VPC Endpoint

VPC endpoints enable you to connect your VPC resources to supported AWS services and other VPCs without requiring an internet gateway, NAT gateway, VPN or a DC connection.

This runbook simulates the Gateway VPC endpoints:

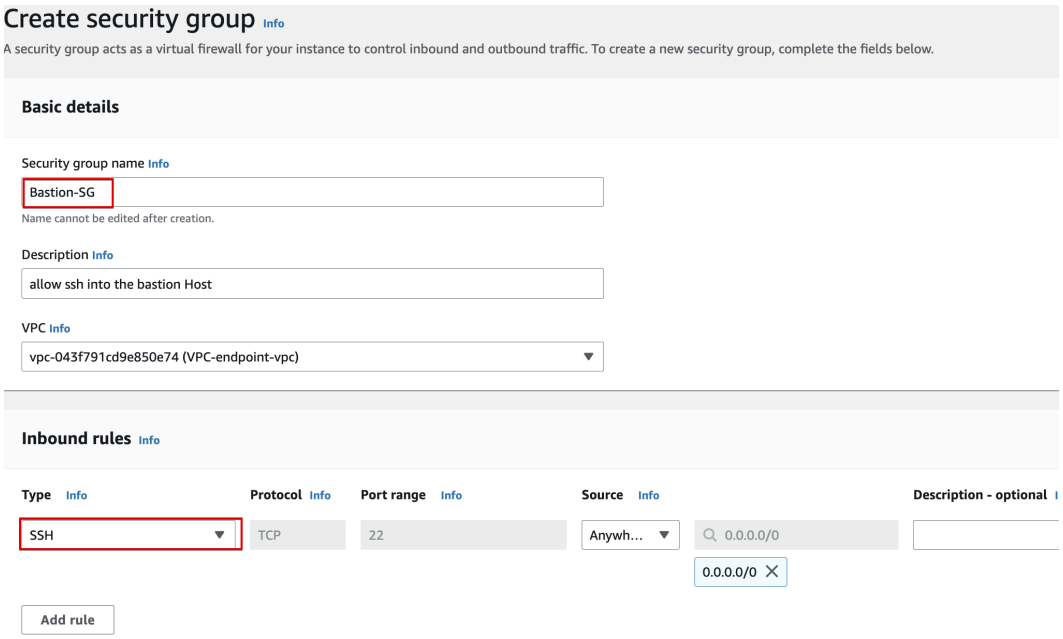
- Gateway endpoints provide access to S3 and DynamoDB to resources in a private subnet without using public addressing.

Prerequisite

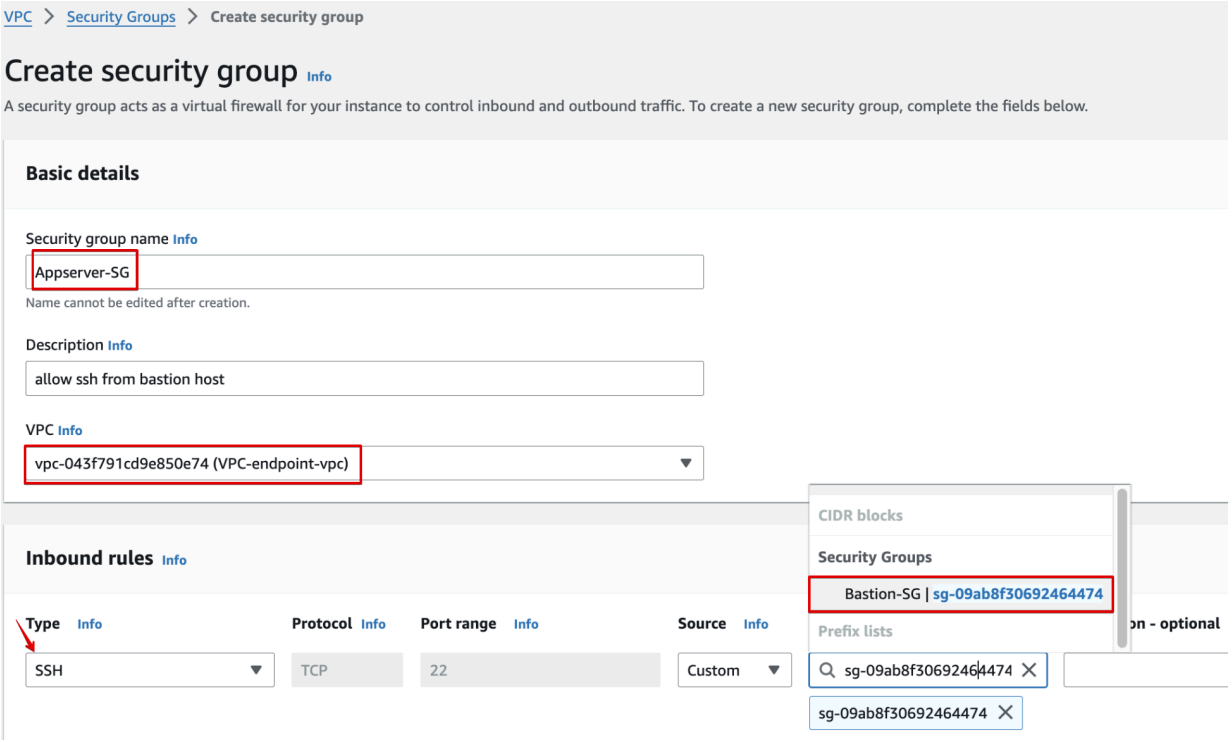
- VPC
- min 1 public subnet (you will need a jump box in a public subnet)
- min 1 private subnet (Don't include NAT Gateway in private route table)

TIP: You can use the VPC launch wizard to create the above networking configuration

1. Create a Security group and give it a name **Bastion-SG**. Open port 22 to the internet.

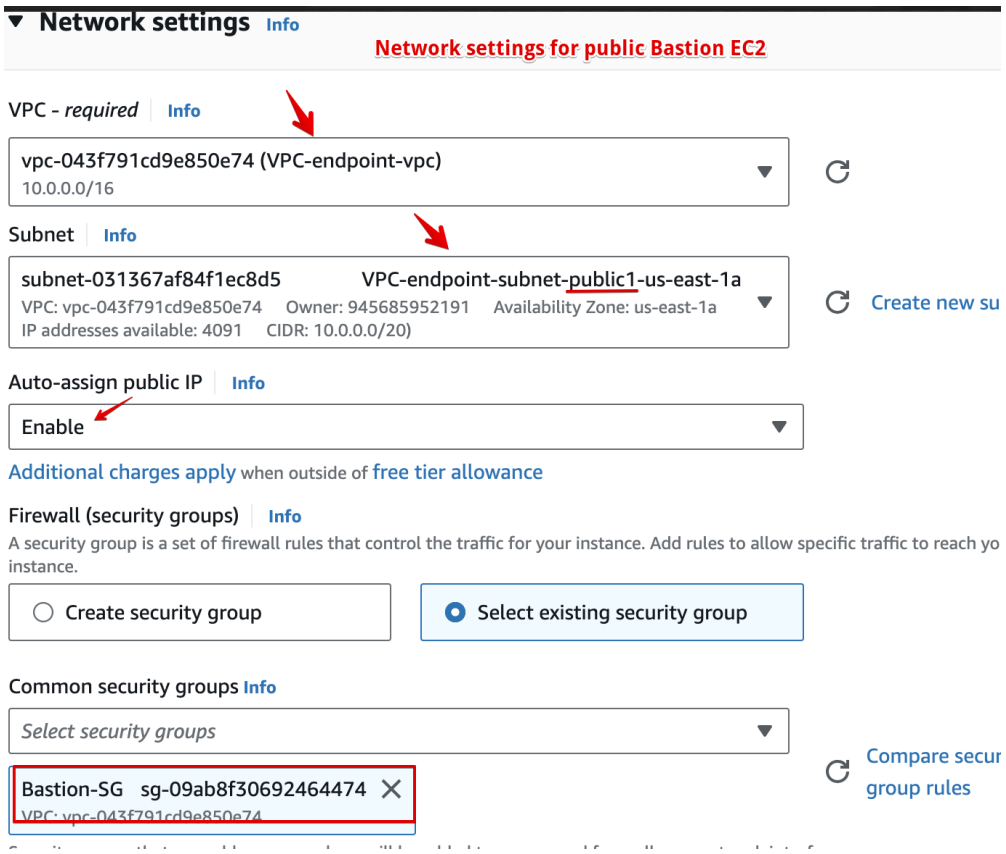


2. Create another Security group with the name **Appserver-SG**. Open port 22 to Bastion-SG

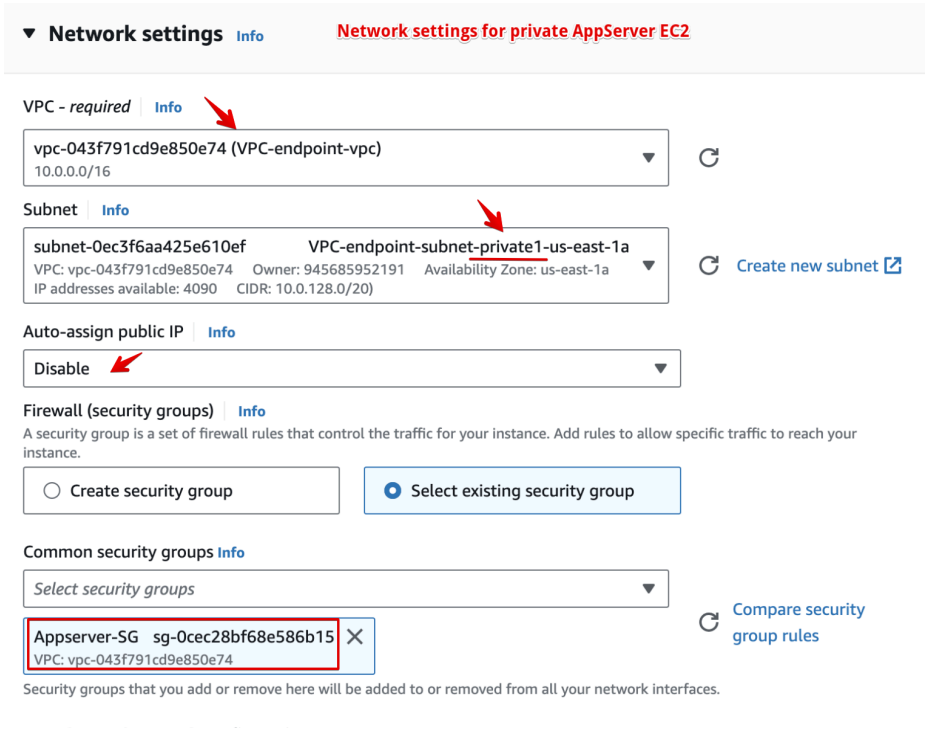


3. create a keypair for ssh named e.g **bastion**

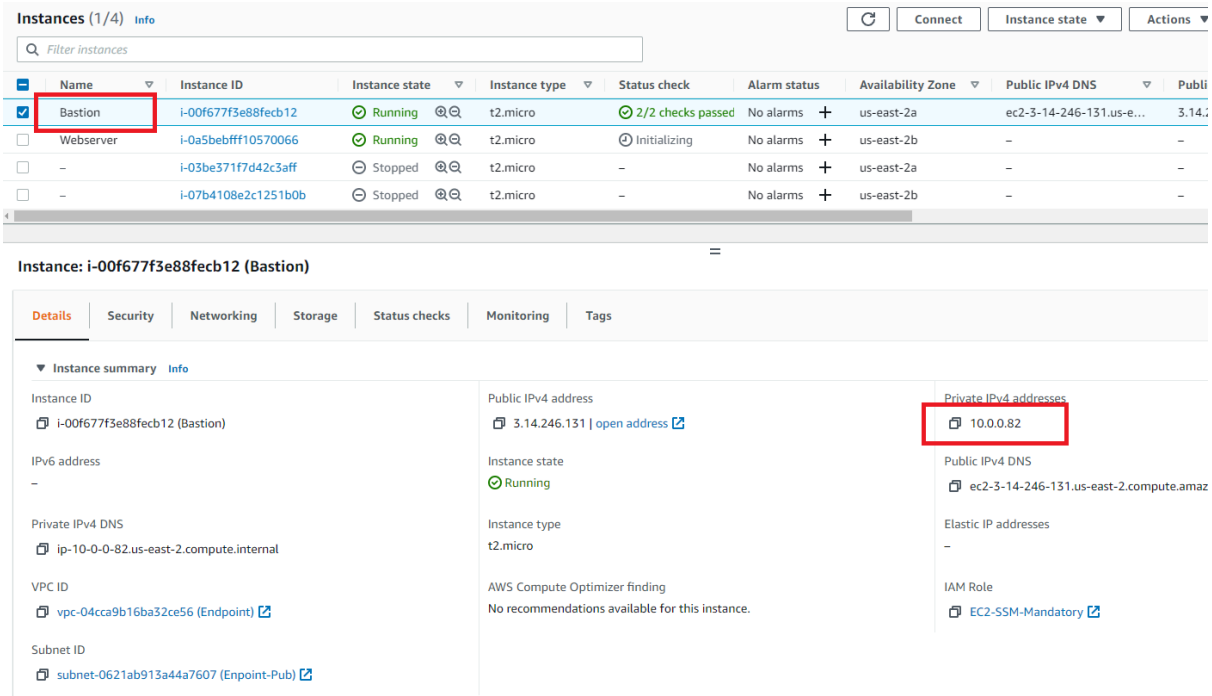
4. Create 1 instance in the public subnet ***of the VPC-endpoint VPC*** using Amazon linux 2 AMI and give it a name **JJtech-Bastion**. Attach the Bastion security group (Bastion-SG) to the instance

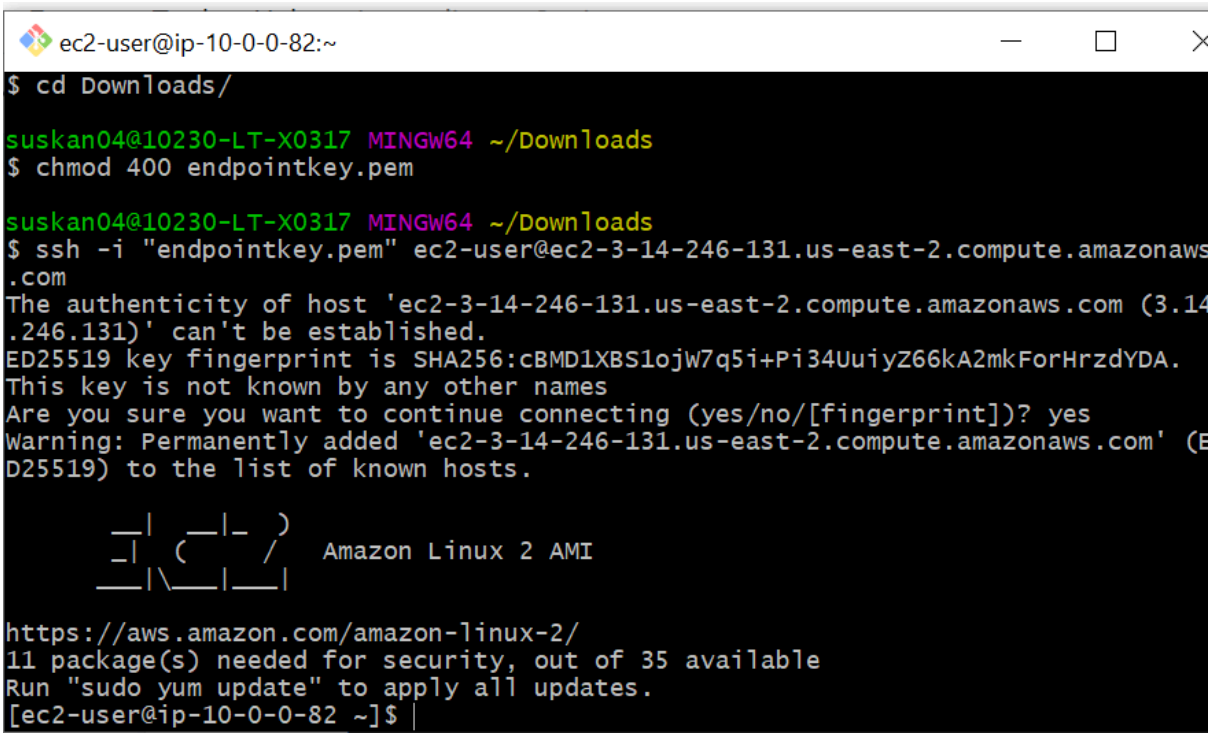


5. Create another instance in the private subnet ***of the VPC-endpoint VPC*** using Amazon linux 2 AMI and give it a name **JJtech-AppServer**. Use the Appserver-SG created above



6. SSH into the Bastion server

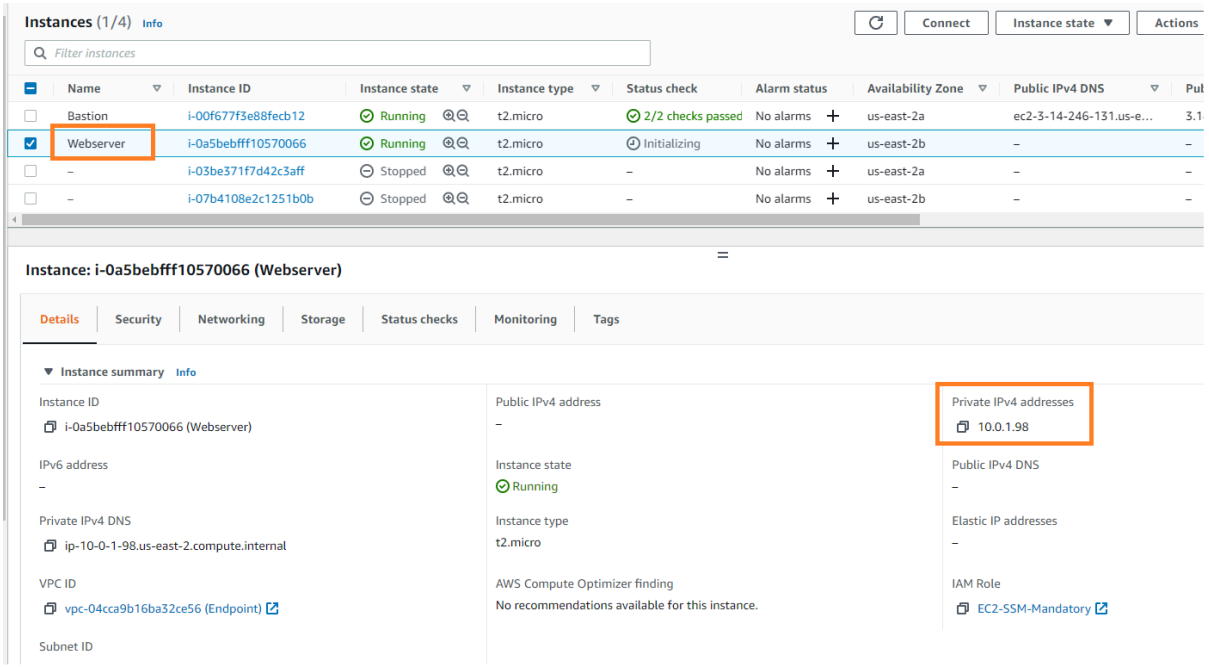




7. While in the Bastion server SSH into the Appserver.
    a. Create a file bastion.pem
    b. copy the content of the pem file from the downloads folder to the bastion.pem

c. Windows users:

i. Open file explorer and open file using notepad. Copy content to to bastion.pem



```
ec2-user@ip-10-0-1-98:~
[ec2-user@ip-10-0-0-82 ~]$ vi bastion.pem
[ec2-user@ip-10-0-0-82 ~]$ cat bastion.pem
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAsAqAF1O0tcJjzo6bT8hoUaoM6K4JDjUOLzIikR0ER9VVo8kE
ksyz3YB8xIYIARffBj/iSW/CL1UMPYcCqejddHpp7eXi4RUPv/mvQ+R31VAWNrkq
JaW4sFIm7xxX19rNYsZF8RkXnA/ZgYoMv5Yx1oulsE83Cz3+LXbJWljLwWpBPPCZ
hCId/+/WC9kv46KMJ4yGiaeHUoR2uHBsPh8Ktt1+LCbzkXAs3bIyIyuhCNXtQlvK
GQkgfbJw/1kyRoHzLajSz5p+6+3vt9TJXtkASOOjLmodvkDOlve78pnhZlCr7wzm
AVA4+1ITRfaa+iv/LFQeKrrFb6Jm4xGDlUlaAwIDAQABAoIBAAOAOYV/gRELUiOn
FIFH46xkSp/Eepa6BFon8bWV1wMXFkQKTHQq+f2Zx50b6Otrv+TOQv/5aPXl6gmB
NwklUXWQtNIE8ER/MbKT1gXFkbQHPhy8gAhXvNQIvSdbiIFAf3qT+gZcPAoigYW3
lElx5ixaE9p5fy8tXOAuraAmfqXB+8Dm8IkERpC7RV7+ZkxL/2n4h+6Ll24k8Wv8
Czma1b8fPIXYaEBJj1oi67ifCyqXACDEWB5p5V6qWCJpSpmHFT7YdRBzqmdsDZV9
cCZ+QDMOXYMb80TnMOXehtii7XQAVVcolsC476HM1x//1U3Q7t7ZSivxaf90woVy
oRiZXkECgYEA2oPT75E5BxH+PZw6/qz/ReXWhcziZ2PGvGZAEGy6ov5RE248S6Mm
QVVCzjPiviXUA38v50pH/RLWoraQrMlHfdAN9ZHkEfzYgecq75ltJ+bVhOQbjZUv
BN1OWW8rusu3p3SC2QbKVZOS+e7nppp6rnG55FIDYrTw0Fh6lhx/G+0CgYEAzj1p
mXLeHCpbDsupwqGSJw0+k52xxHFCnevsRly1QmGKiBfI58nNiSs5V3nttfKMjzj9
t4Bd7GEkOe8AiLmmAEPqNTTJvSrUACPcwJkTel53Nc1nMOifG4veByjIzcORiqQd
1lL5z1X4YrXloSOzLuOjeygTvTw9iv/zP9A/768CgYAFfPYfuDgEc3E9PuVEbDfl
G4atyZ2OFzVwmejWAMUXPufuYwBkre5SCcApyafSOsT+aX1cg8MXGhgF8ivkCxIe
mNEg788YnI8bhCDR77qMHAIU2l3OyoZpytOi5eXlRSSRsh1vMfp2+AD4AgYTayHV
q8mNcHnhSsYZlX9OsdyHaQKBgQDHdu3iOw2t/+kBbkhJTSqlSlHzQtjjPQdI5Rwn
ERLdmKj65sYQJOT6HSvgRrR4/JSlEGGSUDyGmYOH2veRRLwgFY821k8m/Xz8hbLD
MOl7WFHDX1OmGFWJtsSN+Av9vw/wHrocxzOEK4mHLpVgO77Y4qECQ8iThOegv9rr
JOYxUQKBgQDYIitAKV9fBOaGNv4xt6zXFU/kcRx3ZOgdw9dtmLTXG4GGGjONd3mf
9d6R+o842thDBSmZzOCz6fwQBgjnSqhrQytjwvEtmTaTe9iUkuz/2bp6pfN8OvnO
3ejeZU72afB9gR8RxZSheBD6x+Nb5gpjgSrRzn+rJjU4O6JSR4o9ig==
-----END RSA PRIVATE KEY-----
[ec2-user@ip-10-0-0-82 ~]$ chmod 400 bastion.pem
[ec2-user@ip-10-0-0-82 ~]$ ssh -i bastion.pem ec2-user@10.0.1.98

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

https://aws.amazon.com/amazon-linux-2/
11 package(s) needed for security, out of 35 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-10-0-1-98 ~]$
```

From the above screen you see that you are now in the private instance.

Note:

*Steps 6 and 7 could be achieved using **SSH agent forwarding***

- *Add the private key to the ssh agent. Change into the directory with the private key*
  - ***ssh-add [bastion.pem]***
- *ssh -A [username]@[server–public-address] to ssh into the public bastion host*

- ***ssh -A [ec2-user]@[3.87.73.227]***

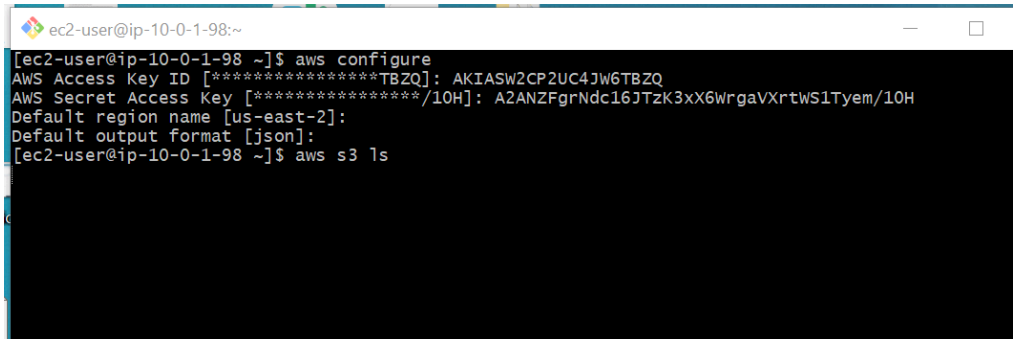
- ***You should be in the public bastion host. confirm this by comparing its private IP with the private IP on the AWS console***

  from the bastion host, you can confirm the ssh key from your local has been forwarded into the bastion host using the command

  ssh-add -L

  - ***ssh into the private server from the bastion host using***
    - ***ssh [ec2-user]@[private-IP-of-Appserver]***
      e.g ssh ec2-user@10.0.132.120

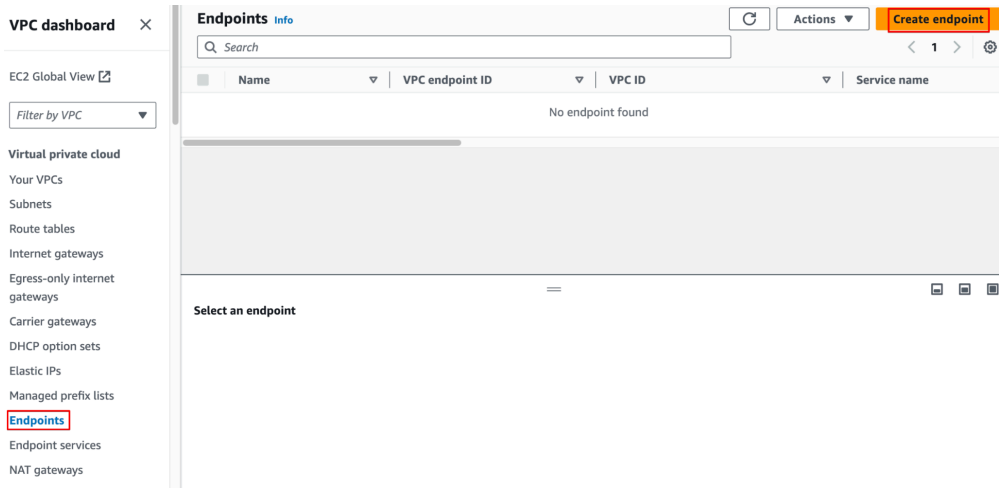
8. Since this is an amazon linux instance it comes with AWS CLI already Run aws configure and give the accesskey and secret key and try to access s3
   a. Run aws s3 ls
   b. It will not list the buckets in your account. You will notice that it will time out. To make connection possible we need to create a VPC endpoint



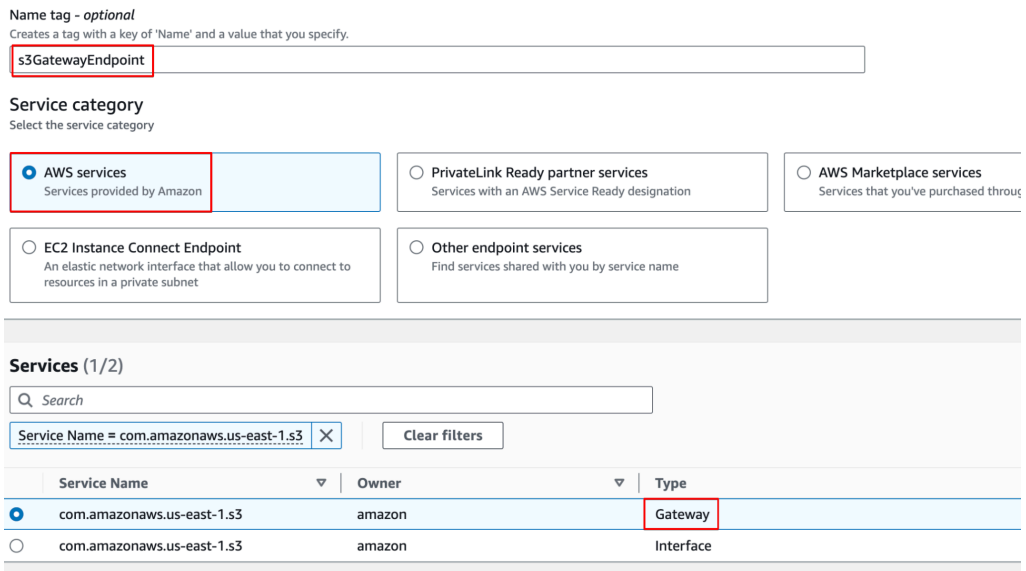
9. Creating Gateway endpoint:

   Now we will create a VPC endpoint for S3.

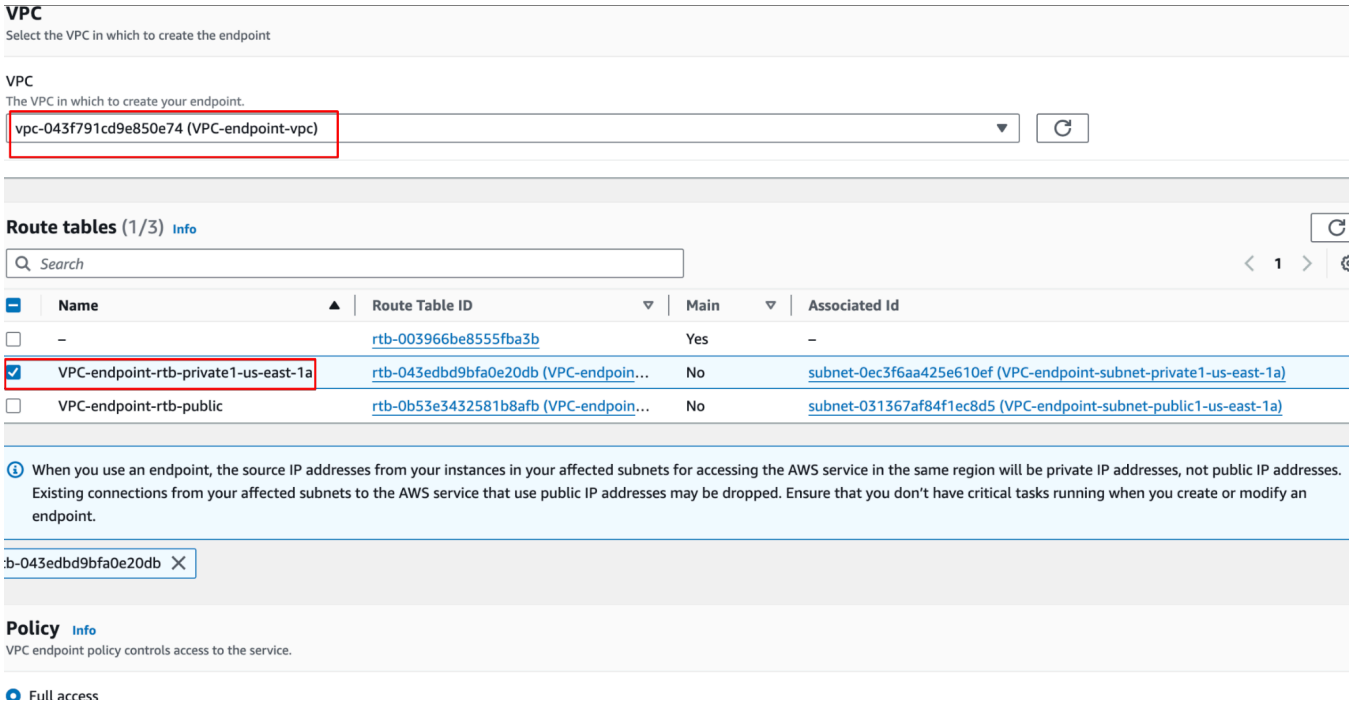
Go to the VPC console, select **Endpoints** from drop down menu and click on create Endpoint



10. Enter configuration details:
    a. Name the Endpoint (e.g s3GatewayEndpoint) to be created
    b. Under **Service category,** select *AWS services* and under **Services**, search for *s3* and select the s3 service endpoint.

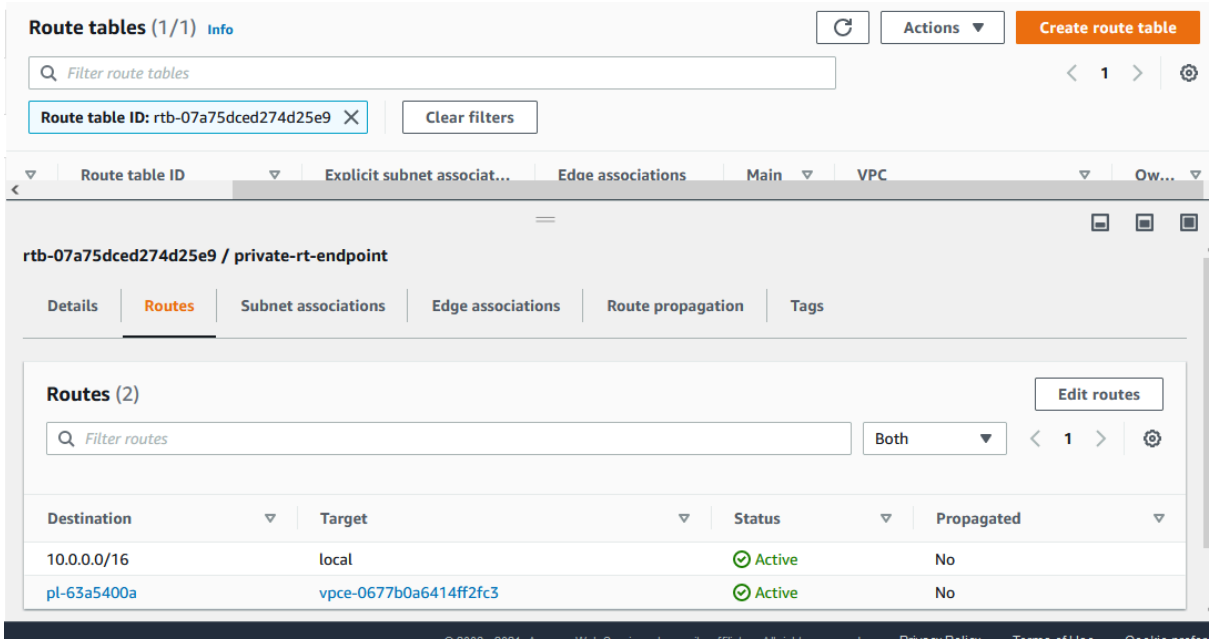


    c. Choose the vpc and select the private subnet route table since we will be accessing S3 from the private subnet.



11. Click on **create endpoint** and you will see the endpoint created in the console.

12. Next check the private subnet route table and you will notice that a route has been added for the VPC endpoint as shown below.



13. Finally try the command to access S3 and you will notice that you now have access to S3.

$ aws s3 ls

```
ec2-user@ip-10-0-1-98:~

suskan04@10230-LT-X0317 MINGW64 ~/Downloads
.comh -i "endpointkey.pem" ec2-user@ec2-3-14-246-131.us-east-2.compute.amazonaws.
Last login: Mon Sep 27 23:00:28 2021 from adsl-76-198-95-106.dsl.bkfd14.sbcglobal.net

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

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-0-82 ~]$ ssh -i bastion.pem ec2-user@10.0.1.98
Last login: Mon Sep 27 23:43:52 2021 from ip-10-0-0-82.us-east-2.compute.internal

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

https://aws.amazon.com/amazon-linux-2/
11 package(s) needed for security, out of 35 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-10-0-1-98 ~]$ aws s3 ls
2021-08-09 16:43:25 amazon-connect-8c32434d8a62
2021-08-09 10:55:35 amazon-connect-f2604b5e259c
2021-05-06 04:04:05 aws-application-discovery-service-6cku1wlkpsr0ns8r6g8ldtg43
2021-08-27 19:43:40 aws-cloudtrail-logs-186433656069-09cc2ce6
2021-03-30 13:03:59 aws-glue-scripts-186433656069-us-east-2
2021-03-30 13:04:00 aws-glue-temporary-186433656069-us-east-2
2021-04-09 07:21:33 aws-logs-186433656069-us-east-2
2021-08-09 11:02:05 catchupbucket
2021-08-06 09:25:02 central-logging-bucket123
2021-08-09 10:55:29 cf-templates-n4mkzpvylu80-us-east-1
2021-03-05 14:11:17 cf-templates-n4mkzpvylu80-us-east-2
2021-06-13 16:32:46 cf-templates-n4mkzpvylu80-us-west-2
2021-08-09 10:55:36 cloudtrail-awslogs-186433656069-soe1vou9-isengard-do-not-delete
2021-03-05 14:39:26 config-bucket-186433656069
```

Now you can see all the buckets are visible from the private server. That is because you created a gateway endpoint