 0;
Query OK, 0 rows affected (0,000 sec)
```

Nous modifions le fichier de configuration zabbix\_server.conf :

```
nano /etc/zabbix/zabbix_server.conf
```

Nous devons vérifier que les éléments suivants soient correctement remplis et les modifier si nécessaire :

- DBHost=10.31.178.33 - DBName=zabbix\_sp1 - DBUser=zabbix\_sp1 - DBPassword=password

```
### Option: DBHost
#      Database host name.
#      If set to localhost, socket is used for MySQL.
#      If set to empty string, socket is used for PostgreSQL.
#      If set to empty string, the Net Service Name connection method is used to connect
#      the TNS_ADMIN environment variable to specify the directory where the tnsnames.ora
#
# Mandatory: no
# Default:
DBHost=10.31.178.33
```

```
### Option: DBName
# Database name.
# If the Net Service Name connection method is used to connect to Oracle,
# the tnsnames.ora file or set to empty string; also see the TWO_TASK environment variable.
#
# Mandatory: yes
# Default:
# DBName=

DBName=zabbix_sp1
```

```
### Option: DBUser
# Database user.
#
# Mandatory: no
# Default:
# DBUser=
```

```
DBUser=zabbix_sp1
```

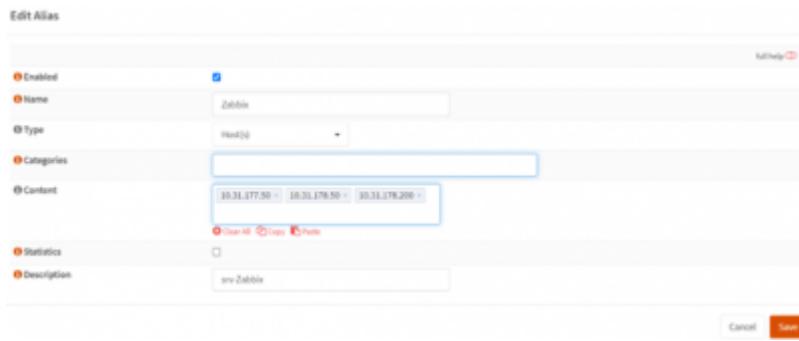
```
### Option: DBPassword
# Database password.
# Comment this line if no password is used.
#
# Mandatory: no
# Default:
DBPassword=password
```

Nous pouvons redémarrer le service zabbix-server :

```
systemctl restart zabbix-server
```

## C) Installation via l'interface web

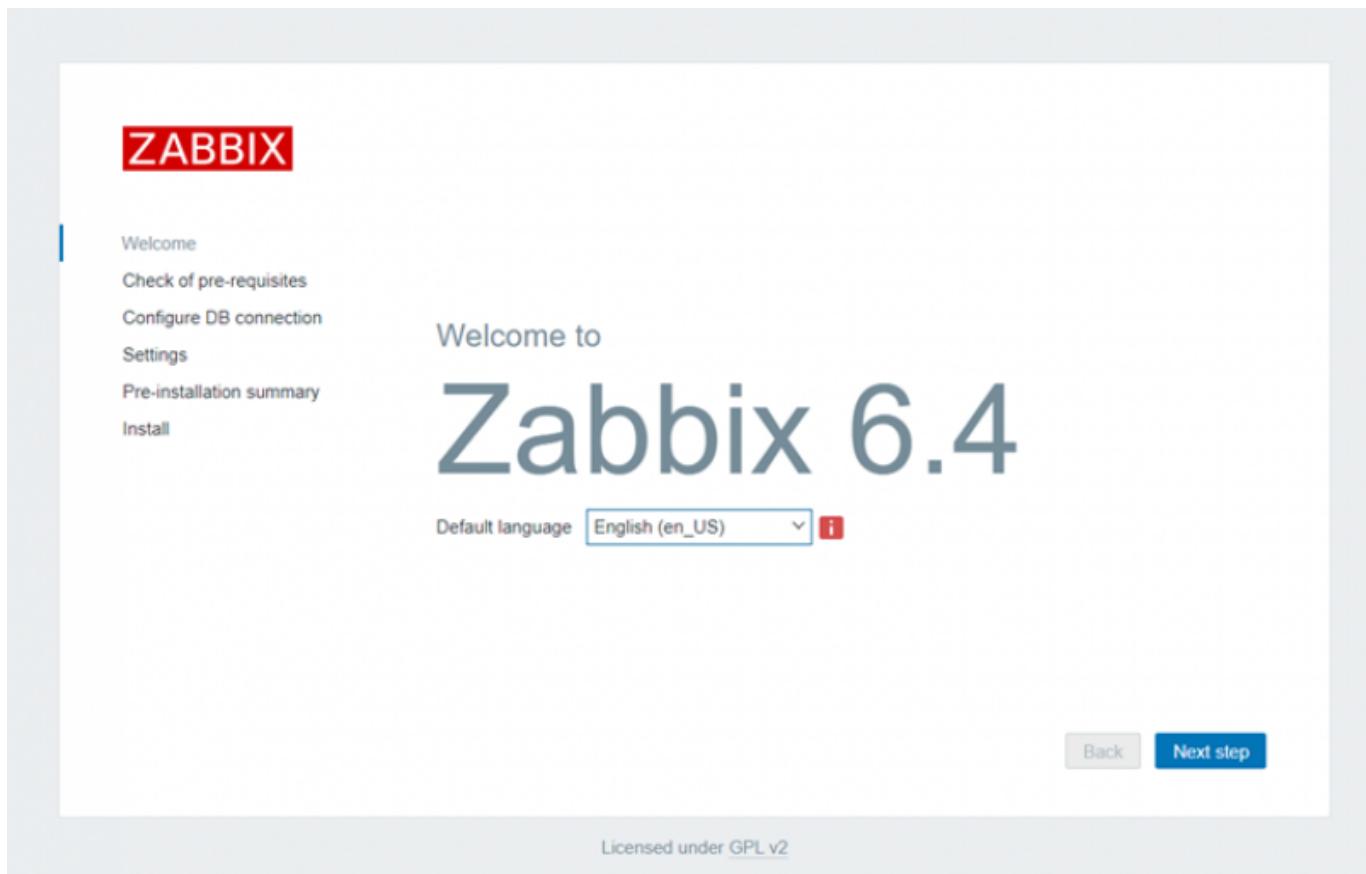
Pour accéder à l'interface graphique, nous devons ajouter notre serveur à l'alias Zabbix dans notre pare-feu, puis le redémarrer afin de prendre en compte le changement dans la règle.



The screenshot shows the 'Edit Alias' configuration page. The 'Name' field is set to 'Zabbix'. The 'Content' field contains three IP addresses: 10.31.177.50, 10.31.178.50, and 10.31.179.200. The 'Description' field is set to 'srv-Zabbix'. The 'Type' dropdown is set to 'Host(s)'. The 'Statistics' section is collapsed.

Nous nous rendons sur l'interface graphique d'installation via le lien <http://10.31.178.200/zabbix> :

Nous laissons l'interface en anglais pour l'installation.



The screenshot shows the Zabbix 6.4 installation welcome screen. The main area displays 'Welcome to Zabbix 6.4'. A 'Default language' dropdown is set to 'English (en\_US)'. At the bottom right are 'Back' and 'Next step' buttons, and a note stating 'Licensed under GPL v2'.

Nous regardons si tous les paquets nécessaires sont installés. Dans le cas contraire, nous les

installons avant de démarrer l'installation de Zabbix.

The screenshot shows the Zabbix pre-requisites check page. On the left, there is a vertical navigation menu with the following items: Welcome, Check of pre-requisites (which is selected and highlighted in red), Configure DB connection, Settings, Pre-installation summary, and Install. The main content area is titled "Check of pre-requisites". It contains a table with the following data:

	Current value	Required	
PHP version	8.2.7	7.4.0	OK
PHP option "memory_limit"	128M	128M	OK
PHP option "post_max_size"	16M	16M	OK
PHP option "upload_max_filesize"	2M	2M	OK
PHP option "max_execution_time"	300	300	OK
PHP option "max_input_time"	300	300	OK
PHP databases support	MySQL		OK
PHP bcmath	on		OK
PHP mbstring	on		OK
PHP option "mbstring.func_overload"	off	off	OK

At the bottom right of the table are two buttons: "Back" and "Next step". Below the table, a small note says "Licensed under [GPL v2](#)".

En cas de problème de langue, suivre les étapes de configuration de langue trouvables après la partie sur l'installation de Zabbix.

Nous entrons les informations pour connecter Zabbix à notre base de données.

**ZABBIX**

## Configure DB connection

Please create database manually, and set the configuration parameters for connection to this database.  
Press "Next step" button when done.

Welcome  
Check of pre-requisites  
Configure DB connection  
**Settings**  
Pre-installation summary  
Install

Database type: MySQL

Database host: 10.31.178.33

Database port: 3306 (0 - use default port)

Database name: zabbix\_sp1

Store credentials in: Plain text (selected), HashiCorp Vault, CyberArk Vault

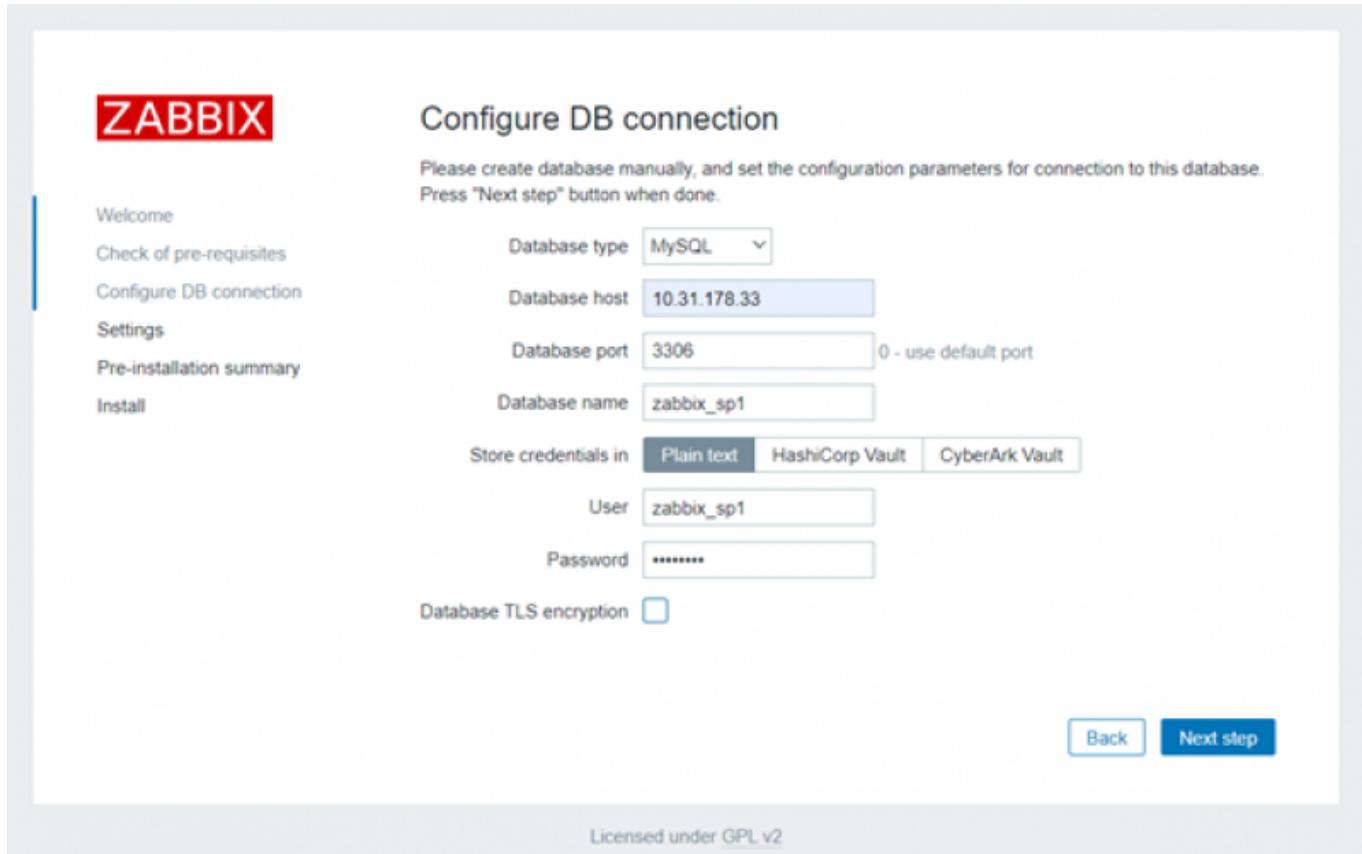
User: zabbix\_sp1

Password:

Database TLS encryption:

[Back](#) [Next step](#)

Licensed under GPL v2



Nous choisissons les paramètres de Zabbix (en activant le thème sombre).

**ZABBIX**

## Settings

Welcome  
Check of pre-requisites  
Configure DB connection  
**Settings**  
Pre-installation summary  
Install

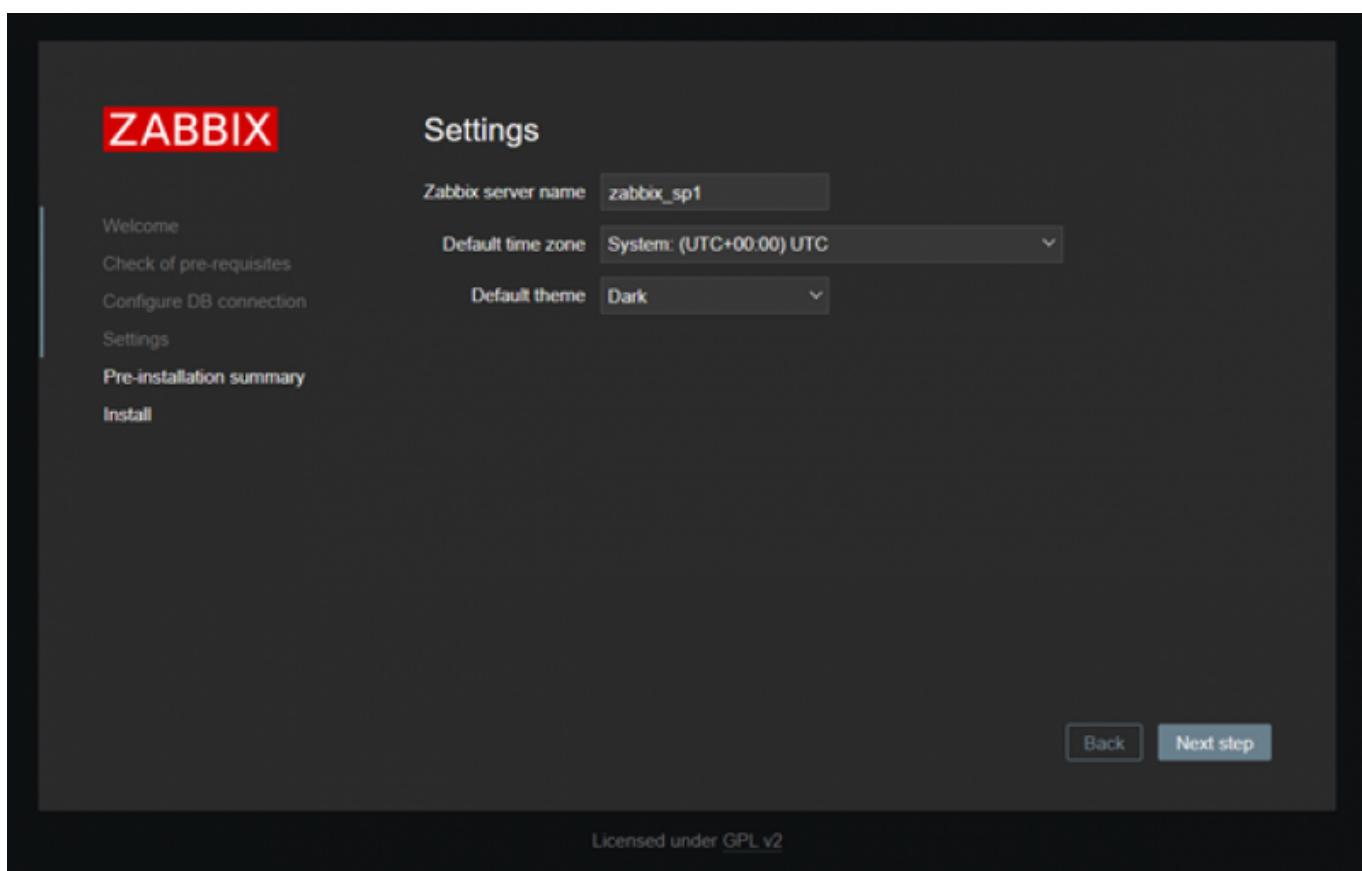
Zabbix server name: zabbix\_sp1

Default time zone: System: (UTC+00:00) UTC

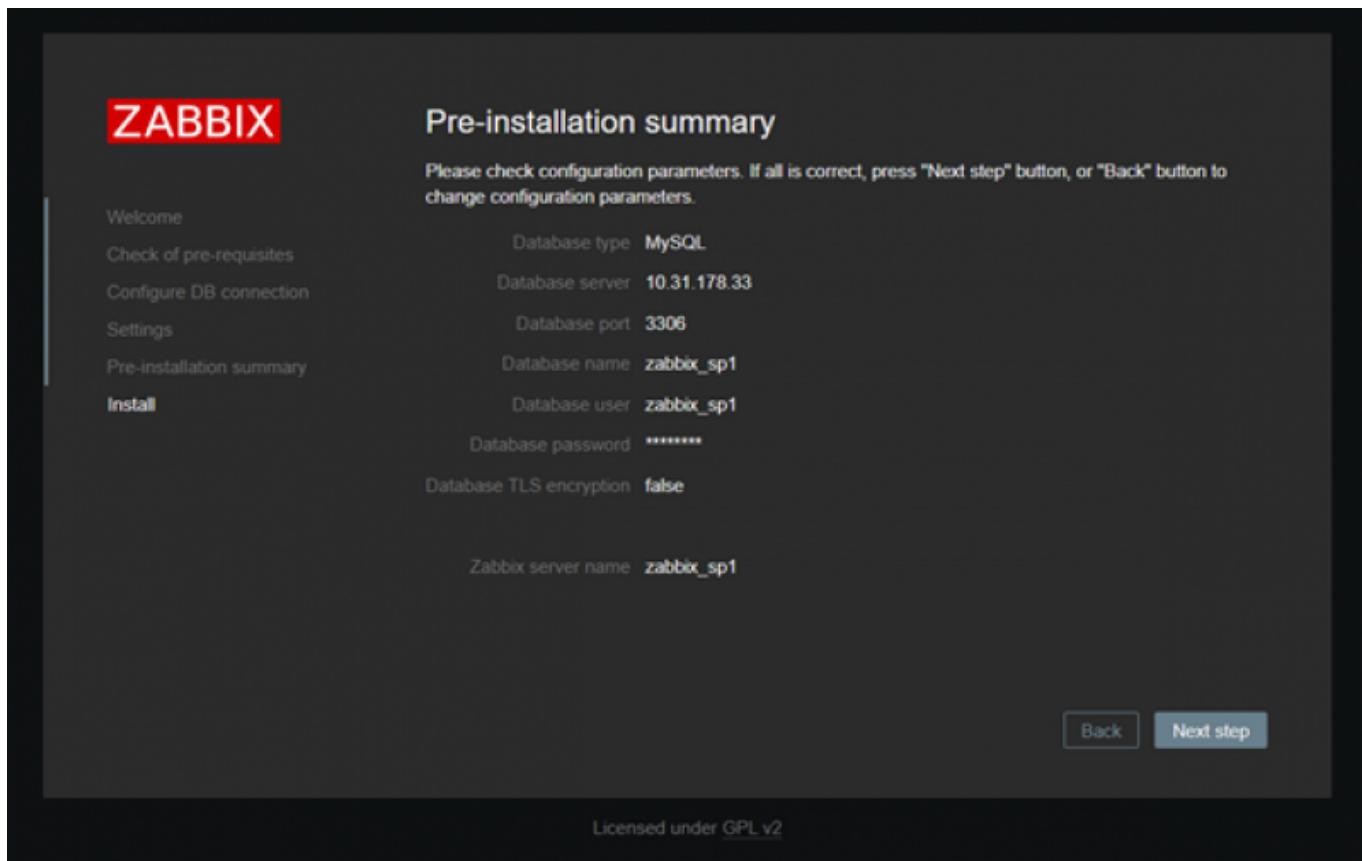
Default theme: Dark

[Back](#) [Next step](#)

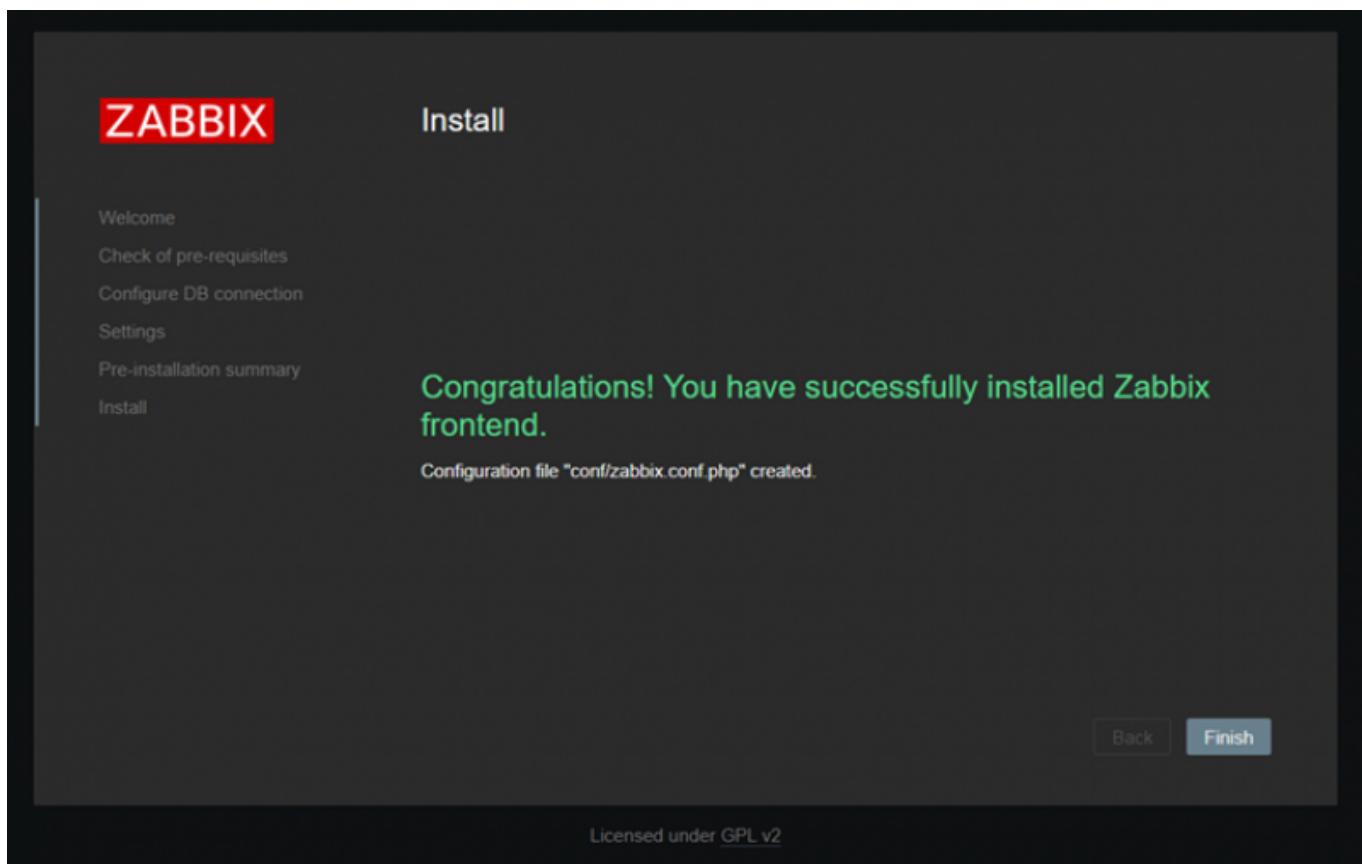
Licensed under GPL v2



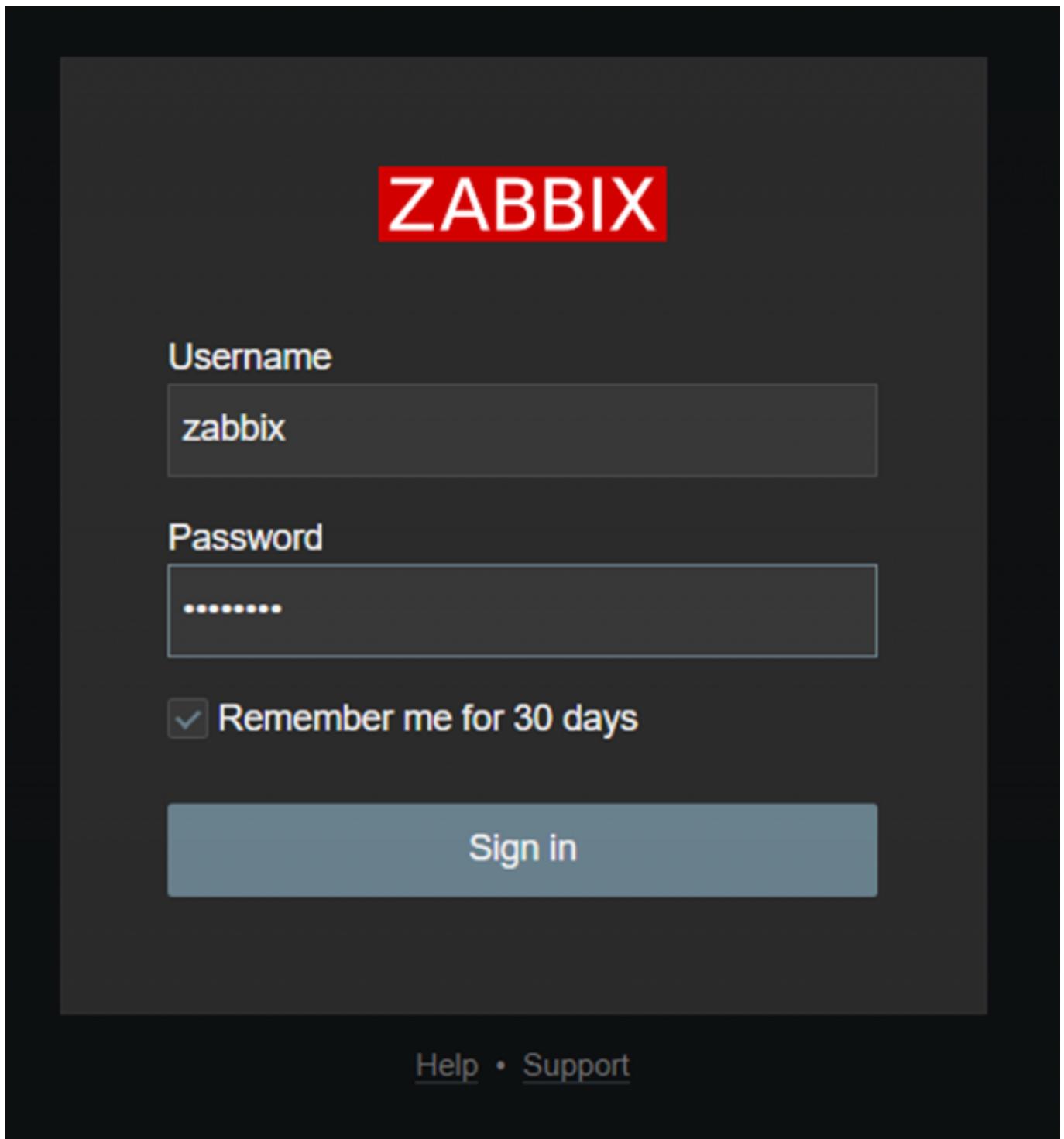
Nous vérifions que les éléments entrés soient corrects.



Nous pouvons terminer l'installation.



Nous pouvons maintenant nous connecter avec les identifiants par défaut : Admin/zabbix :

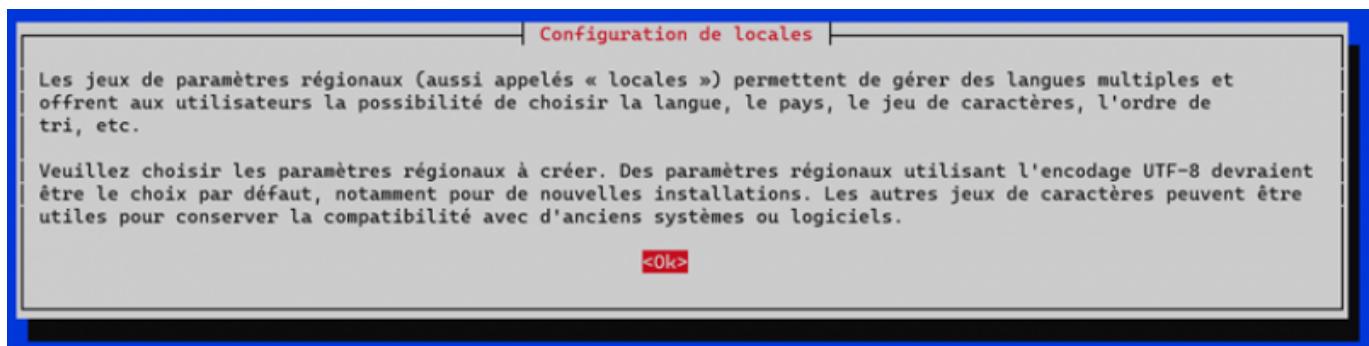


Nous pouvons voir sur notre tableau de bord que beaucoup d'erreurs empêchent le bon fonctionnement des graphes.

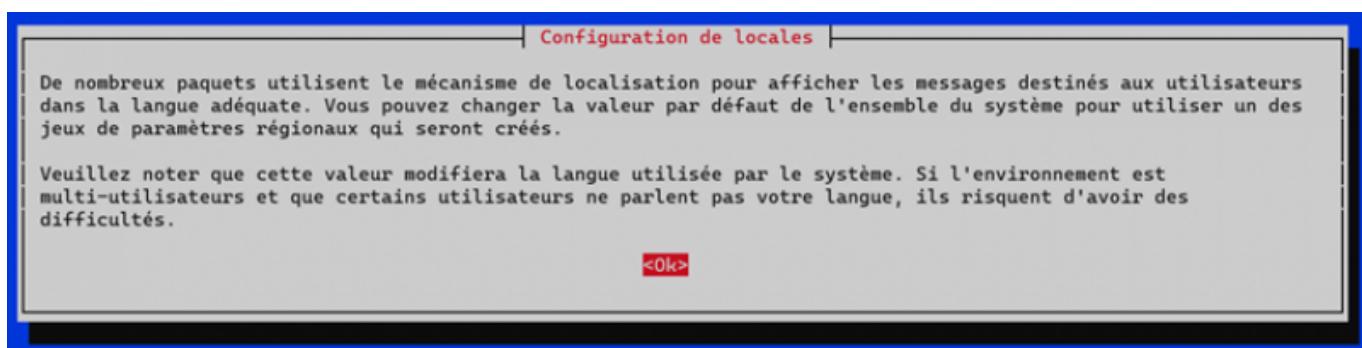
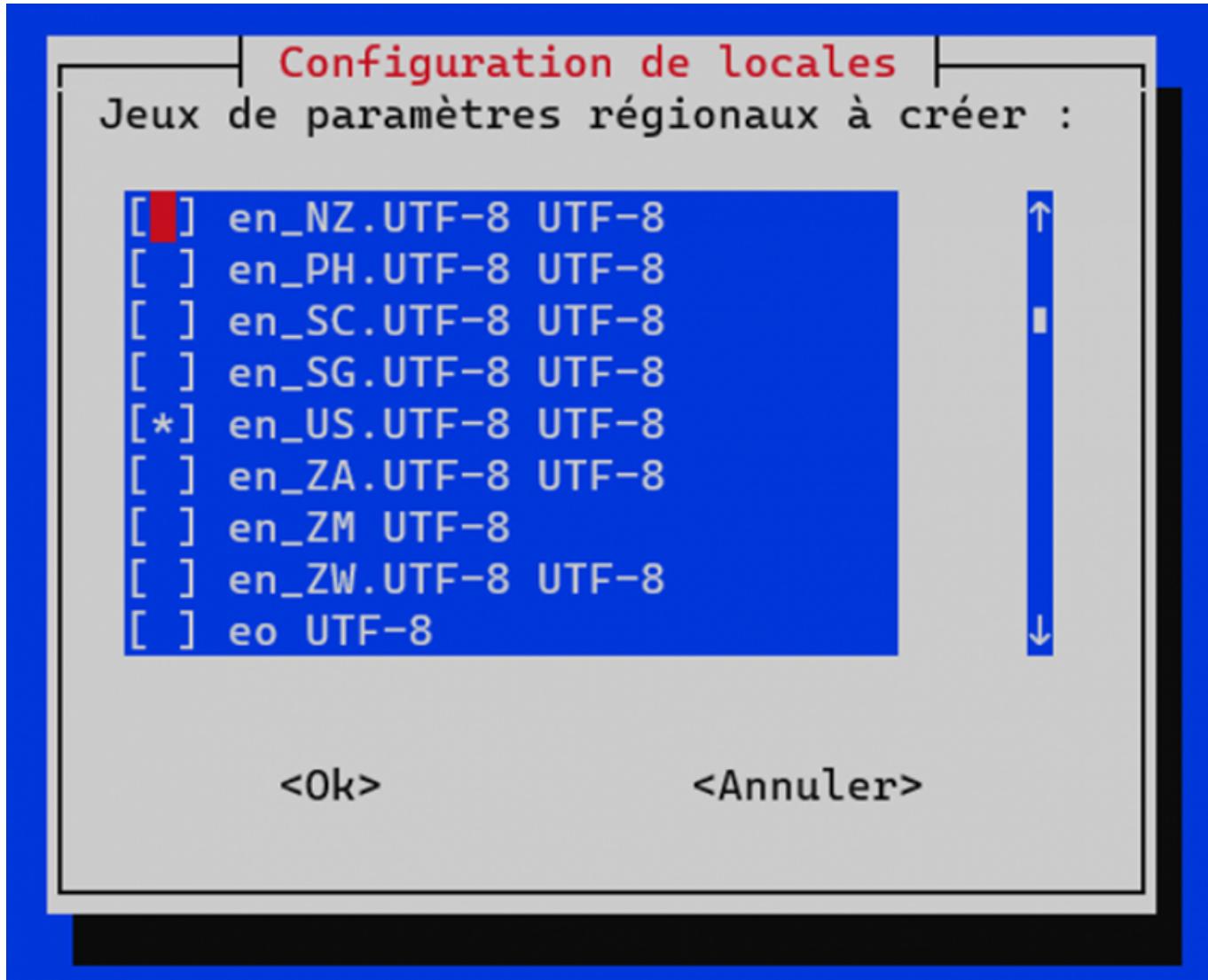
The screenshot shows the Zabbix Global view dashboard. On the left, there's a sidebar with navigation links: Dashboards, Monitoring, Services, Inventory, Reports, Data collection, Alerts, Users, Administration, Support, Integrations, Help, User settings, and Sign out. The main area has a title "Global view". Below it, there are several cards with error notifications. One card says "Top hosts by CPU utilization" and another says "Host availability". There are also sections for "Problems by severity", "Current problems", and "System information". Each card contains a detailed error message about locale issues and a link to the Zabbix interface.

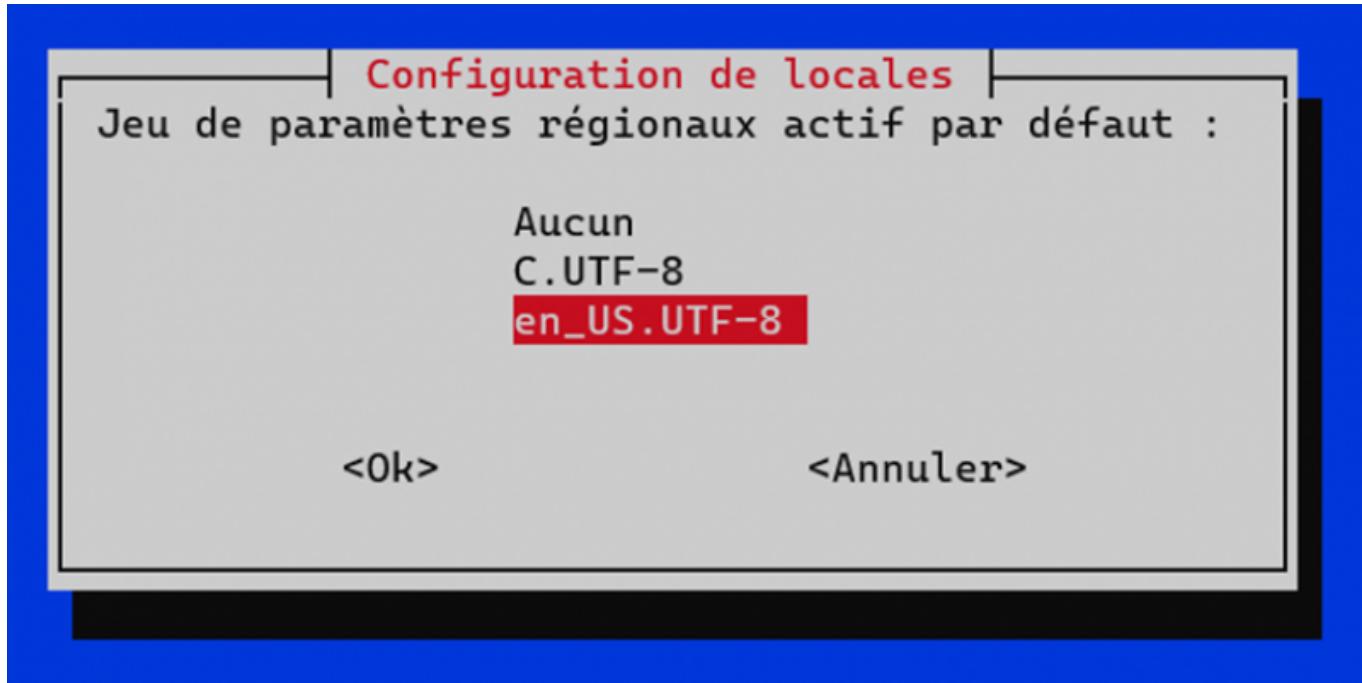
Pour ce faire, nous devons installer un nouveau paquet :

```
apt install locales
```



Nous choisissons les paramètres régionaux en\_US.UTF-8. Ce paramètre nous permettra d'enlever toutes les erreurs :





Nous entrons ensuite la commande suivante pour sauvegarder les changements :

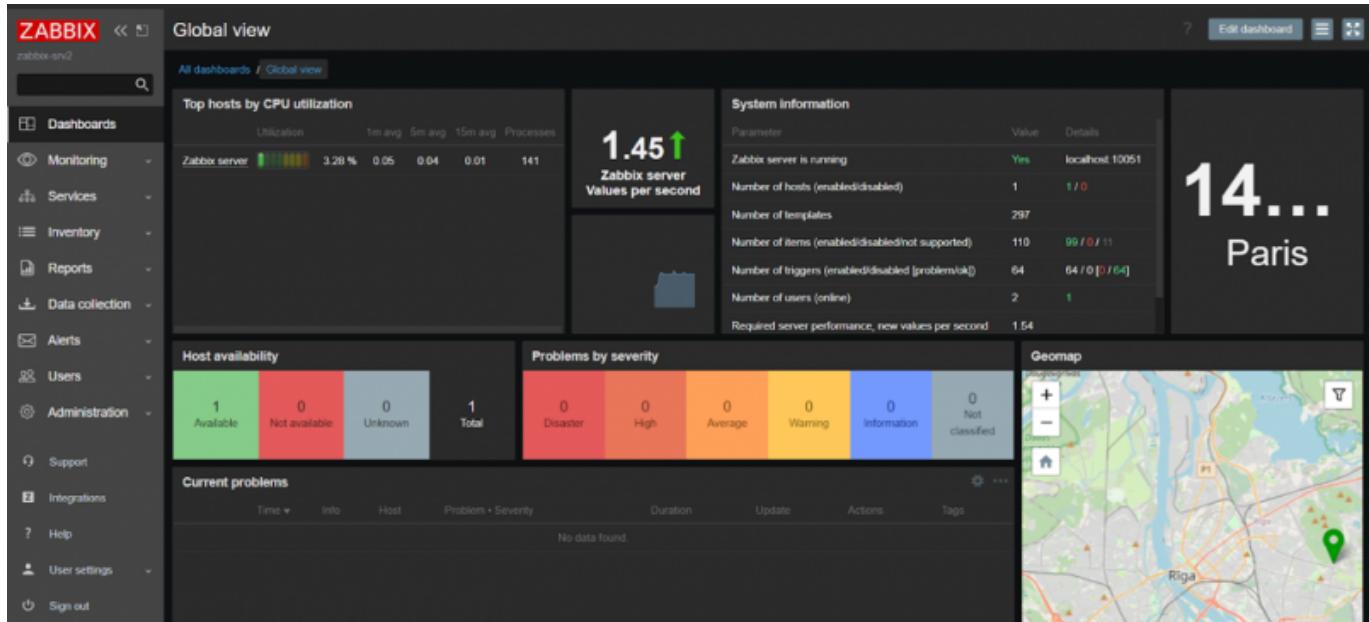
```
dpkg-reconfigure locales
```

```
root@zabbix-srv2:/etc# dpkg-reconfigure locales
Generating locales (this might take a while)...
    en_US.UTF-8... done
Generation complete.
```

Nous redémarrons le service zabbix\_server :

```
systemctl restart zabbix_server
```

Nous pouvons nous rendre dès à présent sur notre tableau de bord.



</panel> <panel type="info" title="III) Mise en place de la supervision">

## A) Installation de l'agent sur la machine à moniturer

Nous pouvons maintenant installer le dépôt officiel de Zabbix :

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

```
root@srv-web2-1:~# wget https://repo.zabbix.com/zabbix/6.4/debian/pool/main/z/zabbix-release/zabbix-release_6.4-1+debian
12_all.deb
--2023-12-18 14:57:27-- https://repo.zabbix.com/zabbix/6.4/debian/pool/main/z/zabbix-release/zabbix-release_6.4-1+debia
n12_all.deb
Résolution de repo.zabbix.com (repo.zabbix.com)... 178.128.6.101, 2604:a880:2:d0::2062:d001
Connexion à repo.zabbix.com (repo.zabbix.com)|178.128.6.101|:443... connecté.
requête HTTP transmise, en attente de la réponse... 200 OK
Taille : 3540 (3,5K) [application/octet-stream]
Sauvegarde en : « zabbix-release_6.4-1+debian12_all.deb »

zabbix-release_6.4-1+debian12 100%[=====] 3,46K --.-KB/s   0s
2023-12-18 14:57:28 (109 MB/s) - « zabbix-release_6.4-1+debian12_all.deb » sauvegardé [3540/3540]
```

Nous dépaquetons le dépôt officiel de Zabbix :

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

```
root@srv-web2-1:~# dpkg -i zabbix-release_6.4-1+debian12_all.deb
Sélection du paquet zabbix-release précédemment désélectionné.
(Lecture de la base de données... 44530 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de zabbix-release_6.4-1+debian12_all.deb ...
Dépaquetage de zabbix-release (1:6.4-1+debian12) ...
Paramétrage de zabbix-release (1:6.4-1+debian12) ...
```

```
apt update && apt upgrade
apt install zabbix-agent2 zabbix-agent2-plugin-*
```

Nous modifions le fichier de configuration zabbix\_agent2.conf. Nous entrons l'adresse IP de notre serveur Zabbix :

Server=10.31.178.200

ServerActive=10.31.178.200

```
##### Passive checks related

### Option: Server
#      List of comma delimited IP addresses, optionally in CIDR notation,
#      Incoming connections will be accepted only from the hosts listed here.
#      If IPv6 support is enabled then '127.0.0.1', '::127.0.0.1', '::ffff:127.0.0.1'
#      and '::/0' will allow any IPv4 or IPv6 address.
#      '0.0.0.0/0' can be used to allow any IPv4 address.
#      Example: Server=127.0.0.1,192.168.1.0/24,:1,2001:db8::/32,zabbix.
#
# Mandatory: yes
# Default:
# Server=

Server=10.31.178.200
```

```
##### Active checks related

### Option: ServerActive
#      Zabbix server/proxy address or cluster configuration to get active checks
#      Server/proxy address is IP address or DNS name and optional port separator
#      Cluster configuration is one or more server addresses separated by semicolon
#      Multiple Zabbix servers/clusters and Zabbix proxies can be specified
#      More than one Zabbix proxy should not be specified from each Zabbix server
#      If Zabbix proxy is specified then Zabbix server/cluster for that proxy is used
#      Multiple comma-delimited addresses can be provided to use several instances of a proxy
#      If port is not specified, default port is used.
#      IPv6 addresses must be enclosed in square brackets if port for that proxy is specified
#      If port is not specified, square brackets for IPv6 addresses are optional
#      If this parameter is not specified, active checks are disabled.
# Example for Zabbix proxy:
#     ServerActive=127.0.0.1:10051
# Example for multiple servers:
#     ServerActive=127.0.0.1:20051,zabbix.domain,[::1]:30051,::1,127.0.0.2:40051
# Example for high availability:
#     ServerActive=zabbix.cluster.node1;zabbix.cluster.node2:20051
# Example for high availability with two clusters and one server:
#     ServerActive=zabbix.cluster.node1;zabbix.cluster.node2:20051

#
# Mandatory: no
# Default:
# ServerActive=

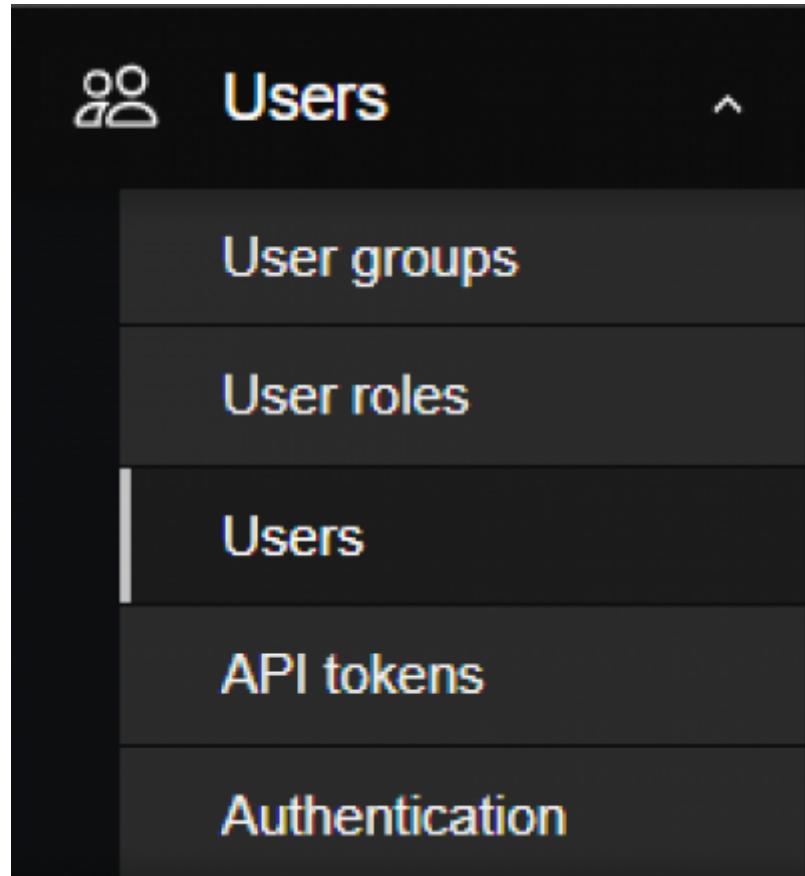
ServerActive=10.31.178.200
```

Nous pouvons redémarrer notre service :

```
systemctl restart zabbix_agent2
```

## B) Configuration de Zabbix

Nous pouvons maintenant créer un nouvel utilisateur. Pour cela, nous allons dans le menu des utilisateurs :



Users												Info
<input type="button" value="Create user"/> <input type="button" value="Filter"/>												
Username	Name	Last name	User role	Groups	Is online?	Login	Frontend access	API access	Debug mode	Status	Provisioned	Info
Admin	Zabbix	Administrator	Super admin role	Internal, Zabbix administrators	Yes (2023-12-19 13:30:16)	Ok	Internal	Enabled	Disabled	Enabled		
guest			Guest role	Disabled, Guests, Internal	No	Ok	Internal	Disabled	Disabled	Disabled		

Users												Info
<input checked="" type="checkbox"/> User added <input type="button" value="Create user"/> <input type="button" value="Filter"/>												
Username	Name	Last name	User role	Groups	Is online?	Login	Frontend access	API access	Debug mode	Status	Provisioned	Info
Admin	Zabbix	Administrator	Super admin role	Internal, Zabbix administrators	Yes (2023-12-19 13:30:16)	Ok	Internal	Enabled	Disabled	Enabled		
guest			Guest role	Disabled, Guests, Internal	No	Ok	Internal	Disabled	Disabled	Disabled		

Nous créons un nouvel utilisateur qui aura pour rôle “Super admin role”. Nous cliquons donc sur le bouton Create User.

Username	Name	Last name	User role	Groups	Is online?	Login	Frontend access	API access	Debug mode	Status	Provisioned	Info
Admin	Zabbix	Administrator	Super admin role	Internal, Zabbix administrators	Yes (2023-12-21 09:39:23)	Ok	Internal	Enabled	Disabled	Enabled		
guest			Guest role	Disabled, Guests, Internal	No	Ok	Internal	Disabled	Disabled	Disabled		
Lude			Super admin role	Zabbix administrators	No	Ok	System default	Enabled	Disabled	Enabled		

Hosts

Host groups: type here to search

Status: Any Enabled Disabled

Monitored by: Any Server Proxy

Name:

DNS:

IP:

Port:

Proxy:

Tags: And/Or Or

Add tag: tag:  Contains  Remove

Apply  Reset

## page des hôtes ^

New host

Host  IPMI  Tags  Macros  Inventory  Encryption  Value mapping

\* Host name: web-pub

Visible name: web-pub

Templates: Linux by Zabbix agent

\* Host groups: Virtual machines

Interfaces

Type	IP address	DNS name	Connect to	Port	Default
Agent	10.31.186.80		IP	10050	<input checked="" type="radio"/> Remove

Add

Description:

Monitored by proxy: (no proxy)

Add  Cancel

## création d'un hôte

Hosts

Host groups: type here to search

Status: Any Enabled Disabled

Monitored by: Any Server Proxy

Name:

DNS:

IP:

Port:

Proxy:

Tags: And/Or Or

Add tag: tag:  Contains  Remove

Apply  Reset

Name	Items	Triggers	Graphs	Discovery	Web	Interface	Proxy	Templates	Status	Availability	Agent encryption	Info	Tags
web-pub	Items 43	Triggers 15	Graphs 8	Discovery 3	Web	10.31.186.80:10050		Linux by Zabbix agent	Enabled	ZBX	None		
Zabbix server	Items 128	Triggers 69	Graphs 24	Discovery 5	Web	127.0.0.1:10050		Linux by Zabbix agent, Zabbix server health	Enabled	ZBX	None		

affichage des hôtes

The screenshot shows the 'Items' configuration page in Zabbix. The top navigation bar includes links for 'All hosts / web-pub', 'Enabled', 'ZBX', 'Items 67', 'Triggers 25', 'Graphs 13', 'Discovery rules 3', and 'Web scenarios'. The main form is for creating a new item:

- Name:** CPU Load
- Type:** Zabbix agent
- Key:** system.cpu.load
- Type of information:** Numeric (float)
- Host interface:** 10.31.186.80:10050
- Units:** (empty)
- Update interval:** 10s
- Custom intervals:** A table with one entry: Type: Flexible, Interval: 50s, Period: 1-7,00-00-24:00, Action: Remove. An 'Add' button is also present.
- History storage period:** Do not keep history, Storage period: 90d
- Trend storage period:** Do not keep trends, Storage period: 365d
- Value mapping:** type here to search
- Populates host inventory field:** -None-
- Description:** (empty text area)

création d'un item pour l'alerting

The screenshot shows the search interface in Zabbix, indicated by the 'Filter' button. The search criteria for the trigger creation are:

- Host groups:** type here to search
- Hosts:** web-pub
- Name:** (empty)
- Key:** (empty)
- Type:** all
- Type of information:** all
- History:** (empty)
- Trends:** (empty)
- Update interval:** (empty)
- Tags:** And/Or, Or
- Value mapping:** type here to search
- Tags:** tag Contains value
- State:** all, Normal, Not supported
- Status:** all, Enabled, Disabled
- Triggers:** all, Yes, No
- Inherited:** all, Yes, No
- Discovered:** all, Yes, No

item ajouter

The screenshot shows the Zabbix navigation bar with the following items:

- web-pub
- Items 68
- Triggers 26
- Graphs 13
- Discovery 3
- Web
- 10.31.186.80:10050
- Zabbix server
- Items 128
- Triggers 69
- Graphs 24
- Discovery 5
- Web
- 127.0.0.1:10050

triggers pour les hôte (alerte)

## Triggers

All hosts / web-pub   Enabled   ZBX   Items 68   Triggers 25   Graphs 13   Discovery rules 3   Web scenarios

**Trigger**   Tags   Dependencies

\* Name: CPU Load

Event name: CPU Load

Operational data:

Severity: Not classified   Information   Warning   Average   High   Disaster

\* Expression: avg(/web-pub/system.cpu.load,5s)>5   **Add**

OK event generation: Expression   Recovery expression   None

PROBLEM event generation mode: Single   Multiple

OK event closes: All problems   All problems if tag values match

Allow manual close:

Menu entry name: ? Trigger URL

Menu entry URL:

Description:

création d'un triggers pour un hote

**Condition**

\* Item: web-pub: CPU Load   **Select**

Function: avg() - Average value of a period T

\* Last of (T): 5s   Time

Time shift: now-h   Time

\* Result: > 5

**Insert**   **Cancel**

condition du trigger

The screenshot shows the 'Trigger added' dialog box in Zabbix. It includes a header with 'All hosts / web-pub' and 'Enabled'. Below the header are several search and filter fields:

- Host groups:** A search field with placeholder 'type here to search' and a 'Select' button.
- Hosts:** A search field with placeholder 'web-pub X' and a 'Select' button.
- Name:** An empty text input field.
- Tags:** A dropdown menu set to 'And/Or' with an 'Add' button.
- Inherited:** Buttons for 'all', 'Yes', and 'No'.
- Severity:** Buttons for 'Not classified', 'Warning', 'High', 'Information', 'Average', and 'Disaster'.
- Discovered:** Buttons for 'all', 'Yes', and 'No'.
- With dependencies:** Buttons for 'all', 'Yes', and 'No'.
- State:** Buttons for 'all', 'Normal', and 'Unknown'.
- Status:** Buttons for 'all', 'Enabled', and 'Disabled'.
- Value:** Buttons for 'all', 'Ok', and 'Problem'.

At the bottom are 'Apply' and 'Reset' buttons.

triggers ajouté

The screenshot shows the 'Users' dialog box in Zabbix. It lists users with columns for Username, Name, and Last name:

Username	Name	Last name
Admin	Zabbix	Administrator
guest		
Lucie		

At the bottom are 'Select' and 'Cancel' buttons.

user

The screenshot shows the 'New action' dialog box in Zabbix. It has tabs for 'Action' (selected) and 'Operations 2'. The 'Action' tab contains:

- Name:** CPU Load
- Conditions:** A table with one row labeled 'Label' and 'Add'.
- Enabled:** A checked checkbox.
- A note: 'At least one operation must exist.'

At the bottom are 'Add' and 'Cancel' buttons.

trigger action

New action

Action Operations 2

\* Default operation step duration 1h

Operations	Steps	Details	Start in	Duration	Action
	1	Send message to users: Lucie via Discord	Immediately	Default	<a href="#">Edit</a> <a href="#">Remove</a>
	<a href="#">Add</a>				
Recovery operations		Details			Action
		Send message to users: Lucie via Discord			<a href="#">Edit</a> <a href="#">Remove</a>
	<a href="#">Add</a>				
Update operations		Details			Action
	<a href="#">Add</a>				
Pause operations for symptom problems	<input checked="" type="checkbox"/>				
Pause operations for suppressed problems	<input checked="" type="checkbox"/>				
Notify about canceled escalations	<input checked="" type="checkbox"/>				
* At least one operation must exist.					

[Add](#) [Cancel](#)

trigger action operation

Operation details

Operation Send message

Steps 1 - 1 (0 - infinitely)

Step duration 0 (0 - use action default)

\* At least one user or user group must be selected.

Send to user groups  [Select](#)

Send to users  [Select](#)

Send only to

Custom message

Conditions

Label	Name	Action
<a href="#">Add</a>		

[Add](#) [Cancel](#)

detail operation trigger

## Operation details

Operation **Send message**

\* At least one user or user group must be selected.

Send to user groups	<input type="text" value="type here to search"/>	<b>Select</b>
Send to users	<b>Lucie</b> <span style="color: red;">X</span> <input type="text" value="type here to search"/>	<b>Select</b>
Send only to	<b>Discord</b>	<span style="color: blue;">▼</span>
Custom message	<input type="checkbox"/>	

**Add** **Cancel**

### detail operation trigger suite

Trigger actions				
<input checked="" type="checkbox"/> Action added				
Name	<input type="text"/>	Status	Any	Enabled
		Apply	Reset	
Name	Conditions	Operations	Status	
CPU Load		Send message to users: Lucie via Discord	Enabled	
Report problems to Zabbix administrators		Send message to user groups: Zabbix administrators via all media	Enabled	

action ajouté



# Administration



General >

Audit log

Housekeeping

Proxies

Macros

Queue >

sidebar pour les macro

Macro	Value	Description	
{\$SNMP_COMMUNITY}	public	T description	<a href="#">Remove</a>
{\$ZABBIX_URL}	http://10.31.178.50/zabbix	T description	<a href="#">Remove</a>

Add      Update

ajout des macro pour message discord

Macros updated

Macro	Value	Description	
{\$SNMP_COMMUNITY}	public	T description	<a href="#">Remove</a>
{\$ZABBIX_URL}	http://10.31.178.50/zabbix	T description	<a href="#">Remove</a>

Add      Update

ajout des macro pour message discord

**Edit widget**

Type: Top hosts

Name: Top hosts by CPU utilization

Refresh interval: 10 seconds

Host groups: type here to search [Select](#)

Hosts: Zabbix server [X](#) web-pub [X](#) type here to search [Select](#)

Host tags: And/Or    Or

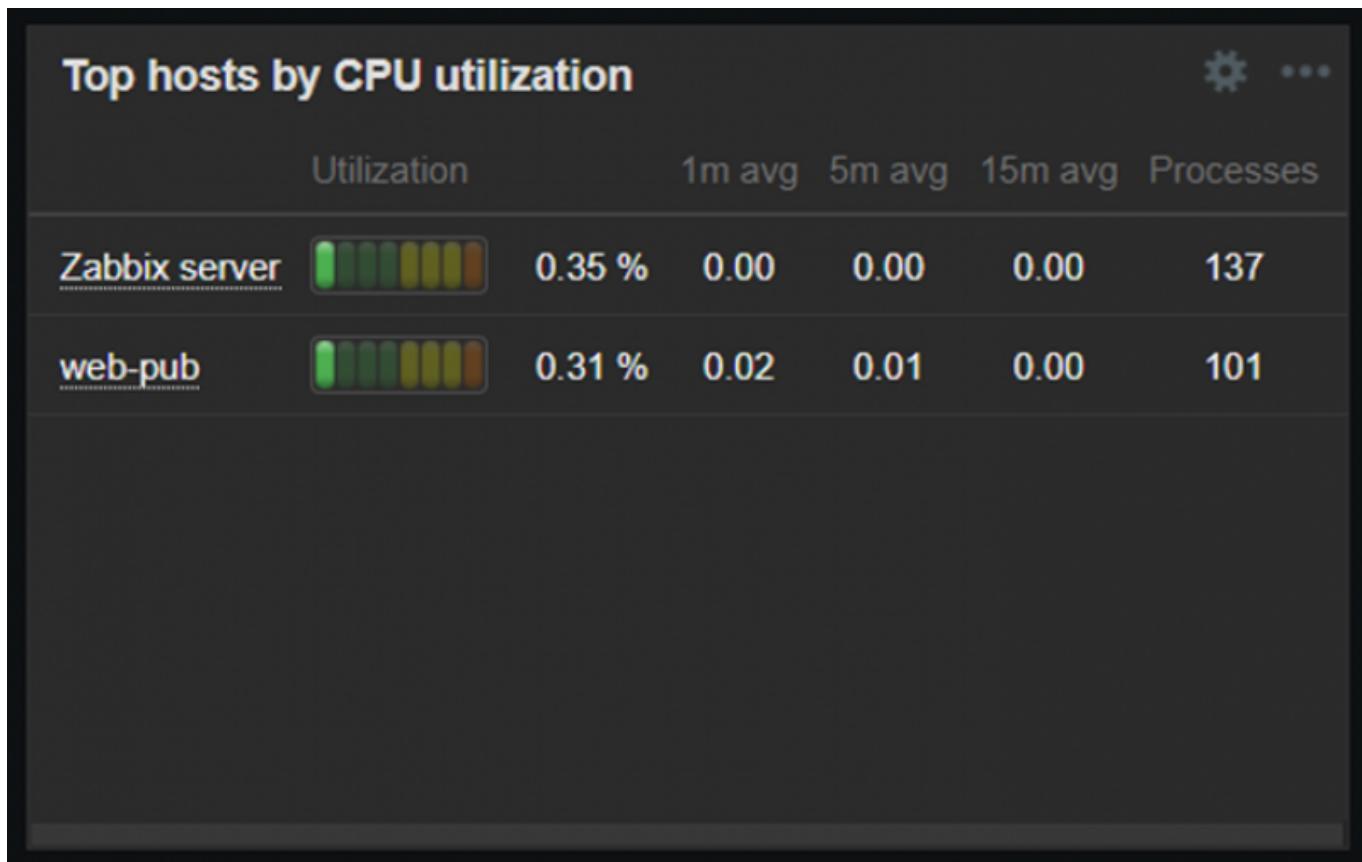
Columns:

Name	Data	Action
Host name	Host name	<a href="#">Edit</a> <a href="#">Remove</a>
Utilization	Linux: CPU utilization	<a href="#">Edit</a> <a href="#">Remove</a>
1m avg	Linux: Load average (1m avg)	<a href="#">Edit</a> <a href="#">Remove</a>
5m avg	Linux: Load average (5m avg)	<a href="#">Edit</a> <a href="#">Remove</a>
15m avg	Linux: Load average (15m avg)	<a href="#">Edit</a> <a href="#">Remove</a>
Processes	Linux: Number of processes	<a href="#">Edit</a> <a href="#">Remove</a>

Columns: [Add](#)

Apply      Cancel

configuration dashboard



dashboard avant test

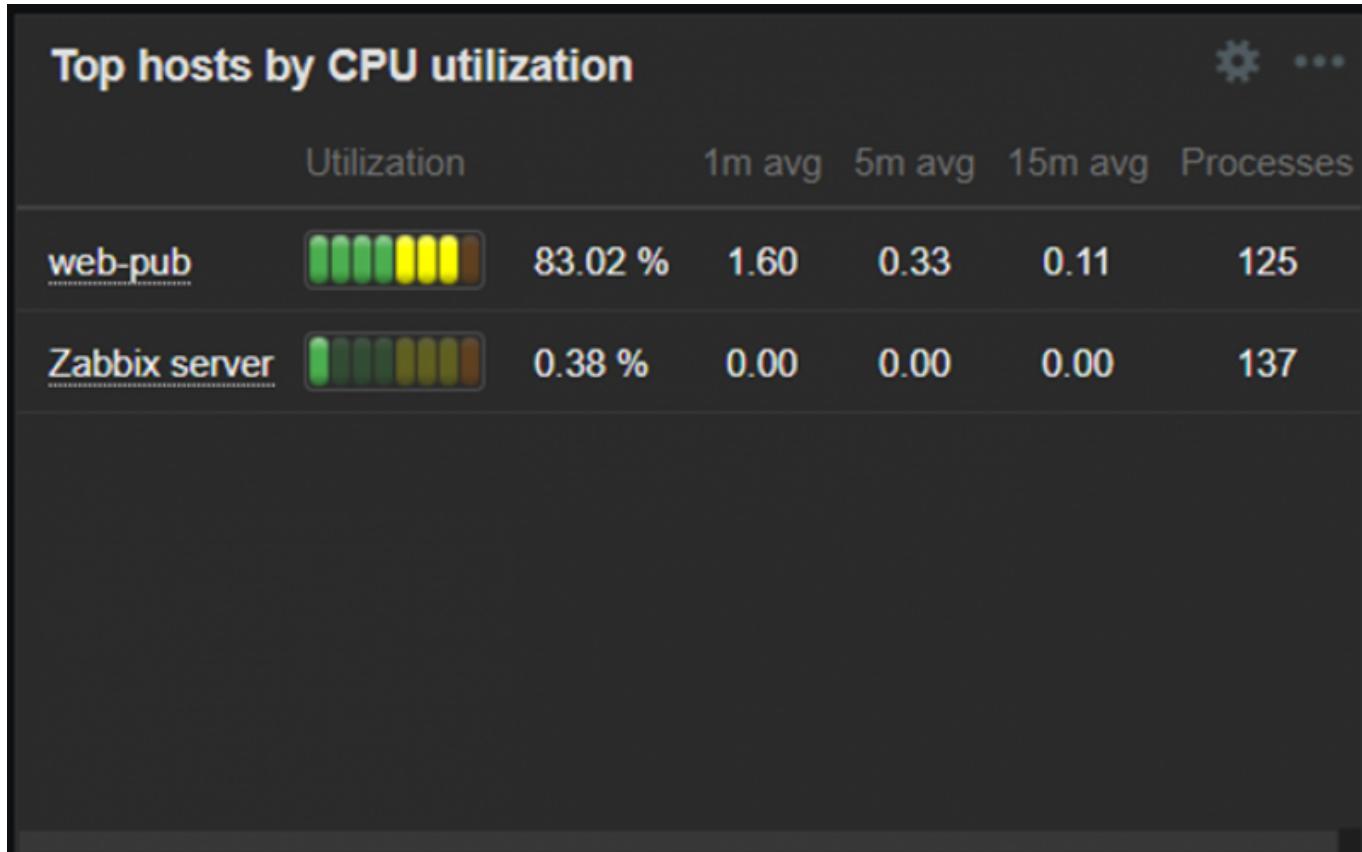
```
root@srv-web2-1:~# stress --cpu 20
stress: info: [123356] dispatching hogs: 20 cpu, 0 io, 0 vm, 0 hdd
^C
root@srv-web2-1:~#
```

test stress cpu

```
top - 14:11:32 up 34 days, 22:18, 4 users, load average: 10,43, 6,23, 2,84
Tâches: 106 total, 1 en cours, 105 en veille, 0 arrêté, 0 zombie
%Cpu(s): 0,0 ut, 0,0 sy, 0,0 ni,100,0 id, 0,0 wa, 0,0 hi, 0,0 si, 0,0
MiB Mem : 1966,9 total, 528,4 libr, 589,9 util, 1116,3 tresp/cache
MiB Éch : 975,0 total, 975,0 libr, 0,0 util. 1377,0 dispo Mem
```

PID	UTIL.	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TEMPS+	COM.
-----	-------	----	----	------	-----	-----	---	------	------	--------	------

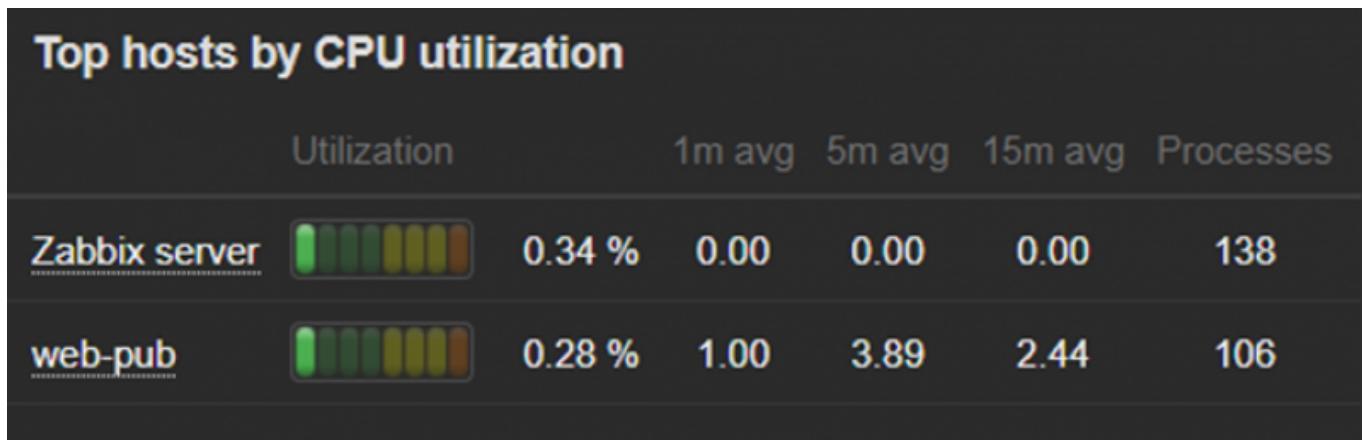
stress cpu



dashboard pendant le test

Current problems							
Time	Info	Host	Problem • Severity	Duration	Update	Actions	Tags
14:06:12		web-pub	CPU Load	38s	Update		

alerte dans zabbix



dashboard après le test

From:  
<https://sisr2.beaupeyrat.com/> - Documentations SIO2 option SISR

Permanent link:  
[https://sisr2.beaupeyrat.com/doku.php?id=sisr2-asie:sp2\\_lucie](https://sisr2.beaupeyrat.com/doku.php?id=sisr2-asie:sp2_lucie)

Last update: 2024/05/30 11:50



