

# VIRTUAL PRIVATE CLOUD WITH LINUX:

**Step1:**create vpc

**Step2:**Create Subnet(public& private)

**Step3:**Create Internet Gateway And Attach Vpc

**Step4:**Create Public And Private Route Table

**Step5:** Subnet Association Add

**Step6:** Internet Gateway Add Success For Public and Private Route Table.

**Step7:** Nat Gateway For Only Public Route Table

**Step8:** Create Security Group For Public

Create Security Group---->Security Group Name(Public Security)----  
>Vpc(Select Created Vpc)---->Inbound Rules--->1.SSH---->Source(Anywhere)----  
->2.HTTP----> Source(Anywhere)-----> Create Security Group..

**Create security group** [info](#)

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

**Basic details** [info](#)

Security group name [info](#)  
public security  
Name cannot be edited after creation.

Description [info](#)  
ssh

VPC [info](#)  
vpc-0b3d7529f98a981

**Inbound rules** [info](#)

Protocol	Port range	Source	Description - optional
SSH	TCP	Anywhere-IPv4	0.0.0.0/0
HTTP	TCP	Anywhere-IPv4	0.0.0.0/0

[Add rule](#)

**Outbound rules** [info](#)

Type	Protocol	Port range	Destination	Description - optional
All traffic	All	All	Custom	0.0.0.0/0

[Add rule](#)

**Tags - optional** [info](#)

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

[Add new tag](#)  
You can add up to 50 more tags.

[Cancel](#) [Create security group](#)

Public Security Group Created...

## Step9: Create Security Group For Private

Create Security Group---->Security Group Name(Privatesecurity)----  
>Vpc(Select Created Vpc)---->Inbound Rules--->All Tcp---->Source(Custom)-----  
>Select Public Security Id(Public Security )---->create security group

The screenshot shows the 'Create security group' page in the AWS Management Console. The browser tabs include 'Launch an instance | EC2 Manag...', 'EC2 Management Console', and 'VPC Management Console'. The URL is 'ap-south-1.console.aws.amazon.com/vpc/home?region=ap-south-1#CreateSecurityGroup:'. The page title is 'Create security group'. A description states: 'A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.'

**Basic details**

- Security group name: private
- Description: sgh
- VPC: vpc-0b3d75297f98af981

**Inbound rules**

Type	Protocol	Port range	Source	Description - optional
All TCP	TCP	0 - 65535	Custom sg-0181ee44a24dd09d9	

**Outbound rules**

Type	Protocol	Port range	Destination	Description - optional
All traffic	All	All	Custom 0.0.0.0	

**Tags - optional**

No tags associated with the resource.

Buttons: Cancel, Create security group

## Step10: Public Ec2 LINUX Instance Create:

The screenshot shows the 'Launch instance' page in the AWS Management Console. The page title is 'Launch instance'. The 'Instance type' is 't2.micro'. The 'Key pair (login)' is 'mum1358'. The 'Network settings' section shows 'VPC' as 'vpc-0b3d75297f98af981 (myvpc1)' and 'Subnet' as 'subnet-002986aaa149e7740'. The 'Firewall (security groups)' section shows 'Create security group' as 'public security sg-0e38fca0530b4405e'. The 'Summary' section shows 'Number of instances' as '1', 'Software image (AMI)' as 'Amazon Linux 2 Kernel 5.10 AML...', 'Virtual server type (instance type)' as 't2.micro', 'Firewall (security group)' as 'public security', and 'Storage (volumes)' as '1 volume(s) - 8 GiB'. Buttons: Cancel, Launch instance

## Step11: Private Ec2 LINUX Instance Create:

the instance.

Key pair name - required  
mum1358 [Create new key pair](#)

**Network settings** [Info](#)

VPC - required [Info](#)  
vpc-0b3d75297f98af981 (myvpc1)  
10.0.0.0/16

Subnet [Info](#)  
subnet-03e4fabfac6f2449f private subnet  
VPC: vpc-0b3d75297f98af981 Owner: 795071115491  
Availability Zone: ap-south-1b IP addresses available: 250 CIDR: 10.0.2.0/24 [Create new subnet](#)

Auto-assign public IP [Info](#)  
Disable

Firewall (security groups) [Info](#)  
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.  
☐ Create security group ☒ Select existing security group

Common security groups [Info](#)  
Select security groups  
private security sg-029235d931bafbd1f1 [Compare security group rules](#)  
VPC: vpc-0b3d75297f98af981  
Security groups that you add or remove here will be added to or removed from all your network interfaces.

[Advanced network configuration](#)

**Configure storage** [Info](#) [Advanced](#)

1x 8 GiB gp2 Root volume (Not encrypted)

[Free tier eligible customers can get up to 30 GB of EBS General Purpose \(SSD\) or Magnetic storage](#)

Cancel [Launch instance](#)

Software Image (AMI)  
Amazon Linux 2 Kernel 5.10 AMI...[read more](#)  
ami-0cca134ec43cf708f

Virtual server type (instance type)  
t2.micro

Firewall (security group)  
private security

Storage (volumes)  
1 volume(s) - 8 GiB

## Step12: instance created

Instances (1/3) <a href="#">Info</a>													
Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4	Elastic IP	IPv6 IP	Monitoring	Security group name	Key name
public	i-008kz410f66173c	Running	t2.micro	2/2 checks passed	No alarms	ap-south-1a		45.205.216.147			disabled	public security	mum2212
private	i-002f5241e7716d3e	Terminated	t2.micro		No alarms	ap-south-1b					disabled		mum2214
private	i-0e2a152c496585305	Running	t2.micro	2/2 checks passed	No alarms	ap-south-1b					disabled	private security group	mum2215

**Instance: i-0e2a152c496585305 (private)**

[Details](#) [Security](#) [Networking](#) [Storage](#) [Status checks](#) [Monitoring](#) [Tags](#)

**Instance summary** [Info](#)

Instance ID i-0e2a152c496585305 (private)	Public IPv4 address -	Private IPv4 address copied
IPv6 address -	Instance state Running	10.0.2.89
Hostname type IP name: ip-10-0-2-89-ap-south-1-compute.internal	Private IP DNS name (IPv4 only) ip-10-0-2-89-ap-south-1-compute.internal	Public IPv4 DNS -
Answer private resource DNS name IPV4 (A)	Instance type t2.micro	Elastic IP addresses -
Auto-assigned IP address -	VPC ID vpc-0a5484768caaff44 (myvpc)	AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations. <a href="#">Learn more</a>
IAM Role -	Subnet ID subnet-0d8f739c510c246d1 (private subnet)	Auto Scaling Group name -

**Instance details** [Info](#)

Platform Amazon Linux (infused)	AMI ID ami-0cca134ec43cf708f	Monitoring disabled
Platform details Linux/UNIX	AMI name amazon2-ami-kernel-5.10-hvm-2.0.20221210.1-486_64-gp2	Termination protection Disabled
Stop protection Disabled	Launch time Fri Dec 30 2022 22:54:17 GMT+05:30 (India Standard Time) (17 minutes)	AMI location amazon/amazon2-ami-kernel-5.10-hvm-2.0.20221210.1-486_64-gp2
Instance auto-recovery Default	Lifecycle normal	Stop-Hibernate behavior disabled

**Step12:**Putty Open--->put public instance puic ip---->Login ec2-user--->change root user(sudo -i)

**Step13:**Login Private Instance

⇒ Ssh [ec2-user@10.0.2.10\(private ip\)](#)

⇒ Vi demo1.pem----->(upload key file)

```
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAmHV7oI/q4xoM3VyXsb9/o6gs9Jf5nLpw+yc1FJIXpTN/Wv86
rYnypq8R1cnFqWgpiyf0x1PlVNTlTLNRNy9g3UWaL4h4g2nd3Z0cFMvckylDfLDg
EBHDDFCrrKA5DgPo/kU6kzLNlaB/RAZ4JRjtFwLEBZg2g+nsJvqE1FF8AMlR8EVC
EU3GyRddqN+boQ84rZlognhEm+uqRj4/DFb6GgkS8gdUDYMCiVmlCjtE9ybQM5Fw
jCci01RDBO6d6MDHSimysG3h4naZr1D4EUCA4U9ByUMc4esZ2oOGFa9wWPNV4gD
irgYJeeWfPYTR2nR9eOwM5KneGSY1D49k5HJDQIDAQABAoIBAA/0w8KTLWclU9Fb
Im5Wf3pWYJYczcAMd0Sh3t1PTPA6SorwiWgzCtVNH08I9gn7Ma5huSmfazINYDW9
OrMu3zlpTnDJHKvMSa8nAUhf6a7xM6H6NQkZgstoKf+AKViR6RGrlyzOtVuCl687
Shkf2bh+fMMFIj2tMxfjcVW3d6Lca32phJbJwCvtd+24AMNUZ2VNkvmHw0w+sLi
acdWGidV7tIrvDyBD9jesJzz3vdsKxPJJ+oJ9IurAJuv+JHIY/pVIdqKXlhwc7w
cMqXiJuO8XC5fRmZdoeX9g//FmOHBt6W9HyIRSPHN304hUBwUNDv/77KarNQyzWw
+QYYR9UCgYEA4nzi7/dsp/mqRAjkkzd72Qt5lho12+JJvIYZ+fsky+EoXebVrM/G
3mLVpIIY/GMRD2bkr3eqT9LtdAWSjNdd46Yva9Qcoog9hg5+6JoQ8Xp+OLjl0eCK
a+62jg0VXue+F0saG/jmPIRCy9a8AhHm9l+u0QE6US/M3pf3UDoTEncCgYEAfMp
cMEplq7tqF7S2JEWsGEmHj8r5LOCp1oi9RfE9FrWsuAHDWLJ3YBcJ2vespPitlf
iClYcY9yH/VzaBVU3o5hZUE0UdG8YkdticKmWGXjZTULQcfI9M/HGgmuFbrIf5
/gJjpbQ1TRK6S2sfAjTy+IwG1yzJy69DWtDq/ZsCgYAGsMndbPu4upddCyY1cx4l
b0FMPdmAdV7YQt3hlJmXrcUVIqY03lRyNjK7EtzKF+MZIWD8+3v8f66kDsYVgwcZ
AmXE0a/e3Udz/1mhZWu6tnOkGVIwsQFlztDlus020IG9DmrnCKNEhmOywdUr+nto
K8tuQSsH2vGiYbrck9qcYQKBgFC5NDRph/3aO+IfaU2hyashFqYzmgosPQv9Fd0S
EWUGGIT6hNM0b15Y3RvQAh/XHXMJuMKL500C/HYrzA/jB5VvL/rvb66L0nLsQrCZ
j64cmSHI2QZ5GM8QodOvtrhW0Qb105HxxJSNneVY3IMWclQpUzg0oA+0H2OW2kp0
l1/5AoGAR/2NmuvauBAnGaJ5M1C+YuBxC+/QMAqOQqaEEnyawG881XxpNXTsYQRL
aa/7SRR73EsNefka1bLHTMJG+CeKglKUooOpBYH+KdHFU9DQr+Va4qsaG2lMQrDE
K4VUJCacyf0glBVTIo9HdZOMBIAvg5roDatC1Cyw0gWx699FdE=
-----END RSA PRIVATE KEY-----
```

⇒ chmod 400 demo1.pem (permission change)

⇒ Ssh -i demo1.pem [ec2-user@10.0.2.10\(private ip\)](#)---->login

```
ec2-user@ip-10-0-2-10:~
[root@ip-10-0-1-184 ~]# pinggoogle.com
-bash: pinggoogle.com: command not found
[root@ip-10-0-1-184 ~]# ping google.com
PING google.com (142.251.42.78) 56(84) bytes of data.
64 bytes from bom12s21-in-f14.1e100.net (142.251.42.78): icmp_seq=1 ttl=110 time
=1.33 ms
64 bytes from bom12s21-in-f14.1e100.net (142.251.42.78): icmp_seq=2 ttl=110 time
=1.39 ms
64 bytes from bom12s21-in-f14.1e100.net (142.251.42.78): icmp_seq=3 ttl=110 time
=1.37 ms
64 bytes from bom12s21-in-f14.1e100.net (142.251.42.78): icmp_seq=4 ttl=110 time
=1.41 ms
^C
--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 1.339/1.379/1.412/0.046 ms
[root@ip-10-0-1-184 ~]# ssh ec2-user@10.0.2.10
The authenticity of host '10.0.2.10 (10.0.2.10)' can't be established.
ECDSA key fingerprint is SHA256:vwOaQ2mDosOmEFj8ac7SktZdAN3RDjJtL2pwih7CVwg.
ECDSA key fingerprint is MD5:02:cb:46:13:38:e7:4a:18:37:7b:87:96:b0:65:a0:37.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.2.10' (ECDSA) to the list of known hosts.
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
[root@ip-10-0-1-184 ~]# vi demo1.pem
[root@ip-10-0-1-184 ~]# chmod 400 demo1.pem
[root@ip-10-0-1-184 ~]# ssh -i demo1.pem ec2-user@10.0.2.10

 _ _ | _ _ | _ _ |
 _ _ | ( _ _ | _ _ |
 _ _ | \ _ _ | _ _ |

Amazon Linux 2 AMI

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-2-10 ~]$
```

**Private instance login suuefully..**



