1. **Install Zabbix Server 5 on VM that includes:**
- **Zabbix Server**
- **Database**
- **Apache**
- **PHP**
- **Zabbix Server-Modules for Apache & Database**
- **Zabbix Frontend**

Installing Database **Mysql**

sudo apt install mysql-server

```
done!
update-alternatives: using /var/lib/mecab/dic/ipadic-utf8 to provide /var/lib/me
cab/dic/debian (mecab-dictionary) in auto mode
Setting up mysql-server-8.0 (8.0.27-0ubuntu0.20.04.1) ...
update-alternatives: using /etc/mysql/mysql.cnf to provide /etc/mysql/my.cnf (my
.cnf) in auto mode
Renaming removed key_buffer and myisam-recover options (if present)
mysqld will log errors to /var/log/mysql/error.log
mysqld is running as pid 2712
Created symlink /etc/systemd/system/multi-user.target.wants/mysql.service → /lib
/systemd/system/mysql.service.
Setting up mysql-server (8.0.27-0ubuntu0.20.04.1) ...
Processing triggers for systemd (245.4-4ubuntu3.13) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for libc-bin (2.31-0ubuntu9.2) ...
bibek@metricbeat:~$
```

Setting mysql server password

sudo mysql_secure_installation

And configured password strength 2

```
Remove test database and access to it? (Press y|Y for Yes, any other key for No)
 : y
 - Dropping test database...
Success.

 - Removing privileges on test database...
Success.

Reloading the privilege tables will ensure that all changes
made so far will take effect immediately.

Reload privilege tables now? (Press y|Y for Yes, any other key for No) : y
Success.

All done!
bibek@metricbeat:~$
```

Creating user and database for Zabbix

sudo mysql -u root -p

```
bibek@metricbeat:~$ sudo mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 10
Server version: 8.0.27-0ubuntu0.20.04.1 (Ubuntu)

Copyright (c) 2000, 2021, Oracle and/or its affiliates.

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

mysql>
```

Creating Database

create database zabbix character set utf8 collate utf8_bin;

```
mysql> create database zabbix character set utf8 collate utf8_bin;
Query OK, 1 row affected, 2 warnings (0.10 sec)
```

Creating user

create user zabbix@localhost identified by 'Zabbix@123';

Granting all privileges

grant all privileges on zabbix.* to zabbix@localhost;

flush privileges;

```
mysql> create user zabbix@localhost identified by 'Zabbix@123';
Query OK, 0 rows affected (0.08 sec)

mysql> grant all privileges on zabbix.* to zabbix@localhost;
Query OK, 0 rows affected (0.14 sec)

mysql> flush privileges;
Query OK, 0 rows affected (0.01 sec)
```

Installing **PHP**

sudo apt install php libapache2-mod-php php-mysql

```
bibek@metricbeat:~$ php -v
PHP 7.4.3 (cli) (built: Oct 25 2021 18:20:54) ( NTS )
Copyright (c) The PHP Group
Zend Engine v3.4.0, Copyright (c) Zend Technologies
    with Zend OPcache v7.4.3, Copyright (c), by Zend Technologies
bibek@metricbeat:~$
```

Installing **Apache**

sudo apt install apache2

```
bibek@metricbeat:~$ sudo apt install apache2
Reading package lists... Done
Building dependency tree
Reading state information... Done
apache2 is already the newest version (2.4.41-4ubuntu3.8).
apache2 set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 13 not upgraded.
bibek@metricbeat:~$
```

Already installed

Installing **Zabbix-5**

wget

https://repo.zabbix.com/zabbix/5.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_5.0

-1+focal_all.deb

sudo dpkg -i zabbix-release_5.0-1+focal_all.deb

```
bibek@metricbeat:~$ ls | grep zabbix
zabbix-release_5.0-1+focal_all.deb
bibek@metricbeat:~$ sudo dpkg -i zabbix-release_5.0-1+focal_all.deb
Selecting previously unselected package zabbix-release.
(Reading database ... 177171 files and directories currently installed.)
Preparing to unpack zabbix-release_5.0-1+focal_all.deb ...
Unpacking zabbix-release (1:5.0-1+focal) ...
Setting up zabbix-release (1:5.0-1+focal) ...
bibek@metricbeat:~$
```

sudo apt update

Installing **Zabbix server modules** for **mysql and apache**

sudo apt install zabbix-server-mysql zabbix-apache-conf

Installing Zabbix frontend

sudo apt install zabbix-frontend-php

```
bibek@metricbeat:~$ sudo apt install zabbix-frontend-php
Reading package lists... Done
Building dependency tree
Reading state information... Done
zabbix-frontend-php is already the newest version (1:5.0.18-1+focal).
zabbix-frontend-php set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 23 not upgraded.
bibek@metricbeat:~$
```

Already installed

Set up the schema and import the data into the zabbix database

zcat /usr/share/doc/zabbix-server-mysql*/create.sql.gz | mysql -u zabbix -p zabbix

And giving the password for zabbix user, it takes some time

For the Zabbix server to use this database, We need to set the database password in the Zabbix server configuration file

sudo vi /etc/zabbix/zabbix_server.conf

Set DBPassword
Set DBHost
Save & exit

Setting time zone

vi /etc/zabbix/apache.conf

php_value date.timezone Asia/Kathmandu

Setting hostname

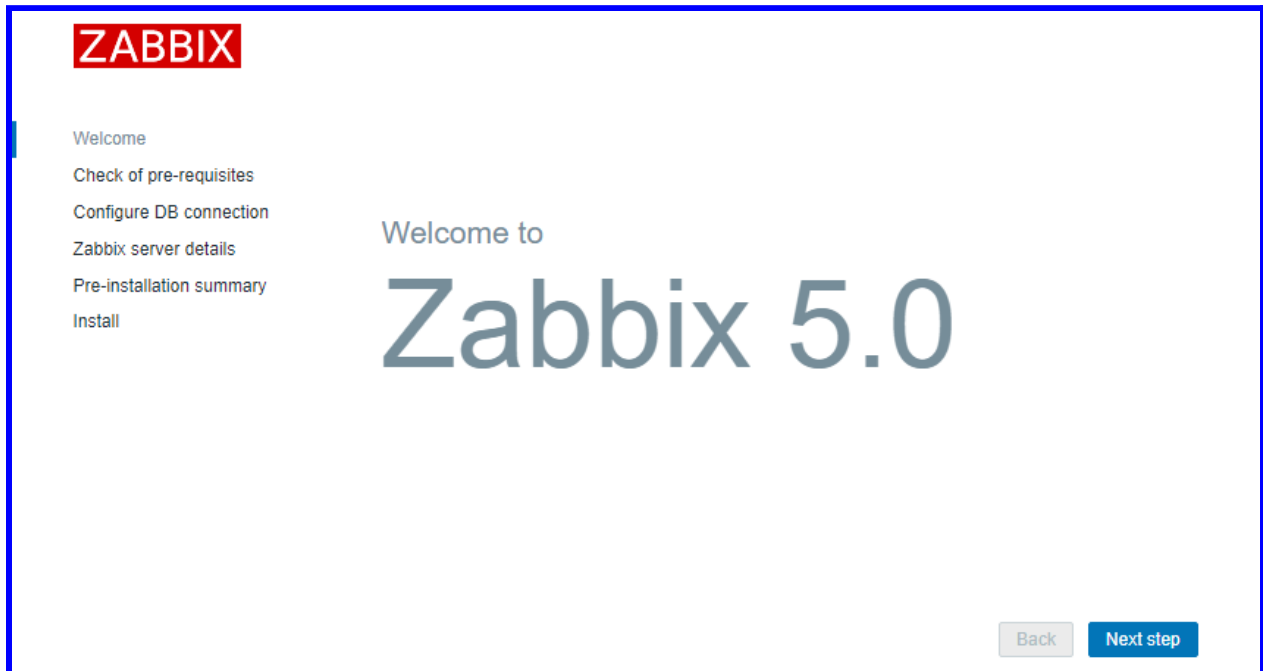**sudo hostnamectl set-hostname ubuntu-zabbix**

Restart the zabbix and apache

systemctl restart zabbix-server.service apache2.service

2. Provide screenshot of
- **Running Zabbix Server service,**
- **Database config parameter in server config file**
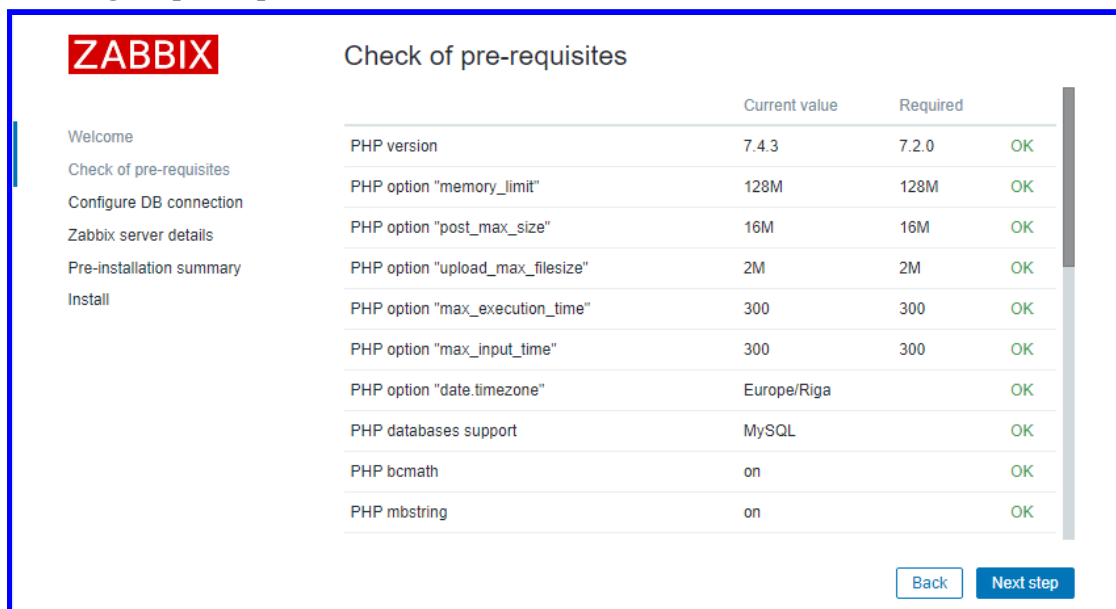- **Server Dashboard**

When we hit the web-page with **http://<serverIP/zabbix>**
We get this page

>> **Next step**
Checking for pre-requisites

>> Configure DB connection

Configure DB connection

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

Database type	MySQL
Database host	localhost
Database port	0 0 - use default port
Database name	zabbix
User	zabbix
Password	••••••••
Database TLS encryption	Connection will not be encrypted because it uses a socket file (on Unix) or shared memory (Windows).

Welcome
Check of pre-requisites
Configure DB connection
Zabbix server details
Pre-installation summary
Install

Back   Next step

>> Zabbix server details

Zabbix server details

Please enter the host name or host IP address and port number of the Zabbix server, as well as the name of the installation (optional).

Host	localhost
Port	10051
Name	Zabbix-LF-Technology

Welcome
Check of pre-requisites
Configure DB connection
Zabbix server details
Pre-installation summary
Install

Back   Next step

>> Pre-installation summary

>> Successful message

>> Zabbix login page
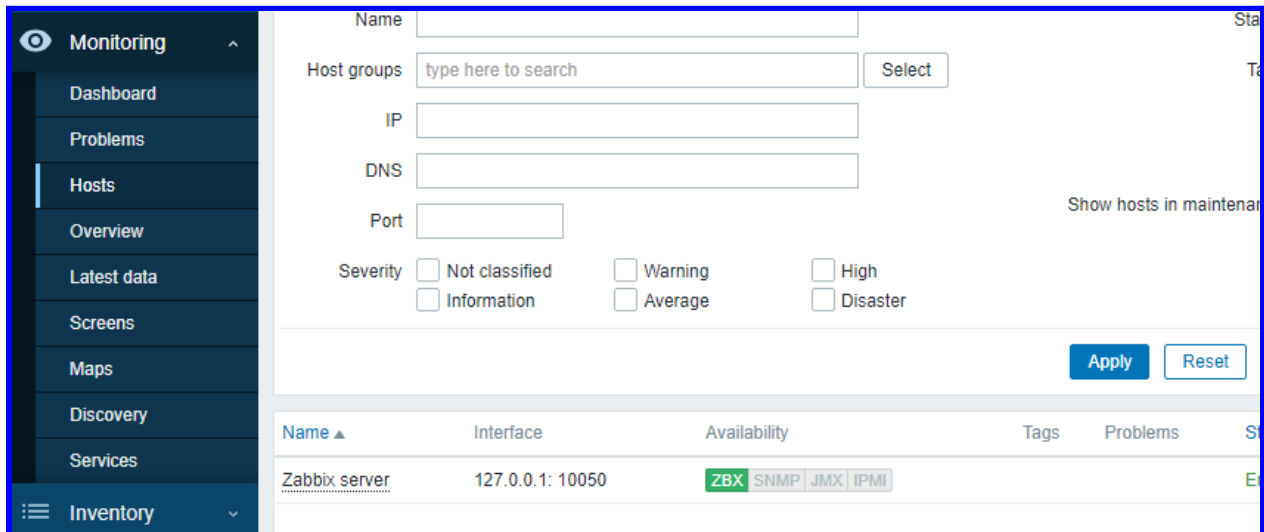

>> Dashboard
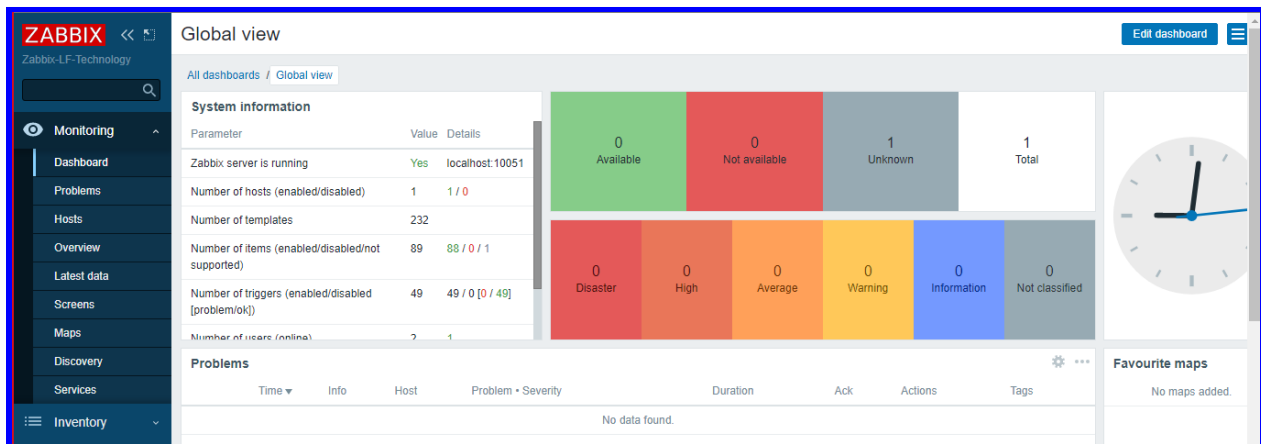
>> Status of running Zabbix-server

```
bibek@ubuntu-zabbix:/var/log/zabbix$ sudo systemctl status zabbix-server.service
● zabbix-server.service - Zabbix Server
     Loaded: loaded (/lib/systemd/system/zabbix-server.service; disabled; vendor preset: enabled)
     Active: active (running) since Thu 2021-12-02 20:59:04 +0545; 5min ago
    Process: 20397 ExecStart=/usr/sbin/zabbix_server -c $CONFFILE (code=exited, status=0/SUCCESS)
   Main PID: 20399 (zabbix_server)
      Tasks: 38 (limit: 1092)
     Memory: 29.9M
     CGroup: /system.slice/zabbix-server.service
             ├─20399 /usr/sbin/zabbix_server -c /etc/zabbix/zabbix_server.conf
             ├─20400 /usr/sbin/zabbix_server: configuration syncer [synced configuration in 0.117432 sec, idle 60 sec]
             ├─20408 /usr/sbin/zabbix_server: alert manager #1 [sent 0, failed 0 alerts, idle 5.007051 sec during 5.007217 sec]
             ├─20409 /usr/sbin/zabbix_server: alerter #1 started
             ├─20410 /usr/sbin/zabbix_server: alerter #2 started
             ├─20411 /usr/sbin/zabbix_server: alerter #3 started
             ├─20412 /usr/sbin/zabbix_server: preprocessing manager #1 [queued 1, processed 11 values, idle 5.001991 sec during 5.002394 sec]
             ├─20413 /usr/sbin/zabbix_server: preprocessing worker #1 started
             ├─20414 /usr/sbin/zabbix_server: preprocessing worker #2 started
             └─20415 /usr/sbin/zabbix_server: preprocessing worker #3 started
```

>> When this green sign comes in Hosts, the Zabbix-Server is running

3. **Install Latest Zabbix Agent on VM or host machine or server itself to fetch logs, steps include:**
- **Run as active check agent**
- **Add a logging item to the same template for fetching /var/log/syslog(Ubuntu) or /var/log/messages (CentOS)**
- **Fetch those logs from the host (Make sure required permissions are set for zabbix-agent to pull logs)**
- **Provide agent configuration file & screenshots for target machine graph & logs**

Installing zabbix agent in the same host(Zabbix-server)

sudo apt install zabbix-agent

Configuring Zabbix agent configuration

sudo vi /etc/zabbix/zabbix_agentd.conf

ServerActive=192.168.1.147
Hostname=ubuntu-zabbix

Restarting zabbix-agent service

sudo systemctl restart zabbix-agent.service

Configuration >> Host >> Create Host

*Give the **host-name** same as we have given in the configuration file*

*Select Groups - **Linux Servers***

Interfaces - Agent <IP> -** for Active Check **Port - 10051

Selecting Template **- Template OS Linux by Zabbix agent active**

After creating host

Name ▲	Applications	Items	Triggers	Graphs	Discovery	Web	Interface	Proxy	Templates	Status	Availability	Agent encryption
ubuntu-zabbix	Applications 15	Items 63	Triggers 22	Graphs 13	Discovery 3	Web	192.168.1.147: 10051		Template OS Linux by Zabbix agent active (Template Module Linux block devices by Zabbix agent active, Template Module Linux CPU by Zabbix agent active, Template Module Linux filesystems by Zabbix	Enabled	ZBX SNMP JMX IPMI	NONE

Giving access to Zabbix user to read **log of syslog**

*Syslog is accessed (read) by **adm** group*

*Adding **Zabbix user** to **adm group***

sudo usermod -aG adm zabbix

```
bibek@ubuntu-zabbix:/var/log$ cat /etc/passwd | grep zabbix
zabbix:x:132:140::/var/lib/zabbix/:/usr/sbin/nologin
bibek@ubuntu-zabbix:/var/log$ sudo usermod -aG adm zabbix
[sudo] password for bibek:
bibek@ubuntu-zabbix:/var/log$ |||
```

Restarting the zabbix-agent service

sudo systemctl restart zabbix-agent.service

Checking whether zabbix can access syslog or not

sudo -H -u zabbix bash -c 'tail -f /var/log/syslog'

```
bibek@ubuntu-zabbix:/var/log$ sudo systemctl restart zabbix-agent.service
bibek@ubuntu-zabbix:/var/log$ sudo -H -u zabbix bash -c 'tail -f /var/log/syslog'
Dec  2 22:13:38 ubuntu-zabbix whoopsie[766]: [22:13:38] online
Dec  2 22:13:47 ubuntu-zabbix systemd[1]: NetworkManager-dispatcher.service: Succeeded.
Dec  2 22:17:01 ubuntu-zabbix CRON[4190]: (root) CMD (   cd / && run-parts --report /etc/cron.hourly)
Dec  2 22:27:07 ubuntu-zabbix systemd[1]: Stopping Zabbix Agent...
Dec  2 22:27:07 ubuntu-zabbix systemd[1]: zabbix-agent.service: Succeeded.
Dec  2 22:27:07 ubuntu-zabbix systemd[1]: Stopped Zabbix Agent.
Dec  2 22:27:07 ubuntu-zabbix systemd[1]: Starting Zabbix Agent...
```

Here we can see it can fetch syslog through zabbix user

Creating **Item** to get **syslog** from ubuntu-host

Configuration >> Hosts >> Items >> **Create Item**

Name - *ubuntu-sys-log,* **Type** - *Zabbix agent (**active**),* **Key** - *log[/var/log/syslog,,,,,,,,],* **New Application** - *Name*

Monitoring >> Latest Data >> syslogs (ubuntu sys logs) >> History

*We can see the **logs** coming from the **ubuntu-zabbix** server through **zabbix-agent.***

ubuntu-zabbix: ubuntu-sys-logs

View as | Values | As plain text

‹ Zoom out › Last 1 hour 🕐 Filter

From | now-1h | 📅
To | now | 📅

Apply

Last 2 days	Yesterday	Today	Last 5 minute
Last 7 days	Day before yesterday	Today so far	Last 15 minu
Last 30 days	This day last week	This week	Last 30 minu
Last 3 months	Previous week	This week so far	Last 1 hour
Last 6 months	Previous month	This month	Last 3 hours
Last 1 year	Previous year	This month so far	Last 6 hours
Last 2 years		This year	Last 12 hours
		This year so far	Last 1 day

Timestamp	Local time	Value
2021-12-02 22:34:09		Dec 1 01:49:28 metricbeat tracker-miner-f[851]: Unable to get XDG user directory path for special directory &PICTURES. Ignoring this location.
2021-12-02 22:34:09		Dec 1 01:49:28 metricbeat dbus-daemon[1461]: [session uid=1000 pid=1461] Activating via systemd: service name='org.gtk.vfs.GoaVolumeMonitor' unit='gvfs-goa-volume-monitor.service' requested by ':1.1' (uid=1000 pid=1060 comm="/usr/libexec/tracker-miner-fs " label="unconfined")
2021-12-02 22:34:09		Dec 1 01:49:28 metricbeat tracker-miner-f[851]: Unable to get XDG user directory path for special directory &MUSIC. Ignoring this location.
2021-12-02 22:34:09		Dec 1 01:49:28 metricbeat dbus-daemon[1461]: [session uid=1000 pid=1461] Successfully activated service 'org.gtk.vfs.MTPVolumeMonitor'
2021-12-02 22:34:09		Dec 1 01:49:28 metricbeat tracker-miner-f[851]: Unable to get XDG user directory path for special directory &DOCUMENTS. Ignoring this

Timestamp	Local time	Value
2021-12-03 00:19:14		Dec 3 00:18:46 ubuntu-zabbix systemd[1]: NetworkManager-dispatcher.service: Succeeded.
2021-12-03 00:19:14		Dec 3 00:18:37 ubuntu-zabbix whoopsie[766]: [00:18:37] online
2021-12-03 00:19:14		Dec 3 00:18:35 ubuntu-zabbix whoopsie[766]: [00:18:35] Found usable connection: /org/freedesktop/N
2021-12-03 00:19:14		Dec 3 00:18:35 ubuntu-zabbix whoopsie[766]: [00:18:35] Not a paid data plan: /org/freedesktop/Netw
2021-12-03 00:19:14		Dec 3 00:18:35 ubuntu-zabbix whoopsie[766]: [00:18:35] The default IPv4 route is: /org/freedesktop
2021-12-03 00:19:14		Dec 3 00:18:35 ubuntu-zabbix NetworkManager[569]: <info> [1638470015.7229] manager: NetworkManage
2021-12-03 00:19:14		Dec 3 00:18:35 ubuntu-zabbix systemd[1]: Started Network Manager Script Dispatcher Service.
2021-12-03 00:19:14		Dec 3 00:18:35 ubuntu-zabbix dbus-daemon[568]: [system] Successfully activated service 'org.freede
2021-12-03 00:19:14		Dec 3 00:18:35 ubuntu-zabbix systemd[1]: Starting Network Manager Script Dispatcher Service...