# VPC_Endpoints: -

**Problem Statement:**

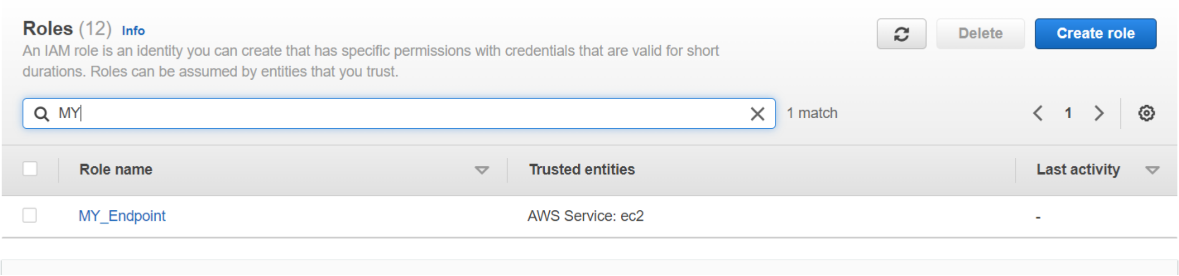
Working for an organization, you are required to provide them a safe and secure environment for the deployment of their resources. They might require different types of connectivity.

Implement the following to fulfill the requirements of the company. Tasks To Be Performed:

1. Create a VPC endpoint for a S3 bucket of your choice for secure access to the files.

**Procedure**: -

- Create the VPC and a public instance and the private instance.
- Search for Iam and Click on role and create role, select the AWS service, and select the EC2.
- Search for s3 and select the s3. In the permission policies search for s3 and choose the option as AmazonS3FullAccess. Click on next and give the name for the role and click on create role. Therefore, the role is created.



Roles (12) Info

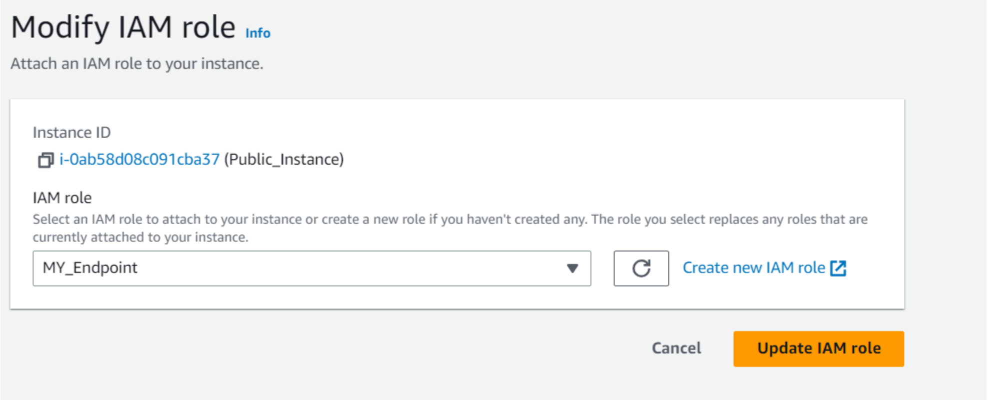
An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

MY

1 match

| Role name | Trusted entities | Last activity |
|---|---|---|
| MY_Endpoint | AWS Service: ec2 | - |

- Now select the Public_Instance and click on actions>>security>>Modify Iam role.
- Choose the IAM role as MY_Endpoint and Update IAM role.



Modify IAM role Info

Attach an IAM role to your instance.

Instance ID

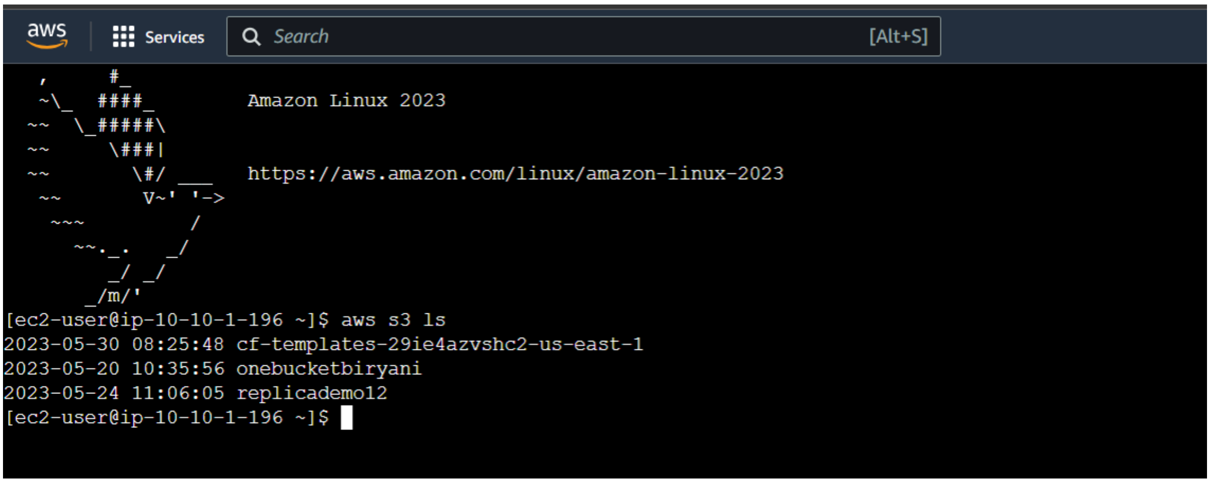
i-0ab58d08c091cba37 (Public_Instance)

IAM role

Select an IAM role to attach to your instance or create a new role if you haven't created any. The role you select replaces any roles that are currently attached to your instance.

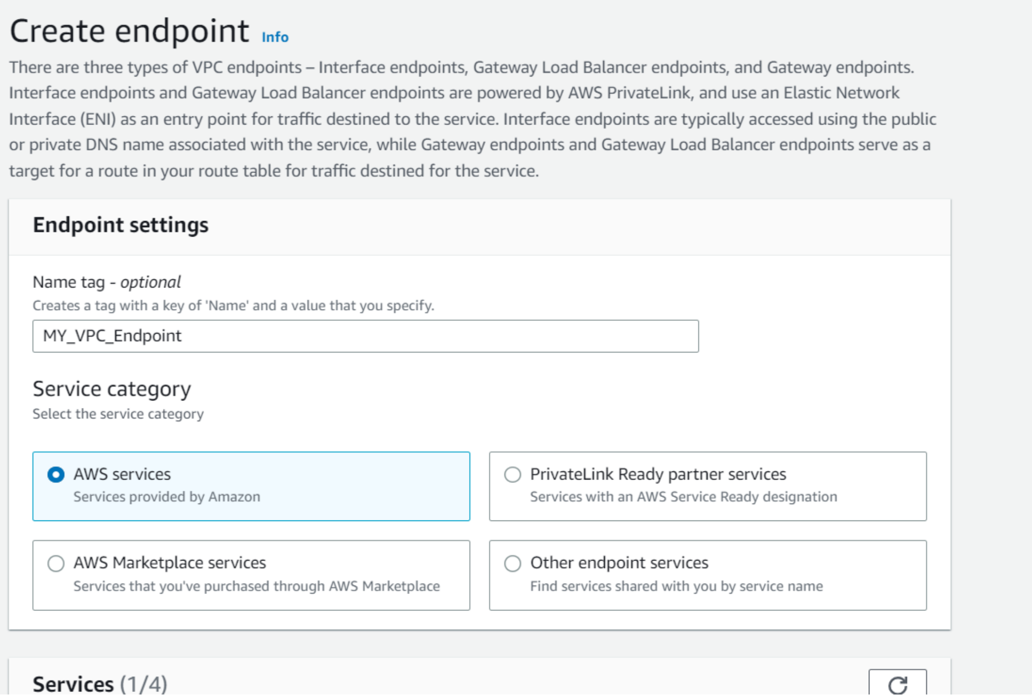
MY_Endpoint

- Connect the Public instance and open the command prompt.
- Run the following command.
  - ➢ aws s3 ls
- You will see that you are able to access the s3. Your will see the list of s3 buckets created.



```
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
[ec2-user@ip-10-10-1-196 ~]$ aws s3 ls
2023-05-30 08:25:48 cf-templates-29ie4azvshc2-us-east-1
2023-05-20 10:35:56 onebucketbiryani
2023-05-24 11:06:05 replicademo12
[ec2-user@ip-10-10-1-196 ~]$
```

- **Conclusion:** We can access the public instance with **IAM Role.** No Endpont is needed.
- Now we will try to access the s3 bucket with the private instance. For this we need two things.
  - ➢ IAM Role
  - ➢ VPC endpoint
- Therefore, we need to create the endpoint. Goto VPC>>Endpoint>>create Endpoint.



Create endpoint Info

There are three types of VPC endpoints – Interface endpoints, Gateway Load Balancer endpoints, and Gateway endpoints. Interface endpoints and Gateway Load Balancer endpoints are powered by AWS PrivateLink, and use an Elastic Network Interface (ENI) as an entry point for traffic destined to the service. Interface endpoints are typically accessed using the public or private DNS name associated with the service, while Gateway endpoints and Gateway Load Balancer endpoints serve as a target for a route in your route table for traffic destined for the service.

Endpoint settings

Name tag - *optional*
Creates a tag with a key of 'Name' and a value that you specify.
MY_VPC_Endpoint

Service category
Select the service category

● AWS services
Services provided by Amazon

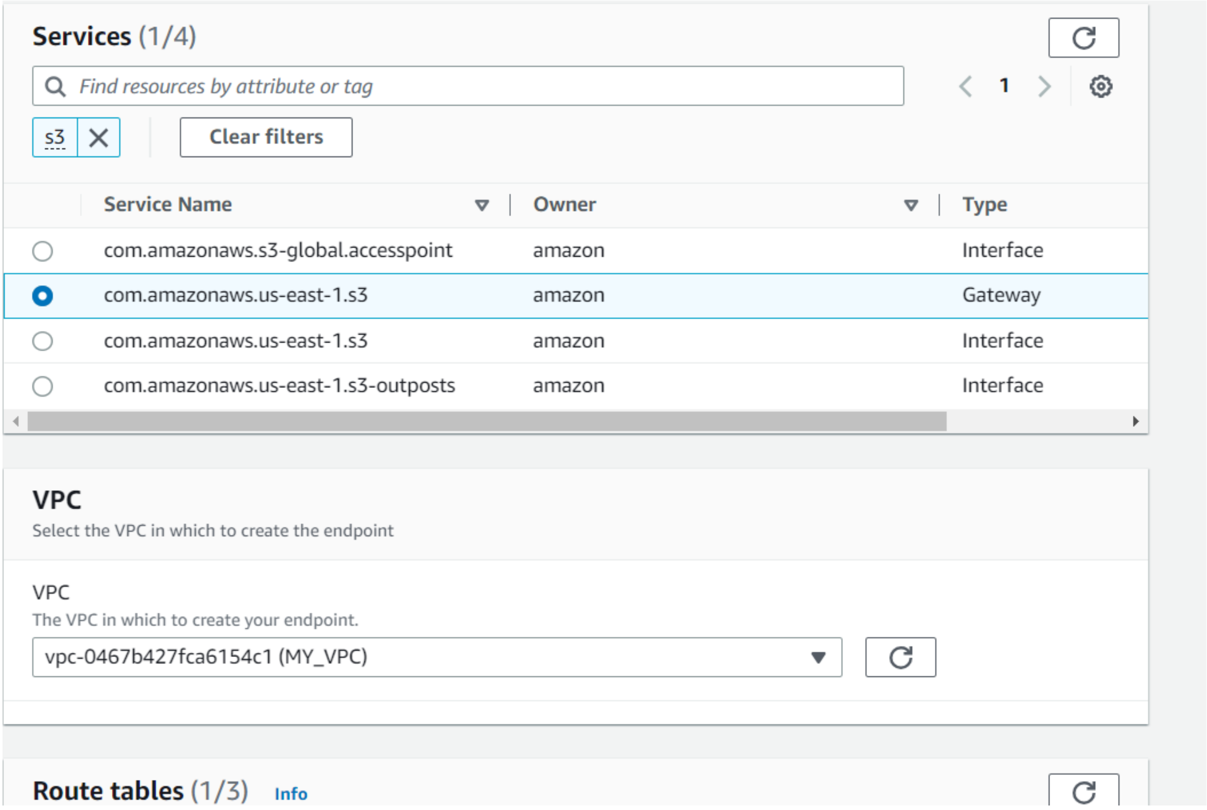
○ PrivateLink Ready partner services
Services with an AWS Service Ready designation

○ AWS Marketplace services
Services that you've purchased through AWS Marketplace

○ Other endpoint services
Find services shared with you by service name

Services (1/4)

- Simply create on endpoint.



**Services** (1/4)

Find resources by attribute or tag

s3 ✕ | Clear filters

|   | Service Name | Owner | Type |
|---|---|---|---|
| ○ | com.amazonaws.s3-global.accesspoint | amazon | Interface |
| ● | com.amazonaws.us-east-1.s3 | amazon | Gateway |
| ○ | com.amazonaws.us-east-1.s3 | amazon | Interface |
| ○ | com.amazonaws.us-east-1.s3-outposts | amazon | Interface |

**VPC**

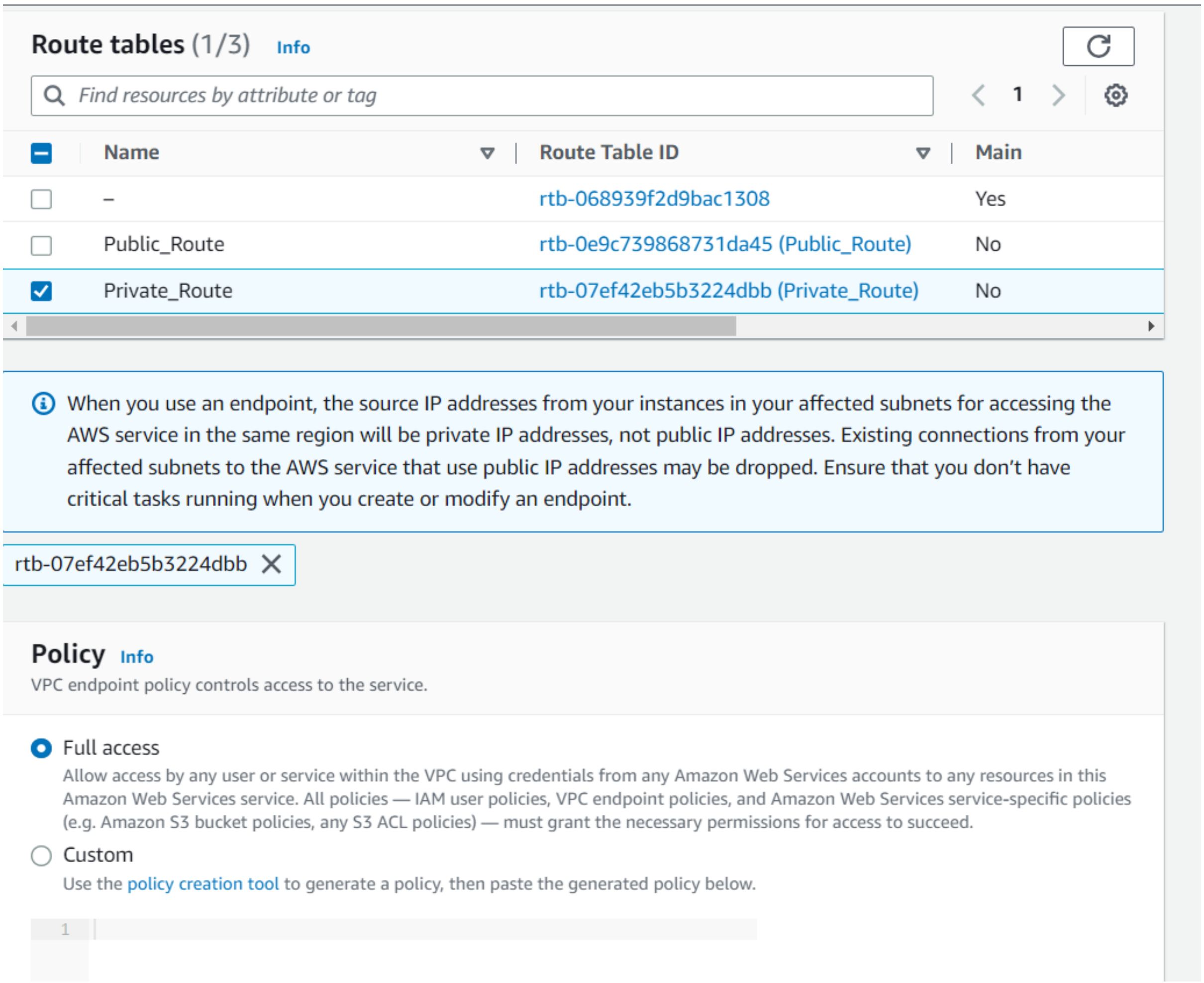
Select the VPC in which to create the endpoint

VPC

The VPC in which to create your endpoint.

vpc-0467b427fca6154c1 (MY_VPC)

**Route tables** (1/3) Info



**Route tables** (1/3) Info

Find resources by attribute or tag

|   | Name | Route Table ID | Main |
|---|---|---|---|
| □ | – | rtb-068939f2d9bac1308 | Yes |
| □ | Public_Route | rtb-0e9c739868731da45 (Public_Route) | No |
| ☑ | Private_Route | rtb-07ef42eb5b3224dbb (Private_Route) | No |

When you use an endpoint, the source IP addresses from your instances in your affected subnets for accessing the AWS service in the same region will be private IP addresses, not public IP addresses. Existing connections from your affected subnets to the AWS service that use public IP addresses may be dropped. Ensure that you don't have critical tasks running when you create or modify an endpoint.

rtb-07ef42eb5b3224dbb ✕

**Policy** Info

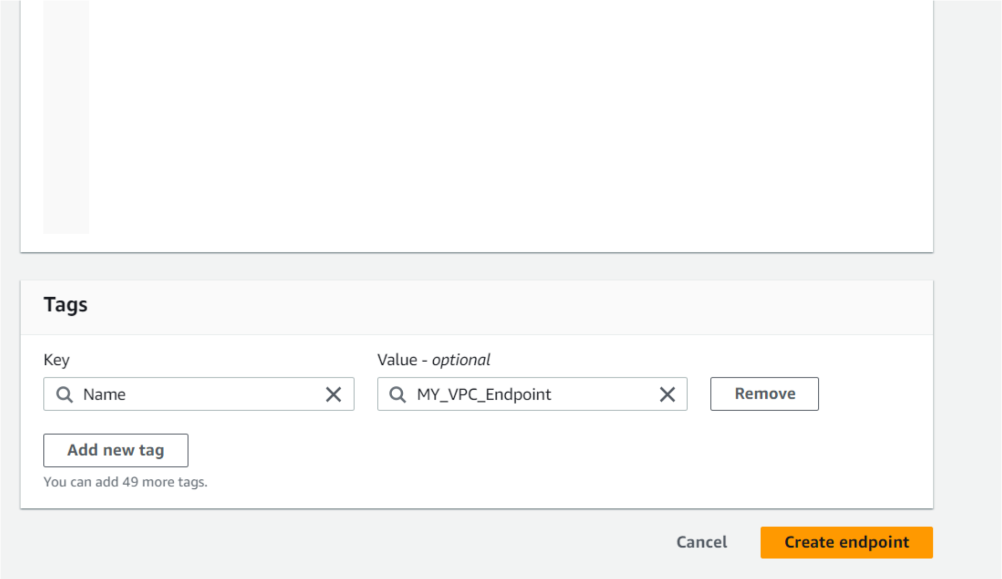
VPC endpoint policy controls access to the service.

● Full access

Allow access by any user or service within the VPC using credentials from any Amazon Web Services accounts to any resources in this Amazon Web Services service. All policies — IAM user policies, VPC endpoint policies, and Amazon Web Services service-specific policies (e.g. Amazon S3 bucket policies, any S3 ACL policies) — must grant the necessary permissions for access to succeed.

○ Custom

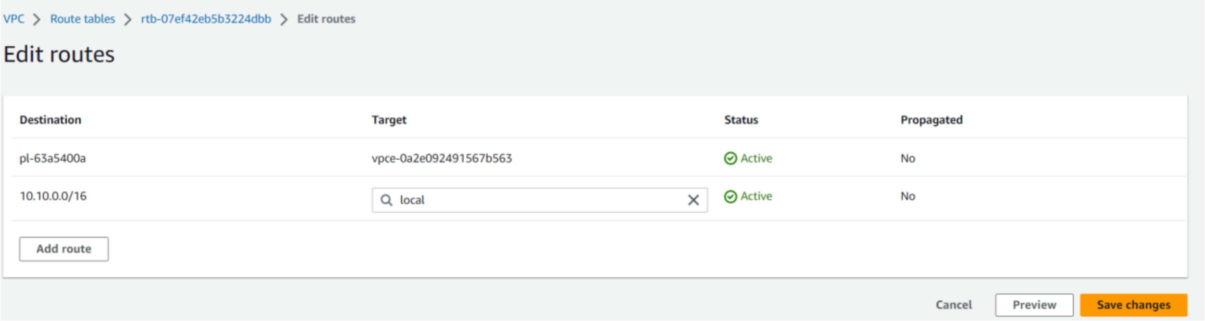
Use the policy creation tool to generate a policy, then paste the generated policy below.



Tags

| Key | Value - *optional* |
|---|---|
| Name | MY_VPC_Endpoint |

- Now if we go to Route tables>>Private_Route>>Routes>>edit routes.
- You will see the the MY_VPC_Endpoint will automatically appear.

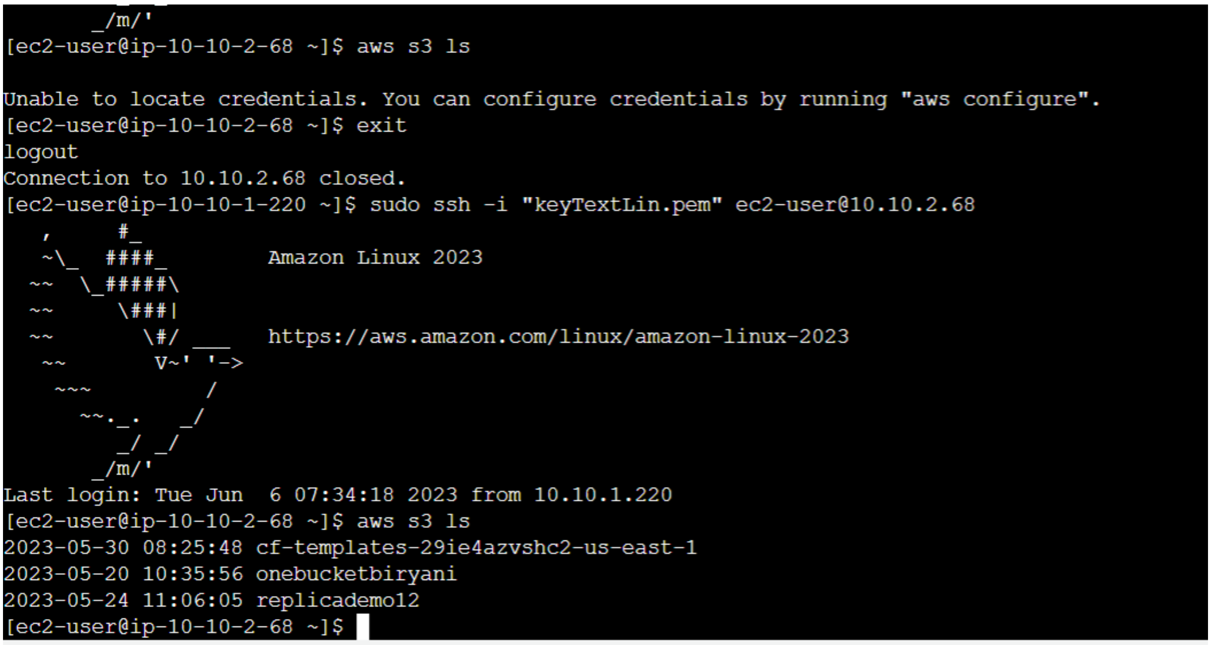


VPC > Route tables > rtb-07ef42eb5b3224dbb > Edit routes

Edit routes

| Destination | Target | Status | Propagated |
|---|---|---|---|
| pl-63a5400a | vpce-0a2e092491567b563 | Active | No |
| 10.10.0.0/16 | local | Active | No |

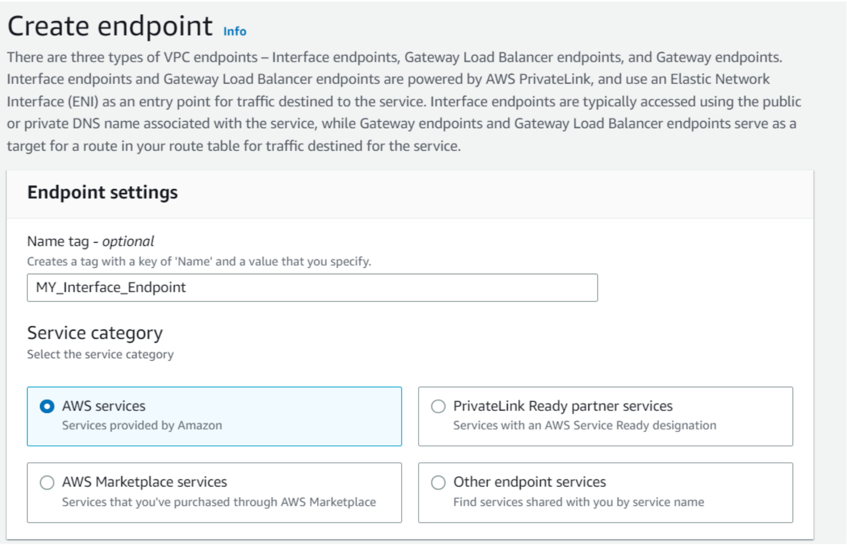
- When we create the endpoint the route table automatically targets the vpc endpoint.
- Now let us access the private instance from the public instance.
  - sudo nano keyTextLin.pem (create a pem file).
  - ls (to check the file)
  - sudo chmod 400 keyTextLin.pem
  - sudo ssh -i "keyTextLin.pem" ec2-user@10.10.2.68
- Goto Private_Instance>>actions>>security>>Modify IAM role. Select the MY_Endpoint and update IAM role.
- Now on the command prompt logout and login the private_instance.
  - exit
  - sudo ssh -i "keyTextLin.pem" ec2-user@10.10.2.68
  - aws s3 ls
- Now you will see that you will be able to access the s3 bucket through private_Instance with the help of **IAM role and VPC Endpoint.**



```
       _/m/'
[ec2-user@ip-10-10-2-68 ~]$ aws s3 ls

Unable to locate credentials. You can configure credentials by running "aws configure".
[ec2-user@ip-10-10-2-68 ~]$ exit
logout
Connection to 10.10.2.68 closed.
[ec2-user@ip-10-10-1-220 ~]$ sudo ssh -i "keyTextLin.pem" ec2-user@10.10.2.68
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Tue Jun  6 07:34:18 2023 from 10.10.1.220
[ec2-user@ip-10-10-2-68 ~]$ aws s3 ls
2023-05-30 08:25:48 cf-templates-29ie4azvshc2-us-east-1
2023-05-20 10:35:56 onebucketbiryani
2023-05-24 11:06:05 replicademo12
[ec2-user@ip-10-10-2-68 ~]$ 
```

- The above example was for **Gateway endpoints**
- Now we will performe for the **interface endpoints.**
- Let us create the new endpoint. Gotto Endpoint>>create endpoint.



Create endpoint Info

There are three types of VPC endpoints – Interface endpoints, Gateway Load Balancer endpoints, and Gateway endpoints. Interface endpoints and Gateway Load Balancer endpoints are powered by AWS PrivateLink, and use an Elastic Network Interface (ENI) as an entry point for traffic destined to the service. Interface endpoints are typically accessed using the public or private DNS name associated with the service, while Gateway endpoints and Gateway Load Balancer endpoints serve as a target for a route in your route table for traffic destined for the service.

Endpoint settings

Name tag - *optional*
Creates a tag with a key of 'Name' and a value that you specify.
MY_Interface_Endpoint

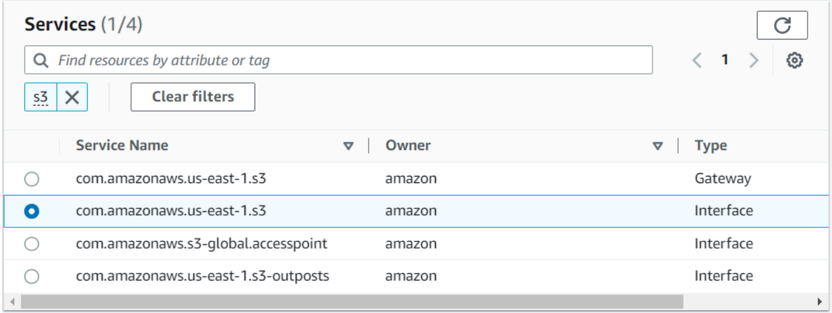
Service category
Select the service category

● AWS services
Services provided by Amazon

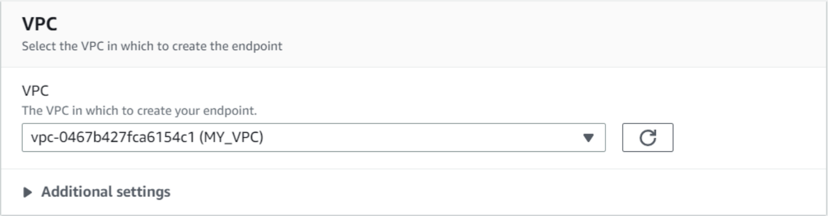
○ PrivateLink Ready partner services
Services with an AWS Service Ready designation

○ AWS Marketplace services
Services that you've purchased through AWS Marketplace

○ Other endpoint services
Find services shared with you by service name

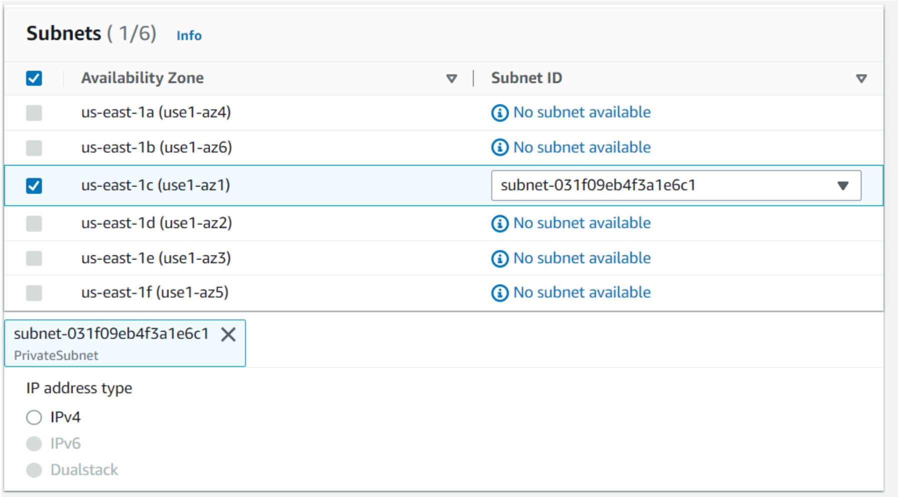


| | Service Name | Owner | Type |
|---|---|---|---|
| ○ | com.amazonaws.us-east-1.s3 | amazon | Gateway |
| ● | com.amazonaws.us-east-1.s3 | amazon | Interface |
| ○ | com.amazonaws.s3-global.accesspoint | amazon | Interface |
| ○ | com.amazonaws.us-east-1.s3-outposts | amazon | Interface |



VPC
Select the VPC in which to create the endpoint

VPC
The VPC in which to create your endpoint.
vpc-0467b427fca6154c1 (MY_VPC)



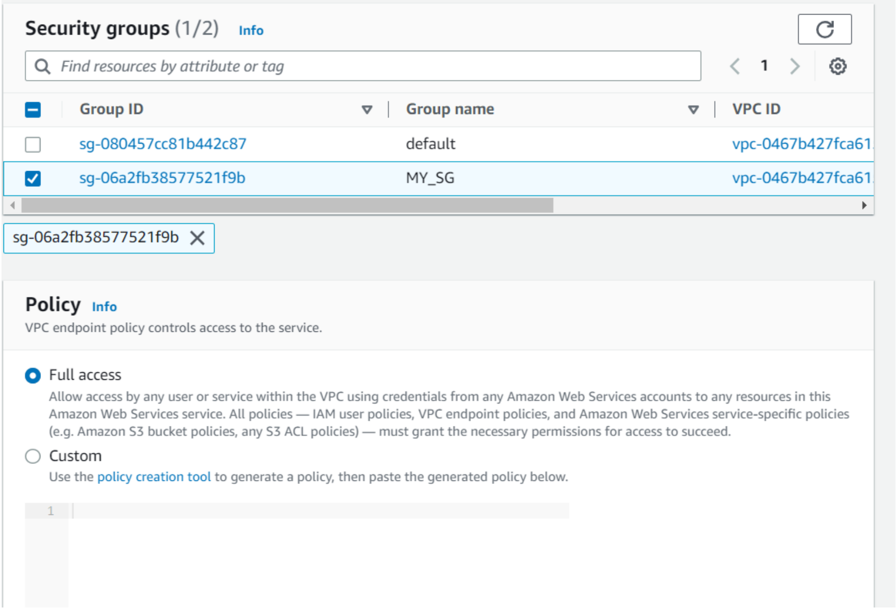
**Subnets** ( 1/6) Info

| ☑ | Availability Zone | Subnet ID |
|---|---|---|
| □ | us-east-1a (use1-az4) | ⓘ No subnet available |
| □ | us-east-1b (use1-az6) | ⓘ No subnet available |
| ☑ | us-east-1c (use1-az1) | subnet-031f09eb4f3a1e6c1 ▼ |
| □ | us-east-1d (use1-az2) | ⓘ No subnet available |
| □ | us-east-1e (use1-az3) | ⓘ No subnet available |
| □ | us-east-1f (use1-az5) | ⓘ No subnet available |

subnet-031f09eb4f3a1e6c1 ✕
PrivateSubnet

IP address type

○ IPv4
○ IPv6
○ Dualstack



**Security groups** (1/2) Info

Find resources by attribute or tag

| ▬ | Group ID | Group name | VPC ID |
|---|---|---|---|
| □ | sg-080457cc81b442c87 | default | vpc-0467b427fca61 |
| ☑ | sg-06a2fb38577521f9b | MY_SG | vpc-0467b427fca61 |

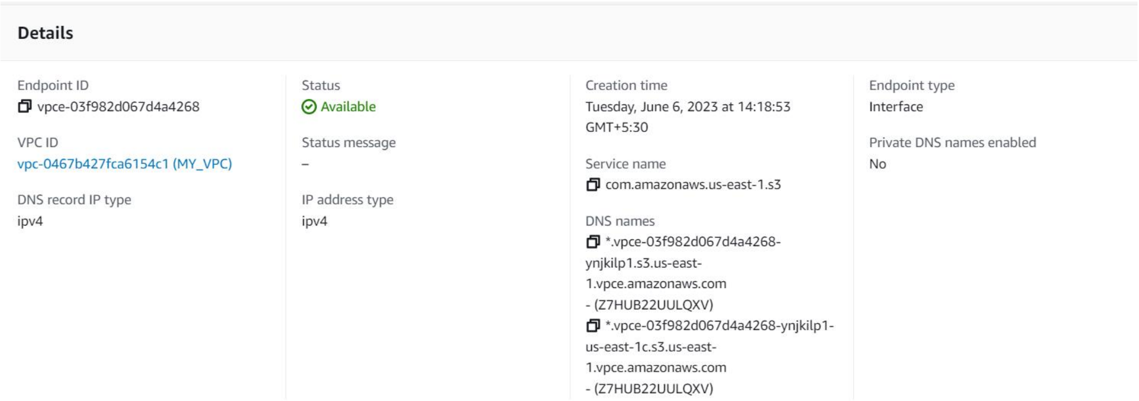
sg-06a2fb38577521f9b ✕

**Policy** Info
VPC endpoint policy controls access to the service.

● Full access
Allow access by any user or service within the VPC using credentials from any Amazon Web Services accounts to any resources in this Amazon Web Services service. All policies — IAM user policies, VPC endpoint policies, and Amazon Web Services service-specific policies (e.g. Amazon S3 bucket policies, any S3 ACL policies) — must grant the necessary permissions for access to succeed.

○ Custom
Use the policy creation tool to generate a policy, then paste the generated policy below.

- Click on create end point.
- Logout and login from the private machine.
- Now we should be able to access the s3 bucket using the dns.
- Run the following command
- aws s3 ls --endpoint-url http://vpce-03f982d067d4a4268-ynjkilp1.s3.us-east-1.vpce.amazonaws.com



**Details**

Endpoint ID
vpce-03f982d067d4a4268

VPC ID
vpc-0467b427fca6154c1 (MY_VPC)

DNS record IP type
ipv4

Status
✓ Available

Status message
–

IP address type
ipv4

Creation time
Tuesday, June 6, 2023 at 14:18:53 GMT+5:30

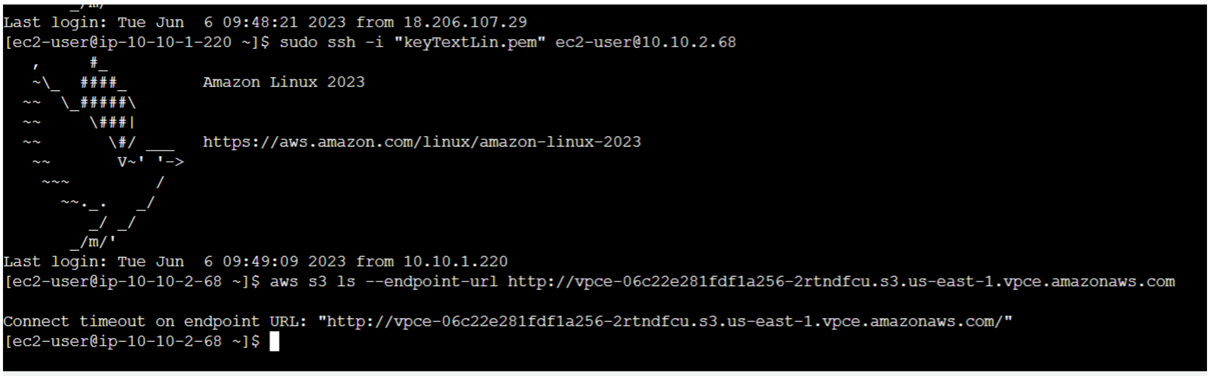
Service name
com.amazonaws.us-east-1.s3

DNS names
*.vpce-03f982d067d4a4268-ynjkilp1.s3.us-east-1.vpce.amazonaws.com - (Z7HUB22UULQXV)
*.vpce-03f982d067d4a4268-ynjkilp1-us-east-1c.s3.us-east-1.vpce.amazonaws.com - (Z7HUB22UULQXV)

Endpoint type
Interface

Private DNS names enabled
No

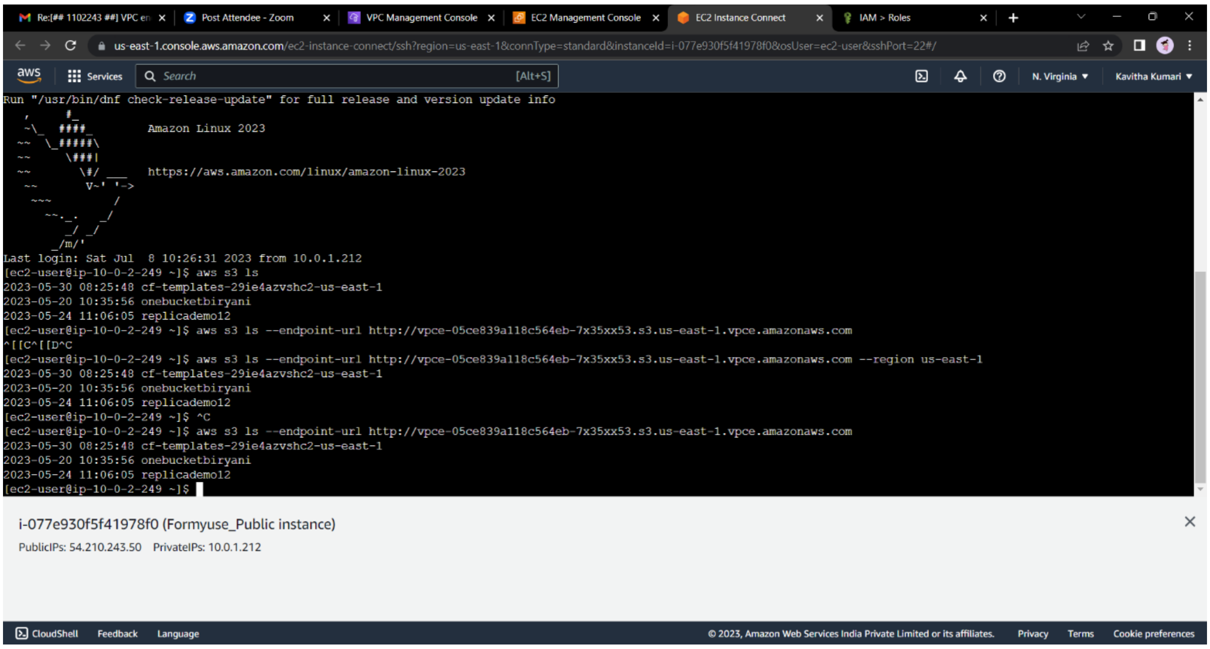
- aws s3 ls --endpoint-url http://vpce-03f982d067d4a4268-ynjkilp1-us-east-1c.s3.us-east-1.vpce.amazonaws.com



```
Last login: Tue Jun  6 09:48:21 2023 from 18.206.107.29
[ec2-user@ip-10-10-1-220 ~]$ sudo ssh -i "keyTextLin.pem" ec2-user@10.10.2.68
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Tue Jun  6 09:49:09 2023 from 10.10.1.220
[ec2-user@ip-10-10-2-68 ~]$ aws s3 ls --endpoint-url http://vpce-06c22e281fdf1a256-2rtndfcu.s3.us-east-1.vpce.amazonaws.com

Connect timeout on endpoint URL: "http://vpce-06c22e281fdf1a256-2rtndfcu.s3.us-east-1.vpce.amazonaws.com/"
[ec2-user@ip-10-10-2-68 ~]$ 
```

**Important note:** WE also need to provide the http rule in the private instance because we are accessing the s3 bucket through the Private instance.


Re:[## 1102243 ##] VPC en
Post Attendee - Zoom
VPC Management Console
EC2 Management Console
EC2 Instance Connect
IAM > Roles
us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?region=us-east-1&connType=standard&instanceId=i-077e930f5f41978f0&osUser=ec2-user&sshPort=22#/
aws
Services
Search
[Alt+S]
N. Virginia
Kavitha Kumari
CloudShell
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences

```
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Sat Jul  8 10:26:31 2023 from 10.0.1.212
[ec2-user@ip-10-0-2-249 ~]$ aws s3 ls
2023-05-30 08:25:48 cf-templates-29ie4azvshc2-us-east-1
2023-05-20 10:35:56 onebucketbiryani
2023-05-24 11:06:05 replicademo12
[ec2-user@ip-10-0-2-249 ~]$ aws s3 ls --endpoint-url http://vpce-05ce839a118c564eb-7x35xx53.s3.us-east-1.vpce.amazonaws.com
^[[C^[[D^C
[ec2-user@ip-10-0-2-249 ~]$ aws s3 ls --endpoint-url http://vpce-05ce839a118c564eb-7x35xx53.s3.us-east-1.vpce.amazonaws.com --region us-east-1
2023-05-30 08:25:48 cf-templates-29ie4azvshc2-us-east-1
2023-05-20 10:35:56 onebucketbiryani
2023-05-24 11:06:05 replicademo12
[ec2-user@ip-10-0-2-249 ~]$ ^C
[ec2-user@ip-10-0-2-249 ~]$ aws s3 ls --endpoint-url http://vpce-05ce839a118c564eb-7x35xx53.s3.us-east-1.vpce.amazonaws.com
2023-05-30 08:25:48 cf-templates-29ie4azvshc2-us-east-1
2023-05-20 10:35:56 onebucketbiryani
2023-05-24 11:06:05 replicademo12
[ec2-user@ip-10-0-2-249 ~]$ 
```

i-077e930f5f41978f0 (Formyuse_Public instance)

PublicIPs: 54.210.243.50 PrivateIPs: 10.0.1.212

--------End---------