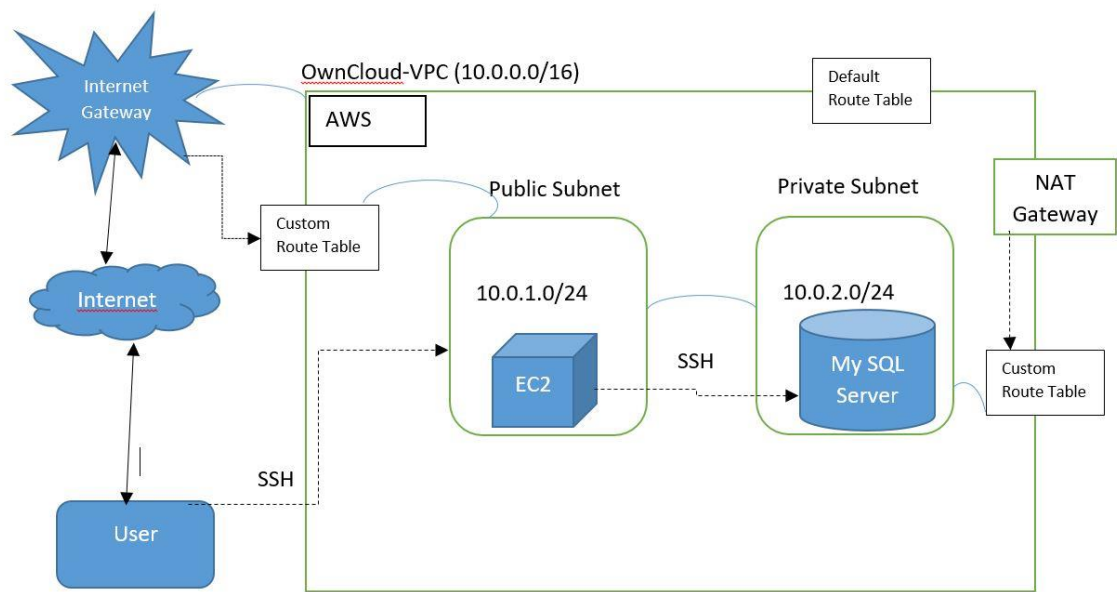


Own Cloud VPC Architecture



1. Creating a Custom VPC from Services with CIDR block 10.0.0.0/16

Create VPC

A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances. You must specify an IPv4 address range for your VPC. Specify the IPv4 address range as a Classless Inter-Domain Routing (CIDR) block; for example, 10.0.0.0/16. You cannot specify an IPv4 CIDR block larger than /16. You can optionally associate an Amazon-provided IPv6 CIDR block with the VPC.

Name tag Owncloud-VPC ⓘ

IPv4 CIDR block* 10.0.0.0/16 ⓘ

IPv6 CIDR block
☒ No IPv6 CIDR Block ⓘ
☐ Amazon provided IPv6 CIDR block

Tenancy Default ⓘ

* Required

Cancel Create

VPCs

Create VPC Actions

Filter by tags and attributes or search by keyword

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP options set	Main Route table	Main Network ACL
Owncloud-VPC	vpc-028af629a6603a9b0	available	10.0.0.0/16	-	dopt-ffafa684	rtb-00a09e07a99d965de	acl-0edf9676eca
vpc-b1deb2cb	vpc-b1deb2cb	available	172.31.0.0/20	-	dopt-ffafa684	rtb-0bf81275	acl-c68452bb

2. Create Public Subnet under Subnet tab with CIDR block 10.0.10.0/24

Create subnet

Specify your subnet's IP address block in CIDR format; for example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and /28 netmask, and can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag Public-subnet ⓘ

VPC* vpc-028af629a6603a9b0 ⓘ

VPC CIDRs

CIDR	Status	Status Reason
10.0.0.0/16	associated	

Availability Zone us-east-1a ⓘ

IPv4 CIDR block* 10.0.10.0/24 ⓘ

* Required

Cancel Create

Subnets

Create subnet Actions

Filter by tags and attributes or search by keyword

Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR	Availability Zone
Public-subnet	subnet-0e0604f8f6eef5ce	available	vpc-028af629a6603a9b0	10.0.10.0/24	251	-	us-east-1a
default-vpc-1c	subnet-17b9e739	available	vpc-b1deb2cb	172.31.80.0/20	4091	-	us-east-1c
default-vpc-1f	subnet-4335204c	available	vpc-b1deb2cb	172.31.64.0/20	4091	-	us-east-1f
default-vpc-1a	subnet-6683df3a	available	vpc-b1deb2cb	172.31.32.0/20	4091	-	us-east-1a
default-vpc-1b	subnet-b44615d3	available	vpc-b1deb2cb	172.31.0.0/20	4091	-	us-east-1b
default-vpc-1e	subnet-db96f1e5	available	vpc-b1deb2cb	172.31.48.0/20	4091	-	us-east-1e
default-vpc-1d	subnet-f804e7b5	available	vpc-b1deb2cb	172.31.16.0/20	4091	-	us-east-1d

3. Create Private Subnet with CIDR block 10.0.2.0/24

Subnets > Create subnet

Create subnet

Specify your subnet's IP address block in CIDR format; for example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and /28 netmask, and can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag:

VPC*:

VPC CIDRs	CIDR	Status	Status Reason
	10.0.0.0/16	associated	

Availability Zone:

IPv4 CIDR block*:

* Required

[Cancel](#) [Create](#)

Services > **Resource Groups**

Create subnet **Actions**

Filter by tags and attributes or search by keyword

Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6	Availability Zone	Availability Zone ID
Public-subnet	subnet-0e0604f8fc6eef6ce	available	vpc-028af629a6603a9b0 [...]	10.0.1.0/24	251	-	us-east-1a	use1-az6
Private-Subnet	subnet-0edb0eeb79bf964c3	available	vpc-028af629a6603a9b0 [...]	10.0.2.0/24	251	-	us-east-1b	use1-az1
default-vpc-1c	subnet-17b9e739	available	vpc-b1deb2cb	172.31.80.0/20	4091	-	us-east-1c	use1-az2
default-vpc-1f	subnet-4335204c	available	vpc-b1deb2cb	172.31.64.0/20	4091	-	us-east-1f	use1-az5
default-vpc-1a	subnet-6683df3a	available	vpc-b1deb2cb	172.31.32.0/20	4091	-	us-east-1a	use1-az6
default-vpc-1b	subnet-b44615d3	available	vpc-b1deb2cb	172.31.0.0/20	4091	-	us-east-1b	use1-az1
default-vpc-1e	subnet-db96f1e5	available	vpc-b1deb2cb	172.31.48.0/20	4091	-	us-east-1e	use1-az3
default-vpc-1d	subnet-f804e7b5	available	vpc-b1deb2cb	172.31.16.0/20	4091	-	us-east-1d	use1-az4

Subnets: subnet-0e0604f8fc6eef6ce, subnet-0edb0eeb79bf964c3

4. Making Public –subnet expose to public by creating an Internet gateway

aws **Services** > **Resource Groups**

Internet gateways > Create internet gateway

Create internet gateway

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Name tag:

* Required

[Cancel](#) [Create](#)

5. Attach Oc-igw internet gateway to Custom VPC(Owncloud-VPC)

aws **Services** > **Resource Groups**

Internet gateways > Attach to VPC

Attach to VPC

Attach an internet gateway to a VPC to enable communication with the internet. Specify the VPC you would like to attach below.

VPC*:

AWS Command Line Interface command

* Required

[Cancel](#) [Attach](#)

Services Resource Groups

Create internet gateway Actions

Filter by tags and attributes or search by keyword

Name	ID	State	VPC	Owner
Oc-igw	igw-0d7a1f50f454...	attached	vpc-028af629a66...	985220814883
	igw-f693418d	attached	vpc-b1deb2cb	985220814883

6. Create route table for custom VPC

aws Services Resource Groups

Route Tables > Create route table

Create route table

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Name tag public-rt

VPC* vpc-028af629a6603a9b0

* Required

Cancel Create

7. Edit the Routes under Route tab

aws Services Resource Groups

Route Tables > Edit routes

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
0.0.0.0/0	igw-0d7a1f50f454e6bb0		No

Add route

* Required

Cancel Save routes

Services Resource Groups

Create route table Actions

Filter by tags and attributes or search by keyword

Name	Route Table ID	Explicit subnet association	Main	VPC ID	Owner
	rtb-00a09e07a99d965de	-	Yes	vpc-028af629a6603a9b0 [...]	985220814883
public-rt	rtb-0730985f8e2bd15cd	-	No	vpc-028af629a6603a9b0 [...]	985220814883
	rtb-0bf81275	-	Yes	vpc-b1deb2cb	985220814883

Route Table: rtb-0730985f8e2bd15cd

Summary Routes Subnet Associations Route Propagation Tags

Edit routes

View All routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
0.0.0.0/0	igw-0d7a1f50f454e6bb0	active	No

8. Subnet Associations under public-Route Table

Route Tables > Edit subnet associations

Edit subnet associations

Route table: rtb-0730985f8e2bd15cd (public-rt)

Associated subnets: subnet-0e0604f8fc6eef6ce

Filter by attributes or search by keyword

Subnet ID	IPv4 CIDR	IPv6 CIDR	Current Route Table
subnet-0e0604f8fc6eef6ce Public-subnet	10.0.1.0/24	-	Main
subnet-0edc0eeb79bf964c3 Private-Su...	10.0.2.0/24	-	Main

* Required

Cancel Save

Services > Resource Groups > Create route table

Create route table

Filter by tags and attributes or search by keyword

Name	Route Table ID	Explicit subnet associations	Main	VPC ID	Owner
	rtb-00a09e07a99d965de	-	Yes	vpc-028af629a6603a9b0 ...	985220814883
public-rt	rtb-0730985f8e2bd15cd	subnet-0e0604f8fc6eef6ce	No	vpc-028af629a6603a9b0 ...	985220814883
	rtb-0bf81275	-	Yes	vpc-b1deb2cb	985220814883

Route Table: rtb-0730985f8e2bd15cd

Summary Routes Subnet Associations Route Propagation Tags

Edit subnet associations

Subnet ID	IPv4 CIDR	IPv6 CIDR
subnet-0e0604f8fc6eef6c...	10.0.1.0/24	-

9. Public route table associated with public subnet

Services > Resource Groups > Create subnet

Create subnet

Filter by tags and attributes or search by keyword

Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR	Availability Zone	Availability Zone
Public-subnet	subnet-0e0604f8fc6eef6ce	available	vpc-028af629a6603a9b0 ...	10.0.1.0/24	251	-	us-east-1a	use1-az6
Private-Subnet	subnet-0edc0eeb79bf964c3	available	vpc-028af629a6603a9b0 ...	10.0.2.0/24	251	-	us-east-1b	use1-az1
default-vpc-1c	subnet-17b9e739	available	vpc-b1deb2cb	172.31.80.0/20	4091	-	us-east-1c	use1-az2
default-vpc-1f	subnet-4335204c	available	vpc-b1deb2cb	172.31.64.0/20	4091	-	us-east-1f	use1-az5
default-vpc-1a	subnet-6683df3a	available	vpc-b1deb2cb	172.31.32.0/20	4091	-	us-east-1a	use1-az6
default-vpc-1b	subnet-b44615d3	available	vpc-b1deb2cb	172.31.0.0/20	4091	-	us-east-1b	use1-az1
default-vpc-1e	subnet-db96f1e5	available	vpc-b1deb2cb	172.31.48.0/20	4091	-	us-east-1e	use1-az3
default-vpc-1d	subnet-f804e7b5	available	vpc-b1deb2cb	172.31.16.0/20	4091	-	us-east-1d	use1-az4

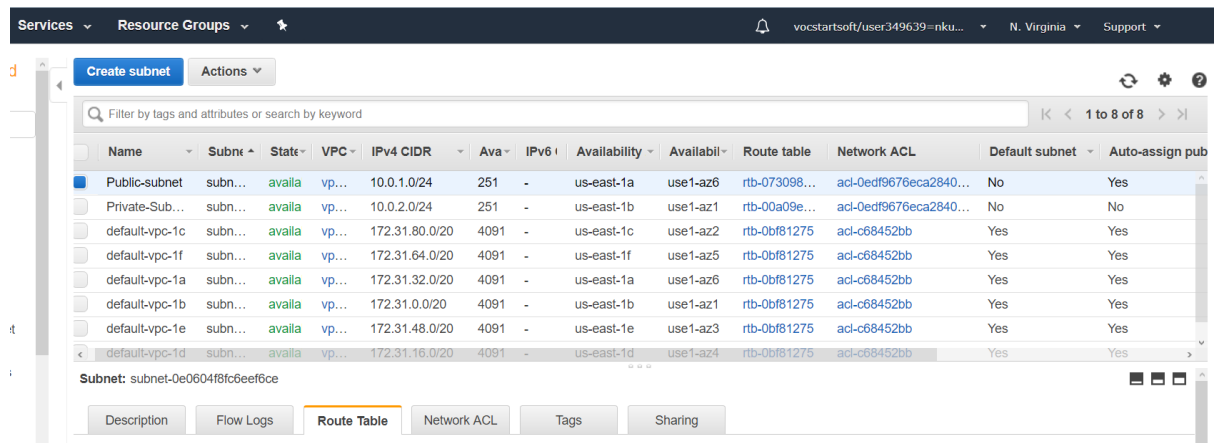
Description Flow Logs Route Table Network ACL Tags Sharing

Edit route table association

Route Table: rtb-0730985f8e2bd15cd | public-rt

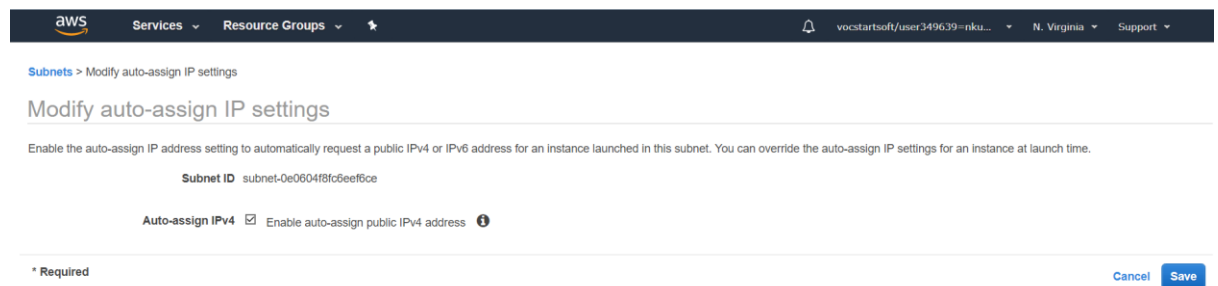
Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-0d7a1f50f454e6bb0

10. Auto Assigning the IP address for Public subnet



The screenshot shows the AWS Management Console interface for the 'Subnets' page. The 'Public-subnet' is selected, and the 'Route Table' tab is active. The subnet is associated with the 'Public-subnet' route table.

Name	Subnet	State	VPC	IPv4 CIDR	Avail...	IPv6	Availability	Availabil...	Route table	Network ACL	Default subnet	Auto-assign pub
Public-subnet	subn...	avalla	vp...	10.0.1.0/24	251	-	us-east-1a	use1-az6	rtb-073098...	acl-0edf9676eca2840...	No	Yes
Private-Sub...	subn...	avalla	vp...	10.0.2.0/24	251	-	us-east-1b	use1-az1	rtb-00a09e...	acl-0edf9676eca2840...	No	No
default-vpc-1c	subn...	avalla	vp...	172.31.80.0/20	4091	-	us-east-1c	use1-az2	rtb-0bf81275	acl-c68452bb	Yes	Yes
default-vpc-1f	subn...	avalla	vp...	172.31.64.0/20	4091	-	us-east-1f	use1-az5	rtb-0bf81275	acl-c68452bb	Yes	Yes
default-vpc-1a	subn...	avalla	vp...	172.31.32.0/20	4091	-	us-east-1a	use1-az6	rtb-0bf81275	acl-c68452bb	Yes	Yes
default-vpc-1b	subn...	avalla	vp...	172.31.0.0/20	4091	-	us-east-1b	use1-az1	rtb-0bf81275	acl-c68452bb	Yes	Yes
default-vpc-1e	subn...	avalla	vp...	172.31.48.0/20	4091	-	us-east-1e	use1-az3	rtb-0bf81275	acl-c68452bb	Yes	Yes
default-vpc-1d	subn...	avalla	vp...	172.31.16.0/20	4091	-	us-east-1d	use1-az4	rtb-0bf81275	acl-c68452bb	Yes	Yes



The screenshot shows the 'Modify auto-assign IP settings' page in the AWS Management Console. The 'Auto-assign IPv4' checkbox is checked, and the 'Enable auto-assign public IPv4 address' option is selected.

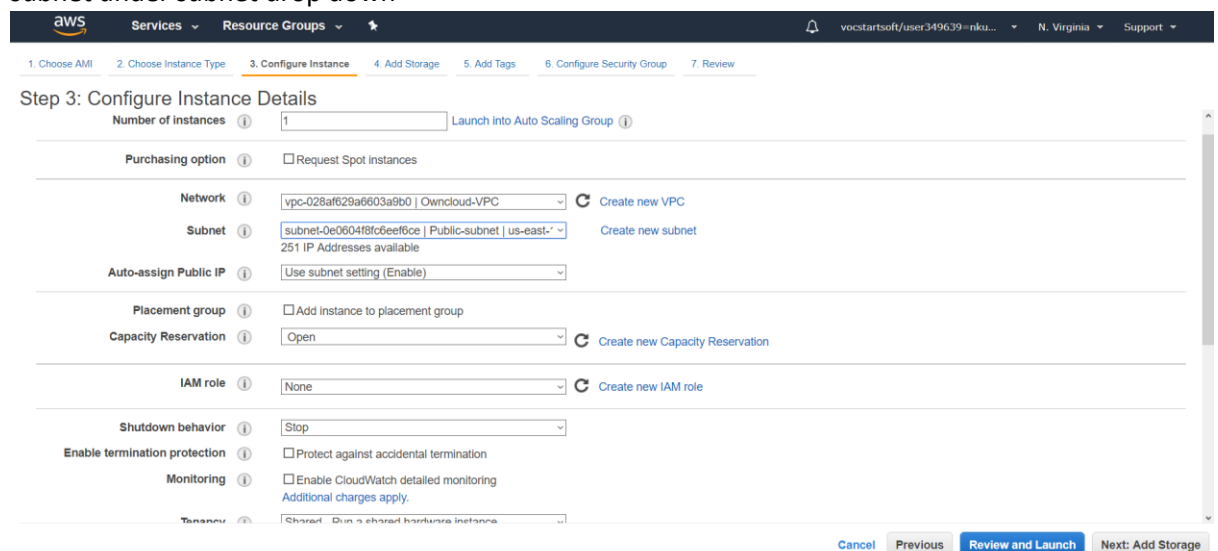
Subnet ID: subnet-0e0604f8fc6eeef6ce

Auto-assign IPv4 ☒ Enable auto-assign public IPv4 address ⓘ

* Required

Cancel Save

11. Create EC2 instance and choose custom VPC under Network drop down and select public subnet under subnet drop down



The screenshot shows the 'Step 3: Configure Instance Details' page in the AWS Management Console. The 'Network' dropdown is set to 'vpc-028af629a6603a9b0 | Owncloud-VPC', and the 'Subnet' dropdown is set to 'subnet-0e0604f8fc6eeef6ce | Public-subnet | us-east-1'. The 'Auto-assign Public IP' dropdown is set to 'Use subnet setting (Enable)'.

Number of instances ⓘ 1 Launch into Auto Scaling Group ⓘ

Purchasing option ⓘ ☐ Request Spot instances

Network ⓘ vpc-028af629a6603a9b0 | Owncloud-VPC ⓘ Create new VPC

Subnet ⓘ subnet-0e0604f8fc6eeef6ce | Public-subnet | us-east-1 ⓘ Create new subnet

Auto-assign Public IP ⓘ Use subnet setting (Enable) ⓘ

Placement group ⓘ ☐ Add instance to placement group

Capacity Reservation ⓘ Open ⓘ Create new Capacity Reservation

IAM role ⓘ None ⓘ Create new IAM role

Shutdown behavior ⓘ Stop ⓘ

Enable termination protection ⓘ ☐ Protect against accidental termination

Monitoring ⓘ ☐ Enable CloudWatch detailed monitoring

Additional charges apply.

Next: Add Storage

aws

Services

Resource Groups

vocstartsoft/user349639=nku...

N. Virginia

Support

1. Choose AMI

2. Choose Instance Type

3. Configure Instance

4. Add Storage

5. Add Tags

6. Configure Security Group

7. Review

Step 3: Configure Instance Details

Elastic Inference

☐ Add an Elastic Inference accelerator
[Additional charges apply.](#)

T2/T3 Unlimited

☐ Enable
[Additional charges may apply](#)

Network interfaces

Device	Network Interface	Subnet	Primary IP	Secondary IP addresses	IPv6 IPs
eth0	New network interface	subnet-0e0604f8f	Auto-assign	Add IP	Add IP

Add Device

Advanced Details

User data

☒ As text
☐ As file
☐ Input is already base64 encoded

```
yum install httpd -y
service httpd start
chkconfig httpd on
IP_ADDR=$(curl http://169.254.169.254/latest/meta-data/public-ip4)
echo "Manual instance with IP $IP_ADDR" >/var/www/html/index.html
echo "ok" > /var/www/html/health.html
```

Cancel

Previous

Review and Launch

Next: Add Storage

12. Create new security group

1. Choose AMI

2. Choose Instance Type

3. Configure Instance

4. Add Storage

5. Add Tags

6. Configure Security Group

7. Review

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group:

☒ Create a new security group
☐ Select an existing security group

Security group name:

0c-sg

Description:

Opens port 80 and 22

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Anywhere 0.0.0.0/0, ::0	e.g. SSH for Admin Desktop
HTTP	TCP	80	Anywhere 0.0.0.0/0, ::0	e.g. SSH for Admin Desktop

Add Rule

Warning

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

13. SSH the public IP of EC2 from Terminal and check the Httpd service status

```
ec2-user@ip-10-0-1-226:~  
File Edit View Search Terminal Help  
nkumar@ubuntu:~$ cd /downloads  
bash: cd: /downloads: No such file or directory  
nkumar@ubuntu:~$ cd downloads  
bash: cd: downloads: No such file or directory  
nkumar@ubuntu:~$ cd Downloads  
nkumar@ubuntu:~/Downloads$ ls -al *.pem  
-r----- 1 nkumar nkumar 1696 Aug  6 01:28 Def-kp.pem  
-rw-rw-r-- 1 nkumar nkumar 1692 Aug 10 02:59 oc-kp.pem  
nkumar@ubuntu:~/Downloads$ chmod 400 oc-kp.pem  
nkumar@ubuntu:~/Downloads$ ssh -i oc-kp.pem ec2-user@54.242.210.37  
The authenticity of host '54.242.210.37 (54.242.210.37)' can't be established.  
ECDSA key fingerprint is SHA256:G5LYUGL39QeMVdbh86m8k2uTZP4xKZCe35S5a9PYgE0.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added '54.242.210.37' (ECDSA) to the list of known hosts.  
  
  _ | _ | _ )  
 _ | ( _ | /  Amazon Linux AMI  
_ _ | \ _ _ | _ _ |  
  
https://aws.amazon.com/amazon-linux-ami/2018.03-release-notes/  
[ec2-user@ip-10-0-1-226 ~]$ sudo service httpd status  
httpd (pid 8346) is running...  
[ec2-user@ip-10-0-1-226 ~]$
```

14. Create another EC2 instance in private subnet and custom VPC

The screenshot shows the AWS Management Console interface for creating a new EC2 instance. The 'Configure Instance Details' step is active, showing various configuration options:

- Network:** vpc-028af628a6003a9b0 | Owncloud-VPC. A link to 'Create new VPC' is available.
- Subnet:** subnet-0ed80eeb79bf964c3 | Private-Subnet | us-... A link to 'Create new subnet' is available.
- Auto-assign Public IP:** Use subnet setting (Disable).
- Placement group:** Add instance to placement group (unchecked).
- Capacity Reservation:** Open. A link to 'Create new Capacity Reservation' is available.
- IAM role:** None. A link to 'Create new IAM role' is available.
- Shutdown behavior:** Stop.
- Enable termination protection:** Protect against accidental termination (unchecked).
- Monitoring:** Enable CloudWatch detailed monitoring (unchecked). A link to 'Additional charges apply' is available.
- Tenancy:** Shared - Run a shared hardware instance. A link to 'Additional charges will apply for dedicated tenancy' is available.
- Elastic Inference:** Add an Elastic Inference accelerator (unchecked). A link to 'Additional charges apply' is available.
- T2/T3 Unlimited:** Enable (unchecked).

At the bottom, there are buttons for 'Cancel', 'Previous', 'Review and Launch', and 'Next: Add Storage'.

15. Create security group to allow traffic from public subnet as below

aws

ServicesResource Groups

1. Choose AMI2. Choose Instance Type3. Configure Instance4. Add Storage5. Add Tags6. Configure Security Group7. Review

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group:

☒ Create a new security group

☐ Select an existing security group

Security group name:Public-subnet traffic allowed

Description:Receives traffic from public subnet only

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Custom10.0.1.0/24	e.g. SSH for Admin Desktop
MYSQIAurc	TCP	3306	Custom10.0.1.0/24	e.g. SSH for Admin Desktop

Add Rule

Cancel

Previous

Review and Launch

16. DB-server EC2 Summary

ServicesResource Groups

Launch InstanceConnectActions

Filter by tags and attributes or search by keyword

1 to 2 of 2

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP	IPv6 IPs	Key Name	Monitoring
App-Server	i-067e928a1f64c3ad5	t2.micro	us-east-1a	running	2/2 checks ...	None		54.242.210.37	-	oc-kp	disabled
db-server	i-0f5221f15dbd9b0bd	t2.micro	us-east-1b	running	Initializing	None		-	-	oc-kp	disabled

Description

Status Checks

Monitoring

Tags

Instance ID

i-0f5221f15dbd9b0bd

Public DNS (IPv4)

-

Instance state

running

IPv4 Public IP

-

Instance type

t2.micro

IPv6 IPs

-

Elastic IPs

-

Private DNS

ip-10-0-2-91.ec2.internal

Availability zone

us-east-1b

Private IPs

10.0.2.91

Security groups

Public-subnet traffic allowed. view inbound rules. view outbound rules

Secondary private IPs

-

Scheduled events

No scheduled events

VPC ID

vpc-028af629a603a0b0 (Owncloud-VPC)

AMI ID

amzn-ami-hvm-2018.03.0.20190611-x86_64-gp2 (ami-035b3c7efe6d61d5)

Subnet ID

subnet-0ed30ee679b9f64c3 (Private-Subnet)

Platform

-

Network interfaces

eth0

IAM role

-

Source/dest. check

True

Key pair name

oc-kp

T2/T3 Unlimited

Disabled

Owner

985220814883

EBS-optimized

False

Launch time

August 10, 2019 at 3:16:37 AM UTC-7 (less than one hour)

Root device type

ebs

Termination protection

False

Root device

/dev/xvda

Lifecycle

normal

Block devices

/dev/xvda

Monitoring

basic

Elastic Graphics ID

-

Alarm status

None

Elastic Inference accelerator ID

-

17. Copying the pem file to /opt folder

```
nkumar@ubuntu: ~/Downloads
File Edit View Search Terminal Help
[ec2-user@ip-10-0-1-226 ~]$ cd /opt/
[ec2-user@ip-10-0-1-226 opt]$ sudo chown ec2-user:ec2-user -R /opt
[ec2-user@ip-10-0-1-226 opt]$ ls -al
total 12
drwxr-xr-x  3 ec2-user ec2-user 4096 Jun 11 00:40 .
dr-xr-xr-x 25 root      root    4096 Aug 10 10:01 ..
drwxr-xr-x  5 ec2-user ec2-user 4096 Jun 11 00:40 aws
[ec2-user@ip-10-0-1-226 opt]$ exit
logout
Connection to 54.242.210.37 closed.
nkumar@ubuntu:~/Downloads$ ls -al *.pem
-r----- 1 nkumar nkumar 1696 Aug  6 01:28 Def-kp.pem
-r----- 1 nkumar nkumar 1692 Aug 10 02:59 oc-kp.pem
nkumar@ubuntu:~/Downloads$ scp -i oc-kp.pem ./oc-kp.pem ec2-user@54.242.210.37:/
opt
oc-kp.pem                                100% 1692      3.1KB/s   00:00
nkumar@ubuntu:~/Downloads$
```

18. SSH using public ip

```
ec2-user@ip-10-0-1-226:/opt
File Edit View Search Terminal Help
logout
Connection to 54.242.210.37 closed.
nkumar@ubuntu:~/Downloads$ ls -al *.pem
-r----- 1 nkumar nkumar 1696 Aug  6 01:28 Def-kp.pem
-r----- 1 nkumar nkumar 1692 Aug 10 02:59 oc-kp.pem
nkumar@ubuntu:~/Downloads$ scp -i oc-kp.pem ./oc-kp.pem ec2-user@54.242.210.37:/
opt
oc-kp.pem                                100% 1692      3.1KB/s   00:00
nkumar@ubuntu:~/Downloads$ ssh -i oc-kp.pem ec2-user@54.242.210.37
Last login: Sat Aug 10 10:04:20 2019 from 171.61.93.130

  _|_  _|_  )
 _|_ ( _|_ /  Amazon Linux AMI
__|_\_|_|_|_

https://aws.amazon.com/amazon-linux-ami/2018.03-release-notes/
[ec2-user@ip-10-0-1-226 ~]$ cd /opt
[ec2-user@ip-10-0-1-226 opt]$ ls -al
total 16
drwxr-xr-x  3 ec2-user ec2-user 4096 Aug 10 10:23 .
dr-xr-xr-x 25 root      root    4096 Aug 10 10:01 ..
drwxr-xr-x  5 ec2-user ec2-user 4096 Jun 11 00:40 aws
-r-----  1 ec2-user ec2-user 1692 Aug 10 10:23 oc-kp.pem
[ec2-user@ip-10-0-1-226 opt]$
```

19. SSH using private ip

```
ec2-user@ip-10-0-2-91:~  
File Edit View Search Terminal Help  
_ | ( / Amazon Linux AMI  
__ | \__ | __ |  
  
https://aws.amazon.com/amazon-linux-ami/2018.03-release-notes/  
[ec2-user@ip-10-0-1-226 ~]$ cd /opt  
[ec2-user@ip-10-0-1-226 opt]$ ls -al  
total 16  
drwxr-xr-x 3 ec2-user ec2-user 4096 Aug 10 10:23 .  
dr-xr-xr-x 25 root root 4096 Aug 10 10:01 ..  
drwxr-xr-x 5 ec2-user ec2-user 4096 Jun 11 00:40 aws  
-r----- 1 ec2-user ec2-user 1692 Aug 10 10:23 oc-kp.pem  
[ec2-user@ip-10-0-1-226 opt]$ ssh -i oc-kp.pem ec2-user@10.0.2.91  
The authenticity of host '10.0.2.91 (10.0.2.91)' can't be established.  
ECDSA key fingerprint is SHA256:dMiPv2XFAjwuc/MNVXvroomju71Mu0MtFnPOw6fLLQ3U.  
ECDSA key fingerprint is MD5:3f:cf:18:87:16:2b:5b:a9:b2:59:df:75:a1:d7:71:51.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added '10.0.2.91' (ECDSA) to the list of known hosts.  
  
_ | ( _ | _ )  
_ | ( / Amazon Linux AMI  
__ | \__ | __ |  
  
https://aws.amazon.com/amazon-linux-ami/2018.03-release-notes/  
[ec2-user@ip-10-0-2-91 ~]$
```

20. Create Route table and associate it to private subnet

Route table: **rtb-0b83d33523675eb2f (Private-rt)**

Associated subnets: **subnet-0edbd0eeb79b9964c3**

Subnet ID	IPv4 CIDR	IPv6 CIDR	Current Route Table
subnet-0e0604f8c6eeffce Public-sub...	10.0.1.0/24	-	rtb-0730985f8e2bd15cd
subnet-0edbd0eeb79b9964c3 Private-S...	10.0.2.0/24	-	Main

* Required

Cancel Save

21. Search for NAT instance from community AMI's

Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Search: NAT

Quick Start (0)
My AMIs (0)
AWS Marketplace (18)
Community AMIs (484)

Operating system

- ☐ Amazon Linux
- ☐ CentOS
- ☐ Debian
- ☐ Fedora
- ☐ Gentoo
- ☐ openSUSE
- ☐ Other Linux
- ☐ Red Hat
- ☐ SUSE Linux
- ☐ Ubuntu
- ☐ Windows

Architecture

Image ID	Image Name	Image Description	Root device type	Virtualization type	ENA Enabled	Architecture
amzn-ami-vpc-nat-hvm-2018.03.0.20181116-x86_64-eb3	Amazon Linux AMI 2018.03.0.20181116 x86_64 VPC HVM EBS	Root device type: ebs Virtualization type: hvm ENA Enabled: Yes	ebs	hvm	Yes	x86_64
amzn-ami-vpc-nat-hvm-2017.09.1.20180108-x86_64-eb3	Amazon Linux AMI 2017.09.1.20180108 x86_64 VPC NAT HVM EBS	Root device type: ebs Virtualization type: hvm ENA Enabled: Yes	ebs	hvm	Yes	x86_64
amzn-ami-vpc-nat-hvm-2018.03.0.20180811-x86_64-eb3	Amazon Linux AMI 2018.03.0.20180811 x86_64 VPC NAT HVM EBS	Root device type: ebs Virtualization type: hvm ENA Enabled: Yes	ebs	hvm	Yes	x86_64
amzn-ami-vpc-nat-hvm-2018.03.0.20190514-x86_64-eb3	Amazon Linux AMI 2018.03.0.20190514 x86_64 VPC HVM EBS	Root device type: ebs Virtualization type: hvm ENA Enabled: Yes	ebs	hvm	Yes	x86_64
amzn-ami-vpc-nat-hvm-2017.09.1-testlongids.20180307-x86_64-eb3	Amazon Linux AMI 2017.09.1-testlongids.20180307 x86_64 VPC NAT HVM EBS	Root device type: ebs Virtualization type: hvm ENA Enabled: Yes	ebs	hvm	Yes	x86_64

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. A copy of a tag can be applied to volumes, instances or both. Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

Key (128 characters maximum) Value (256 characters maximum) Instances (1) Volumes (1)

Name Nat-server

Add another tag (Up to 50 tags maximum)

22. Change the Source/destination check for NAT instance to disable

Launch Instance

Connect Actions

Filter by tags and attributes or search

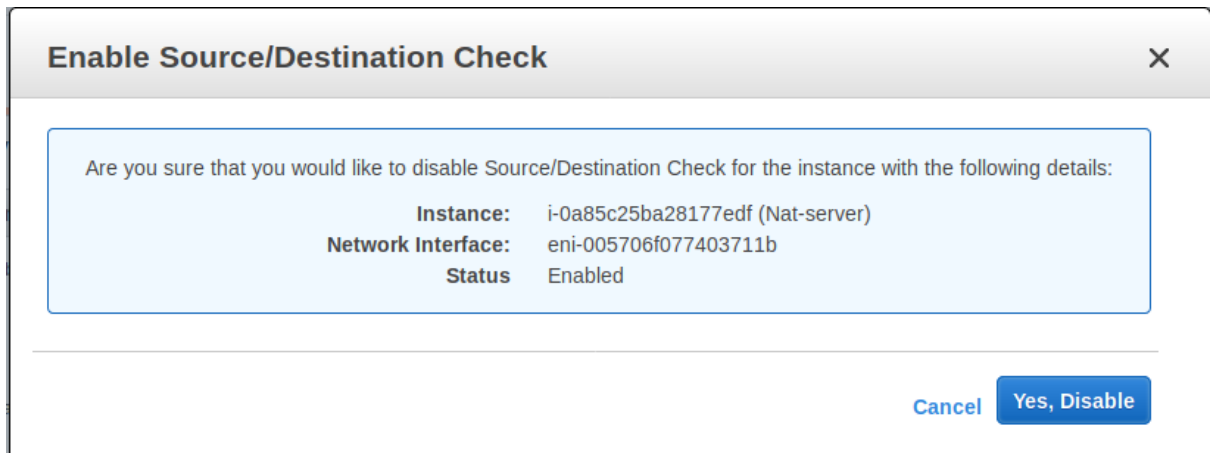
Name	Instance ID	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP	IPv6 IPs	Key Name	Monitoring
App-Server	i-067e928a164c...	us-east-1a	running	2/2 checks ...	None	-	54.242.210.37	-	oc-kp	disabled
Nat-server	i-0a85c25ba2817...	us-east-1a	Initializing	2/2 checks ...	None	-	34.228.213.215	-	oc-kp	disabled
db-server	i-0522115b0b08...	us-east-1b	running	2/2 checks ...	None	-	-	-	oc-kp	disabled

Instance: i-0a85c25ba28177edf (Nat-server) Public IP: 34.228.213.215

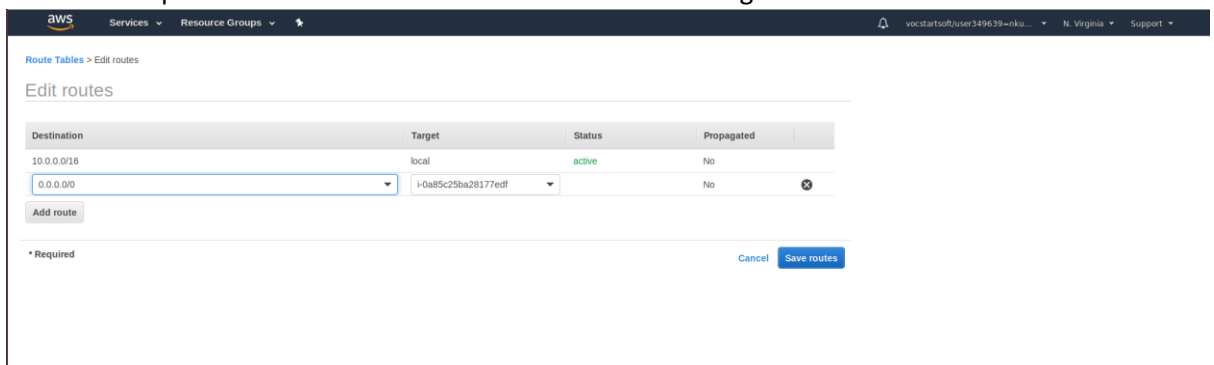
Description Status Checks Monitoring Tags

Instance ID: i-0a85c25ba28177edf
Instance state: running
Instance type: t2.micro
Elastic IPs: -
Availability zone: us-east-1a
Security groups: Allows all traffic for private subnet. view inbound rules. view outbound rules
Scheduled events: No scheduled events
AMI ID: amzn-ami-vpc-nat-hvm-2018.03.0.20181116-x86_64-eb3 (ami-00a904a05375b2763)
Platform: -
IAM role: -
Key pair name: oc-kp
Owner: 985220814883
Launch time: August 10, 2019 at 4:04:54 AM UTC-7 (less than one hour)

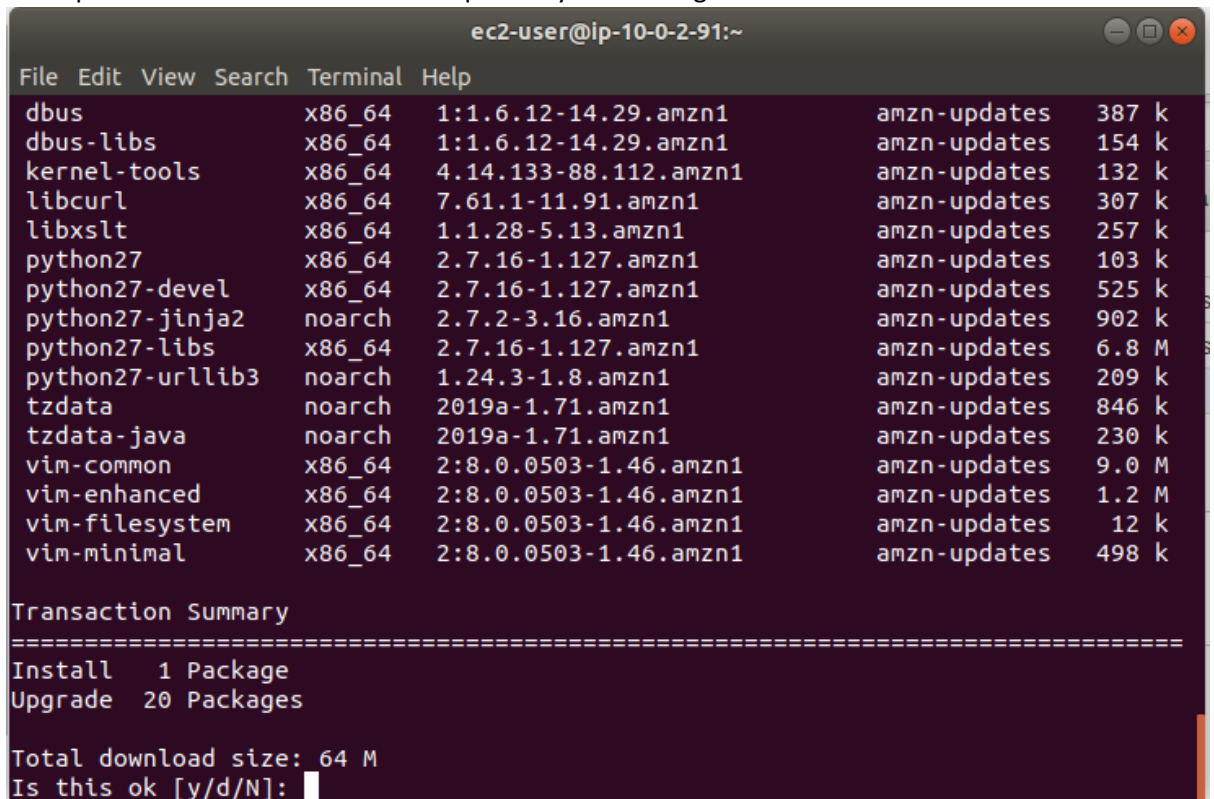
Public DNS (IPv4): -
IPv4 Public IP: 34.228.213.215
IPv6 IPs: -
Private DNS: ip-10-0-1-58.ec2.internal
Private IPs: 10.0.1.58
Secondary private IPs: vpc-028af029a603a0b0 (Dncloud-VPC)
VPC ID: vpc-028af029a603a0b0 (Dncloud-VPC)
Subnet ID: subnet-0a0048bc0ee0f0c (Public-subnet)
Network interfaces: eth0
Source/dest. check: True
T2/T3 Unlimited: Disabled
EBS-optimized: False
Root device type: ebs



23. Add route in private subnet and associate NAT instance in Target as below



24. From private instance we are able to update by connecting to internet



```
ec2-user@ip-10-0-2-91:~  
File Edit View Search Terminal Help  
Updated:  
amazon-ssm-agent.x86_64 0:2.3.662.0-1.amzn1  
bind-libs.x86_64 32:9.8.2-0.68.rc1.60.amzn1  
bind-utils.x86_64 32:9.8.2-0.68.rc1.60.amzn1  
curl.x86_64 0:7.61.1-11.91.amzn1  
dbus.x86_64 1:1.6.12-14.29.amzn1  
dbus-libs.x86_64 1:1.6.12-14.29.amzn1  
kernel-tools.x86_64 0:4.14.133-88.112.amzn1  
libcurl.x86_64 0:7.61.1-11.91.amzn1  
libxslt.x86_64 0:1.1.28-5.13.amzn1  
python27.x86_64 0:2.7.16-1.127.amzn1  
python27-devel.x86_64 0:2.7.16-1.127.amzn1  
python27-jinja2.noarch 0:2.7.2-3.16.amzn1  
python27-libs.x86_64 0:2.7.16-1.127.amzn1  
python27-urllib3.noarch 0:1.24.3-1.8.amzn1  
tzdata.noarch 0:2019a-1.71.amzn1  
tzdata-java.noarch 0:2019a-1.71.amzn1  
vim-common.x86_64 2:8.0.0503-1.46.amzn1  
vim-enhanced.x86_64 2:8.0.0503-1.46.amzn1  
vim-filesystem.x86_64 2:8.0.0503-1.46.amzn1  
vim-minimal.x86_64 2:8.0.0503-1.46.amzn1  
  
Complete!  
[ec2-user@ip-10-0-2-91 ~]$
```

25. Install Mysql-server

```
ec2-user@ip-10-0-2-91:~  
File Edit View Search Terminal Help  
vim-enhanced.x86_64 2:8.0.0503-1.46.amzn1  
vim-filesystem.x86_64 2:8.0.0503-1.46.amzn1  
vim-minimal.x86_64 2:8.0.0503-1.46.amzn1  
  
Complete!  
[ec2-user@ip-10-0-2-91 ~]$ sudo yum install mysql-server  
Loaded plugins: priorities, update-motd, upgrade-helper  
amzn-main | 2.1 kB 00:00  
amzn-updates | 2.5 kB 00:00  
Resolving Dependencies  
--> Running transaction check  
---> Package mysql-server.noarch 0:5.5-1.6.amzn1 will be installed  
--> Processing Dependency: mysql55-server >= 5.5 for package: mysql-server-5.5-1.6.amzn1.noarch  
--> Running transaction check  
---> Package mysql55-server.x86_64 0:5.5.62-1.23.amzn1 will be installed  
--> Processing Dependency: real-mysql55-libs(x86-64) = 5.5.62-1.23.amzn1 for package: mysql55-server-5.5.62-1.23.amzn1.x86_64  
--> Processing Dependency: real-mysql55(x86-64) = 5.5.62-1.23.amzn1 for package: mysql55-server-5.5.62-1.23.amzn1.x86_64  
--> Processing Dependency: perl-DBD-MySQL(mysql55) for package: mysql55-server-5.5.62-1.23.amzn1.x86_64  
--> Processing Dependency: perl(Data::Dumper) for package: mysql55-server-5.5.62-1.23.amzn1.x86_64
```

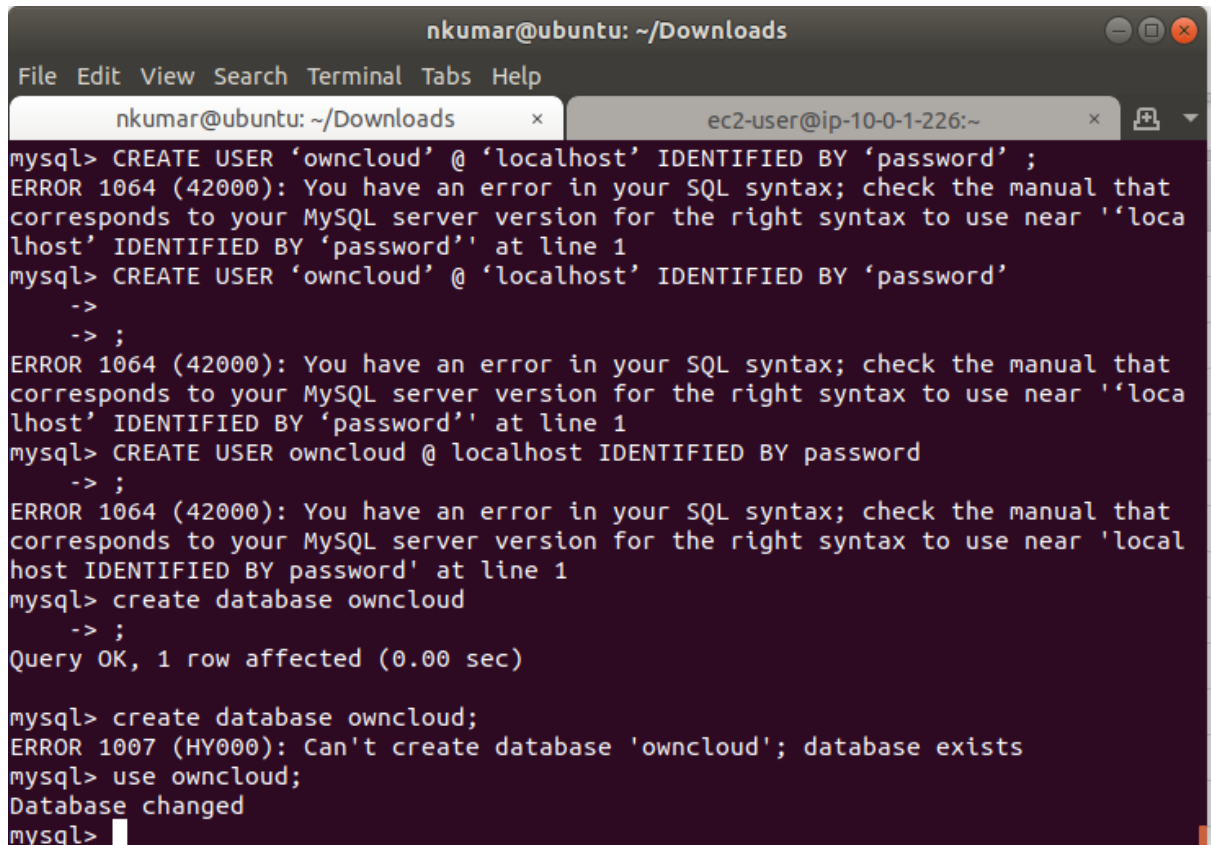
26. Install mysql-server

```
nkumar@ubuntu: ~/Downloads
File Edit View Search Terminal Tabs Help
nkumar@ubuntu: ~/Downloads x ec2-user@ip-10-0-1-226:~ x
Verifying : mysql-server-5.5-1.6.amzn1.noarch 13/13
Installed:
mysql-server.noarch 0:5.5-1.6.amzn1
Dependency Installed:
mysql-config.x86_64 0:5.5.62-1.23.amzn1
mysql55.x86_64 0:5.5.62-1.23.amzn1
mysql55-libs.x86_64 0:5.5.62-1.23.amzn1
mysql55-server.x86_64 0:5.5.62-1.23.amzn1
perl-Compress-Raw-Bzip2.x86_64 0:2.061-3.11.amzn1
perl-Compress-Raw-Zlib.x86_64 1:2.061-4.1.amzn1
perl-DBD-MySQL55.x86_64 0:4.023-5.23.amzn1
perl-DBI.x86_64 0:1.627-4.8.amzn1
perl-Data-Dumper.x86_64 0:2.145-3.5.amzn1
perl-IO-Compress.noarch 0:2.061-2.12.amzn1
perl-Net-Daemon.noarch 0:0.48-5.5.amzn1
perl-PlRPC.noarch 0:0.2020-14.7.amzn1
Complete!
[ec2-user@ip-10-0-2-91 ~]$ packet_write_wait: Connection to 54.242.210.37 port 2
2: Broken pipe
nkumar@ubuntu:~/Downloads$ sudo apt-get install mysql-server
[sudo] password for nkumar:
```

27. Open Mysql terminal

```
nkumar@ubuntu: ~/Downloads
File Edit View Search Terminal Tabs Help
nkumar@ubuntu: ~/Downloads x ec2-user@ip-10-0-1-226:~ x
: m
... skipping.
Reloading the privilege tables will ensure that all changes
made so far will take effect immediately.
Reload privilege tables now? (Press y|Y for Yes, any other key for No) : n
... skipping.
All done!
nkumar@ubuntu:~/Downloads$ sudo mysql
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 4
Server version: 5.7.27-0ubuntu0.18.04.1 (Ubuntu)
Copyright (c) 2000, 2019, Oracle and/or its affiliates. All rights reserved.
Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
mysql>
```

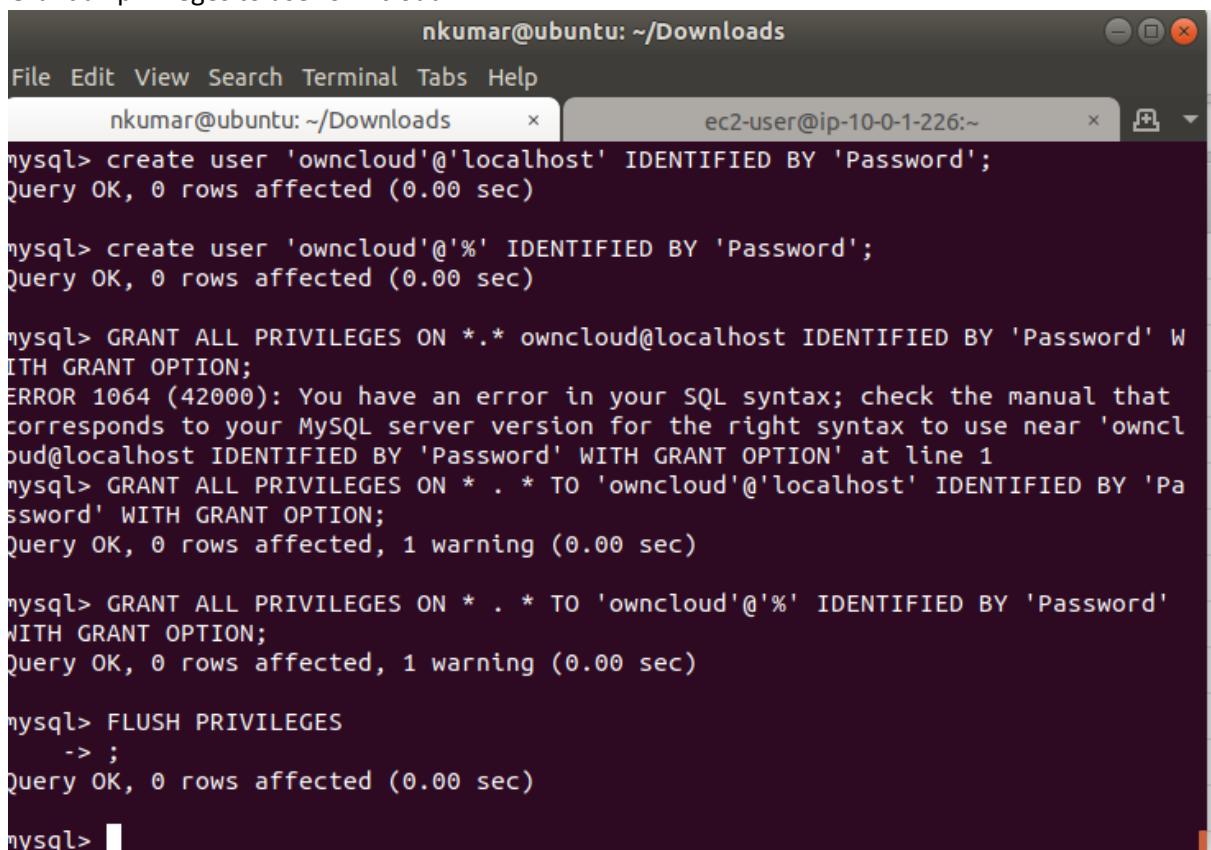

28. Create new DB and use Owncloud database



```
nkumar@ubuntu: ~/Downloads
File Edit View Search Terminal Tabs Help
nkumar@ubuntu: ~/Downloads x ec2-user@ip-10-0-1-226:~ x
mysql> CREATE USER 'owncloud' @ 'localhost' IDENTIFIED BY 'password' ;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that
corresponds to your MySQL server version for the right syntax to use near ''loca
lhost' IDENTIFIED BY 'password'' at line 1
mysql> CREATE USER 'owncloud' @ 'localhost' IDENTIFIED BY 'password'
->
-> ;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that
corresponds to your MySQL server version for the right syntax to use near ''loca
lhost' IDENTIFIED BY 'password'' at line 1
mysql> CREATE USER owncloud @ localhost IDENTIFIED BY password
-> ;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that
corresponds to your MySQL server version for the right syntax to use near 'local
host IDENTIFIED BY password' at line 1
mysql> create database owncloud
-> ;
Query OK, 1 row affected (0.00 sec)

mysql> create database owncloud;
ERROR 1007 (HY000): Can't create database 'owncloud'; database exists
mysql> use owncloud;
Database changed
mysql>
```

29. Grant all privileges to user owncloud



```
nkumar@ubuntu: ~/Downloads
File Edit View Search Terminal Tabs Help
nkumar@ubuntu: ~/Downloads x ec2-user@ip-10-0-1-226:~ x
mysql> create user 'owncloud'@'localhost' IDENTIFIED BY 'Password';
Query OK, 0 rows affected (0.00 sec)

mysql> create user 'owncloud'@'%' IDENTIFIED BY 'Password';
Query OK, 0 rows affected (0.00 sec)

mysql> GRANT ALL PRIVILEGES ON *.* owncloud@localhost IDENTIFIED BY 'Password' W
ITH GRANT OPTION;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that
corresponds to your MySQL server version for the right syntax to use near 'owncl
oud@localhost IDENTIFIED BY 'Password' WITH GRANT OPTION' at line 1
mysql> GRANT ALL PRIVILEGES ON * . * TO 'owncloud'@'localhost' IDENTIFIED BY 'Pa
ssword' WITH GRANT OPTION;
Query OK, 0 rows affected, 1 warning (0.00 sec)

mysql> GRANT ALL PRIVILEGES ON * . * TO 'owncloud'@'%' IDENTIFIED BY 'Password'
WITH GRANT OPTION;
Query OK, 0 rows affected, 1 warning (0.00 sec)

mysql> FLUSH PRIVILEGES
-> ;
Query OK, 0 rows affected (0.00 sec)

mysql>
```