WWW.BESTMONITORINGTOOLS.COM
How to Install
Zabbix Agent
on Linux
The Definitive Step-by-Step
Linux Server Monitoring Guide
ZABBIX
CentOS
Best Monitoring tools

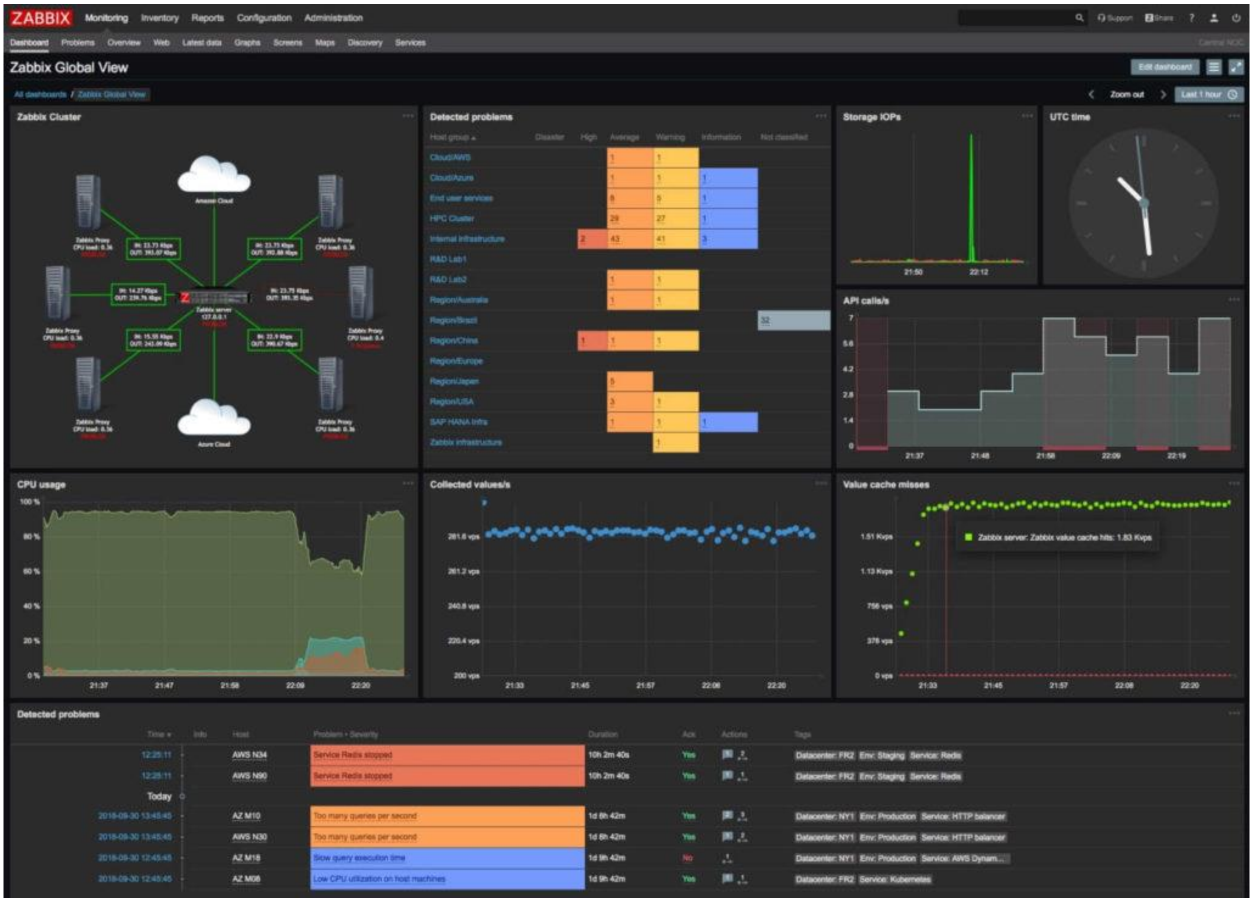
Zabbix Agent (Linux): Install on Ubuntu, CentOS, RHEL, Debian, etc.

In this tutorial, I will show you how to install Zabbix agent (Linux) on Ubuntu, CentOS, RHEL, Debian, Rasbian (Raspberry Pi) and how to monitor Linux server with Zabbix monitoring system.

You can use this guide to install Zabbix Agent 4.0 or 5.0 LTS version on almost any popular Linux distributions:

- Ubuntu 20.04 LTS (Focal), Ubuntu 18.04 LTS (Bionic), Ubuntu 16.04 LTS, and Ubuntu 14.04 LTS
- RHEL / CentOS 8, RHEL / CentOS 7, and RHEL / CentOS 6
- Debian 10 (Buster), Debian 9 (Stretch), and Debian 8 (Jessie)
- Rasbian 10 (Rasberry Pi) and Rasbian 9 (Rasberry Pi)

Installing and configuring Zabbix Agent on Linux is a fairly straightforward task and only takes a few minutes, but if you want to know more then read the full article.



Detected problems

Host group ▲	Disaster	High	Average	Warning	Information	Not classified
Cloud/AWS			1	1		
Cloud/Azure			1	1	1	
End user services			8	5	1	
HPC Cluster			29	27	1	
Internal infrastructure		2	43	41	3	
R&D Lab1						
R&D Lab2			1	1		
Region/Australia			1	1		
Region/Brazil						32
Region/China		1	1	1		
Region/Europe						
Region/Japan			5			
Region/USA			3	1		
SAP HANA Infra			1	1	1	
Zabbix infrastructure				1		

Detected problems

Time ▾	Info	Host	Problem • Severity	Duration	Ack	Actions	Tags
12:25:11		AWS N34	Service Redis stopped	10h 2m 40s	Yes		Datacenter: FR2 Env: Staging Service: Redis
12:25:11		AWS N90	Service Redis stopped	10h 2m 40s	Yes		Datacenter: FR2 Env: Staging Service: Redis
Today							
2018-09-30 13:45:45		AZ M10	Too many queries per second	1d 8h 42m	Yes		Datacenter: NY1 Env: Production Service: HTTP balancer
2018-09-30 13:45:45		AWS N30	Too many queries per second	1d 8h 42m	Yes		Datacenter: NY1 Env: Production Service: HTTP balancer
2018-09-30 12:45:45		AZ M18	Slow query execution time	1d 9h 42m	No		Datacenter: NY1 Env: Production Service: AWS Dynam...
2018-09-30 12:45:45		AZ M08	Low CPU utilization on host machines	1d 9h 42m	Yes		Datacenter: FR2 Service: Kubernetes

Example of the Zabbix dashboard that is customized for server monitoring

In short, Zabbix agent is a lightweight application that can collect various performance data from the operating system – such as CPU, memory, disk, and network interface utilization – and forward it to a central point (server) for storage and visualization. It runs on any modern operating system and is very flexible because its functionality can be extended with scripts and modules.

You can read more about the Zabbix agent on the Zabbix official site and if you stumbled on this tutorial by accident and you never heard of the Zabbix monitoring system, then stop whatever you doing and install it on your favorite Linux distribution in less than 10 minutes: CentOS/RHEL, Ubuntu, Debian, Raspberry (Rasbian).

Step 1: Configure repository and install Zabbix agent

In this tutorial, I will use the latest Zabbix agent 5.0 LTS version, that version is compatible with Zabbix server 5.x or newer. However, if you are still on Zabbix server 4.x then use agent 4.0 LTS version.

Select the appropriate OS repository and install the Zabbix agent using the provided instructions.

a. Ubuntu 20.04 / 18.04 / 16.04 / 14.04

```
Zabbix 5.0 LTS version (supported until May 31, 2025)
sudo wget https://repo.zabbix.com/zabbix/5.0/ubuntu/pool/main/z/zabbix-
release/zabbix-release_5.0-1+$(lsb_release -sc)_all.deb
sudo dpkg -i zabbix-release_5.0-1+$(lsb_release -sc)_all.deb

                              OR

Zabbix 4.0 LTS version (supported until October 31, 2023)
sudo wget https://repo.zabbix.com/zabbix/4.0/ubuntu/pool/main/z/zabbix-
release/zabbix-release_4.0-3+$(lsb_release -sc)_all.deb
sudo dpkg -i zabbix-release_4.0-3+$(lsb_release -sc)_all.deb
sudo apt update
sudo apt -y install zabbix-agent
```

b. RHEL & Centos 8 / 7 / 6

```
Zabbix 5.0 LTS version (supported until May 31, 2025)
rpm -Uvh https://repo.zabbix.com/zabbix/5.0/rhel/$(rpm -E
%{rhel})/x86_64/zabbix-release-5.0-1.el$(rpm -E %{rhel}).noarch.rpm

                             OR

Zabbix 4.0 LTS version (supported until October 31, 2023)
rpm -Uvh https://repo.zabbix.com/zabbix/4.0/rhel/$(rpm -E
%{rhel})/x86_64/zabbix-release-4.0-2.el$(rpm -E %{rhel}).noarch.rpm
yum clean all
yum -y install zabbix-agent
```

c. Debian 10 / 9 / 8

```
Zabbix 5.0 LTS version (supported until May 31, 2025)
sudo wget https://repo.zabbix.com/zabbix/5.0/debian/pool/main/z/zabbix-
release/zabbix-release_5.0-1+$(lsb_release -sc)_all.deb
sudo dpkg -i zabbix-release_5.0-1+$(lsb_release -sc)_all.deb

                              OR

Zabbix 4.0 LTS version (supported until October 31, 2023)
sudo wget https://repo.zabbix.com/zabbix/4.0/debian/pool/main/z/zabbix-
release/zabbix-release_4.0-3+$(lsb_release -sc)_all.deb
sudo dpkg -i zabbix-release_4.0-3+$(lsb_release -sc)_all.deb
sudo apt update
sudo apt -y install zabbix-agent
```

d. Raspberry Pi OS (Rasbian) 10 / 9

```
Zabbix 5.0 LTS version (supported until May 31, 2025)
sudo wget https://repo.zabbix.com/zabbix/5.0/raspbian/pool/main/z/zabbix-
release/zabbix-release_5.0-1+$(lsb_release -sc)_all.deb
sudo dpkg -i zabbix-release_5.0-1+$(lsb_release -sc)_all.deb

                             OR

Zabbix 4.0 LTS version (supported until October 31, 2023)
sudo wget https://repo.zabbix.com/zabbix/4.0/raspbian/pool/main/z/zabbix-
release/zabbix-release_4.0-3+$(lsb_release -sc)_all.deb
sudo dpkg -i zabbix-release_4.0-3+$(lsb_release -sc)_all.deb
sudo apt update
sudo apt -y install zabbix-agent
```

Step 2: Configure Zabbix agent on Linux OS

Keep in mind that in this tutorial I will use a Zabbix server with IP address **192.168.5.43** to monitor a Linux server called **l01mylab** that has IP address **192.168.5.114** – don't forget to change those settings to match your environment. Feel free to check the official Zabbix documentation if you need more information about Zabbix agent configuration parameters.

Let's update some Zabbix agent configuration parameters, open Zabbix agent configuration file with with your favorite text editor:

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

And update these parameters:

```
Server=192.168.5.43
ServerActive=192.168.5.43
HostMetadata=Linux
HostnameItem=system.hostname
```

In the “`Server`” and “`ServerActive`” parameters put the IP address of your Zabbix server or proxy!

“`HostMetadata`” can be anything, any description of the system or a word that can help you later on in auto-registration process on the Zabbix frontend.

“`HostnameItem`” parameter will automatically generate a hostname that is defined on the Linux server, however by default that parameter is ignored if the “`Hostname`” parameter is defined. You can either enter a hostname manually in the “`Hostname`” parameter or you can you let Zabbix agent do that automatically by commenting the “`Hostname=`” line:

```
#Hostname=Zabbix Server
```

Finally, you must restart the Zabbix agent for the configuration to apply, so go to the next step.

Step 3: Start Zabbix agent and set it to boot on startup

Don’t forget to restart Zabbix agent service and set it to always start on boot with the “`enable`” command.

```
sudo systemctl restart zabbix-agent
sudo systemctl enable zabbix-agent
```

Sometimes you will need to check / start / stop Zabbix agent service, so use “`systemctl`” tool to do so:

```
sudo systemctl <status/restart/start/stop> zabbix-agent
```

Step 4: Configure firewall for the Zabbix agent

Zabbix agent, that is running in passive mode, must be able to respond to the Zabbix server inquiries over TCP port 10050.

Use these commands to open TCP port 10050 on CentOS / RHEL server where Zabbix agent is installed:

```
firewall-cmd --permanent --zone=public --add-port=10050/tcp
firewall-cmd –reload
```

And if you have an UFW firewall installed on Ubuntu / Debian / Rasbian, you can use this command to permit Zabbix agent TCP port 10050:

```
sudo ufw allow 10050/tcp
```

WELL DONE!

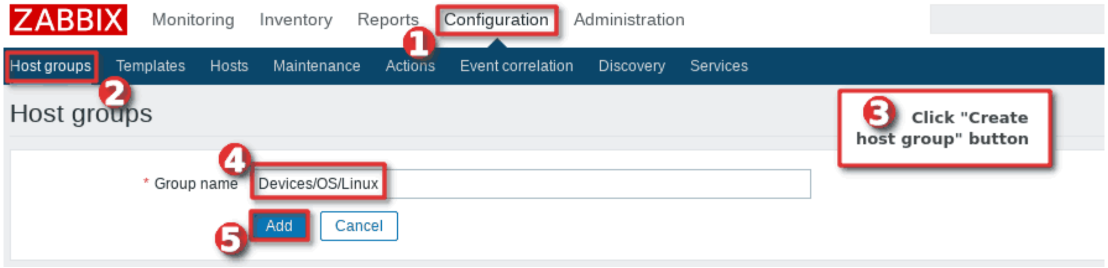
You have successfully installed and configured Zabbix agent on your Linux OS!

Now it’s time to add that Linux host to Zabbix monitoring system.

Step 5: Add Linux host to Zabbix monitoring system

I hope you already have the Zabbix monitoring system installed, and if not then install it on your favorite Linux distribution in less than 10 minutes: [CentOS/RHEL](), [Ubuntu](), [Debian](), [Rasbian]().

You can add a host to existing host group or you can create a new host group for your Linux servers. I will create host group "`Devices/OS/Linux`" using "*Host groups*" option under "*Configuration*" section on the Zabbix frontend. Click "*Create host group*" button, define "*Group name*" and click "*Add*" (**you only need to create host group once**):

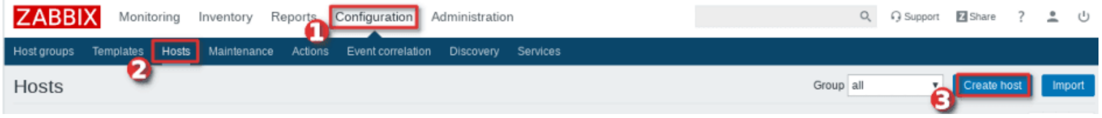


3 Click "Create host group" button

* Group name: Devices/OS/Linux

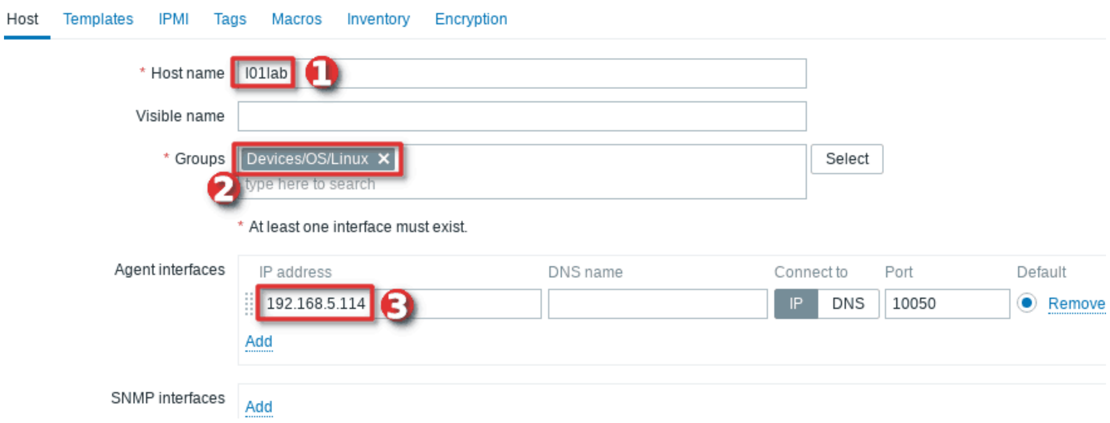
Create Zabbix host group for Linux servers

Navigate to "*Host*" menu under "*Configuration*" tab and then click "*Create host*" option to create a host in Zabbix:



Add Linux host to Zabbix – Step 1

Define "*Hostname*" and set "*Groups*" using your newly created host group. Then set the IP address of the Linux server under "*Agent interfaces*" section



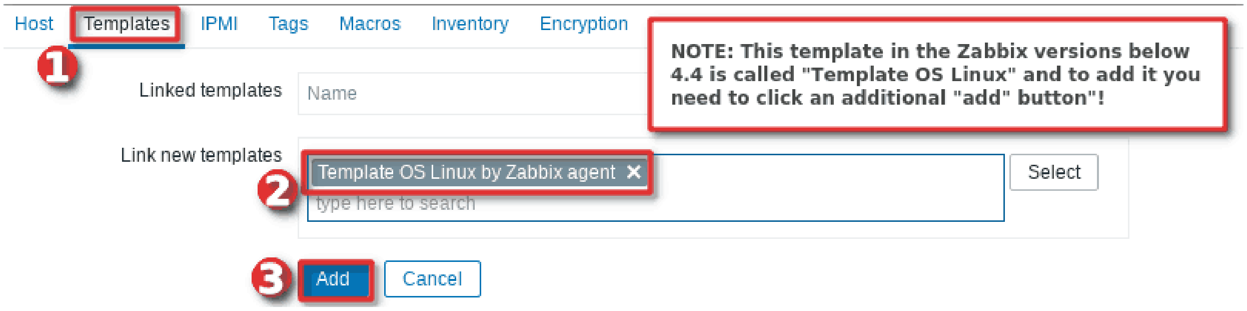
* Host name: l01lab
Visible name:
* Groups: Devices/OS/Linux ✕
* At least one interface must exist.

Agent interfaces

IP address	DNS name	Connect to	Port	Default
192.168.5.114		IP DNS	10050	● Remove

Add Linux host to Zabbix – Step 2

Switch to tab "*Templates*" and choose the "*Template OS* Linux by Zabbix agent" template under section "*Link new template*" by typing "*OS Linux*" and click the "*Add*" button to add the host to Zabbix.



NOTE: This template in the Zabbix versions below 4.4 is called "Template OS Linux" and to add it you need to click an additional "add" button"!

Linked templates: Name

Link new templates: Template OS Linux by Zabbix agent ✕

Add Linux host to Zabbix – Step 3

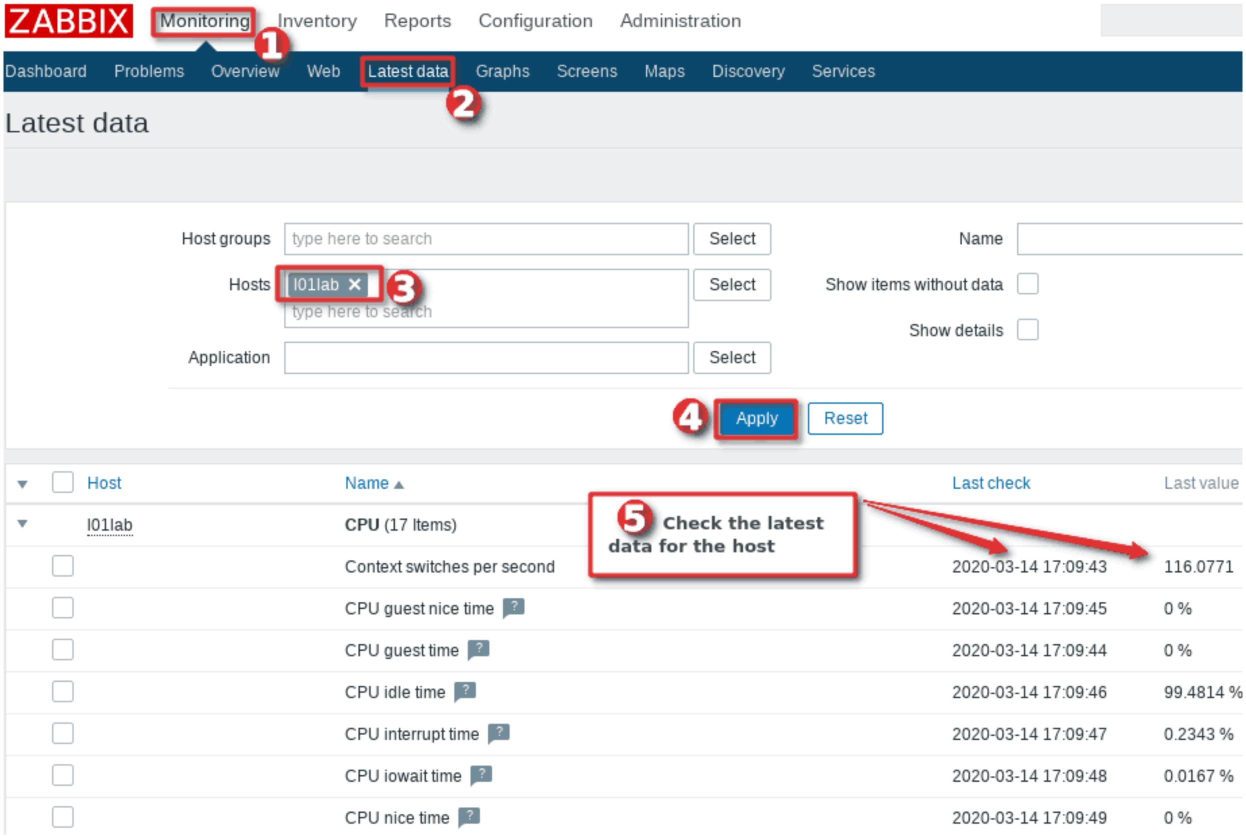
And you're done! If you are interested in automating this whole process of adding Linux hosts to Zabbix see the section "Configure auto registration for Linux Zabbix agents"

Note that in this tutorial I m using a template "*Template OS Linux by Zabbix agent*" that can only monitor passive Zabbix agents. However, if you want to monitor your host using Zabbix agents in active mode use a template called "*Template OS Linux by Zabbix agent active*".

Check out the section **"**Understanding Active vs Passive Zabbix Agent mode" to learn more about the differences between the active and passive agent mode.

Step 6: Check if Zabbix Agent is working correctly

You can check that the Zabbix agent is working properly by using the "*Latest Data*" option on the Zabbix frontend. Wait up to 5 minutes after you have installed and started Zabbix agent to allow for data to be collected. Look at columns "*Last check*" and "*Latest value*" just as showing in the image next page and if they are updating then the agent is working.



Latest data

Host groups: type here to search

Hosts: I01lab ✕ type here to search

Application:

Name:

Show items without data ☐

Show details ☐

5 Check the latest data for the host

	Host	Name ▲	Last check	Last value
▾	I01lab	**CPU** (17 Items)		
☐		Context switches per second	2020-03-14 17:09:43	116.0771
☐		CPU guest nice time	2020-03-14 17:09:45	0 %
☐		CPU guest time	2020-03-14 17:09:44	0 %
☐		CPU idle time	2020-03-14 17:09:46	99.4814 %
☐		CPU interrupt time	2020-03-14 17:09:47	0.2343 %
☐		CPU iowait time	2020-03-14 17:09:48	0.0167 %
☐		CPU nice time	2020-03-14 17:09:49	0 %

How to check the latest data collected on the Zabbix host

Your agent should be working and collecting data by now, but if you experience any problems, restart the Zabbix agent and check the log "`/var/log/zabbix/zabbix_agentd.log`". And if there is nothing unusual in the log file then check the firewall – make sure that TCP port 10050 on the host (where Zabbix agent is installed) and TCP port 10051 on the Zabbix server side are open.

CONGRATULATIONS!

You have successfully installed Zabbix Agent and your Linux server is being monitored!

No need to do anything else as other steps are optional!

CONTINUE TO LEARN MORE:

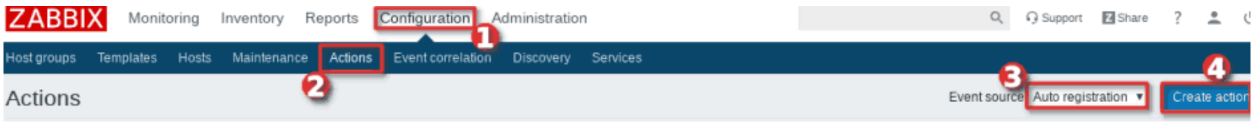
Auto registration of Zabbix agents (Linux OS)

Step 7: Configure auto registration for Linux Zabbix Agents

Adding one or two hosts to Zabbix manually is not a big problem. However, what if you need to add more servers to Zabbix? Or you just want to automate that tedious process of adding Linux hosts to Zabbix and linking them with the correct template and host group?

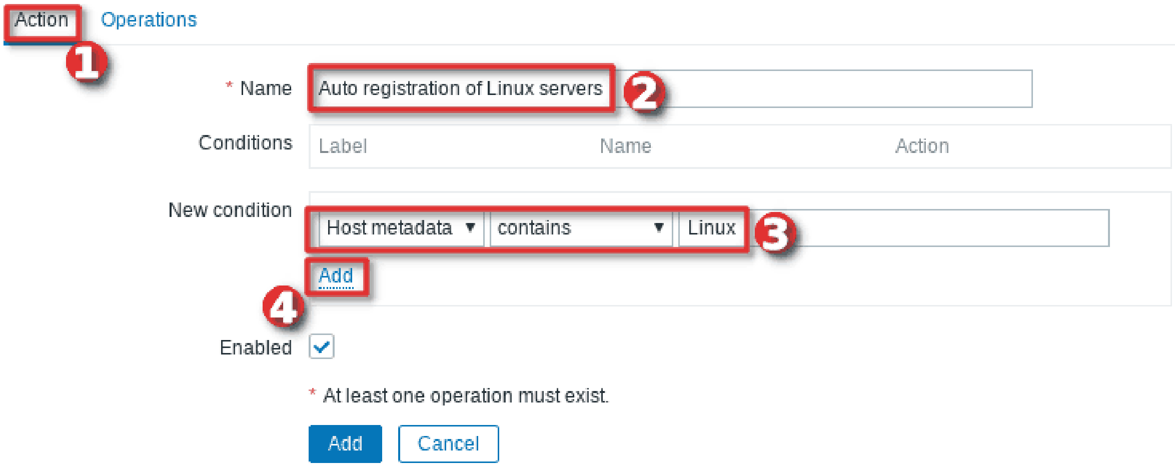
Don't worry, you don't have to write the script because Zabbix has a tool called "Auto registration"

Go to the "*Actions*" tool under the "*Configuration*" section, then select "*Auto registration*" from the "*Event source*" option and click the "*Create action*" button.



How to configure auto-registration of agents (Linux servers) in Zabbix – Step 1

On the "*Action*" tab define the "*Name*" of the action and add a "New condition" that will check if the "Host metadata" contains the word "Linux".



* Name: Auto registration of Linux servers

Conditions

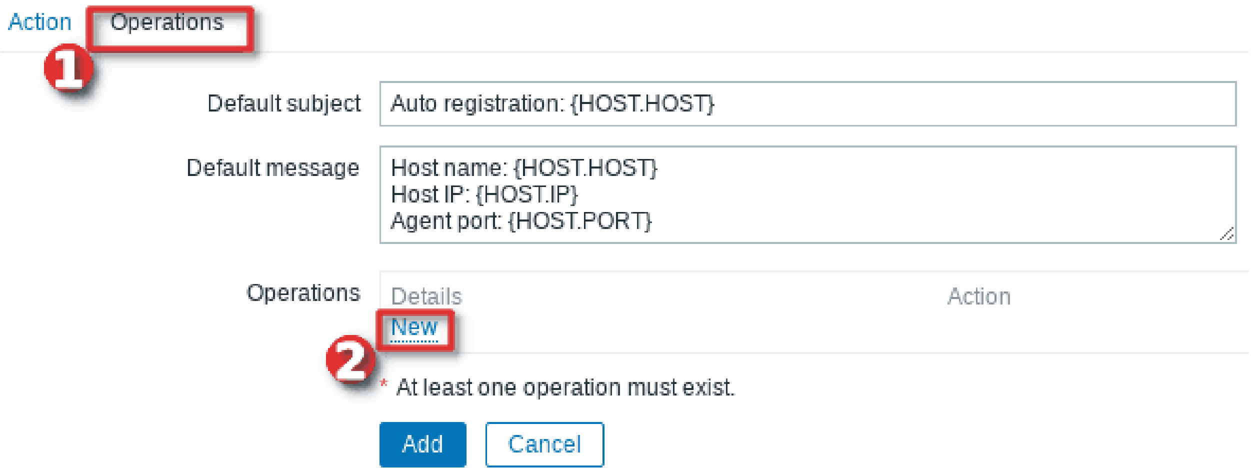
New condition: Host metadata ▾ contains ▾ Linux

Enabled ☑

* At least one operation must exist.

How to configure auto-registration of agents (Linux servers) in Zabbix – Step 2

Then, change tab to “Operations” and add new operation.



Default subject: Auto registration: {HOST.HOST}

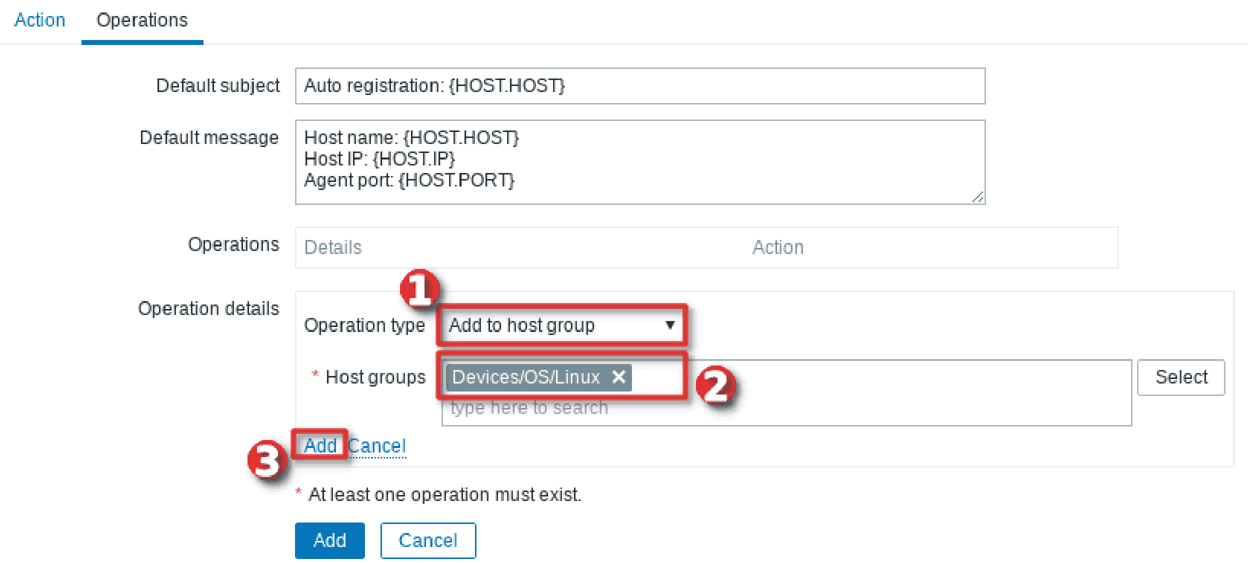
Default message:

```
Host name: {HOST.HOST}
Host IP: {HOST.IP}
Agent port: {HOST.PORT}
```

* At least one operation must exist.

How to configure auto-registration of agents (Linux servers) in Zabbix – Step 3

Define “*Operation type*” as “*Add to host group*” and then select to which “*Host groups*” will Linux hosts be added when discovered. In my case, I will use my custom host group called “*Devices/OS/Linux*“.



Default subject: Auto registration: {HOST.HOST}

Default message:

```
Host name: {HOST.HOST}
Host IP: {HOST.IP}
Agent port: {HOST.PORT}
```

Operation details

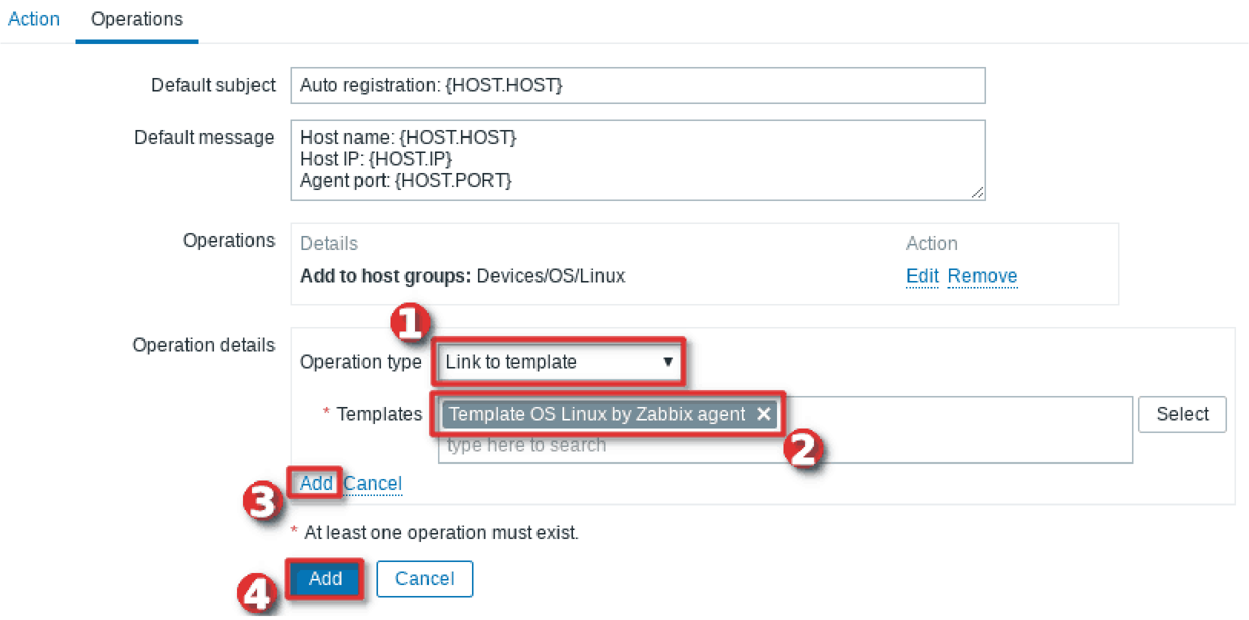
Operation type: Add to host group

* Host groups: Devices/OS/Linux

* At least one operation must exist.

How to configure auto-registration of agents (Linux servers) in Zabbix – Step 4

After that, you need to add a new operation by setting "*Link to the template*" as "Operation type" and then select which templates will be linked with the newly discovered Linux hosts. In my example, I will use template "*Template OS Linux by Zabbix agent*" (passive checks).



Default subject: Auto registration: {HOST.HOST}

Default message:
Host name: {HOST.HOST}
Host IP: {HOST.IP}
Agent port: {HOST.PORT}

Operations: **Add to host groups:** Devices/OS/Linux

Operation details

Operation type: Link to template

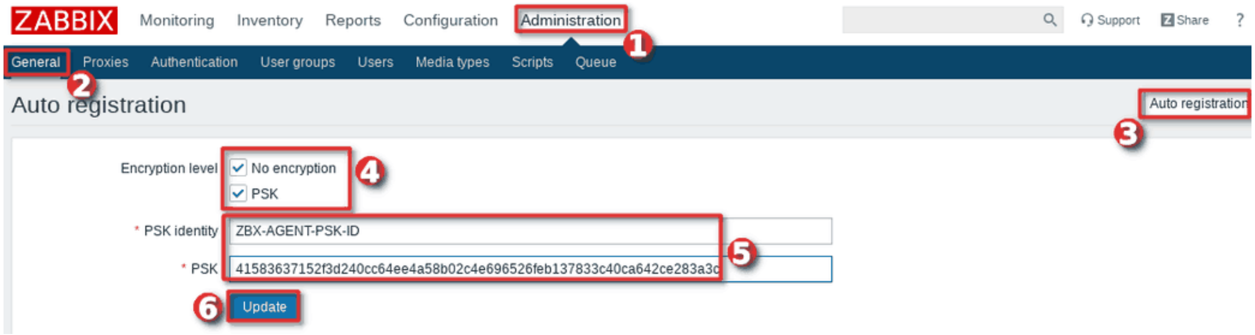
* Templates: Template OS Linux by Zabbix agent ✕

* At least one operation must exist.

How to configure auto-registration of agents (Linux servers) in Zabbix – Step 5

Well done! Auto-registration is configured. Wait a few minutes and your Linux server should appear in Zabbix. From now on, every time you install a Zabbix agent on a Linux OS, it will automatically be added to the Zabbix and linked with the appropriate host group and template.

Using PSK encryption on the Zabbix agents? Then there is one more step left, you need to add your PSK identity and PSK key using the "*Auto Registration*" option under the "*Administration*"→"*General*" section just as shown in the image below:



Auto registration

Encryption level: ☑ No encryption ☑ PSK

* PSK identity: ZBX-AGENT-PSK-ID

* PSK: 41583637152f3d240cc64ee4a58b02c4e696526feb137833c40ca642ce283a3c

How to configure PSK encryption for auto-registration in the Zabbix frontend

From now on, during the auto registration process, Zabbix will configure provided PSK identity and key on each registered host.

Step 8: Configure PSK encryption on the Zabbix Agent (Linux)

Zabbix supports encrypted communications between Zabbix server and Zabbix agent using Transport Layer Security (TLS) protocol v.1.2. You can use certificate-based and pre-shared key-based encryption (PSK), but in this tutorial we will configure PSK encryption.

a. Generate PSK key

Generate 256-bit (32 bytes) PSK key with openssl tool and save it with command:

```
sudo openssl rand -hex 32 > /etc/zabbix/zabbix_agent.psk
```

And set the correct file permission on the newly created file:

```
sudo chown zabbix:zabbix /etc/zabbix/zabbix_agent.psk
sudo chmod 700 /etc/zabbix/zabbix_agent.psk
```

Remember that you can always read your PSK key from the "`zabbix_agent.psk`" file :

```
cat /etc/zabbix/zabbix_agent.psk
41583637152f3d240cc64ee4a58b02c4e696526feb137833c40ca642ce283a3c
```

b. Configure Zabbix agent to support PSK encryption

Open "`zabbix_agentd.conf`" file with command

```
sudo vi /etc/zabbix/zabbix_agentd.conf
```

and add this configuration anywhere in file:

```
TLSConnect=psk
TLSAccept=psk
TLSPSKFile=/etc/zabbix/zabbix_agent.psk
TLSPSKIdentity=ZBX-AGENT-PSK-ID
```

Save and exit file.

Keep in mind that "*TLSPSKIdentity*" can be anything, so for security reasons set something else – don't use the sample!

Don't forget to restart Zabbix agent service after changing the configuration file:

```
sudo systemctl restart zabbix-agent
```

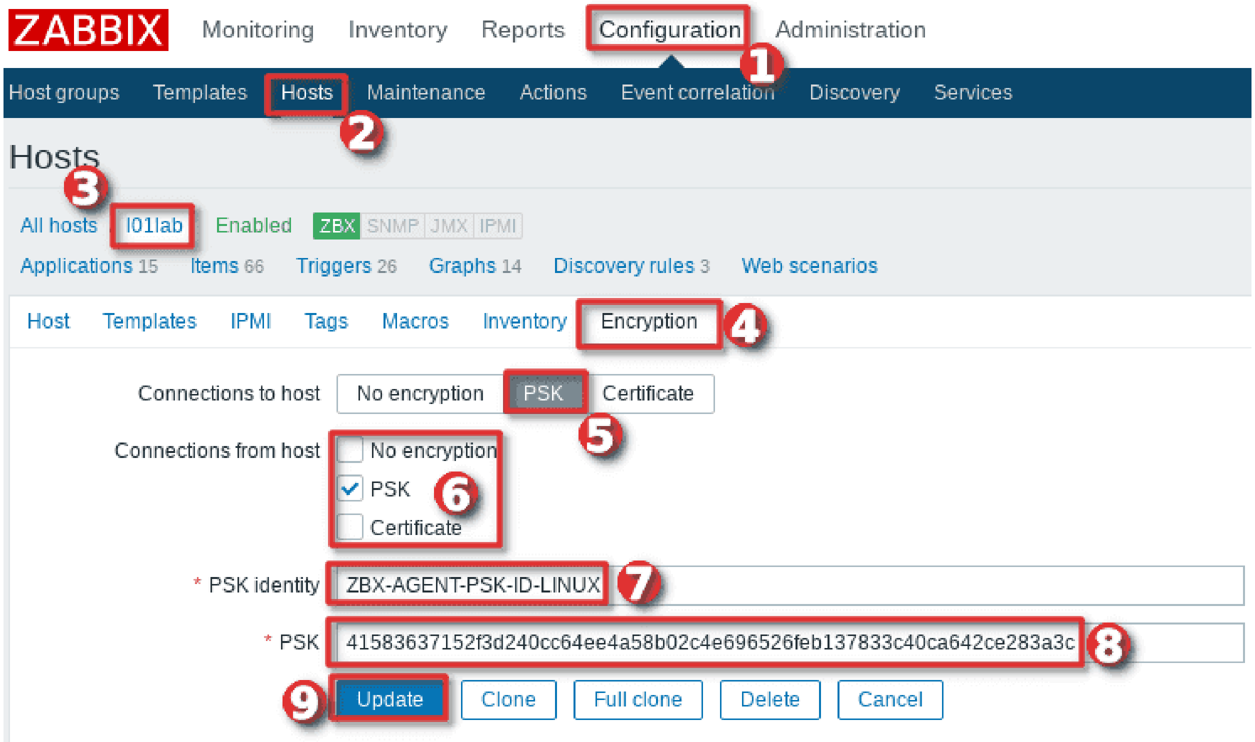
c. Enable PSK encryption on the agent in Zabbix frontend

Communication between Zabbix agent and server is not yet encrypted because we have enabled PSK encryption on the agent side but not on the server side.

We need to enable encryption on the server side so go to web frontend and select your "*Hosts*" tab under the "*Configuration*" section and find and click on your Linux hosts.

On the "*Encryption*" tab set PSK under "*Connections from hosts*" option and copy/paste "*PSK identity*" and "*PSK*" (key) that is configured on the Zabbix agent.

When you are done with configuration click the "*Update*" button just as shown in the image below.



Connections to host: No encryption [✓ PSK] Certificate

Connections from host: ☐ No encryption ☑ PSK ☐ Certificate

* PSK identity: ZBX-AGENT-PSK-ID-LINUX

* PSK: 41583637152f3d240cc64ee4a58b02c4e696526feb137833c40ca642ce283a3c

How to configure PSK encryption on Zabbix agent in the frontend

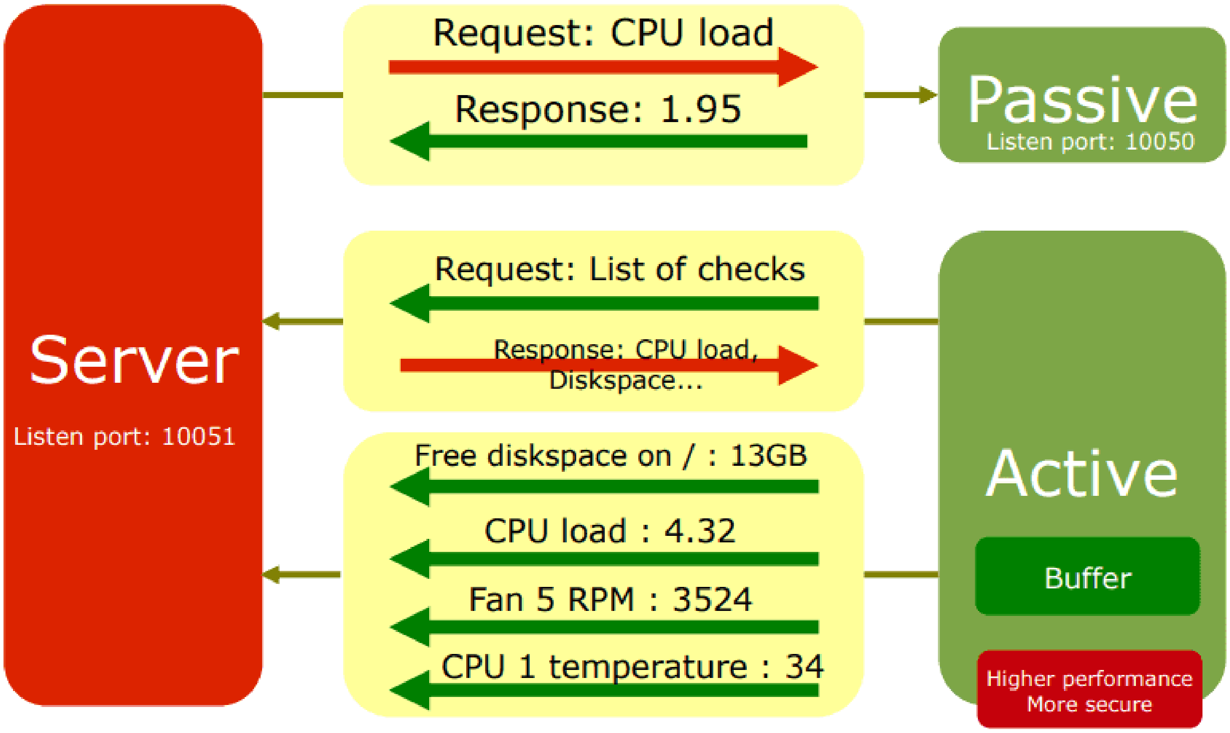
Keep in mind, that you can automate the configuration of the host encryption (PSK) on the frontend using the Zabbix auto registration process.

Step 9: Understanding Active vs Passive Zabbix Agent mode

When using a Zabbix agent in active mode, it will connect to the Zabbix server via port 10051 to retrieve configuration and send data. This is a great feature that allows an active Zabbix agent to work behind the firewall and to offload the Zabbix server in large environments.

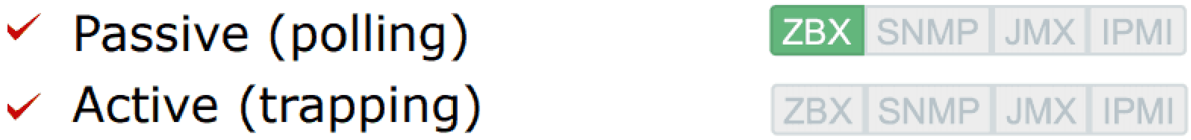
On the other hand, if you use a Zabbix agent in passive mode Zabbix server will initiate a connection via port 10050 and retrieve data from the agent. The Zabbix server will do this for every metric (item) every few minutes – which is very inefficient! Because of this, active mode is more recommended.

An additional advantage of the Zabbix agent in active mode is that it can read logs from the device and that is not possible if the Zabbix agent is used in passive mode.



Differences between Zabbix agent active and passive check (Source: Zabbix)

You can detect on Zabbix host if the agent is working in active or passive mode. Passive mode will show red or green “ZBX” icon in the agent status bar and active mode will show grey “ZBX” icon:



- ✓ Passive (polling)
- ✓ Active (trapping)

Thank you for reading!

LNC 22082020