

How to Create a Virtual Machine in GCP?

written by sysadmin | 11 January 2025

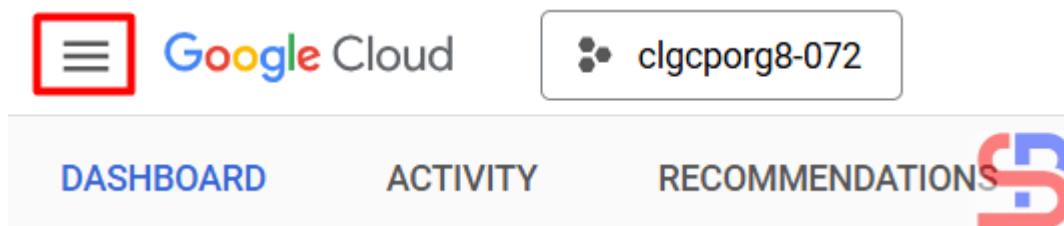
Many people use cloud technology provided by cloud providers such as AWS, GCP, and Azure to support their business operations. One of the features of this technology is the use of a virtual machine, or VM.

Problem

How to create a virtual machine in GCP?

Solution

There are several ways to create a virtual machine or a VM in GCP, but this article will explain how to create a virtual machine in the GCP console. In the GCP Console, at the top left corner, click the Navigation menu, which is symbolized by three lines as in the image below:



Click the icon

Then click **Compute Engine > VM Instances** as in the image below:


The image shows the Google Cloud console navigation menu. On the left, the 'Compute Engine' option is highlighted with a red box. A red arrow points from this box to the 'VM instances' option, which is also highlighted with a red box in the right-hand dropdown menu. Other visible options in the dropdown include 'Instance templates', 'Sole-tenant nodes', 'Machine images', 'TPUs', 'Committed use discounts', 'Reservations', and 'Migrate to Virtual Machines'. Below the dropdown, categories like 'STORAGE' and 'INSTANCE GROUPS' are visible.

Click the VM instance

After that, click the **CREATE INSTANCE** button, then a display will appear as below:

VM instances **CREATE INSTANCE** IMPORT VM REFRESH

INSTANCES OBSERVABILITY INSTANCE SCHEDULES

VM instances 

Click the button

You will see a display like the image below:

- Machine configuration
e2-medium, us-west1-a
- OS and storage
Debian GNU/Linux 12
(bookworm)
- Networking
1 network interface
- Observability
- Security
- Advanced

Machine configuration

Name *

Region * Zone *

Region is permanent Zone is permanent

✓ General purpose

Compute optimized

Memory optimized

Storage optimized

GPUs


Machine types for common workloads, optimized for cost and flexibility

	Series ?	Description	vCPUs ?	Memory ?	Platform
<input type="radio"/>	C4	Consistently high performance	2 - 192	4 - 1,488 GB	Intel Emerald Rapi
<input type="radio"/>	C4A	Arm-based consistently high performance	1 - 72	2 - 576 GB	Google Axion
<input type="radio"/>	N4	Flexible & cost-optimized	2 - 80	4 - 640 GB	Intel Emerald Rapi
<input type="radio"/>	C3	Consistently high performance	4 - 192	8 - 1,536 GB	Intel Sapphire Rapi
<input type="radio"/>	C3D	Consistently high performance	4 - 360	8 - 2,880 GB	AMD Genoa
<input checked="" type="radio"/>	E2	Low cost, day-to-day computing	0.25 - 32	1 - 128 GB	Based on availabili
<input type="radio"/>	N2	Balanced price & performance	2 - 128	2 - 864 GB	Intel Cascade and I
<input type="radio"/>	N2D	Balanced price & performance	2 - 224	2 - 896 GB	AMD EPYC
<input type="radio"/>	T2A	Scale-out workloads	1 - 48	4 - 192 GB	Ampere Altra Arm
<input type="radio"/>	T2D	Scale-out workloads	1 - 60	4 - 240 GB	AMD EPYC Milan
<input type="radio"/>	N1	Balanced price & performance	0.25 - 96	0.6 - 624 GB	Intel Skylake

Machine type
Choose a machine type with preset amounts of vCPUs and memory that suit most workloads. Or, you can create a custom machine for your workload's particular needs. [Learn more](#)

PRESET

CUSTOM


vCPU
1-2 vCPU (1 shared core)

Memory
4 GB

✓ ADVANCED CONFIGURATIONS

Fill in the columns in the machine configuration section

In the **Machine Configuration** section, you have to write the name of the VM, the location of the VM, the CPU, the RAM, and the type of machine that will be used in your VM. I

wrote down my VM requirements as in the picture above. After filling in this section, click the **OS and storage** section. Here you can choose the OS you use and how many hard disk sizes you want in the VM using the **CHANGE** button:

Machine configuration
e2-medium, us-west1-a

OS and storage
Debian GNU/Linux 12 (bookworm)

Networking
1 network interface

Observability

Security

Advanced

Operating system and storage

Name	my-first-vm
Type	New balanced persistent disk
Size	10 GB
Snapshot schedule [?]	No schedule selected
License type [?]	Free
Image	Debian GNU/Linux 12 (bookworm)

CHANGE

Additional storage and VM backups

+ ADD NEW DISK + ATTACH EXISTING DISK + ADD LOCAL SSD

Backup plan ^{PREVIEW}

Secure your backups against deletion through backup vault storage and enable centralized backup management across projects. Managed by Backup and DR Service, a separate service from Compute Engine with independent certifications and accreditation. [Learn more](#)

Backup plan SELECT A PLAN [?]

Container [?]

Deploy a container image to this VM instance

DEPLOY CONTAINER

Fill in the OS and storage section

After that, in the Networking section, you have to fill in the network requirements for the VM. I filled it in as shown in the image below. I don't fill in the **Observability**, **Security**, and **Advanced** sections because I don't need them for my virtual machine.

- Machine configuration
e2-medium, us-west1-a
- OS and storage
Debian GNU/Linux 12
(bookworm)
- Networking**
2 firewall rules, 1 network interface
- Observability
- Security
- Advanced

Networking

Firewall ?

Add tags and firewall rules to allow specific network traffic from the Internet

- Allow HTTP traffic
- Allow HTTPS traffic
- Allow Load Balancer Health Checks

Network tags ?

Hostname ?

Set a custom hostname for this instance or leave it default. Choice is permanent

IP forwarding ?

Enable

Network performance configuration

Network bandwidth ?

Enable per VM Tier_1 networking performance

Maximum outbound network bandwidth: 2Gbps
VM to Public IP: 2Gbps

Network interfaces ?

Network interface is permanent

▼ default default IPv4 (10.138.0.0/20) 🗑️

[ADD A NETWORK INTERFACE](#)

CREATE CANCEL [EQUIVALENT CODE](#)

Fill in the Networking section

After that, I press the **CREATE** button and wait until the virtual machine creation process completes:

VM instances [CREATE INSTANCE](#) [IMPORT VM](#) [REFRESH](#)

[INSTANCES](#) [OBSERVABILITY](#) [INSTANCE SCHEDULES](#)

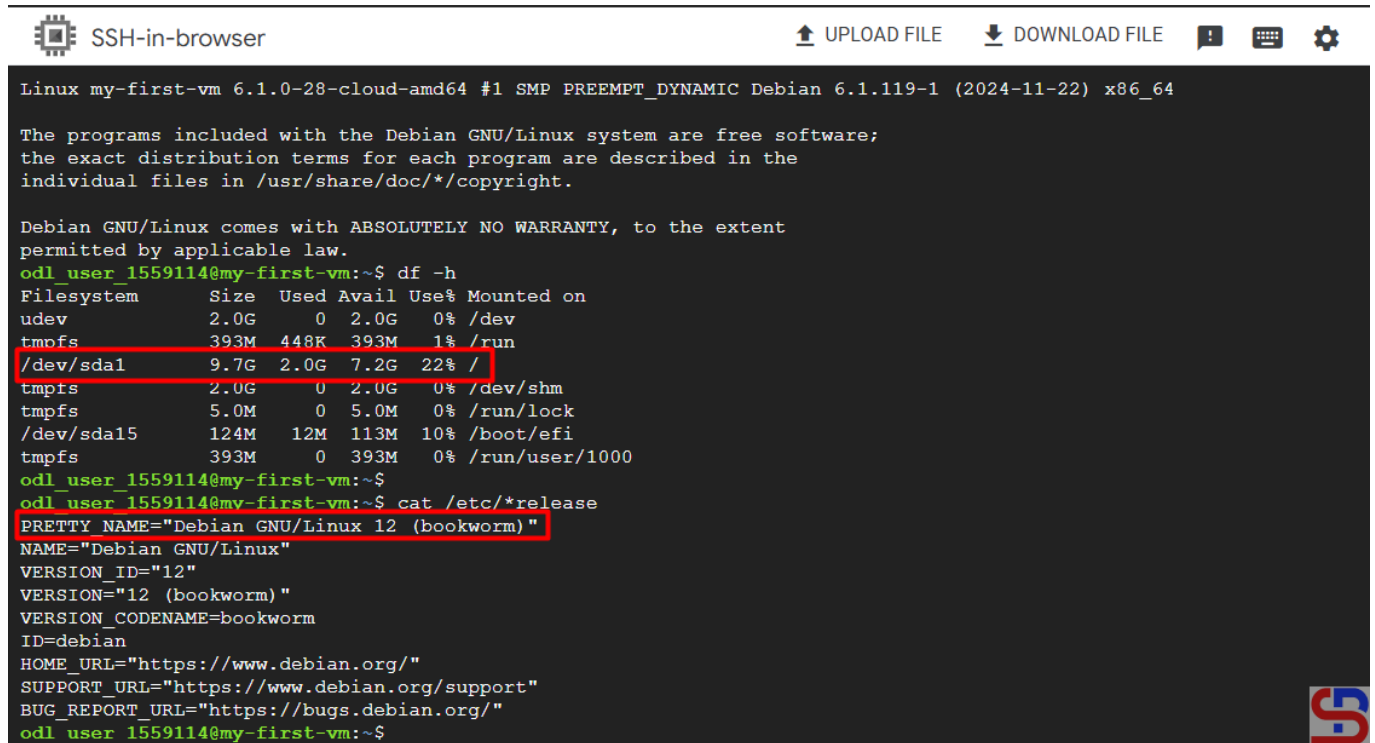
VM instances

☰ Filter Enter property name or value

<input type="checkbox"/> Status	Name ↑	Zone	Recommendations	In use by	Internal IP	External IP	Connect
<input checked="" type="checkbox"/>	my-first-vm	us-west1-a			10.138.15.202 (nic0)	35.197.111.231 (nic0)	SSH ▼

The new VM has been created

If you want to access your VM, then press the **SSH** button, and you can see the OS and HDD size on your VM in the image below:



The screenshot shows an SSH terminal window titled "SSH-in-browser". The terminal output includes the following information:

```
Linux my-first-vm 6.1.0-28-cloud-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.119-1 (2024-11-22) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
odl_user_1559114@my-first-vm:~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            2.0G   0  2.0G   0% /dev
tmpfs           393M  448K  393M   1% /run
/dev/sda1       9.7G  2.0G  7.2G  22% /
tmpfs           2.0G   0  2.0G   0% /dev/shm
tmpfs           5.0M   0  5.0M   0% /run/lock
/dev/sda15      124M  12M  113M  10% /boot/efi
tmpfs           393M   0  393M   0% /run/user/1000
odl_user_1559114@my-first-vm:~$
odl_user_1559114@my-first-vm:~$ cat /etc/*release
PRETTY_NAME="Debian GNU/Linux 12 (bookworm)"
NAME="Debian GNU/Linux"
VERSION_ID="12"
VERSION="12 (bookworm)"
VERSION_CODENAME=bookworm
ID=debian
HOME_URL="https://www.debian.org/"
SUPPORT_URL="https://www.debian.org/support"
BUG_REPORT_URL="https://bugs.debian.org/"
odl_user_1559114@my-first-vm:~$
```

The terminal window also features a top navigation bar with "SSH-in-browser" on the left, and "UPLOAD FILE", "DOWNLOAD FILE", and a settings gear icon on the right. A small "SS" logo is visible in the bottom right corner of the terminal area.

Access to the VM using the SSH button

Note

At first glance, it seems easy to create a virtual machine in GCP. However, if you work in real conditions, there will be many options that must be filled in when creating your virtual machine.

References

- diana-moraa.medium.com
- techrepublic.com

[How to Set Up Passwordless SSH in](#)

Putty?

written by sysadmin | 11 January 2025

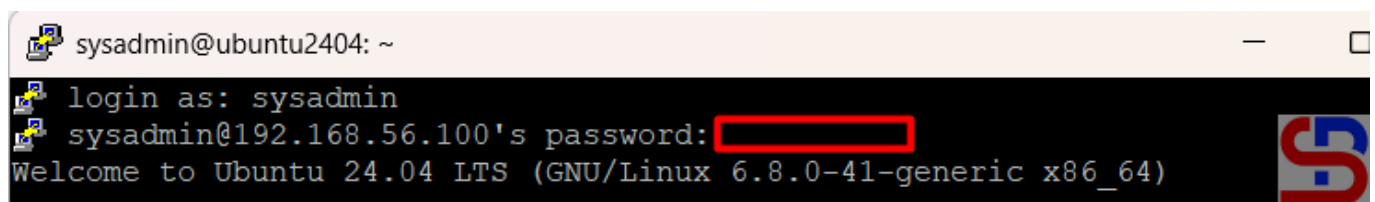
[The previous article](#) explained how to create a passwordless SSH login. However, the article is useful if a sysadmin accesses a Linux server through another Linux server. In general, many sysadmins use PuTTY to access their Linux servers.

Problem

How to set up passwordless SSH in Putty?

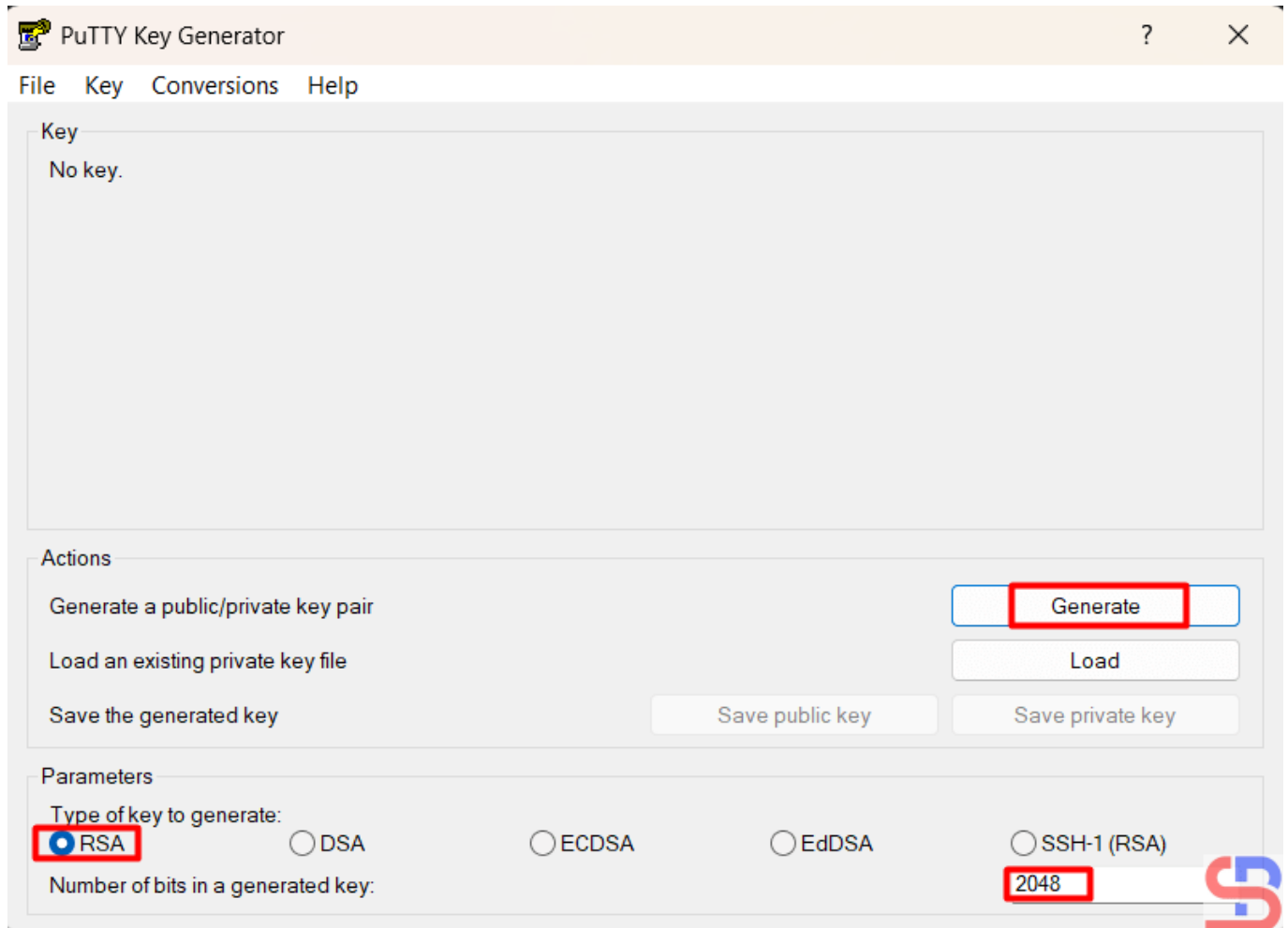
Solution

Putty is a tool created by Simon Tatham to access a device using SSH, Telnet, rlogin, and serial protocols. As of January 2025, the stable version of PuTTY is 0.82. You can visit [this page](#) to see the latest version and download PuTTY. Just like accessing a Linux server via SSH from another server, if you access a Linux server using PuTTY, you will be asked to enter a username and password, as in the image below:



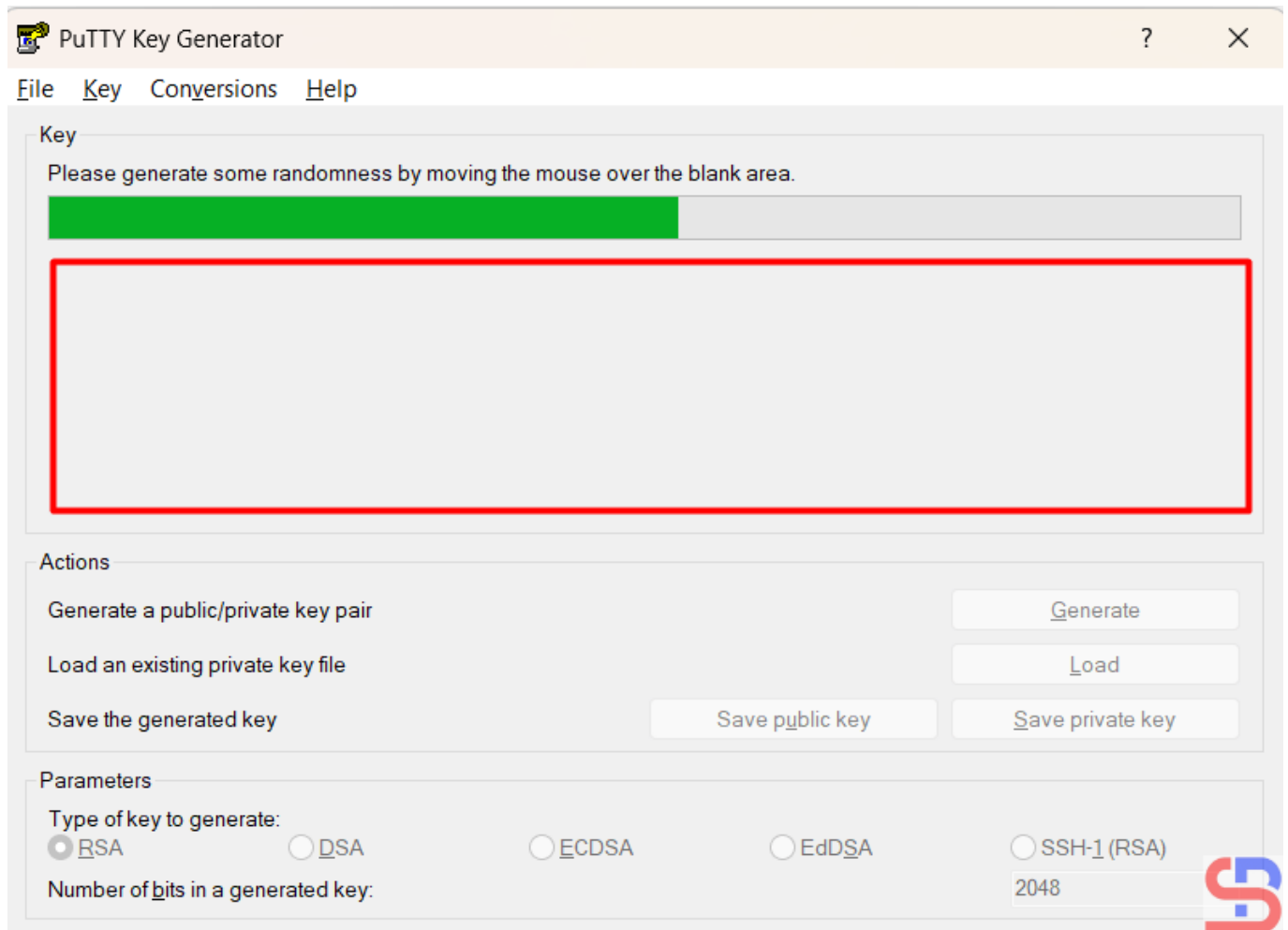
Access to the Linux server using PuTTY

To set up passwordless SSH in Putty, download the Puttygen application [here](#) to create your private/public keypair. After that, run the Puttygen application and you can choose the key according to your wishes, but in this article, we use an RSA key with 2048 bits.



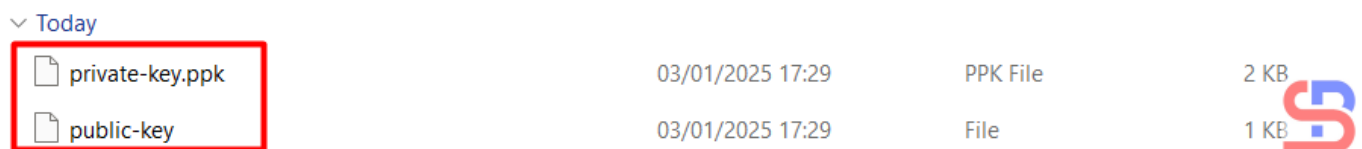
Choose the RSA key and click the Generate button

Press the **Generate** button and move your mouse randomly in the blank area of this application until the key is generated. Please see the image below for more details:



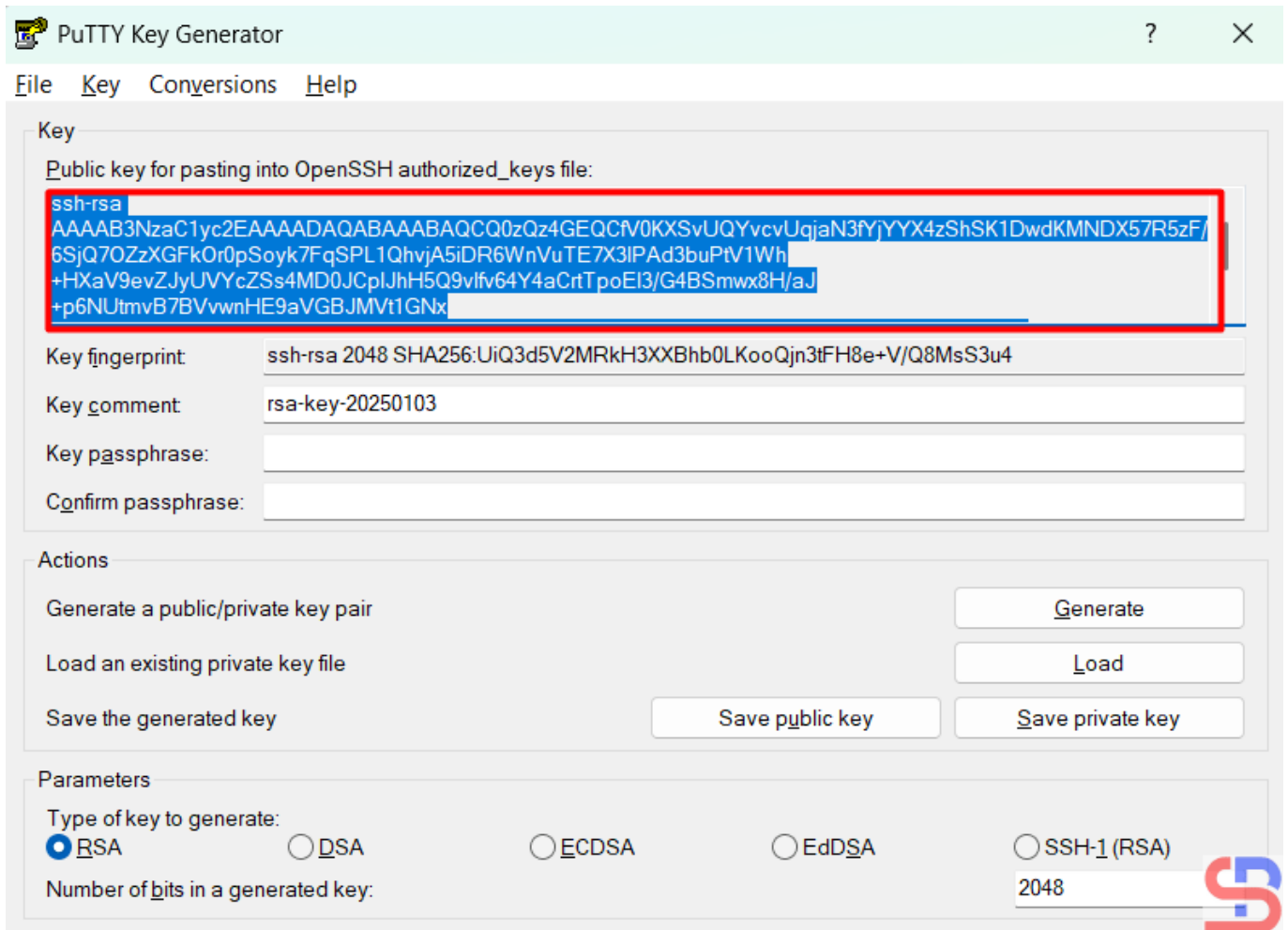
Move your mouse randomly on the blank area

After that, press the save **public key** and **save private key** buttons to save the two keys on your computer. Press the **Yes** button if you are asked a question when you click the Save Private Key button. On your computer, there should be 2 keys as in the image below:



Two key files from puttygen

Then copy the public key by opening the public key file or copying it directly from Puttygen, as in the image below:



Copy the public key

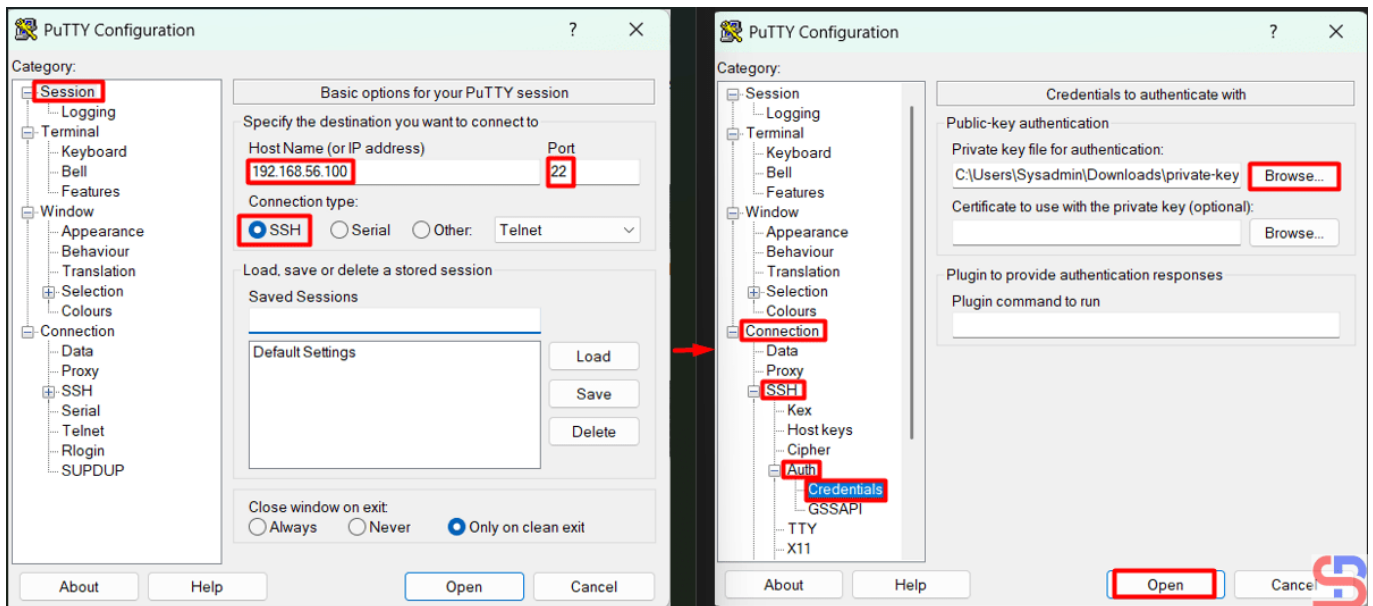
After that, go to the remote server, open the `.ssh/authorized_keys` file, and enter the public key from Puttygen into that file:

```
sysadmin@ubuntu2404:~$ cat .ssh/authorized_keys
sysadmin@ubuntu2404:~$
sysadmin@ubuntu2404:~$ vi .ssh/authorized_keys
sysadmin@ubuntu2404:~$
sysadmin@ubuntu2404:~$ cat .ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQBAQCQ0zQz4GEQCFv0KXsvUQYvcvUqjaN3fYjYYX4zShSK1DwdKMNDX57R5zF/6SjQ7OZzXGFkOr0pSoyk7FqSPL1Qhvja5iDR6WnVuTE7X3lPAd3buPtV1Wh+HXaV9evZJyUVYcZSs4MD0JCplJhH5Q9vlfv64Y4aCrtTpoEI3/G4BSmwx8H/aJ+p6NUtmvB7BVvwnHE9aVGBJMVt1GNx+snUY7SLCsBcdWrtcol6oX9hBRUqj2ARki/sbS7WP4ysSSwC4Gwm08l/XgxtUorbWUsNV52xYTEizZ+i0p54CqrLo/dOOzutAaejFCCF4vHKqzEQ584GMKNS3Z0clsDtk/IH rsa-key-20250103
sysadmin@ubuntu2404:~$
```

Put the public key into the remote server

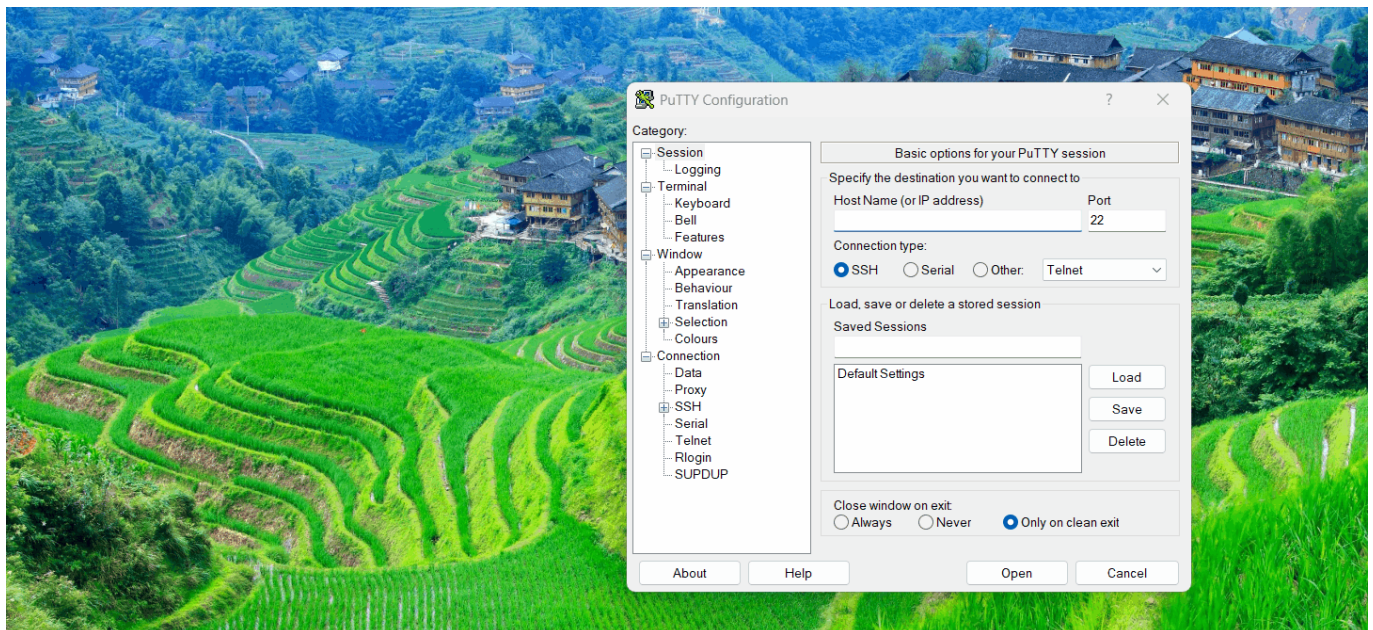
After that, try the remote server to test the SSH Passwordless login. Open Putty, then go to the **Session** and enter the IP of the remote server in the HostName section.

After that, go to the **Connection > Auth > Credentials > Browse** section in the Private key file for the authentication section as in the image below:



Configure PuTTY to access the Linux server without a password

Press the **Enter** or **Open** button, and you should be able to access the server without having to enter a password as in the image below:

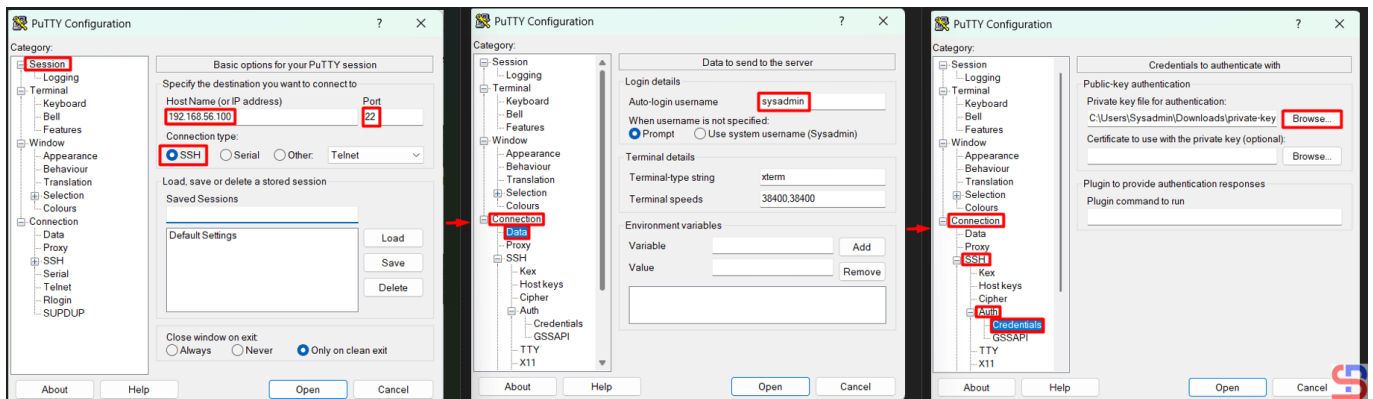


Steps to access the Linux server without a password using PuTTY

Note

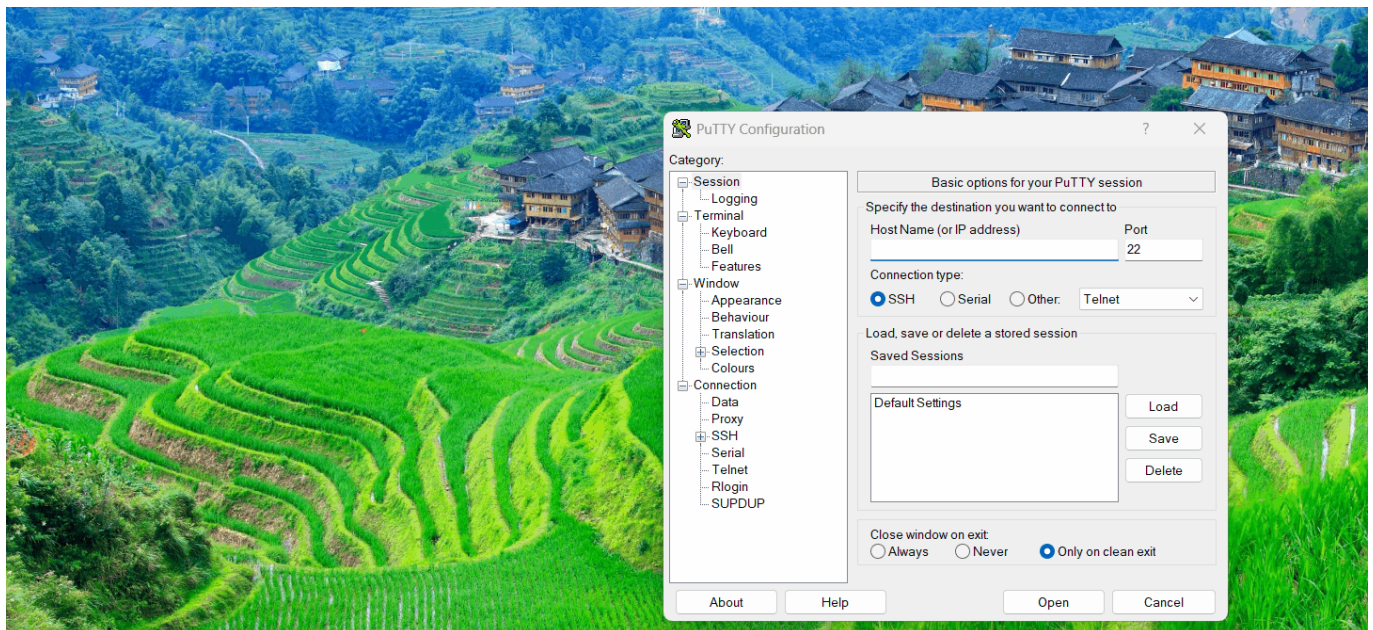
To speed up access to the Linux server, you can also not

write your username to Putty by configuring it in **Connection** > **Data** > Enter your username in the **Auto-login username** column, as in the image below:



Steps to not write your username in Putty

Press the **Enter** or **Open** button, and you should be able to access the server without having to enter the username and password, as in the image below:



Steps to access the Linux server without a username and password using Putty

References

- en.wikipedia.org
- portal.nutanix.com
- help.dreamhost.com
- tecmint.com
- filecloud.com

How to Allow Access to the Linux Server Only Using SSH Key Authentication?

written by sysadmin | 11 January 2025

By default, the Linux server will ask to enter a username and a password if someone accesses the server via SSH. However, [the previous article](#) explained that you can access the Linux server using the passwordless SSH login method. Now I want my Linux servers to only allow access via SSH key authentication or SSH passwordless login.

Problem

How to allow access to the Linux server only using SSH key authentication?

Solution

You can make the security of your Linux server stronger by restricting access to the Linux server using SSH key authentication. It means the remote server can only be accessed for those who already use SSH passwordless login, so that if another user wants to access the server, it will be rejected. To allow access to the Linux server only using SSH key authentication, change the configuration in the `/etc/ssh/sshd_config` file by looking for the line containing **PasswordAuthentication** and setting it to **no**, as in the script below:

```
PasswordAuthentication no
```

After that, restart the SSH service using the command below:

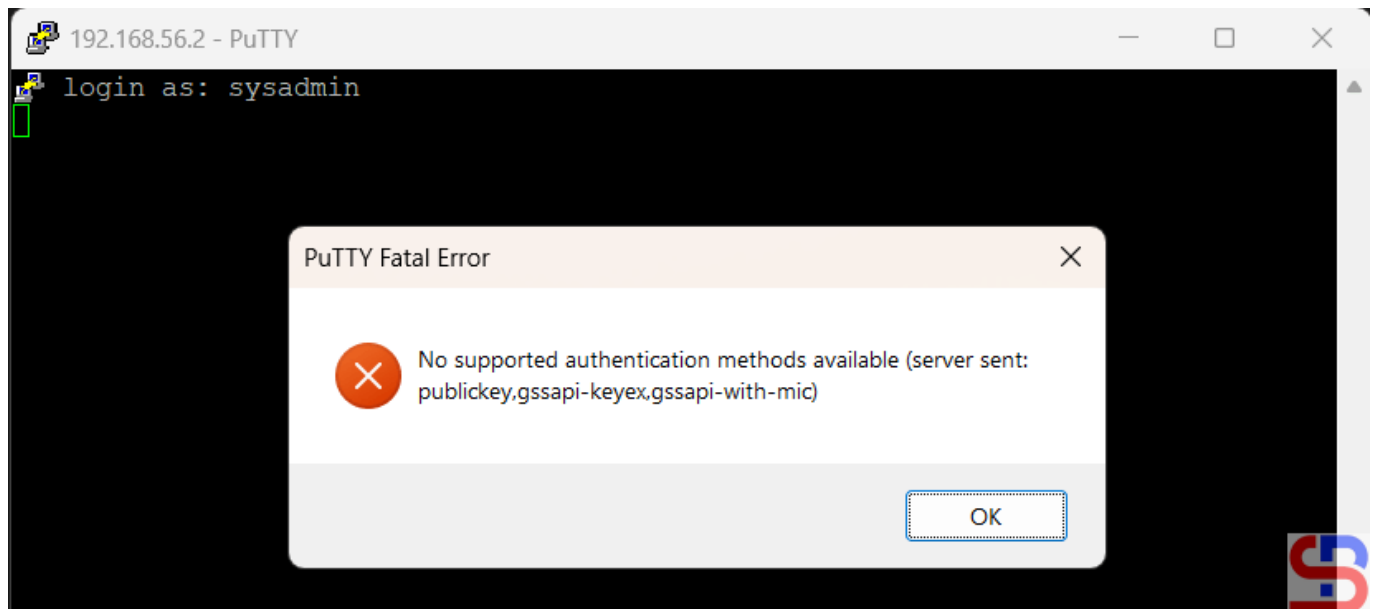
Ubuntu/Debian

```
systemctl restart ssh
```

RockyLinux/AlmaLinux/CentOS

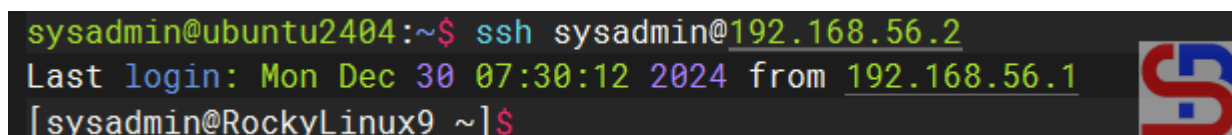
```
systemctl restart sshd
```

You should not be able to access the server when you try to connect to it using SSH. This means your SSH configuration is correct. Below is an example of an error that occurs when accessing via Putty:



Can not access the server from Putty

For example, in the previous article, the sysadmin user on the Ubuntu server could access the RockyLinux server because he had used SSH Passwordless Login as in the image below:



Can access the server from the Ubuntu server

I can not access the RockyLinux server if I access it via the OpenSUSE server, as in the image:

```
sysadmin@opensuse15:~> ssh sysadmin@192.168.56.2
sysadmin@192.168.56.2: Permission denied (publickey,gssapi-keyex,gssapi-with-mic)
sysadmin@opensuse15:~>
```



Can not access the server from the OpenSUSE server

If you want to add another user to be able to access the server, you have to copy the `.ssh/id_rsa.pub` file and put it into the remote server in the `.ssh/authorized_keys` file. You can use the help of a user who can access the server to put the file. Look at the image below, where I have included the `id_rsa.pub` file for the `sysadmin` user on the OpenSUSE server on the RockyLinux server:

```
sysadmin@ubuntu2404:~$ ssh sysadmin@192.168.56.2
Last login: Tue Dec 31 05:37:24 2024 from 192.168.56.100
[sysadmin@RockyLinux9 ~]$
[sysadmin@RockyLinux9 ~]$ cat .ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGDRCk1jeyQovqFYLcascZiz37Cx5qBCSTTYNkfmzcnllmCg7P2DvFri+2uH+1PjP1HNTqFCIVy2HcbLmXn1KAgZBYbhk74euIpsHWD14DB9gWYCzEYDr605FgfweXtpBXeVKcGMqVCK7LkedqGw1Uqx48RU
AIz4WIAxc5m7Zq3ghv7BsIX3fZG311jGSQhEkCq1/n15T/eEH8zXqgtv4ADHGz9M/Yq2JK3qiv15TRMjotDc5zRtiJyHLDjs/yET+UwhbxLLRdNF7m9ygg52scmadMs4R8BBQ8AthKe5agy9NN8SEzS1x8LP5qVHsPGMQXkKJ7XXT46GeAFhjF06e94D
YdvzNJFfh+scXePQFG43CKn+d8vcmQYDJkCALF4r3d7TK42q9z1EIdhyujYZ0VZ53B/pQJFC0p0B1w/UsKtML0MONS541y8Iz9KJLLp9RXD1mEq120E3UHxUNjbdcpvA59PChvFCKG14VUkrdZdMVoTr7bqZeAELPeDtyAs- sysadmin@ubuntu2404
[sysadmin@RockyLinux9 ~]$
[sysadmin@RockyLinux9 ~]$ vi .ssh/authorized_keys
[sysadmin@RockyLinux9 ~]$
[sysadmin@RockyLinux9 ~]$ cat .ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGDRCk1jeyQovqFYLcascZiz37Cx5qBCSTTYNkfmzcnllmCg7P2DvFri+2uH+1PjP1HNTqFCIVy2HcbLmXn1KAgZBYbhk74euIpsHWD14DB9gWYCzEYDr605FgfweXtpBXeVKcGMqVCK7LkedqGw1Uqx48RU
AIz4WIAxc5m7Zq3ghv7BsIX3fZG311jGSQhEkCq1/n15T/eEH8zXqgtv4ADHGz9M/Yq2JK3qiv15TRMjotDc5zRtiJyHLDjs/yET+UwhbxLLRdNF7m9ygg52scmadMs4R8BBQ8AthKe5agy9NN8SEzS1x8LP5qVHsPGMQXkKJ7XXT46GeAFhjF06e94D
YdvzNJFfh+scXePQFG43CKn+d8vcmQYDJkCALF4r3d7TK42q9z1EIdhyujYZ0VZ53B/pQJFC0p0B1w/UsKtML0MONS541y8Iz9KJLLp9RXD1mEq120E3UHxUNjbdcpvA59PChvFCKG14VUkrdZdMVoTr7bqZeAELPeDtyAs- sysadmin@ubuntu2404
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGDRCk1jeyQovqFYLcascZiz37Cx5qBCSTTYNkfmzcnllmCg7P2DvFri+2uH+1PjP1HNTqFCIVy2HcbLmXn1KAgZBYbhk74euIpsHWD14DB9gWYCzEYDr605FgfweXtpBXeVKcGMqVCK7LkedqGw1Uqx48RU
myD0it5Wxy5vQic+e2BJ+beZsn7V/ReGMZadp1vS5h7kv0NFUD9wX8BGCx7ghv31Z1qb281Vyrpiy:3YQx165aEzH1QJSA+KrmFmAsvar+EsVEB86gP36RmUccAyaJPeX1KS4N/3U1HXCxMXZQXEuSceK/vvGs/d055nw1wp5Yvbk5RP4h92jHLBL8Zs
cg93qr2Km1uA71YkFKNJAXP1+FEbZr1WsxhKVRD13C0uzIEanoJmihVH0ic7qoPv32Ijm/gT6CqDizjCjUR4C3WFpSfJ1X8T2io02CR23FK8CoSV/C9LduzXJy1uN2gzUxwFsa+TILtQL0B1Trnf5PtUoqmx58BSsqUm00- sysadmin@opensuse15
[sysadmin@RockyLinux9 ~]$
```

Put the `id_rsa.pub` into the remote server

I tried to connect again to the RockyLinux server using the `sysadmin` user on the OpenSUSE server. I can access the server as shown in the image below:

```
sysadmin@opensuse15:~> ssh sysadmin@192.168.56.2
sysadmin@192.168.56.2: Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
sysadmin@opensuse15:~>
sysadmin@opensuse15:~>
sysadmin@opensuse15:~> ssh sysadmin@192.168.56.2
Last login: Tue Dec 31 05:38:37 2024 from 192.168.56.100
[sysadmin@RockyLinux9 ~]$
```



Can access the server from the OpenSUSE server

Note

Make sure the remote server already contains `authorized_keys` files from other servers so that it doesn't make things difficult for you in the future.

References

strongdm.com
tecmint.com
linuxize.com

[How to Set Up Passwordless SSH Login?](#)

written by sysadmin | 11 January 2025

As a sysadmin, remote to a Linux server is a daily job to perform various checks on a Linux server. By default, if a sysadmin accesses a server, the sysadmin must enter a username and password. However, when the sysadmin has many servers, it is sometimes difficult for the sysadmin to enter the password for each server, especially if each server has a different password. Therefore, it needs to be made so that SSH does not need to enter a password when accessing a Linux server via SSH.

Problem

How to set up passwordless SSH Login?

Solution

There are 3 steps to setting up passwordless SSH:

1. Generate a key pair

Use `ssh-keygen` to generate a key pair consisting of a public key and a private key on the client computer:

```
ssh-keygen -t rsa
```

The `-t rsa` option specifies that the type of the key should be the RSA algorithm. Hit **Enter** to accept the default.

```
sysadmin@ubuntu2404:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/sysadmin/.ssh/id_rsa): Hit the Enter key
Enter passphrase (empty for no passphrase): Hit the Enter key
Enter same passphrase again: Hit the Enter key
Your identification has been saved in /home/sysadmin/.ssh/id_rsa
Your public key has been saved in /home/sysadmin/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:gg7kX2UI7jdc7AuArZ8ATu3zWGQ0N4cP6XIIfHJSmKM sysadmin@ubuntu2404
The key's randomart image is:
+---[RSA 3072]-----+
|
| . =
| + 0 + o
|. X X = S
|.E & X = .
|o.= & 0 .
| =.+.= + .
| +o.oo .
+----[SHA256]-----+
sysadmin@ubuntu2404:~$
```



Running the ssh-keygen command

2. Upload the public key to the remote server

Use **ssh-copy-id** to propagate the public key to the server:

```
ssh-copy-id remote_username@remote_server_ip_address
```

For example, if you want to upload it to the server 192.168.56.2 with the username sysadmin, then use the command below:

```
ssh-copy-id sysadmin@192.168.56.2
```

Type **yes** when prompted and type the password for the remote server.

```
sysadmin@ubuntu2404:~$ ssh-copy-id sysadmin@192.168.56.2
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/sysadmin/.ssh/id_rsa.pub"
The authenticity of host '192.168.56.2 (192.168.56.2)' can't be established.
ED25519 key fingerprint is SHA256:q/E0kK5y9mMkVxtz3FbvMk1MEWmpW6HKZo0+FhBr8AE.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
sysadmin@192.168.56.2's password: type the password

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'sysadmin@192.168.56.2'"
and check to make sure that only the key(s) you wanted were added.

sysadmin@ubuntu2404:~$
```

Running the ssh-copy-id command

For your information, the `id_rsa.pub` file will be saved in the `.ssh/authorized_keys` file on the remote server, like in the image below:

```
[sysadmin@RockyLinux9 ~]$ cat .ssh/authorized_keys
ssh-rsa AAAAAB3NzaC1yc2EAAAADAQABAAQDRKJJeJQovqFYLcascZiz370x5qBCSTTYNkfmzen1mCg7P2DvFr1+2uH+1PJP1HNTqFGIYy2HcL_Mxn1KAqZBvbk74euIpSHND14DB9gWYCzEYDr605FgfwhXtpBxWkGmQVCK7LkedqGw1UQx48RU
ATZ4WIAxc5m7Zq3ghv7BsIX3fjZG311jGS0hEkCq1/nl5T/eEMH8zXqatv4ADHhGz9M/Yq2JK3q1v15tRMUotDc5zRt1jyHLDjs/yET+UwhbxLLRdNF7m9ygg5M2scmadMs4R0BBQ8AthKe5agy9NN8SEzS1x8LPsqVHsPQMqXkNj7XXT46GeAFhjF06e94D
YdvzNJFfh-scXepQF643Ckn-d8vcmQYDJKcALF4r3d71K42q9z1ElDhyujYZ8VZ53B/pqJFC0p081w/UsKtMl0M0NS541y8IZ9KJLLp9RXd1mEq120E3UHxUNjbdcpvA59PchvFCKG14VUkrdZdNVoTr7bqZeAELPeDTyAs- sysadmin@ubuntu2404
[sysadmin@RockyLinux9 ~]$
```

The `authorized_keys` file

3. Test login via SSH

Try to connect to the server using SSH, you should be able to directly access the server without entering the password first. For example, I have 2 Linux servers, each of which uses Ubuntu OS with IP 192.168.56.100 and RockyLinux OS with IP 192.168.56.2. I want to access the RockyLinux server from the Ubuntu server without entering a password. I ran the three steps above to set up passwordless SSH on an Ubuntu server, and the results are as in the image below:

```
sysadmin@ubuntu2404:~$ ssh sysadmin@192.168.56.2
Last login: Mon Dec 30 05:38:18 2024 from 192.168.56.100
[sysadmin@RockyLinux9 ~]$
```

Access the server without entering a username and password

From the image above, you can see that I can directly access the server without entering the server password.

Note

By default, the system will generate a 2048-bit key in the first step when you run the `ssh-keygen` command. However, if you want to be more secure, you can use 4096-bit encryption by using the command below:

```
ssh-keygen -t rsa -b 4096
```

Besides RSA, you can also use several other public key algorithms, such as ECDSA or ED25519. Elliptic Curve Digital Signature Algorithm, or ECDSA, is one of the more complex public key cryptography encryption algorithms that supports three key sizes: 256, 384, and 521 bits. You can use the command below when using ECDSA:

```
ssh-keygen -t ecdsa -b 521
```

Ed25519 is an elliptic curve signing algorithm using EdDSA and Curve25519, and this is a new algorithm added in OpenSSH. You can use the command below when using ed25519:

```
ssh-keygen -t ed25519
```

Unfortunately, support for this among clients is not yet universal. Therefore, its use in general-purpose applications may not be advisable.

References

strongdm.com

phoenixnap.com

ssh.com

encryptionconsulting.com

cryptography.io