

How to Install Nagios on Ubuntu?

written by sysadmin | 12 February 2025

Nagios is an event monitoring system created by Ethan Galstad and first released in 2002, which offers monitoring and alerting services for servers, switches, applications, and services. It alerts users when things go wrong and alerts them again when the problem has been resolved. There are [2 types of Nagios](#): Nagios XI for the enterprise version and Nagios Core for the free version. This article will explain how to install Nagios Core on Ubuntu.

Problem

How to install Nagios on Ubuntu?

Solution

Here are the steps to install Nagios on Ubuntu, and these steps work on Ubuntu 24.04 and below and I think it should also work on Debian.

1. Download the packages

Install the packages needed to install Nagios using the command below:

```
sudo apt-get install autoconf gcc libc6 make wget unzip apache2 php  
libapache2-mod-php libgd-dev libssl-dev
```

2. Create a user and a group

After that, create a user and group for Nagios using the commands:

```
sudo useradd nagios  
sudo groupadd nagcmd  
sudo usermod -a -G nagcmd nagios  
sudo usermod -a -G nagcmd www-data
```

3. Download Nagios

Use the commands below to download Nagios, where at the time of this writing (February 2025), the latest version of Nagios is version 4.5.9:

```
cd /tmp
wget
https://github.com/NagiosEnterprises/nagioscore/archive/refs/heads/master.zip
-O nagios.zip
unzip nagios.zip
cd nagioscore-master/
```

4. Install Nagios

By default, Linux will create a Nagios folder in the /usr/local folder to save Nagios configuration files. So, use the following commands to install Nagios:

```
sudo ./configure --with-command-group=nagcmd --with-httpd-
conf=/etc/apache2/sites-enabled
```

Info

If you want to save all Nagios files in a non-default folder, for example, in the /data folder, then use the following command: **sudo ./configure --prefix=/data/nagios --with-command-group=nagcmd --with-httpd-conf=/etc/apache2/sites-enabled**

After that, run the following commands:

```
sudo make all
sudo make install
sudo make install-init
sudo make install-daemoninit
sudo make install-config
sudo make install-commandmode
sudo make install-webconf
sudo a2enmod rewrite
sudo a2enmod cgi
```

5. Create the password

Create a password for the user Nagios to access the Nagios application. Nagiosadmin is usually a popular username for Nagios, but you can create another.

```
sudo htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
```

```
sysadmin@ubuntu2404:/tmp/nagioscore-master$ sudo htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
New password:
Re-type new password:
Adding password for user nagiosadmin
sysadmin@ubuntu2404:/tmp/nagioscore-master$
```

Create the password

Info

If you installed Nagios in a non-default folder, for example, in the /data folder, execute the below command: **sudo htpasswd -c /data/nagios/etc/htpasswd.users nagiosadmin**

6. Download Nagios Plugins

Plugins are compiled executables or scripts (Perl, shell, Python, PHP, Ruby, etc.) that can be run from a command line to check the status of a host or service. Nagios Core uses the results from plugins to determine the current status of hosts and services on your network. As of this writing (February 2025), the latest version of Nagios plugins is version 2.4.12. You can check the latest version of Nagios plugins on this site. Run the following commands to download Nagios plugins:

```
cd /tmp
wget
https://github.com/nagios-plugins/nagios-plugins/archive/refs/heads/master.zip
p -O nagios-plugins.zip
unzip nagios-plugins.zip
cd nagios-plugins-master/
```

7. Install Nagios Plugins

After that, install Nagios plugins using the following commands:

```
./tools/setup
sudo ./configure --with-nagios-user=nagios --with-nagios-group=nagios
sudo make
sudo make install
```

8. Check the configuration

After installing Nagios and Nagios plugins, run the following command to check the configuration of Nagios:

```
sudo /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
```

Info

If you installed Nagios in a non-default folder, for example, in the /data folder, execute the below command: **sudo /data/nagios/bin/nagios -v /data/nagios/etc/nagios.cfg**

and make sure there is no error like in the image below:

```
sysadmin@ubuntu2404:/tmp/nagios-plugins-master$ sudo /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

Nagios Core 4.5.9
Copyright (c) 2009-present Nagios Core Development Team and Community Contributors
Copyright (c) 1999-2009 Ethan Galstad
Last Modified: 2024-12-19
License: GPL

Website: https://www.nagios.org
Reading configuration data...
  Read main config file okay...
  Read object config files okay...

Running pre-flight check on configuration data...

Checking objects...
  Checked 8 services.
  Checked 1 hosts.
  Checked 1 host groups.
  Checked 0 service groups.
  Checked 1 contacts.
  Checked 1 contact groups.
  Checked 24 commands.
  Checked 5 time periods.
  Checked 0 host escalations.
  Checked 0 service escalations.
Checking for circular paths...
  Checked 1 hosts
  Checked 0 service dependencies
  Checked 0 host dependencies
  Checked 5 timeperiods
Checking global event handlers...
Checking obsessive compulsive processor commands...
Checking misc settings...

Total Warnings: 0
Total Errors: 0

Things look okay - No serious problems were detected during the pre-flight check
sysadmin@ubuntu2404:/tmp/nagios-plugins-master$
```

Check the Nagios configuration



9. Turn on the services

Turn on the services using the commands below:

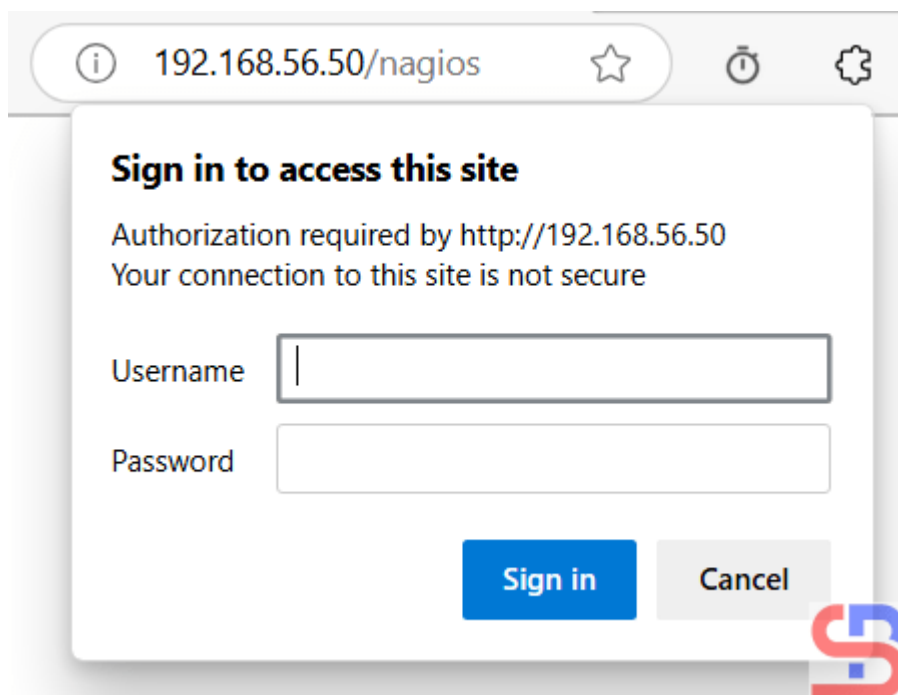
```
sudo systemctl start nagios.service
sudo systemctl enable nagios
sudo systemctl restart apache2.service
```

10. Check the application

Open your browser, and type in your browser:

```
http://your_ip_address_server/nagios
```

And there should be a display like the image below:

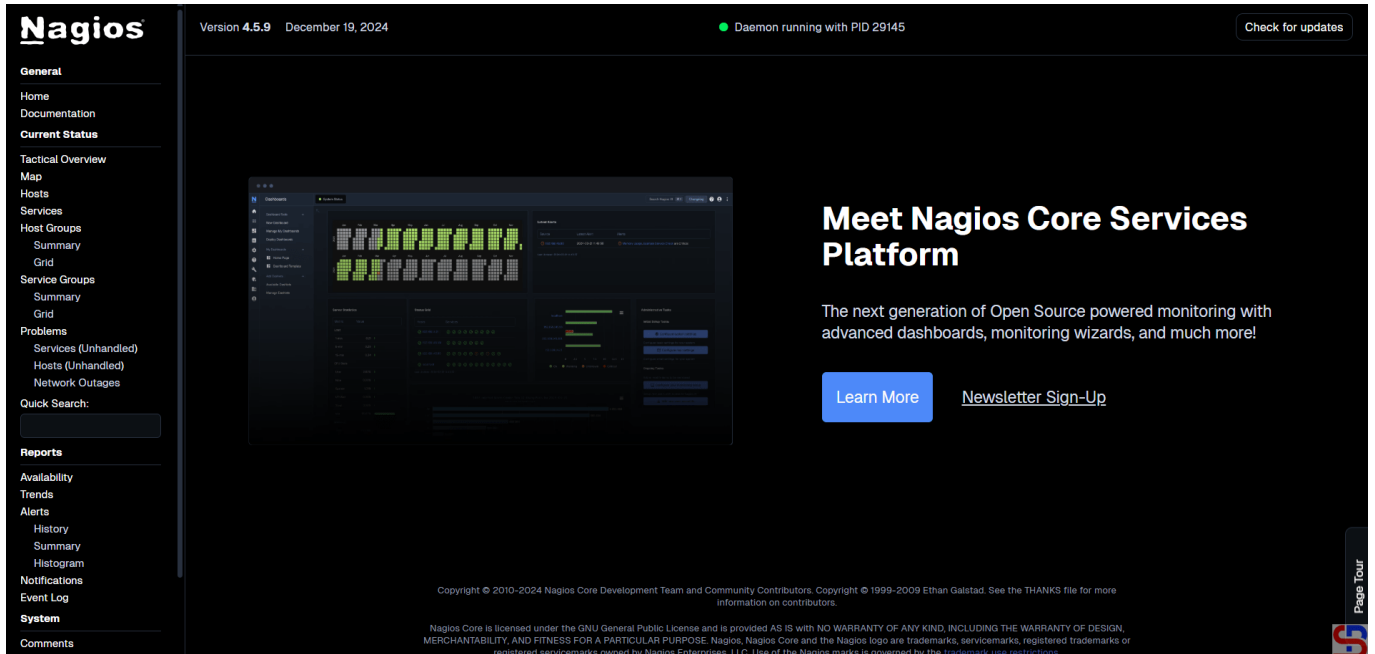


Open Nagios in the browser

If you don't see the image like the above image in your browser, maybe the Firewall/IPTables is still on your server. Run the following commands:

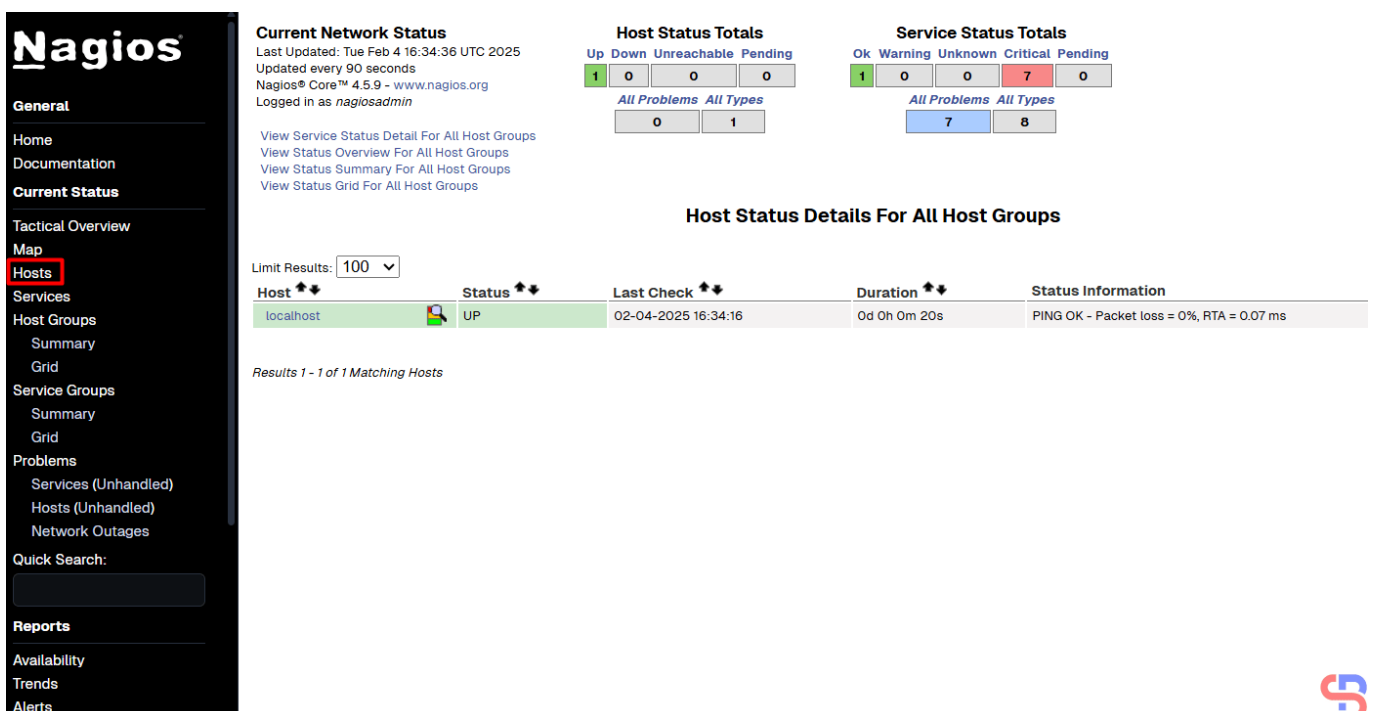
```
sudo ufw allow Apache
sudo ufw reload
```

Back to your browser again, and it should work now. Insert the username (**nagiosadmin**) and the password for Nagios. If the username and the password are right, the Nagios application will appear like this:



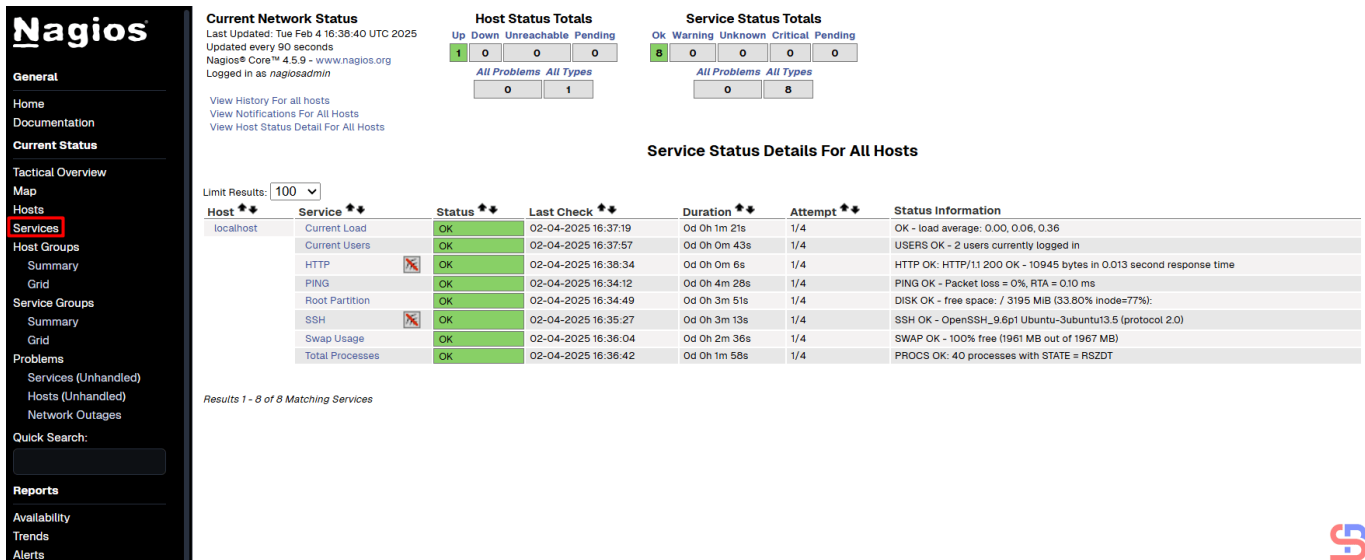
Nagios application

If you want to know which hosts are being monitored by Nagios, click **Hosts**, and Nagios will display the hosts that are being monitored:



Hosts monitored by Nagios

You can see from the picture above, Nagios only monitors the Nagios server or localhost. If you want to know which services are being monitored by Nagios, click **Services** then Nagios will display the services that are being monitored:



The screenshot shows the Nagios web interface. On the left is a navigation menu with 'Services' highlighted. The main content area displays 'Current Network Status', 'Host Status Totals', and 'Service Status Totals'. Below these is a table titled 'Service Status Details For All Hosts' showing 8 services for the localhost host. The services listed are Current Load, Current Users, HTTP, PING, Root Partition, SSH, Swap Usage, and Total Processes. All services are in an 'OK' state. The interface also shows a sidebar with navigation options like Home, Documentation, Tactical Overview, and Reports.

Host	Service	Status	Last Check	Duration	Attempt	Status Information
localhost	Current Load	OK	02-04-2025 16:37:19	0d 0h 1m 21s	1/4	OK - load average: 0.00, 0.06, 0.36
localhost	Current Users	OK	02-04-2025 16:37:57	0d 0h 0m 43s	1/4	USERS OK - 2 users currently logged in
localhost	HTTP	OK	02-04-2025 16:38:34	0d 0h 0m 6s	1/4	HTTP OK: HTTP/1.1 200 OK - 10945 bytes in 0.013 second response time
localhost	PING	OK	02-04-2025 16:34:12	0d 0h 4m 28s	1/4	PING OK - Packet loss = 0%, RTA = 0.10 ms
localhost	Root Partition	OK	02-04-2025 16:34:49	0d 0h 3m 51s	1/4	DISK OK - free space: / 3195 MIB (33.80% inode=77%):
localhost	SSH	OK	02-04-2025 16:35:27	0d 0h 3m 13s	1/4	SSH OK - OpenSSH_9.6p1 Ubuntu-3ubuntu13.5 (protocol 2.0)
localhost	Swap Usage	OK	02-04-2025 16:36:04	0d 0h 2m 36s	1/4	SWAP OK - 100% free (1961 MB out of 1967 MB)
localhost	Total Processes	OK	02-04-2025 16:36:42	0d 0h 1m 58s	1/4	PROCS OK: 40 processes with STATE = RSZDT

Services monitored by Nagios

From the picture above, Nagios monitors 8 services for the Nagios server or localhost.

Note

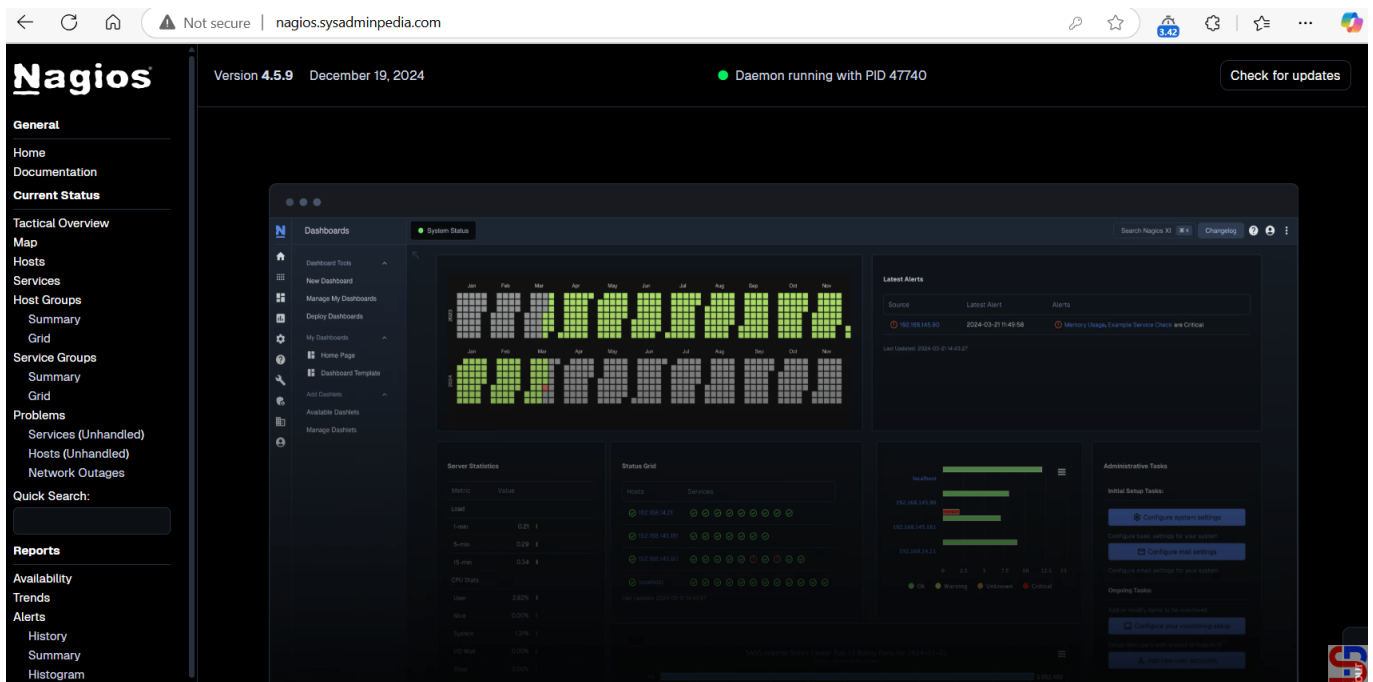
If you have a domain/subdomain and want to use that domain/subdomain for the Nagios application, create a virtual host on your web server. For example, I have the domain sysadminpedia.com and want to use the subdomain nagios.sysadminpedia.com for the Nagios application. So, I created the script below in the file `/etc/apache2/sites-enabled/nagios.sysadminpedia.com.conf`:

```
<VirtualHost *:80>
    ServerName nagios.sysadminpedia.com
    ServerAdmin sysadmin@nagios.sysadminpedia.com
    DocumentRoot /usr/local/nagios/share
    <Directory /usr/local/nagios/share>
        Options -Indexes +FollowSymLinks
```

```
AllowOverride All
</Directory>
```

```
ErrorLog /var/log/apache2/nagios.sysadminpedia.com-error.log
CustomLog /var/log/apache2/nagios.sysadminpedia.com-access.log combined
</VirtualHost>
```

Restart the webserver, open your browser, and type your domain/subdomain for Nagios, and it should be like the image below:



Using a domain/subdomain for the Nagios application

Info

If you installed Nagios in a non-default folder, for example, in the /data folder, you can copy the script above, but you must change the word /usr/local to /data

References

- en.wikipedia.org
- assets.nagios.com
- techoverflow.net

How to Make a Linux User Have the sudo Function?

written by sysadmin | 12 February 2025

SUDO stands for “**SuperUser DO**” and it is a program for Unix-like computer operating systems that enables users to run programs with the security privileges of another user, by default, the superuser. With sudo, a normal user can install or delete an application, change the server network, or even reboot or shut down the server.

Problem

How to make a Linux user have the sudo function?

Solution

This article will explain how to make a Linux user have the sudo function on RockyLinux/AlmaLinux/CentOS, Ubuntu/Debian, and OpenSUSE distros. For example, you want to add the user john to these distros and want that user to be able to use the sudo function. As far as I know, there are two methods to do it:

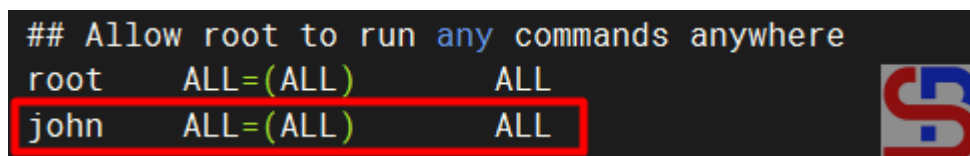
1. Change the sudoers file

Open the /etc/sudoers file or use the command below:

```
visudo
```

Add to the file the user name as in the image below:

```
## Allow root to run any commands anywhere
root    ALL=(ALL)    ALL
john    ALL=(ALL)    ALL
```



Add the user in the sudoers file

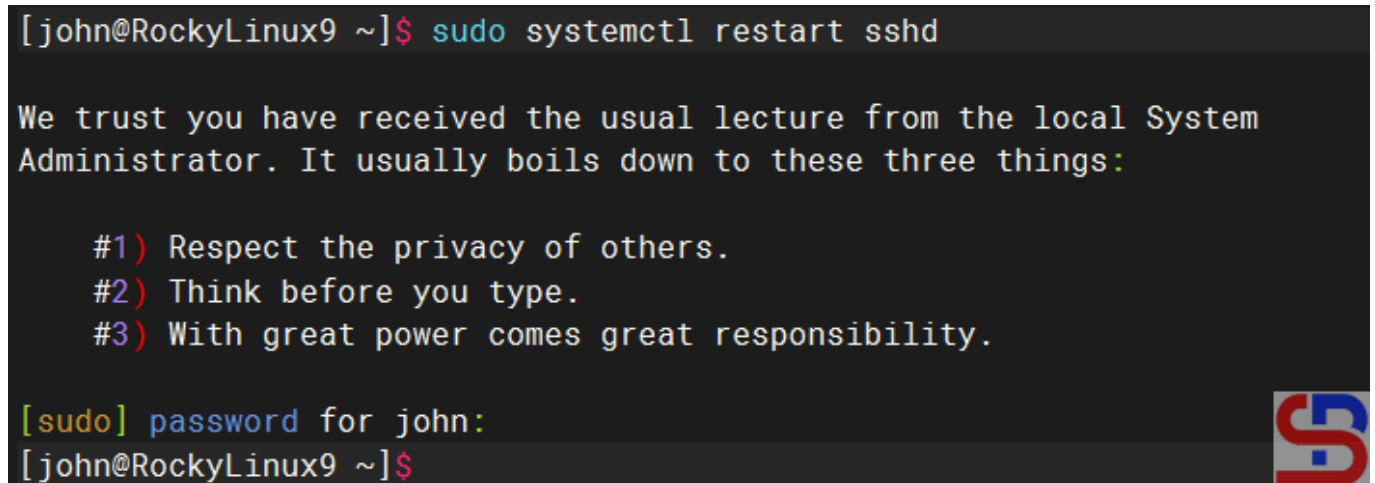
After that, save the file and then try to add a new user using the user john, if there is a display like the image below:

```
[john@RockyLinux9 ~]$ sudo systemctl restart sshd

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for john:
[john@RockyLinux9 ~]$
```



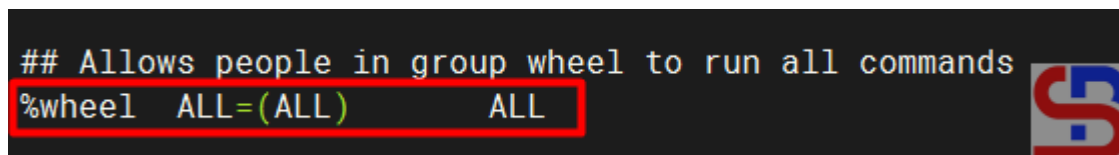
Choose number 1

Then select number **1**, and the user should successfully add a new user as in the image above.

2. Add the user to the sudo group

Add the user to the sudo group, where the name of this sudo group can vary in each distro. To see the name of the sudo group, look in the sudoers file and look for a sentence similar to '**Allows people in group to execute any command**'. For example, in RockyLinux and OpenSUSE, the name of the sudo group is **wheel**, **sudo** in Ubuntu, and don't forget to make sure to uncomment the section as in the image below:

```
## Allows people in group wheel to run all commands
%wheel  ALL=(ALL)  ALL
```



Check the sudo group in the sudoers file

Then type the command below so that a user can use sudo:

RockyLinux & OpenSUSE

```
usermod -aG wheel john
```

```
[root@RockyLinux9 ~]# usermod -aG wheel john
[root@RockyLinux9 ~]#
[root@RockyLinux9 ~]# su - john
Last login: Wed Jan 15 05:51:59 EST 2025 on pts/0
[john@RockyLinux9 ~]$ sudo adduser edward
[sudo] password for john:
[john@RockyLinux9 ~]$
```



Add the user to the sudo group

Ubuntu/Debian

```
usermod -aG sudo john
```

Note

The two methods above can provide the sudo feature to a user on Linux so that the user can run commands that can only be executed by root if the user uses the sudo command by writing down the password. However, if you want the bob user not to have to enter a password when running the sudo command, then in the sudoers file, type the script below:

```
bob                ALL=(ALL)        NOPASSWD: ALL
```

Use the command below if you want the robin user to only be able to perform reboot commands using sudo, but not other commands using sudo:

```
robin              ALL=(ALL)        /usr/sbin/reboot
```

```
[robin@RockyLinux9 ~]$ sudo systemctl restart sshd
[sudo] password for robin:
Sorry, user robin is not allowed to execute '/bin/systemctl restart sshd' as root on RockyLinux9.
[robin@RockyLinux9 ~]$
```



Give the partial sudo function to the user

References

- en.wikipedia.org
- askubuntu.com
- phoenixnap.com

[How to Open and Close a Port in Ubuntu?](#)

written by sysadmin | 12 February 2025

[The previous article](#) explained how to open and close ports in RockyLinux/AlmaLinux/CentOS. This article will explain how to open and close a port in Ubuntu.

Problem

How to open and close a port in Ubuntu?

Solution

A. Check the firewall

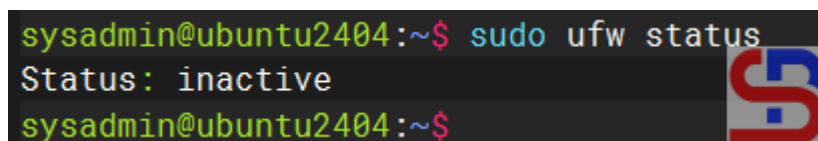
By default, Ubuntu and Debian use the UFW or Uncomplicated Firewall application as the default firewall, and it is installed automatically when you install Ubuntu/Debian. If the firewall is not installed on your Ubuntu/Debian distro, use the command below:

```
sudo apt install ufw
```

To see whether ufw is running or not, use the command below:

```
sudo ufw status
```

```
sysadmin@ubuntu2404:~$ sudo ufw status
Status: inactive
sysadmin@ubuntu2404:~$
```

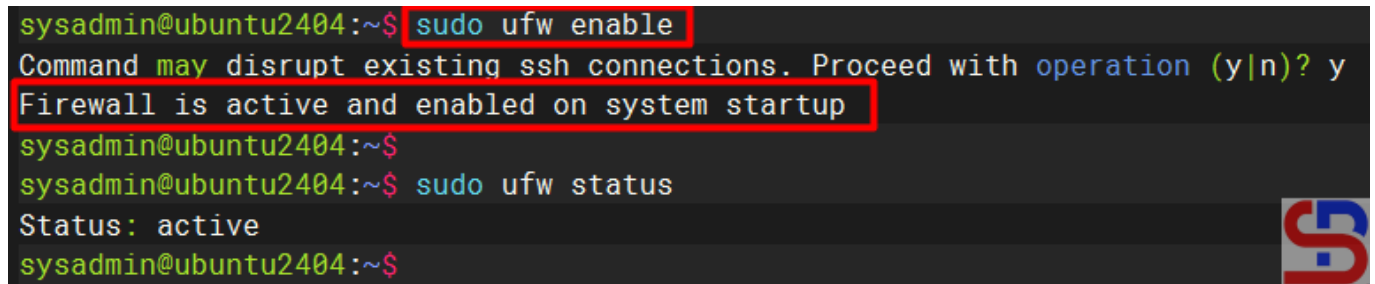
A terminal window screenshot with a dark background. The prompt is 'sysadmin@ubuntu2404:~\$'. The command 'sudo ufw status' is entered. The output is 'Status: inactive'. The prompt is repeated. To the right of the terminal output is a large, stylized 'S' logo in red and blue.

Check status ufw

From the image above, you can see that the application is not yet active. To enable it, type the command below:

```
sudo ufw enable
```

```
sysadmin@ubuntu2404:~$ sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
sysadmin@ubuntu2404:~$
sysadmin@ubuntu2404:~$ sudo ufw status
Status: active
sysadmin@ubuntu2404:~$
```

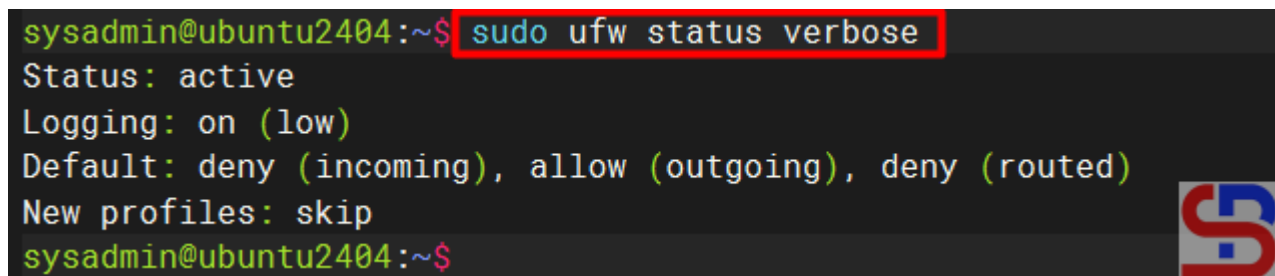


Enable ufw

If you want to see the complete current status of the firewall, use the command below:

```
sudo ufw status verbose
```

```
sysadmin@ubuntu2404:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), deny (routed)
New profiles: skip
sysadmin@ubuntu2404:~$
```

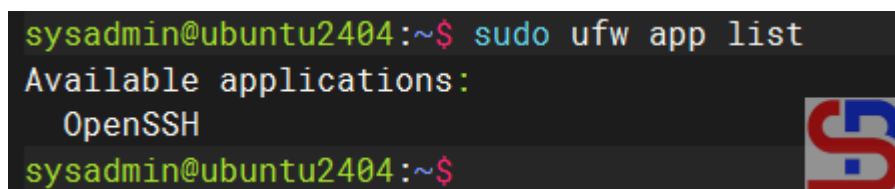


Display the complete current status of the firewall

By default, the firewall only opens the OpenSSH service, which you can view by using the command below:

```
sudo ufw app list
```

```
sysadmin@ubuntu2404:~$ sudo ufw app list
Available applications:
  OpenSSH
sysadmin@ubuntu2404:~$
```



Display the service that is open in the firewall

B. Open the port

To open a port, for example, port 43210, use the command below:

```
sudo ufw allow 43210
```

```
sysadmin@ubuntu2404:~$ sudo ufw allow 43210
Rule added
Rule added (v6)
sysadmin@ubuntu2404:~$
sysadmin@ubuntu2404:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To Action From
--
43210 ALLOW IN Anywhere
43210 (v6) ALLOW IN Anywhere (v6)

sysadmin@ubuntu2404:~$
```

Open the port

WARNING

If you open the port using the command above, it means you will open the port for both TCP and UDP.

To open a port range, for example, from port numbers 45000 to 45010 with the TCP protocol, use the command below:

```
sudo ufw allow 45000:45010/tcp
```

```
sysadmin@ubuntu2404:~$ sudo ufw allow 45000:45010/tcp
Rule added
Rule added (v6)
sysadmin@ubuntu2404:~$
sysadmin@ubuntu2404:~$ sudo ufw status
Status: active

To Action From
--
43210 ALLOW Anywhere
25/tcp ALLOW Anywhere
22 ALLOW 192.168.56.1
45000:45010/tcp ALLOW Anywhere
43210 (v6) ALLOW Anywhere (v6)
25/tcp (v6) ALLOW Anywhere (v6)
45000:45010/tcp (v6) ALLOW Anywhere (v6)

sysadmin@ubuntu2404:~$
```

Open the range ports

C. Open the service

You can see from the image above that port 43210 has been opened on your Ubuntu server. You can also use the service name when opening a port. For example, if you want to open the SMTP service on your Ubuntu server, then use the command below:

```
sudo ufw allow smtp
```

```
sysadmin@ubuntu2404:~$ sudo ufw allow smtp
Rule added
Rule added (v6)
sysadmin@ubuntu2404:~$
sysadmin@ubuntu2404:~$ sudo ufw status
Status: active

To Action From
--
43210 ALLOW Anywhere
25/tcp ALLOW Anywhere
43210 (v6) ALLOW Anywhere (v6)
25/tcp (v6) ALLOW Anywhere (v6)

sysadmin@ubuntu2404:~$
```

Open the SMTP service

D. Open the port from a certain IP

If you want to open a port from a certain IP, for example, you only allow IP 192.168.56.1 to access port 22 on this server, then use the command below:

```
sudo ufw allow from 192.168.56.1 to any port 22
```

```
sysadmin@ubuntu2404:~$ sudo ufw allow from 192.168.56.1 to any port 22
Rule added
sysadmin@ubuntu2404:~$
sysadmin@ubuntu2404:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To Action From
--
43210 ALLOW IN Anywhere
25/tcp ALLOW IN Anywhere
22 ALLOW IN 192.168.56.1
43210 (v6) ALLOW IN Anywhere (v6)
25/tcp (v6) ALLOW IN Anywhere (v6)

sysadmin@ubuntu2404:~$
```

Allow the IP to a certain port

To allow the 192.168.56.0 subnet to the SMTP service, use the command below:

```
sudo ufw allow from 192.168.56.0/24 to any port 25
```

```
sysadmin@ubuntu2404:~$ sudo ufw allow from 192.168.56.0/24 to any port 25
Rule added
sysadmin@ubuntu2404:~$
sysadmin@ubuntu2404:~$ sudo ufw status
Status: active

To Action From
-- --
43210 ALLOW Anywhere
25/tcp ALLOW Anywhere
22 ALLOW 192.168.56.1
45000:45010/tcp ALLOW Anywhere
25 ALLOW 192.168.56.0/24
43210 (v6) ALLOW Anywhere (v6)
25/tcp (v6) ALLOW Anywhere (v6)
45000:45010/tcp (v6) ALLOW Anywhere (v6)

sysadmin@ubuntu2404:~$
```



Allow the subnet to a certain port

E. Close the port

To close port 25, use the command below:

```
sudo ufw deny 25
```

```
sysadmin@ubuntu2404:~$ sudo ufw deny 25
Rule added
Rule added (v6)
sysadmin@ubuntu2404:~$
sysadmin@ubuntu2404:~$ sudo ufw status
Status: active

To Action From
--
43210 ALLOW Anywhere
25/tcp ALLOW Anywhere
22 ALLOW 192.168.56.1
45000:45010/tcp ALLOW Anywhere
25 ALLOW 192.168.56.0/24
25 DENY Anywhere
43210 (v6) ALLOW Anywhere (v6)
25/tcp (v6) ALLOW Anywhere (v6)
45000:45010/tcp (v6) ALLOW Anywhere (v6)
25 (v6) DENY Anywhere (v6)

sysadmin@ubuntu2404:~$
```

Close the port

F. Delete the port

You can also close a port and delete the port that has been opened, for example, port 43210, using the syntax below:

```
sudo ufw delete number
```

```

sysadmin@ubuntu2404:~$ sudo ufw status numbered
Status: active

    To Action From
    --
[ 1] 43210 ALLOW IN Anywhere
[ 2] 25/tcp ALLOW IN Anywhere
[ 3] 22 ALLOW IN 192.168.56.1
[ 4] 45000:45010/tcp ALLOW IN Anywhere
[ 5] 25 ALLOW IN 192.168.56.0/24
[ 6] 25 DENY IN Anywhere
[ 7] 43210 (v6) ALLOW IN Anywhere (v6)
[ 8] 25/tcp (v6) ALLOW IN Anywhere (v6)
[ 9] 45000:45010/tcp (v6) ALLOW IN Anywhere (v6)
[10] 25 (v6) DENY IN Anywhere (v6)

```

```

sysadmin@ubuntu2404:~$ sudo ufw delete 1
Deleting:
  allow 43210
Proceed with operation (y|n)? y
Rule deleted
sysadmin@ubuntu2404:~$

```

Close and delete the port

WARNING

You don't need to run **sudo ufw reload** after each rule change using ufw commands (such as `ufw allow` or `ufw deny`). However, you will need to run **sudo ufw reload** if you are editing the ufw configuration file manually (such as `/etc/ufw/before.rules` or `/etc/ufw/after.rules`), or if you want to make sure all the latest rules and settings are loaded.

Note

You can remove all the rules in ufw by using the command below:

```
sudo ufw reset
```

After that, enable the ufw by using the command below:

```
sudo ufw enable
```



```
sysadmin@Ubuntu2404:~$ sudo ufw reset
Resetting all rules to installed defaults. This may disrupt existing ssh
connections. Proceed with operation (y|n)? y
Backing up 'user.rules' to '/etc/ufw/user.rules.20250515_081802'
Backing up 'before.rules' to '/etc/ufw/before.rules.20250515_081802'
Backing up 'after.rules' to '/etc/ufw/after.rules.20250515_081802'
Backing up 'user6.rules' to '/etc/ufw/user6.rules.20250515_081802'
Backing up 'before6.rules' to '/etc/ufw/before6.rules.20250515_081802'
Backing up 'after6.rules' to '/etc/ufw/after6.rules.20250515_081802'

sysadmin@Ubuntu2404:~$ sudo ufw status
Status: inactive

sysadmin@Ubuntu2404:~$ sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup

sysadmin@Ubuntu2404:~$
```

Reset ufw

By default, if you open a port, it will automatically open in IPv4 and IPv6, and likewise, if you close the port. To see the UFW settings, open the `/etc/default/ufw` file.

```
sysadmin@ubuntu2404:~$ cat /etc/default/ufw
# /etc/default/ufw
#

# Set to yes to apply rules to support IPv6 (no means only IPv6 on loopback
# accepted). You will need to 'disable' and then 'enable' the firewall for
# the changes to take affect.
IPV6=yes

# Set the default input policy to ACCEPT, DROP, or REJECT. Please note that if
# you change this you will most likely want to adjust your rules.
DEFAULT_INPUT_POLICY="DROP"

# Set the default output policy to ACCEPT, DROP, or REJECT. Please note that if
# you change this you will most likely want to adjust your rules.
DEFAULT_OUTPUT_POLICY="ACCEPT"

# Set the default forward policy to ACCEPT, DROP or REJECT. Please note that
# if you change this you will most likely want to adjust your rules
DEFAULT_FORWARD_POLICY="DROP"

# Set the default application policy to ACCEPT, DROP, REJECT or SKIP. Please
# note that setting this to ACCEPT may be a security risk. See 'man ufw' for
# details
DEFAULT_APPLICATION_POLICY="SKIP"
```

Configuration of ufw

References

cyberciti.biz
phoenixnap.com
digitalocean.com
help.ubuntu.com
askubuntu.com

[How to Install gcloud on Ubuntu?](#)

written by sysadmin | 12 February 2025

[The previous article](#) explained how to install gcloud on RockyLinux/AlmaLinux/CentOS. This article will explain how to install gcloud on Ubuntu.

Problem

How to install gcloud on Ubuntu?

Solution

Here are the steps to install gcloud on Ubuntu/Debian:

A. Install gcloud

As far as I know, there are 3 methods to install gcloud on Ubuntu/Debian and the methods recommend using a user other than root.

1. Using the script

Before you download the script, install the packages using the command below:

```
sudo apt update  
sudo apt-get install curl tar
```

Use the below command to download and install the script:

```
curl https://sdk.cloud.google.com | bash
```

Then you will see a display like the one below:

```
sysadmin@ubuntu2404:~$ curl https://sdk.cloud.google.com | bash
% Total % Received % Xferd Average Speed Time Time Time Current
      Dload Upload Total Spent Left Speed
100 443 100 443 0 0 522 0 --:--:-- --:--:-- --:--:-- 522
Downloading Google Cloud SDK install script: https://dl.google.com/dl/cloudsdk/channels/rapid/install_google_cloud_sdk_bash
##### 100.0%
Running install script from: /tmp/tmp.KdzEssdMdb/install_google_cloud_sdk_bash
which curl
curl -# -f https://dl.google.com/dl/cloudsdk/channels/rapid/google-cloud-sdk.tar.gz
##### 100.0%

Installation directory (this will create a google-cloud-sdk subdirectory) (/home/sysadmin):
mkdir -p /home/sysadmin
tar -C /home/sysadmin -zxvf /tmp/tmp.JCXui5IeAi/google-cloud-sdk.tar.gz
google-cloud-sdk/install/download/
google-cloud-sdk/install/core.manifest
google-cloud-sdk/install/core.snapshot.json
google-cloud-sdk/install/gcloud-deps.manifest
google-cloud-sdk/install/gcloud-deps.snapshot.json
```

Install gcloud using the script

Wait until it's finished, and you will see a display like the one below:

```
Modify profile to update your $PATH and enable shell command completion?
Do you want to continue (Y/n)?  Y
The Google Cloud SDK installer will now prompt you to update an rc file to bring the Google Cloud CLIs into your environment.
Enter a path to an rc file to update, or leave blank to use [/home/sysadmin/.bashrc]:
Backing up [/home/sysadmin/.bashrc] to [/home/sysadmin/.bashrc.backup].
[/home/sysadmin/.bashrc] has been updated.
==> Start a new shell for the changes to take effect.

For more information on how to get started, please visit:
https://cloud.google.com/sdk/docs/quickstarts

sysadmin@ubuntu2404:~$
```

Installation complete

From the image above, you are asked to create a new SSH connection so that the effect can be seen, and type the command below:

```
gcloud version
```

However, you can use the command below:

```
source /home/sysadmin/.bashrc
```

So you don't need to create a new SSH connection to run the gcloud version command, which results in the image below:

```
Modify profile to update your $PATH and enable shell command completion?
Do you want to continue (Y/n)? Y
The Google Cloud SDK installer will now prompt you to update an rc file to bring the Google Cloud CLIs into your environment.
Enter a path to an rc file to update, or leave blank to use [/home/sysadmin/.bashrc]:
Backing up [/home/sysadmin/.bashrc] to [/home/sysadmin/.bashrc.backup].
[/home/sysadmin/.bashrc] has been updated.
==> Start a new shell for the changes to take effect.

For more information on how to get started, please visit:
https://cloud.google.com/sdk/docs/quickstarts

sysadmin@ubuntu2404:~$ source /home/sysadmin/.bashrc
sysadmin@ubuntu2404:~$ gcloud version
Google Cloud SDK 504.0.1
bq 2.1.11
bundled-python3-unix 3.11.9
core 2024.12.19
gcloud-crc32c 1.0.0
gsutil 5.33
sysadmin@ubuntu2404:~$
```

Check the result of the installation

2. Using the repository

Type the following commands to install gcloud on the Ubuntu/Debian distro:

```
sudo apt update
echo 'deb [signed-by=/usr/share/keyrings/cloud.google.gpg]
https://packages.cloud.google.com/apt cloud-sdk main' | sudo tee -a
sudo apt-get -y install apt-transport-https ca-certificates gnupg
curl https://packages.cloud.google.com/apt/doc/apt-key.gpg | sudo apt-key --
keyring /usr/share/keyrings/cloud.google.gpg add -
sudo apt update
sudo apt-get install -y google-cloud-sdk
```

3. Using the snap

Run the below command to install gcloud:

```
sudo snap install google-cloud-sdk --classic
```

B. Connect to GCP

After you install gcloud on your server, type the command

below:

gcloud init

Then there will be a display like the image below:

```
sysadmin@ubuntu2404:~$ gcloud init
Welcome! This command will take you through the configuration of gcloud.

Your current configuration has been set to: [default]

You can skip diagnostics next time by using the following flag:
  gcloud init --skip-diagnostics

Network diagnostic detects and fixes local network connection issues.
Checking network connection...done.
Reachability Check passed.
Network diagnostic passed (1/1 checks passed).

You must sign in to continue. Would you like to sign in (Y/n)? Y

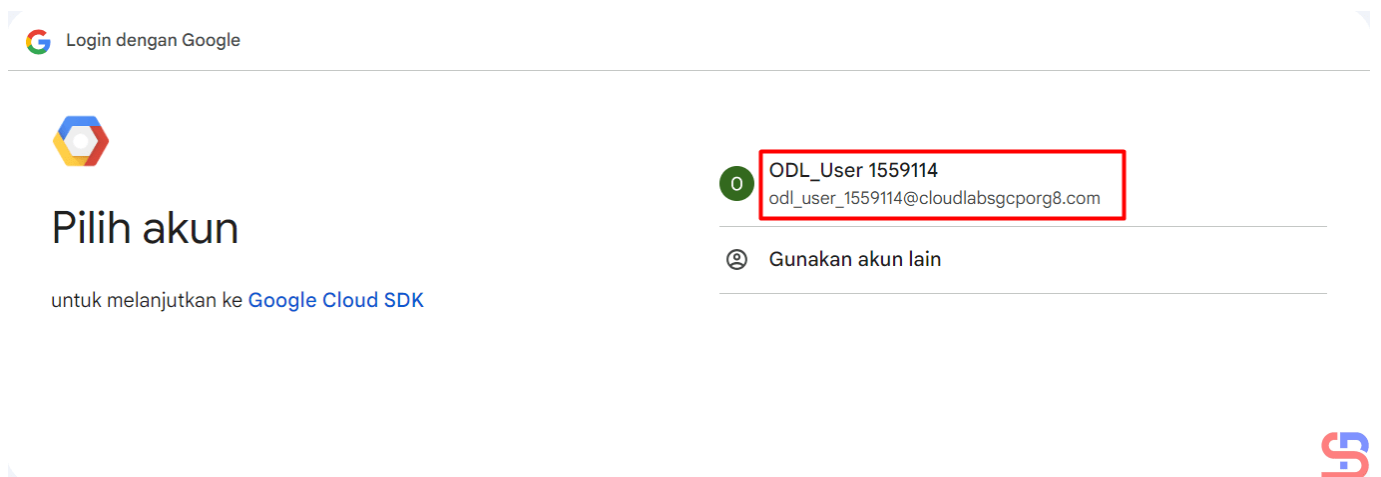
Go to the following link in your browser, and complete the sign-in prompts:

  https://accounts.google.com/o/oauth2/auth?response_type=code&client_id=32555940559.apps.googleusercontent.com&redirect_uri=https%3A%2F%2Fsdk.cloud.google.com%2Fauthcode.html&scope=openid+h
  ttps%3A%2F%2Fwww.googleapis.com%2Fauth%2Fuserinfo.email+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fcloud-platform+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fappengine.admin+https%3A%2F%2Fwww.goo
  gleapis.com%2Fauth%2Fsqlservice.login+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fcompute+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Faccounts.reauth&state=08JBQKFxFCBeS5df0da1xJ40e1Pt7&prompt=co
  nsent&token_usage=remote&access_type=offline&code_challenge=-kFwpqTjuiD-4h6mgUkv8m_dnb9vYU09yFTCN8Y138&code_challenge_method=S256

Once finished, enter the verification code provided in your browser: █
```

Click the link

You can open the link in a browser by clicking the **Ctrl+Click** button located in the red box. If you are having trouble doing so, copy what is included in the red box and paste it into your browser. This will allow you to view a display similar to the one that is shown below:



Click the account

When you click on your Google account, that will allow you to access GCP, and a display similar to the one shown below will appear:



Sign in to Google Cloud SDK

odl_user_1559114@cloudlabsgcporg8.com

By continuing, Google will share your name, email address, language preference, and profile picture with Google Cloud SDK. See Google Cloud SDK's Privacy Policy and Terms of Service.

You can manage Sign in with Google in your [Google Account](#).

Cancel

Continue



Click the Continue button

After you click the **Continue** button, the screen below will show:



Google Cloud SDK wants to access your Google Account

odl_user_1559114@cloudlabsgcporg8.com

This will allow Google Cloud SDK to:

- See, edit, configure, and delete your Google Cloud data and see the email address for your Google Account. ⓘ
- View and sign in to your Google Cloud SQL instances ⓘ
- View and manage your Google Compute Engine resources ⓘ
- View and manage your applications deployed on Google App Engine ⓘ

Make sure you trust Google Cloud SDK

[Learn why you're not seeing links to Google Cloud SDK's Privacy Policy or Terms of Service](#)

Review Google Cloud SDK's Privacy Policy and Terms of Service to understand how Google Cloud SDK will process and protect your data.

To make changes at any time, go to your [Google Account](#).

Learn how Google helps you [share data safely](#).

Cancel

Allow



Click the Allow button

When you click the **Allow** button, the screen below will show:



Sign in to the gcloud CLI

You are seeing this page because you ran the following command in the gcloud CLI from this or another machine. If this is not the case, close this tab.

```
gcloud auth login --no-launch-browser
```

Enter the following verification code in gcloud CLI on the machine you want to log into. This is a credential **similar to your password** and should not be shared with others.

```
4/0AanRRrswAY7X0gBsec0s-DSAx70HXWZEW  
hBaLFucEXKuLBbqEgawA3a2tgSvWtcEBc-g
```

Copy

You can close this tab when you're done.



Click the Copy button

Click the **Copy** button, and paste it into the CLI on your server as in the image below:

```
sysadmin@ubuntu2404:~$ gcloud init
Welcome! This command will take you through the configuration of gcloud.

Your current configuration has been set to: [default]

You can skip diagnostics next time by using the following flag:
  gcloud init --skip-diagnostics

Network diagnostic detects and fixes local network connection issues.
Checking network connection...done.
Reachability Check passed.
Network diagnostic passed (1/1 checks passed).

You must sign in to continue. Would you like to sign in (Y/n)? Y

Go to the following link in your browser, and complete the sign-in prompts:

  https://accounts.google.com/o/oauth2/auth?response_type=code&client_id=32555940559.apps.googleusercontent.com&redirect_uri=https%3A%2F%2Fsdk.cloud.google.com%2Fauthcode.html&scope=openid+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fuserinfo_email+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fcloud-platform+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fappengine.admin+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fsqlservice.login+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fcompute+https%3A%2F%2Fwww.googleapis.com%2Fauth%2Faccounts.reauth&state=08JBQKFxFC8eS5dfda1xJ4oelPt7&prompt=consent&token_usage=remote&access_type=offline&code_challenge=KfwpgTjuiD-4h6mgUkv8m_dnk9yYU0eyFTCN8Yi38&code_challenge_method=S256

Once finished, enter the verification code provided in your browser: 4/0AanRRrswAY7X0gBsec0s-DSAx70HXWZEWhBaLFucEXKuLBBqEgawA3a2tgSVWtcEBc-g
You are signed in as: [odl_user_1559114@cloudlabsgcporg8.com].

Pick cloud project to use:
  [1] clgcporg8-072
  [2] Enter a project ID
  [3] Create a new project
Please enter numeric choice or text value (must exactly match list item):
```

Paste the code

Select the project and configure the zone as in the image above. After that, the gcloud configuration is complete, like in the image below:

```
Created a default .boto configuration file at [/home/sysadmin/.boto]. See this file and
[https://cloud.google.com/storage/docs/gsutil/commands/config] for more
information about configuring Google Cloud Storage.
The Google Cloud CLI is configured and ready to use!

* Commands that require authentication will use odl_user_1559114@cloudlabsgcporg8.com by default
* Commands will reference project `clgcporg8-072` by default
* Compute Engine commands will use region `asia-southeast1` by default
* Compute Engine commands will use zone `asia-southeast1-a` by default

Run `gcloud help config` to learn how to change individual settings

This gcloud configuration is called [default]. You can create additional configurations if you work with multiple accounts and/or projects.
Run `gcloud topic configurations` to learn more.

Some things to try next:

* Run `gcloud --help` to see the Cloud Platform services you can interact with. And run `gcloud help COMMAND` to get help on any gcloud command.
* Run `gcloud topic --help` to learn about advanced features of the CLI like arg files and output formatting
* Run `gcloud cheat-sheet` to see a roster of go-to `gcloud` commands.
sysadmin@ubuntu2404:~$
```

Installation of GCP is complete

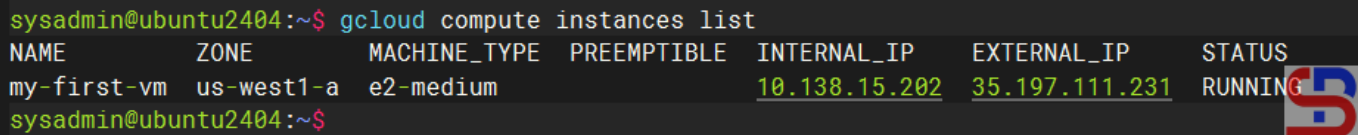
C. Test gcloud

Now, try gcloud to access your GCP. I try to list my virtual machine in GCP using the below command:

```
gcloud compute instances list
```

Then the display below will appear:

```
sysadmin@ubuntu2404:~$ gcloud compute instances list
NAME          ZONE          MACHINE_TYPE  PREEMPTIBLE  INTERNAL_IP  EXTERNAL_IP  STATUS
my-first-vm   us-west1-a    e2-medium     10.138.15.202  35.197.111.231  RUNNING
```



Display virtual machine in GCP using gcloud

If you get a display like the image above, then you have successfully used your GCloud to access your GCP.

Note

If you have many projects on your GCP, you can choose one of these projects as the starting point for your gcloud on GCP. You can switch projects using the command:

```
gcloud config set project PROJECT_ID
```

Change **PROJECT_ID** to the project ID you want to switch to.

References

cloud.google.com

liquidweb.com

bacancytechnology.com

attuneops.io

tecadmin.net