Install Zabbix

Welcome to our install guide of the Zabbix monitoring service! In these 7 steps we will tell you how you can prepare your Zabbix master, how you can configure the Zabbix web interface, how to prepare your Zabbix client, add them to the web interface and how you can use notifications.

1) Install apache, mysql and php op Zabbix Server

   For this first task, you will need a full operating LAMP stack. This is an acronym. First of all, you'll need Linux. We will use Ubuntu server 18.04 for this example. Secondly, you'll need Apache, which is a webserver. This is used for the Zabbix web interface. Next, we will use MySQL, because Zabbix uses a database. Finally, you'll need to install PHP.

   Installing Apache and Updating the Firewall

   We always start off with updating all available packages so we're sure we have the latest packages:

   Sudo apt-get update

   Sudo apt-get upgrade

   Now we can install the apache package!

   Sudo apt-get install apache2

   Done? It's possible you've enabled the UFW firewall. This needs to allow http and https traffic. Check if UFW has an application profile for Apache:

   sudo ufw app list

   You should get an output like this:

```
zabbix@zabbix:~$
zabbix@zabbix:~$ sudo ufw app list
Available applications:
  Apache
  Apache Full
  Apache Secure
  OpenSSH
zabbix@zabbix:~$
```

   You can type in the next command to see which ports are enabled for traffic:

   sudo ufw app info "Apache Full"

   You should get an output like this:

```
zabbix@zabbix:~$
zabbix@zabbix:~$
zabbix@zabbix:~$ sudo ufw app info "Apache Full"
Profile: Apache Full
Title: Web Server (HTTP,HTTPS)
Description: Apache v2 is the next generation of the omnipresent Apache web
server.

Ports:
  80,443/tcp
zabbix@zabbix:~$
```

You can see it allows TCP ports 80 and 443. Those are for HTTP and HTTPS. Now it's important to allow this traffic:
sudo ufw allow in "Apache Full"
Okay, so if everything went right, you should be able to visit your IP address in a web browser. Just type in:
http://[your ip here]
You should now see the Apache 2 default webpage! Congrats!

Installing MySQL
Now we will install the database management system "MySQL". Type in the next command:
sudo apt install mysql-server
When the installation is complete, you can run a security script. This one is already installed and removes non-secure defaults and locks down access to the database:
sudo mysql_secure_installation + '*y*' + *1*
For the other questions being asked, you can just press y!
Now you can test if what you've done, went well. Use this command to see if everything worked:
sudo mysql
You should get an output like this:

```
zabbix@zabbix:~$
zabbix@zabbix:~$ sudo mysql
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 4
Server version: 5.7.30-0ubuntu0.18.04.1 (Ubuntu)

Copyright (c) 2000, 2020, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

The last rule is the most important: mysql>. This means you're in the mysql prompt!

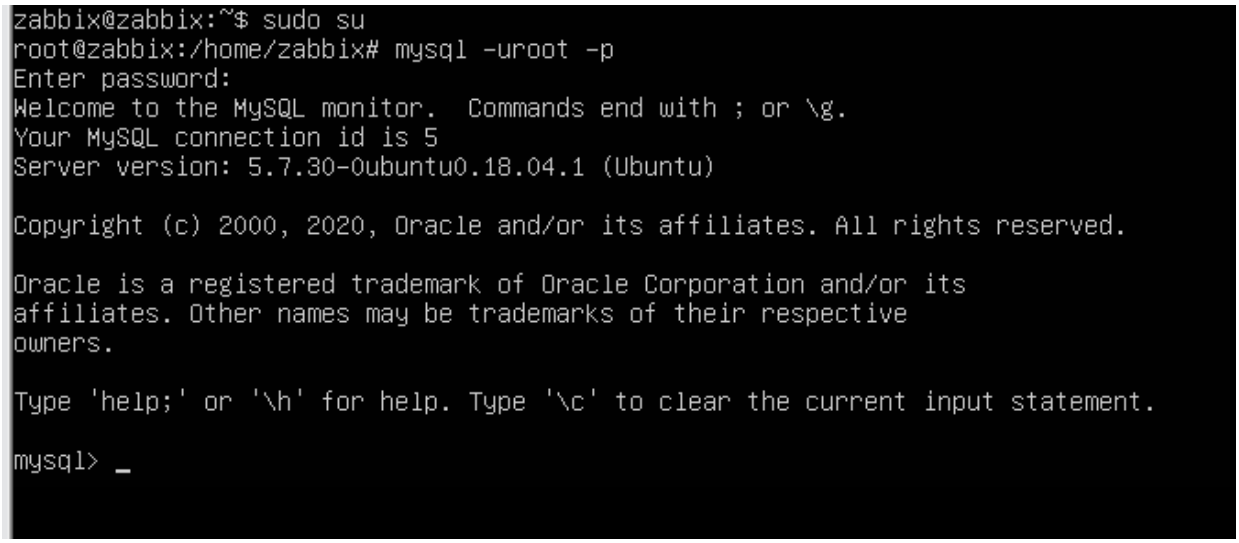
Installing PHP
The last part includes installing PHP. You only need one command for this one:
Sudo apt install php libapache2-mod-php php-mysql

2) Install Zabbix server
Great, you've done excellent work already. Now it's time to install the Zabbix server on the virtual machine on which you previously installed the LAMP stack. There is a package ready in Linux, but apparently it's outdated, so we won't be using that one. Instead, we'll use the "official Zabbix repository":

wget https://repo.zabbix.com/zabbix/4.2/ubuntu/pool/main/z/zabbix-release/zabbix-release_4.2-1+bionic_all.deb
sudo dpkg -i zabbix-release_4.2-1+bionic_all.deb
It's important to update the packages so the new repository is added:
sudo apt update
Now you can install the Zabbix server and the web frontend:
sudo apt install zabbix-server-mysql zabbix-frontend-php
You can also install the Zabbix agent. This makes it possible to collect data about the Zabbix server status:
sudo apt install zabbix-agent

3) Configuring MySQL database for Zabbix

Did you think you were already done? Wrong! It's time to setup a database now that will collect data from its agents. First we will change ourselves to the root account:
Sudo su
Now you can log into MySQL. You're required to type the password you've inserted in the MySQL server installation:
Mysql -uroot -p
This should be the result:



Now we will write some sql code!
First we'll create the Zabbix database with UTF-8 character support:
Create database Zabbix character set utf8 collate utf8_bin;
Now we'll create a user that the server will use. We will give it access to the new database and set the password:
Grant all privileges on Zabbix. to zabbix@localhost identified by 'Abcd1234!';*
Apply these permissions by typing in the next command:
Flush privileges;
Great, you can now exit the database!
Quit;

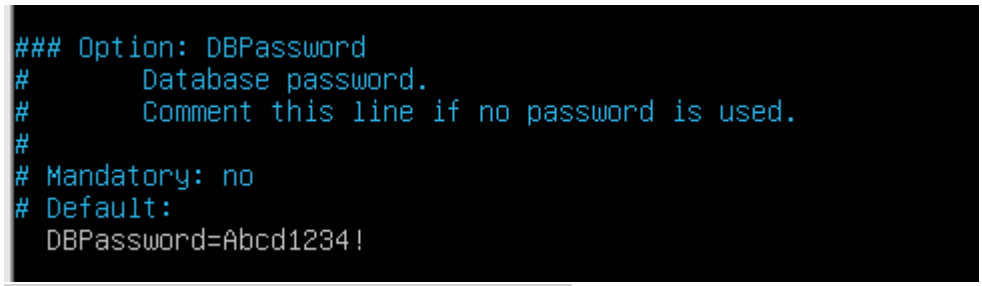
So, it's time to import the initial schema and data. Don't worry, there's already a file for that. You can just type in the next command:

zcat /usr/share/doc/zabbix-server-mysql/create.sql.gz | mysql -uzabbix -p Zabbix

In order to use this database, you'll need to edit this file:

sudo nano /etc/zabbix/zabbix_server.conf

Now find this part in that file and edit this:



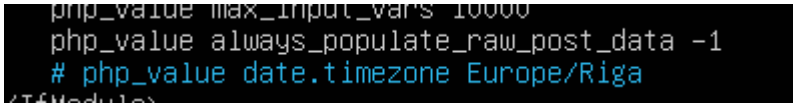
DBPassword=your_zabbix_mysql_password

4) <u>Configure PHP for Zabbix</u>

We need to create a small readjustment for the time settings. Start by opening this file:

Sudo nano /etc/zabbix/apache.conf

In here, you need to change a line. It's normally a comment line:



Remove the comment line, and change it to your own timezone!

Once done, you need to restart Apache to apply this setting:

sudo systemctl restart apache2

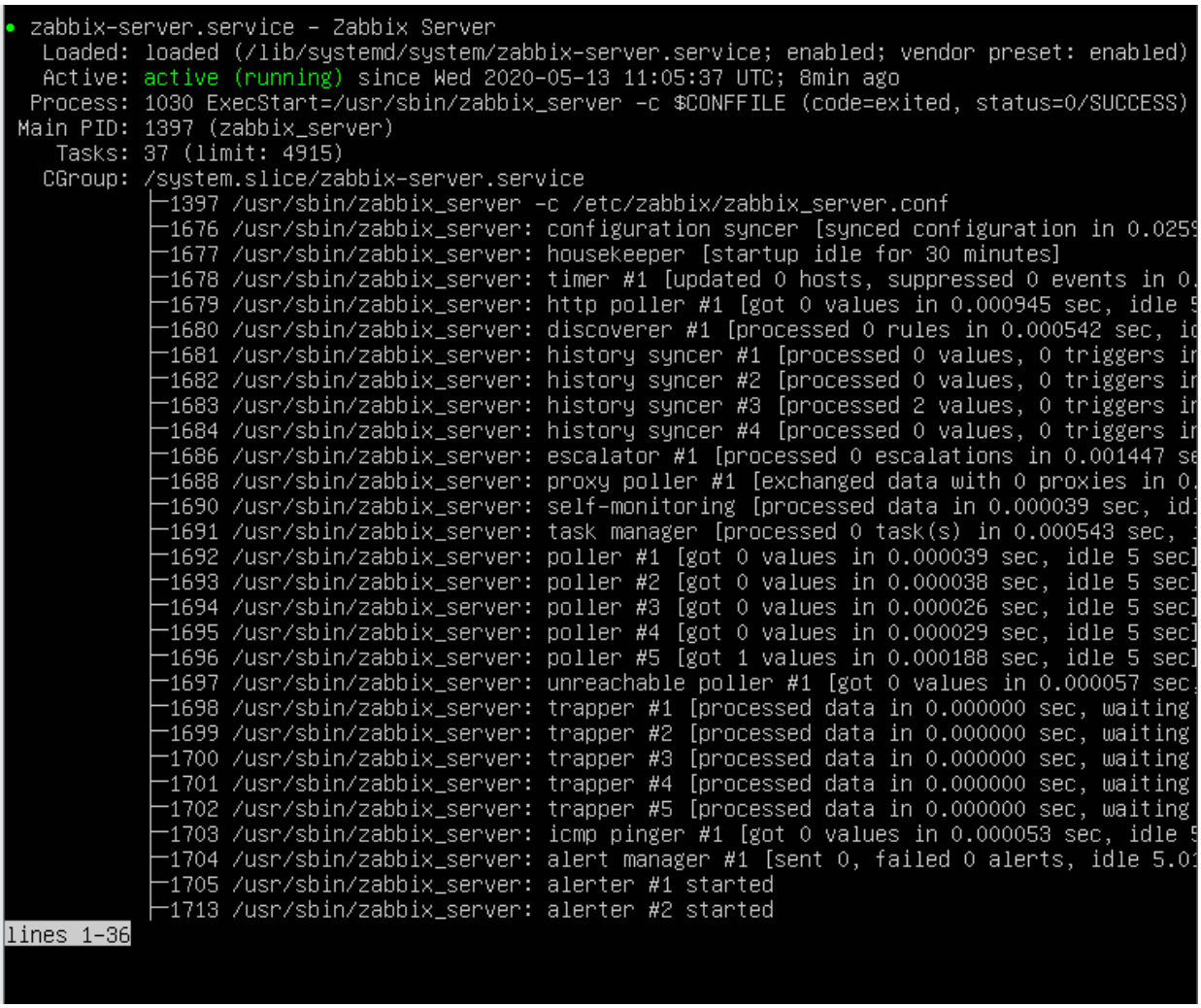
And also start the Zabbix server:

sudo systemctl start Zabbix-server

Now it's time to see if the Zabbix server is running by typing in the following command:

sudo systemctl status zabbix-server

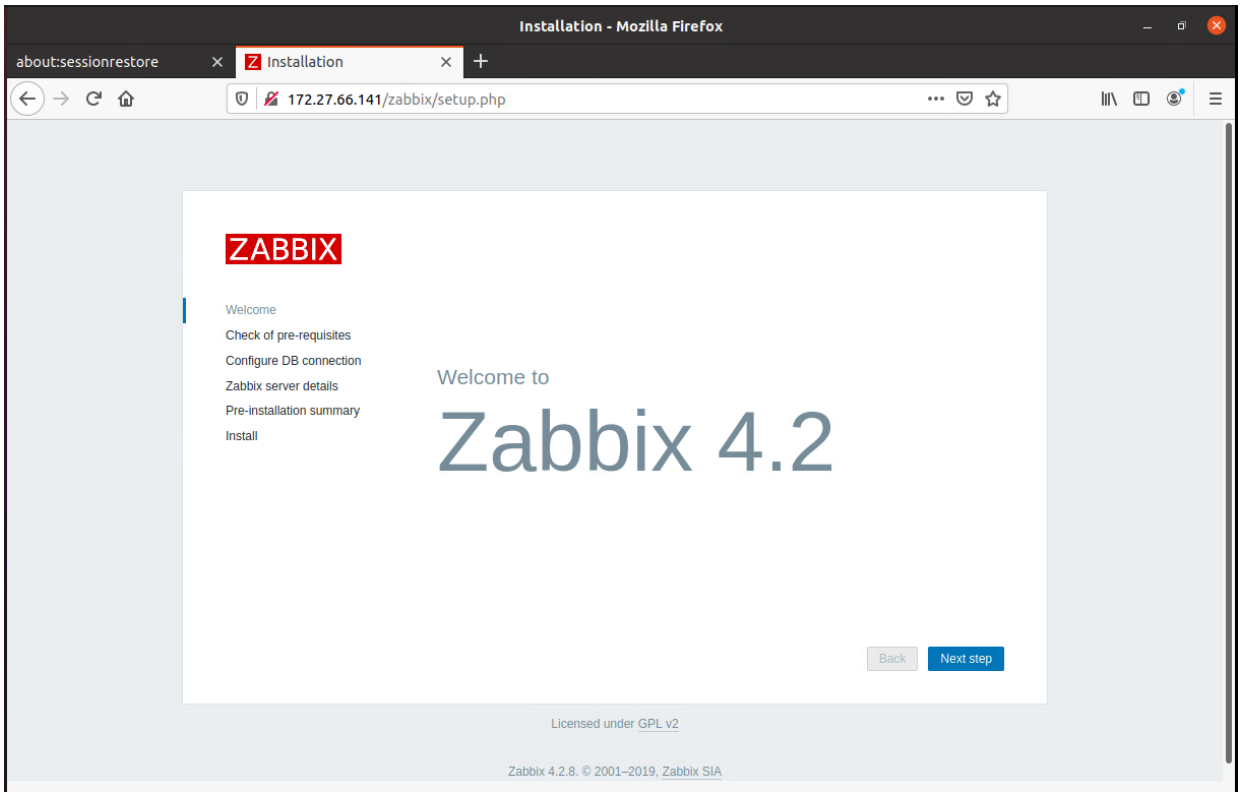
If everything worked correctly, you should have the following output:



The last step here is to enable the server at boot time:
sudo systemctl enable zabbix-server

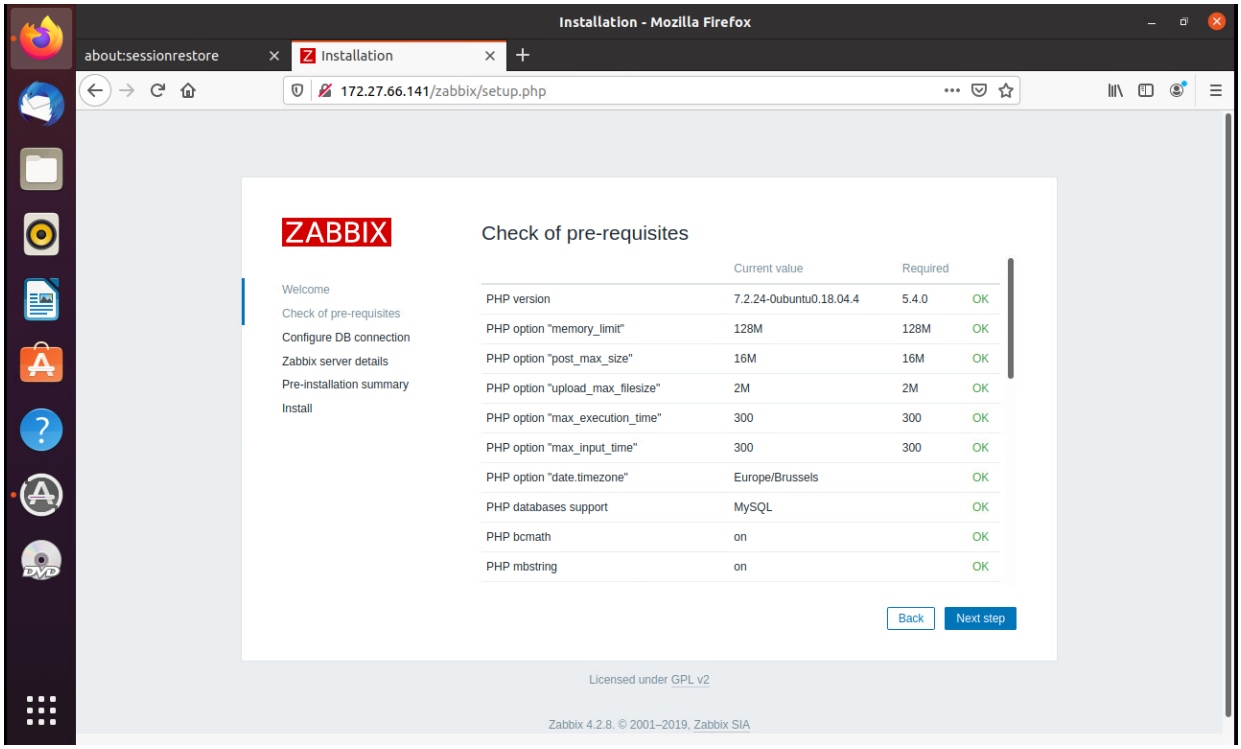
5) Configuring Settings for the Zabbix Web Interface

For this part, we will only need to work on the GUI of Linux. You need another machine which has a GUI with for example Firefox. First start with connecting to the web interface! The Zabbix_server_name is the ip address of the Zabbix server you've created in the previous steps. In our case it's 172.27.66.141:
http://zabbix_server_name/zabbix/

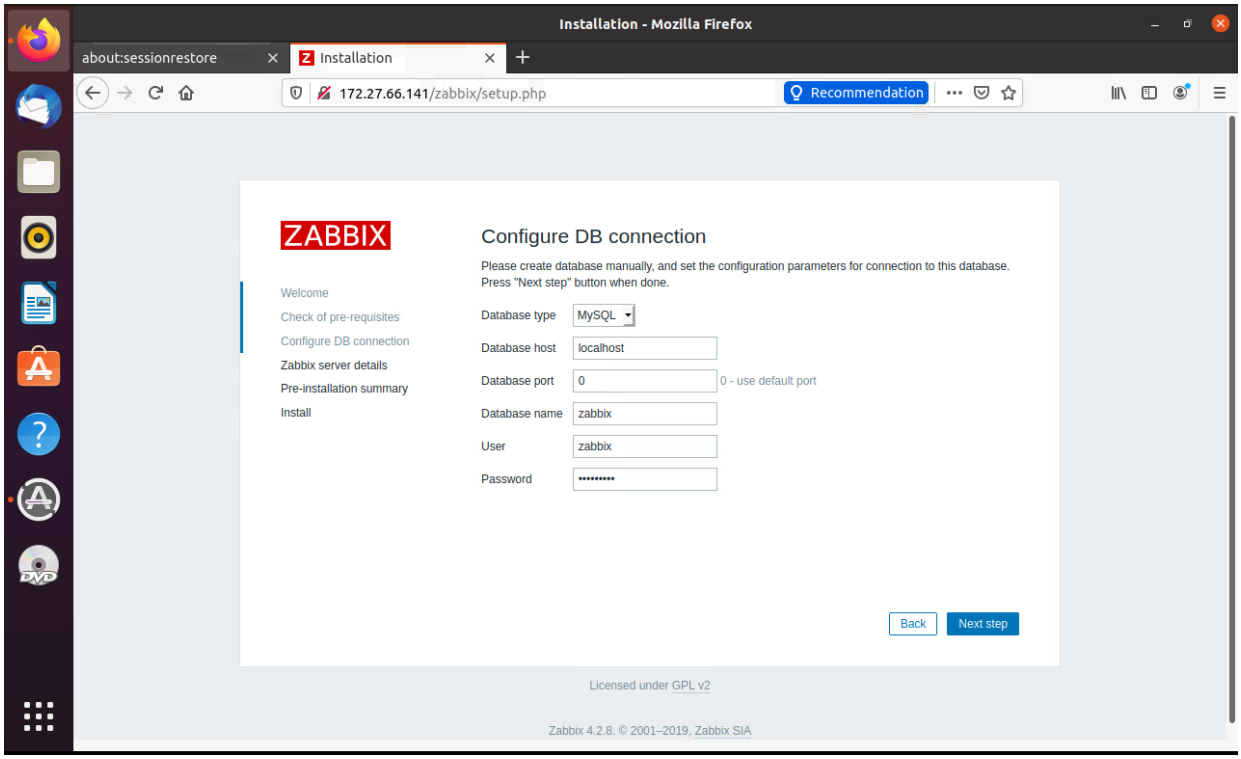


You can just click next there.

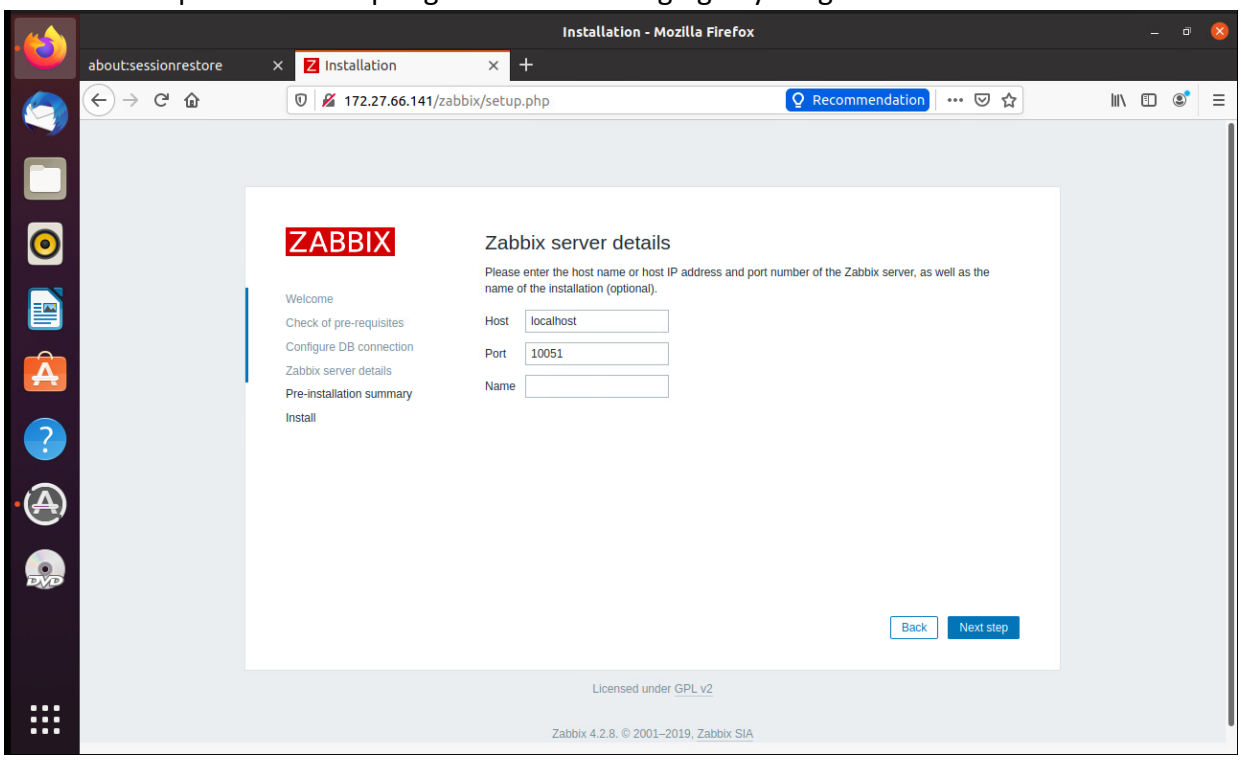
On the next screen, you will see of list of prerequisites to run Zabbix. If all of them have a green “ok” behind them, you’re safe to press “next step” on the bottom right corner.



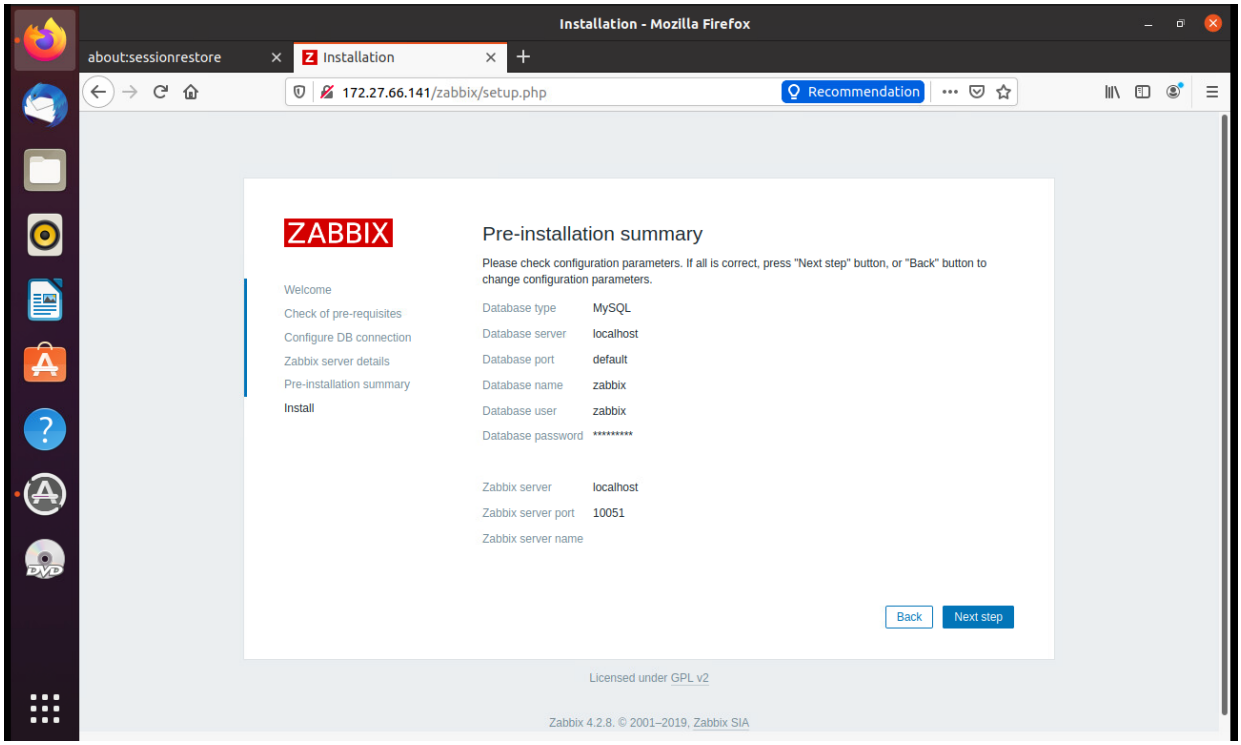
The next screen asks for a database connection. You need to type in your username and password for the user you've created in step 3. After you've filled in the correct credentials, you can press "next step" again.



The next screen is about the Zabbix server details. The name is completely optional. You can now press "next step" again without changing anything.



The next screen shows a summary. Confirm if all the details are right. If so, you can proceed to the next step.



The installation is now complete!
You can login with these credentials:

Username: Admin
Password: zabbix

6) Installing and Configuring the Zabbix Agent

Okay, we've installed the master server and connected to the GUI! Now it's time to add our first Zabbix Agent to monitor. For this part, I've created a new Ubuntu 18.04 server.

Agent install

First start off with installing the repository configuration package:

wget https://repo.zabbix.com/zabbix/4.2/ubuntu/pool/main/z/zabbix-release/zabbix-release_4.2-1+bionic_all.deb

sudo dpkg -i zabbix-release_4.2-1+bionic_all.deb

Remember to always update the packages!

Sudo apt update

Now install the Zabbix agent:

sudo apt install zabbix-agent

Encryption

It's possible to secure the connection between the server and the agent. To do this, we first need to generate a PSK (pre-shared keys):

sudo sh -c "openssl rand -hex 32 > /etc/zabbix/zabbix_agentd.psk"

The key is stored in the /etc/Zabbix/Zabbix_agentd.psk file. Remember this file, because we will need it. The result should be something like this:

```
agent@agent:~$ sudo sh -c "openssl rand -hex 32 > /etc/zabbix/zabbix_agentd.psk"
agent@agent:~$ cat /etc/zabbix/zabbix_agentd.psk
141ef38f4b95a4f02821fd312df983338ec7b8d7a5ef351d7af19922172ee19f
agent@agent:~$ _
```

Now it's time to edit the Zabbix agent settings because these are still the default settings. You can open them with nano:

sudo nano /etc/zabbix/zabbix_agentd.conf

Here we need to edit a couple of things.

First, edit the IP address of the Zabbix server. Normally, this is still 127.0.0.1 Change it to the server's IP address.

```
### Option: Server
#       List of comma delimited IP addresses, optionally in CIDR notation, or DNS names of Zabb
#       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' are trea
#       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.example.com
#
# Mandatory: yes, if StartAgents is not explicitly set to 0
# Default:
# Server=

Server=172.27.66.141
```

Next you need to find the TLSConnect option. Change this to "*TLSConnect=PSK*".

```
### Option: TLSConnect
#       How the agent should connect to server or proxy. Used for active checks.
#       Only one value can be specified:
#               unencrypted - connect without encryption
#               psk         - connect using TLS and a pre-shared key
#               cert        - connect using TLS and a certificate
#
# Mandatory: yes, if TLS certificate or PSK parameters are defined (even for 'unencrypted' conn
# Default:
# TLSConnect=unencrypted
TLSConnect=psk
```

Next, it's time for the TLSAccept section. Change this one to *"TLSAccept=PSK"*.

```
### Option: TLSAccept
#       What incoming connections to accept.
#       Multiple values can be specified, separated by comma:
#               unencrypted - accept connections without encryption
#               psk         - accept connections secured with TLS and a pre-shared key
#               cert        - accept connections secured with TLS and a certificate
#
# Mandatory: yes, if TLS certificate or PSK parameters are defined (even for 'unencrypted' conn
# Default:
# TLSAccept=unencrypted
TLSAccept=psk_
```

We also need to create a unique name for the key you just generated. It's done with *"TLSPSKIdentity=name_of_choice"*.

```
### Option: TLSPSKIdentity
#       Unique, case sensitive string used to identify the pre-shared key.
#
# Mandatory: no
# Default:
# TLSPSKIdentity=
TLSPSKIdentity=PSK 001_
```

At last, we need to point the Zabbix agent to the location of where your PSK key is stored: *"TLSPSKFile=/etc/Zabbix/Zabbix_agentd.psk"*.

```
### Option: TLSPSKFile
#       Full pathname of a file containing the pre-shared key.
#
# Mandatory: no
# Default:
# TLSPSKFile=
TLSPSKFile=/etc/zabbix/zabbix_agentd.psk_
```

When this is done, save and close the file. Now we need to restart the service and make it start at boot time:

sudo systemctl restart zabbix-agent

sudo systemctl enable zabbix-agent

If all went well and you type in this command:

sudo systemctl status zabbix-agent

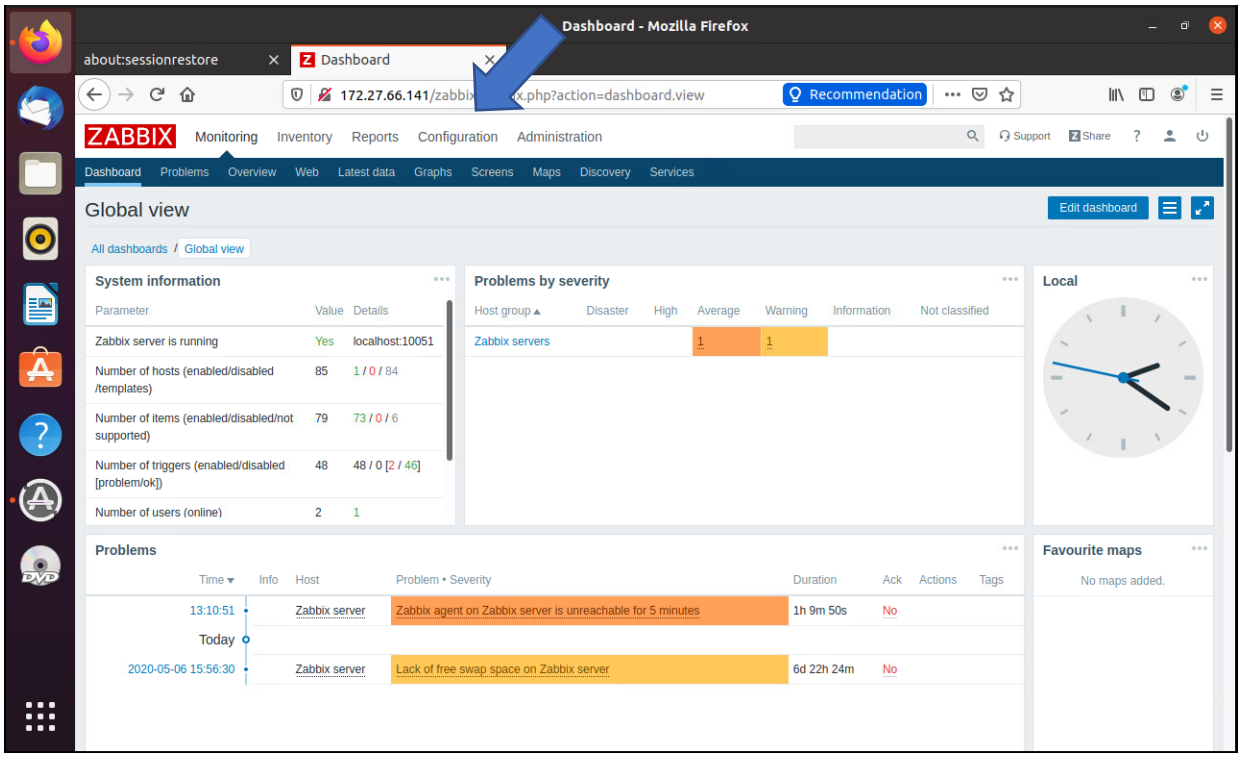
You will see that the agent service is running:

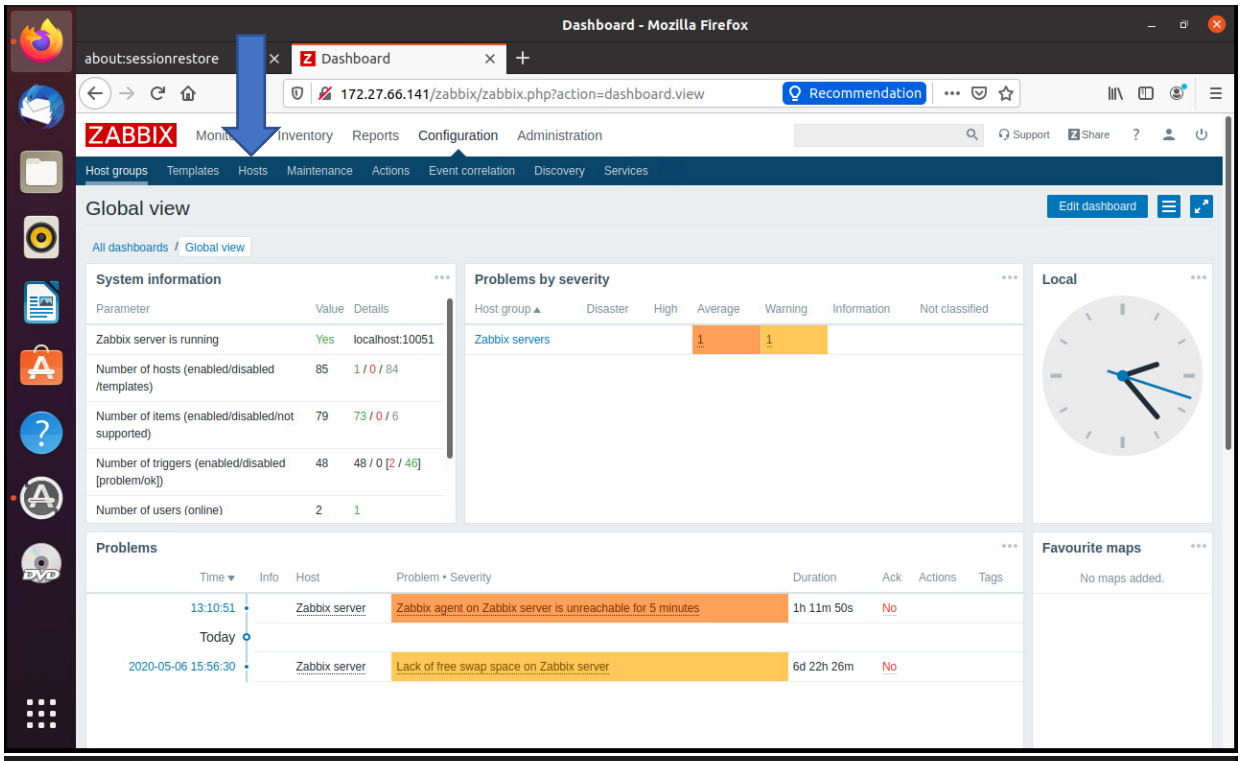
```
agent@agent:~$
agent@agent:~$ sudo systemctl restart zabbix-agent
agent@agent:~$ sudo systemctl enable zabbix-agent
Synchronizing state of zabbix-agent.service with SysV service script with /lib/systemd/systemd-
install.
Executing: /lib/systemd/systemd-sysv-install enable zabbix-agent
agent@agent:~$ sudo systemctl status zabbix-agent
● zabbix-agent.service - Zabbix Agent
   Loaded: loaded (/lib/systemd/system/zabbix-agent.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2020-05-13 12:13:31 UTC; 20s ago
 Main PID: 2685 (zabbix_agentd)
    Tasks: 6 (limit: 4915)
   CGroup: /system.slice/zabbix-agent.service
           ├─2685 /usr/sbin/zabbix_agentd -c /etc/zabbix/zabbix_agentd.conf
           ├─2687 /usr/sbin/zabbix_agentd: collector [idle 1 sec]
           ├─2688 /usr/sbin/zabbix_agentd: listener #1 [waiting for connection]
           ├─2689 /usr/sbin/zabbix_agentd: listener #2 [waiting for connection]
           ├─2690 /usr/sbin/zabbix_agentd: listener #3 [waiting for connection]
           └─2691 /usr/sbin/zabbix_agentd: active checks #1 [idle 1 sec]

May 13 12:13:31 agent systemd[1]: Starting Zabbix Agent...
May 13 12:13:31 agent systemd[1]: zabbix-agent.service: Can't open PID file /run/zabbix/zabbix_
May 13 12:13:31 agent systemd[1]: zabbix-agent.service: Supervising process 2685 which is not c
May 13 12:13:31 agent systemd[1]: Started Zabbix Agent.
lines 1-17/17 (END)
```

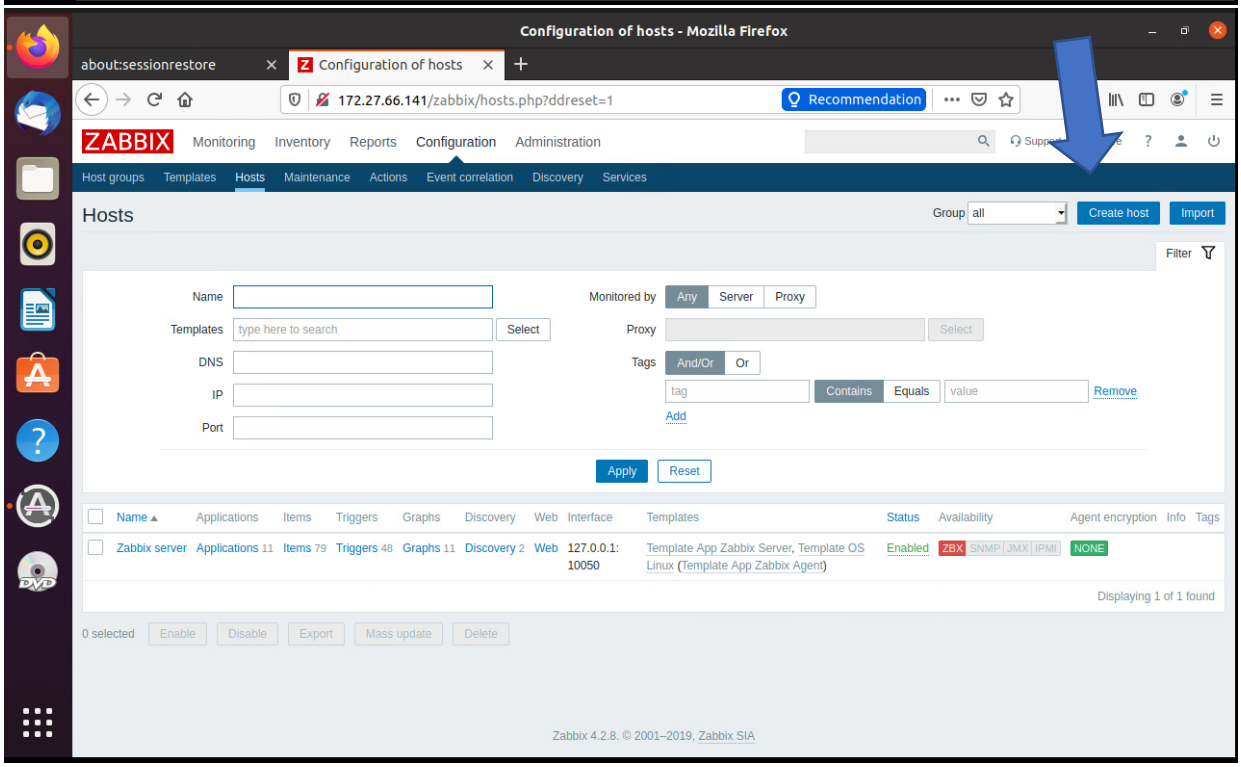
The last but least, you will need to open port 10050:
sudo ufw allow 10050/tcp
Now the agent is up and running!

7) Adding the new host to the Zabbix server

In this step we will add the agent to the Zabbix server, so we can monitor it.
We go back to the GUI. Now login with the default credentials. Right here, you have to click “Configuration” and then “Hosts”. Now click on the “Create host” button. Here we can add one.



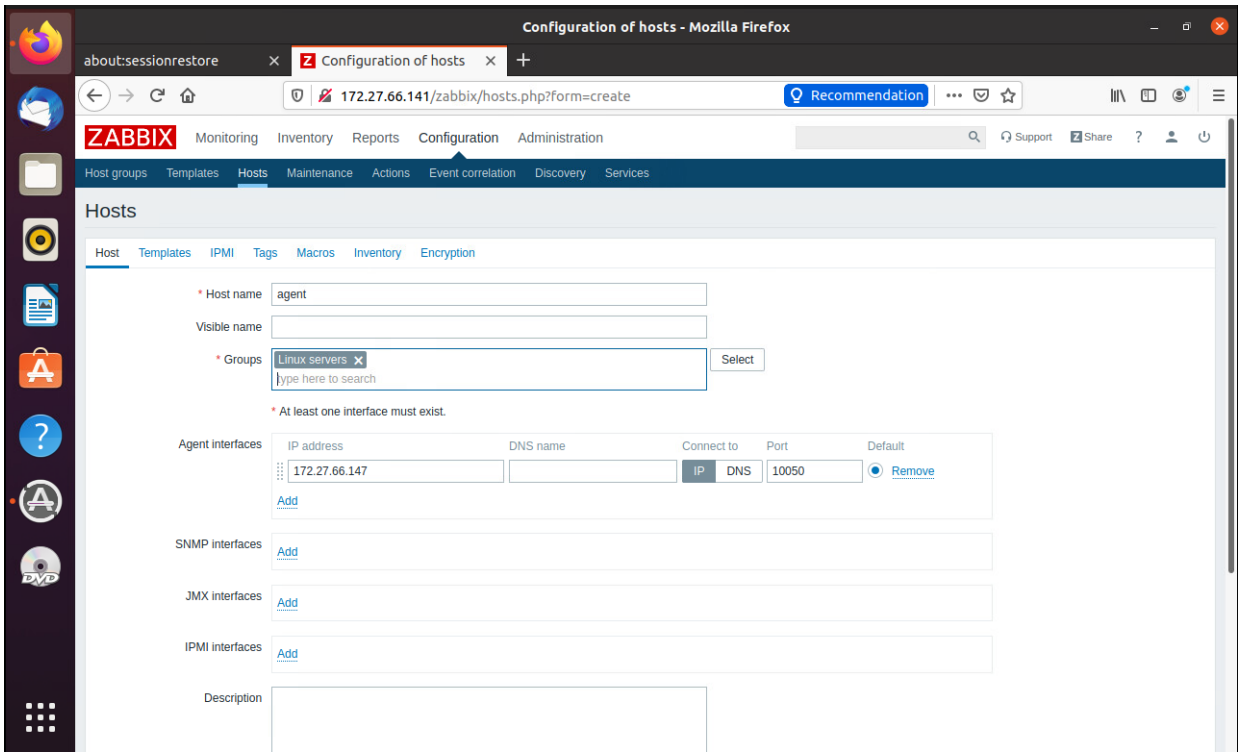




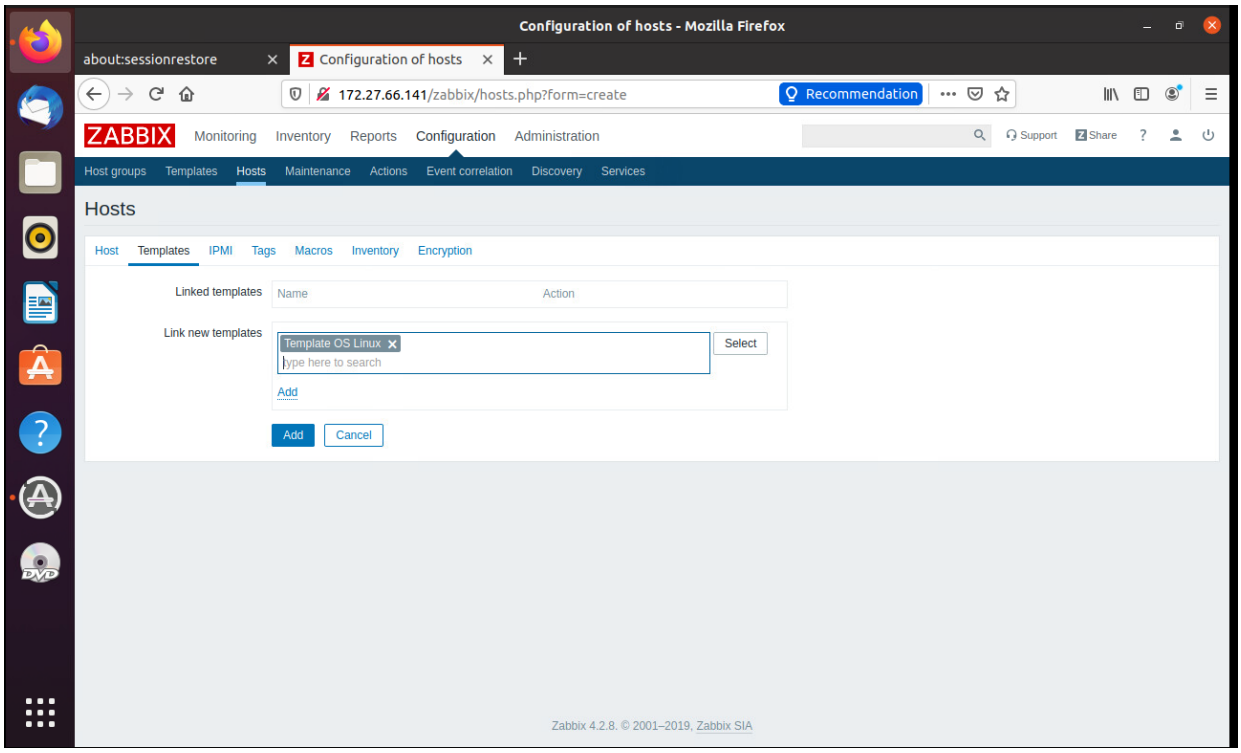
First adjust the hostname and the IP address of the agent. To find the host name on the agent, type:

Hostnamectl

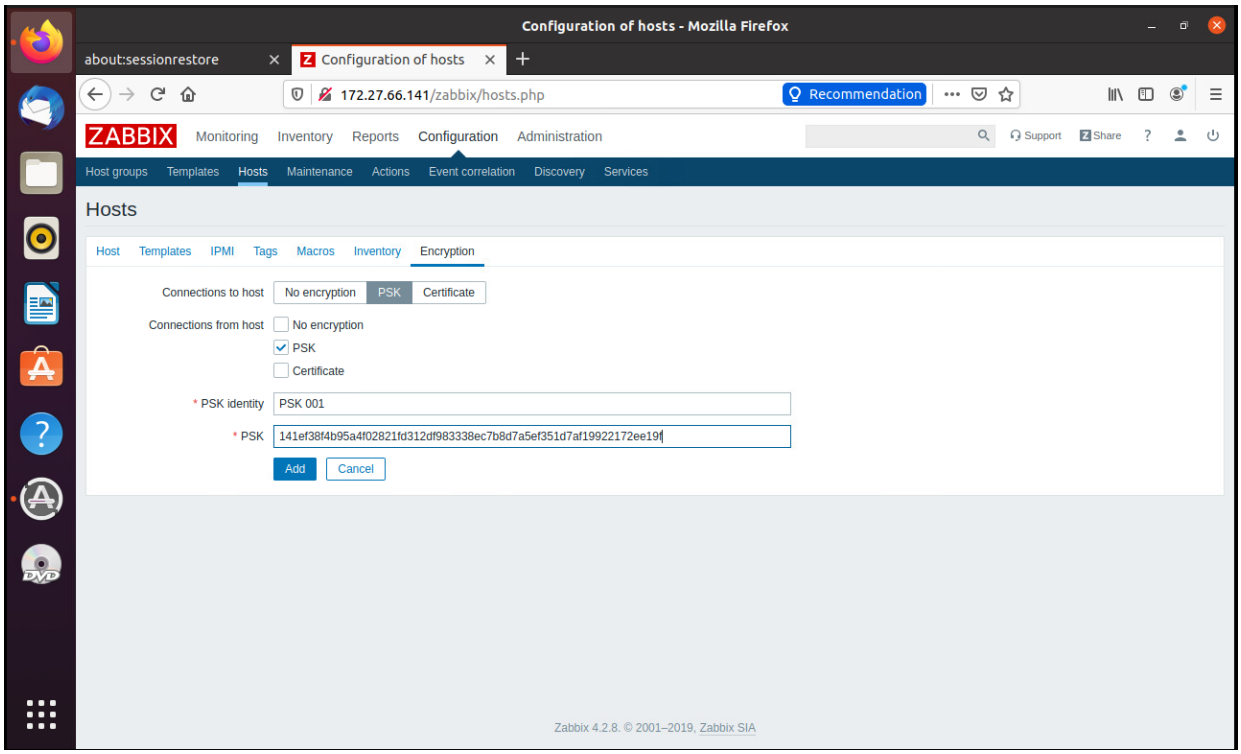
Now you can add this one to a group of your choice, or create a new one.



Done? Click now the templates tab. We've created a Linux vm, so we type *"Template OS Linux"* and click Add.



Finally we need to go the encryption tab. Select only PSK and set the PSK identity to the one you choose in the configuration file. Remember the generated key? You'll need to type in the PSK field. When you're ready, press Add.



You've officially added a new host to the Zabbix server.

8) <u>Configuring notifications</u>

Zabbix also uses something nice to use. You can use notifications for email when for example you're server doesn't work. First of all, you need to create an email account. For this tutorial, we'll use gmail.

Once done, we need to install ssmpt on the linux with GUI:

Sudo apt-get update

sudo apt-get install ssmtp

Now, we need to edit this file:

Sudo nano /etc/ssmtp/ssmtp.conf

You should change the settings to this:

```
  GNU nano 4.8                    /etc/ssmtp/ssmtp.conf
#
# Config file for sSMTP sendmail
#
# The person who gets all mail for userids < 1000
# Make this empty to disable rewriting.
root=gmail

# The place where the mail goes. The actual machine name is required no
# MX records are consulted. Commonly mailhosts are named mail.domain.com
mailhub=smtp.gmail.com:465
FromLineOverride=YES
AuthUser=gmail
AuthPass=wachtwoord
# Where will the mail seem to come from?
#rewriteDomain=

# The full hostname
UseTLS=YES

# Are users allowed to set their own From: address?

^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File  ^\ Replace   ^U Paste Text ^T To Spell  ^_ Go To Line
```

Change root to your gmail account, AuthUser to your gmail account and AuthPass to your email password!

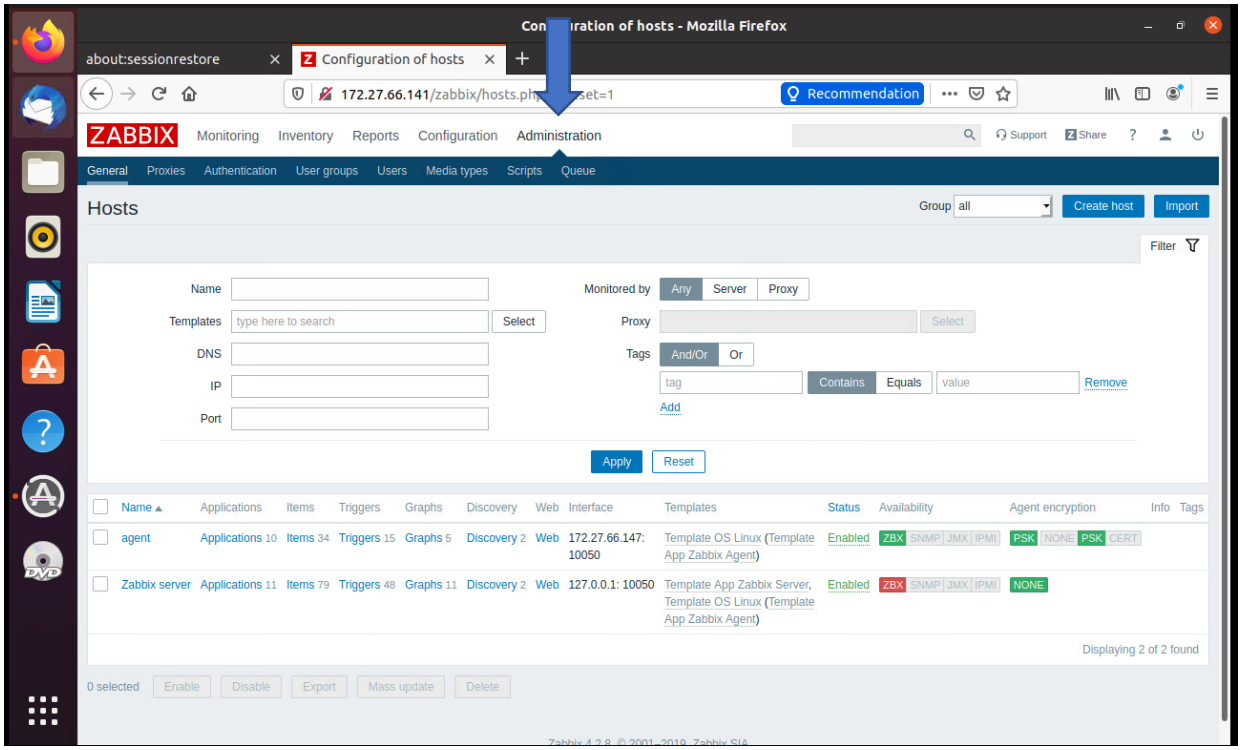
It's recommended to test this already out with the following command:

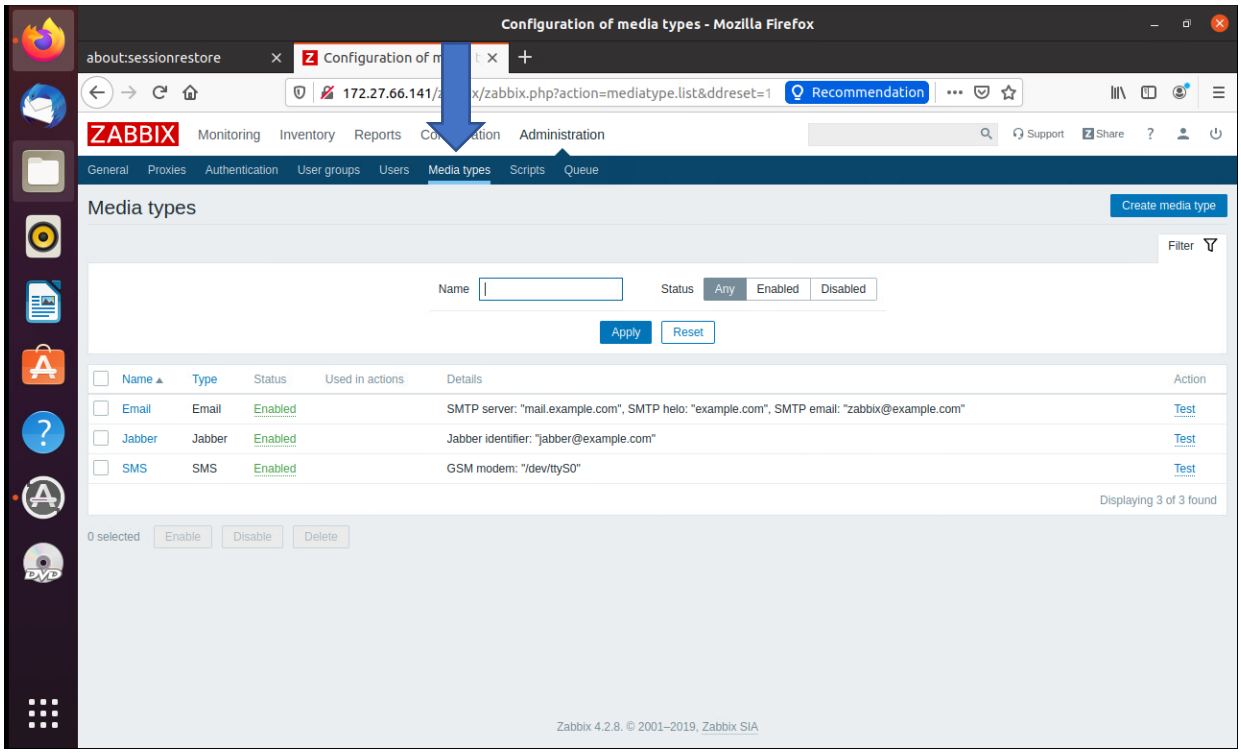
echo "E-Mail using the command-line" | ssmtp email@gmail.com

You should have received an email!

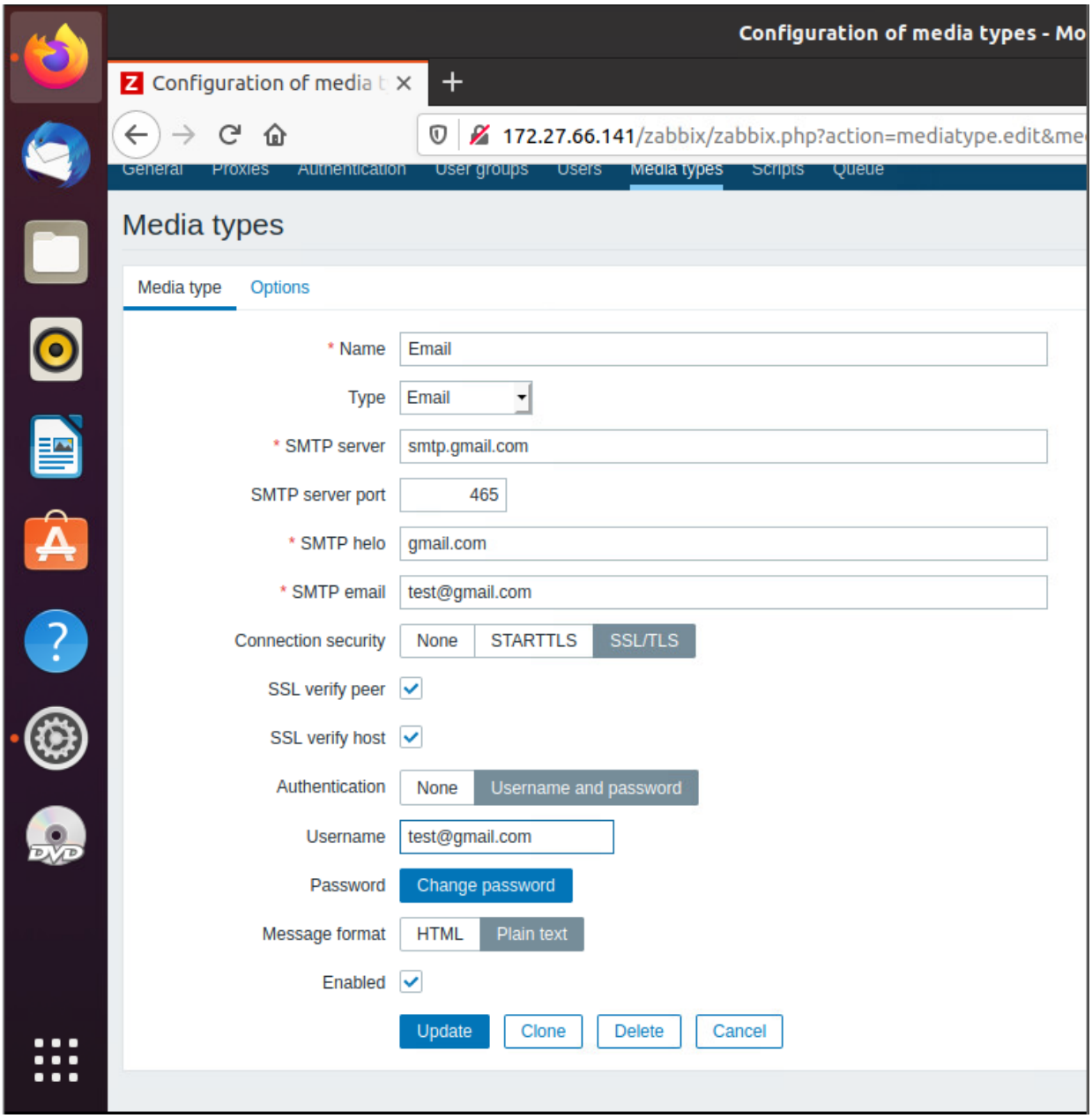
Now we are going to configure Zabbix, so an email will sent everytime something will go wrong.

To do so, click on administration and then media types:





In this screen, you can press email. You can adjust the settings here like I do in the screenshot! I use an outlook email:

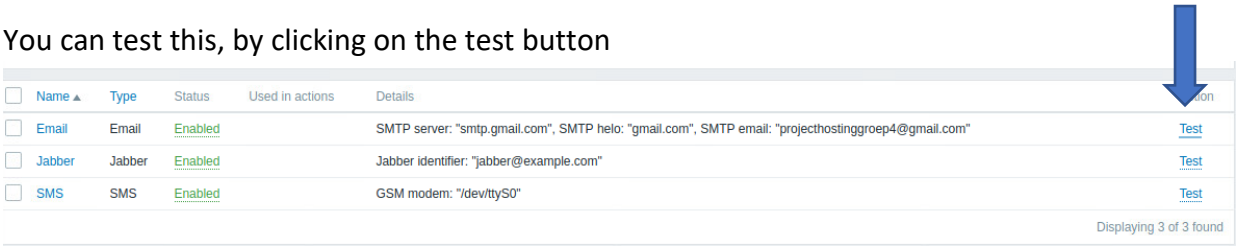


So what should we change?

- Name → Just give it a name, doesn't care what it is.
- Type → Should be email, obviously!
- SMTP server → This should be the smtp server of the mail service you're using. For gmail, it's "smtp.gmail.com".
- SMTP server port → This needs to be port 465
- SMTP helo → This is the domain name of your email.
- SMTP email → This is your email account
- Connection security → We would like to send the email over an SSL/TLS connection.
- Authentication → Use your username and password for your email.

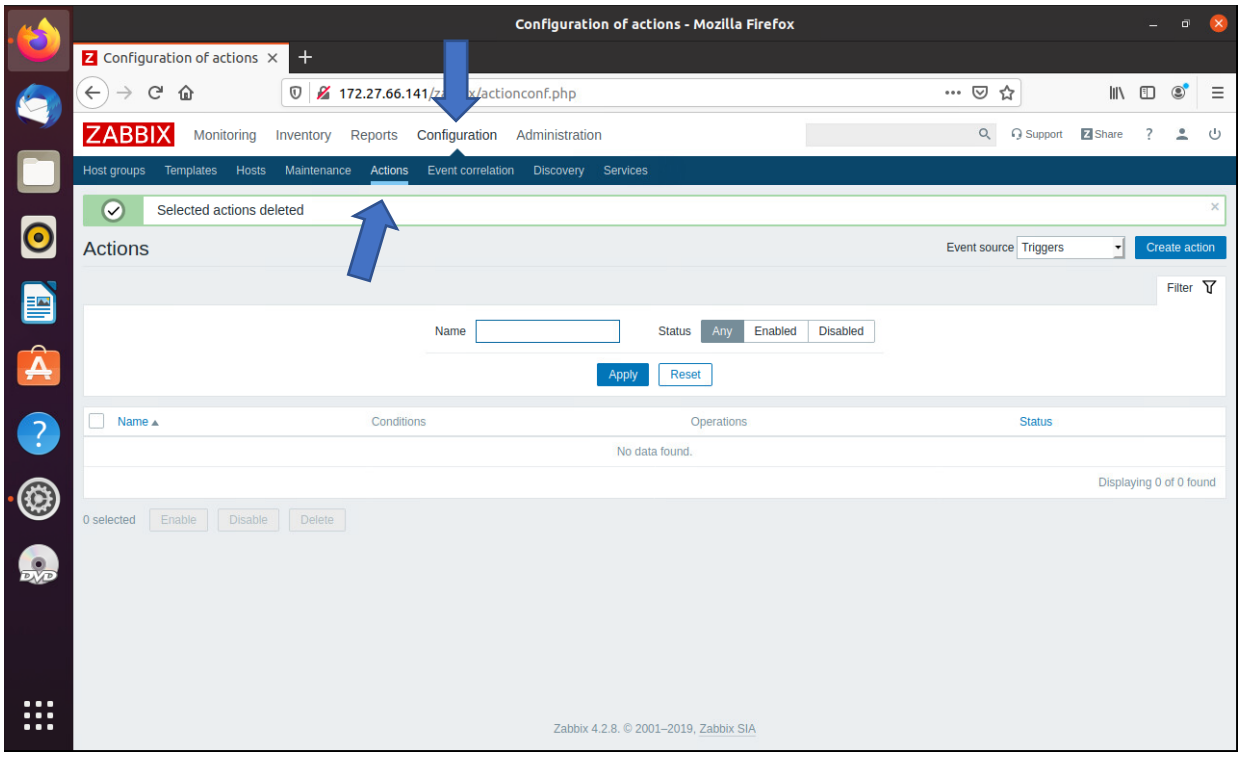
Click update now.

You can test this, by clicking on the test button



You should have received a mail from Zabbix.

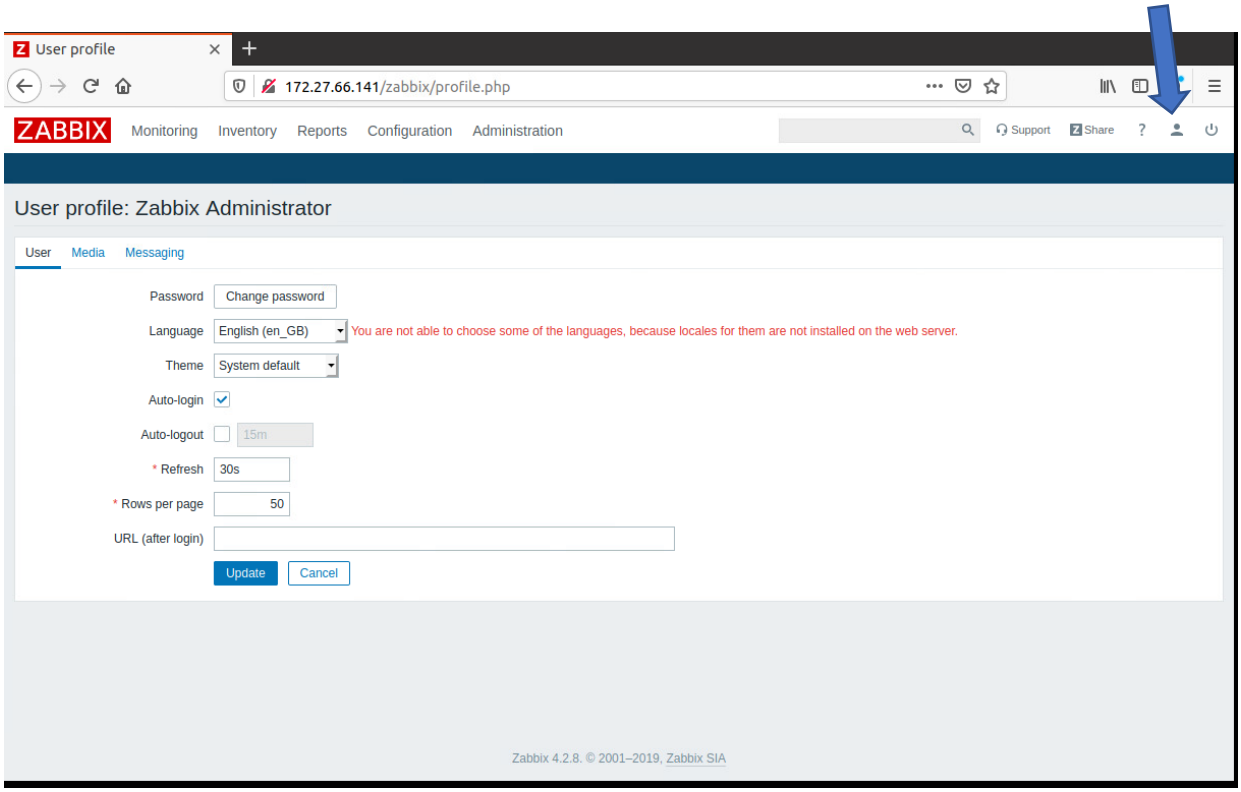
Now let's go to the configuration menu and action option:



Here you should already see an action! Click on the red status 'disabled' to enable this.

The last step is to assign an email address to the admin.

On the top right, you can access the profile settings:



If you click on media, you can use the email address we've already used so much.

And that's it! Now you can play around with the settings. You can change the notification settings so you only receive warnings when there's a critical alert, when something happens on server x,…