# Zabbix with Apache2 Ubuntu 20.04

sudo apt update

sudo apt install apache2 libapache2-mod-php

sudo apt install mysql-server

sudo apt install php php-mbstring php-gd php-xml php-bcmath php-ldap php-mysql

sudo nano /etc/php/7.4/apache2/php.ini

memory\_limit 256M

upload\_max\_filesize 16M

post\_max\_size 16M

max\_execution\_time 300

max\_input\_time 300

max\_input\_vars 10000

date.timezone = 'Asia/Kolkata'

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

sudo apt update

sudo apt install zabbix-server-mysql zabbix-frontend-php zabbix-agent zabbix-apache-conf

## Create Zabbix Database and User

mysql -u root -p

CREATE DATABASE zabbix character set utf8 collate utf8\_bin;

CREATE USER 'zabbix'@'localhost' IDENTIFIED BY 'password';

GRANT ALL PRIVILEGES ON zabbix.\* TO 'zabbix'@'localhost' WITH GRANT OPTION;

FLUSH PRIVILEGES;

cd /usr/share/doc/zabbix-server-mysql

zcat create.sql.gz | mysql -u zabbix -p zabbix

If above command not works :- sudo apt reinstall zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-agent

## Update Zabbix Configuration

sudo nano /etc/zabbix/zabbix\_server.conf

DBHost=localhost

DBName=zabbixdb

DBUser=zabbix

DBPassword=password

sudo nano /etc/zabbix/apache.conf

...

<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 always\_populate\_raw\_post\_data -1

php\_value date.timezone Europe/Riga

</IfModule>

sudo systemctl restart zabbix-server zabbix-agent apache2

sudo systemctl enable zabbix-server zabbix-agent apache2

## Tweaking the Firewall With UFW

sudo ufw allow 80/tcp

sudo ufw allow 443/tcp

sudo ufw reload

## Installing and Configuring the Zabbix Agent

wget https://repo.zabbix.com/zabbix/5.0/ubuntu/pool/main/z/zabbix-release/zabbix-release\_5.0-1+bionic\_all.deb

sudo dpkg -i zabbix-release\_5.0-1+bionic\_all.deb

sudo apt update

sudo apt install zabbix-agent

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

cat /etc/zabbix/zabbix\_agentd.psk

sudo nano /etc/zabbix/zabbix\_agentd.conf

...

Server=zabbix\_server\_ip\_address

ServerActive=zabbix\_server\_ip\_address

…

sudo systemctl restart zabbix-agent

sudo systemctl enable zabbix-agent

sudo systemctl status zabbix-agent

sudo ufw allow 10050/tcp

## Adding the New Host to the Zabbix Server

<http://zabbix_server_name/zabbix>

When you have logged in, click on Configuration, and then Hosts in the top navigation bar. Then click the Create host button in the top right corner of the screen. This will open the host configuration page.

Adjust the Host name and IP address to reflect the host name and IP address of your second Ubuntu server, then add the host to a group. You can select an existing group, for example Linux servers, or create your own group. The host can be in multiple groups. To do this, enter the name of an existing or new group in the Groups field and select the desired value from the proposed list.

Once you’ve added the group, click the Templates tab.

Type Template OS Linux in the Search field and then click Add to add this template to the host.

Next, navigate to the Encryption tab. Select PSK for both Connections to host and Connections from host. Then set PSK identity to PSK 001, which is the value of the TLSPSKIdentity setting of the Zabbix agent you configured previously. Then set PSK value to the key you generated for the Zabbix agent. It’s the one stored in the file /etc/zabbix/zabbix\_agentd.psk on the agent machine.

Finally, click the Add button at the bottom of the form to create the host.

You will see your new host in the list. Wait for a minute and reload the page to see green labels indicating that everything is working fine and the connection is encrypted.

If you have additional servers you need to monitor, log in to each host, install the Zabbix agent, generate a PSK, configure the agent, and add the host to the web interface following the same steps you followed to add your first host.

The Zabbix server is now monitoring your second Ubuntu server. Now, set up email notifications to be notified about problems.

## Configuring Email Notifications

Zabbix automatically supports several types of notifications: email, [Jabber](https://www.jabber.org/), SMS, etc. You can also use alternative notification methods, such as Telegram or Slack. You can see the full list of integrations [here](https://www.zabbix.com/ru/integrations/?cat=notifications_alerting).

The simplest communication method is email, and this tutorial will configure notifications for this media type.

Click on Administration, and then Media types in the top navigation bar. You will see the list of all media types. Click on Email.

Adjust the SMTP options according to the settings provided by your email service. This tutorial uses Gmail’s SMTP capabilities to set up email notifications; if you would like more information about setting this up, see [How To Use Google’s SMTP Server](https://www.digitalocean.com/community/tutorials/how-to-use-google-s-smtp-server).

Note: If you use 2-Step Verification with Gmail, you need to generate an App Password for Zabbix. You don’t need to remember it, you’ll only have to enter an App password once during setup. You will find instructions on how to generate this password in the [Google Help Center](https://support.google.com/accounts/answer/185833?hl=en).

You can also choose the message format—html or plain text. Finally, click the Update button at the bottom of the form to update the email parameters.

Now, create a new user. Click on Administration, and then Users in the top navigation bar. You will see the list of users. Then click the Create user button in the top right corner of the screen. This will open the user configuration page.

Enter the new username in the Alias field and set up a new password. Next, add the user to the administrator’s group. Type Zabbix administrators in the Groups field and select it from the proposed list.

Once you’ve added the group, click the Media tab and click on the Add underlined link. You will see a pop-up window.

Enter your email address in the Send to field. You can leave the rest of the options at the default values. Click the Add button at the bottom to submit.

Now navigate to the Permissions tab. Select Zabbix Super Admin from the User type drop-down menu.

Finally, click the Add button at the bottom of the form to create the user.

Now you need to enable notifications. Click on the Configuration tab, and then Actions in the top navigation bar. You will see a pre-configured action, which is responsible for sending notifications to all Zabbix administrators. You can review and change the settings by clicking on its name. For the purposes of this tutorial, use the default parameters. To enable the action, click on the red Disabled link in the Status column.

Now you are ready to receive alerts. In the next step, you will generate one to test your notification setup.

## Step 8 — Generating a Test Alert

In this step, you will generate a test alert to ensure everything is connected. By default, Zabbix keeps track of the amount of free disk space on your server. It automatically detects all disk mounts and adds the corresponding checks. This discovery is executed every hour, so you need to wait a while for the notification to be triggered.

Create a temporary file that’s large enough to trigger Zabbix’s file system usage alert. To do this, log in to your second Ubuntu server if you’re not already connected.

ssh sammy@second\_ubuntu\_server\_ip\_address

Next, determine how much free space you have on the server. You can use the df command to find out:

1. df -h

n this case, the free space is 23GB. Your free space may differ.

Use the fallocate command, which allows you to pre-allocate or de-allocate space to a file, to create a file that takes up more than 80% of the available disk space. This will be enough to trigger the alert:

fallocate -l 20G /tmp/temp.img

Copy

After around an hour, Zabbix will trigger an alert about the amount of free disk space and will run the action you configured, sending the notification message. You can check your inbox for the message from the Zabbix server. You will see a message like:

You can also navigate to the Monitoring tab, and then Dashboard to see the notification and its details.

Now that you know the alerts are working, delete the temporary file you created so you can reclaim your disk space:

rm -f /tmp/temp.img

Copy

After a minute Zabbix will send the recovery message and the alert will disappear from main dashboard.