Install Zabbix Agent on Windows (msi) | Server Monitoring Guide

In this tutorial, I will show you how to install Zabbix agent for Windows server using an MSI Installer package and how to monitor Windows server with Zabbix monitoring system.

Using this guide you can monitor almost the entire Windows OS family: Windows server 2012 R2, Windows Server 2016, Windows Server 2019, Windows 10, Windows 8 and Windows 7.

Installation is quite simple, just download and install the Zabbix agent MSI installer following steps 1 and 2, but if you want to learn more, read the full guide.

Zabbix 5 dashboard

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, Rasbian.

Need help with installing Zabbix agent on Linux OS? Check out this guide: Zabbix Agent (Linux): Install on Ubuntu, CentOS, RHEL, Debian, etc.

Step 1: Download Zabbix Agent Installer for Windows (msi)

In this tutorial, I will use the latest Zabbix agent 5.0.2 LTS version, that version is compatible with Zabbix server 5.x or newer.

Windows Zabbix Agent LTS v5.0.2 (**recommended)**	Download: 64-bit or 32-bit
Windows Zabbix Agent LTS v4.0.22	Download: 64-bit or 32-bit

I always recommend using the latest LTS version to take full advantage of new features and improved performance so make sure to download installer zabbix_agent-5.0.2-windows-amd64-openssl.msi for **64-bit Windows** or zabbix_agent-5.0.2-windows-i386-openssl for **32-bit Windows**. However, if you are still on Zabbix server 4.x then use agent 4.0.22 version.

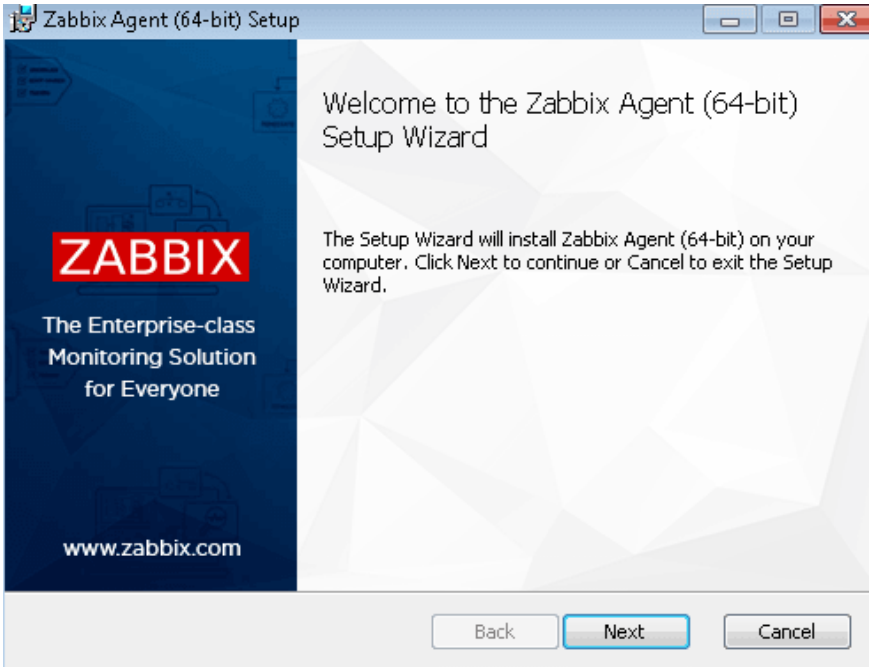
And don't try to install a 32-bit package on 64-bit Windows because it won't work!

Step 2: Install Zabbix Agent on Windows using MSI installer

I will install Zabbix Agent on Windows server using installation wizard but if you prefer command-line based installation check out section "Install Zabbix agent via Windows command-line (CMD)"

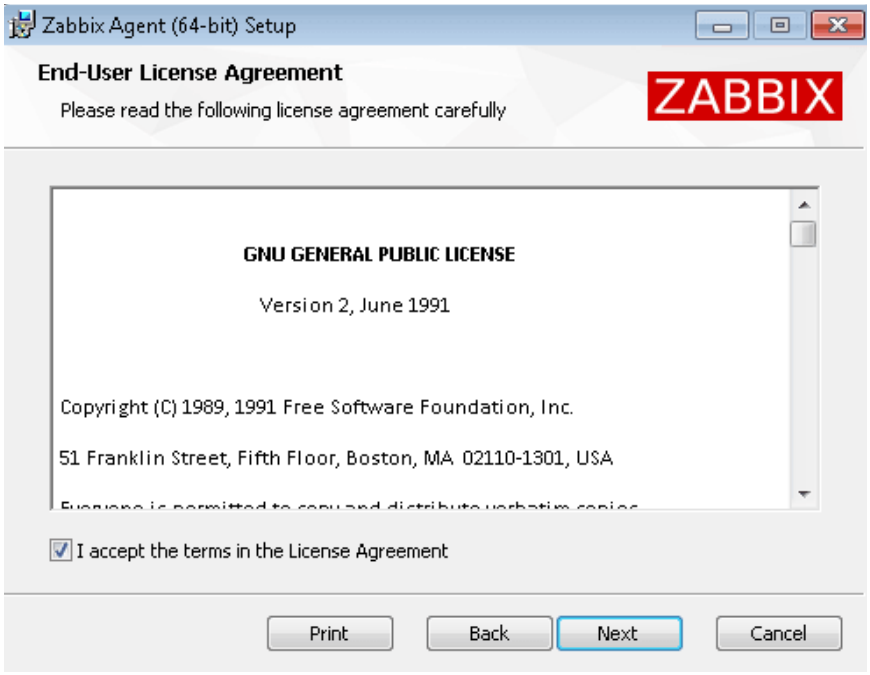
Just to make clear, in this tutorial I will use Zabbix server with IP address **192.168.5.43** to monitor Windows machine called **w01services** with IP address **192.168.5.22**.

Double click on Zabbix MSI installer that you have downloaded in the previous step and click "*Next*" just as shown in the image below.



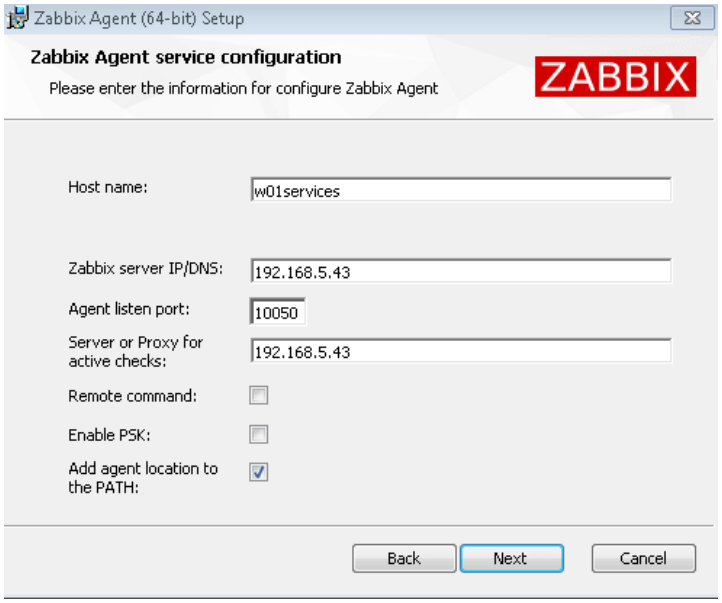
Install Zabbix Agent on Windows using MSI installer – Step 1

Accept the terms and click the "*Next*" button.



Install Zabbix Agent on Windows using MSI installer – Step 2

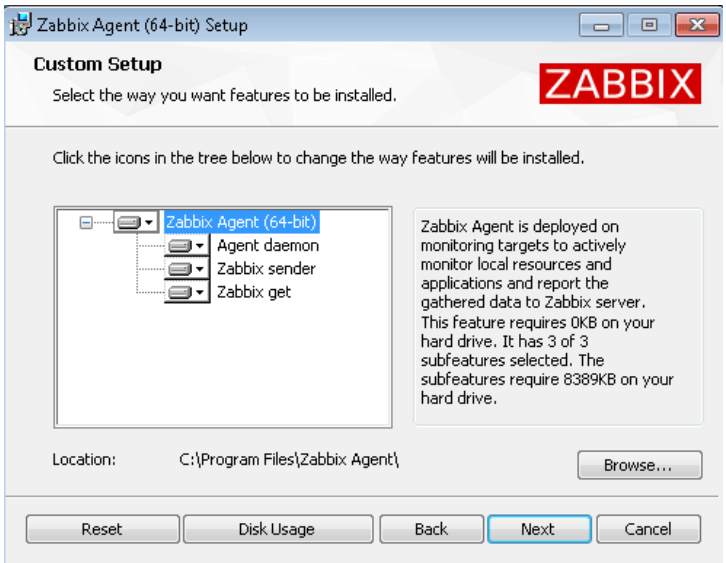
Define custom "*Host name*" or use fully qualified domain name (FQDN) of the Windows machine in the "*Host name*" field. Then enter IP address of the Zabbix server under "*Zabbix server IP/DNS*" and "*Server or Proxy for active checks*" field and you are done.



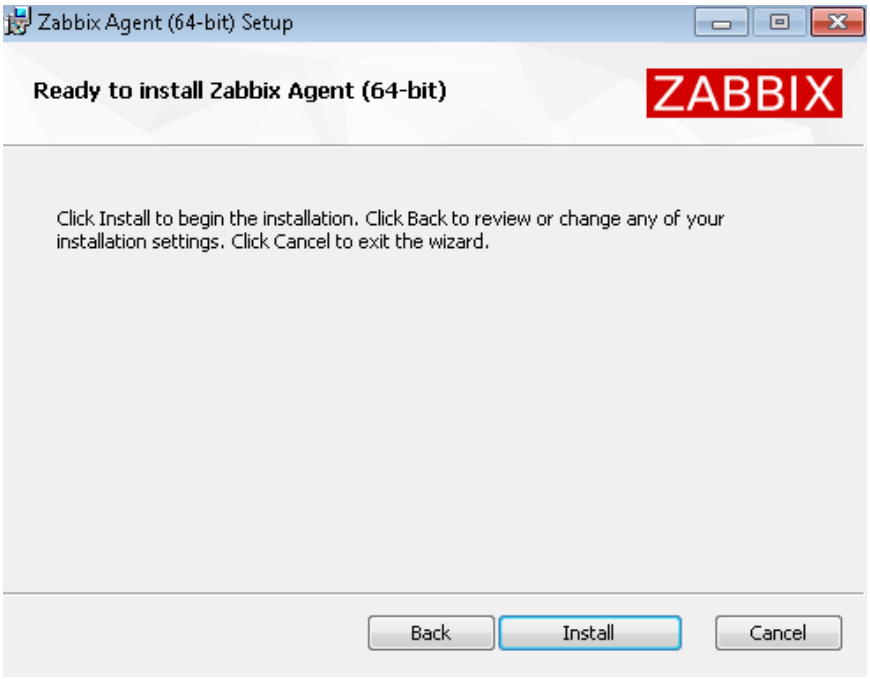
Install Zabbix Agent on Windows using MSI installer – Step 3

Only select "*Remote Command*" if you have need to execute remote commands on Windows from the Zabbix server, but be careful as this option increases security risk on Windows OS.

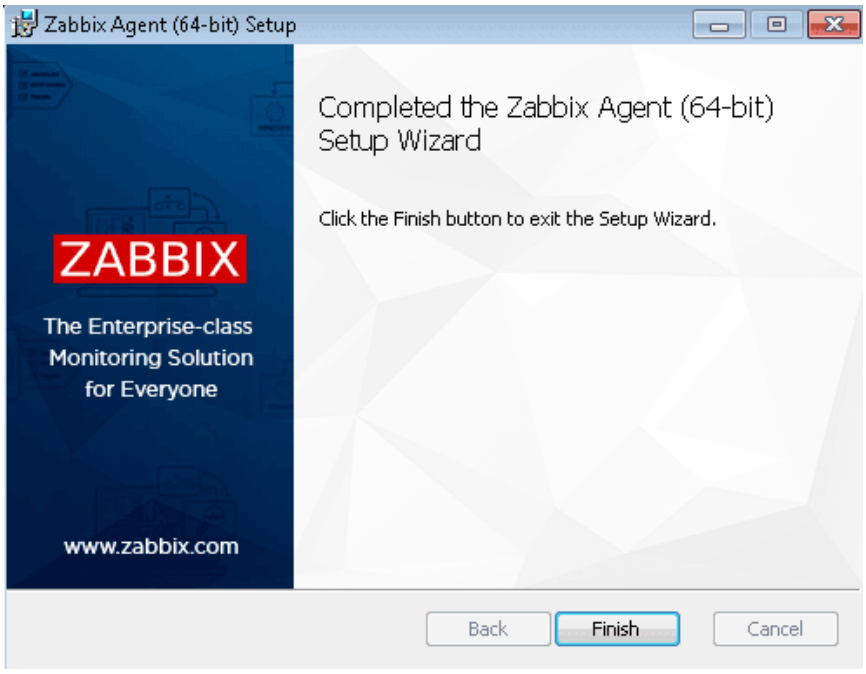
Go through the rest of the installation by clicking "*Next*", "*Install*" and "*Finish*".



Install Zabbix Agent on Windows using MSI installer – Step 4



Install Zabbix Agent on Windows using MSI installer – Step 5

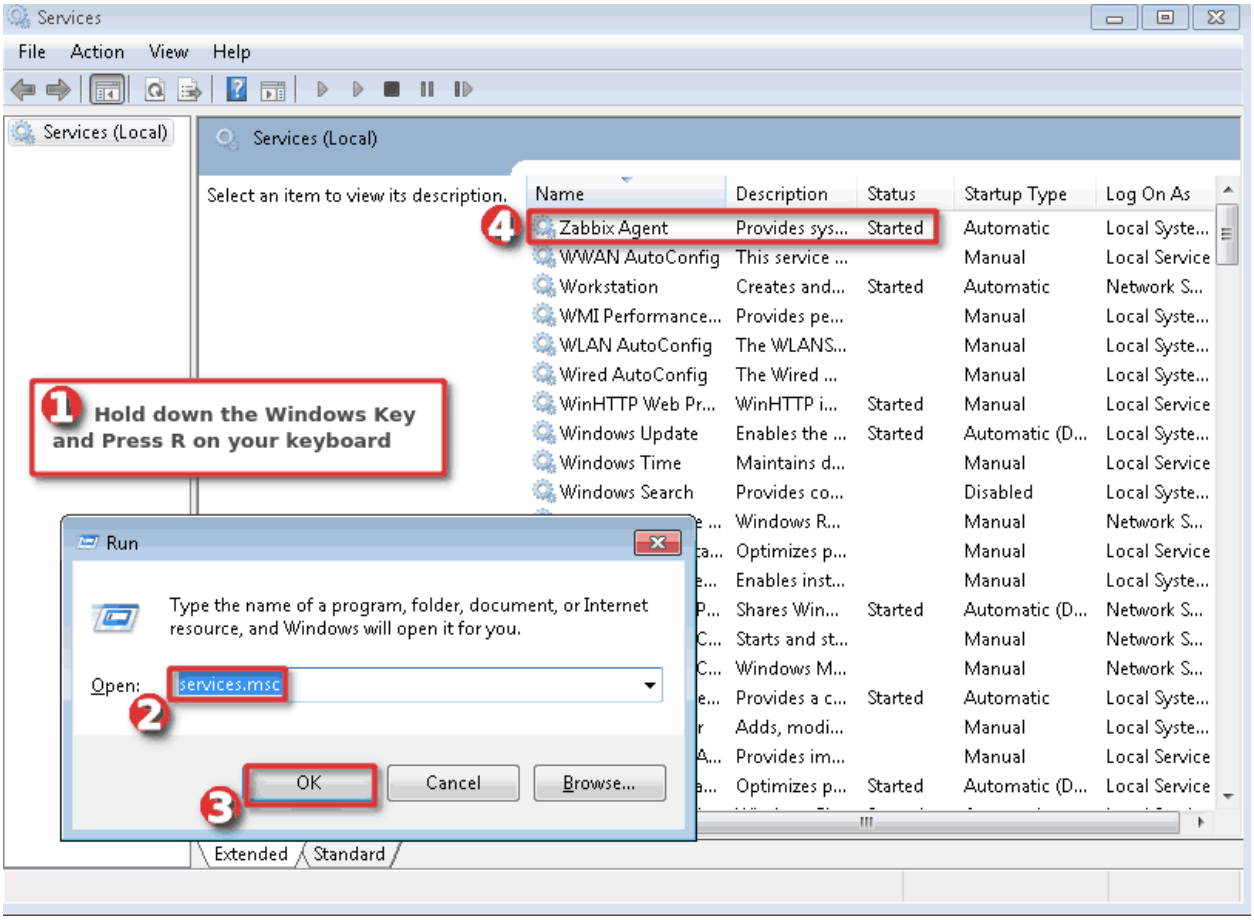


Install Zabbix Agent on Windows using MSI installer – Step 6

You don't need to configure Windows firewall manually because the MSI installer will automatically add a firewall rule to permit Zabbix TCP port 10050.

Finally, we need to check that the Zabbix agent is up and running.

Hold down the "*Windows key*" and press "*R*" on the keyboard, type "*services.msc*", press "OK" and check the "Status" column for "*Zabbix Agent*" service exactly as shown in the picture below. Status should be "*Started*" if the installation was successful.



How to check Zabbix agent service on Windows

WELL DONE!

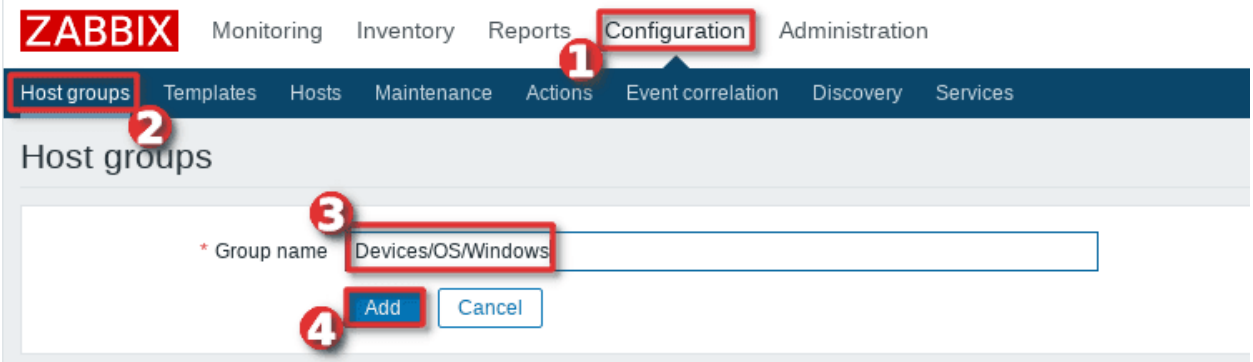
You have successfully installed and configured Zabbix agent on Windows OS!

Now it's time to add that Windows host to Zabbix monitoring system.

Step 3: Add Windows host to Zabbix monitoring system

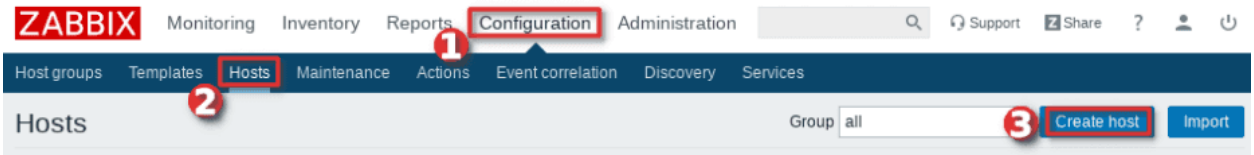
I hope you already have the Zabbix monitoring system installed, and if not then install it on your favorite Linux distribution in less than 10 minutes: CentOS/RHEL, Ubuntu, Debian, Rasbian.

You can add a host to existing host group or you can create a new host group for your Windows servers. I will create host group "`Devices/OS/Windows`" 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**):



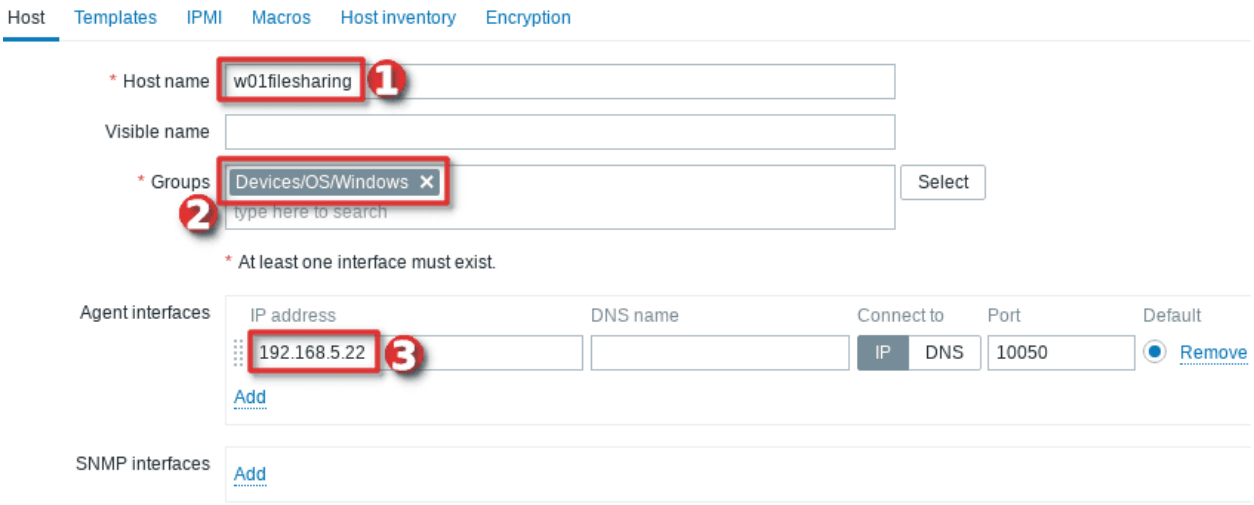
Create Zabbix host group for Windows servers

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



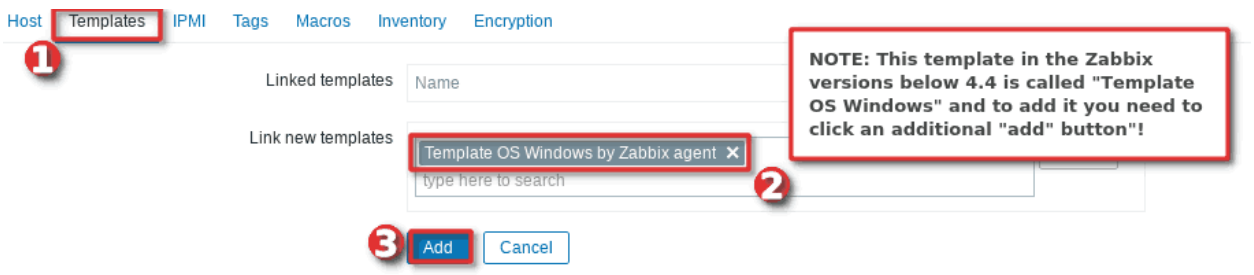
Add Windows host to Zabbix – Step 1

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



Add Windows host to Zabbix – Step 2

Switch to tab "*Templates*" and choose the "*Template OS Windows*" template under section "*Link new template*" by typing "*OS Windows*".



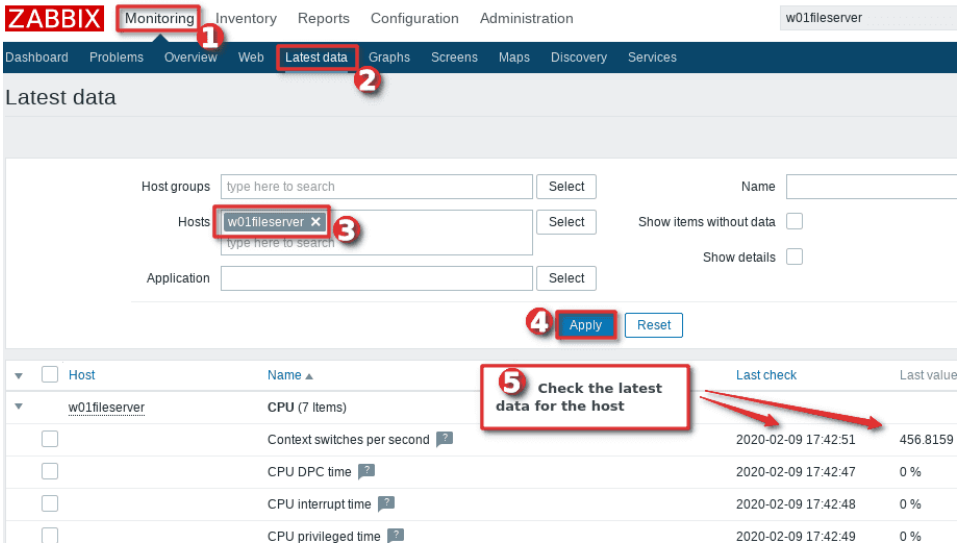
Add Windows host to Zabbix – Step 3

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

Note that in this tutorial I m using a template "*Template OS Windows 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 Windows 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 4: 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*" and if they are updating then the agent is working.



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 Zabbix agent service and check the log "`C:\Program Files\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 Windows server is being monitored!
No need to do anything else as other steps are optional!

CONTINUE TO LEARN MORE:

How to manage Zabbix agent service on Windows
Auto registration of Zabbix agents (Windows OS)
Learn how to Secure Zabbix Agent
Alternative Zabbix agent installation via Windows command-line (CLI)
Understanding Active vs Passive Zabbix Agent mod

Step 5: Restart Zabbix Agent service on Windows

In the previous steps, we learned how to check the status of Zabbix agent service using the "services.msc" option, and now we will learn how to use the command line interface (CMD) to stop or start the agent and check its status.

Click on "*Windows Start*" button and type "cmd" in the search bar, right-click on "cmd" icon and select option "*Run as administrator*" and use these commands to start/stop the agent:

```
net stop "Zabbix Agent"
net start "Zabbix Agent"
```

And to check Zabbix agent service status use the command:

```
sc query "Zabbix Agent" | findstr /i "STATE"
```

You should get status "*RUNNING*" if the Zabbix agent is up and running!

Step 6: Configure auto registration for Windows 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 Windows 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".

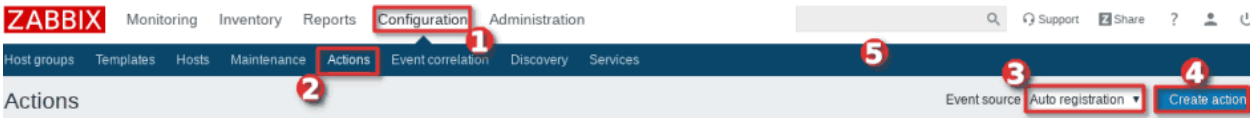
Before we configure Zabbix frontend, make sure that all of your Zabbix agents have "`HostMetadata=Windows`" line in their configuration file (default path: "`C:\Program Files\zabbix\zabbix_agentd.conf`"). And if that line does not exist, add it and restart the Zabbix Agent afterward. You can automate that via CLI like this:

```
echo HostMetadata=Windows >> C:\"Program Files"\zabbix\zabbix_agentd.conf
net stop "Zabbix Agent"
net start "Zabbix Agent"
```

In the future always install the Zabbix agent on Windows with the "`HostMetadata=Windows`" parameter if you are planning to use the auto-registration feature!

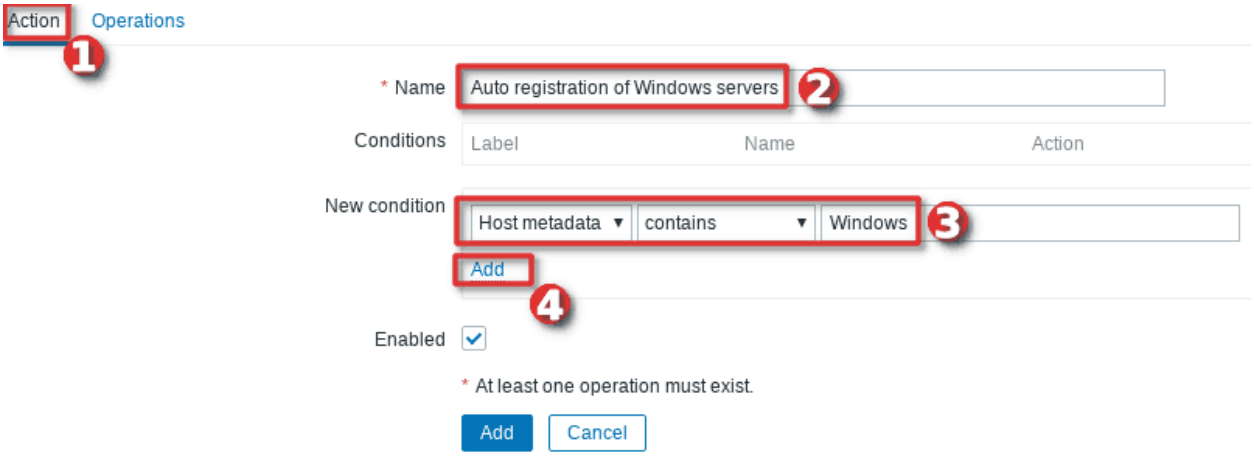
Now that we've clarified that let's configure auto-registration on the Zabbix frontend.

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



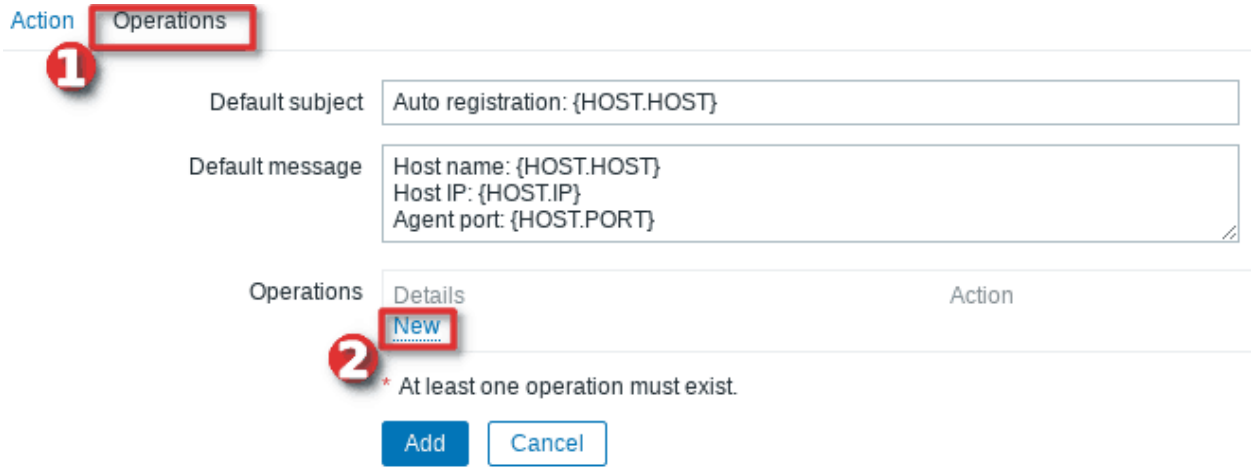
How to configure auto-registration of agents (Windows servers) in Zabbix – Step 1

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 "windows".



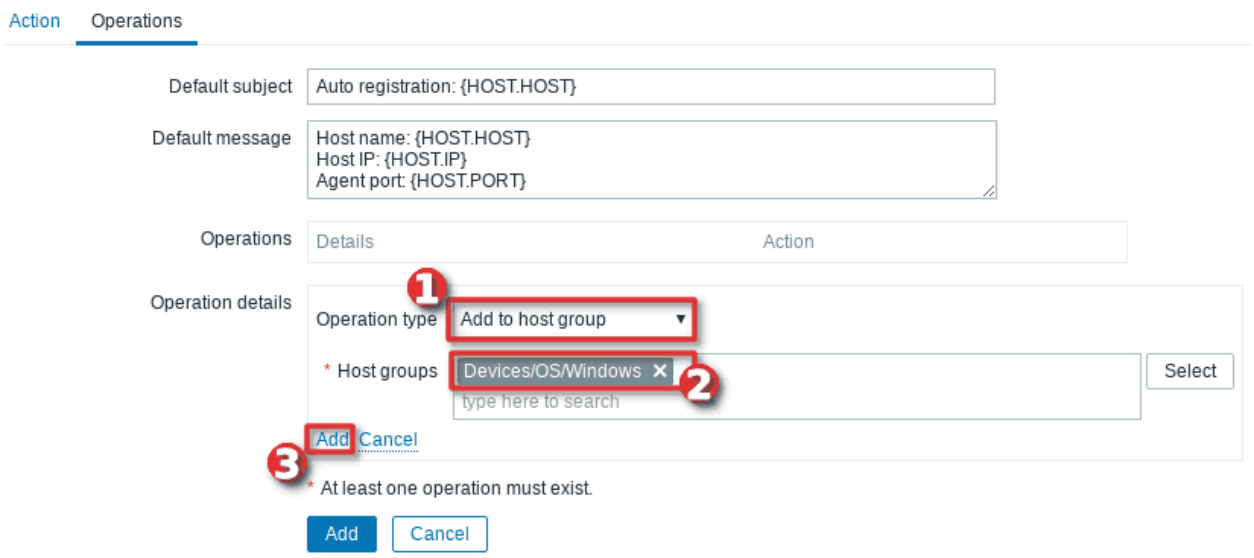
How to configure auto-registration of agents (Windows servers) in Zabbix – Step 2

Then, change tab to "Operations" and add new operation.



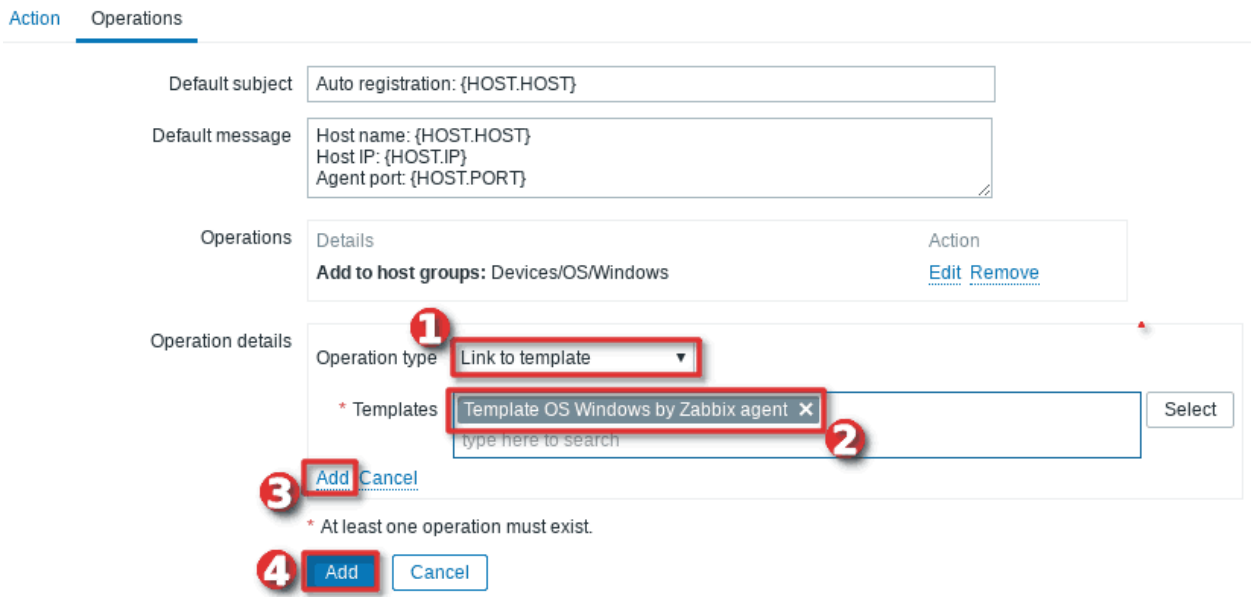
How to configure auto-registration of agents (Windows servers) in Zabbix – Step 3

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



How to configure auto-registration of agents (Windows 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 Windows hosts. In my example, I will use template "*Template OS Windows by Zabbix agent*" (passive checks)

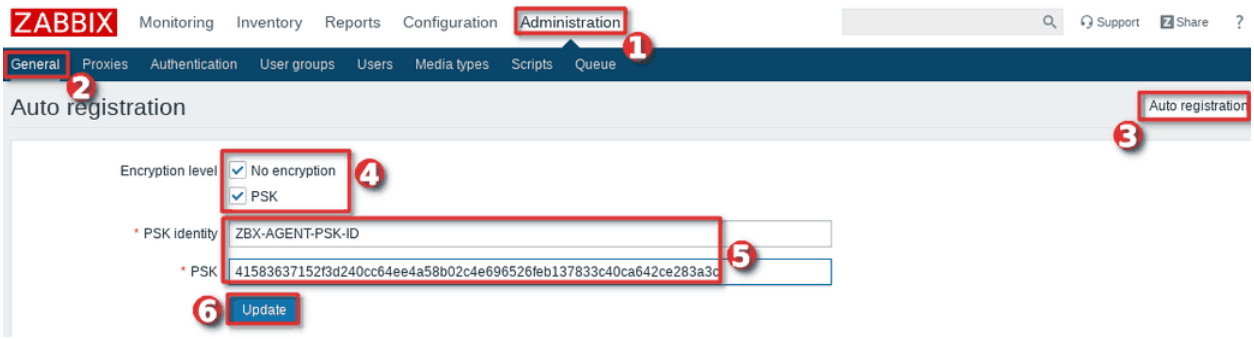


How to configure auto-registration of agents (Windows servers) in Zabbix – Step 5

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

Note, that you can add anything you want to the "`HostMetadata`" parameter. For example, you can have a host that has in Zabbix agent configuration file defined "`HostMetadata=Windows:Tomcat:Prod`" or another with "`HostMetadata=Windows:MSSQL:Test`". For the first host, you can configure auto-registration to add to host groups: "Windows", "Web servers" and "Production servers" and to link templates that can monitor Windows and Tomcat server. And the second host can be added to host groups: "Windows", "Databases", and "Test servers" and linked with templates that can monitor Windows server and Microsoft SQL database.

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:



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 7: Configure PSK encryption on Zabbix Agent (Windows)

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.

In this step, I will show you how to configure PSK encryption on an already installed Zabbix agent, but keep in mind that all of these configurations can be configured during the installation

a. Generate PSK key

Generate 256-bit (32 bytes) PSK key with openssl command on Zabbix server (or use some other tool on Windows):

```
$ openssl rand -hex 32
 1b38eac9d870a319f201fb1da989c081faba993e3d91940193224a100cdcdb86
```

On Windows server, create a new text file "`ZabbixAgentPSK.txt`" in the default Zabbix agent installation folder ("`C:\Program Files\zabbix`") and put that PSK key in the first line of the file. Don't forget to save the file before closing.

b. Configure Zabbix agent to support PSK encryption

Open "`C:\Program Files\zabbix\zabbix_agentd.conf`" file with text editor (Notepad++) and add this configuration anywhere in file:

```
TLSConnect=psk
TLSAccept=psk
TLSPSKFile=C:\Program Files\zabbix\ZabbixAgentPSK.txt
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!

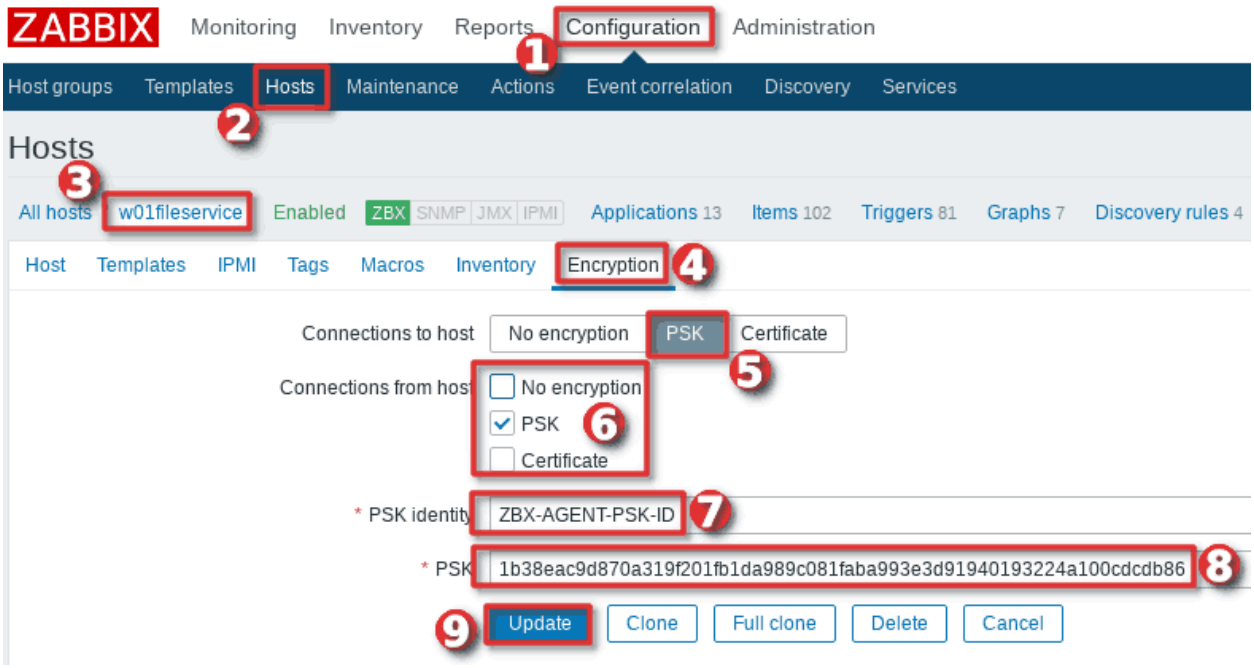
c. Enable PSK encryption on the agent in Zabbix frontend

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 Windows 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.



How to configure PSK encryption on Zabbix agent in the frontend

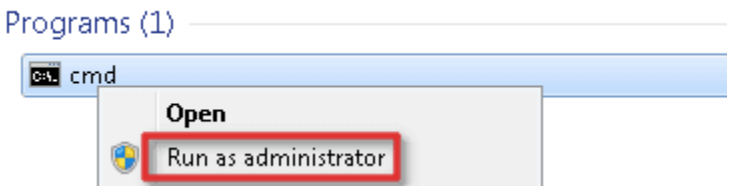
Keep in mind, that you can automate the configuration of the host encryption (PSK) on the frontend using the Zabbix auto registration process.

Step 8: Install Zabbix agent via Windows command-line (CMD)

This step is for those who prefer command-line based installation instead of wizard-based installation.

a. Run CMD as administrator

Click on "*Windows Start*" button and type "CMD" in the search bar, right-click on "cmd" and select option "*Run as administrator*":



b. Download Zabbix agent

Download installer zabbix_agent-5.0.2-windows-amd64-openssl.msi for **64-bit Windows** or zabbix_agent-5.0.2-windows-i386-openssl for **32-bit Windows** and save it on a "C:\" disk or somewhere else.

c. Change directory and set installation folder

Change directory to the path where you have downloaded the MSI file and set the installation folder with commands:

```
cd C://
SET INSTALLFOLDER=C:\Program Files\zabbix
```

d. Install Zabbix agent using msiexec

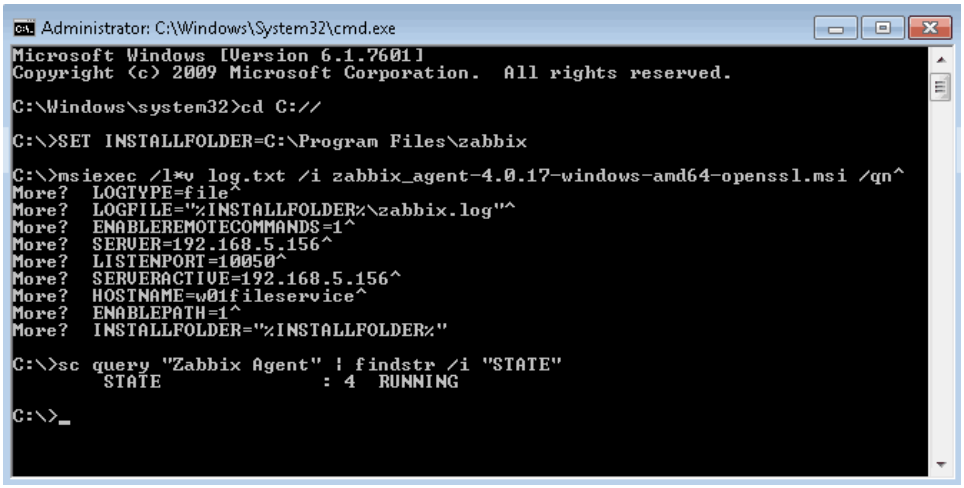
Here is an example of Zabbix agent installation that will work for most people, just change parameteres "*SERVER*," "*SERVERACTIVE*" and "*HOSTNAME*" to suit your enviroment.

```
msiexec /l*v log.txt /i zabbix_agent-4.0.17-windows-amd64-openssl.msi /qn^
 LOGTYPE=file^
 LOGFILE="%INSTALLFOLDER%\zabbix.log"^
 SERVER=192.168.5.156^
 LISTENPORT=10050^
 SERVERACTIVE=192.168.5.156^
 HOSTNAME=w01fileservice^
 ENABLEPATH=1^
 INSTALLFOLDER="%INSTALLFOLDER%"
```

Check "*Zabbix agent*" service status with the command:

```
sc query "Zabbix Agent" | findstr /i "STATE"
```

If the Zabbix agent is up and running then the status should be "*RUNNING*".



Picture showing how to install Zabbix agent on Windows server using the command line (CMD)

Note, if you are planning to use the auto-registration feature don't forget to add "`HostMetadata=Windows`" parameter to "`zabbix_agentd.conf`" and restart Zabbix agent afterward because Zabbix CLI installation doesn't support "`HostMetadata`" parameter:

```
echo HostMetadata=Windows >> C:\"Program Files"\zabbix\zabbix_agentd.conf
net stop "Zabbix Agent"
net start "Zabbix Agent"
```

e. Example of Zabbix agent installation with additional options

You can set almost any Zabbix agent parameter during installation, here is one example of an installation where many parameters are used.

```
SET INSTALLFOLDER=C:\Program Files\zabbix

msiexec /l*v log.txt /i zabbix_agent-4.0.17-windows-amd64-openssl.msi /qn^
 LOGTYPE=file^
 LOGFILE="%INSTALLFOLDER%\zabbix.log"^
 ENABLEREMOTECOMMANDS=1^
 SERVER=10.10.10.162^
 LISTENPORT=10055^
 SERVERACTIVE=10.10.10.162^
 HOSTNAME=cmr_server^
 TLSCONNECT=psk^
 TLSACCEPT=psk^
 TLSPSKIDENTITY=CompanyPSKID^
```

```
TLSPSKFILE="%INSTALLFOLDER%\company_key.psk"^
TLSCAFILE="c:\temp\file1.txt"^
TLSCRLFILE="c:\temp\fil2.txt"^
TLSSERVERCERTISSUER="Company CA"^
TLSSERVERCERTSUBJECT="Company Cert"^
TLSCERTFILE="c:\temp\file4.txt"^
TLSKEYFILE="c:\temp\file5.txt"^
ENABLEPATH=1^
INSTALLFOLDER="%INSTALLFOLDER%"
SKIP=fw
```

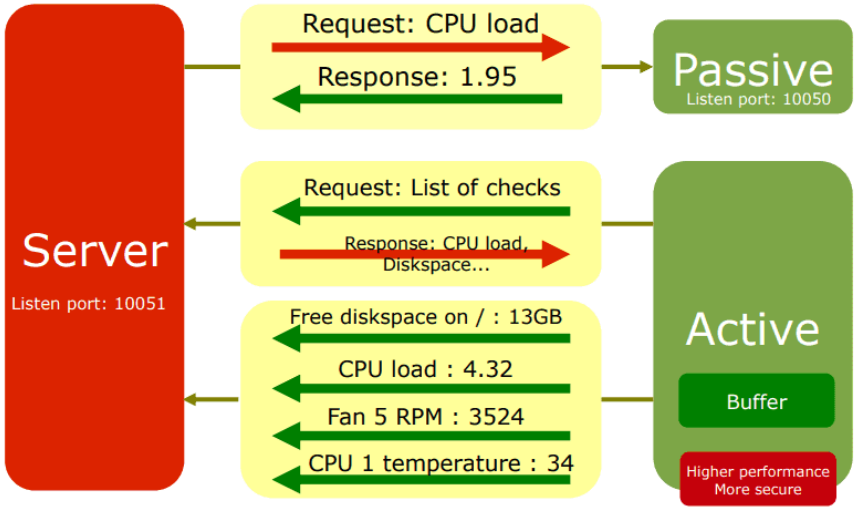
Parameter "*SKIP=fw*" means that the firewall exception rule will not be added. Explanations of other parameters can be found in the official Zabbix documentation section Zabbix Agent (Windows).

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:

Thank you for reading!

LNC 22082020