Module 5: VPC Endpoints Assignment

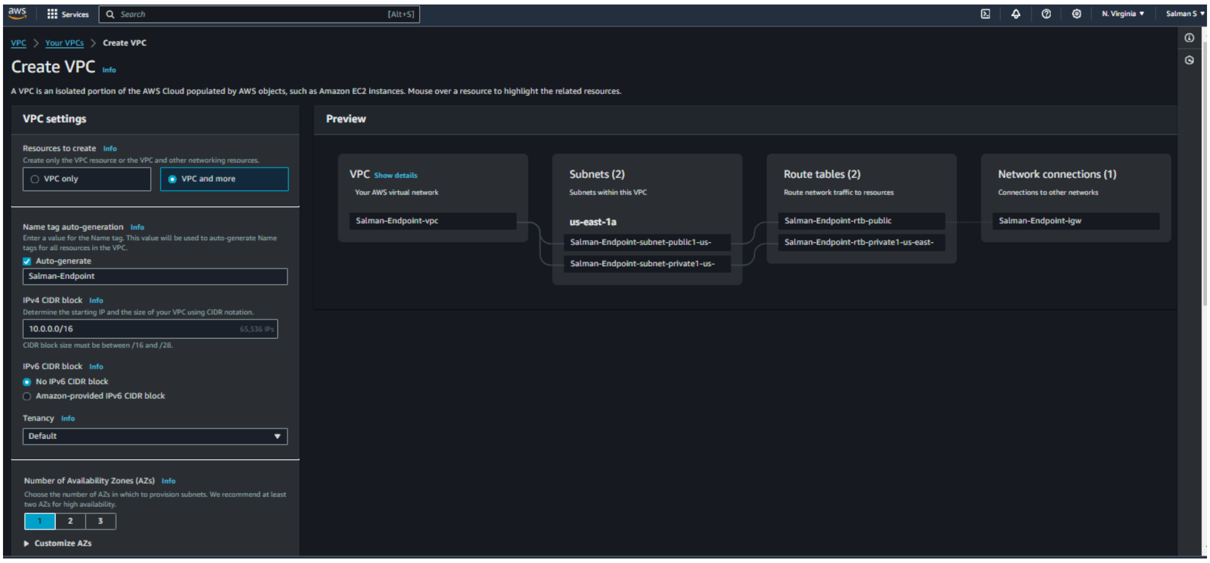
Problem Statement:

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.

1. Creating 1 VPC and 2 subnets and 1 private and 1 public



Create VPC Info

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances. Mouse over a resource to highlight the related resources.

VPC settings

Resources to create Info
Create only the VPC resource or the VPC and other networking resources.
○ VPC only ● VPC and more

Name tag auto-generation Info
Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.
☑ Auto-generate
Salman-Endpoint

IPv4 CIDR block Info
Determine the starting IP and the size of your VPC using CIDR notation.
10.0.0.0/16 65,536 IPs
CIDR block size must be between /16 and /28.

IPv6 CIDR block Info
● No IPv6 CIDR block
○ Amazon-provided IPv6 CIDR block

Tenancy Info
Default ▾

Number of Availability Zones (AZs) Info
Choose the number of AZs in which to provision subnets. We recommend at least two AZs for high availability.
[1] 2 3

▸ Customize AZs

Preview

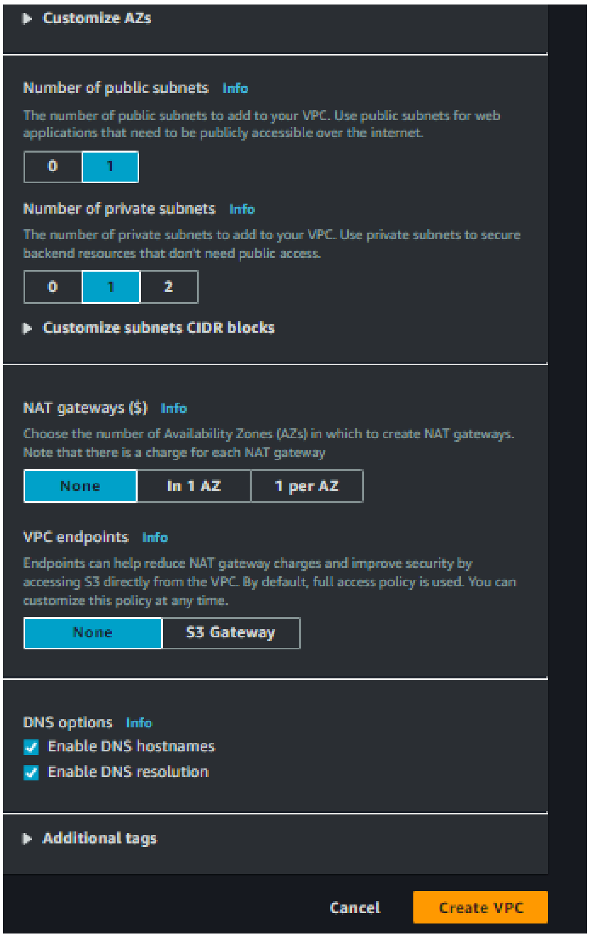
VPC Show details
Your AWS virtual network
Salman-Endpoint-vpc

Subnets (2)
Subnets within this VPC
us-east-1a
Salman-Endpoint-subnet-public1-us-
Salman-Endpoint-subnet-private1-us-

Route tables (2)
Route network traffic to resources
Salman-Endpoint-rtb-public
Salman-Endpoint-rtb-private1-us-east-

Network connections (1)
Connections to other networks
Salman-Endpoint-igw

2. Here we are not selecting endpoint in upcoming we are configure



▶ Customize AZs

Number of public subnets Info

The number of public subnets to add to your VPC. Use public subnets for web applications that need to be publicly accessible over the internet.

Number of private subnets Info

The number of private subnets to add to your VPC. Use private subnets to secure backend resources that don't need public access.

▶ Customize subnets CIDR blocks

NAT gateways ($) Info

Choose the number of Availability Zones (AZs) in which to create NAT gateways. Note that there is a charge for each NAT gateway

VPC endpoints Info

Endpoints can help reduce NAT gateway charges and improve security by accessing S3 directly from the VPC. By default, full access policy is used. You can customize this policy at any time.

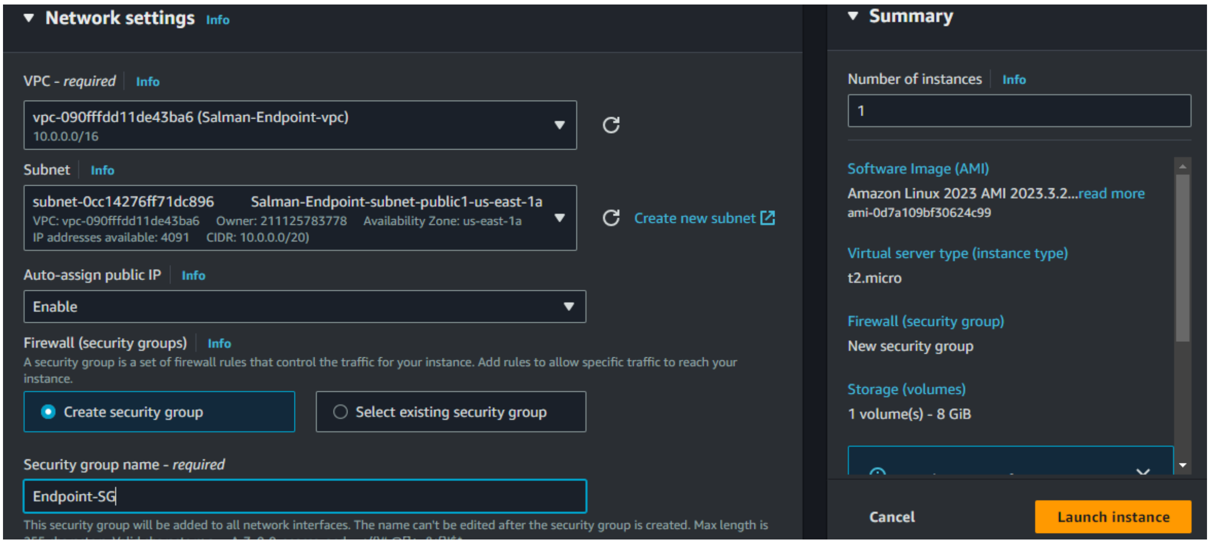
DNS options Info

☑ Enable DNS hostnames

☑ Enable DNS resolution

▶ Additional tags

3. Launching ec2 instances and configuring network settings select created VPC and Public subnet and Create Security groups



▼ Network settings Info

VPC - *required* Info

vpc-090fffdd11de43ba6 (Salman-Endpoint-vpc)
10.0.0.0/16

Subnet Info

subnet-0cc14276ff71dc896 Salman-Endpoint-subnet-public1-us-east-1a
VPC: vpc-090fffdd11de43ba6 Owner: 211125783778 Availability Zone: us-east-1a
IP addresses available: 4091 CIDR: 10.0.0.0/20)

Auto-assign public IP Info

Enable

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

Security group name - *required*

Endpoint-SG

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is

▼ Summary

Number of instances Info

1

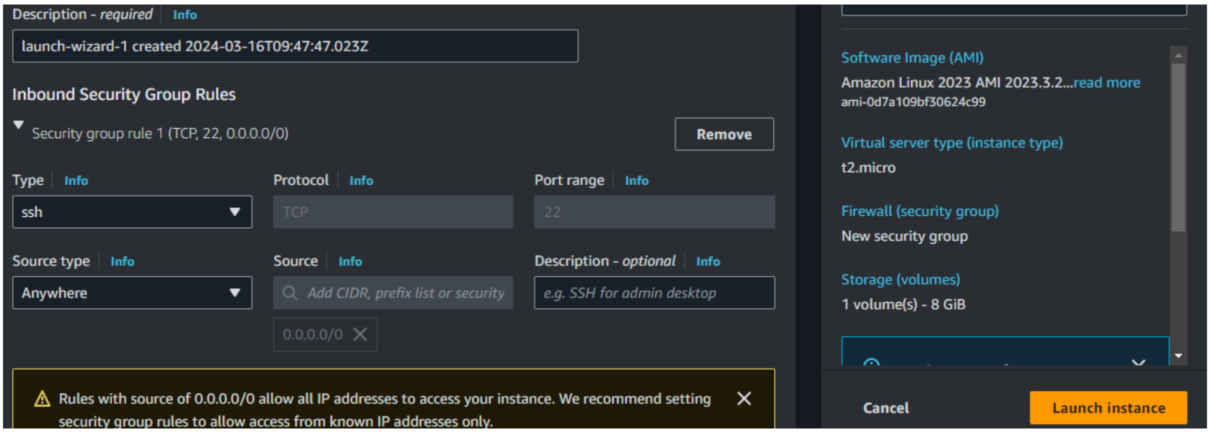
Software Image (AMI)
Amazon Linux 2023 AMI 2023.3.2...read more
ami-0d7a109bf30624c99

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

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

4. Inbound Traffic leave as default



Description - *required* Info
launch-wizard-1 created 2024-03-16T09:47:47.023Z

Inbound Security Group Rules

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0) Remove

Type: ssh
Protocol: TCP
Port range: 22
Source type: Anywhere
Source: *Add CIDR, prefix list or security* 0.0.0.0/0 ✕
Description - *optional*: *e.g. SSH for admin desktop*

⚠ 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.

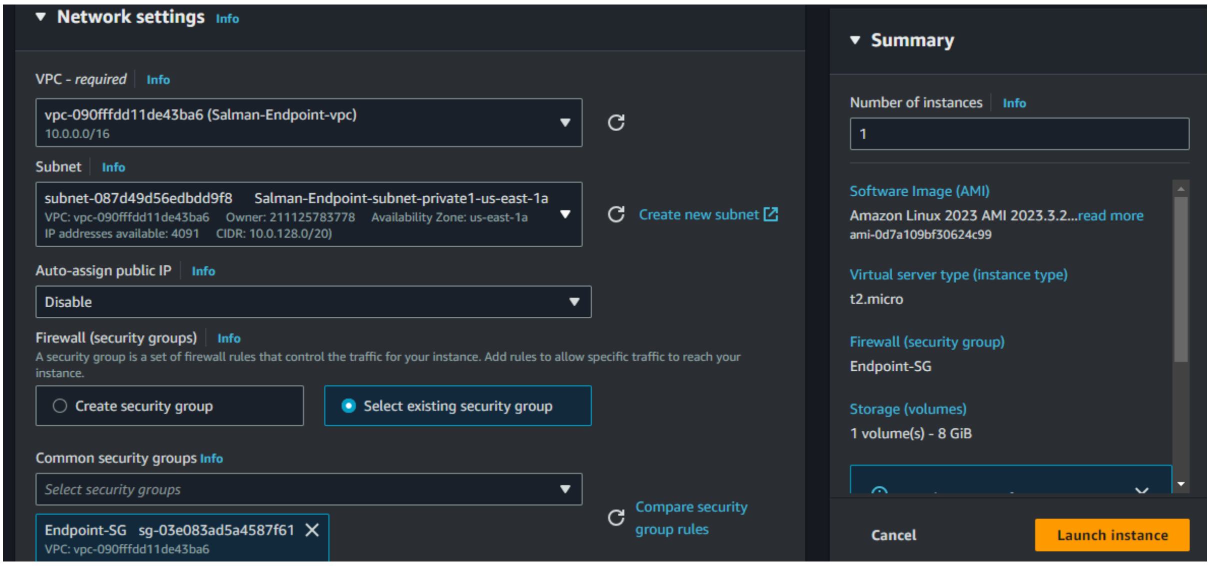
Software Image (AMI)
Amazon Linux 2023 AMI 2023.3.2...read more
ami-0d7a109bf30624c99

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

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

5. Launching Private EC2 Instances and Selecting Private Subnet and Launch



▼ Network settings Info

VPC - *required*: vpc-090fffdd11de43ba6 (Salman-Endpoint-vpc) 10.0.0.0/16

Subnet: subnet-087d49d56edbdd9f8 Salman-Endpoint-subnet-private1-us-east-1a
VPC: vpc-090fffdd11de43ba6 Owner: 211125783778 Availability Zone: us-east-1a
IP addresses available: 4091 CIDR: 10.0.128.0/20

Create new subnet

Auto-assign public IP: 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
Endpoint-SG sg-03e083ad5a4587f61 ✕
VPC: vpc-090fffdd11de43ba6

Compare security group rules

▼ Summary

Number of instances: 1

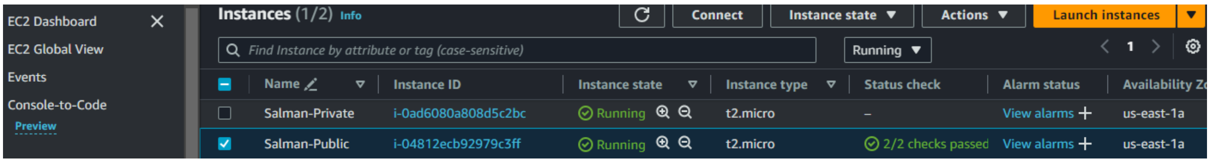
Software Image (AMI)
Amazon Linux 2023 AMI 2023.3.2...read more
ami-0d7a109bf30624c99

Virtual server type (instance type)
t2.micro

Firewall (security group)
Endpoint-SG

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

6. Select Public and Connect to SSH

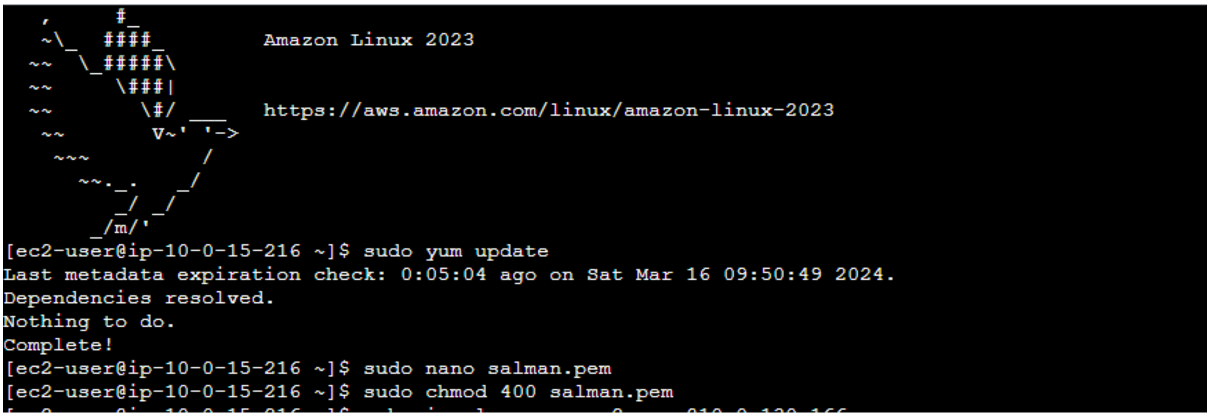


Instances (1/2) Info

Find Instance by attribute or tag (case-sensitive) Running

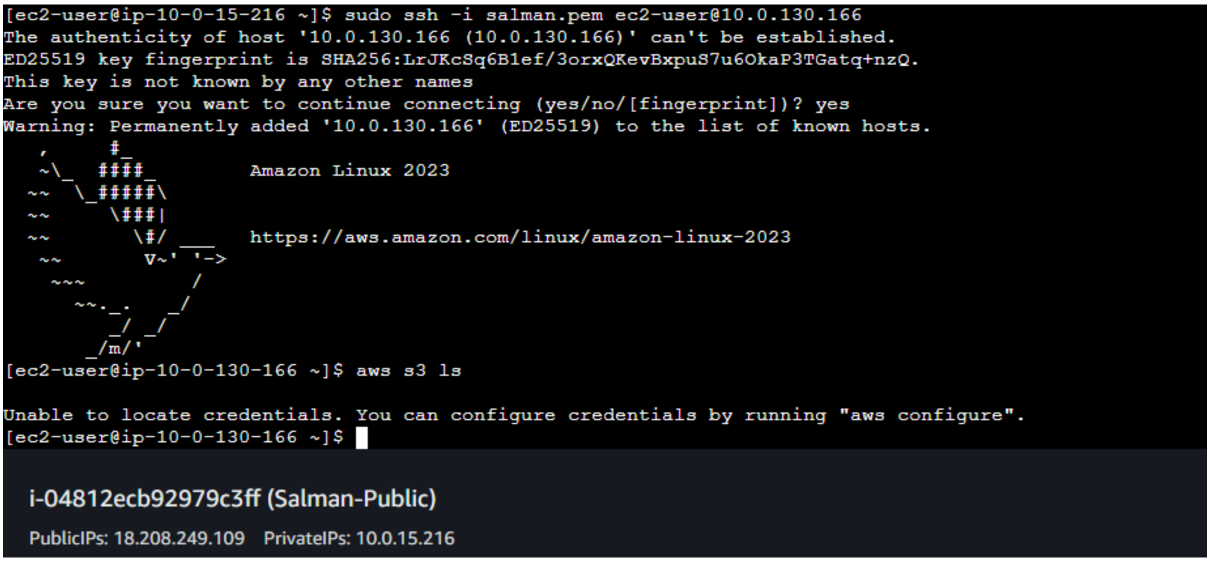
	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zo
□	Salman-Private	i-0ad6080a808d5c2bc	Running	t2.micro	–	View alarms +	us-east-1a
☑	Salman-Public	i-04812ecb92979c3ff	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a

7. Follow the commands to Connect another server



```
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
[ec2-user@ip-10-0-15-216 ~]$ sudo yum update
Last metadata expiration check: 0:05:04 ago on Sat Mar 16 09:50:49 2024.
Dependencies resolved.
Nothing to do.
Complete!
[ec2-user@ip-10-0-15-216 ~]$ sudo nano salman.pem
[ec2-user@ip-10-0-15-216 ~]$ sudo chmod 400 salman.pem
```

8. We Connected to Private Ec2 instances through Public EC2 and aws s3 ls not working



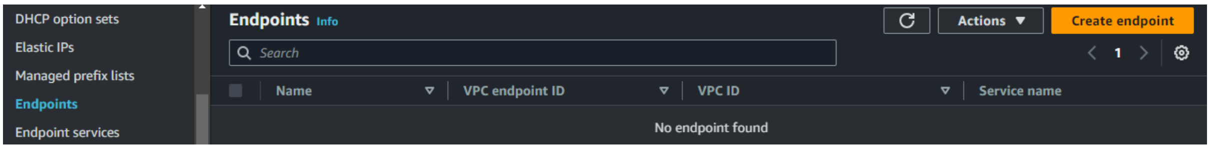
```
[ec2-user@ip-10-0-15-216 ~]$ sudo ssh -i salman.pem ec2-user@10.0.130.166
The authenticity of host '10.0.130.166 (10.0.130.166)' can't be established.
ED25519 key fingerprint is SHA256:LrJKcSq6B1ef/3orxQKevBxpuS7u6OkaP3TGatq+nzQ.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.130.166' (ED25519) to the list of known hosts.
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
[ec2-user@ip-10-0-130-166 ~]$ aws s3 ls

Unable to locate credentials. You can configure credentials by running "aws configure".
[ec2-user@ip-10-0-130-166 ~]$
```

i-04812ecb92979c3ff (Salman-Public)

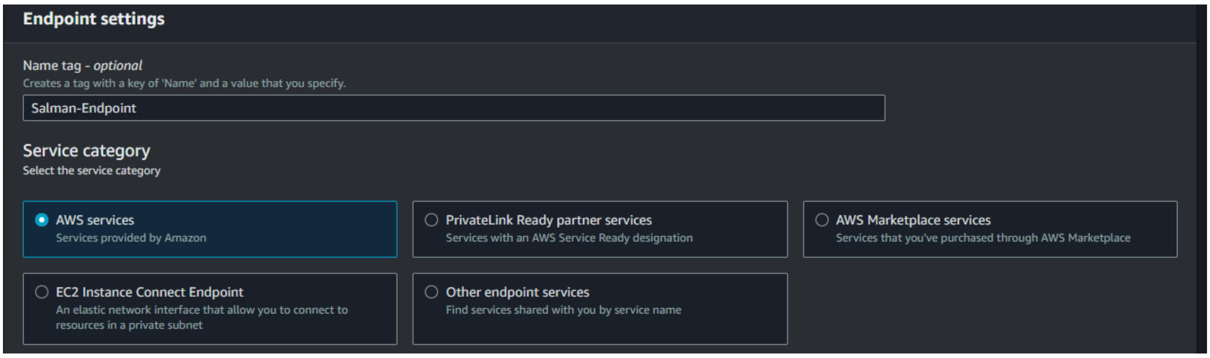
PublicIPs: 18.208.249.109 PrivateIPs: 10.0.15.216

9. Need to Create endpoints now



☐	Name	VPC endpoint ID	VPC ID	Service name
		No endpoint found		

10. Select AWS Service



Endpoint settings

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

Service category
Select the service category

● AWS services
Services provided by Amazon

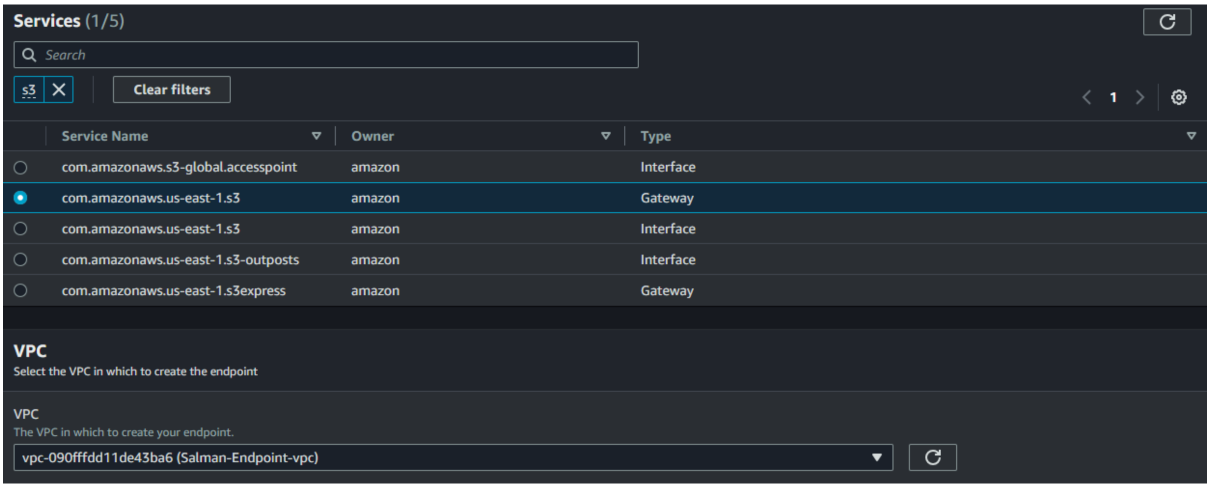
○ PrivateLink Ready partner services
Services with an AWS Service Ready designation

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

○ EC2 Instance Connect Endpoint
An elastic network interface that allow you to connect to resources in a private subnet

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

11. Services > Select Gateway Type

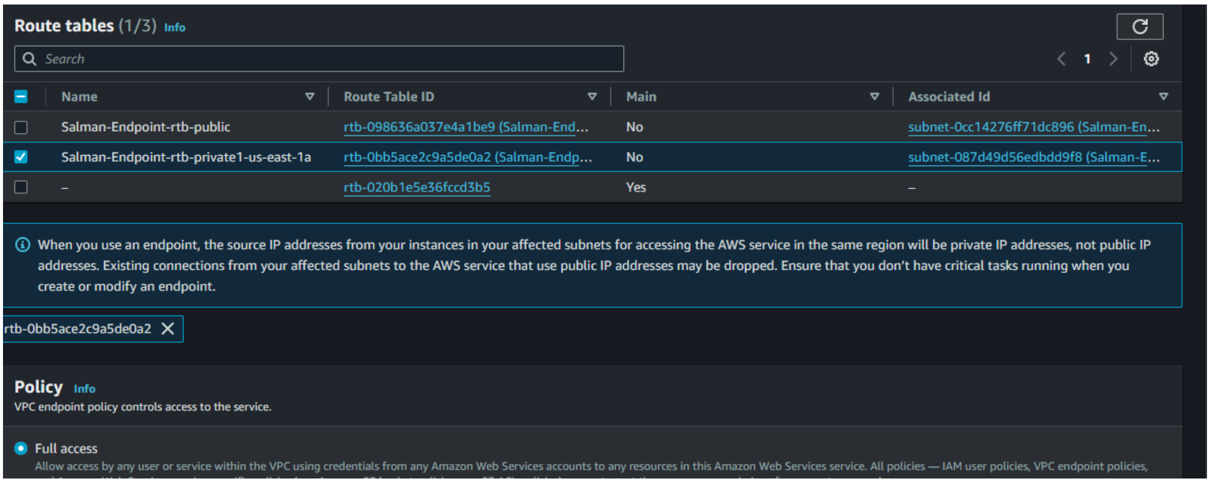


	Service Name	Owner	Type
○	com.amazonaws.s3-global.accesspoint	amazon	Interface
●	com.amazonaws.us-east-1.s3	amazon	Gateway
○	com.amazonaws.us-east-1.s3	amazon	Interface
○	com.amazonaws.us-east-1.s3-outposts	amazon	Interface
○	com.amazonaws.us-east-1.s3express	amazon	Gateway

VPC
Select the VPC in which to create the endpoint

VPC
The VPC in which to create your endpoint.
vpc-090fffdd11de43ba6 (Salman-Endpoint-vpc)

12. And Private RT Endpoint



Route tables (1/3) Info

☐	Name	Route Table ID	Main	Associated Id
☐	Salman-Endpoint-rtb-public	rtb-098636a037e4a1be9 (Salman-End...	No	subnet-0cc14276ff71dc896 (Salman-En...
☑	Salman-Endpoint-rtb-private1-us-east-1a	rtb-0bb5ace2c9a5de0a2 (Salman-Endp...	No	subnet-087d49d56edbdd9f8 (Salman-E...
☐	–	rtb-020b1e5e36fccd3b5	Yes	–

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-0bb5ace2c9a5de0a2 ✕

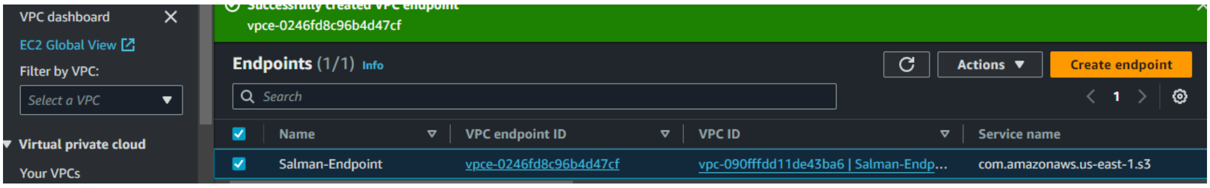
Policy Info

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,

13. Now Endpoint Created

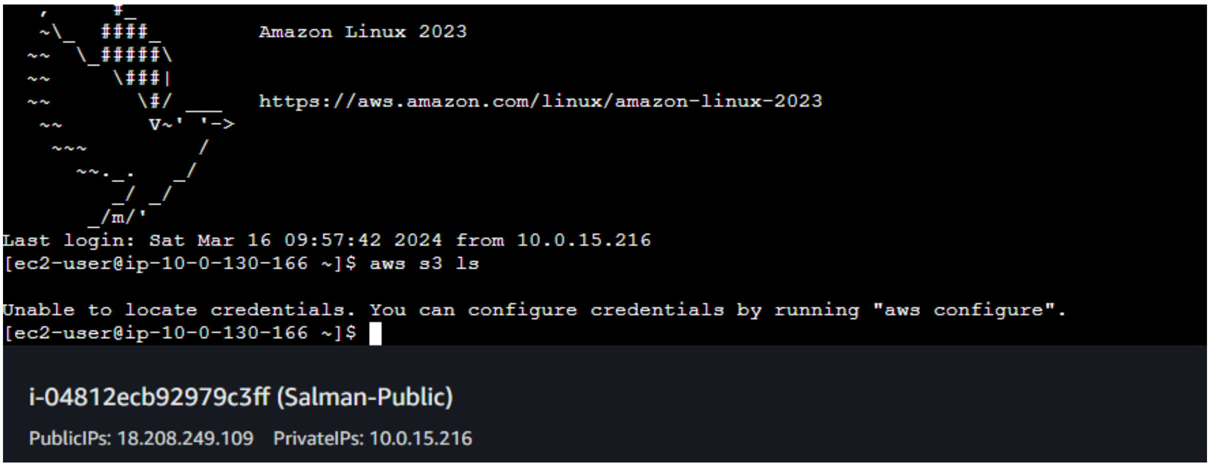


Successfully created VPC endpoint vpce-0246fd8c96b4d47cf

Endpoints (1/1) Info

☑	Name	VPC endpoint ID	VPC ID	Service name
☑	Salman-Endpoint	vpce-0246fd8c96b4d47cf	vpc-090fffdd11de43ba6 | Salman-Endp...	com.amazonaws.us-east-1.s3

14. Still Its not Working, Why Because we are not provide any Permission to EC2 and we are not add Role in IAM



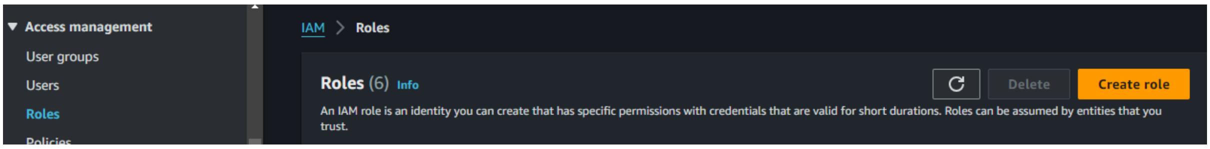
```
       ,     #_
    ~\_  ####_        Amazon Linux 2023
   ~~  \_#####\
   ~~     \###|
   ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
    ~~       V~' '->
     ~~~         /
       ~~._.   _/
          _/ _/
        _/m/'
Last login: Sat Mar 16 09:57:42 2024 from 10.0.15.216
[ec2-user@ip-10-0-130-166 ~]$ aws s3 ls

Unable to locate credentials. You can configure credentials by running "aws configure".
[ec2-user@ip-10-0-130-166 ~]$
```

i-04812ecb92979c3ff (Salman-Public)

PublicIPs: 18.208.249.109 PrivateIPs: 10.0.15.216

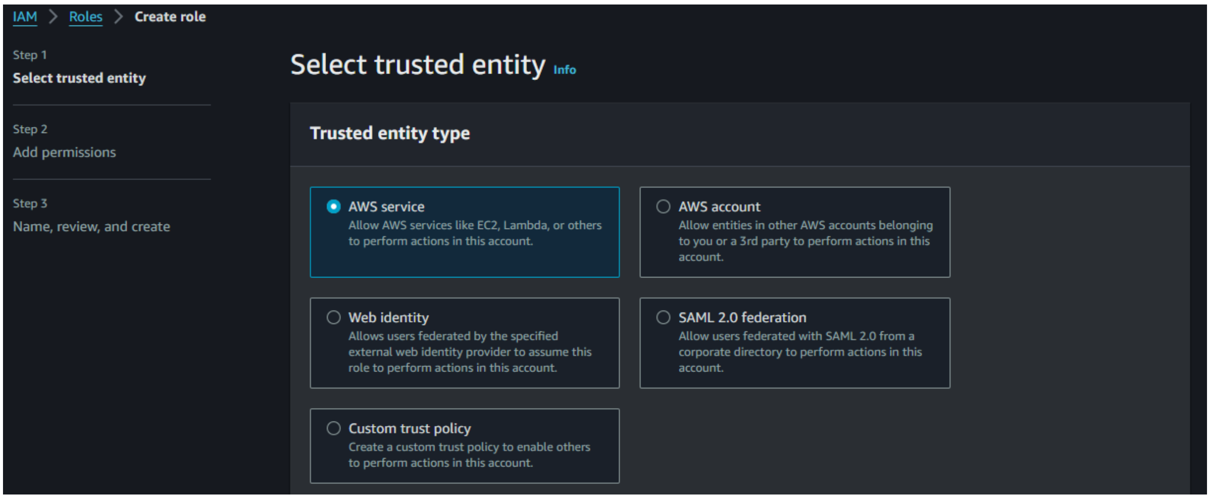
15. Go to IAM Create Role



Roles (6) 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.

16. Select AWS Service



IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Select trusted entity Info

Trusted entity type

● AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

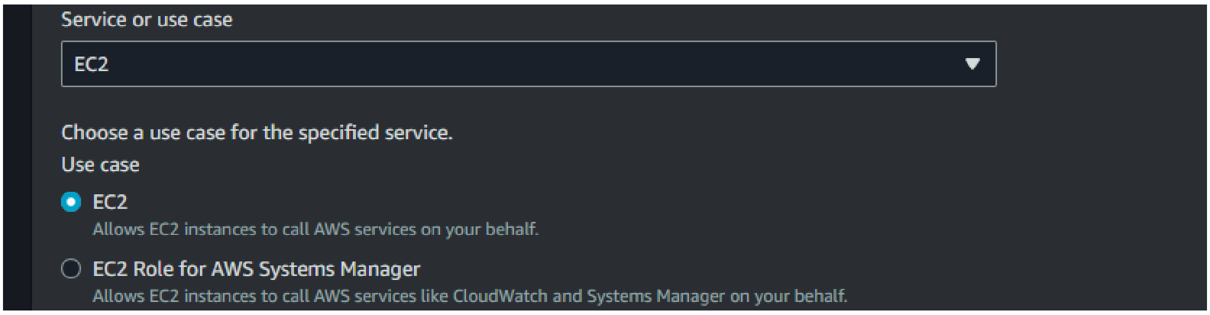
○ AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

○ Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

○ SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

○ Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

17. Select EC2



Service or use case

EC2 ▼

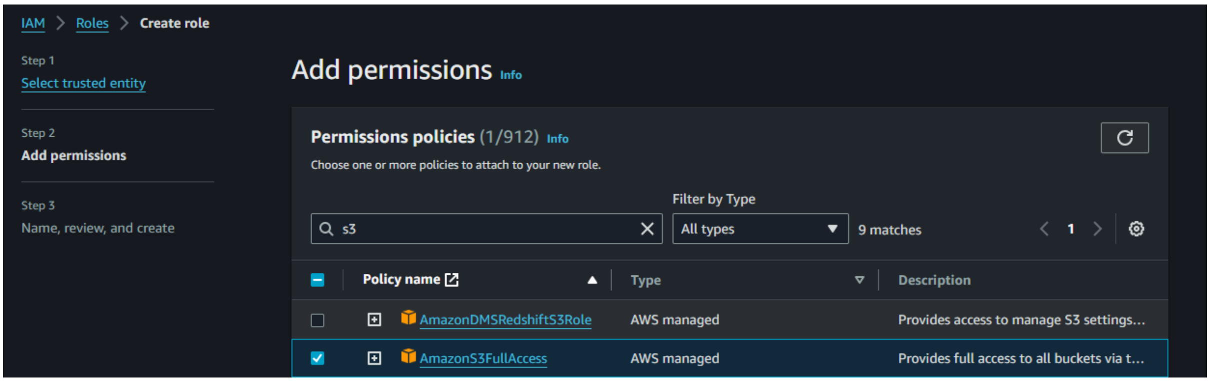
Choose a use case for the specified service.

Use case

● EC2
Allows EC2 instances to call AWS services on your behalf.

○ EC2 Role for AWS Systems Manager
Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf.

18. Add Permissions Full Access to S3



IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Add permissions Info

Permissions policies (1/912) Info

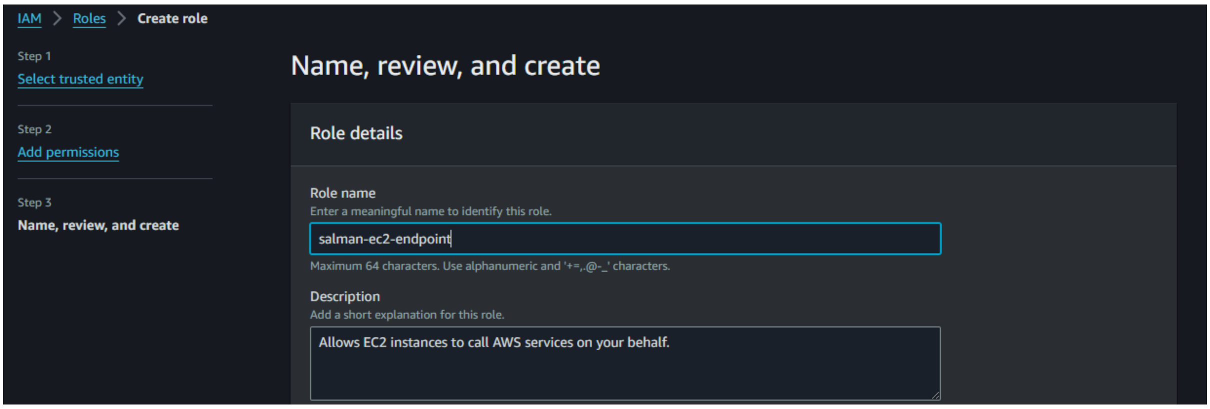
Choose one or more policies to attach to your new role.

Filter by Type

s3 | All types ▼ | 9 matches | < 1 >

▬	Policy name ▲	Type	Description
☐	AmazonDMSRedshiftS3Role	AWS managed	Provides access to manage S3 settings...
☑	AmazonS3FullAccess	AWS managed	Provides full access to all buckets via t...

19. Give the Role Name and Description and Create the Role



IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

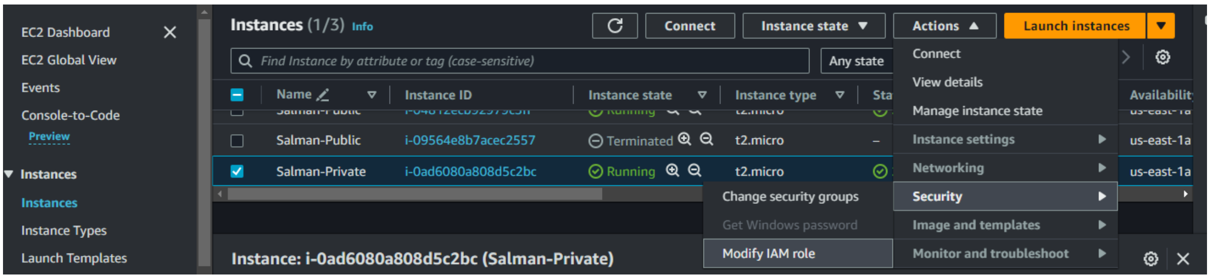
Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.
salman-ec2-endpoint
Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.

Description
Add a short explanation for this role.
Allows EC2 instances to call AWS services on your behalf.

20. Go To Private EC2 Instances and Select and Actions > Security > Modify IAM Role

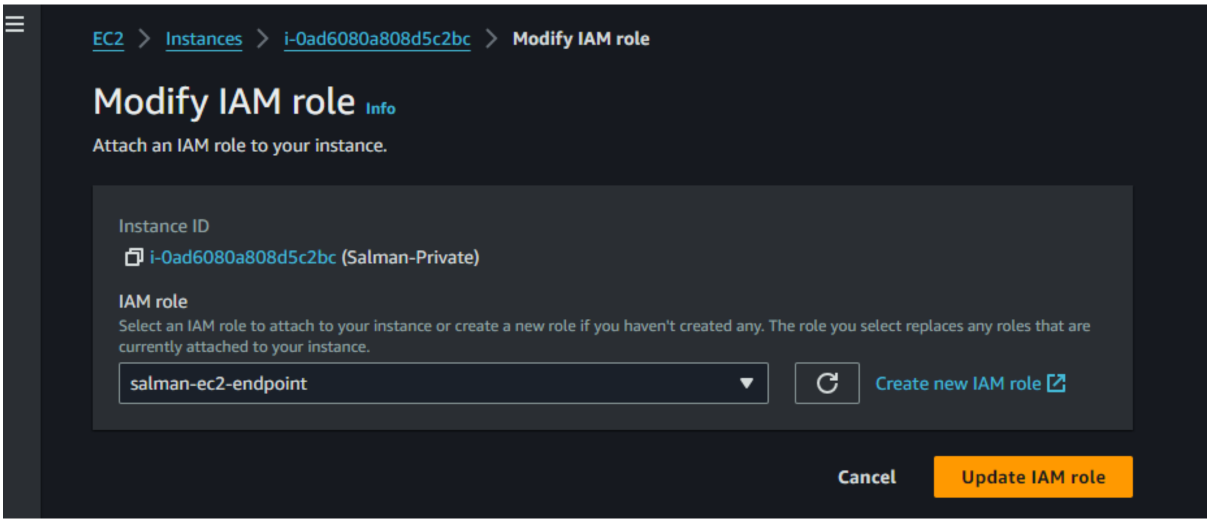


Instances (1/3) Info

☐	Name	Instance ID	Instance state	Instance type	Sta	Availabilit
☐	Salman-Public	i-09564e8b7acec2557	Terminated	t2.micro	–	us-east-1a
☑	Salman-Private	i-0ad6080a808d5c2bc	Running	t2.micro	✓	us-east-1a

Instance: i-0ad6080a808d5c2bc (Salman-Private)

21. Select your IAM Role and Update



EC2 > Instances > i-0ad6080a808d5c2bc > Modify IAM role

Modify IAM role Info

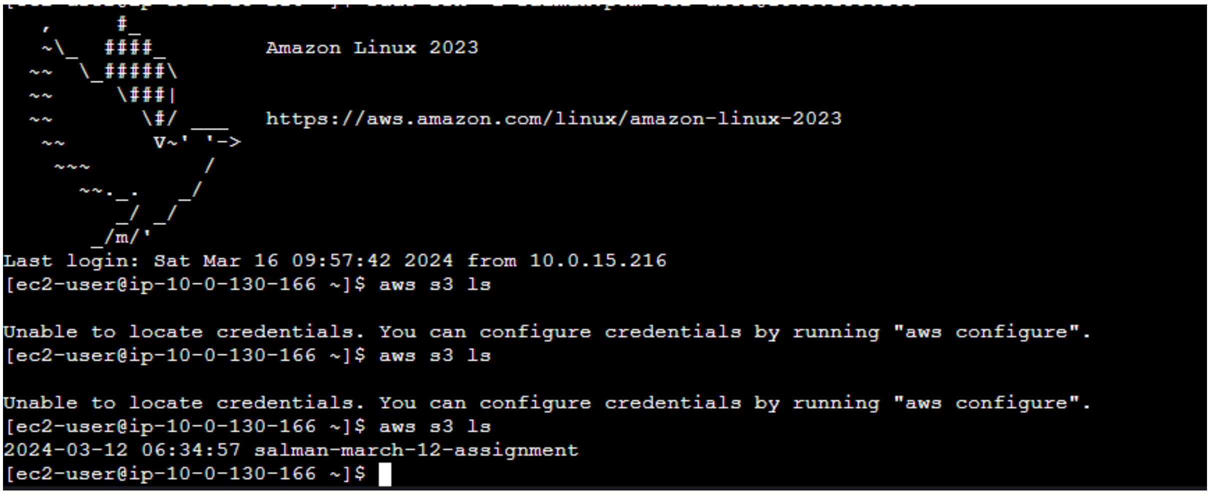
Attach an IAM role to your instance.

Instance ID
i-0ad6080a808d5c2bc (Salman-Private)

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.

salman-ec2-endpoint

22. Now Check in your Private Instance can access s3 through endpoints



```
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Sat Mar 16 09:57:42 2024 from 10.0.15.216
[ec2-user@ip-10-0-130-166 ~]$ aws s3 ls

Unable to locate credentials. You can configure credentials by running "aws configure".
[ec2-user@ip-10-0-130-166 ~]$ aws s3 ls

Unable to locate credentials. You can configure credentials by running "aws configure".
[ec2-user@ip-10-0-130-166 ~]$ aws s3 ls
2024-03-12 06:34:57 salman-march-12-assignment
[ec2-user@ip-10-0-130-166 ~]$
```

Thank You