

# Report:

# ZABBIX

**Monitoring and Performance Management with  
Zabbix: Deployment and Configuration of Ubuntu,  
Windows, PaloAlto, FortiGate, and ESXi Platforms.**

ET.TAKI Omar



# Table of Contents:

<b>Introduction</b>	<b>4</b>
<b>Install Zabbix on Ubuntu server 22.04</b>	<b>5</b>
<b>Architecture</b>	<b>5</b>
Install Zabbix server, frontend, and agent	6
Configure database	8
Start Zabbix server and agent processes	12
Configure Zabbix frontend	12
Login to frontend using Zabbix default login credentials	17
The Zabbix dashboard:	18
Creating and configuring Zabbix users, user groups, and user roles	20
Creating User Groups	20
<b>Monitoring Ubuntu machine with Zabbix using agent</b>	<b>25</b>
Updating our System	25
Installing Zabbix Agent	25
Configuring Zabbix Agent	26
Starting and Enabling Zabbix Agent Service	27
Adding the Zabbix Client to the Zabbix Server	27
<b>Monitoring Windows machine with Zabbix using agent</b>	<b>30</b>
Installing Zabbix Agent	30
Configuring Zabbix Agent	31
Adding the Zabbix Client to the Zabbix Server	32
<b>Monitoring Palo Alto with Zabbix via SNMPv3</b>	<b>34</b>
Configuring and enabling SNMP on Palo Alto	34
Adding PaloAlto to Zabbix server	37
<b>Monitoring FortiGate with Zabbix via SNMPv3</b>	<b>39</b>
Configuring and enabling SNMP on FortiGate	39
Adding FortiGate to Zabbix server	41
<b>Monitoring ESXI with Zabbix via SNMPv3</b>	<b>42</b>
Configuring and enabling SNMP on ESXI	42
Enabling SSH Access on ESXi	42
ESXi SNMP Configuration	43
Configuring parameters of an SNMP agent	44
Configuring ESXi Firewall	46
Configuring SNMP v3	46
Adding ESXI to Zabbix server	47
<b>Zabbix Maps for Better Visualization</b>	<b>49</b>
Creating a new map	50
Configuring new map	51
Linking map elements	53
<b>Conclusion</b>	<b>55</b>

# Introduction

The Zabbix project is focused on the deployment and configuration of a comprehensive monitoring and performance management platform. This project aims to implement Zabbix, a powerful tool for surveillance and analysis, to ensure efficient monitoring of various components within the network architecture.

The primary objective of this project is to establish a centralized monitoring system using Zabbix, enabling real-time visibility into the performance and health of critical network elements. By leveraging Zabbix's capabilities, including data storage in a relational database and a user-friendly web interface, the project seeks to empower administrators with the tools necessary to effectively monitor and manage the network infrastructure.

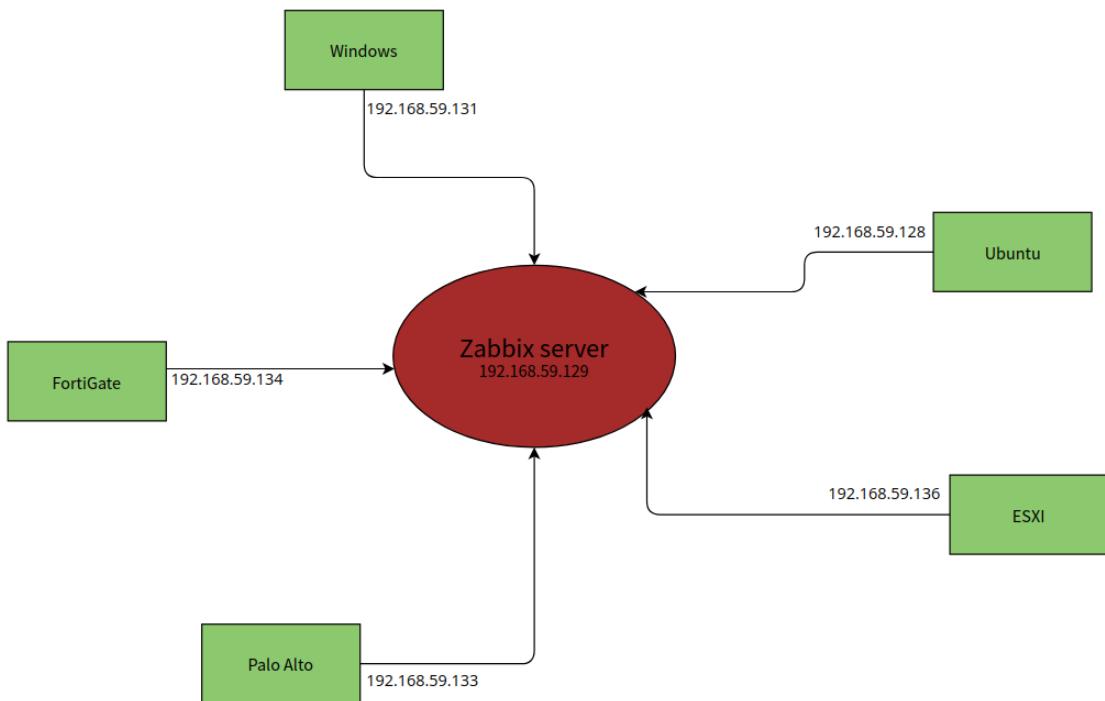
Throughout the project, special attention will be given to deploying Zabbix on an Ubuntu server, as well as configuring client machines and servers, such as Ubuntu, Windows, PaloAlto, FortiGate, and ESXi, to act as monitoring agents. These agents will facilitate the collection and analysis of vital system metrics, ensuring prompt detection of issues and proactive performance optimization.

By implementing Zabbix, this project aims to provide a holistic view of the network, empowering administrators with the insights required to make informed decisions and ensure optimal performance. The following sections will delve into the specific tasks involved in the installation, configuration, and management of Zabbix, as well as highlight the expected benefits and outcomes of this project.

# Install Zabbix on Ubuntu server 22.04

## Architecture

Here's the architecture of the network :



## Install Zabbix server, frontend, and agent

On ubuntu server, to check for the internal IP address, we execute the following command:

```
> ip a
```

```
zabbix@zabbix:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:8b:68:db brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.59.129/24 metric 100 brd 192.168.59.255 scope global dynamic ens33
        valid_lft 1572sec preferred_lft 1572sec
    inet6 fe80::20c:29ff:fe8b:68db/64 scope link
        valid_lft forever preferred_lft forever
zabbix@zabbix:~$ _
```

Then, we connect to the Zabbix server via SSH using the following command:

```
> ssh zabbix@192.168.59.129
```

```
ubuntu@ubuntu-virtual-machine:~$ ssh zabbix@192.168.59.129
zabbix@192.168.59.129's password:
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-72-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

System information as of Fri May 26 04:44:03 PM UTC 2023

System load:  0.0087890625   Processes:           213
Usage of /:   28.4% of 9.75GB  Users logged in:      1
Memory usage: 9%                IPv4 address for ens33: 192.168.59.129
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

52 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Fri May 26 16:44:04 2023 from 192.168.59.128
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
```

To gain superuser privileges and access elevated permissions on the Ubuntu server, the command 'sudo su' is executed.

```

root@zabbix: ~
[sudo] password for zabbix:
[sudo] password for zabbix:
root@zabbix:~/home/zabbix# apt update && apt upgrade -y
Hit:1 http://ma.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://ma.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Get:3 http://ma.archive.ubuntu.com/ubuntu jammy-backports InRelease [108 kB]
Get:4 http://ma.archive.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Fetched 337 kB in 2s (201 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
52 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages will be upgraded:
  apparmor apt apt-utils bind9-host dnsutils bind9-libs distro-info-data dpkg isc-dhcp-client isc-dhcp-common libapparmor1 libapt-pkg6.0 libglib2.0-0
  libglib2.0-bin libglib2.0-data libgssapi-krb5-2 libkrb5support0 libidn2-2.5.0 libldap-common libmbim-glib4 libmbim-proxy libmm-glib6 libnetplan0
  libnss-systemd libpam-systemd libpq5 libssl3 libtasl2-2 modules-lbsasl2-modules-db libudev libudev mdadm modernmanager netplan.io python3-apport
  python3-problem-report python3-software-properties python3-tz software-properties-common systemd systemd-hwe-hwdb systemd-sysv systemd-timesyncd tcpdump tzdata
  ubuntu-advantage-tools udev update-notifier-common
52 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Need to get 20.0 MB of archives.
After this operation, 1443 kB of additional disk space will be used.
Get:1 http://ma.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libnss-systemd amd64 249.11.0ubuntu3.9 [133 kB]
Get:2 http://ma.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libsystemd amd64 249.11.0ubuntu3.9 [318 kB]
Get:3 http://ma.archive.ubuntu.com/ubuntu jammy-updates/main amd64 systemd-timesyncd amd64 249.11.0ubuntu3.9 [31.2 kB]
Get:4 http://ma.archive.ubuntu.com/ubuntu jammy-updates/main amd64 systemd-sysv amd64 249.11.0ubuntu3.9 [16.5 kB]
Get:5 http://ma.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libpam-systemd amd64 249.11.0ubuntu3.9 [203 kB]
Get:6 http://ma.archive.ubuntu.com/ubuntu jammy-updates/main amd64 systemd amd64 249.11.0ubuntu3.9 [4581 kB]
Get:7 http://ma.archive.ubuntu.com/ubuntu jammy-updates/main amd64 udev amd64 249.11.0ubuntu3.9 [1557 kB]
Get:8 http://ma.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libudev amd64 249.11.0ubuntu3.9 [77.1 kB]
Get:9 http://ma.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libapparmor amd64 3.0.4-2ubuntu2.2 [39.2 kB]
Get:10 http://ma.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libapparmor1 amd64 2.4.9 [906 kB]
Get:11 http://ma.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libapparmor1 libapparmor1 amd64 2.4.9 [1239 kB]
Get:12 http://ma.archive.ubuntu.com/ubuntu jammy-updates/main amd64 apt amd64 2.4.9 [1379 kB]
Get:13 http://ma.archive.ubuntu.com/ubuntu jammy-updates/main amd64 apt-utils amd64 2.4.9 [211 kB]
Get:14 http://ma.archive.ubuntu.com/ubuntu jammy-updates/main amd64 update-notifier-common all 3.19.54.6 [185 kB]
Get:15 http://ma.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libk5crypto3 amd64 1.19.2-2ubuntu0.2 [86.3 kB]
Get:16 http://ma.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libkrb5support0 amd64 1.19.2-2ubuntu0.2 [32.3 kB]
Get:17 http://ma.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libkrb5-3 amd64 1.19.2-2ubuntu0.2 [357 kB]
Get:18 http://ma.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libgssapi-krb5-2 amd64 1.19.2-2ubuntu0.2 [145 kB]
Get:19 http://ma.archive.ubuntu.com/ubuntu jammy-updates/main amd64 distro-info-data all 0.52ubuntu0.4 [4986 B]
Get:20 http://ma.archive.ubuntu.com/ubuntu jammy-updates/main amd64 isc-dhcp-client amd64 4.4.1-2.3ubuntu2.4 [235 kB]
Get:21 http://ma.archive.ubuntu.com/ubuntu jammy-updates/main amd64 isc-dhcp-common amd64 4.4.1-2.3ubuntu2.4 [45.0 kB]

```

We install Zabbix 6 deb package on the Ubuntu server, using the following commands:

```

> wget
https://repo.zabbix.com/zabbix/6.4/ubuntu/pool/main/z/zabbix-release/zabbix-release_6.4-1+ubuntu$(lsb_release -rs)_all.deb
> sudo dpkg -i zabbix-release_6.4-1+ubuntu$(lsb_release -rs)_all.deb
> sudo apt update
> sudo apt -y install zabbix-server-mysql zabbix-frontend-php
zabbix-apache-conf zabbix-sql-scripts zabbix-agent

```

```

root@zabbix: ~/home/zabbix#
root@zabbix:~/home/zabbix# wget https://repo.zabbix.com/zabbix/6.4/ubuntu/pool/main/z/zabbix-release/zabbix-release_6.4-1+ubuntu$(lsb_release -rs)_all.deb
--2023-05-26 16:47:15-- https://repo.zabbix.com/zabbix/6.4/ubuntu/pool/main/z/zabbix-release/zabbix-release_6.4-1+ubuntu22.04_all.deb
Resolving repo.zabbix.com (repo.zabbix.com)... 178.128.6.101, 2604:3880:2: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: 3676 (3.6K) [application/octet-stream]
Saving to: "zabbix-release_6.4-1+ubuntu22.04_all.deb"

zabbix-release_6.4-1+ubuntu22.04_all.deb    100%[=====] 3.59K ---KB/s   in 0s
2023-05-26 16:47:16 (1.09 GB/s) - 'zabbix-release_6.4-1+ubuntu22.04_all.deb' saved [3676/3676]

```

```

root@zabbix:~/home/zabbix# dpkg -i zabbix-release_6.4-1+ubuntu$(lsb_release -rs)_all.deb
Selecting previously unselected package zabbix-release.
(Reading database ... 74024 files and directories currently installed.)
Preparing to unpack zabbix-release_6.4-1+ubuntu22.04_all.deb ...
Unpacking zabbix-release (1:6.4-1+ubuntu22.04) ...
Setting up zabbix-release (1:6.4-1+ubuntu22.04) ...

```

```
root@zabbix:/home/zabbix# apt update
Hit:1 http://ma.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://ma.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:3 http://ma.archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:4 http://ma.archive.ubuntu.com/ubuntu jammy-security InRelease
Get:5 https://repo.zabbix.com/zabbix-agent2-plugins/1/ubuntu jammy InRelease [4952 B]
Get:6 https://repo.zabbix.com/zabbix-agent2-plugins/1/ubuntu jammy/main Sources [1002 B]
Get:7 https://repo.zabbix.com/zabbix-agent2-plugins/1/ubuntu jammy/main amd64 Packages [624 B]
Get:8 https://repo.zabbix.com/zabbix/6.0/ubuntu jammy/main Sources [1943 B]
Get:9 https://repo.zabbix.com/zabbix/6.0/ubuntu jammy/main amd64 Packages [5485 B]
Fetched 19.0 kB in 1s (13.6 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
```

```
root@zabbix:/home/zabbix# apt -y install zabbix-server-mysql zabbix-frontend-php zabbix-apache-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:
  apache2 apache2-bin apache2-data apache2-utils bzip2 fontconfig-config fonts-dejavu fonts-dejavu-core fonts-dejavu-extra fping libapache2-mod-php8.1 libapril1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap libdeflate libevent2.1-7 libfontconfig1 libfdbsd1 libjbig0 libjpeg-turbo8 libjpeg8 libltdl17 libluas3.0 libmodbus5 libmysqlclient11 libncurses5 libopenpmlib libsensor3 libsnmp-base libsnmp40 libtiff5 libwebp libxpmp4 mailcap mime-support mysql-client mysql-client-8.0
  mysql-client-core-8.0 mysql-common php php-bcmath php-common php-gd php-ldap php-mbstring php-mysql php-xml php8.1-bcmath php8.1-cll php8.1-common php8.1-gd
  php8.1-ldap php8.1-mbstring php8.1-mysql php8.1-opcache php8.1-readline php8.1-xm1 smpd ssl-cert
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom www-browser bztp2-doc php-pear libgd-tools odbc-postgresql tdsodbc lm-sensors snmp-mibs-downloader snmptrapd
  zabbix-nginx.conf virtual-mysql-server
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils bzip2 fontconfig-config fonts-dejavu fonts-dejavu-core fonts-dejavu-extra fping libapache2-mod-php8.1 libapril1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap libdeflate libevent2.1-7 libfontconfig1 libfdbsd1 libjbig0 libjpeg-turbo8 libjpeg8 libltdl17 libluas3.0 libmodbus5 libmysqlclient11 libncurses5 libopenpmlib libsensor3 libsnmp-base libsnmp40 libtiff5 libwebp libxpmp4 mailcap mime-support mysql-client mysql-client-8.0
  mysql-client-core-8.0 mysql-common php php-bcmath php-common php-gd php-ldap php-mbstring php-mysql php-xml php8.1-bcmath php8.1-cll php8.1-common php8.1-gd
  php8.1-ldap php8.1-mbstring php8.1-mysql php8.1-opcache php8.1-readline php8.1-xm1 smpd ssl-cert zabbix-agent zabbix-apache-conf zabbix-frontend-php zabbix-server-mysql
zabbix-sql-scripts
0 upgraded, 68 newly installed, 0 to remove and 0 not upgraded.
Need to get 34.5 MB of archives.
After this operation, 174 MB of additional disk space will be used.
Get:1 http://ma.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libapril1 amd64 1.7.0-8ubuntu0.22.04.1 [108 kB]
Get:2 http://ma.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libaprutil1 amd64 1.6.1-Subuntu4.22.04.1 [92.6 kB]
Get:3 http://ma.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libaprutil1-dbd-sqlite3 amd64 1.6.1-Subuntu4.22.04.1 [11.3 kB]
Get:4 http://ma.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libaprutil1-ldap amd64 1.6.1-Subuntu4.22.04.1 [9168 B]
Get:5 http://ma.archive.ubuntu.com/ubuntu jammy/main amd64 libdeflate1 amd64 5.3.6-Subuntu4.5 [8 kB]
Get:6 http://ma.archive.ubuntu.com/ubuntu jammy/main amd64 libfdbsd1 amd64 2.1.52-Subuntu4.5 [1346 kB]
Get:7 https://repo.zabbix.com/zabbix/6.0/ubuntu jammy/main amd64 zabbix-server-mysql all 1:6.0.17-1+ubuntu22.04 [1346 kB]
Get:8 http://ma.archive.ubuntu.com/ubuntu jammy-updates/main amd64 apache2-data all 2.4.52-1ubuntu4.5 [165 kB]
Get:9 http://ma.archive.ubuntu.com/ubuntu jammy-updates/main amd64 apache2-utils all 2.4.52-1ubuntu4.5 [89.1 kB]
Get:10 http://ma.archive.ubuntu.com/ubuntu jammy/main amd64 mailcap all 3.70+mu1ubuntui [23.8 kB]
Get:11 http://ma.archive.ubuntu.com/ubuntu jammy/main amd64 mime-support all 3.68 [3696 B]
Get:12 http://ma.archive.ubuntu.com/ubuntu jammy-updates/main amd64 apache2 2.4.52-1ubuntu4.5 [97.8 kB]
Get:13 http://ma.archive.ubuntu.com/ubuntu jammy/main amd64 mariadb_Repo_Setup [5274 B]
Get:14 http://ma.archive.ubuntu.com/ubuntu jammy/main amd64 libsensor3 amd64 1:3.6.0-7ubuntui [26.3 kB]
Get:15 http://ma.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libsnmp-base all 5.9.1+dfsg-1ubuntu2.6 [201 kB]
Get:16 http://ma.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libsnmp40 amd64 5.9.1+dfsg-1ubuntu2.6 [1070 kB]
Get:17 http://ma.archive.ubuntu.com/ubuntu jammy-updates/main amd64 snmpd amd64 5.9.1+dfsg-1ubuntu2.6 [60.3 kB]
Get:18 http://ma.archive.ubuntu.com/ubuntu jammy/main amd64 libevent2.1-7 amd64 2.1.12-stable-1ubuntui [148 kB]
Get:19 http://ma.archive.ubuntu.com/ubuntu jammy/main amd64 mysql-common all 5.8+1.0.8 [7212 B]
```

## Configure database

In this installation, we will use password rootDBpass as root password and zabbixDBpass as Zabbix password for DB.

### Install MariaDB 10.6 :

In our terminal, we use the following commands:

```
> sudo apt install software-properties-common -y

> curl -LSS -O
https://downloads.mariadb.com/MariaDB/mariadb_repo_setup
> sudo bash mariadb_repo_setup --mariadb-server-version=10.6

> sudo apt update

> sudo apt -y install mariadb-common mariadb-server-10.6
mariadb-client-10.6
```

```
root@zabbix:/home/zabbix# sudo apt install software-properties-common -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
software-properties-common is already the newest version (0.99.22.7).
software-properties-common set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

```
root@zabbix:/home/zabbix# curl -LsS -O https://downloads.mariadb.com/MariaDB/Mariadb_repo_setup
sudo bash mariadb_repo_setup --mariadb-server-version=10.6
# [info] Checking for script prerequisites
# [info] MariaDB Server version 10.6 is valid
# [info] Repository file successfully written to /etc/apt/sources.list.d/mariadb.list
# [info] Adding trusted package signing keys...
# [info] Running apt-get update...
# [info] Done adding trusted package signing keys
```

```
root@zabbix:/home/zabbix# sudo apt update
Hit:1 http://ma.archive.ubuntu.com/ubuntu jammy InRelease
Get:3 https://dlm.mariadb.com/repo/mariadb-server/10.6/repo/ubuntu jammy InRelease [7767 B]
Hit:4 http://ma.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:5 http://ma.archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:6 http://ma.archive.ubuntu.com/ubuntu jammy-security InRelease
Hit:7 https://download.mariadb.com/tools/ubuntu jammy InRelease
Get:8 https://repo.zabbix.com/mariadb-plugins/1/ubuntu jammy InRelease
Hit:9 https://repo.zabbix.com/mariadb/6.0/ubuntu jammy InRelease
Fetched 17.1 kB in 1s (16.8 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
```

```
root@zabbix:/home/zabbix# sudo apt -y install mariadb-common mariadb-server-10.6 mariadb-client-10.6
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
galera-4 libcgifast-perl libcgipm-perl libclone-perl libdaxctli libdbd-mysql-perl libdbi-perl libencode-locale-perl libfcgi-bin libfcgi-perl libfcgioldbl
libhtml-parser-perl libhtml-tagset-perl libhttplib-template-perl libhttp-perl libhttp-message-perl liblio-html-perl liblwp-mediatypes-perl libmariadb3 libndctl6 libpmem1
libtimeate-perl liburi-perl liburing2 mariadb-client-core-10.6 mariadb-server-core-10.6 socat
Suggested packages:
liblmdm-perl libnet-daemon-perl libsql-statement-perl libdata-dump-perl libipc-sharedcache-perl libbusiness-lsbn-perl libwww-perl mailx mariadb-test
The following packages will be REMOVED:
mysql-client mysql-client-8.0 mysql-client-core-8.0
The following NEW packages will be installed:
galera-4 libcgifast-perl libcgipm-perl libclone-perl libdaxctli libdbd-mysql-perl libdbi-perl libencode-locale-perl libfcgi-bin libfcgi-perl libfcgioldbl
libhtml-parser-perl libhtml-tagset-perl libhttplib-template-perl libhttp-perl libhttp-message-perl liblio-html-perl liblwp-mediatypes-perl libmariadb3 libndctl6 libpmem1
libtimeate-perl liburi-perl liburing2 mariadb-client-10.6 mariadb-client-core-10.6 mariadb-common mariadb-server-10.6 mariadb-server-core-10.6 socat
0 upgraded, 3 newly installed, 3 to remove and 0 not upgraded.
Need to get 26.9 MB of archives.
After this operation, 131 MB of additional disk space will be used.
Get:1 https://dlm.mariadb.com/repo/mariadb-server/10.6/repo/ubuntu jammy/main amd64 mariadb-client-10.6 amd64 1:10.6.13+maria-ubu2204 [2187 kB]
Get:2 http://ma.archive.ubuntu.com/ubuntu jammy/main amd64 libdbi-perl amd64 1.643-3build3 [741 kB]
Get:3 http://ma.archive.ubuntu.com/ubuntu jammy/main amd64 libdaxctli amd64 72.1-1 [19.8 kB]
Get:4 http://ma.archive.ubuntu.com/ubuntu jammy/main amd64 libndctl6 amd64 72.1-1 [57.7 kB]
Get:5 http://ma.archive.ubuntu.com/ubuntu jammy/main amd64 libpmem1 amd64 1.11.1-3build1 [81.4 kB]
Get:6 http://ma.archive.ubuntu.com/ubuntu jammy/main amd64 liburing2 amd64 2.1-2build1 [10.3 kB]
Get:7 http://ma.archive.ubuntu.com/ubuntu jammy/main amd64 socat amd64 1.7.4.1-3ubuntu10 [349 kB]
Get:8 http://ma.archive.ubuntu.com/ubuntu jammy/main amd64 libhttplib-tagset-perl all 3.20-4 [12.5 kB]
Get:9 http://ma.archive.ubuntu.com/ubuntu jammy/main amd64 liburi-perl all 5.10-1 [78.8 kB]
Get:10 http://ma.archive.ubuntu.com/ubuntu jammy/main amd64 libhtml-parser-perl amd64 3.76-1build2 [88.4 kB]
Get:11 http://ma.archive.ubuntu.com/ubuntu jammy/main amd64 libcgipm-perl all 4.54-1 [188 kB]
Get:12 https://dlm.mariadb.com/repo/mariadb-server/10.6/repo/ubuntu jammy/main amd64 mariadb-common all 1:10.6.13+maria-ubu2204 [3928 B]
Get:13 https://dlm.mariadb.com/repo/mariadb-server/10.6/repo/ubuntu jammy/main amd64 libfcgioldbl amd64 2.4.2-2build2 [28.0 kB]
Get:14 https://dlm.mariadb.com/repo/mariadb-server/10.6/repo/ubuntu jammy/main amd64 libmariadb3 amd64 1:10.6.13+maria-ubu2204 [172 kB]
Get:15 https://dlm.mariadb.com/repo/mariadb-server/10.6/repo/ubuntu jammy/main amd64 libfcgi-perl amd64 0.82+ds-1build1 [22.8 kB]
Get:16 https://dlm.mariadb.com/repo/mariadb-server/10.6/repo/ubuntu jammy/main amd64 mariadb-client-core-10.6 amd64 1:10.6.13+maria-ubu2204 [995 kB]
Get:17 http://ma.archive.ubuntu.com/ubuntu jammy/main amd64 libcgifast-perl all 1:2.10-1 [11.5 kB]
Get:18 http://ma.archive.ubuntu.com/ubuntu jammy/main amd64 libclone-perl amd64 0.45-1-1build3 [11.0 kB]
Get:19 http://ma.archive.ubuntu.com/ubuntu jammy/main amd64 libdbd-mysql-perl amd64 4.05-1-1 [187.6 kB]
Get:20 http://ma.archive.ubuntu.com/ubuntu jammy/main amd64 libembed-locale-perl all 1.05.1.1 [11.8 kB]
Get:21 http://ma.archive.ubuntu.com/ubuntu jammy/main amd64 libfcgi-bin amd64 2.4.2-2build2 [11.2 kB]
Get:22 http://ma.archive.ubuntu.com/ubuntu jammy/main amd64 libhttplib-template-perl all 2.97-1.1 [59.1 kB]
Get:23 http://ma.archive.ubuntu.com/ubuntu jammy/main amd64 libtimeate-perl all 2.3300-2 [34.0 kB]
Get:24 http://ma.archive.ubuntu.com/ubuntu jammy/main amd64 libhttp-date-perl all 6.05-1 [9920 B]
Get:25 http://ma.archive.ubuntu.com/ubuntu jammy/main amd64 liblio-html-perl all 1.004-2 [15.4 kB]
Get:26 http://ma.archive.ubuntu.com/ubuntu jammy/main amd64 liblwp-mediatypes-perl all 6.04-1 [19.5 kB]
```

Once the installation is complete, we start the MariaDB service and we enable it using the following commands:

```
> systemctl start mariadb
> systemctl enable mariadb
> systemctl status mariadb
```

```

root@zabbix:/home/zabbix# systemctl start mariadb
root@zabbix:/home/zabbix# systemctl enable mariadb
Synchronizing state of mariadb.service with sysv service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable mariadb
root@zabbix:/home/zabbix# systemctl status mariadb
● mariadb.service - MariaDB 10.6.13 database server
   Loaded: loaded (/lib/systemd/system/mariadb.service; enabled; vendor preset: enabled)
   Drop-In: /etc/systemd/system/mariadb.service.d
             └─migrated-from-my.cnf-settings.conf
     Active: active (running) since Fri 2023-05-26 17:01:44 UTC; 1min 28s ago
       Docs: man:mysqld(7)
              http://mariadb.com/kb/en/library/systemd/
 Main PID: 31380 (mariadb)
 Status: "Taking your SQL requests now..."
   Tasks: 9 (lmi: 4530)
  Memory: 61.0M
    CPU: 254ms
   Corrupt: /system.slice/mariadb.service
           └─31389 /usr/sbin/mariadb

May 26 17:01:44 zabbix mariadb[31389]: 2023-05-26 17:01:44 0 [Note] Plugin 'FEEDBACK' is disabled.
May 26 17:01:44 zabbix mariadb[31389]: 2023-05-26 17:01:44 0 [Note] InnoDB: Loading buffer pool(s) from /var/lib/mysql/ib_buffer_pool
May 26 17:01:44 zabbix mariadb[31389]: 2023-05-26 17:01:44 0 [Warning] You need to use --log-bin to make --expire-logs-days or --binlog-expire-logs-seconds work.
May 26 17:01:44 zabbix mariadb[31389]: 2023-05-26 17:01:44 0 [Note] InnoDB: Server socket created on IP: '127.0.0.1'.
May 26 17:01:44 zabbix mariadb[31389]: 2023-05-26 17:01:44 0 [Note] InnoDB: Buffer pool(s) load completed at 230526 17:01:44
May 26 17:01:44 zabbix mariadb[31389]: 2023-05-26 17:01:44 0 [Note] InnoDB: ready for connections.
May 26 17:01:44 zabbix mariadb[31389]: Version: '10.6.13-MariaDB-1:10.6.13+maria-ubuntu20.04' socket: '/run/mysqld/mysqld.sock' port: 3306 mariadb.org binary distribution
May 26 17:01:44 zabbix systemd[1]: Started MariaDB 10.6.13 database server.
May 26 17:01:44 zabbix /etc/mysql/debian-start[31419]: Checking for insecure root accounts.
May 26 17:01:44 zabbix /etc/mysql/debian-start[31423]: Triggering myisam-recover for all MyISAM tables and aria-recover for all Aria tables

```

## Reset root password for database :

We secure MySQL/MariaDB by changing the default password for MySQL root:

```
> mysql_secure_installation
```

```

Enter current password for root (enter for none): Press Enter
Switch to unix_socket authentication [Y/n] Y
Change the root password? [Y/n] Y
New password: <Enter root DB password>
Re-enter new password: <Repeat root DB password>
Remove anonymous users? [Y/n]: Y
Disallow root login remotely? [Y/n]: Y
Remove test database and access to it? [Y/n]: Y
Reload privilege tables now? [Y/n]: Y

```

```

root@zabbix:/home/zabbix# mysql_secure_installation

NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
      SERVERS IN PRODUCTION USE! PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user. If you've just installed MariaDB, and
haven't set the root password yet, you should just press enter here.

Enter current password for root (enter for none):
OK, successfully used password, moving on...

Setting the root password or using the unix_socket ensures that nobody
can log into the MariaDB root user without the proper authorisation.

You already have your root account protected, so you can safely answer 'n'.

Switch to unix_socket authentication [Y/n] y
Enabled successfully!
Reloading privilege tables..
... Success!

You already have your root account protected, so you can safely answer 'n'.

Change the root password? [Y/n] y
New password:
Re-enter new password:
Password updated successfully!
Reloading privilege tables..
... Success!

By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them. This is intended only for testing, and to make the installation
go a bit smoother. You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] y
... Success!

Normally, root should only be allowed to connect from 'localhost'. This
ensures that someone cannot guess at the root password from the network.

```

## Create database :

```
> mysql -uroot -p'rootDBpass' -e "create database zabbix  
character set utf8mb4 collate utf8mb4_bin;"  
> mysql -uroot -p'rootDBpass' -e "grant all privileges on  
zabbix.* to zabbix@localhost identified by 'zabbixDBpass';"
```

```
All done! If you've completed all of the above steps, your MariaDB  
installation should now be secure.  
Thanks for using MariaDB!  
root@zabbix:/home/zabbix# mysql -uroot -p'rootDBpass' -e "create database zabbix character set utf8mb4 collate utf8mb4_bin;"  
root@zabbix:/home/zabbix# mysql -uroot -p'rootDBpass' -e "grant all privileges on zabbix.* to zabbix@localhost identified by 'zabbixDBpass';"
```

## Import initial schema and data

We import database shema for Zabbix server (could last up to 5 minutes):

```
> zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz |  
mysql --default-character-set=utf8mb4 -uzabbix  
-p'zabbixDBpass' zabbix
```

```
root@zabbix:/home/zabbix# zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql --default-character-set=utf8mb4 -uzabbix -p'zabbixDBpass' zabbix
```

## Enter database password in Zabbix configuration file :

We open zabbix\_server.conf file with command:

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

```
root@zabbix:/home/zabbix# sudo nano /etc/zabbix/zabbix_server.conf
```

and we add database password in this format anywhere in file:

DBPassword=zabbixDBpass

We save and exit file (ctrl+x, followed by y and enter).

## Start Zabbix server and agent processes

```
> sudo systemctl restart zabbix-server zabbix-agent  
> sudo systemctl enable zabbix-server zabbix-agent  
> sudo systemctl status zabbix-server zabbix-agent
```

```
root@zabbixx:/home/zabbixx# systemctl restart zabbix-server zabbix-agent
root@zabbixx:/home/zabbixx# systemctl enable zabbix-server zabbix-agent
● Enabling service zabbix-server.service with SysV service script with /lib/systemd/systemd-sysv-install.
● Synchronizing state of zabbix-server.service with SysV service script with /lib/systemd/systemd-sysv-install.
● Executing: /lib/systemd/systemd-sysv-install enable zabbix-agent
● Executing: /lib/systemd/systemd-sysv-install enable zabbix-agent
'[{"ACreated symlink /etc/systemd/system/multi-user.target.wants/zabbix-server.service → /lib/systemd/system/zabbix-server.service.
root@zabbixx:/home/zabbixx# systemctl status zabbix-server zabbix-agent
● zabbix-server.service - Zabbix Server
   Loaded: loaded (/lib/systemd/system/zabbix-server.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2023-05-26 17:13:59 UTC; 21s ago
 Main PID: 31870 (zabbix_server)
    Tasks: 48 (limit: 4530)
   Memory: 51.1M
      CPU: 156ms
   CGroup: /system.slice/zabbix-server.service
           └─31870 /usr/sbin/zabbix_server -c /etc/zabbix/zabbix_server.conf

May 26 17:13:59 zabbixx zabbix[31870]: [2023-05-26 17:13:59] [INFO] [main|writer|1] configuration syncer [synced configuration in 0.076944 sec, idle 66 sec]
May 26 17:13:59 zabbixx zabbix[31870]: [2023-05-26 17:13:59] [INFO] [main|writer|1] alert manager #1 [sent 0, failed 0 alerts, idle 5.004224 sec during 5.004322 sec]
May 26 17:13:59 zabbixx zabbix[31870]: [2023-05-26 17:13:59] [INFO] [main|writer|1] alerter #1 started
May 26 17:13:59 zabbixx zabbix[31870]: [2023-05-26 17:13:59] [INFO] [main|writer|1] alerter #2 started
May 26 17:13:59 zabbixx zabbix[31870]: [2023-05-26 17:13:59] [INFO] [main|writer|1] alerter #3 started
May 26 17:13:59 zabbixx zabbix[31870]: [2023-05-26 17:13:59] [INFO] [main|writer|1] preprocessing manager #1 [queued 0, processed 5 values, idle 5.003439 sec during 5.003661 sec]
May 26 17:13:59 zabbixx zabbix[31870]: [2023-05-26 17:13:59] [INFO] [main|writer|1] preprocessing worker #1 started
May 26 17:13:59 zabbixx zabbix[31870]: [2023-05-26 17:13:59] [INFO] [main|writer|1] preprocessing worker #2 started
May 26 17:13:59 zabbixx zabbix[31870]: [2023-05-26 17:13:59] [INFO] [main|writer|1] preprocessing worker #3 started
May 26 17:13:59 zabbixx zabbix[31870]: [2023-05-26 17:13:59] [INFO] [main|writer|1] uid manager #1 [processed 0 rules, idle 5.005937sec during 5.006017 sec]
May 26 17:13:59 zabbixx zabbix[31870]: [2023-05-26 17:13:59] [INFO] [main|writer|1] uid worker #1 started
May 26 17:13:59 zabbixx zabbix[31870]: [2023-05-26 17:13:59] [INFO] [main|writer|1] uid worker #2 started
May 26 17:13:59 zabbixx zabbix[31870]: [2023-05-26 17:13:59] [INFO] [main|writer|1] housekeeper [started "idle for 30 minutes"]
May 26 17:13:59 zabbixx zabbix[31870]: [2023-05-26 17:13:59] [INFO] [main|writer|1] timer #1 [updated 0 hosts, suppressed 0 events in 0.000943 sec, idle 59 sec]
May 26 17:13:59 zabbixx zabbix[31870]: [2023-05-26 17:13:59] [INFO] [main|writer|1] http poller #1 [got 0 values in 0.000726 sec, idle 5 sec]
May 26 17:13:59 zabbixx zabbix[31870]: [2023-05-26 17:13:59] [INFO] [main|writer|1] discoverer #1 [processed 0 rules in 0.000277 sec, idle 60 sec]
May 26 17:13:59 zabbixx zabbix[31870]: [2023-05-26 17:13:59] [INFO] [main|writer|1] history syncer #1 [processed 0 values, 0 triggers in 0.000018 sec, idle 1 sec]"
May 26 17:13:59 zabbixx zabbix[31870]: [2023-05-26 17:13:59] [INFO] [main|writer|1] history syncer #2 [processed 1 values, 1 triggers in 0.002282 sec, idle 1 sec]"
May 26 17:13:59 zabbixx zabbix[31870]: [2023-05-26 17:13:59] [INFO] [main|writer|1] history syncer #3 [processed 0 values, 0 triggers in 0.000008 sec, idle 1 sec]"
May 26 17:13:59 zabbixx zabbix[31870]: [2023-05-26 17:13:59] [INFO] [main|writer|1] history syncer #4 [processed 0 values, 0 triggers in 0.000021 sec, idle 1 sec]"
May 26 17:13:59 zabbixx zabbix[31870]: [2023-05-26 17:13:59] [INFO] [main|writer|1] escalator #1 [processed 0 escalations in 0.001391 sec, idle 3 sec]"
May 26 17:13:59 zabbixx zabbix[31870]: [2023-05-26 17:13:59] [INFO] [main|writer|1] proxy poller #1 [exchanged data with 0 proxies in 0.000026 sec, idle 5 sec]"
May 26 17:13:59 zabbixx zabbix[31870]: [2023-05-26 17:13:59] [INFO] [main|writer|1] self-monitoring [processed data in 0.000023 sec, idle 1 sec]"
May 26 17:13:59 zabbixx zabbix[31870]: [2023-05-26 17:13:59] [INFO] [main|writer|1] task manager [processed 0 task(s) in 0.000489 sec, idle 5 sec]"
May 26 17:13:59 zabbixx zabbix[31870]: [2023-05-26 17:13:59] [INFO] [main|writer|1] poller #1 [got 0 values in 0.000011 sec, idle 1 sec]"
May 26 17:13:59 zabbixx zabbix[31870]: [2023-05-26 17:13:59] [INFO] [main|writer|1] poller #2 [got 1 values in 0.0000706 sec, idle 1 sec]"
```

## Configure Zabbix frontend

## Configure PHP for Zabbix frontend :

We edit file /etc/zabbix/apache.conf:

```
> sudo nano /etc/zabbix/apache.conf
```

We uncomment "# php\_value date.timezone Europe/Riga" by removing symbol # and we set the right timezone for our country:

`php_value date.timezone Africa/Casablanca`

We save and exit file (ctrl+x, followed by y and enter)

```

GNU nano 6.2
/etc/zabbix/apache.conf *
# Define /zabbix alias, this is the default
<IfModule mod_alias.c>
  Alias /zabbix /usr/share/zabbix
</IfModule>

<Directory "/usr/share/zabbix">
  Options FollowSymlinks
  AllowOverride None
  Order allow,deny
  Allow from all

  <IfModule mod_php.c>
    php_value max_execution_time 300
    php_value memory_limit 128M
    php_value post_max_size 16M
    php_value upload_max_filesize 2M
    php_value max_input_time 300
    php_value max_input_VARS 10000
    php_value always_populate_raw_post_data -1
  </IfModule>

  <IfModule mod_php7.c>
    php_value max_execution_time 300
    php_value memory_limit 128M
    php_value post_max_size 16M
    php_value upload_max_filesize 2M
    php_value max_input_time 300
    php_value max_input_VARS 10000
    php_value always_populate_raw_post_data -1
    php_value date.timezone Africa/Casablanca
  </IfModule>
</Directory>

<Directory "/usr/share/zabbix/conf">
  Order deny,allow
  Deny from all
  <Files *.php>
    Order deny,allow
    Deny from all
  </Files>
</Directory>

File Name to Write: /etc/zabbix/apache.conf
M-Q Help           M-D DOS Format      M-A Append      M-B Backup File

```

## Restart Apache web server and make it start at system boot :

```

> sudo systemctl restart apache2
> sudo systemctl enable apache2
> sudo systemctl status apache2

```

```

root@zabbix:~# systemctl restart apache2
root@zabbix:~# systemctl enable apache2
Synchronizing state of apache2.service with sysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable apache2
root@zabbix:~# systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2023-05-26 17:17:25 UTC; 17s ago
     Docs: https://httpd.apache.org/docs/2.4/
 Main PID: 32165 (apache2)
   Tasks: 6 (limit: 4530)
   Memory: 12.3M
      CPU: 32ms
   CGroup: /system.slice/apache2.service
           └─32165 /usr/sbin/apache2 -k start
              ├─32167 /usr/sbin/apache2 -k start
              ├─32168 /usr/sbin/apache2 -k start
              ├─32169 /usr/sbin/apache2 -k start
              ├─32170 /usr/sbin/apache2 -k start
              └─32171 /usr/sbin/apache2 -k start

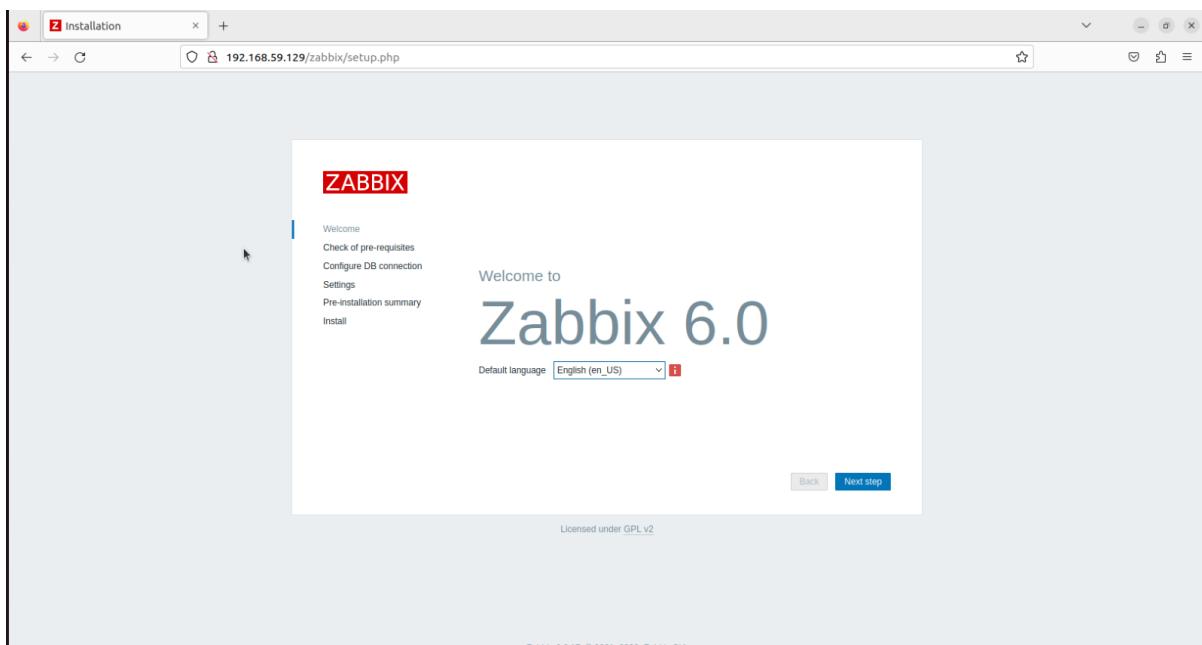
May 26 17:17:25 zabbix systemd[1]: Starting The Apache HTTP Server...
May 26 17:17:25 zabbix apache2[32164]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive.
May 26 17:17:25 zabbix systemd[1]: Started The Apache HTTP Server.

```

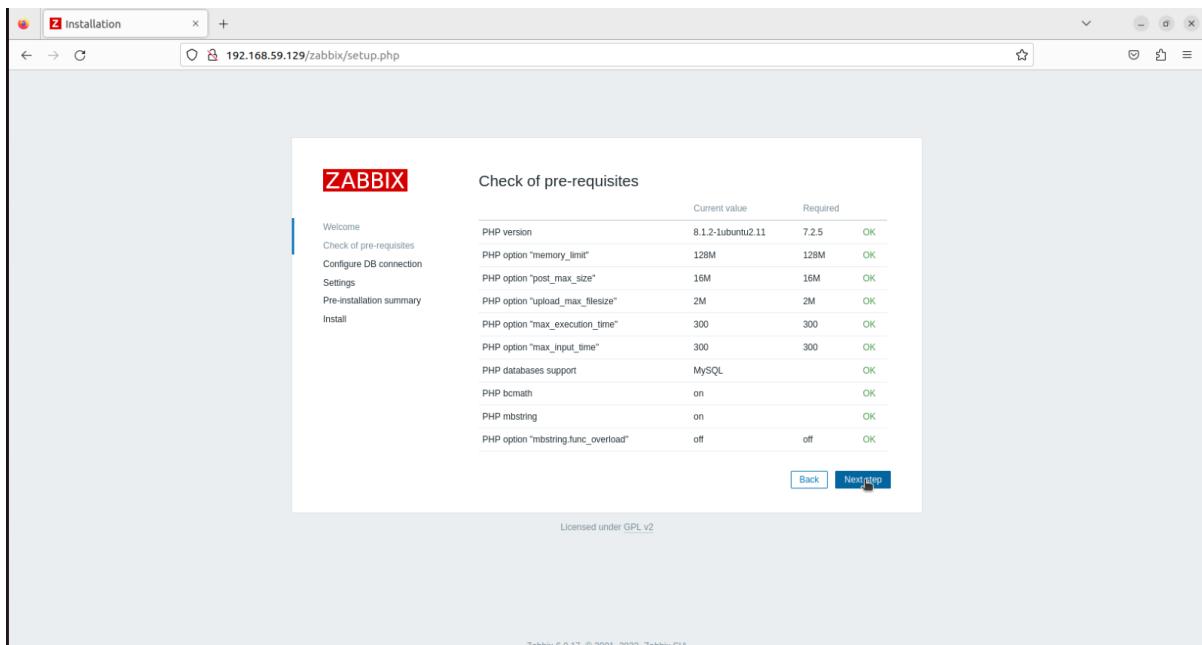
## Configure web frontend :

We connect to our newly installed Zabbix frontend using URL  
[“http://192.168.59.129/zabbix”](http://192.168.59.129/zabbix) to initiate the Zabbix installation wizard.

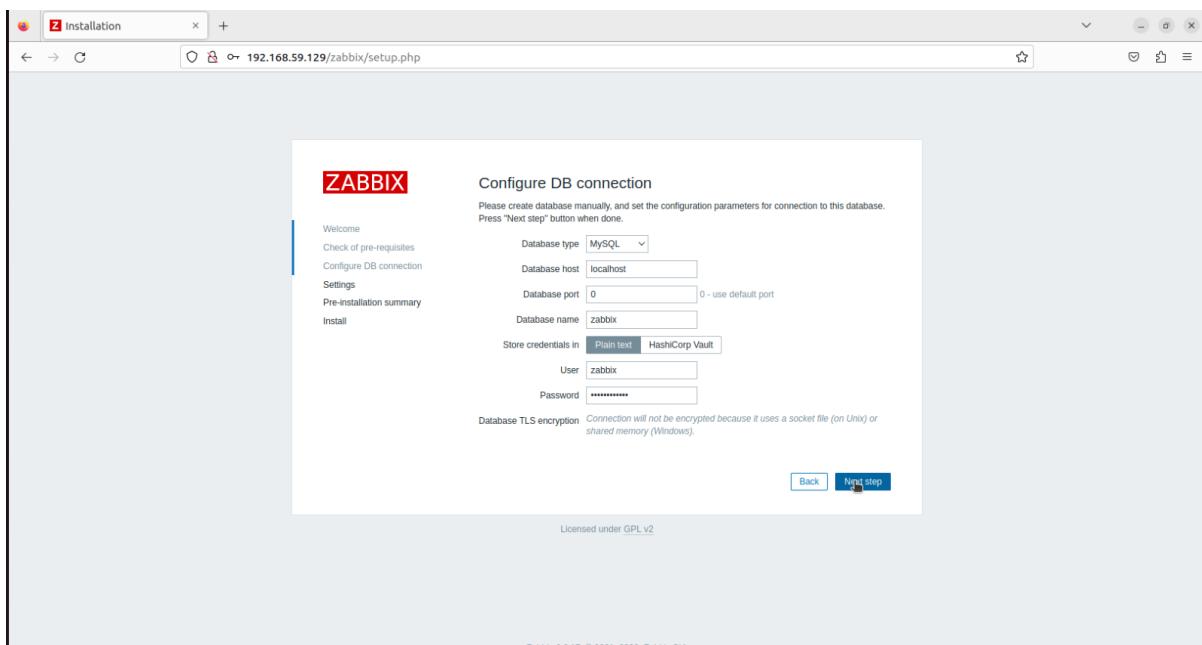
Basically, in this wizard we only need to enter a password for Zabbix DB user and we just click “Next step” for everything else.



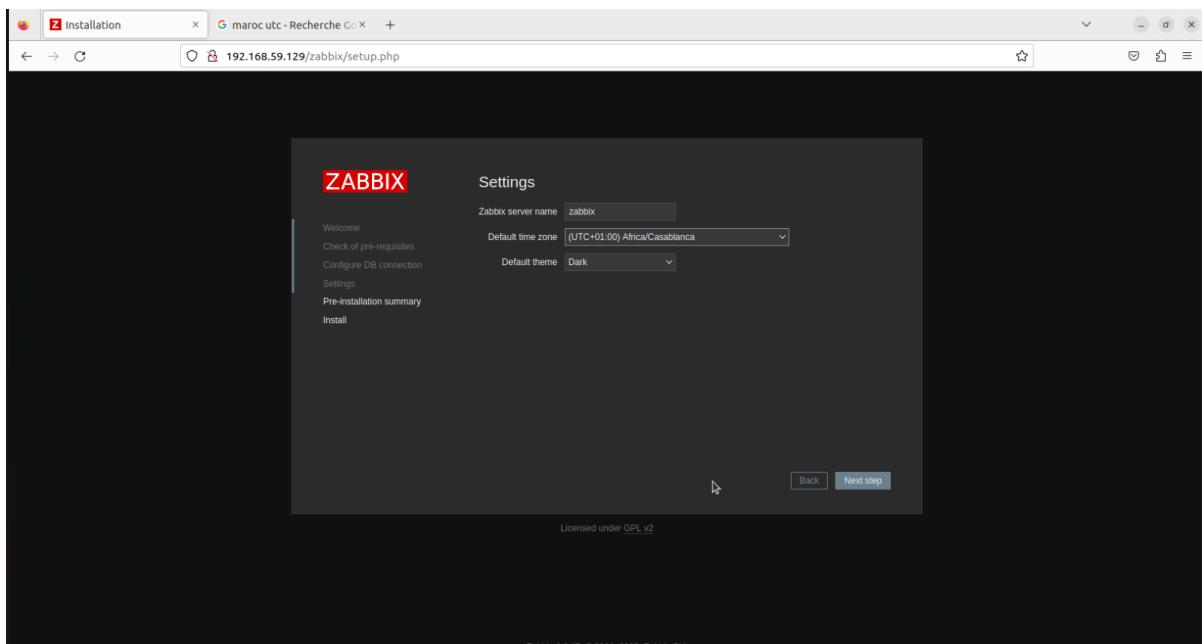
## 1. Installation step: Welcome screen



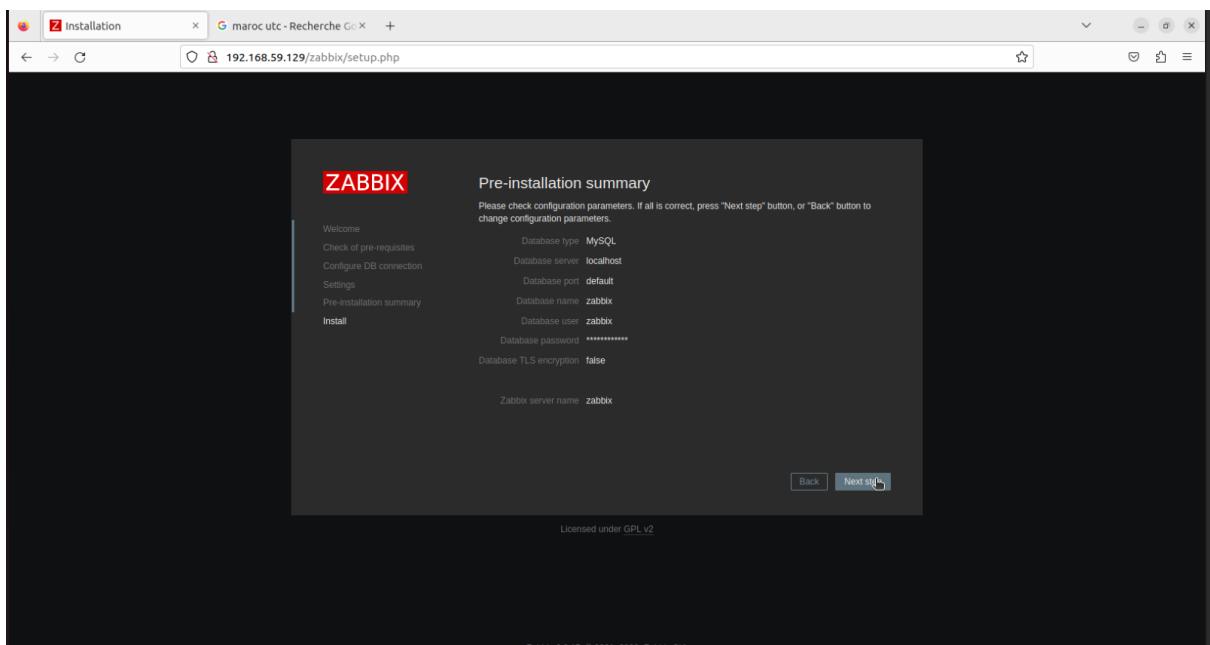
## 2. Installation step: Prerequisites check



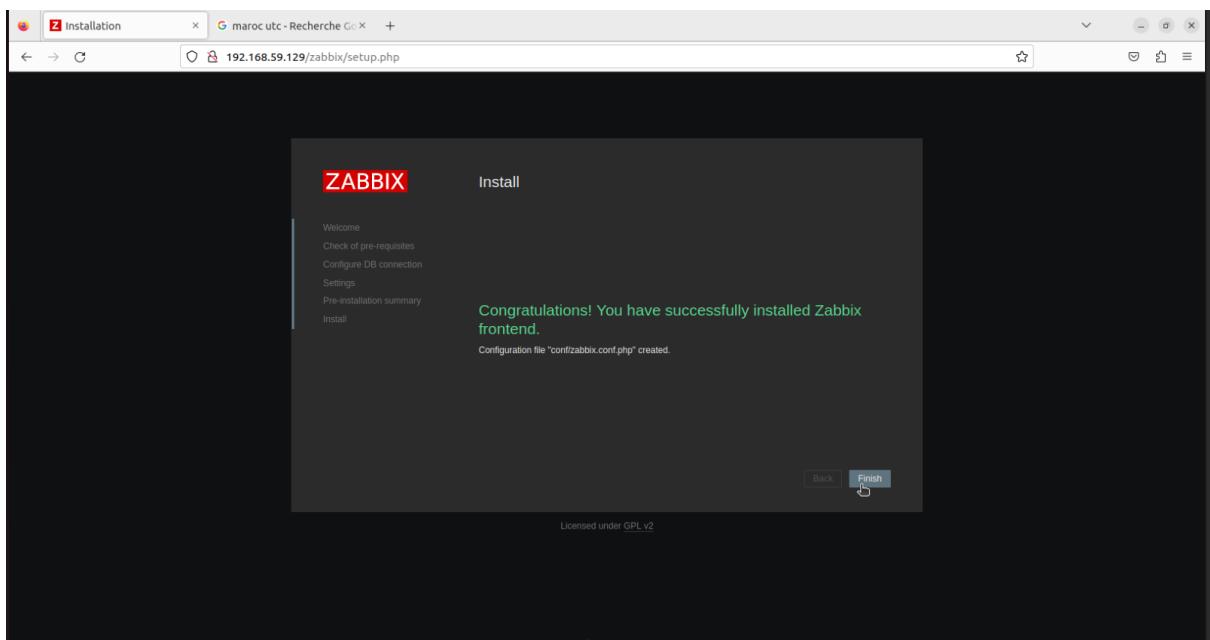
### 3. Installation step: Configure DB connection



### 4. Installation step: Configure Zabbix server



## 5. Installation step: Pre-installation summary

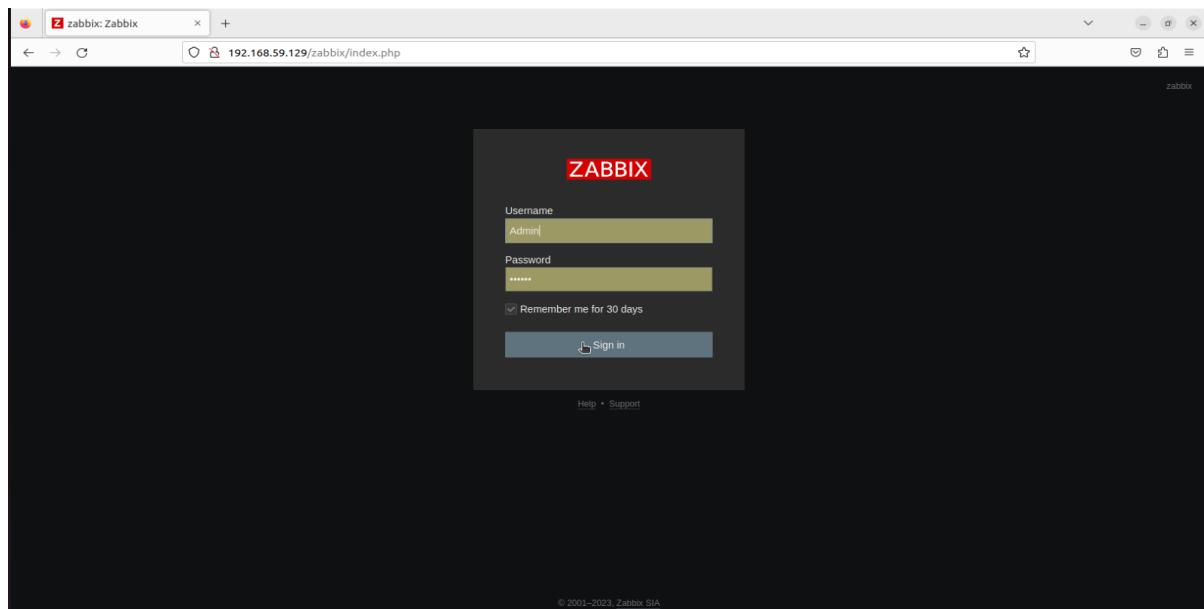


## 6. Installation step: Finish

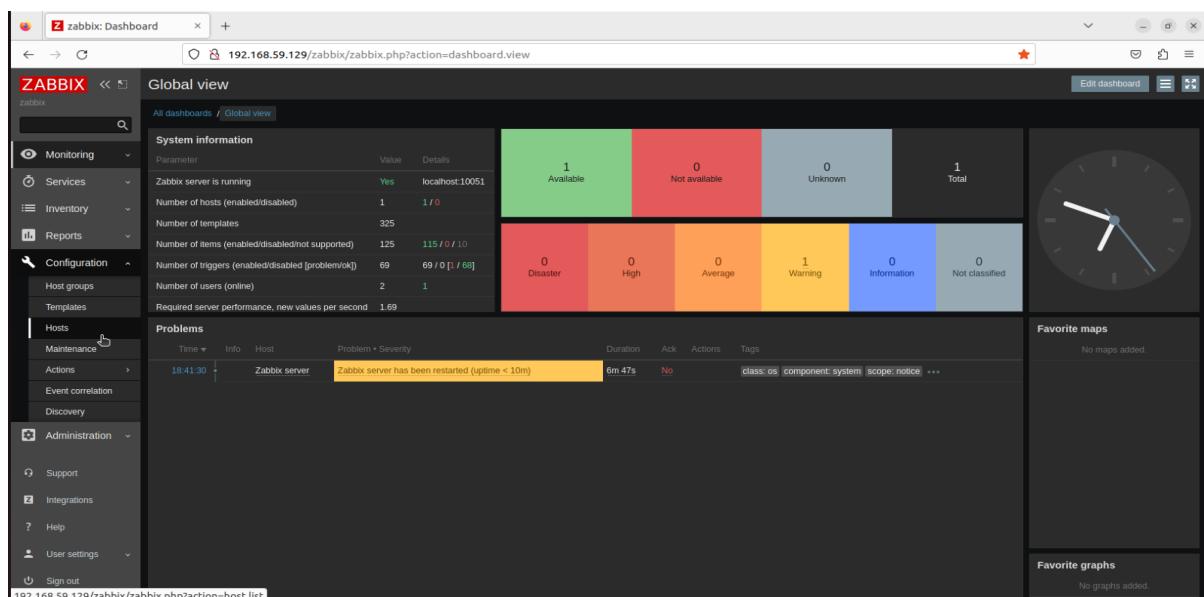
That's it, we have installed the Zabbix monitoring system!

# Login to frontend using Zabbix default login credentials

We use Zabbix default admin username “Admin” and password “zabbix” (without quotes) to login to Zabbix frontend at URL “<http://192.168.59.129/zabbix>” via our browser.



ZABBIX LOGIN PAGE



Zabbix dashboard

## The Zabbix dashboard:

In the realm of IT infrastructure monitoring and management, having a comprehensive and intuitive dashboard is paramount to staying on top of network health and performance. Zabbix offers a robust dashboard feature that enables organizations to visualize critical metrics, monitor network elements, and streamline operations. The capabilities and benefits of Zabbix dashboards, shedding light on how they empower administrators to efficiently monitor their networks and optimize performance.

- An Overview of Zabbix Dashboards:

Zabbix dashboards serve as a centralized hub for monitoring key performance indicators (KPIs), system events, and network components. These dashboards provide administrators with a bird's-eye view of their infrastructure, allowing them to detect issues, track performance trends, and make data-driven decisions. Zabbix's customizable dashboard interface enables users to tailor the display of data to suit their specific monitoring needs.

- Real-Time Monitoring and Alerting:

One of the primary strengths of Zabbix dashboards lies in their real-time monitoring capabilities. Administrators can configure widgets and visual elements to display live data streams, such as graphs, charts, maps, and status indicators. This real-time visibility empowers IT teams to proactively identify and address anomalies or performance bottlenecks before they escalate. Zabbix's alerting system complements the dashboards by providing instant notifications via various channels, including email, SMS, or integrations with popular collaboration tools.

- Customization and Personalization:

Zabbix dashboards offer extensive customization options, allowing administrators to create tailored views that align with their monitoring goals and requirements. Users can select from a rich library of pre-built widgets or design custom ones. These widgets can be arranged and organized within the dashboard to provide a cohesive and intuitive monitoring experience. With the ability to resize, reposition, and adjust

the granularity of displayed data, Zabbix ensures that users have full control over their monitoring interface.

- Drilling Down for Granular Insights:

In complex network environments, it is essential to have the ability to drill down into specific elements to gain deeper insights. Zabbix dashboards support multi-level drill-down, enabling administrators to navigate from high-level overviews to granular details of individual hosts, services, or applications. This functionality facilitates efficient troubleshooting and root cause analysis, saving valuable time and resources.

- Historical Data Analysis:

Zabbix dashboards are not limited to real-time monitoring but also provide access to historical data. The system captures and stores metrics over time, allowing administrators to analyze trends, compare performance across different time periods, and identify long-term patterns or recurring issues. Historical data analysis plays a vital role in capacity planning, performance optimization, and informed decision-making.

- Collaboration and Reporting:

Collaboration among IT teams is essential for effective network management. Zabbix dashboards enable seamless collaboration by providing shared views of monitoring data. Multiple stakeholders can access and interact with the dashboard, fostering collaboration, knowledge sharing, and cross-functional problem-solving. Additionally, Zabbix offers reporting capabilities, allowing administrators to generate detailed reports based on dashboard data, providing stakeholders with comprehensive insights into network performance and trends.

Zabbix dashboards are an asset in the arsenal of network administrators and IT teams. With real-time monitoring, customizable visualizations, multi-level drill-down, historical data analysis, and collaboration features, Zabbix dashboards empower

organizations to streamline operations, optimize network performance, and ensure the health and reliability of their IT infrastructure. By leveraging the power of Zabbix dashboards, administrators can efficiently monitor, troubleshoot, and make informed decisions, ultimately enhancing their network management capabilities.

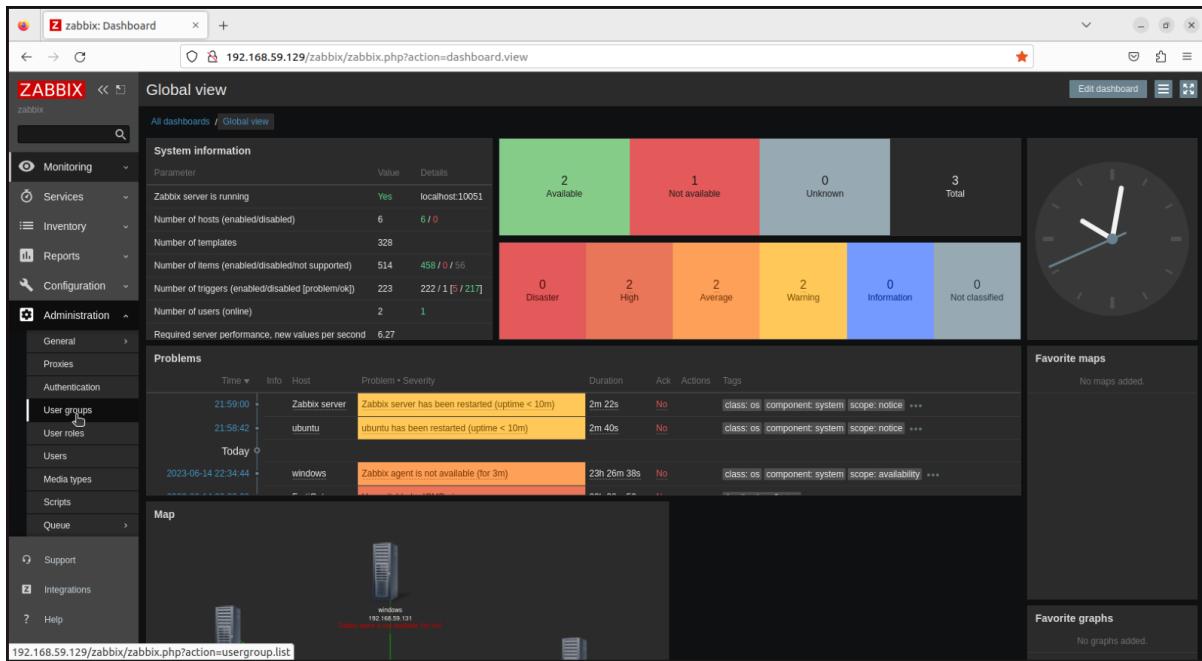
## Creating and configuring Zabbix users, user groups, and user roles

To make the most of Zabbix's features, it's important to create users, user groups, and permissions. This will allow us to control who can access and modify different parts of the monitoring system, ensuring that our data remains secure and that only authorized personnel can make changes. In this report, we'll go through step-by-step instructions on how to create users, user groups, and permissions.

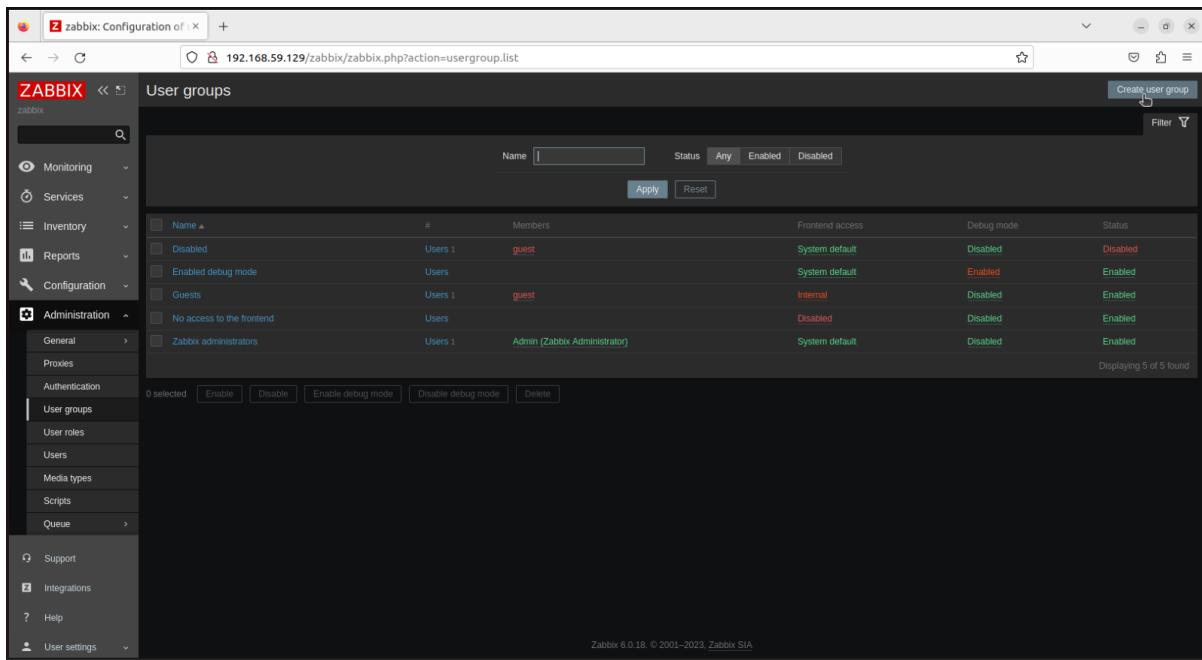
### Creating User Groups

User groups in Zabbix serve to manage and organize users who share similar responsibilities within the monitoring system. User groups allow administrators to assign permissions to a group of users, rather than having to assign permissions to each user individually. This helps to simplify the management of user access and makes it easier to ensure that all users with similar responsibilities have the appropriate level of access.

Go to the Administration tab in the navigation menu, and then click on User groups.



Click on the Create user group button, or the group we need to change.



In the User group details section, fill in the group name.

The screenshot shows the Zabbix web interface with the URL <https://192.168.59.129/zabbix/zabbix.php?action=usergroup.edit>. The left sidebar is open, showing the 'Administration' section with 'User groups' selected. The main content area is titled 'User groups' and has tabs for 'User group', 'Permissions', and 'Tag filter'. Under 'User group', there is a form with fields: 'Group name' (set to 'IT team'), 'Frontend access' (set to 'System default'), 'Enabled' (checkbox checked), and 'Debug mode' (checkbox unchecked). Below the form are 'Add' and 'Cancel' buttons. The 'Permissions' tab is active, showing a table with one row: 'Host group' (set to 'All groups') and 'Permissions' (set to 'Read-write'). There is a search bar and a checkbox for 'Include subgroups'. At the bottom are 'Add' and 'Cancel' buttons.

In the Permissions section, we can specify which host groups and templates, and other objects linked to them the user group can access and read and/or write.

This screenshot is identical to the one above, showing the 'User groups' configuration page for creating a new user group named 'IT team'. The 'Permissions' tab is selected, displaying 'All groups' with 'Read-write' permissions. The interface includes a search bar, an 'Add' button, and a 'Cancel' button at the bottom.

## Creating Users

Click on the Administration tab in the top navigation menu, and then click on Users.

Click on the Create user button, or a user we want to edit.

The screenshot shows the Zabbix 6.0.18 user list page. The left sidebar has a dark theme with various navigation options under 'Administration' like General, Proxies, Authentication, User groups, User roles, and Users. The main content area is titled 'Users' and shows a table with two rows. The columns are: Username, Name, Last name, User role, Groups, Is online?, Login, Frontend access, API access, Debug mode, and Status. The 'Admin' user is listed with 'Zabbix' as the name, 'Administrator' as the role, and 'Super admin role' in the Groups column. The 'guest' user is listed with 'Guest role' in the Groups column. There are buttons at the bottom for '0 selected', 'Unlock', and 'Delete'.

In the User details section, fill in the username and password fields.

In the User group section, select the user group to which the user should belong. If the user group does not exist, we can create it.

The screenshot shows the Zabbix 6.0.18 user edit page. The left sidebar is identical to the previous screenshot. The main content area is titled 'User' and shows a form for creating a new user. The 'Username' field is filled with 'IT Manager'. The 'Groups' dropdown contains 'IT team'. Other fields include 'Name', 'Last name', 'Password', 'Language' (English), 'Time zone' (Africa/Casablanca), 'Theme' (Dark), 'Auto-login' (unchecked), 'Auto-logout' (15m), 'Refresh' (30s), 'Rows per page' (50), and 'URL (after login)'. At the bottom are 'Add' and 'Cancel' buttons. A cursor is hovering over the 'Add' button.

In the Permissions section, we should choose a pre-created role for our user which specifies what UI elements are accessible for this user. It also sets permissions for specific actions, such as acknowledging problems or deleting events.

The screenshot shows the Zabbix configuration interface for managing users. The left sidebar is titled 'ZABBIX' and includes sections for Monitoring, Services, Inventory, Reports, Configuration, Administration (General, Proxies, Authentication, User groups, User roles, Users, Media types, Scripts, Queue), Support, Integrations, and Help. The main content area is titled 'Users' and shows the 'Permissions' tab. A search bar at the top has 'zabbix' typed into it. Below the search bar, there is a dropdown for 'Role' with 'Super admin role' selected, and a 'Select' button. A 'User type' dropdown is set to 'Super admin'. Under 'Permissions', there is a section for 'Host group' with 'All groups' selected and 'Read-write' permissions assigned. A note states: 'Permissions can be assigned for user groups only.' Below this, there are sections for 'Access to UI elements', 'Access to services', 'Access to modules', 'Access to API', and 'Access to actions'. Each section contains a table with columns for 'Monitoring', 'Services', 'Inventory', 'Reports', 'Configuration', and 'Administration', each with several tabs like 'Dashboard', 'Problems', 'Hosts', etc., some of which are highlighted in green.

Here's a simple explanation how to choose Role:

### 1 Utilisateur Zabbix

Accès uniquement au menu « Surveillance ». Il n'a accès à aucune ressource par défaut et toutes les autorisations sur les groupes d'hôtes doivent être explicitement attribuées

### 2 Administrateur Zabbix

Accès aux menus « Surveillance » et « Configuration ». Il n'a accès à aucun groupe d'hôtes par défaut et toutes les autorisations doivent être explicitement attribuées

### 3 Super Administrateur Zabbix

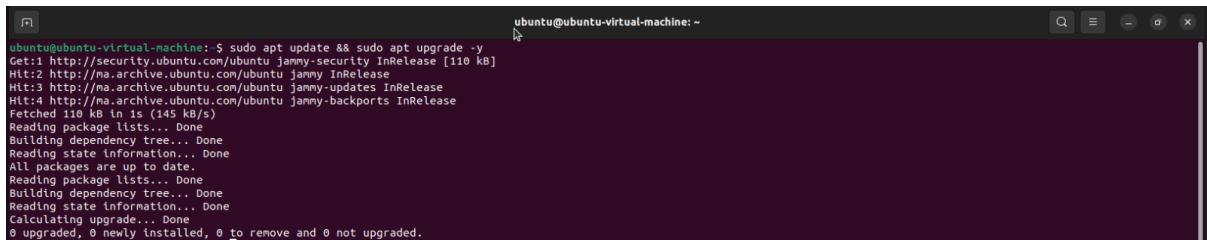
Accès total à tous les menus « Surveillance », « Configuration » et « Administration ». Il dispose d'un accès lecture-écriture à tous les groupes d'hôtes

# Monitoring Ubuntu machine with Zabbix using agent

## Updating our System

Before starting the installation process, it is always recommended to update our system. Open a terminal and execute the following command:

```
> sudo apt update && sudo apt upgrade -y
```

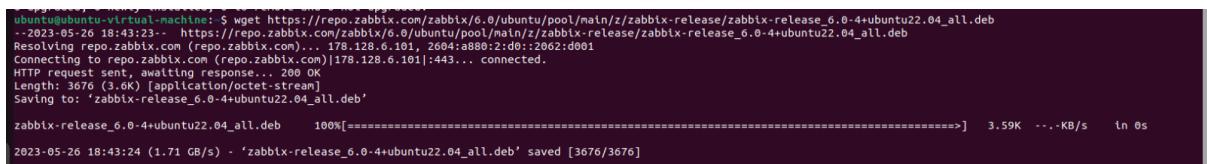


```
ubuntu@ubuntu-virtual-machine: ~
$ sudo apt update && sudo apt upgrade -y
Get:1 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Hit:2 http://ma.archive.ubuntu.com/ubuntu jammy InRelease
Hit:3 http://ma.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:4 http://ma.archive.ubuntu.com/ubuntu jammy-backports InRelease
Fetched 110 kB in 1s (145 kB/s)
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.
```

## Installing Zabbix Agent

Now, we will install the Zabbix Agent from the official Zabbix repository. First, add the Zabbix repository to our system:

```
> wget
https://repo.zabbix.com/zabbix/6.0/ubuntu/pool/main/z/zabbix-release
/zabbix-release_6.0-4+ubuntu22.04_all.deb
> sudo dpkg -i zabbix-release_6.0-4+ubuntu22.04_all.deb
> sudo apt update
```



```
ubuntu@ubuntu-virtual-machine: ~
$ wget https://repo.zabbix.com/zabbix/6.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_6.0-4+ubuntu22.04_all.deb
--2023-05-26 18:43:23-- https://repo.zabbix.com/zabbix/6.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_6.0-4+ubuntu22.04_all.deb
Resolving repo.zabbix.com (repo.zabbix.com)... 178.128.6.101, 2664: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: 3676 (3.0K) [application/octet-stream]
Saving to: 'zabbix-release_6.0-4+ubuntu22.04_all.deb'

zabbix-release_6.0-4+ubuntu22.04_all.deb    100%[=====] 3.59K --.-KB/s   in 0s
2023-05-26 18:43:24 (1.71 GB/s) - 'zabbix-release_6.0-4+ubuntu22.04_all.deb' saved [3676/3676]
```



```
ubuntu@ubuntu-virtual-machine: ~
$ sudo dpkg -i zabbix-release_6.0-4+ubuntu22.04_all.deb
Selecting previously unselected package zabbix-release.
(Reading database ... 19793 files and directories currently installed.)
Preparing to unpack zabbix-release_6.0-4+ubuntu22.04_all.deb ...
Unpacking zabbix-release (1:6.0-4+ubuntu22.04) ...
Setting up zabbix-release (1:6.0-4+ubuntu22.04) ...
```

```

ubuntu@ubuntu-virtual-machine: $ sudo apt update
Hit:1 http://ma.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://security.ubuntu.com/ubuntu jammy-security InRelease
Hit:3 http://ma.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:4 http://ma.archive.ubuntu.com/ubuntu jammy-backports InRelease
Get:5 https://repo.zabbix.com/zabbix-agent2-plugins/1/ubuntu jammy InRelease [4,952 B]
Get:6 https://repo.zabbix.com/zabbix-agent2-plugins/1/ubuntu jammy/main Sources [4,958 B]
Get:7 https://repo.zabbix.com/zabbix-agent2-plugins/1/ubuntu jammy/main amd64 Packages [624 B]
Get:8 https://repo.zabbix.com/zabbix/6.0/ubuntu jammy/main Sources [1,943 B]
Get:9 https://repo.zabbix.com/zabbix/6.0/ubuntu jammy/main amd64 Packages [5,405 B]
Get:10 https://repo.zabbix.com/zabbix/6.0/ubuntu jammy/multiverse Sources [1,943 B]
Get:11 https://repo.zabbix.com/zabbix/6.0/ubuntu jammy/multiverse amd64 Packages [5,405 B]
Fetched 10,8 kB in 2s (10.7 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
N: Skipping acquire of configured file 'main/binary-i386/Packages' as repository 'https://repo.zabbix.com/zabbix/6.0/ubuntu jammy InRelease' doesn't support architecture 'i386'

```

## Next, install the Zabbix Agent:

```
> sudo apt install zabbix-agent
```

```

ubuntu@ubuntu-virtual-machine: $ sudo 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 0 not upgraded.
Need to get 275 kB of additional disk space will be used.
After this operation, 781 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ma.archive.ubuntu.com/ubuntu jammy/universe amd64 libmodbus5 amd64 3.1.6-2 [23.5 kB]
Get:2 http://repo.zabbix.com/zabbix/6.0/ubuntu jammy/main amd64 zabbix-agent amd64 1:6.0.17-1+ubuntu22.04 [252 kB]
Fetched 275 kB in 2s (119 kB/s)
Selecting previously unselected package libmodbus5:amd64.
(Reading database... 197946 files and directories currently installed.)
Preparing to unpack .../libmodbus5_3.1.6-2_amd64.deb ...
Unpacking libmodbus5:amd64 (3.1.6-2) ...
Selecting previously unselected package zabbix-agent.
Preparing to unpack .../zabbix-agent_133ae_0.17-1+ubuntu22.04_amd64.deb ...
Unpacking zabbix-agent (1:6.0.17-1+ubuntu22.04) ...
Setting up libmodbus5:amd64 (3.1.6-2) ...
Setting up zabbix-agent (1:6.0.17-1+ubuntu22.04) ...
Created symlink /etc/systemd/system/multi-user.target.wants/zabbix-agent.service → /lib/systemd/system/zabbix-agent.service.
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.1) ...

```

## Configuring Zabbix Agent

After the installation is complete, we configure the Zabbix Agent to communicate with the Zabbix server. We edit the Zabbix Agent configuration file using nano:

```
> sudo nano /etc/zabbix/zabbix_agentd.conf
```

We find the following lines and we replace them with the correct information:

- Server=<Zabbix\_Server\_IP>
- ServerActive=<Zabbix\_Server\_IP>
- Hostname=<Hostname\_Of\_Ubuntu\_Client>

We replace <Zabbix\_Server\_IP> with the IP address of our Zabbix server, and <Hostname\_Of\_Ubuntu\_Client> with the hostname of our Ubuntu client. We save the changes and close the editor.

```

GNU nano 6.2
# 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=192.168.59.129

### Option: ListenPort
#     Agent will listen on this port for connections from the server.
#
# Mandatory: no
# Range: 1024-32767
# Default:
# ListenPort=10050

### Option: ListenIP
#     List of comma delimited IP addresses that the agent should listen on.
#     First IP address is sent to Zabbix server if connecting to it to retrieve list of active checks.
#
# Mandatory: no
# Default:
# ListenIP=0.0.0.0

### Option: StartAgents
#     Number of pre-forked instances of zabbix_agentd that process passive checks.
#     If set to 0, disables passive checks and the agent will not listen on any TCP port.
#
# Mandatory: no
# Range: 0-100
# Default:
# StartAgents=3

##### Active checks related

### Option: ServerActive
#     Zabbix server/proxy address or cluster configuration to get active checks from.
#     Server/proxy address is IP address or DNS name and optional port separated by colon.
#     Cluster configuration is one or more server addresses separated by semicolon.
#     Multiple Zabbix servers/clusters and Zabbix proxies can be specified, separated by comma.

```

## Starting and Enabling Zabbix Agent Service

Now that the configuration is done, we start the Zabbix Agent service and enable it to start automatically at boot, we check the status of the Zabbix Agent service with the following commands:

```

> sudo systemctl start zabbix-agent
> sudo systemctl enable zabbix-agent
> sudo systemctl status zabbix-agent

```

```

ubuntu@ubuntu-virtual-machine: $ sudo systemctl start zabbix-agent
ubuntu@ubuntu-virtual-machine: $ sudo systemctl enable zabbix-agent
Synchronizing state of zabbix-agent.service with sysv service script with /lib/systemd/systemd-sysv-install.
Executing /lib/systemd/systemd-sysv-install enable zabbix-agent
ubuntu@ubuntu-virtual-machine: $ 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 Fri 2023-05-26 18:44:24 +01; 2min 45s ago
     Main PID: 4390 (zabbix_agentd)
        Tasks: 6 (limit: 4573)
       Memory: 6.5M
          CPU: 49ms
      CGroup: /system.slice/zabbix-agent.service
              └─4390 /usr/sbin/zabbix_agentd -c /etc/zabbix/zabbix_agentd.conf

May 26 18:44:24 ubuntu-virtual-machine systemd[1]: Starting Zabbix Agent...
May 26 18:44:26 ubuntu-virtual-machine systemd[1]: Started Zabbix Agent.

```

## Adding the Zabbix Client to the Zabbix Server

Lastly, we need to add the newly installed Zabbix Agent to the Zabbix server. Log in to the Zabbix web interface, navigate to “Configuration” > “Hosts” > “Create Host”, and fill in the necessary details.

ZABBIX

Hosts

Host groups: type here to search Select

Monitored by: Any Server Proxy

Templates: type here to search Select

Name:

DNS:

IP:

Port:

Tags: AndOr Or

Tag:  Contains  value

Add

Apply Reset

Name	Items	Triggers	Graphs	Discovery	Web	Interface	Proxy	Templates	Status	Availability	Agent encryption	Info	Tags
Zabbix server	Items 125	Triggers 69	Graphs 25	Discovery 4	Web	127.0.0.1:10050	Linux by Zabbix agent, Zabbix server health	Enabled			None	Displaying 1 of 1 found	

0 selected

Zabbix 6.0.17. © 2001–2023, Zabbix SIA

## Adding Zabbix Host to Server

ZABBIX

Hosts

New host

Host IPMI Tags Macros Inventory Encryption Value mapping

\* Host name:

Visible name:

Templates:  Remove

Groups:  Remove

Interfaces

Name	Type	IP address	DNS name	Connect to	Port	Default
Agent	IP	192.168.59.128			10050	<input checked="" type="radio"/> Remove

Add Description

Monitored by proxy: (no proxy)

Enabled

Add Cancel

Zabbix 6.0.17. © 2001–2023, Zabbix SIA

After adding the host, we should see the host status as “Enabled”. Within a few minutes, the Zabbix server will start receiving data from the Zabbix Agent installed on our Ubuntu 22.04 system

zabbix: Configuration of | +

Go back one page (Alt+Left Arrow)  
Right-click or pull down to show history

Hosts

Monitoring Services Inventory Reports Configuration Host groups Templates Hosts Maintenance Actions Event correlation Discovery Administration Support Integrations Help User settings Sign out

Hosts

Host groups: type here to search Select Monitored by: Any Server Proxy

Templates: type here to search Select

Name:  DNS:  IP:  Port:

Proxy:  Select

Tags: AndOr Or

Add tag: Contains value: Remove

Apply Reset

Name	Items	Triggers	Graphs	Discovery	Web	Interface	Proxy	Templates	Status	Availability	Agent encryption	Info	Tags
ubuntu	Items 42	Triggers 14	Graphs 8	Discovery 3	Web	192.168.59.128:10050	Linux by Zabbix agent		Enabled	ZBX	None		
Zabbix server	Items 125	Triggers 69	Graphs 25	Discovery 4	Web	127.0.0.1:10050	Linux by Zabbix agent, Zabbix server health		Enabled	ZBX	None		

Displaying 2 of 2 found

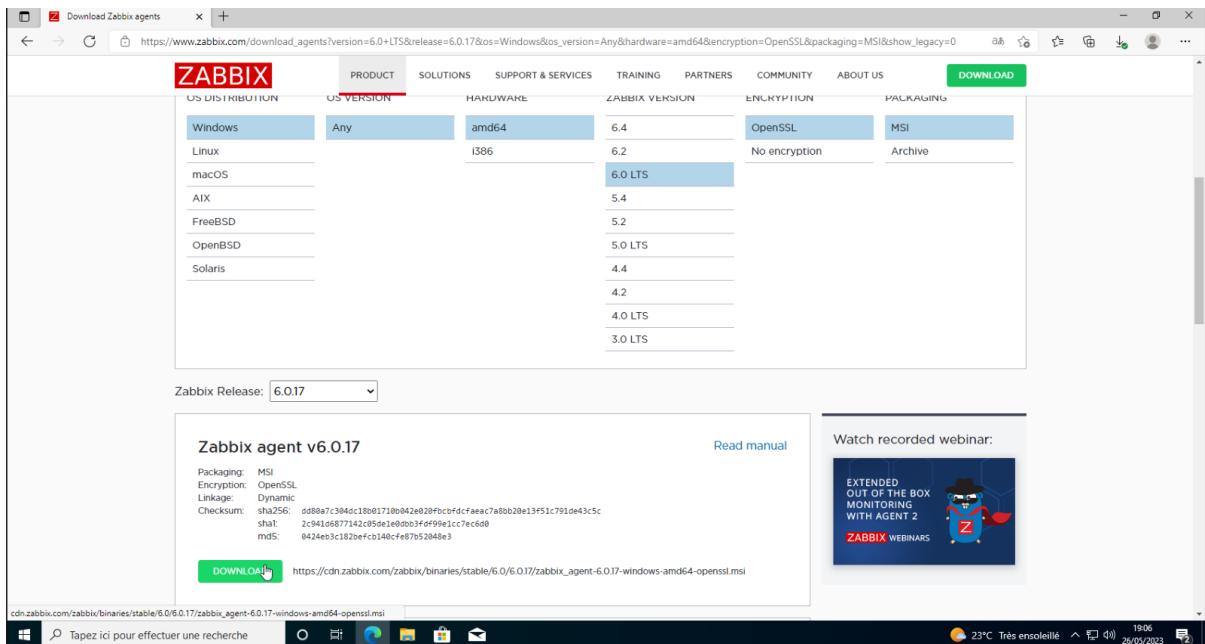
0 selected Enable Disable Export Mass update Delete

Zabbix 6.0.17. © 2001–2023, Zabbix SIA

# Monitoring Windows machine with Zabbix using agent

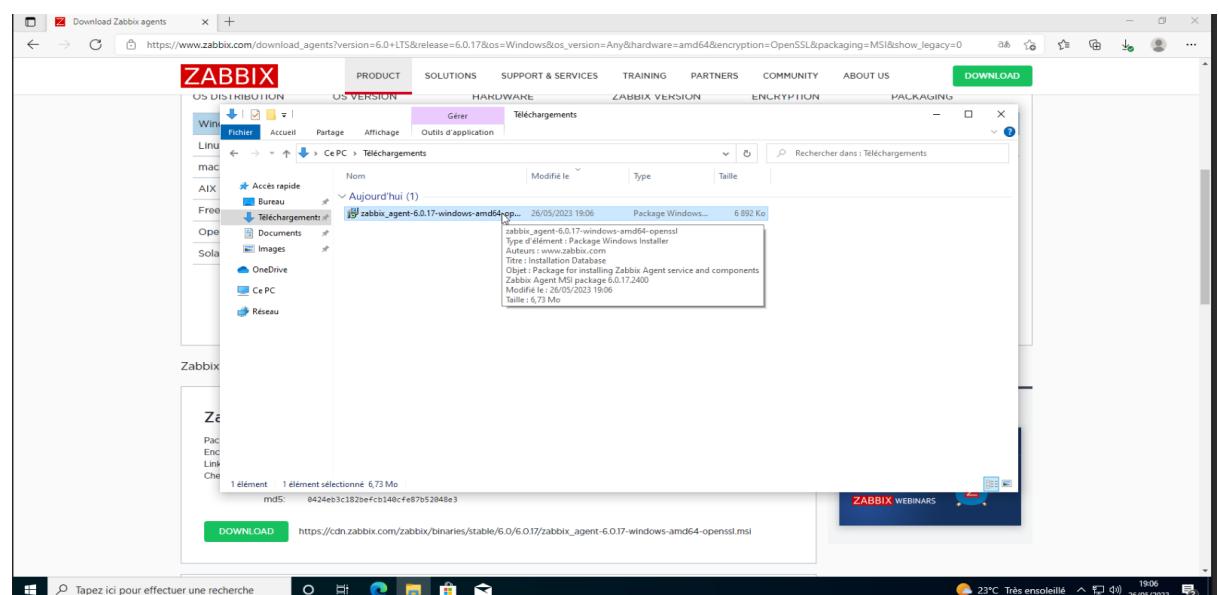
## Installing Zabbix Agent

We download Zabbix Windows agent install from the  
[https://www.zabbix.com/download\\_agents](https://www.zabbix.com/download_agents)



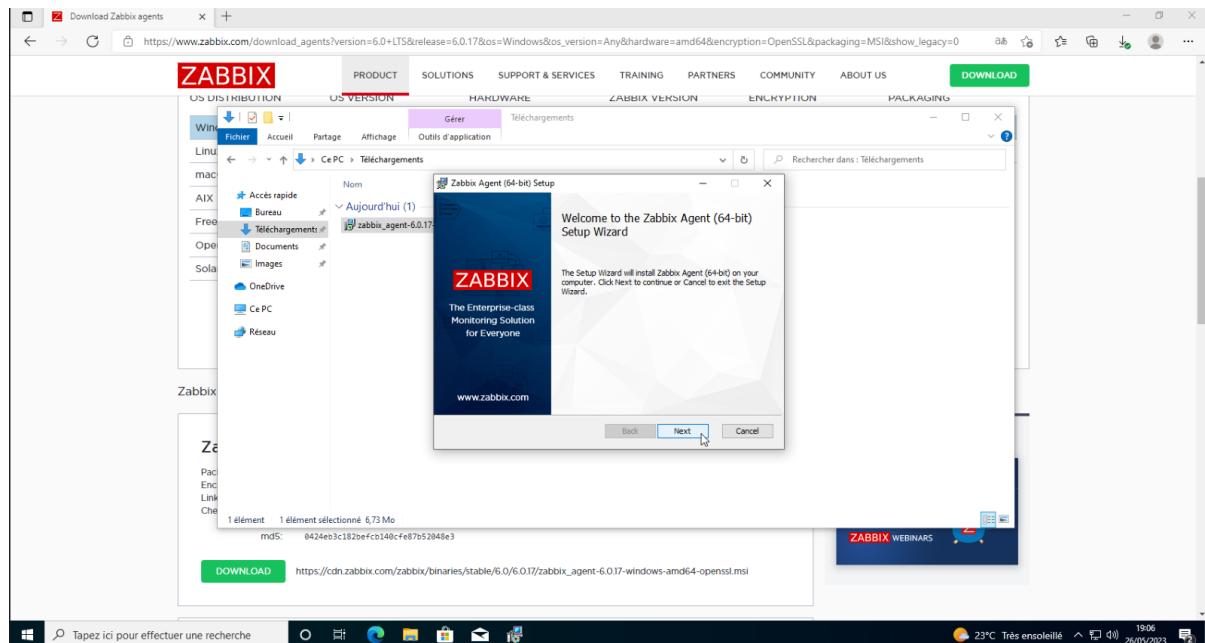
The screenshot shows the Zabbix download page for version 6.0.17. The 'OS VERSION' dropdown is set to 'Windows'. The 'PACKAGING' dropdown shows 'MSI' selected. Below the table, a 'Zabbix Release' dropdown is set to '6.0.17'. A central box displays the 'Zabbix agent v6.0.17' details, including its packaging (MSI), encryption (OpenSSL), and checksums. A 'DOWNLOAD' button is present. To the right, there's a 'Watch recorded webinar' section for 'EXTENDED OUT OF THE BOX MONITORING WITH AGENT 2'.

Launch the installation Wizard



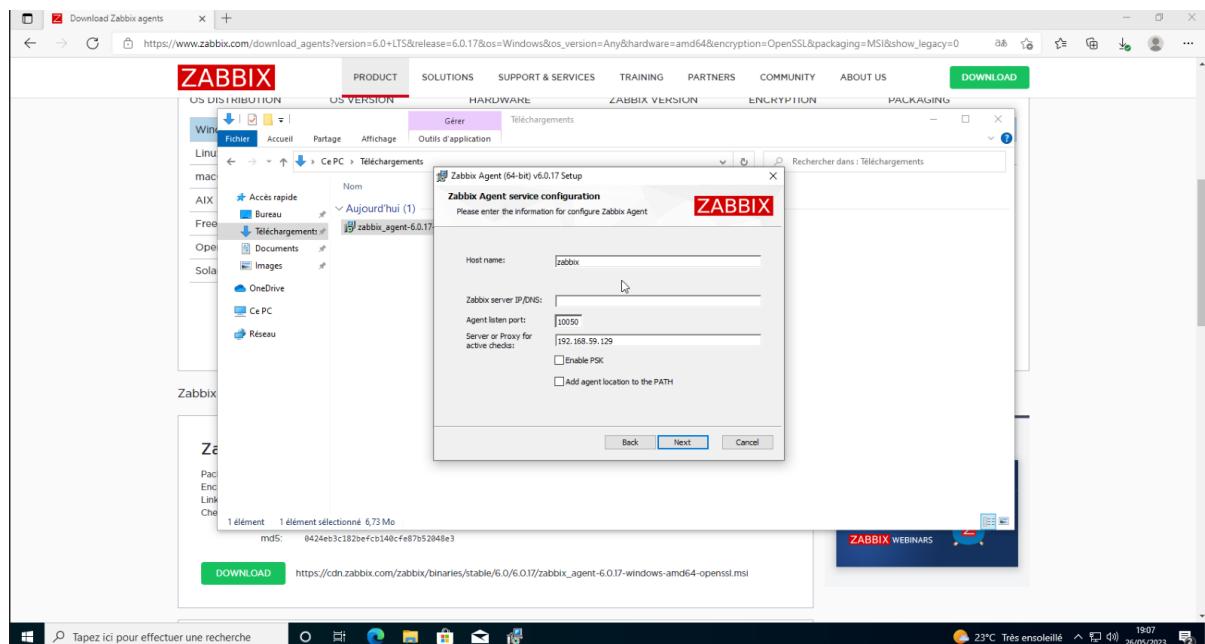
The screenshot shows the Windows File Explorer with a single file selected: 'zabbix\_agent-6.0.17-windows-amd64-openssl.msi'. The file is a 'Package Windows...' type, 6 892 Ko in size, and was modified on 26/05/2023 at 19:06. The file path is 'Ce PC > Téléchargements > Aujourd'hui (1)'. A 'ZABBIX WEBINARS' watermark is visible in the bottom right corner.

Click Next and accept the End User License Agreement.



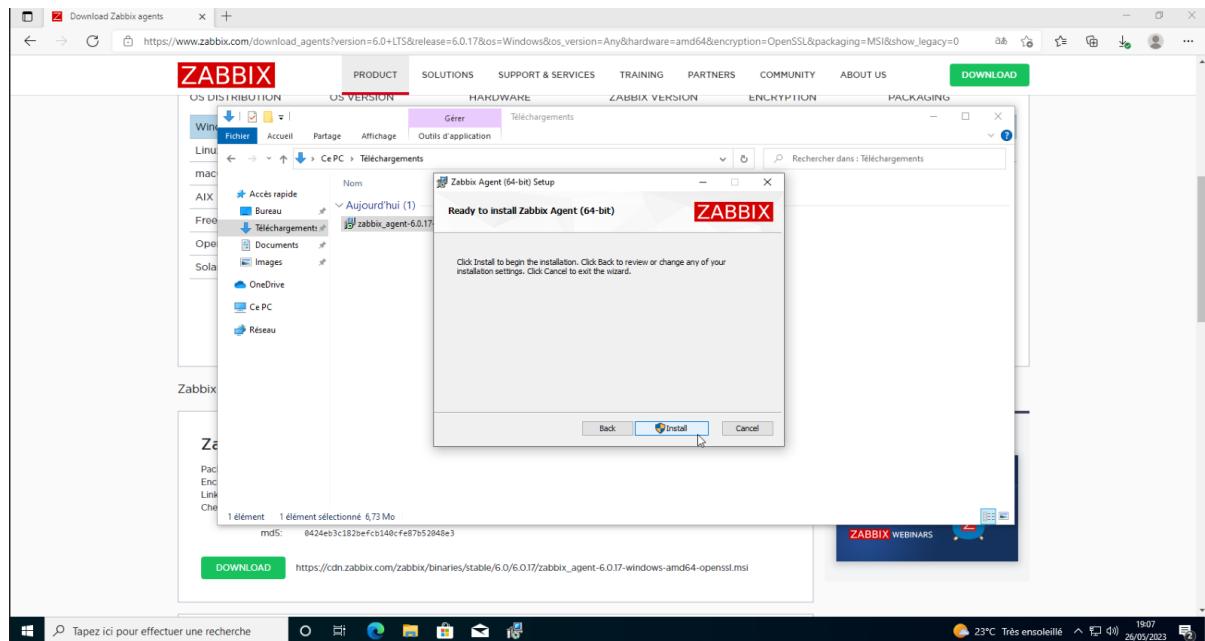
## Configuring Zabbix Agent

Next, Set the Zabbix agent hostname, the Zabbix server IP. Define the correct hostname as this must match the hostname while adding the host to Zabbix server for monitoring.



On Custom setup, just click Next.

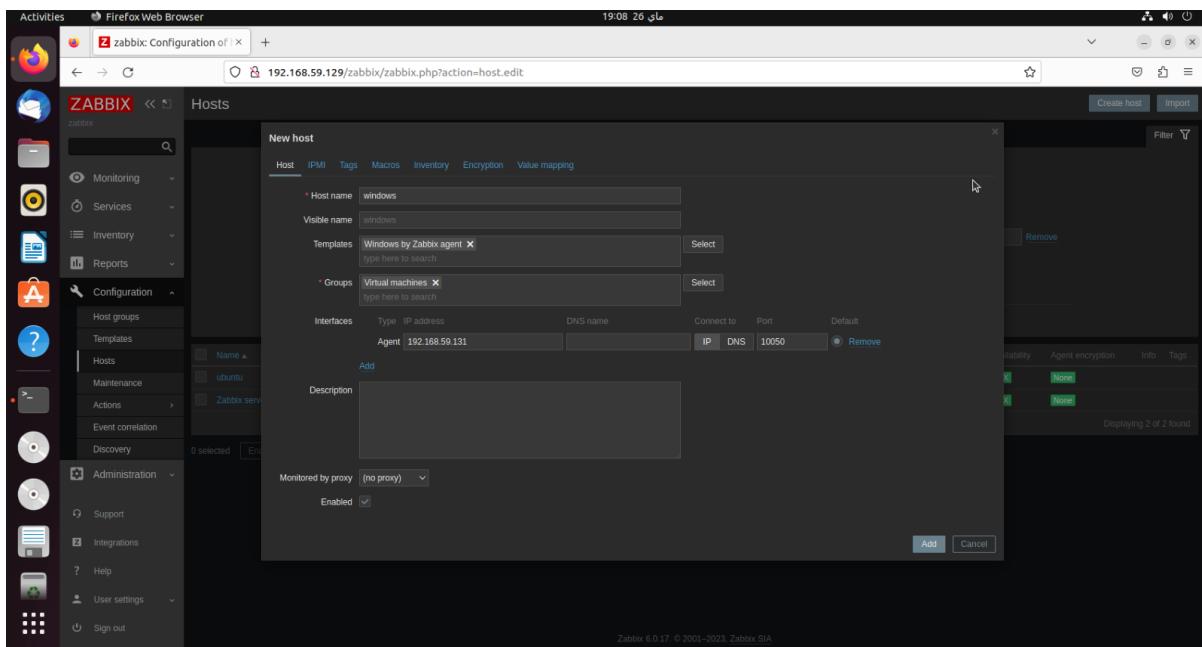
Click Install to install Zabbix agent on Windows.



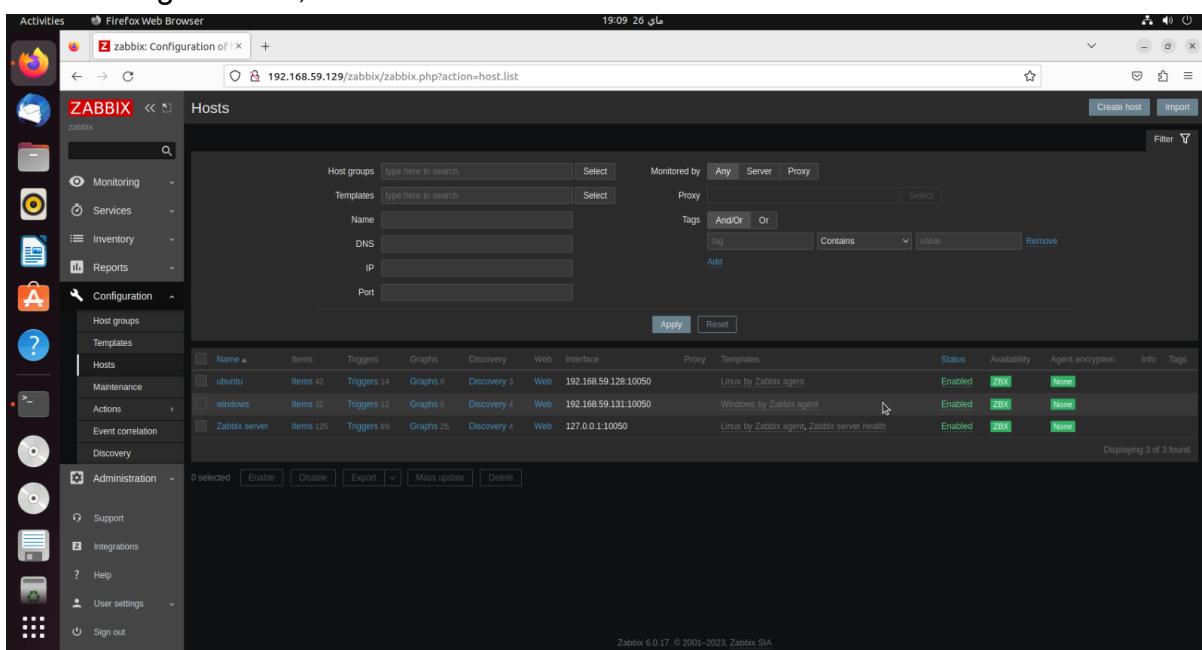
When the installation is done, we click Finish to exit the Zabbix agent installation wizard.

## Adding the Zabbix Client to the Zabbix Server

Lastly, we add the newly installed Zabbix Agent to the Zabbix server. We log into the Zabbix web interface, navigate to “Configuration” > “Hosts” > “Create Host”, and we fill in the necessary details.



After adding the host, we should see the host status as “Enabled”.



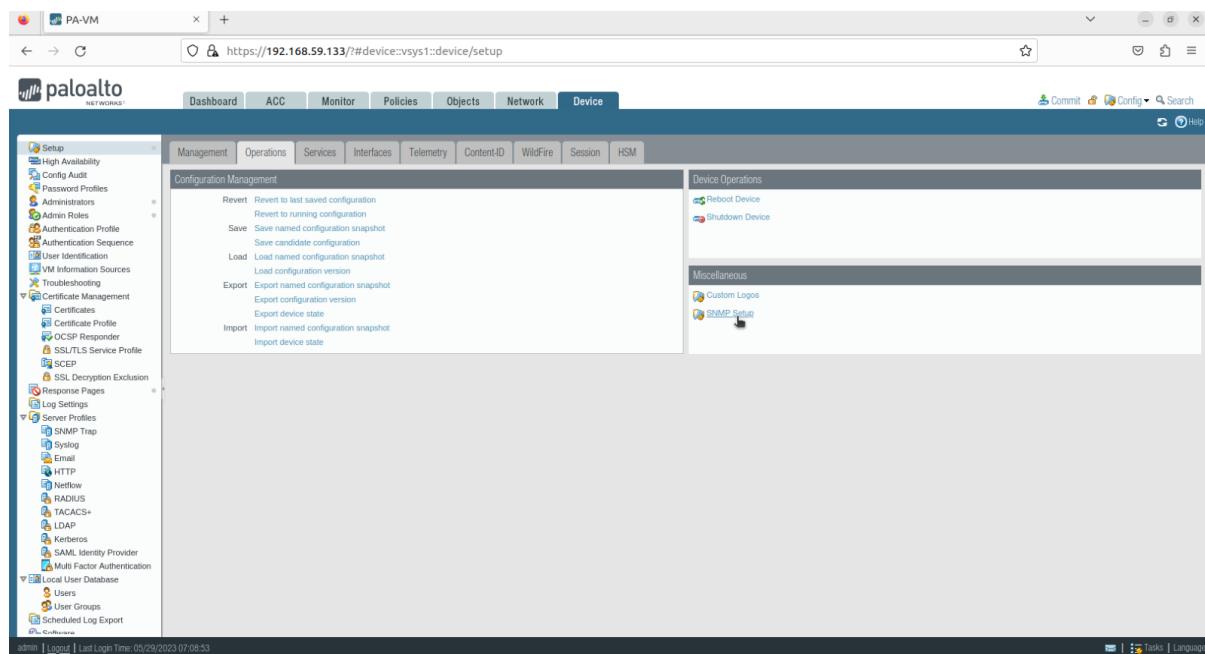
# Monitoring Palo Alto with Zabbix via SNMPv3

## Configuring and enabling SNMP on Palo Alto

First, we should configure and enable SNMP on Palo Alto.

We navigate to Device > Setup > Operations.

In the lower right corner, click SNMP Setup.



We choose the version SNMPv3. In the View section, we click Add. We enter name for the group, then we configure the following for each view we add to the group:

**View:** Specify a name for the view. The name can have up to 31 characters that are alphanumeric, periods, underscores, or hyphens.

**OID:** Specify the OID of the MIB.

**Option:** Select the matching logic to apply to the MIB.

**Mask:** Specify the mask in hexadecimal format.

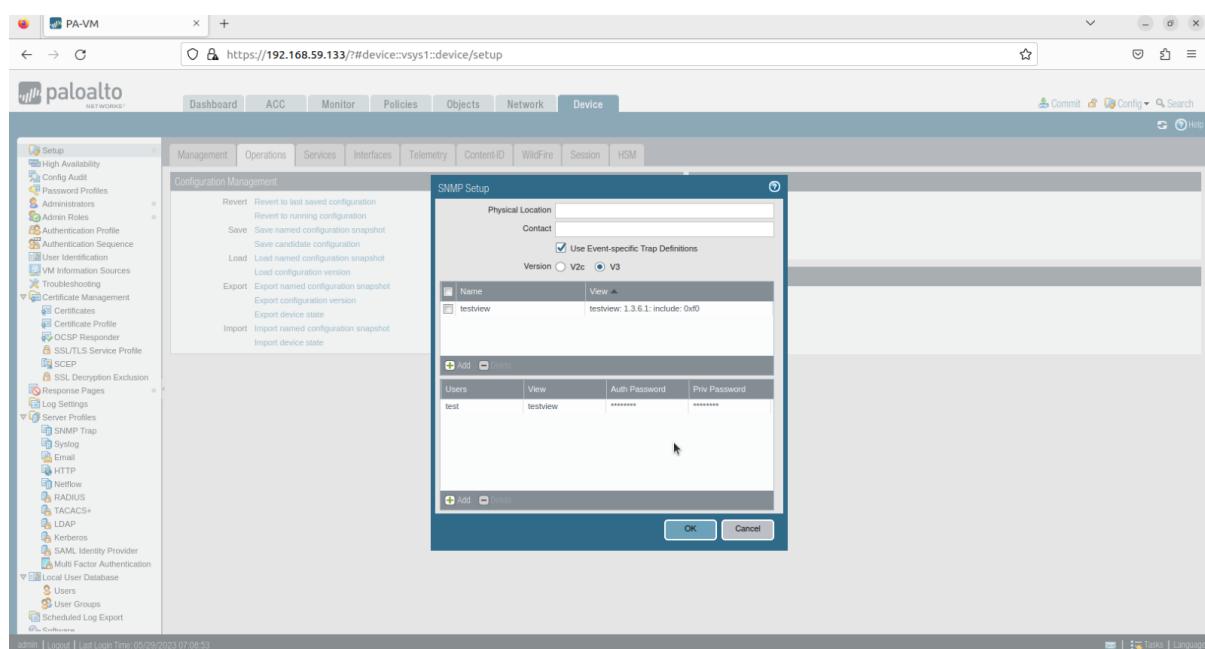
In the User section, we click Add. We enter a name for the user, then we configure the following fields for each view we add to the group:

**User Name:** Specify a username to identify the SNMP user account. The username we configure on the firewall must match the username configured on the SNMP manager. The username can have up to 31 characters.

**View:** Assign a group of views to the user.

**Authentication Password:** Type and confirm the authentication password. The firewall uses the secure hash algorithm (SHA-1 160) to encrypt the password. The password must be between 8 and 256 characters long. All characters are allowed.

**Privacy Password:** Type and confirm privacy password. The firewall uses the password and Advanced Encryption Standard 128 (AES-128) to encrypt SNMP traps and responses to statistics requests. The password must be between 8 and 256 characters long. All characters are allowed.



## Enabling SNMP on the Management interface

Navigate to Device > Setup > Interfaces.

Click the Management button.

Tick the SNMP box.

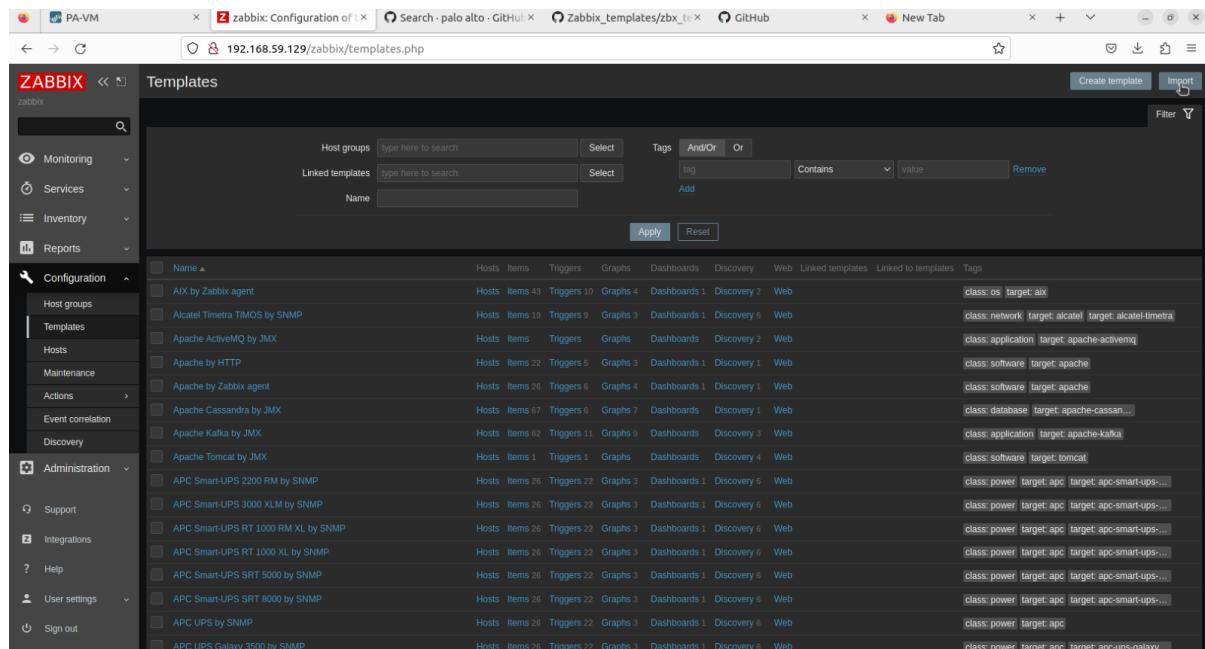
The screenshot shows the Palo Alto Networks Device Setup interface. The URL is <https://192.168.59.133/#device::vsys1::device/setup>. The main navigation bar includes Dashboard, ACC, Monitor, Policies, Objects, Network, and Device. The 'Device' tab is active. On the left, a sidebar lists categories such as Setup, High Availability, Config Audit, Password Profiles, Administrators, Admin Roles, Authentication Profile, Authentication Sequence, User Identification, VM Information Sources, Troubleshooting, Certificate Management, Log Settings, Server Profiles, and Local User Database. The 'Interfaces' tab is selected, showing a table with one row for the 'Management' interface. The table columns are Interface Name, Enabled, Speed, IP Address, and Services Enabled. The 'Management' interface is listed with 'Enabled' checked, 'Speed' as 'auto-negotiate', 'IP Address' as 'auto-negotiate', and 'Services Enabled' as 'Ping,HTTPS,SSH'. At the bottom right of the interface, there are 'Commit', 'Config', 'Search', and other navigation links.

And we click on Commit to valid my configuration

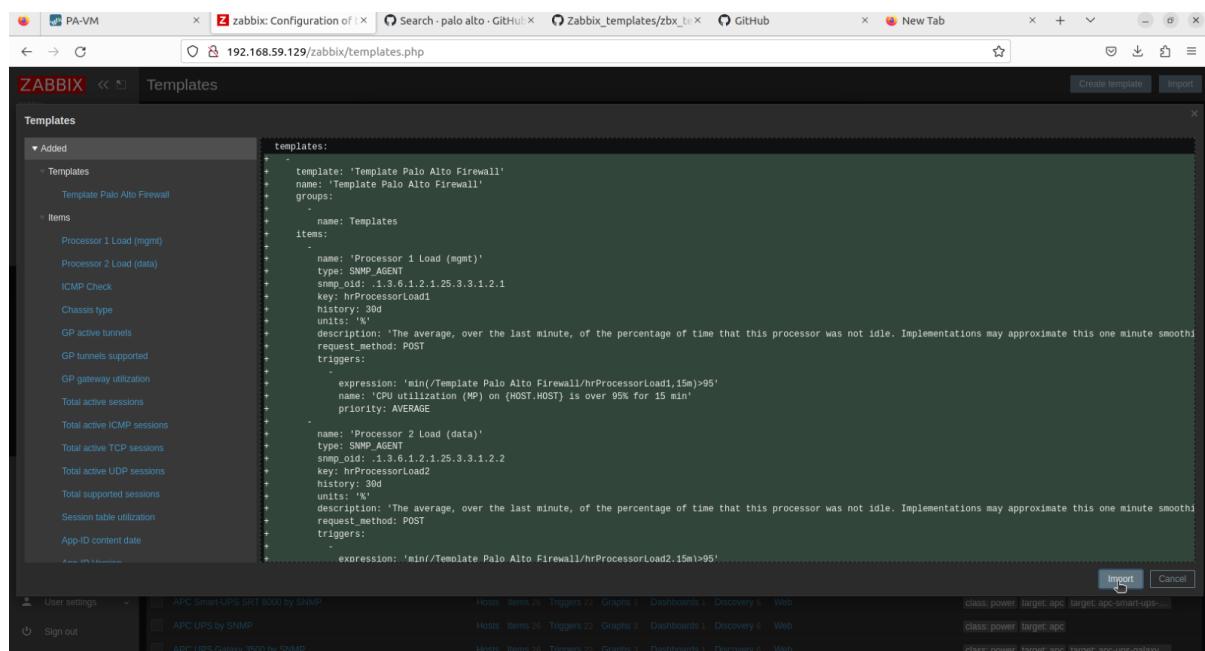
The screenshot shows the same Palo Alto Networks Device Setup interface as the previous one, but with a prominent yellow 'Commit' button highlighted in the top right corner. A message box above the button says 'There are pending configuration changes, please commit.' The rest of the interface and sidebar are identical to the first screenshot.

# Adding PaloAlto to Zabbix server

We log in to the Zabbix web interface, we navigate to “Configuration” > Templates” > “Import”.



We import the template Palo Alto SNMPv3 (we find it on github)



We navigate to “Configuration” > “Hosts” > “Create Host”, and we fill in the necessary details.

The screenshot shows the Zabbix web interface with the URL `192.168.59.129/zabbix/zabbix.php?action=host.edit`. The left sidebar is collapsed, showing the main navigation menu. The main content area is titled "New host" under the "Hosts" section. The host configuration form is filled with the following details:

- Host name:** Palo Alto
- Visible name:** Palo Alto
- Template:** Template Palo Alto Firewall
- Groups:** Virtual machines
- Interfaces:**
  - Name:** SNMP
  - Type:** IP address
  - IP address:** 192.168.59.133
  - DNS name:** (empty)
  - Connect to:** IP
  - Port:** 161
  - Default:** (radio button selected)
  - SNMP version:** SNMPv3
  - Context name:** (empty)
  - Security name:** test
  - Security level:** authPriv
  - Authentication protocol:** SHA1
  - Authentication passphrase:** Password
  - Privacy protocol:** AES128
  - Privacy passphrase:** Password

At the bottom right of the dialog, there are "Add" and "Cancel" buttons. A status bar at the bottom of the page indicates "Zabbix 6.0.17, © 2001-2023, Zabbix SIA".

# Monitoring FortiGate with Zabbix via SNMPv3

## Configuring and enabling SNMP on FortiGate

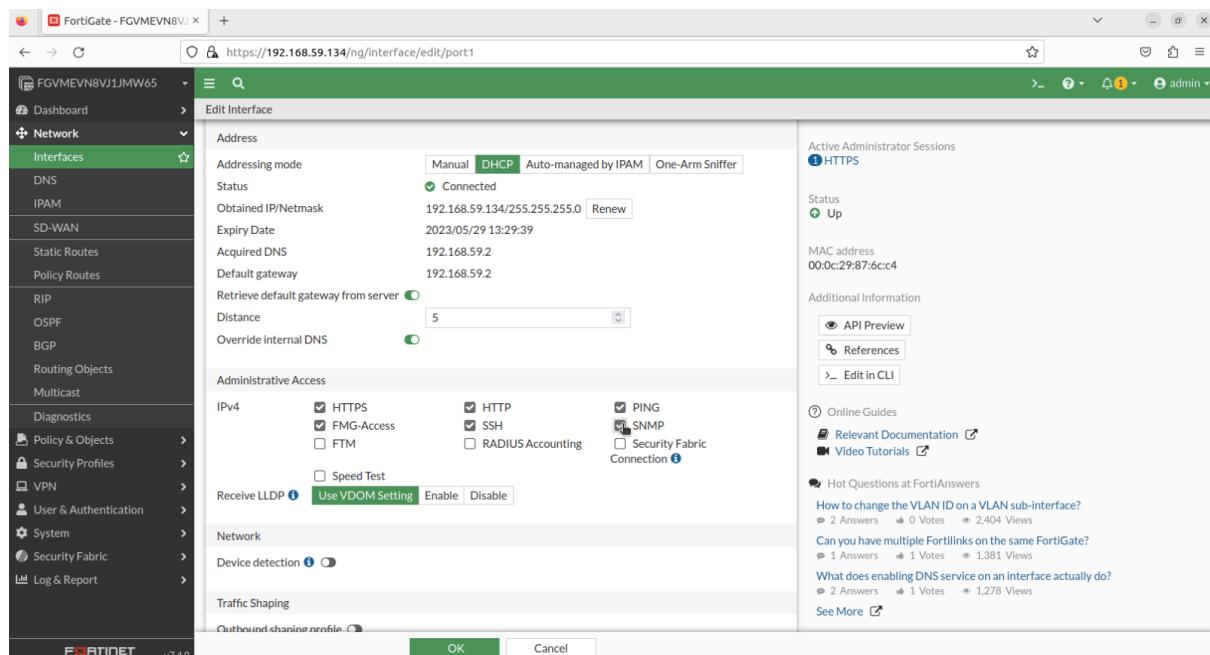
First, we should configure and enable SNMP on FortiGate.

Go to Network -> Interfaces.

Choose an interface that an SNMP manager connects to and select 'Edit'.

In Administrative Access, select 'SNMP'.

Select 'OK'.



Navigate to "System > SNMP"

Click Enable the SNMP Agent

Click "Apply"

To enable SNMP v3:

In the SNMP v3 section, select "Create New"

Set our preferred User Name and Auth level

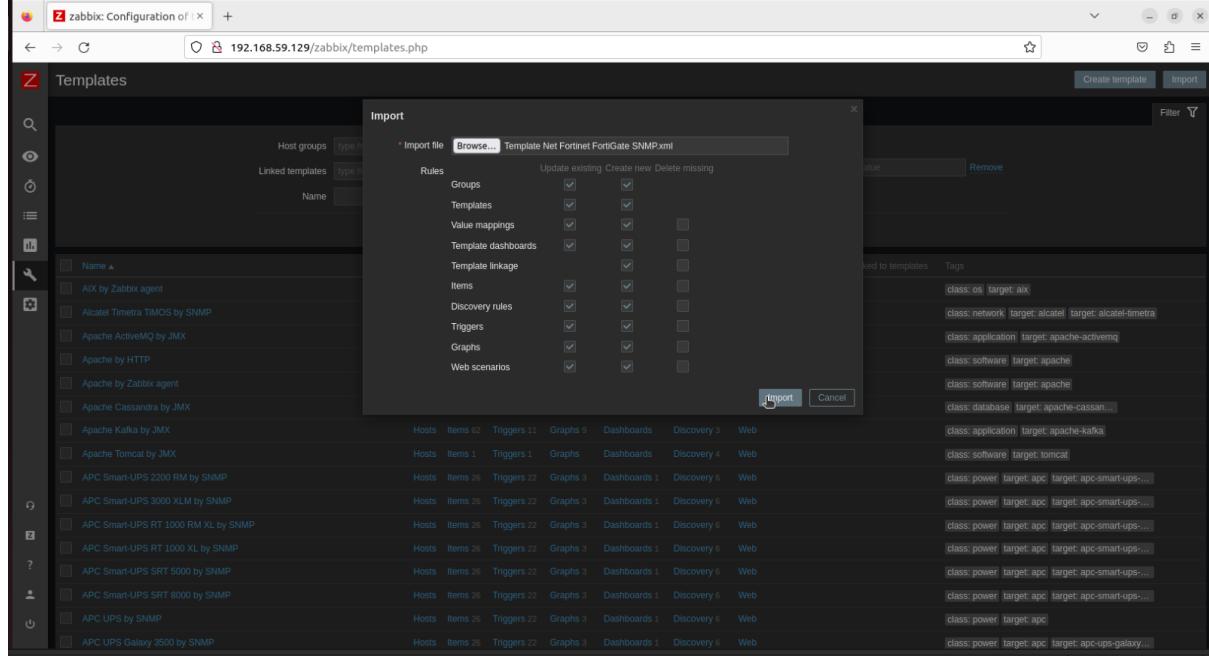
Ensure Enable Query is checked and the port is set to 161

Click "OK".

Name	Security Level	Queries	Traps	Host	Events	Status
admin	Authentication Private	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable	192.168.1.100	37	<input checked="" type="checkbox"/> Enable

# Adding FortiGate to Zabbix server

We log in to the Zabbix web interface, we navigate to “Configuration” > Templates” > “Import”. (We find it on github)



We navigate to “Configuration” > “Hosts” > “Create Host”, and we fill in the necessary details.

# Monitoring ESXi with Zabbix via SNMPv3

## Configuring and enabling SNMP on ESXi

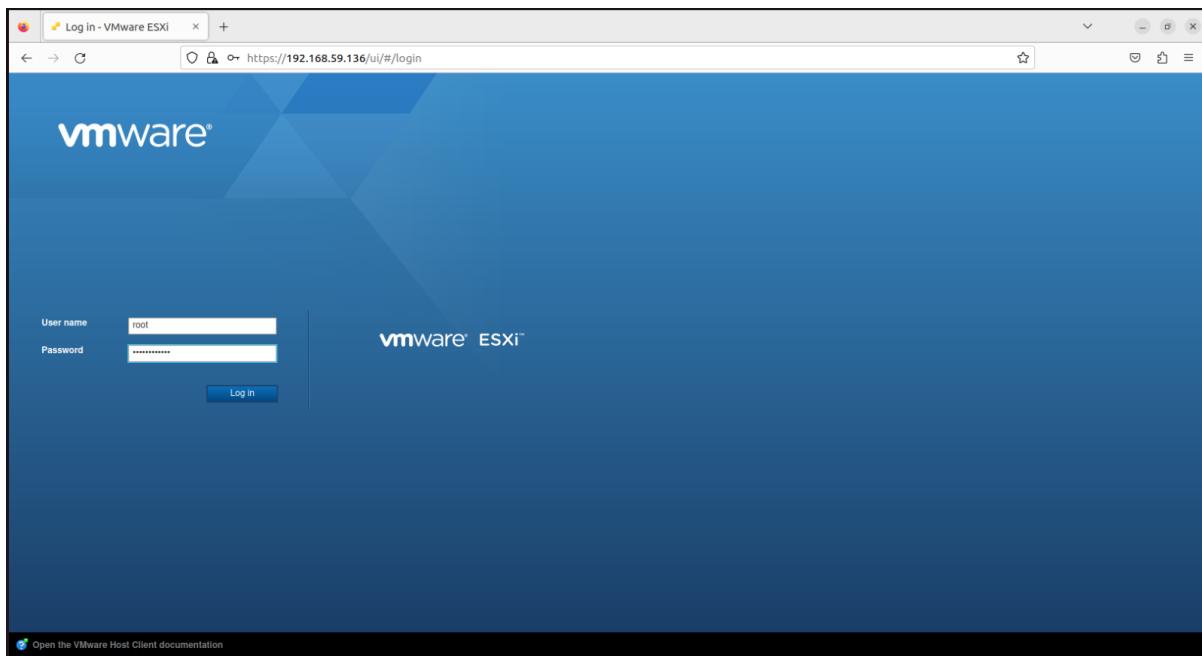
First, we should configure and enable SNMP on ESXi.

Here's how to enable SNMP on ESXi:

- Enable Secure Shell (SSH)
- Configure SNMP
- Configure ESXi Firewall

## Enabling SSH Access on ESXi

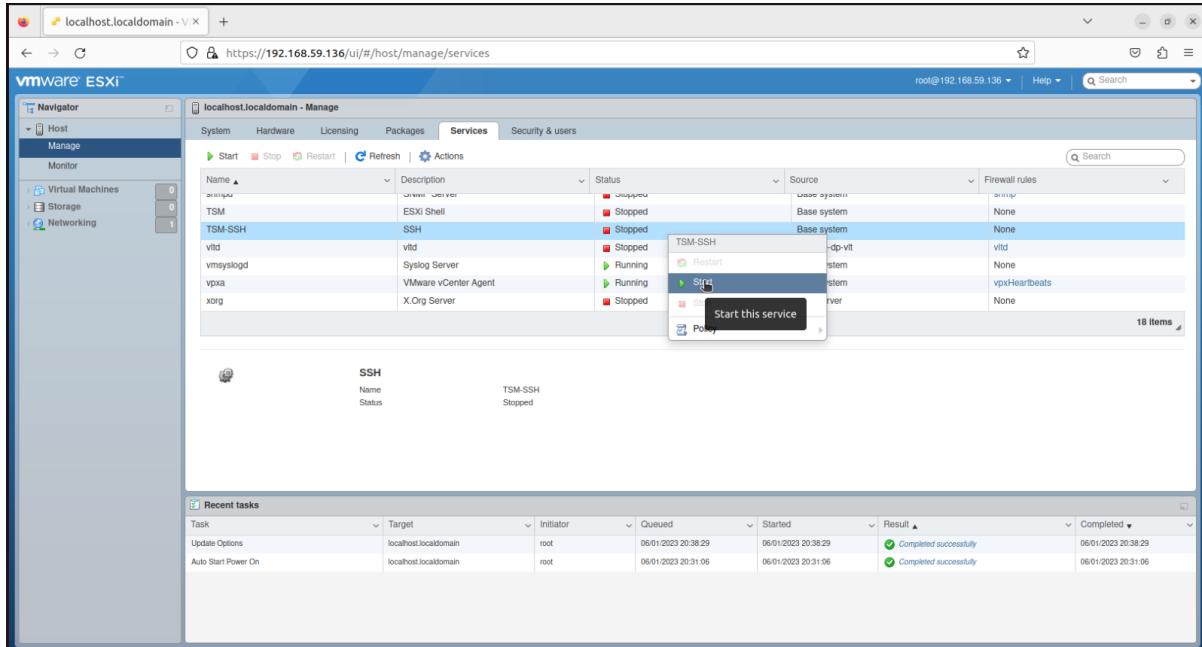
SSH access on an ESXi host is needed to run ESXCLI commands on a host remotely. To enable SSH access to our ESXi host, we can use VMware Host Client. We open a web browser, enter the IP address of our ESXi host in the address bar, then enter credentials to log in.



In the Navigator pane, go to Host > Manage and click the Services tab.

Right-click TSM-SSH and, in the context menu, click Start.

On the screenshot below we see the started SSH server service on the ESXi host.



Now we can connect to the ESXi host from a machine with an SSH client installed. If we're using Windows, we can use PuTTY, a free and convenient SSH client. In Linux, run the SSH client from the command line with the command:

```
> ssh our_username@host_ip_address
```

A screenshot of a terminal window titled 'ubuntu@ubuntu-virtual-machine: ~'. The user is attempting to log in via SSH as 'root' to the IP '192.168.59.136'. The system prompts for a password, which is entered. The terminal then displays a warning about ECDSA key fingerprints and adds the host to the list of known hosts. Finally, it shows the user prompt again.

## ESXi SNMP Configuration

Once SSH access to the ESXi host is established, we can configure VMware ESXi SNMP options. On ESXi hosts, SNMP can be configured only in [the command-line interface](#). The graphical user interface (GUI) allows us only to start, stop, and restart the SNMP service.

We run the command in the console (terminal) and we check the SNMP status on the ESXi host:

```
> esxcli system snmp get
```

SNMP is disabled by default. The output for disabled SNMP on ESXi is shown on the screenshot. Most of the parameters are empty and or not configured.

```
[root@localhost:~] esxcli system snmp get
Authentication:
Communities:
Enable: false
Enginieid:
Hwsrc: indications
Largestorage: true
LogLevel: warning
Notraps:
Port: 161
Privacy:
Remoteusers:
Syscontact:
Syslocation:
Targets:
Users:
V3targets:
```

## Configuring parameters of an SNMP agent

Set SNMP parameters for an SNMP agent on the ESXi host.

Set the community's name.

```
> esxcli system snmp set --communities techsogroup
```

Set the SNMP target. The SNMP target is a server on which monitoring software is installed to handle SNMP traps and collect monitoring information. In my example, the SNMP target is the machine running Zabbix server (192.168.59.29). UDP 161 is the default port used for SNMP and this port is defined in my ESXi SNMP configuration:

```
> esxcli system snmp set --targets=192.168.59.129@161/user
```

Specify a location, for example, the geographical location, address, datacenter, or a room where the server is located:

```
> esxcli system snmp set --syslocation Casablanca
```

Specify contact information. The system administrator's email address can be defined for this parameter:

```
> esxcli system snmp set --syscontact user@techsogroup.com
```

Enable SNMP on ESXi:

```
>esxcli system snmp set --enable true
```

Check the SNMP status on the ESXi host again:

```
>esxcli system snmp get
```

Now we can see that the parameters are configured.

```
[root@localhost:] esxcli system snmp set --communities techsogroup
[root@localhost:] esxcli system snmp set --targets=192.168.59.129@161/user
[root@localhost:] esxcli system snmp set --syslocation Casablanca
[root@localhost:] esxcli system snmp set --syscontact user@techsogroup.com
[root@localhost:] esxcli system snmp set --enable true
[root@localhost:] esxcli system snmp get
  Authentication: SHA1
  Communities: techsogroup
  Enable: true
  Engineid: 800001ADC0512908830881685648637
  Hwsrc: indications
  Largestorage: true
  Loglevel: warning
  Notraps:
  Port: 161
  Privacy: AES128
  Remoteusers:
  Syscontact: user@techsogroup.com
  Syslocation: Casablanca
  Targets: 192.168.59.129@161 user
  Users: user/5fd187207553e6dd5708c7ae4aa1d7e7904c40b1/abcd6919b7469d416104f5d73cd142772ec5001e/priv
  V3targets: 192.168.59.129@161 user priv trap
```

SNMP status is running now. We can also open VMware Host Client, go to Host > Manage > Services, and check the status of the snmpd service.

The screenshot shows the VMware Host Client web interface. The top navigation bar includes links for Home, Host, Manage, Monitor, and Help. The URL is https://192.168.59.136/ui/#/host/manage/services. The left sidebar has sections for Host, Manage (selected), and Monitor, with sub-options like Virtual Machines, Storage, and Networking. The main content area has tabs for Navigator, System, Hardware, Licensing, Packages, Services (selected), and Security & users. Under the Services tab, there is a table with columns: Name, Description, Status, Source, and Firewall rules. The table lists several services: ptpd (Stopped, Base system, ptpd), stcbcd-watchdog (Stopped, Base system, CIMHttpServer, CIMHttpsServer), slpd (Stopped, Base system, CIMSLP), snmpd (Running, Base system, snmp), TSM (Stopped, Base system, None), TSM-SSH (Running, Base system, None), and vftd (Stopped, vmware-dp-vt, vftd). A search bar is at the top right of the table. Below the table is a "Recent tasks" section with a table showing tasks like Update Service Policy, Refresh Services, Start Service, Update Options, Auto Start Power On, and Refresh Services, all completed successfully on 06/01/2023 at various times between 20:39:41 and 20:45:57.

## Configuring ESXi Firewall

We must configure the firewall and enable SNMP access from monitoring servers to the ESXi host. We can set a subnet or a single IP address of allowed devices in the network.

We run these three commands to allow access from the 192.168.59.0/24 network to monitor ESXi via SNMP:

```
>esxcli network firewall ruleset set --ruleset-id snmp --allowed-all false  
  
>esxcli network firewall ruleset allowedip add --ruleset-id snmp  
--ip-address 192.168.59.0/24  
  
>esxcli network firewall ruleset set --ruleset-id snmp --enabled true
```

```
[root@localhost:-] esxcli network firewall ruleset set --ruleset-id snmp --allowed-all false
```

```
[root@localhost:-] esxcli network firewall ruleset allowedip add --ruleset-id snmp --ip-address 192.168.59.0/24
```

```
[root@localhost:-] esxcli network firewall ruleset set --ruleset-id snmp --enabled true
```

## Configuring SNMP v3

SNMP v3 is a more secure version of the protocol providing key authentication and encryption. Below is an overview of how to enable SNMP v3 on an ESXi host.

We set authentication protocol and privacy options.

```
> esxcli system snmp set -a SHA1 -x AES128
```

Where:

SHA1 is the algorithm for cryptographic encryption, the cryptographic hash function (Secure Hash Algorithm 1).

AES128 is the encryption method (Advanced Encryption Standard with a 128-bit encryption key) using the symmetric block cipher.

```
[root@localhost:-] esxcli system snmp set -a SHA1 -x AES128
```

We generate hashes by using the command:

```
> esxcli system snmp hash --auth-hash Password1 --priv-hash  
Password2 --raw-secret  
[root@localhost:-] esxcli system snmp hash --auth-hash Password1 --priv-hash Password2 --raw-secret  
Authhash: 5fd187207553e6dd5708c7ae4aa1d7e7904c40b1  
Prvhash: abed6919b7469d416104f5d73cd142772ec5001e
```

We use the generated hashes and add a user. Adding up to five users is supported.

```
> esxcli system snmp set -e yes -C user -u  
snmpuser/authhash/prvhash/priv
```

Where:

user is the contact email for the user

snmpuser is the username (can be up to 32 characters)

authhash is the authentication hash value

prvhash is the privacy hash value

We add user and use hashes generated in the output of the previous command.

```
[root@localhost:-] esxcli system snmp set -e yes -C user@techsogroup.com -u user/5fd187207553e6dd5708c7ae4aa1d7e7904c40b1/abed6919b7469d416104f5d73cd142772ec5001e/prv
```

Define the SNMP target address:

```
> esxcli system snmp set --v3targets  
192.168.59.129@161/user/priv/trap
```

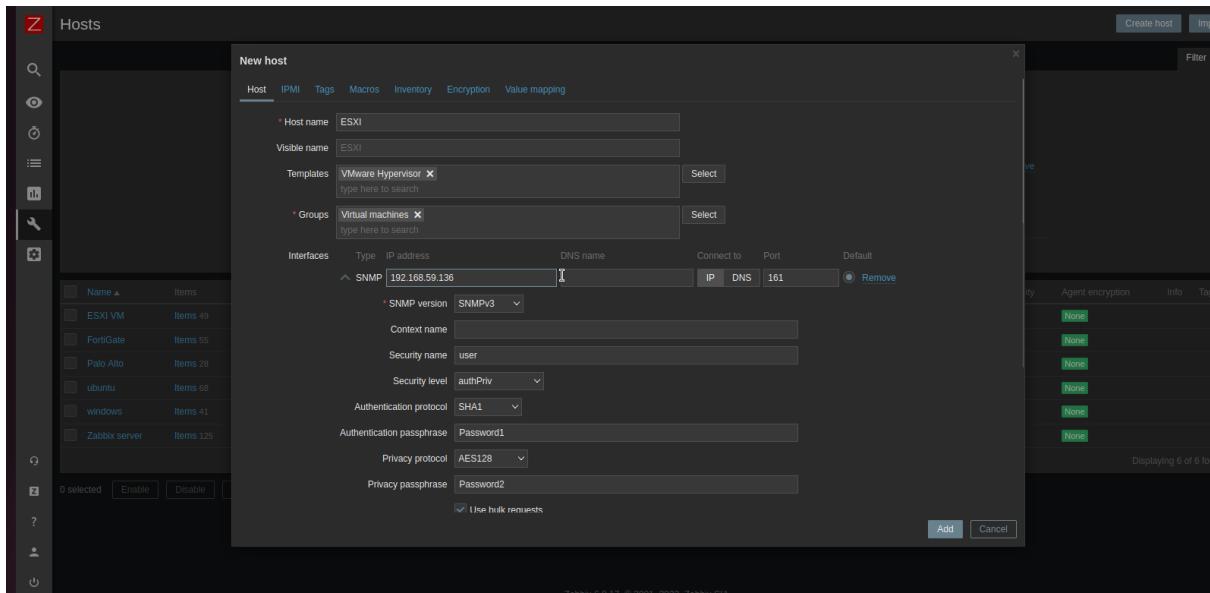
We enable SNMP on ESXi:

```
>esxcli system snmp set --enable true
```

```
[root@localhost:-] esxcli system snmp set --v3targets 192.168.59.129@161/user/priv/trap  
[root@localhost:-] esxcli system snmp set --enable true
```

## Adding ESXI to Zabbix server

We log in to the Zabbix web interface, we navigate to “Configuration” > “Hosts” > “Create Host”, and we fill in the necessary details.



# Zabbix Maps for Better Visualization

Here's a screen from my Zabbix server after adding all hosts.

The screenshot shows the Zabbix 6.0.18 web interface with the URL [https://192.168.59.129/zabbix/zabbix.php?name=&ip=&dns=&port=&status=-1&evaltype=0&tags\[0\]\[tag\]=&tags\[0\]\[operator\]=0&tags\[0\]\[value\]=&maintenance\\_](https://192.168.59.129/zabbix/zabbix.php?name=&ip=&dns=&port=&status=-1&evaltype=0&tags[0][tag]=&tags[0][operator]=0&tags[0][value]=&maintenance_). The left sidebar is visible with various navigation options like Monitoring, Dashboard, Problems, Hosts, Maps, etc. The main content area is titled 'Hosts' and displays a table of currently monitored hosts. The table columns include Name, Interface, Availability, Tags, Status, Latest data, Problems, Graphs, Dashboards, and Web. The hosts listed are:

Name	Interface	Availability	Tags	Status	Latest data	Problems	Graphs	Dashboards	Web
ESXI	192.168.59.136:161	SNMP		Enabled	Latest data 56	0	Graphs 8	Dashboards 2	Web
FortiGate	192.168.59.134:161	SNMP		Enabled	Latest data 55	1	Graphs 7	Dashboards 4	Web
Palo Alto	192.168.59.133:161	SNMP		Enabled	Latest data 28	0	Graphs 2	Dashboards	Web
ubuntu	192.168.59.128:10050	ZBX	class:os target:linux	Enabled	Latest data 68	1	Graphs 14	Dashboards 2	Web
windows	192.168.59.131:10050	ZBX	class:os target:windows	Enabled	Latest data 41	0	Graphs 6	Dashboards 2	Web
Zabbix server	127.0.0.1:10050	ZBX	class:os class:software target:linux ...	Enabled	Latest data 125	0	Graphs 25	Dashboards 4	Web

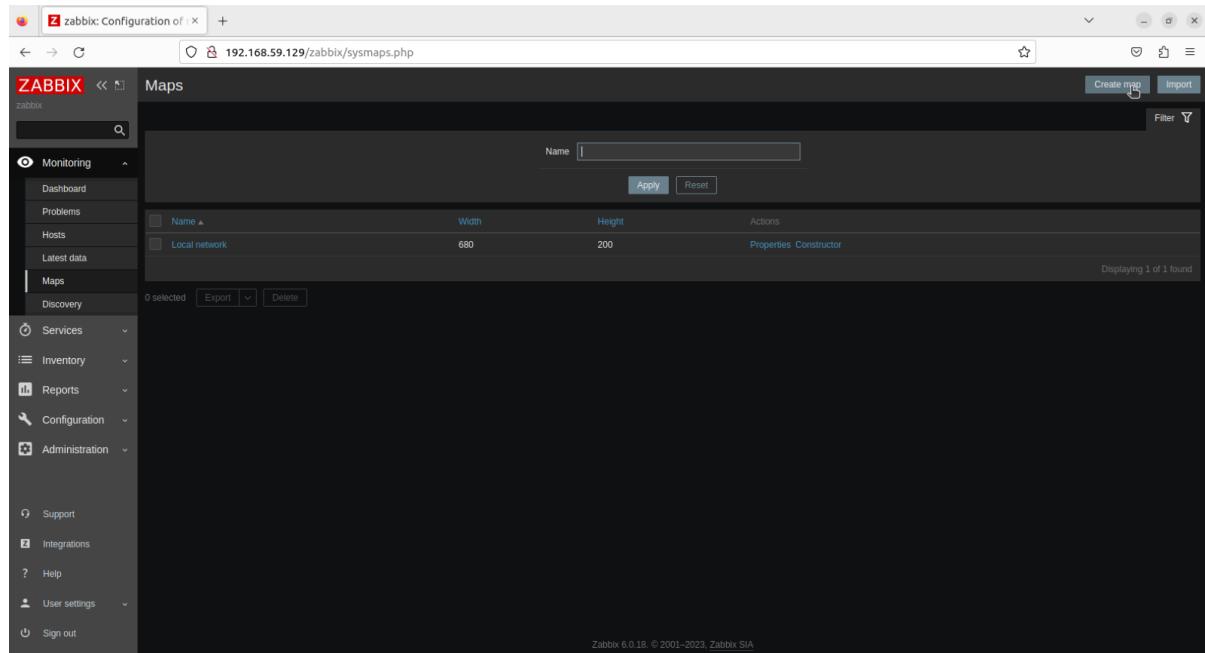
At the bottom of the table, it says 'Displaying 6 of 6 found'. The footer of the page includes the text 'Zabbix 6.0.18 © 2001–2023, Zabbix SIA'.

Maps, one of many visualization options inside the Zabbix, a way to display our collected data, show the problems and create our topology. A map is more than a simple picture. It includes many small but very useful key features.

Maps functionality is not something complicated that we need to do in Configuration, or to collect data from our host, etc. Maps inside Zabbix — one of the visualization options used inside the frontend to visualize what is currently happening in our monitoring environment.

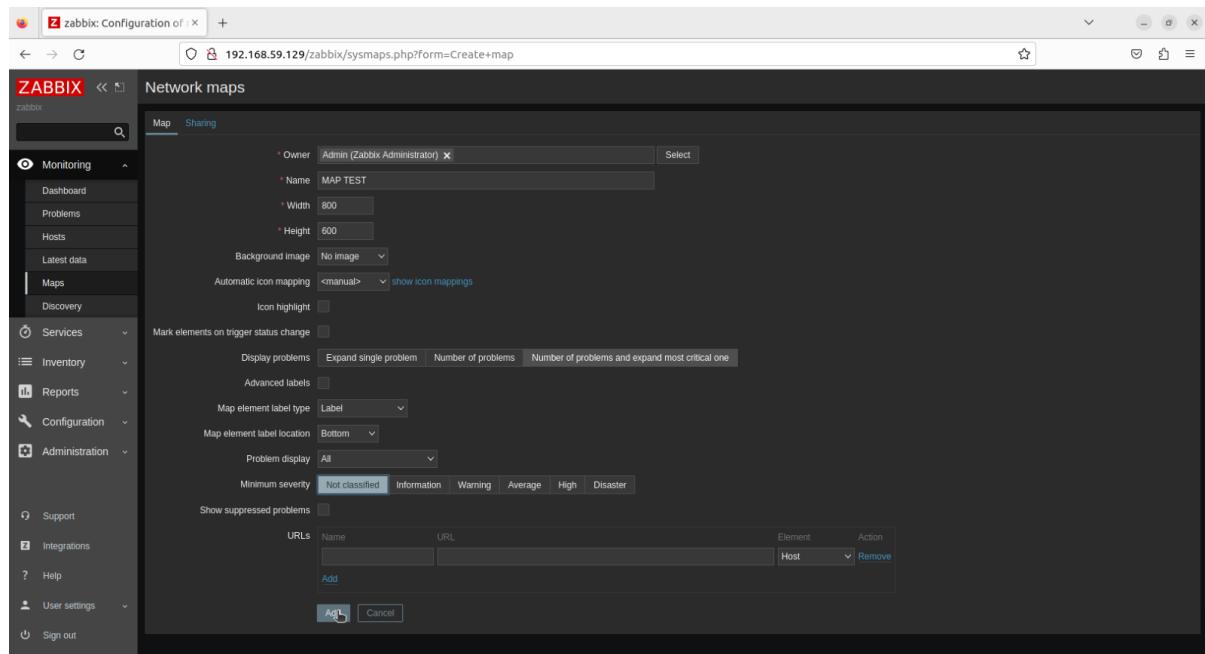
# Creating a new map

To create a map in Zabbix, we go to **Monitoring > Maps** and we click on **Create map**.



The screenshot shows the Zabbix 6.0.18 interface. The left sidebar has 'Monitoring' selected under 'Maps'. The main content area is titled 'Maps' and shows a table with one row: 'Local network' (Width: 680, Height: 200). There are buttons for 'Properties' and 'Constructor' in the Actions column. At the bottom of the table, it says 'Displaying 1 of 1 found'. In the top right, there are 'Create map' and 'Import' buttons, and a 'Filter' dropdown.

We define the needed attributes in the Map tab and Click **Add**.



The screenshot shows the 'Network maps' configuration page with the 'Map' tab selected. The 'Owner' field is set to 'Admin (Zabbix Administrator)'. The 'Name' field contains 'MAP TEST'. The 'Width' is set to 800 and 'Height' to 600. Under 'Background image', 'No image' is selected. The 'Automatic icon mapping' dropdown is set to '<manual>'. The 'Icon highlight' checkbox is unchecked. The 'Display problems' section includes options for 'Expand single problem', 'Number of problems', and 'Number of problems and expand most critical one'. The 'Advanced labels' checkbox is unchecked. The 'Map element label type' is set to 'Label' and 'Map element label location' to 'Bottom'. The 'Problem display' dropdown is set to 'All'. The 'Minimum severity' dropdown includes 'Not classified', 'Information', 'Warning', 'Average', 'High', and 'Disaster'. The 'Show suppressed problems' checkbox is unchecked. At the bottom, there is a table for 'URLs' with columns for 'Name', 'URL', 'Element', and 'Action'. An 'Add' button is available. Below the table are 'AddL' and 'Cancel' buttons.

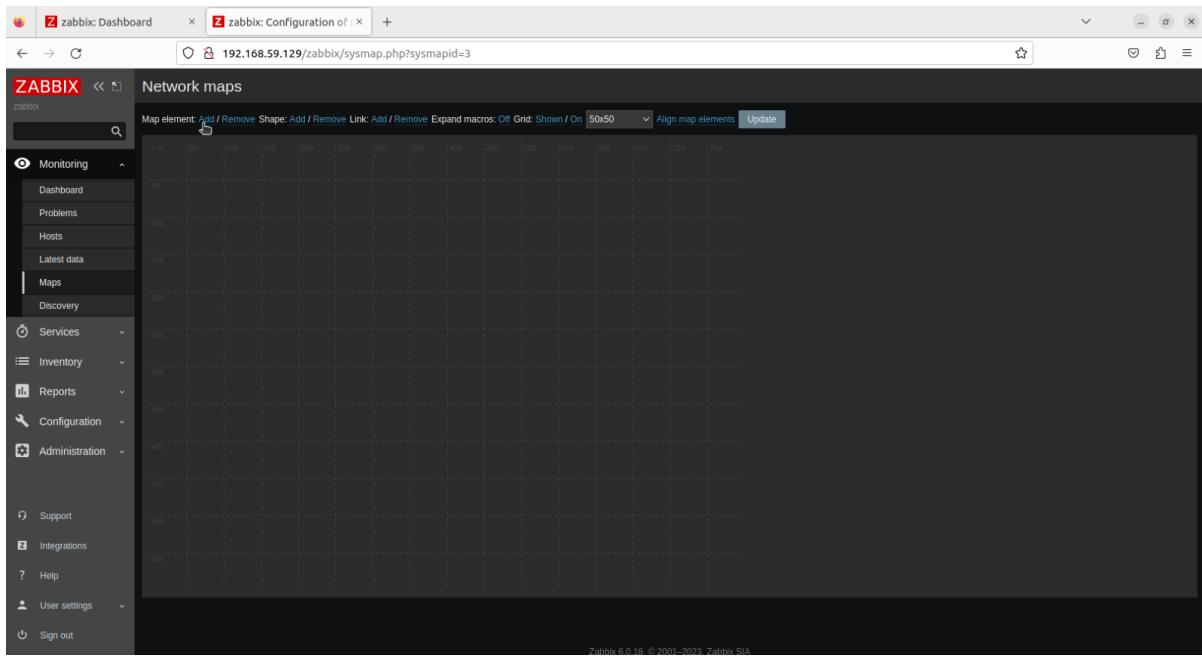
## Configuring new map

We click the new map name to open our new background. Now we can populate the map with elements such as hosts, host groups, triggers, images or other maps.

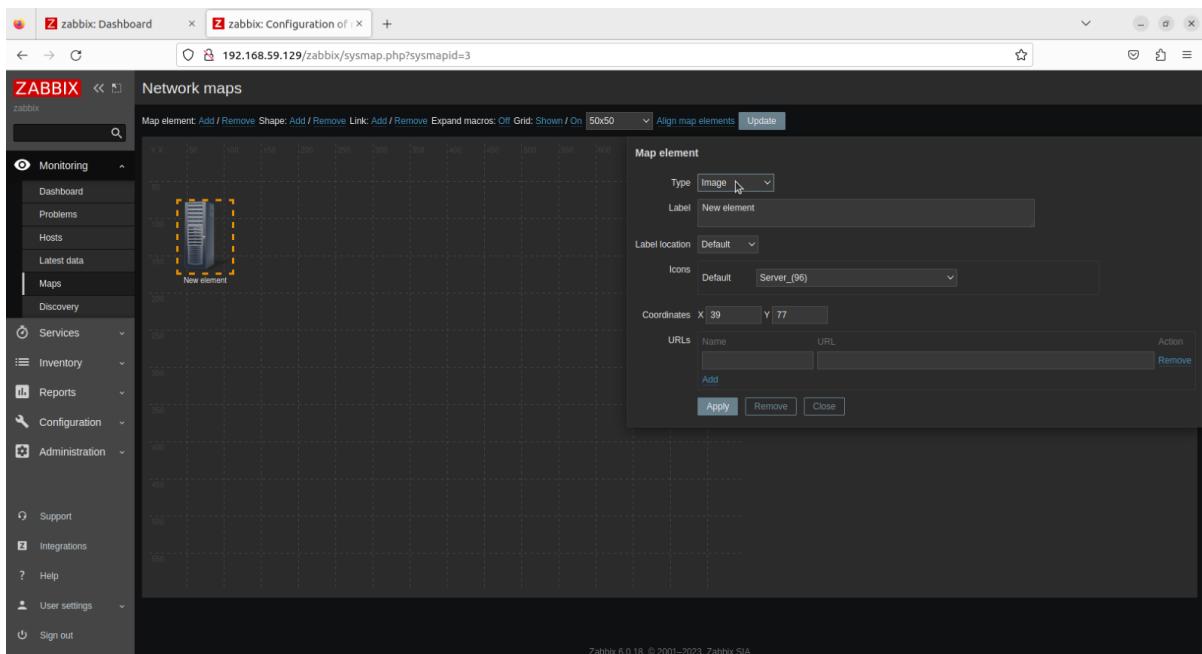
Name	Width	Height	Actions
Local network	680	200	Properties Constructor
MAP TEST	800	600	Properties Constructor

We open the map and we click **Edit map**.

In the settings window, we can start adding elements.

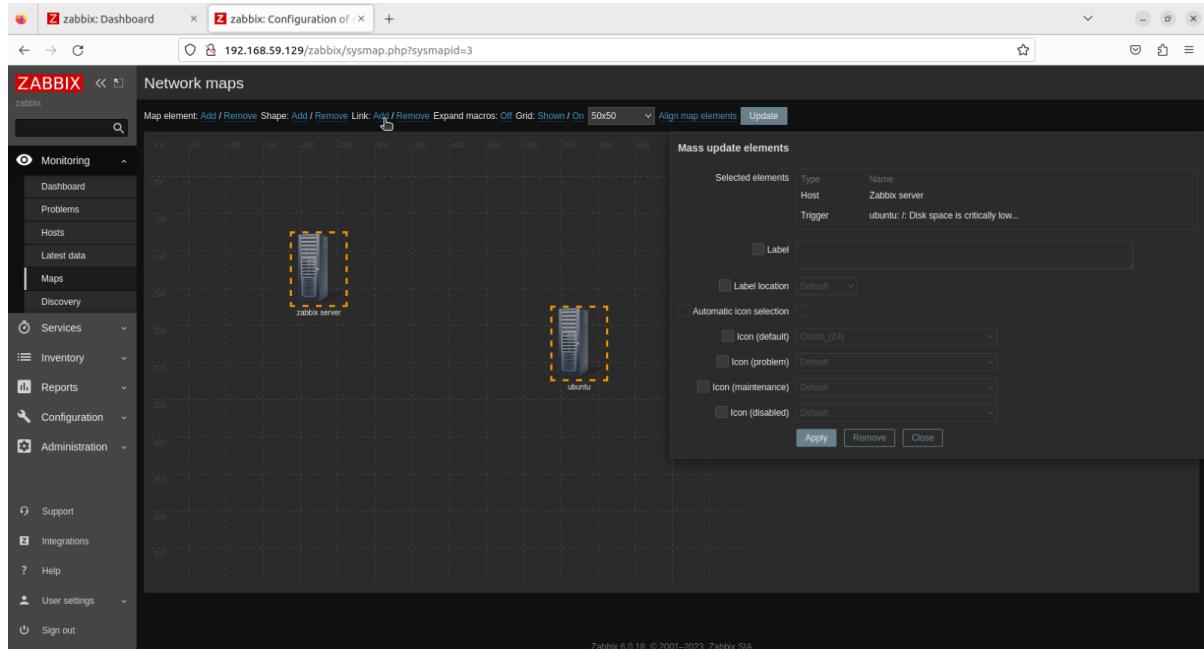


We click **Add** in **Map element** to add a new element. Then double click on it to define the Map element parameters.

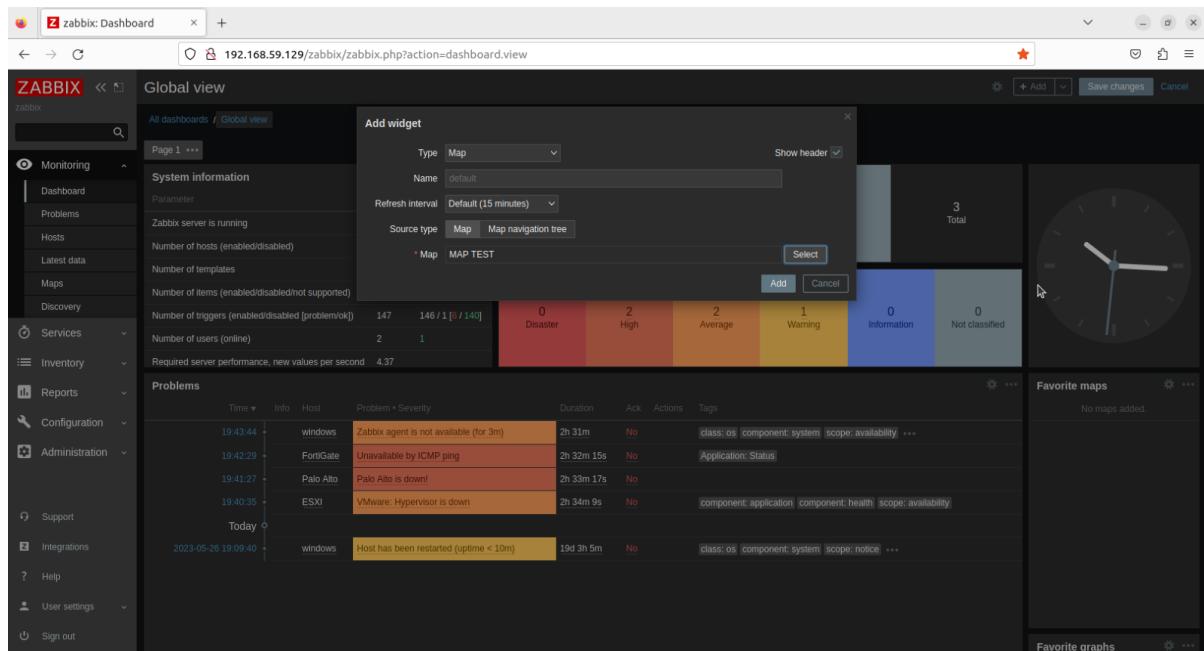


## Linking map elements

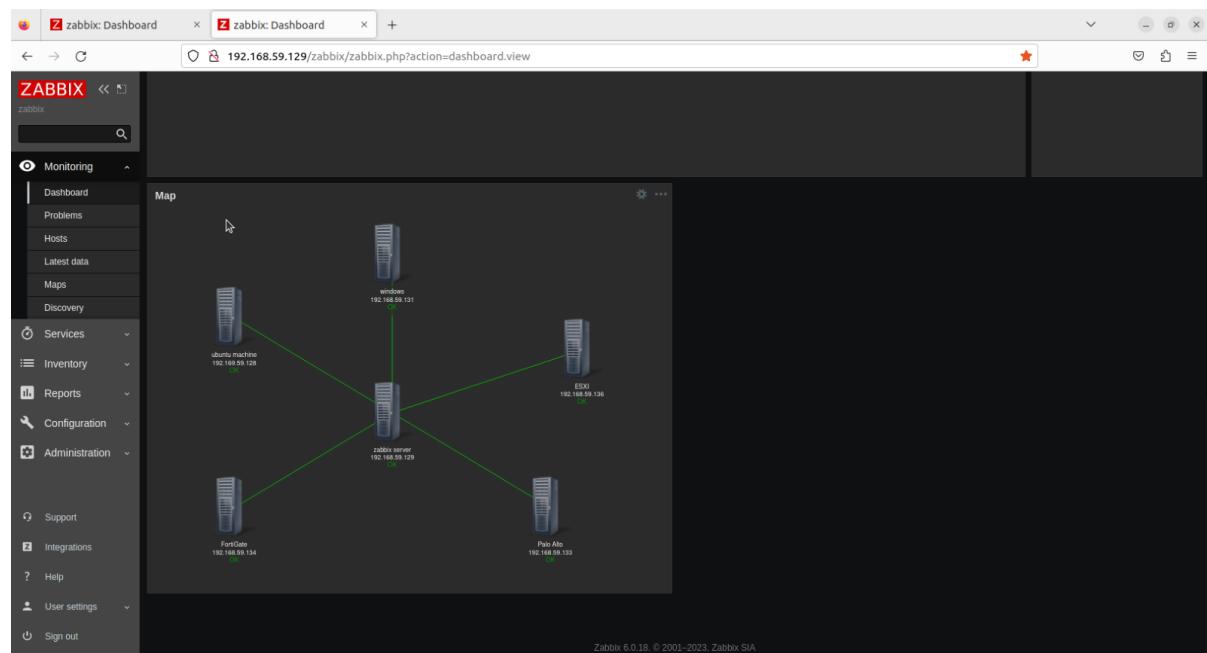
Once we have finished adding the elements, we can start linking them. To link two elements, we need to drag around the two hosts or select them holding a Ctrl key. Then we click Add next to Link.



After adding all hosts and linking them, we go to Dashboard and we click on add widget.



And this is what we got



# Conclusion

The Zabbix project successfully deployed and configured a robust monitoring and performance management platform. The project involved installing and configuring Zabbix on an Ubuntu server, as well as setting up and managing various client machines and servers, including Ubuntu, Windows, PaloAlto, FortiGate, and ESXi.

By leveraging the capabilities of Zabbix, the project achieved comprehensive surveillance and monitoring across the network architecture. The Zabbix server, powered by a relational database, stored monitoring data efficiently, while the web interface provided convenient access to data and system configurations.

Throughout the project, meticulous attention was given to ensuring seamless communication, data collection, and analysis. The implementation of Zabbix agents on client machines and servers allowed for real-time monitoring and performance evaluation.

Overall, this project successfully established a robust monitoring infrastructure that enhances network visibility, facilitates prompt issue detection, and enables effective performance management. The deployment and configuration of Zabbix have laid a solid foundation for continuous monitoring and optimization of the network's performance and reliability.