Create another EC2 inside Private Subnet

EC2 Home_page >> Launch Instances

Selecting Amazon Linux 2

Selecting Instance Type - Free Tier(t2.micro)

Selecting VPC - **Team-D-VPC** and Subnet - **Pvt-Subnet-1**

Step 3: Configure Instance Details
Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take ad

Number of instances (i)	1 Launch into Auto Scaling Group (i)
Purchasing option (i)	☐ Request Spot instances
Network (i)	vpc-0537baf72f80d5930 | Team-D-VPC C Create new VPC
Subnet (i)	subnet-017289753c7257388 | Team-D-Pvt-Subnet-1 Create new subnet 27 IP Addresses available
Auto-assign Public IP (i)	Use subnet setting (Disable)
Hostname type (i)	Use subnet setting (IP name)
DNS Hostname (i)	☑ Enable IP name IPv4 (A record) DNS requests

Creating EBS block of **10 GB**

Step 4: Add Storage
Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.

Volume Type (i)	Device (i)	Snapshot (i)	Size (GiB) (i)	Volume Type (i)	IOPS (i)	Throughput (MB/s) (i)	Delete Termi
Root	/dev/xvda	snap-08c6656b1c27d23c5	10	General Purpose SSD (gp2)	100 / 3000	N/A	☑

Add New Volume

Giving Name - **Team-D-EC2-Pvt** as Tag

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)
Name	Team-D-EC2-Pvt

Add another tag   (Up to 50 tags maximum)

Review Page before Launching EC2 instance

Selecting existing Key Pair **team-D-Key**

Only allow inbound traffic within VPC

NACL Home_Page

Network ACLs (1/4) Info

	Name	Network ACL ID	Associated with	Default	VPC ID	
☑	–	acl-07aaeb662a9ae1bd6	6 Subnets	Yes	vpc-0537baf72f80d5930 / Team-D-VPC	2
☐	team-b-public-nacl	acl-073de536f6fd75ebf	3 Subnets	No	vpc-0129bda0428def1cf / Team-B-VPC	1
☐	–	acl-08410bc3e18e24a12	3 Subnets	Yes	vpc-077c7747a9076e6ae / _	2
☐	–	acl-01b8ac293a01a1f70	3 Subnets	Yes	vpc-0129bda0428def1cf / Team-B-VPC	2

NACL Details

Details Info

Network ACL ID
acl-07aaeb662a9ae1bd6

Owner
949263681218

Associated with
6 Subnets

Default
Yes

VPC ID
vpc-0537baf72f80d5930 / Team-D-VPC

Inbound rules | Outbound rules | Subnet associations | Tags

ⓘ You can now check network connectivity with Reachability Analyzer   Run Reachability Analyzer ✕

Inbound rules (2)   Edit inbound rules

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	⊘ Allow
*	All traffic	All	All	0.0.0.0/0	⊗ Deny

Editing Inbound Rules - **Allow traffic only to Team-D VPC network(10.15.32.0/22)**

VPC > Network ACLs > acl-07aaeb662a9ae1bd6 > Edit inbound rules

Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the VPC.

Rule number Info	Type Info	Protocol Info	Port range Info	Source Info	Allow/Deny Info	
100	All traffic ▼	All ▽	All	0.0.0.0/0	Allow ▼	Remove
1	All traffic ▼	All ▽	All	10.15.32.0/22	Allow ▼	Remove
*	All traffic ▼	All ▽	All	0.0.0.0/0	Deny ▼	

Add new rule   Sort by rule number

Cancel   Preview changes   **Save changes**

Done

⊘ You have successfully updated inbound rules for acl-07aaeb662a9ae1bd6

Owner
□ 949263681218

Team-D-VPC

Inbound rules   Outbound rules   Subnet associations   Tags

ⓘ You can now check network connectivity with Reachability Analyzer   **Run Reachability Analyzer**   ✕

Inbound rules (3)

Edit inbound rules

🔍 Filter inbound rules   < 1 >   ⚙

Rule number ▽	Type ▽	Protocol ▽	Port range ▽	Source ▽	Allow/Deny ▽
100	All traffic	All	All	0.0.0.0/0	⊘ Allow
101	All traffic	All	All	10.15.32.0/22	⊘ Allow
*	All traffic	All	All	0.0.0.0/0	⊗ Deny

Install PostgreSQL and open its port to VPC only.

Login to EC2(Pvt-Subnet) Via EC2 (Pub-Subnet)

```
[ec2-user@ip-10-15-32-4 ~]$ ssh -i team-D-key.pem root@10.15.32.111
The authenticity of host '10.15.32.111 (10.15.32.111)' can't be established.
ECDSA key fingerprint is SHA256:y6yiUJlZOKFvsXUH6PbmH0pd75kOO5yyDLsikfn99gE.
ECDSA key fingerprint is MD5:3d:77:a1:b9:72:4c:69:58:ae:e9:8f:91:2d:ab:2b:30.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.15.32.111' (ECDSA) to the list of known hosts.
Please login as the user "ec2-user" rather than the user "root".

Connection to 10.15.32.111 closed.
[ec2-user@ip-10-15-32-4 ~]$ ssh -i team-D-key.pem ec2-user@10.15.32.111


       __|  __|_  )
       _|  (     /    Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
```

To install **Postgres-12 (Amazon Linux II)**
sudo amazon-linux-extras | grep postgre
sudo tee /etc/yum.repos.d/pgdg.repo<<EOF [pgdg12] name=PostgreSQL 12 for RHEL/CentOS 7 - x86_64 baseurl=https://download.postgresql.org/pub/repos/yum/12/redhat/rhel-7-x86_64 enabled=1 gpgcheck=0 EOF
sudo yum makecache

ScreenShot of Installing Postgres-12

```
[ec2-user@ip-10-15-32-111 ~]$ sudo  amazon-linux-extras | grep postgre
  5  postgresql9.6            available     \
  6  postgresql10             available     [ =10  =stable ]
 41  postgresql11             available     [ =11  =stable ]
 58  postgresql12             available     [ =stable ]
 59  postgresql13             available     [ =stable ]
[ec2-user@ip-10-15-32-111 ~]$ sudo tee /etc/yum.repos.d/pgdg.repo<<EOF
> [pgdg12]
> name=PostgreSQL 12 for RHEL/CentOS 7 - x86_64
> baseurl=https://download.postgresql.org/pub/repos/yum/12/redhat/rhel-7-x86_64
> enabled=1
> gpgcheck=0
> EOF
[pgdg12]
name=PostgreSQL 12 for RHEL/CentOS 7 - x86_64
baseurl=https://download.postgresql.org/pub/repos/yum/12/redhat/rhel-7-x86_64
enabled=1
gpgcheck=0
[ec2-user@ip-10-15-32-111 ~]$ sudo yum makecache
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core                                              | 3.7 kB     00:00
amzn2extra-docker                                       | 3.0 kB     00:00
amzn2extra-kernel-5.10                                  | 3.0 kB     00:00
pgdg12                                                  | 3.6 kB     00:00
```

sudo yum install postgresql12 postgresql12-server

```
[ec2-user@ip-10-15-32-111 ~]$ sudo yum install postgresql12 postgresql12-server
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
1 packages excluded due to repository priority protections
Resolving Dependencies
--> Running transaction check
---> Package postgresql12.x86_64 0:12.9-1PGDG.rhel7 will be installed
--> Processing Dependency: postgresql12-libs(x86-64) = 12.9-1PGDG.rhel7 for pack
age: postgresql12-12.9-1PGDG.rhel7.x86_64
---> Package postgresql12-server.x86_64 0:12.9-1PGDG.rhel7 will be installed
--> Running transaction check
---> Package postgresql12-libs.x86_64 0:12.9-1PGDG.rhel7 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
 Package                Arch          Version              Repository    Size
================================================================================
Installing:
 postgresql12           x86_64        12.9-1PGDG.rhel7     pgdg12        1.6 M
 postgresql12-server    x86_64        12.9-1PGDG.rhel7     pgdg12        5.1 M
Installing for dependencies:
 postgresql12-libs      x86_64        12.9-1PGDG.rhel7     pgdg12        372 k

Transaction Summary
```
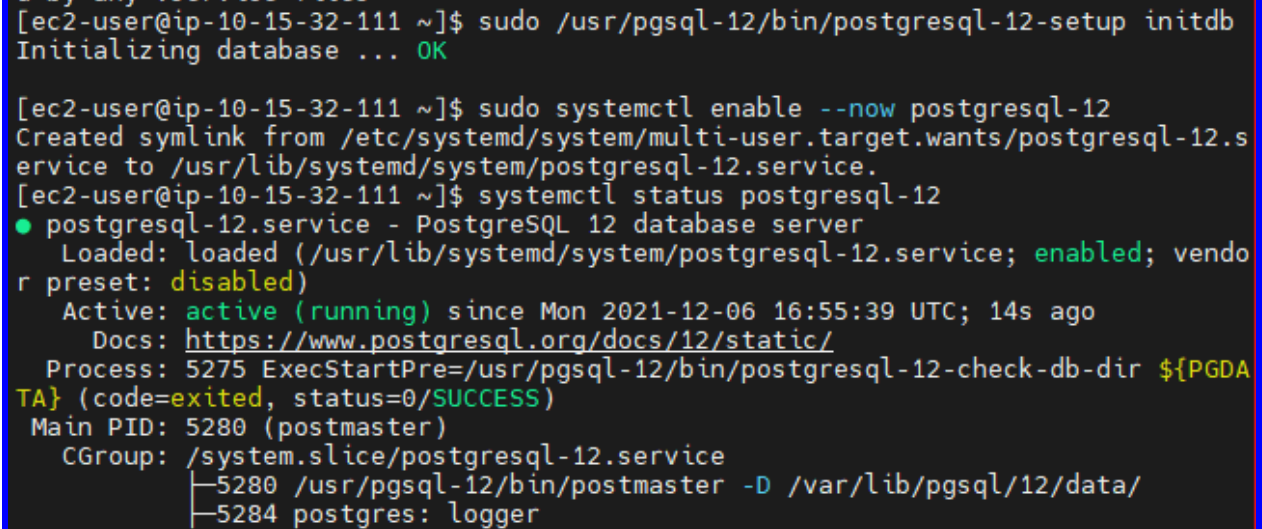
Initializing DB , Enable Postgres 12 , Status
sudo /usr/pgsql-12/bin/postgresql-12-setup initdb   **sudo systemctl enable --now postgresql-12**   **systemctl status postgresql-12**

Screenshot

Login to Postgres User, Setting Password
sudo su - postgres   **psql**   **psql -c "alter user postgres with password 'XXXXX'"**

ScreenShot

```
[ec2-user@ip-10-15-32-111 ~]$ sudo systemctl enable --now postgresql-12
Created symlink from /etc/systemd/system/multi-user.target.wants/postgresql-12.s
ervice to /usr/lib/systemd/system/postgresql-12.service.
[ec2-user@ip-10-15-32-111 ~]$ systemctl status postgresql-12
● postgresql-12.service - PostgreSQL 12 database server
   Loaded: loaded (/usr/lib/systemd/system/postgresql-12.service; enabled; vendo
r preset: disabled)
   Active: active (running) since Mon 2021-12-06 16:55:39 UTC; 14s ago
     Docs: https://www.postgresql.org/docs/12/static/
  Process: 5275 ExecStartPre=/usr/pgsql-12/bin/postgresql-12-check-db-dir ${PGDA
TA} (code=exited, status=0/SUCCESS)
 Main PID: 5280 (postmaster)
   CGroup: /system.slice/postgresql-12.service
           ├─5280 /usr/pgsql-12/bin/postmaster -D /var/lib/pgsql/12/data/
           ├─5284 postgres: logger
           ├─5286 postgres: checkpointer
           ├─5287 postgres: background writer
           ├─5288 postgres: walwriter
           ├─5289 postgres: autovacuum launcher
           ├─5290 postgres: stats collector
           └─5291 postgres: logical replication launcher

Dec 06 16:55:39 ip-10-15-32-111.us-east-2.compute.internal systemd[1]: Starti...
Dec 06 16:55:39 ip-10-15-32-111.us-east-2.compute.internal postmaster[5280]: ...
Dec 06 16:55:39 ip-10-15-32-111.us-east-2.compute.internal postmaster[5280]: ...
Dec 06 16:55:39 ip-10-15-32-111.us-east-2.compute.internal postmaster[5280]: ...
Dec 06 16:55:39 ip-10-15-32-111.us-east-2.compute.internal postmaster[5280]: ...
Dec 06 16:55:39 ip-10-15-32-111.us-east-2.compute.internal postmaster[5280]: ...
Dec 06 16:55:39 ip-10-15-32-111.us-east-2.compute.internal postmaster[5280]: ...
Dec 06 16:55:39 ip-10-15-32-111.us-east-2.compute.internal systemd[1]: Starte...
Hint: Some lines were ellipsized, use -l to show in full.
[ec2-user@ip-10-15-32-111 ~]$ sudo su - postgres
Last login: Mon Dec  6 16:54:23 UTC 2021 on pts/0
-bash-4.2$ psql
psql (12.9)
Type "help" for help.

postgres=#
```

Created database Lf_technology
create database Lf-technology
\l – to view created database

Screenshot


```
/bin/psql: /bin/psql: cannot execute binary file
[root@ip-10-15-32-111 data]# sudo su - postgres
Last login: Mon Dec  6 19:05:11 UTC 2021 on pts/0
-bash-4.2$ psql
Password for user postgres:
psql (12.9)
Type "help" for help.

postgres=# create database lf-technology;
ERROR:  syntax error at or near "-"
LINE 1: create database lf-technology;
                          ^
postgres=# create database lf_technology;
CREATE DATABASE
postgres=# \l
                               List of databases
     Name      |  Owner   | Encoding |   Collate   |    Ctype    |   Access privil
eges
---------------+----------+----------+-------------+-------------+----------------
-------
 lf_technology | postgres | UTF8     | en_US.UTF-8 | en_US.UTF-8 |
 postgres      | postgres | UTF8     | en_US.UTF-8 | en_US.UTF-8 |
 template0     | postgres | UTF8     | en_US.UTF-8 | en_US.UTF-8 | =c/postgres
      +
               |          |          |             |             | postgres=CTc/po
stgres
 template1     | postgres | UTF8     | en_US.UTF-8 | en_US.UTF-8 | =c/postgres
      +
               |          |          |             |             | postgres=CTc/po
stgres
(4 rows)

postgres=#
```

To listen on all IP addresses
vi /var/lib/pgsql/12/data/postgresql.conf


```
#-----------------------------------------------------------------------
# CONNECTIONS AND AUTHENTICATION
#-----------------------------------------------------------------------

# - Connection Settings -

listen_addresses = '*'                  # what IP address(es) to listen on;
                                        # comma-separated list of addresses;
                                        # defaults to 'localhost'; use '*' for a
ll
                                        # (change requires restart)
#port = 5432                            # (change requires restart)
```

To allow all hosts to login
vi /var/lib/pgsql/12/data/pg_hba.conf

```
# TYPE  DATABASE        USER            ADDRESS                 METHOD

# "local" is for Unix domain socket connections only
local   all             all                                     md5
# IPv4 local connections:
host    all             all             0.0.0.0/0               md5
# IPv6 local connections:
host    all             all             ::1/128                 ident
# Allow replication connections from localhost, by a user with the
# replication privilege.
local   replication     all                                     peer
host    replication     all             127.0.0.1/32            ident
host    replication     all             ::1/128                 ident
```

Restarting Postgresql-12
sudo systemctl restart postgresql-12.service
sudo systemctl status postgresql-12.service

```
[root@ip-10-15-32-111 data]# sudo systemctl status postgresql-12.service
● postgresql-12.service - PostgreSQL 12 database server
   Loaded: loaded (/usr/lib/systemd/system/postgresql-12.service; enabled; vendo
r preset: disabled)
   Active: active (running) since Mon 2021-12-06 18:34:51 UTC; 18min ago
     Docs: https://www.postgresql.org/docs/12/static/
  Process: 6671 ExecStartPre=/usr/pgsql-12/bin/postgresql-12-check-db-dir ${PGDA
TA} (code=exited, status=0/SUCCESS)
 Main PID: 6676 (postmaster)
   CGroup: /system.slice/postgresql-12.service
           ├─6676 /usr/pgsql-12/bin/postmaster -D /var/lib/pgsql/12/data/
           ├─6679 postgres: logger
           ├─6681 postgres: checkpointer
           ├─6682 postgres: background writer
           ├─6683 postgres: walwriter
           ├─6684 postgres: autovacuum launcher
           ├─6685 postgres: stats collector
           └─6686 postgres: logical replication launcher

Dec 06 18:34:51 ip-10-15-32-111.us-east-2.compute.internal systemd[1]: Starti...
Dec 06 18:34:51 ip-10-15-32-111.us-east-2.compute.internal postmaster[6676]: ...
Dec 06 18:34:51 ip-10-15-32-111.us-east-2.compute.internal postmaster[6676]: ...
```

Editing Security Group of EC2 Pvt Instance to only allow postgres(5432) login from VPC Network(10.15.32.0/22)

Connect to PostgreSQL from above created EC2.

We have installed postgresql client in EC2 (launched in Public subnet)

Previous Postgres installation process was used


```
psql -h 10.15.32.111 -U postgres -d postgres -W
\l – to show database created "Lf-technology"
```

(Optional) Connect to PostgreSQL server from your local PC (hint: use OpenVPN connection)

Allowed port 1194 on OpenVPN-Server for connecting my Host with Public IP

sgr-064baef81682d1c91	Custom TCP ▼	TCP	1194	Custom ▼	🔍	bibek	Delete
					27.34.104.13/32 ✕		
sgr-067c84a2d93b8613d	SSH ▼	TCP	22	Custom ▼	🔍	bibek_ssh	Delete
					27.34.104.13/32 ✕		

sgr-07022ba42a8375b01	Custom UDP ▼	UDP	1194	Custom ▼	🔍	bibek	Delete
					27.34.104.13/32 ✕		

Connected to the OpenVPN through Host on the local Machine

sudo openvpn –config client.ovpn

```
Tue Dec  7 15:00:45 2021 ROUTE_GATEWAY 192.168.1.254/255.255.255.0 IFACE=enp0s3 HWADDR=08:
Tue Dec  7 15:00:45 2021 GDG6: remote_host_ipv6=n/a
Tue Dec  7 15:00:45 2021 ROUTE6: default_gateway=UNDEF
Tue Dec  7 15:00:45 2021 TUN/TAP device tun0 opened
Tue Dec  7 15:00:45 2021 TUN/TAP TX queue length set to 100
Tue Dec  7 15:00:45 2021 /sbin/ip link set dev tun0 up mtu 1500
Tue Dec  7 15:00:46 2021 /sbin/ip addr add dev tun0 10.8.0.2/24 broadcast 10.8.0.255
Tue Dec  7 15:00:46 2021 /sbin/ip -6 addr add fd42:42:42:42::1000/112 dev tun0
Tue Dec  7 15:00:46 2021 /sbin/ip route add 18.222.3.239/32 via 192.168.1.254
Tue Dec  7 15:00:46 2021 /sbin/ip route add 0.0.0.0/1 via 10.8.0.1
Tue Dec  7 15:00:46 2021 /sbin/ip route add 128.0.0.0/1 via 10.8.0.1
Tue Dec  7 15:00:46 2021 add_route_ipv6(2000::/3 -> fd42:42:42:42::1 metric -1) dev tun0
Tue Dec  7 15:00:46 2021 /sbin/ip -6 route add 2000::/3 dev tun0
Tue Dec  7 15:00:46 2021 add_route_ipv6(::/3 -> fd42:42:42:42::1 metric -1) dev tun0
Tue Dec  7 15:00:46 2021 /sbin/ip -6 route add ::/3 dev tun0
Tue Dec  7 15:00:46 2021 add_route_ipv6(2000::/4 -> fd42:42:42:42::1 metric -1) dev tun0
Tue Dec  7 15:00:46 2021 /sbin/ip -6 route add 2000::/4 dev tun0
Tue Dec  7 15:00:46 2021 add_route_ipv6(3000::/4 -> fd42:42:42:42::1 metric -1) dev tun0
Tue Dec  7 15:00:46 2021 /sbin/ip -6 route add 3000::/4 dev tun0
Tue Dec  7 15:00:46 2021 add_route_ipv6(fc00::/7 -> fd42:42:42:42::1 metric -1) dev tun0
Tue Dec  7 15:00:46 2021 /sbin/ip -6 route add fc00::/7 dev tun0
Tue Dec  7 15:00:46 2021 Initialization Sequence Completed
```

Allowing ICMP signals to verify ping to EC2 in Pvt Subnet

*ICMP signals is allowed in Security Group of EC2 in Pvt Subnet to VPC Network (**10.15.32.0/22**)*

Ping to EC2 in Pvt subnet From Host Machine Success


```
bibek@prometheus:~$ ping 10.15.32.111
PING 10.15.32.111 (10.15.32.111) 56(84) bytes of data.
From 192.168.1.254 icmp_seq=3736 Destination Net Unreachable
From 192.168.1.254 icmp_seq=3737 Destination Net Unreachable
64 bytes from 10.15.32.111: icmp_seq=8136 ttl=63 time=256 ms
64 bytes from 10.15.32.111: icmp_seq=8137 ttl=63 time=257 ms
64 bytes from 10.15.32.111: icmp_seq=8138 ttl=63 time=263 ms
64 bytes from 10.15.32.111: icmp_seq=8139 ttl=63 time=258 ms
64 bytes from 10.15.32.111: icmp_seq=8140 ttl=63 time=260 ms
64 bytes from 10.15.32.111: icmp_seq=8141 ttl=63 time=258 ms
64 bytes from 10.15.32.111: icmp_seq=8142 ttl=63 time=256 ms
64 bytes from 10.15.32.111: icmp_seq=8143 ttl=63 time=260 ms
64 bytes from 10.15.32.111: icmp_seq=8144 ttl=63 time=256 ms
64 bytes from 10.15.32.111: icmp_seq=8145 ttl=63 time=257 ms
64 bytes from 10.15.32.111: icmp_seq=8146 ttl=63 time=256 ms
64 bytes from 10.15.32.111: icmp_seq=8147 ttl=63 time=257 ms
64 bytes from 10.15.32.111: icmp_seq=8148 ttl=63 time=256 ms
64 bytes from 10.15.32.111: icmp_seq=8149 ttl=63 time=256 ms
64 bytes from 10.15.32.111: icmp_seq=8150 ttl=63 time=257 ms
64 bytes from 10.15.32.111: icmp_seq=8151 ttl=63 time=258 ms
64 bytes from 10.15.32.111: icmp_seq=8152 ttl=63 time=259 ms
```

Login to PostgreSQL 12 of EC2 in Pvt subnet From the Host Machine


```
bibek@prometheus:~$ psql -h 10.15.32.111 -U postgres -d postgres -W
Password:
psql (14.1 (Ubuntu 14.1-2.pgdg20.04+1), server 12.9)
Type "help" for help.

postgres=#
```