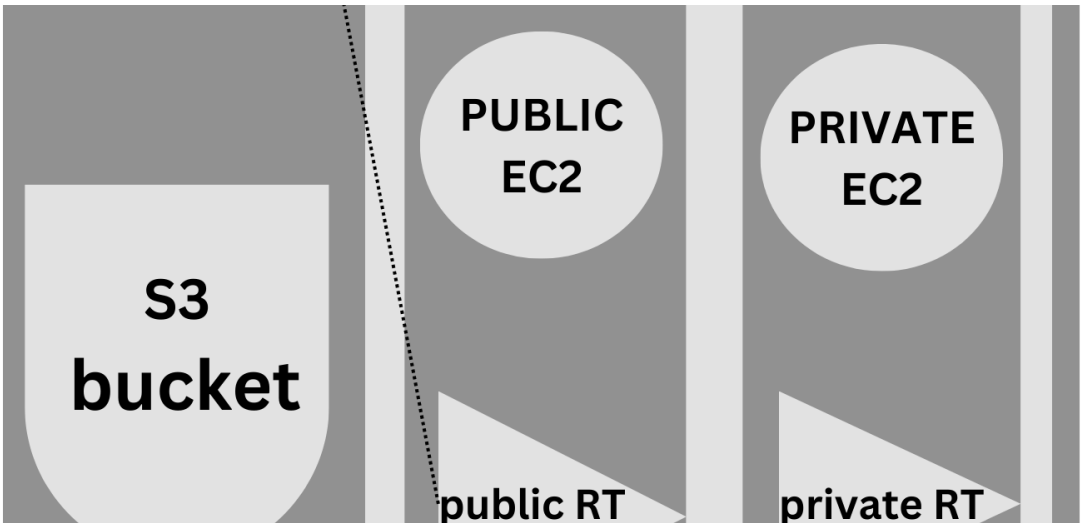
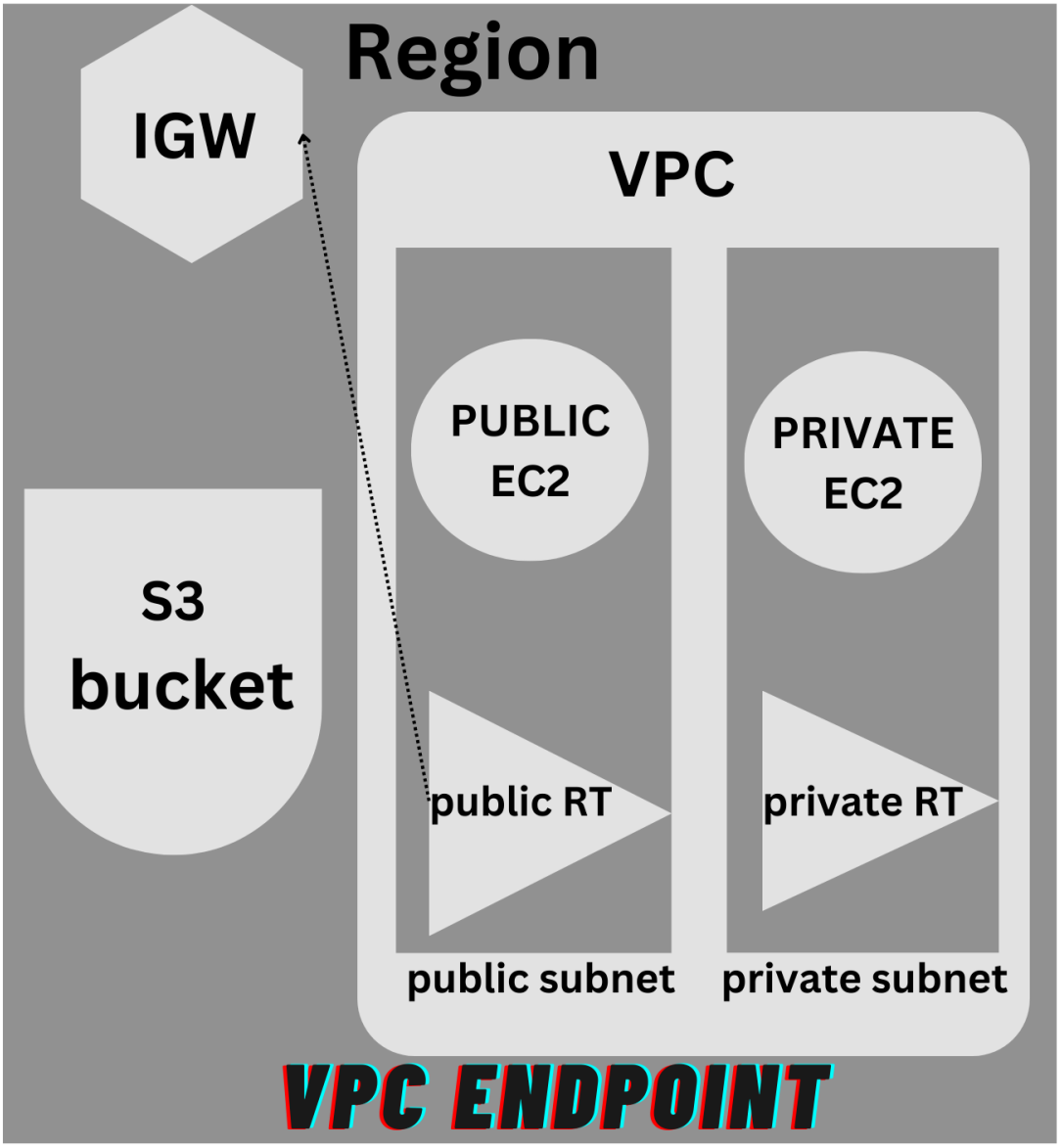


VPC Endpoint

- VPC endpoint enables creation of a private connection between VPC to supported AWS services
- Traffic between VPC and AWS service does not leave the Amazon network.

There are two types of VPC endpoints:

1. **Interface endpoint**
2. **Gateway endpoint**



Step1: Login into your AWS Console

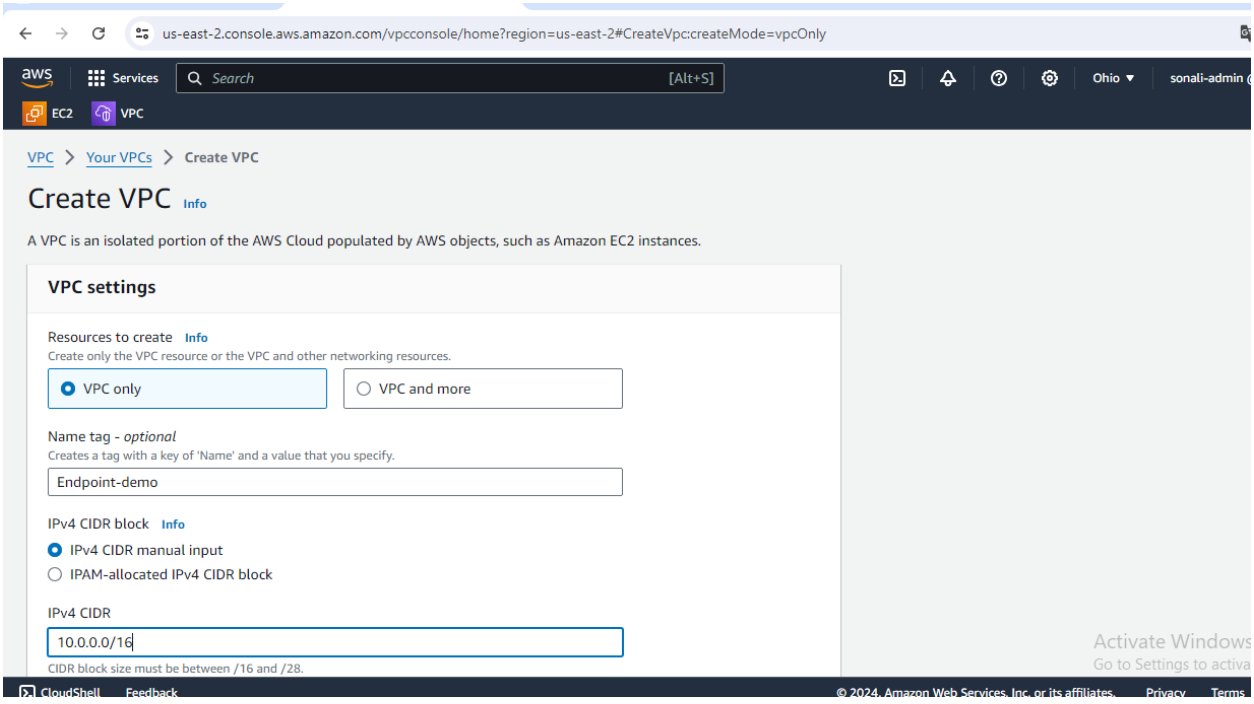
Step2: Create Infrastructure

- Create VPC
- Create 2 Subnet in that one is public and other is Private.
- Make One Public by Enabling in Setting
- Create one IGW for Public Subnet

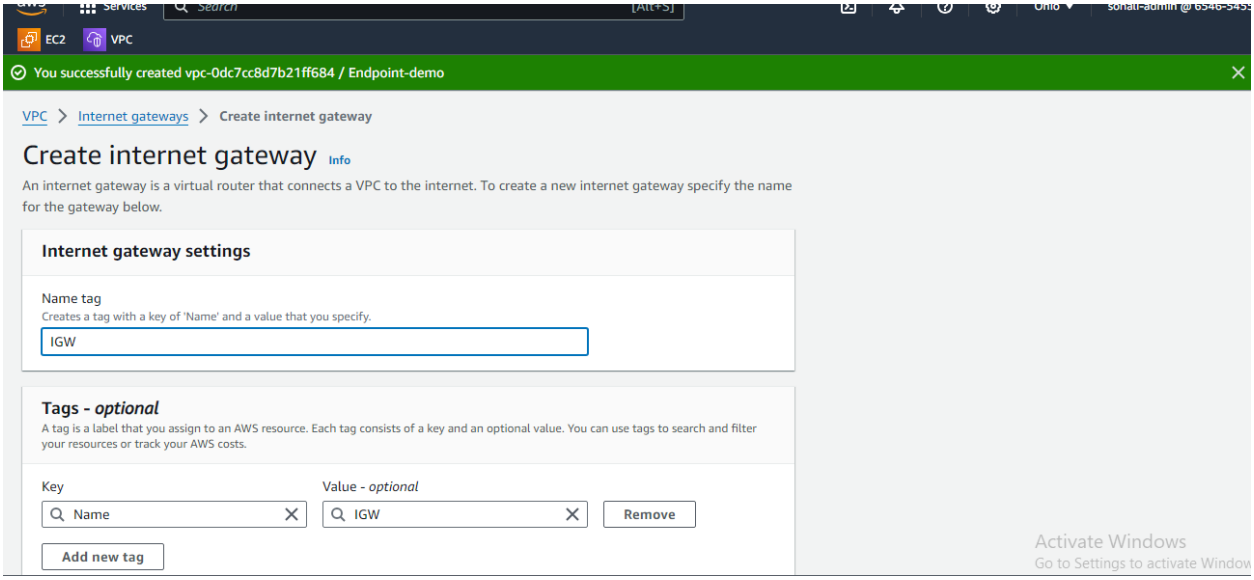
- Attach that subnet to VPC
- Create public Route Table to Public Subnet and add Route of Internet Gateway
- Create private Route Table for private subnet. Don't add any route in it. Because when we create Endpoint at that we are giving this private RT.
- In Private RT Route get added automatically after creating Endpoint
- Create S3 bucket
- Create Role for S3 bucket
- Create Endpoint to access the resources like s3 bucket.

Step 3:

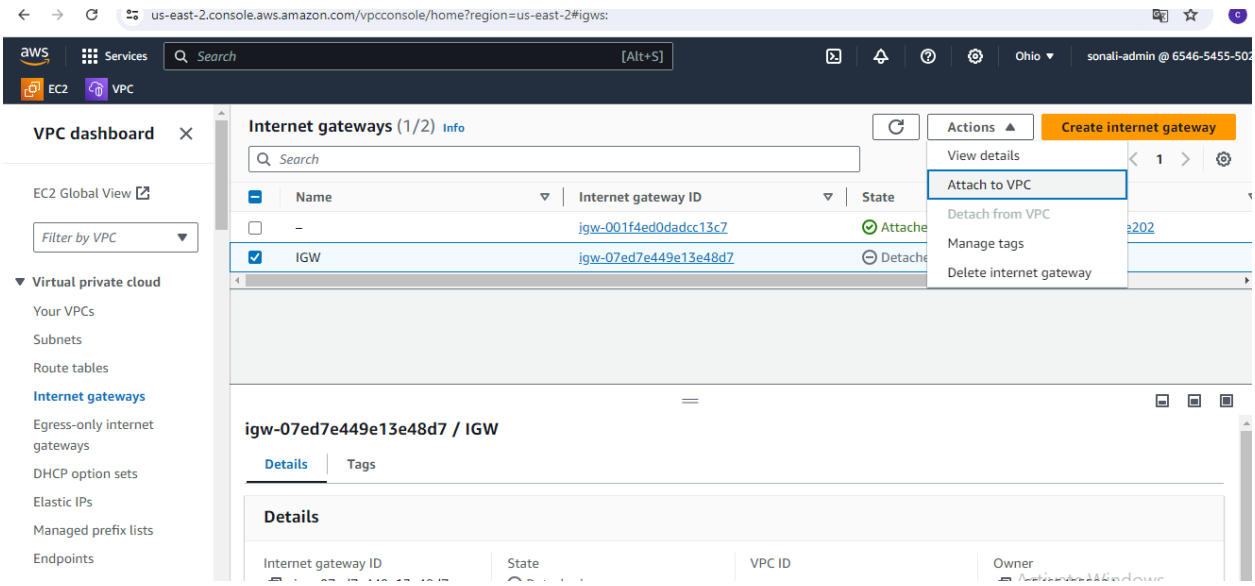
- In the AWS Management Console search bar, enter VPC, and click the VPC result under Services:
- To start creating VPC, in the left down side, Click on **Your VPC** to Create VPC:

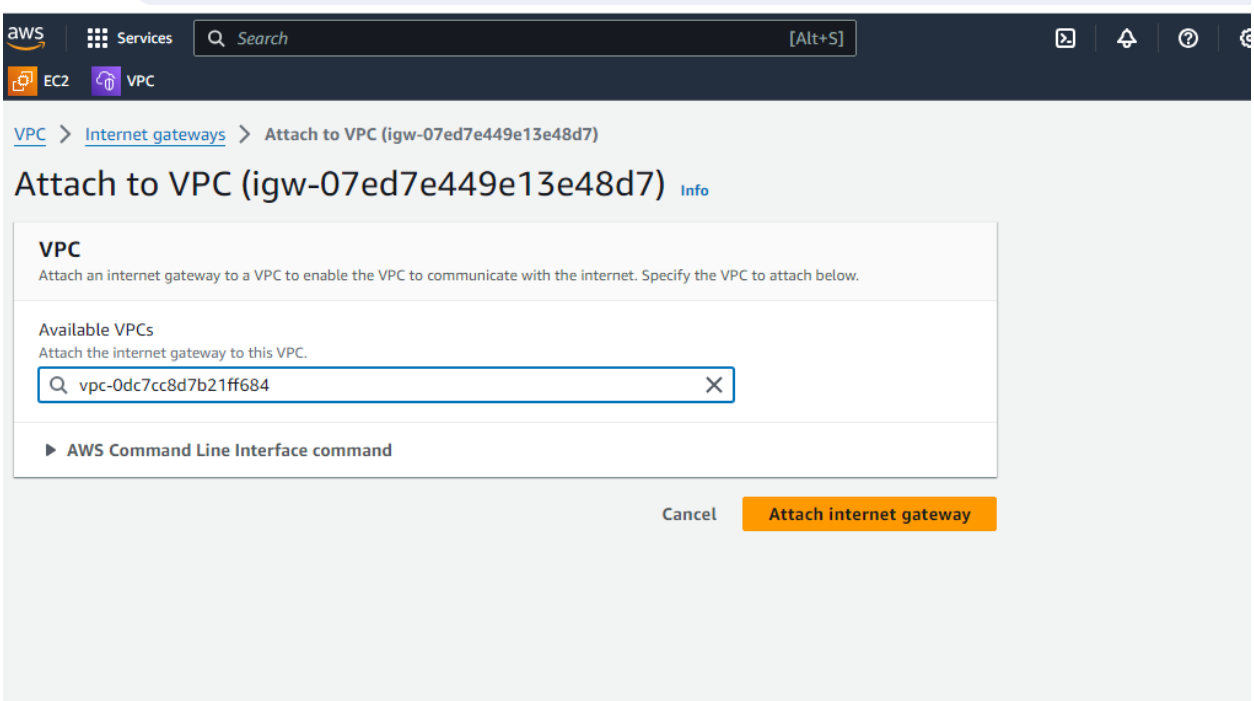


- Create one IGW for Public Subnet

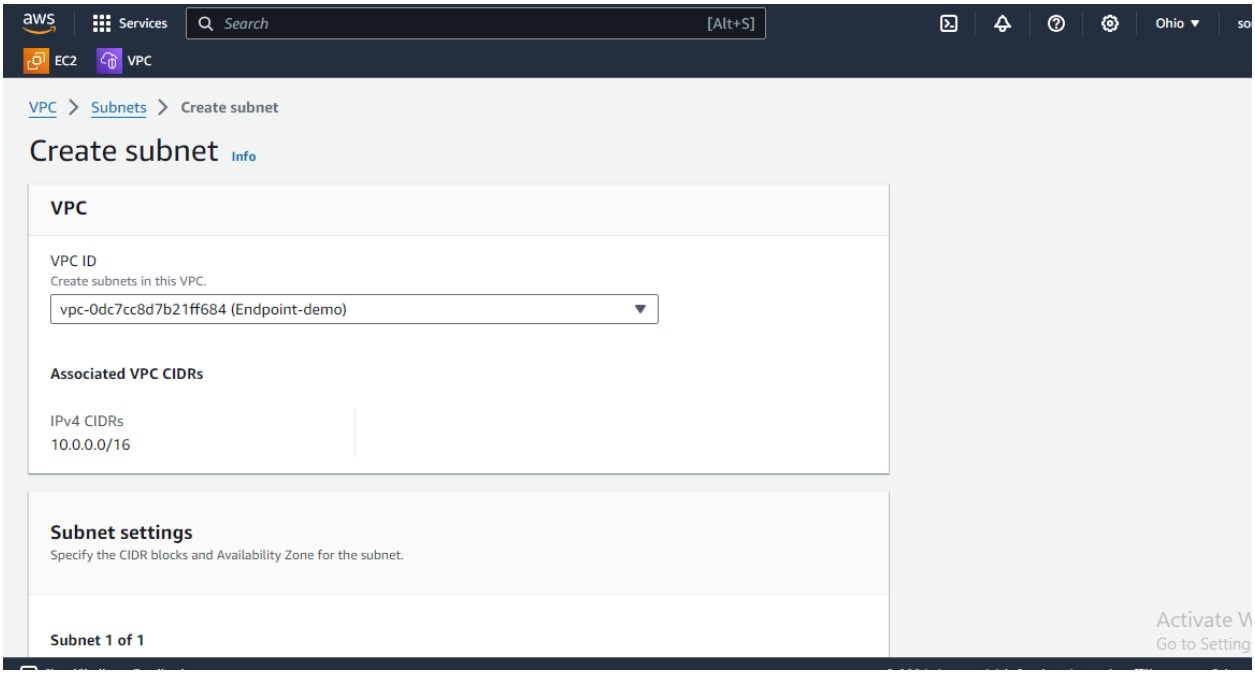


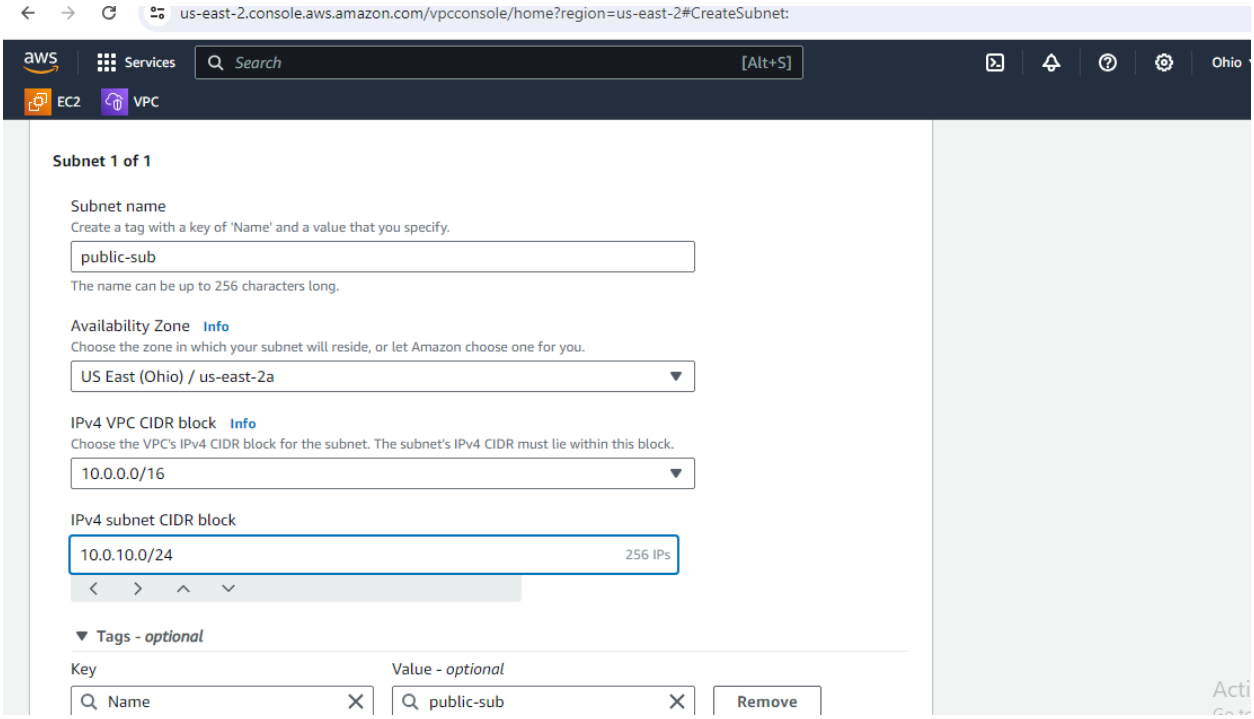
- Attach Internet Gateway to VPC



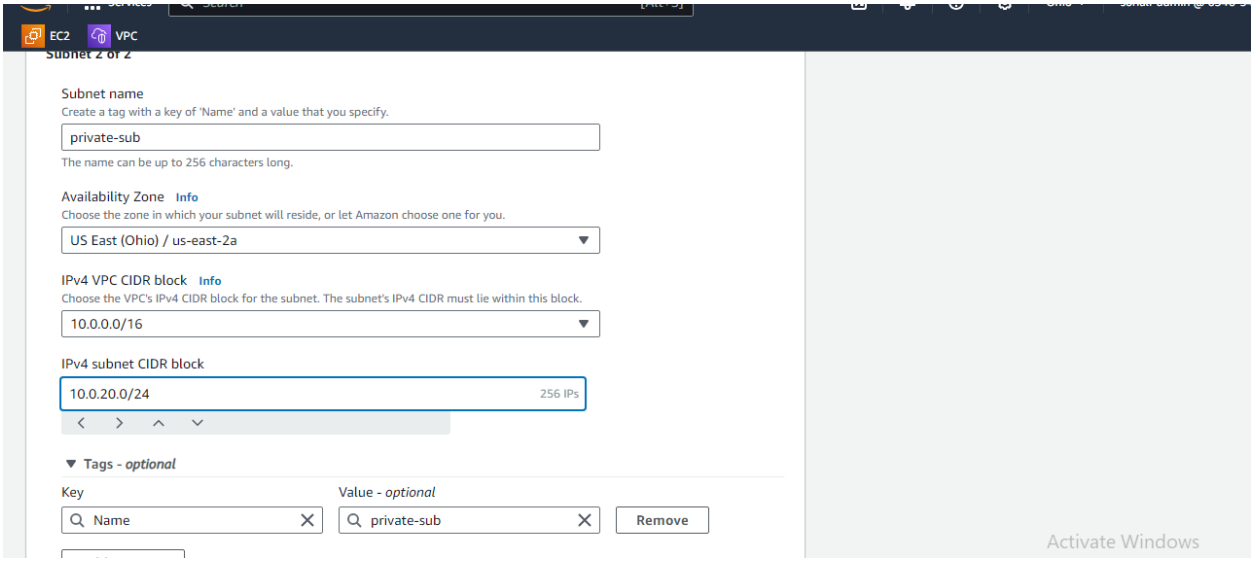


- Create Public Subnet

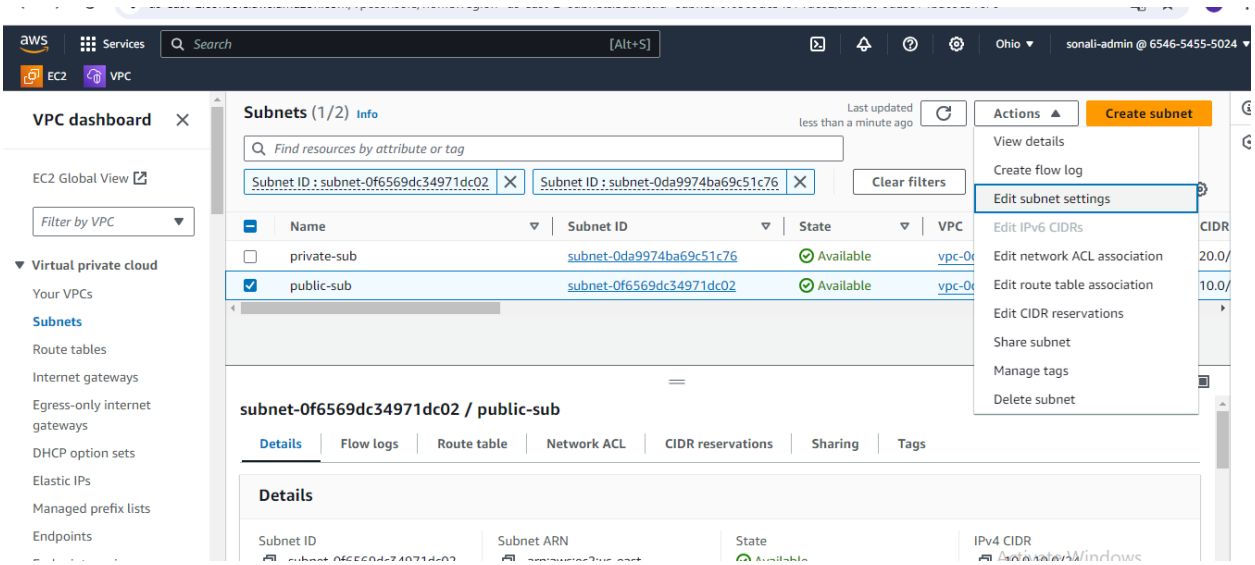


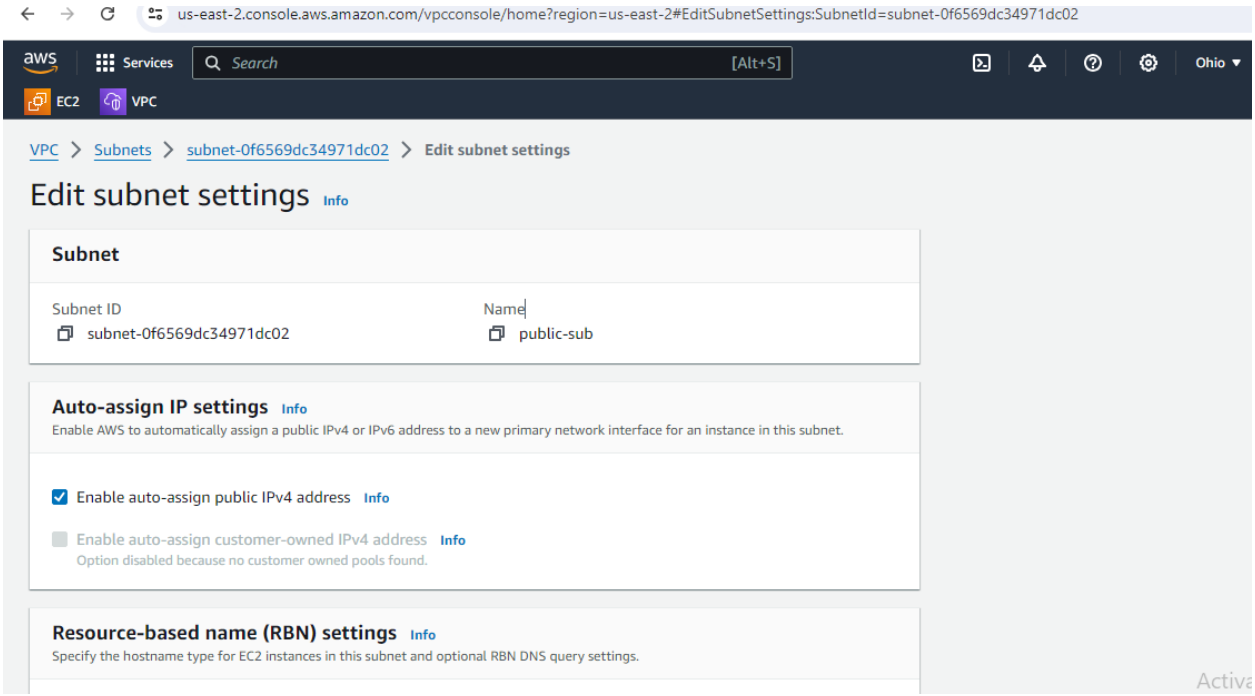


- Create private subnet

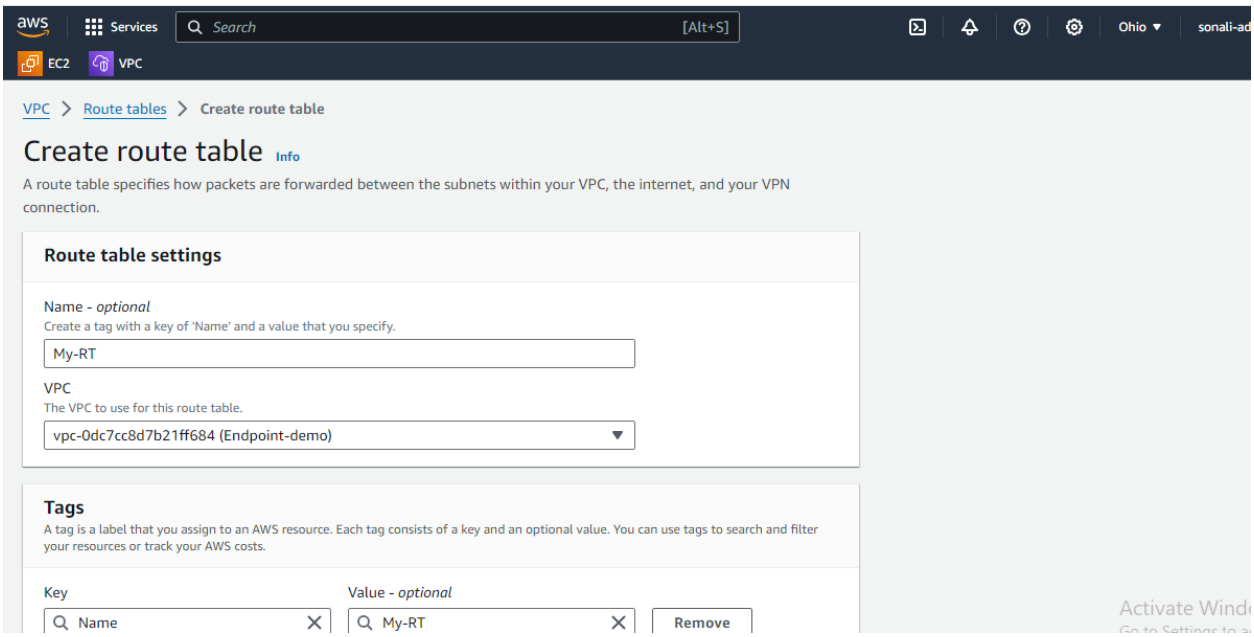


- Make your subnet public by enabling the setting

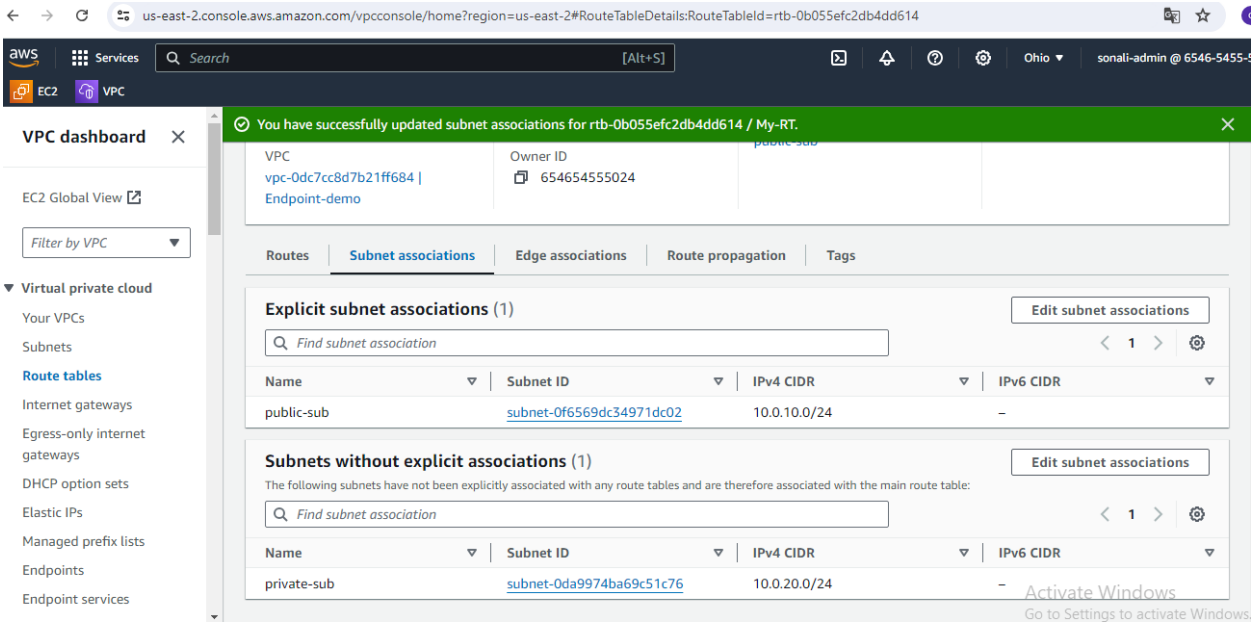




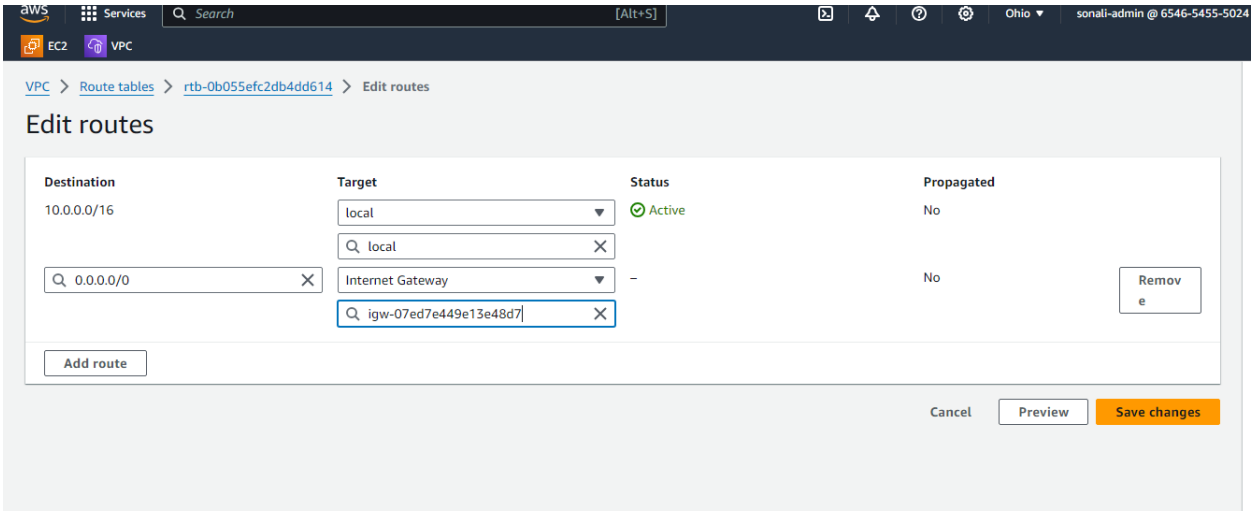
- Create one Route for public subnet



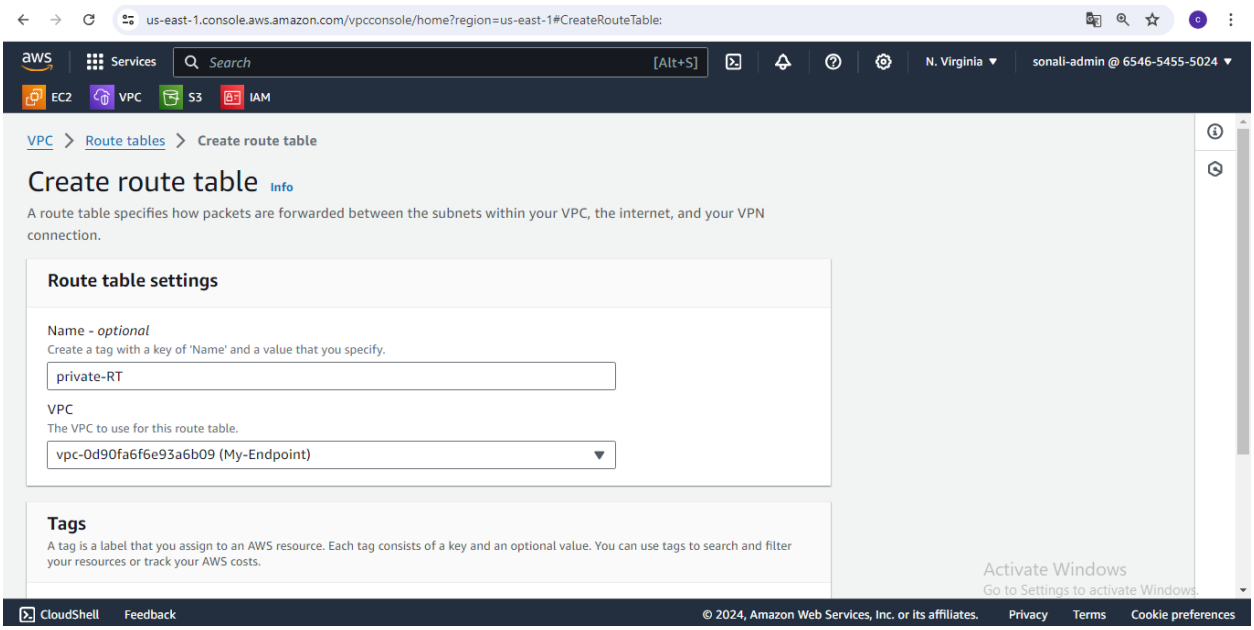
- Do subnet Association with public subnet.



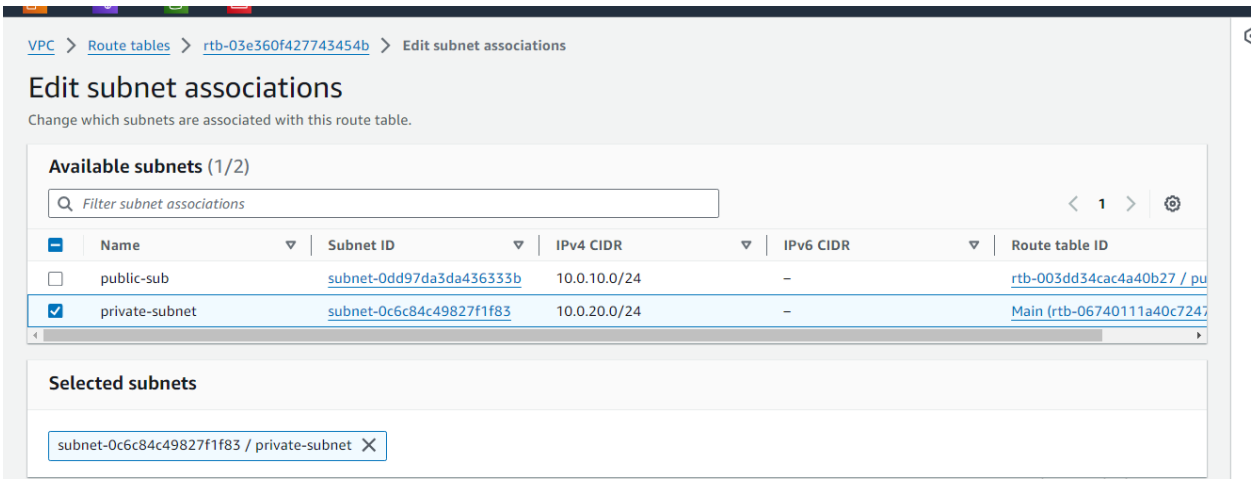
- Add Route of internet gateway to the Route Table



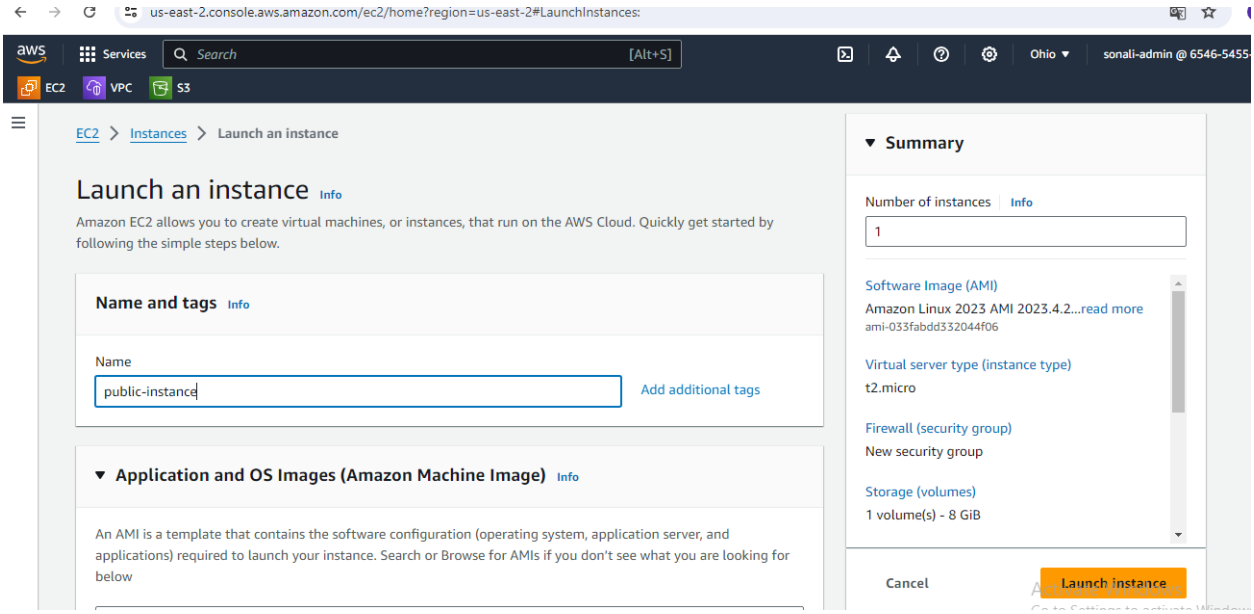
- Create private RT for private subnet.



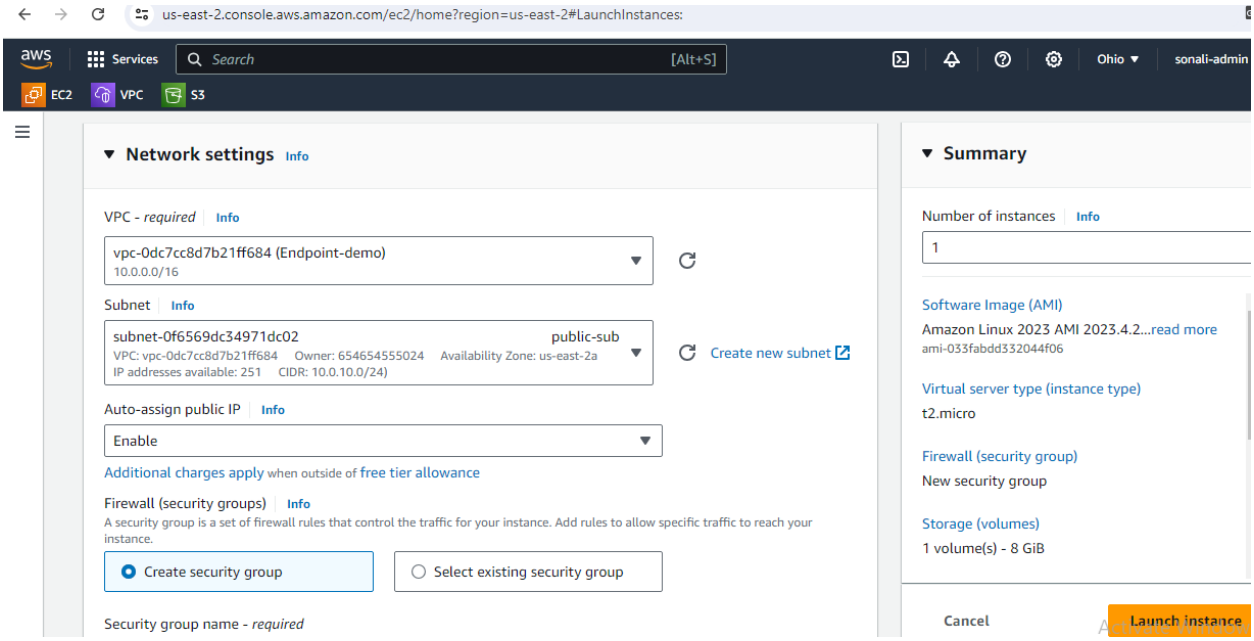
- Do subnet Association with public subnet.



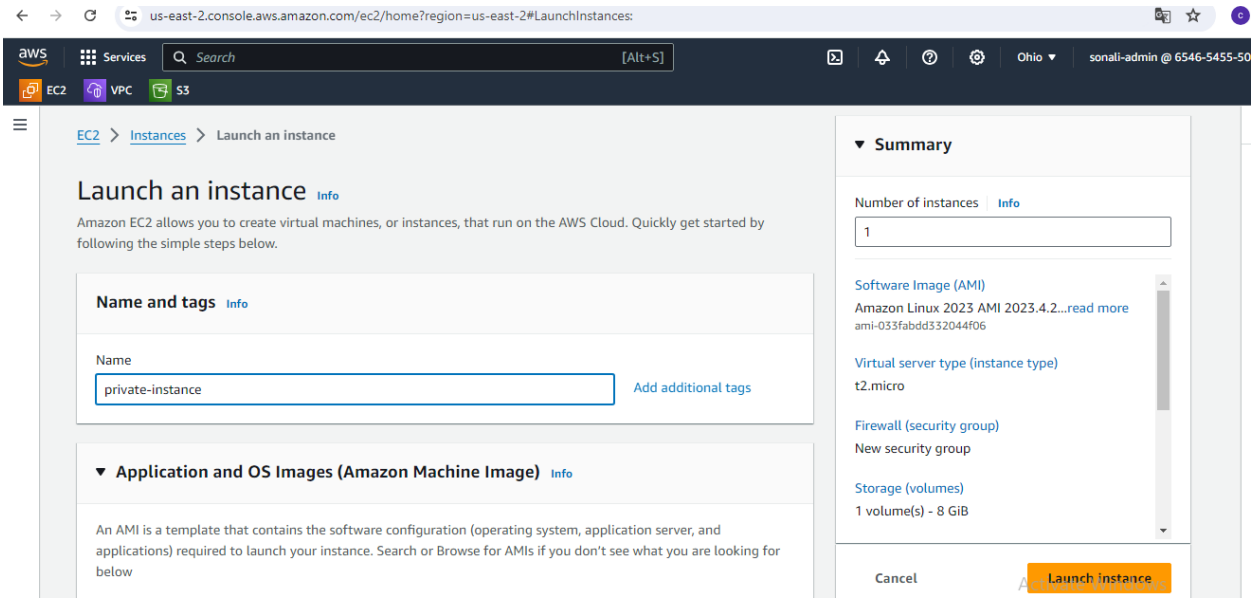
- Launch the public Instance

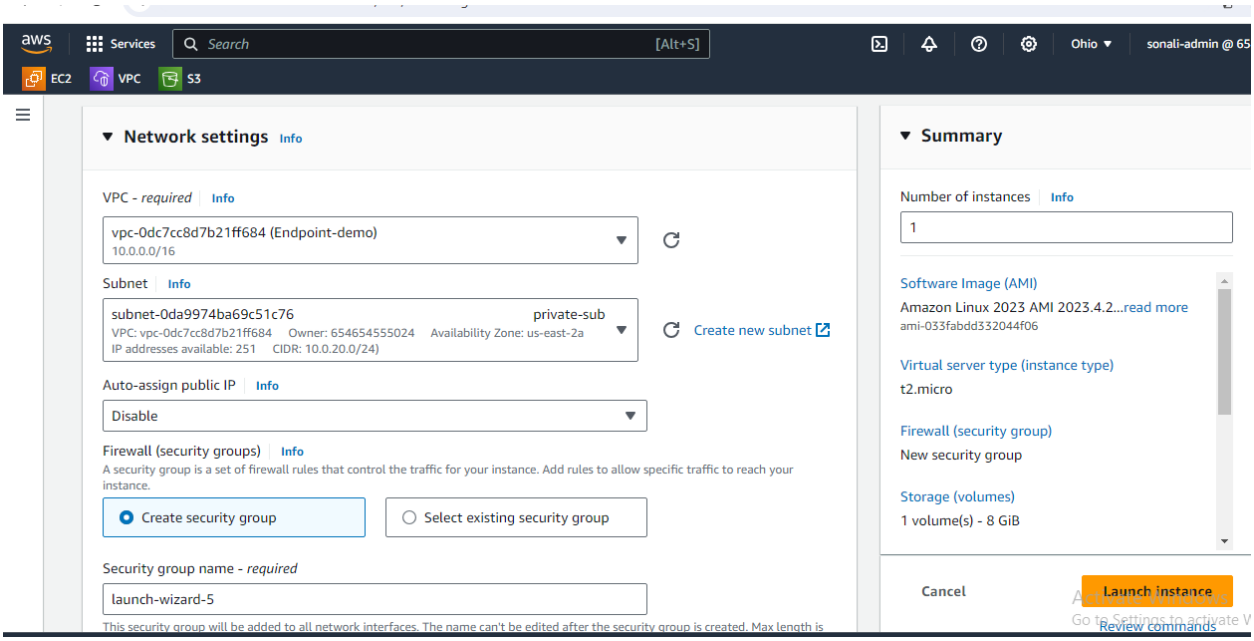


- Select VPC which we have created and public subnet for public ec2

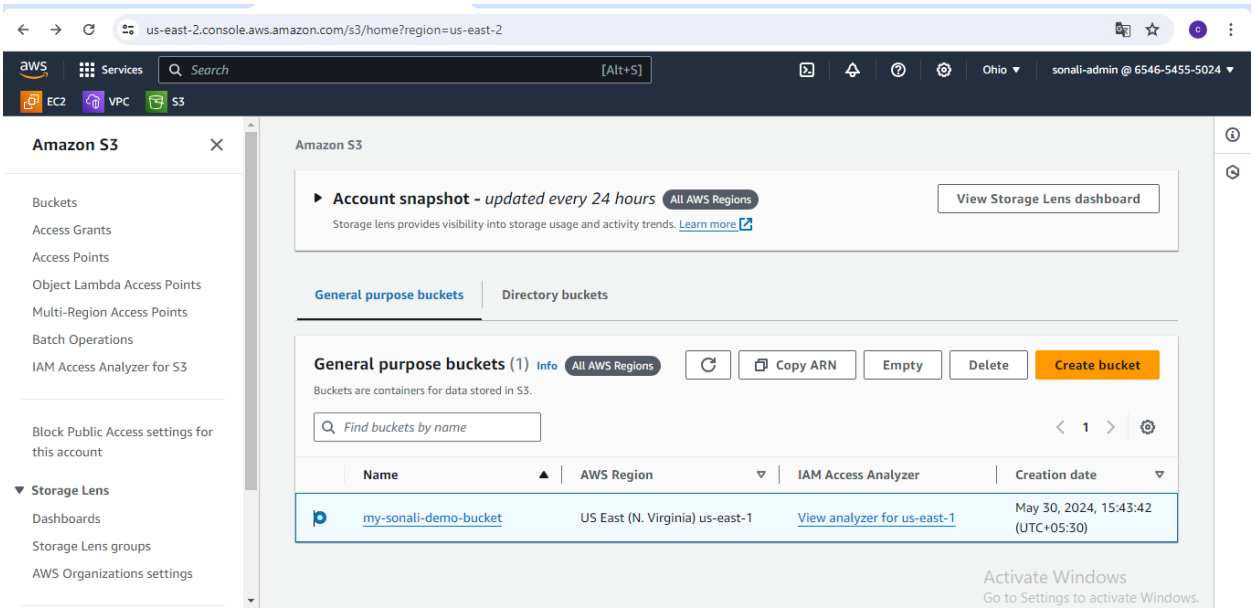


- Launch private instance and select private subnet

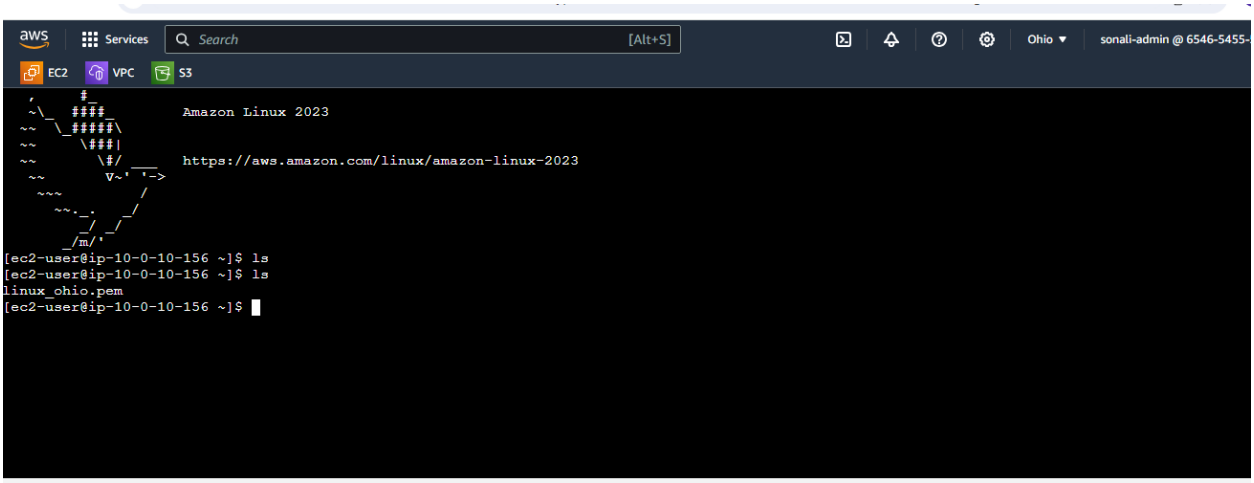




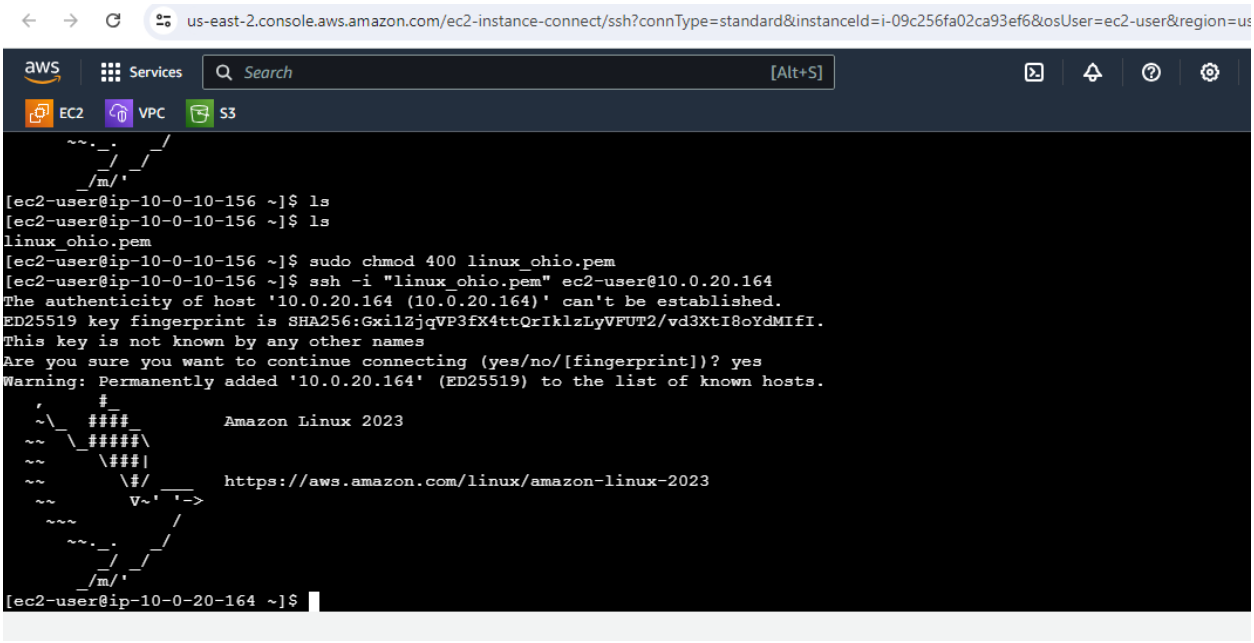
- Create s3 Bucket



- Do scp and copy your key in virtual machine
- Do ssh to private ec2 instance

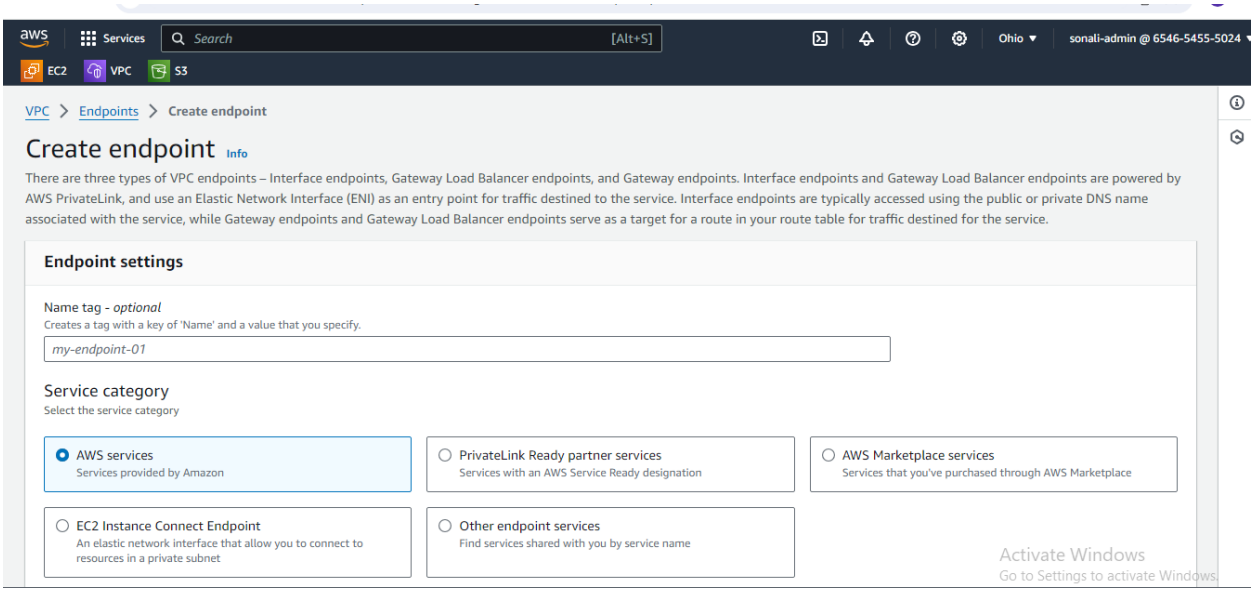

aws
Services
Search
[Alt+S]
Ohio
sonali-admin @ 6546-5455-
EC2
VPC
S3
Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023
[ec2-user@ip-10-0-10-156 ~]$ ls
[ec2-user@ip-10-0-10-156 ~]$ ls
linux_ohio.pem
[ec2-user@ip-10-0-10-156 ~]$

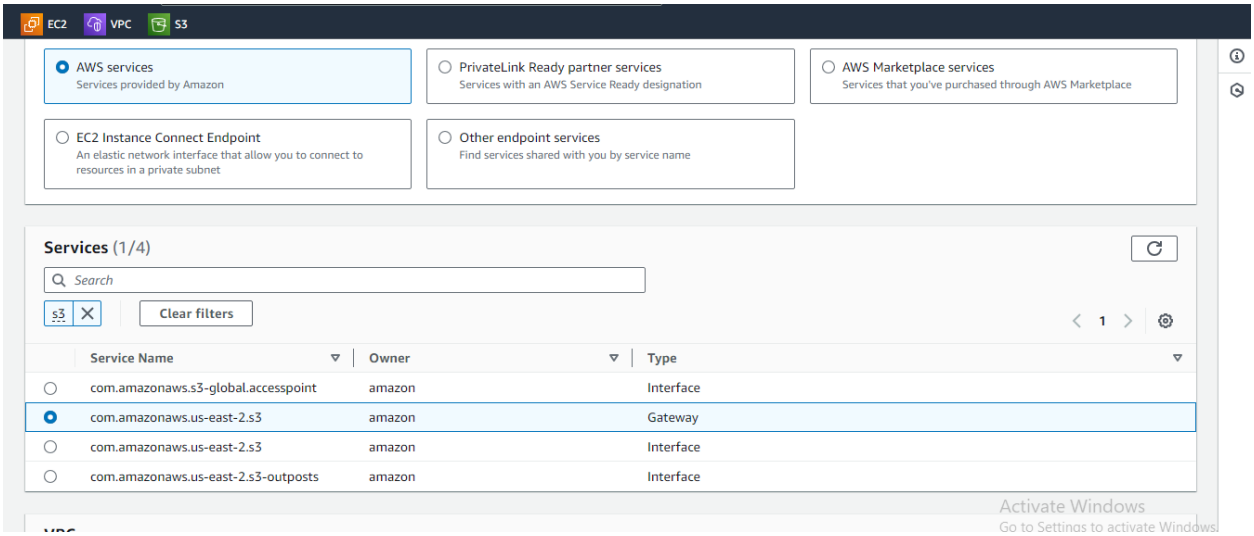

aws
Services
Search
[Alt+S]
Ohio
EC2
VPC
S3
Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023
[ec2-user@ip-10-0-10-156 ~]$ ls
[ec2-user@ip-10-0-10-156 ~]$ ls
linux_ohio.pem
[ec2-user@ip-10-0-10-156 ~]$ sudo chmod 400 linux_ohio.pem
[ec2-user@ip-10-0-10-156 ~]$ ssh -i "linux_ohio.pem" ec2-user@10.0.20.164

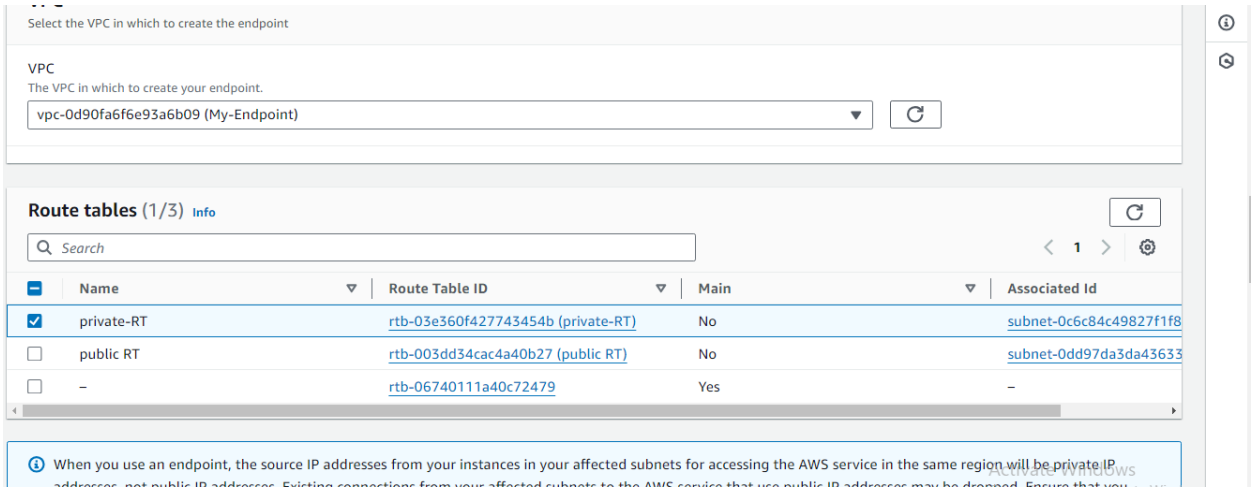


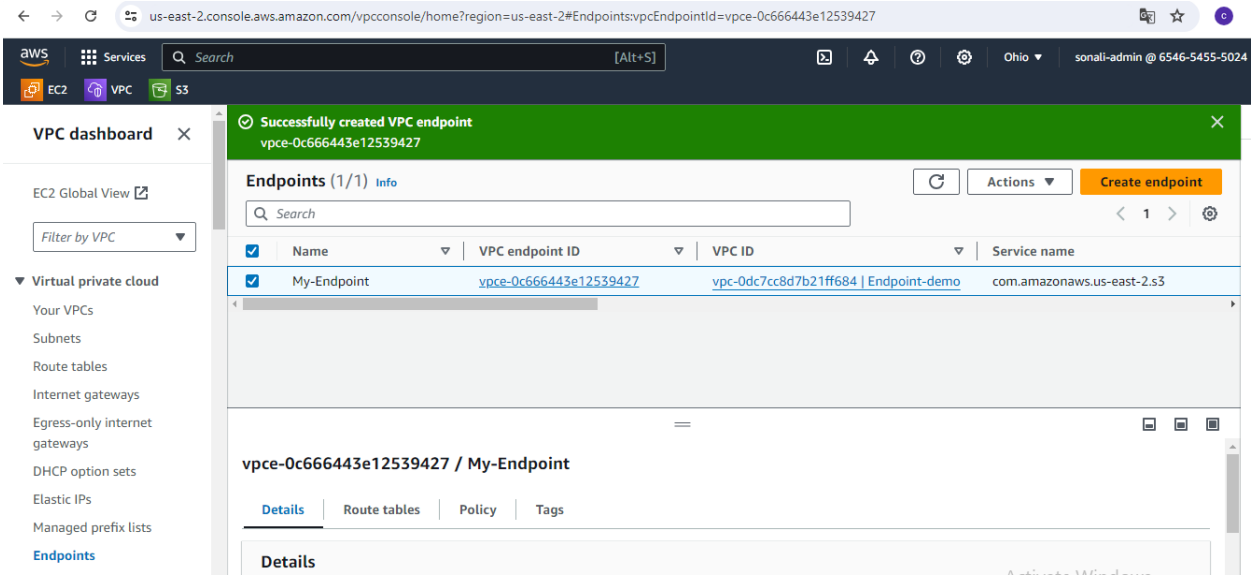
- View the list of bucket using below command .you will not get any output here . because of that you need to create VPC endpoint.

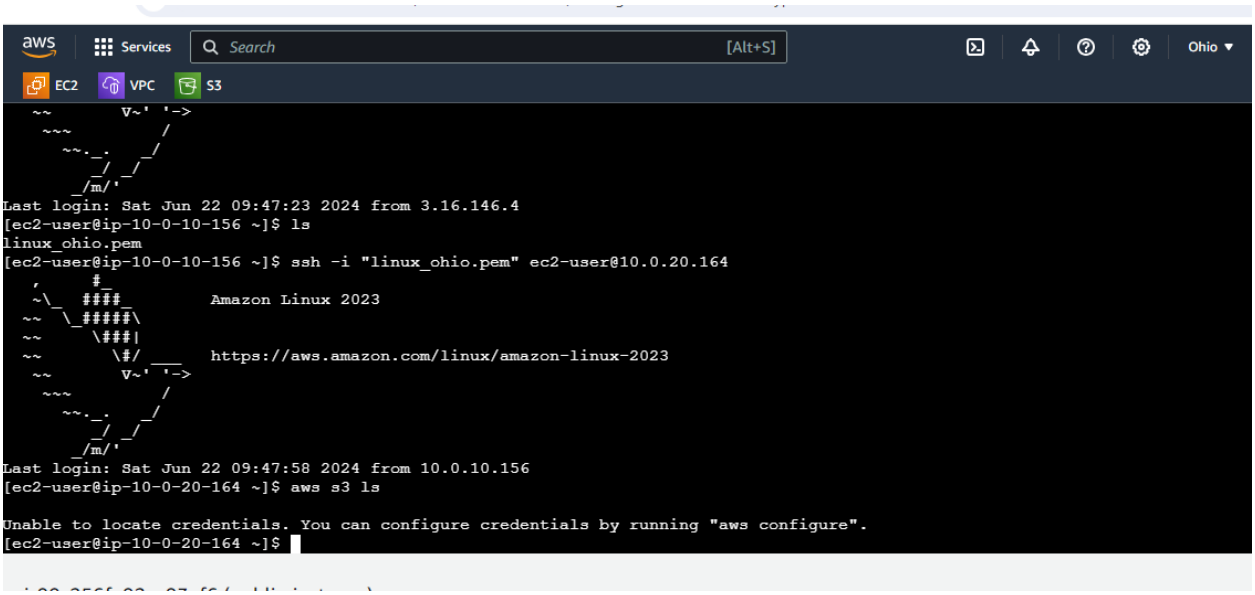
- Create VPC Endpoint


Services
Search
[Alt+S]
Ohio
sonali-admin @ 6546-5455-5024
EC2
VPC
S3
VPC > Endpoints > 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-endpoint-01
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
Activate Windows
Go to Settings to activate Windows.

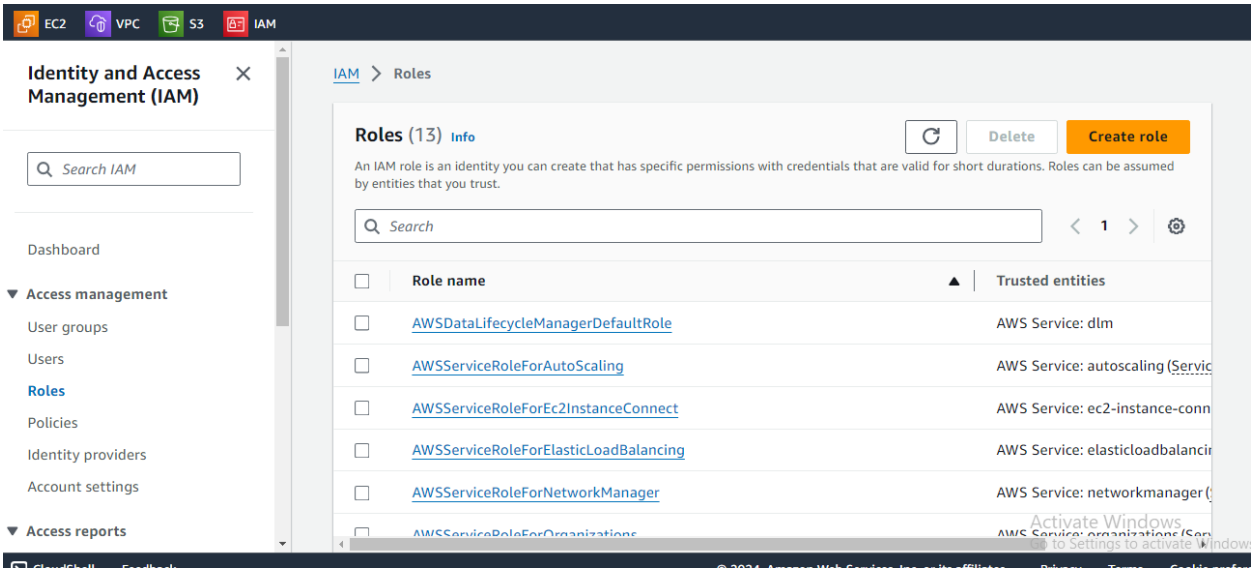

EC2
VPC
S3
AWS services
Services provided by Amazon
PrivateLink Ready partner services
Services with an AWS Service Ready designation
AWS Marketplace services
Services that you've purchased through AWS Marketplace
EC2 Instance Connect Endpoint
An elastic network interface that allow you to connect to resources in a private subnet
Other endpoint services
Find services shared with you by service name
Services (1/4)
Search
s3
Clear filters
1
Service Name
Owner
Type
com.amazonaws.s3-global.accesspoint
amazon
Interface
com.amazonaws.us-east-2.s3
amazon
Gateway
com.amazonaws.us-east-2.s3
amazon
Interface
com.amazonaws.us-east-2.s3-outposts
amazon
Interface
Activate Windows
Go to Settings to activate Windows.

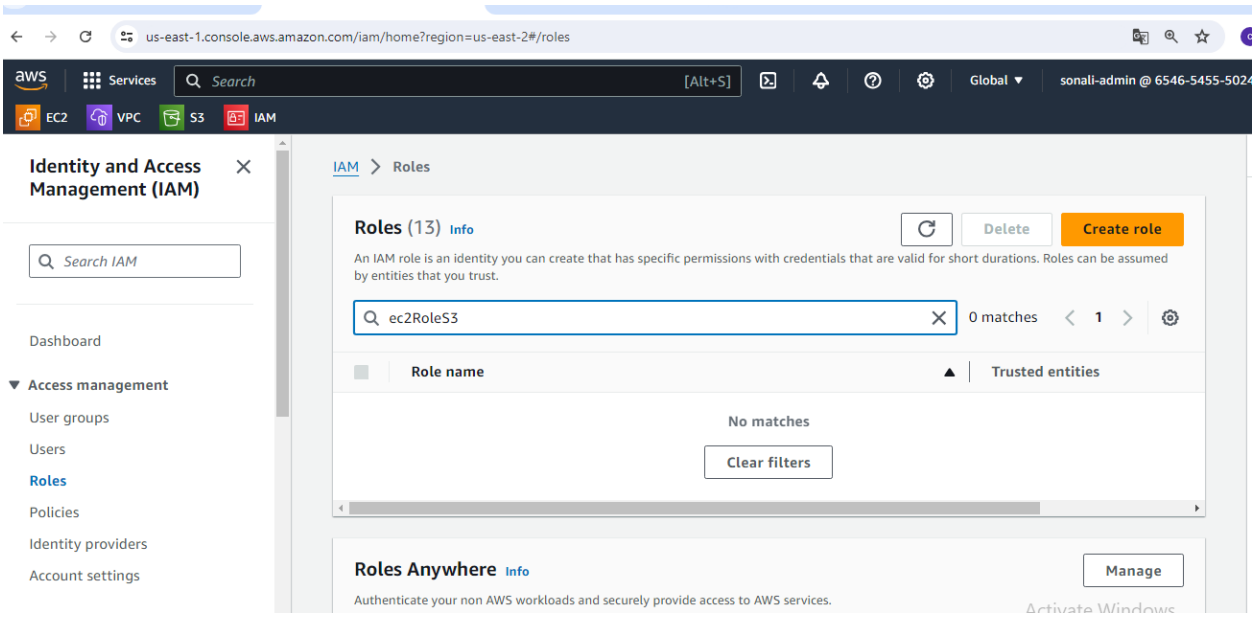

Select the VPC in which to create the endpoint
VPC
The VPC in which to create your endpoint.
vpc-0d90fa6f6e93a6b09 (My-Endpoint)
Route tables (1/3) Info
Search
Name
Route Table ID
Main
Associated Id
private-RT
rtb-03e360f427743454b (private-RT)
No
subnet-0c6c84c49827f1f8
public RT
rtb-003dd34cac4a40b27 (public RT)
No
subnet-0dd97da3da43633
–
rtb-06740111a40c72479
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

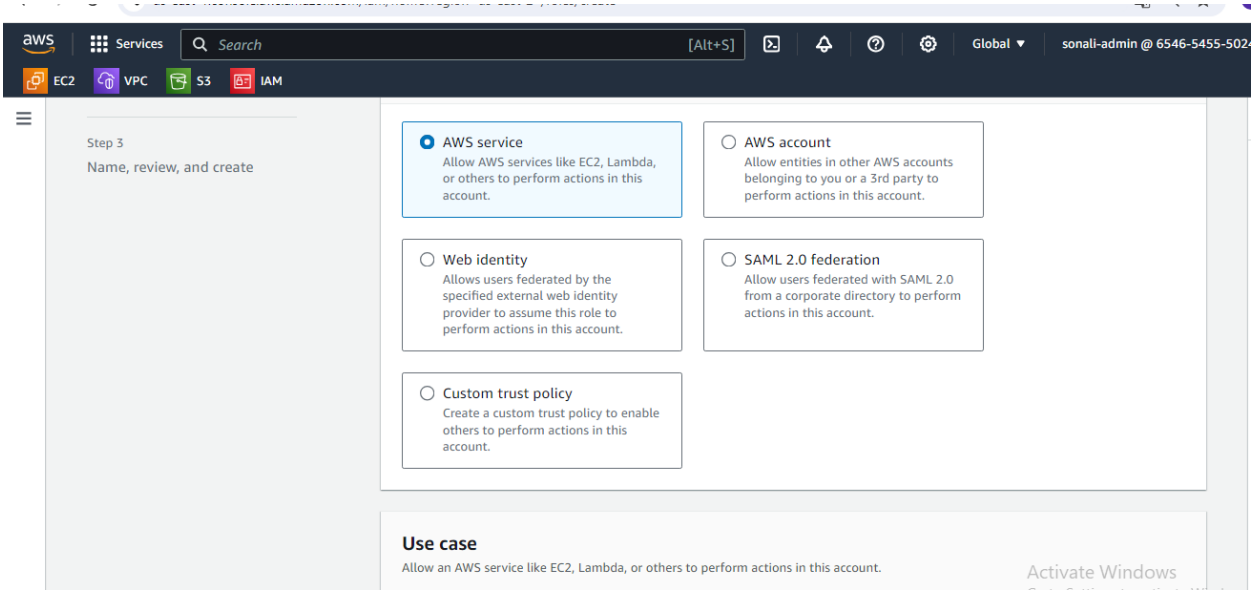

us-east-2.console.aws.amazon.com/vpcconsole/home?region=us-east-2#Endpoints:vpcEndpointId=vpce-0c666443e12539427
Services
Search
[Alt+S]
Ohio
sonali-admin @ 6546-5455-5024
EC2
VPC
S3
VPC dashboard
EC2 Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Successfully created VPC endpoint
vpce-0c666443e12539427
Endpoints (1/1) Info
Actions
Create endpoint
Search
Name
VPC endpoint ID
VPC ID
Service name
My-Endpoint
vpce-0c666443e12539427
vpc-0dc7cc8d7b21ff684 | Endpoint-demo
com.amazonaws.us-east-2.s3
vpce-0c666443e12539427 / My-Endpoint
Details
Route tables
Policy
Tags
Details

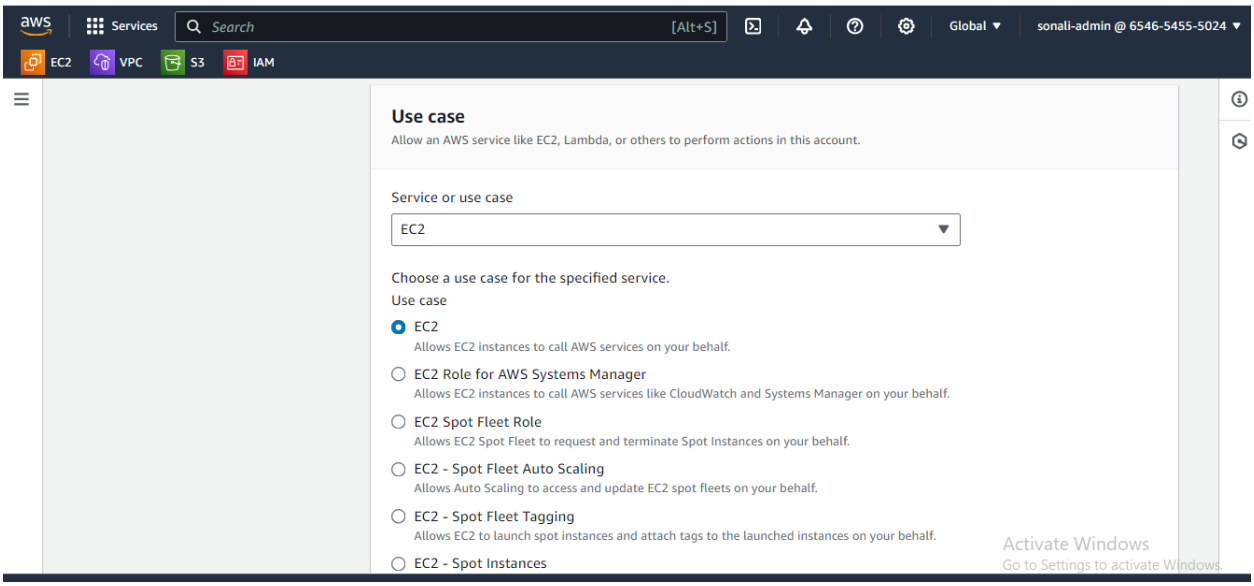


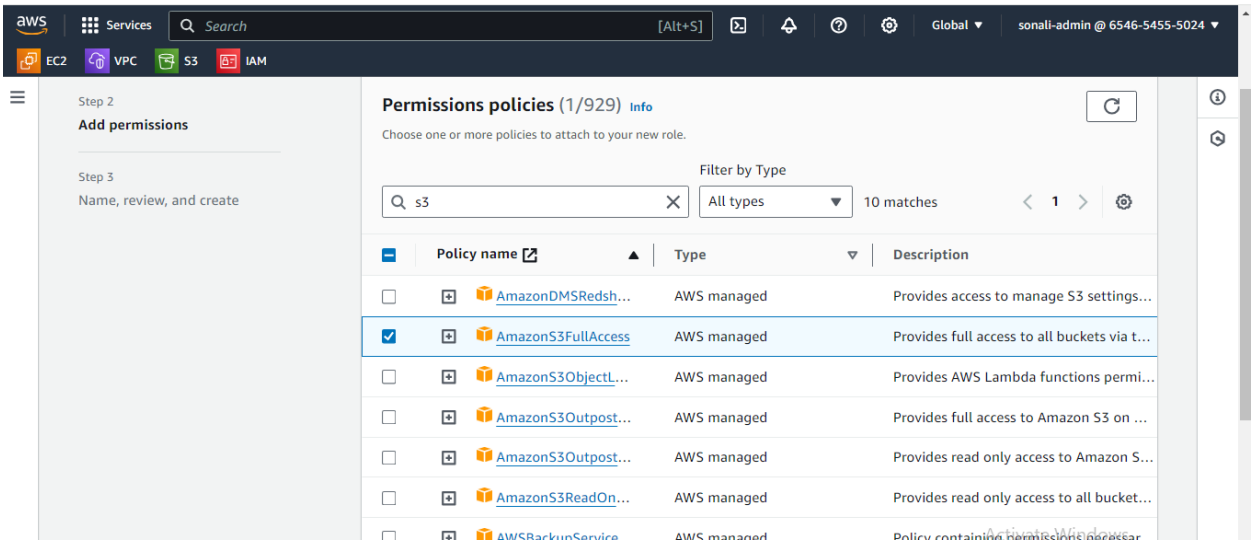
Create Role for password

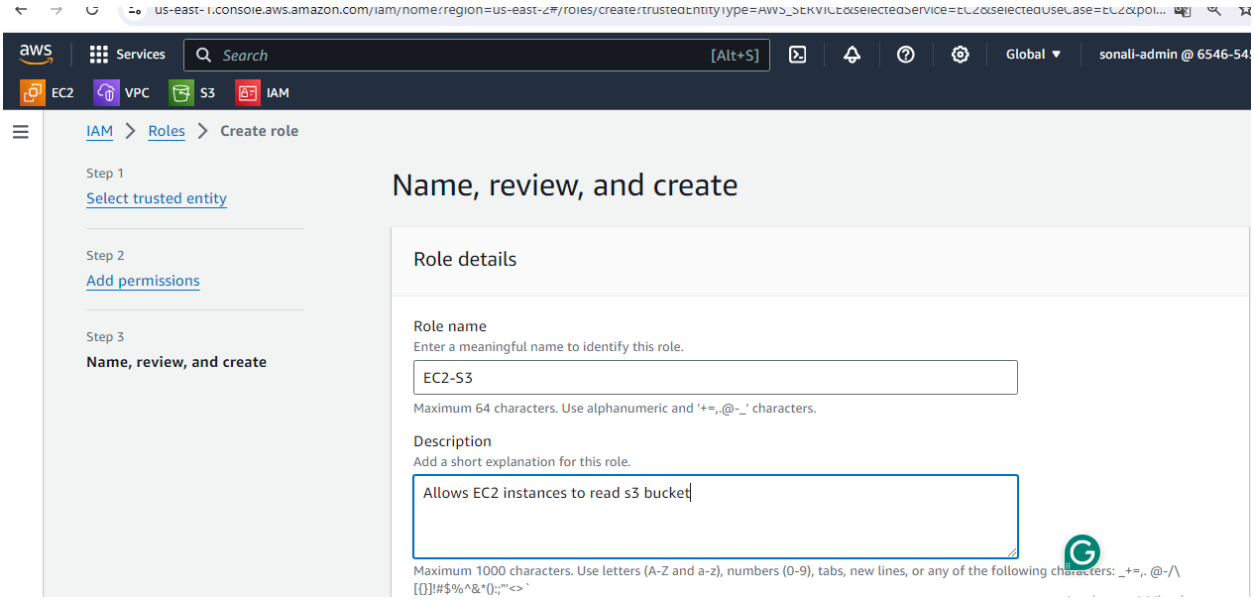


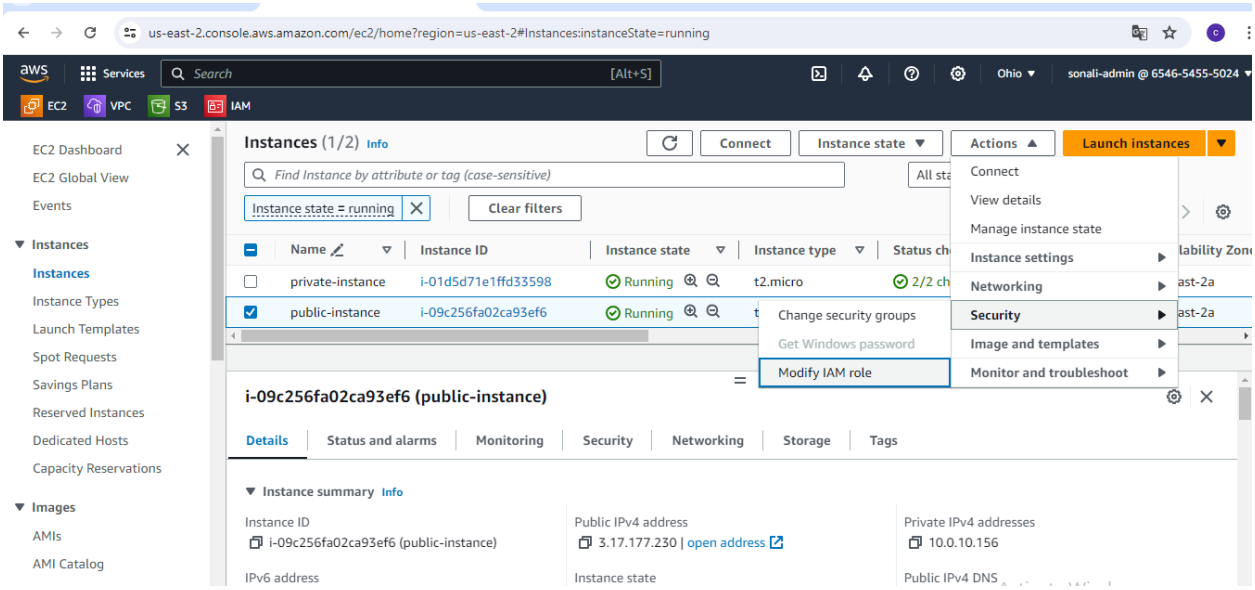

us-east-1.console.aws.amazon.com/iam/home?region=us-east-2#/roles
aws
Services
Search
[Alt+S]
Global
sonali-admin @ 6546-5455-5024
EC2
VPC
S3
IAM
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
IAM > Roles
Roles (13) Info
Delete
Create role
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.
ec2RoleS3
0 matches
1
Role name
Trusted entities
No matches
Clear filters
Roles Anywhere Info
Manage
Authenticate your non AWS workloads and securely provide access to AWS services.

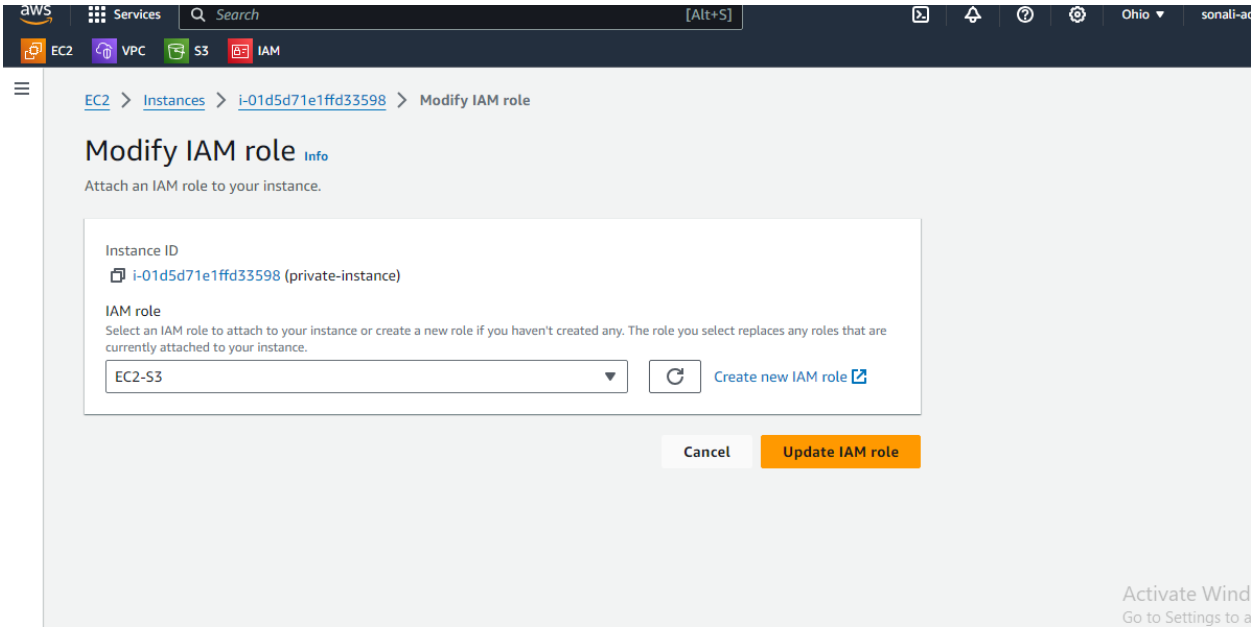

aws
Services
Search
[Alt+S]
Global
sonali-admin @ 6546-5455-5024
EC2
VPC
S3
IAM
Step 3
Name, review, and create
AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.
AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions 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.
Use case
Allow an AWS service like EC2, Lambda, or others to perform actions in this account.


aws
Services
Search
[Alt+S]
Global
sonali-admin @ 6546-5455-5024
EC2
VPC
S3
IAM
Use case
Allow an AWS service like EC2, Lambda, or others to perform actions in this account.
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.
EC2 Spot Fleet Role
Allows EC2 Spot Fleet to request and terminate Spot Instances on your behalf.
EC2 - Spot Fleet Auto Scaling
Allows Auto Scaling to access and update EC2 spot fleets on your behalf.
EC2 - Spot Fleet Tagging
Allows EC2 to launch spot instances and attach tags to the launched instances on your behalf.
EC2 - Spot Instances
Activate Windows
Go to Settings to activate Windows.


aws
Services
Search
[Alt+S]
Global
sonali-admin @ 6546-5455-5024
EC2
VPC
S3
IAM
Step 2
Add permissions
Step 3
Name, review, and create
Permissions policies (1/929) Info
Choose one or more policies to attach to your new role.
Filter by Type
s3
All types
10 matches
1
Policy name
Type
Description
AmazonDMSRedsh...
AWS managed
Provides access to manage S3 settings...
AmazonS3FullAccess
AWS managed
Provides full access to all buckets via t...
AmazonS3ObjectL...
AWS managed
Provides AWS Lambda functions permi...
AmazonS3Outpost...
AWS managed
Provides full access to Amazon S3 on ...
AmazonS3Outpost...
AWS managed
Provides read only access to Amazon S...
AmazonS3ReadOn...
AWS managed
Provides read only access to all bucket...
AWSBackupService
AWS managed
Policy containing permissions necessar...


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.
EC2-S3
Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.
Description
Add a short explanation for this role.
Allows EC2 instances to read s3 bucket
Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: _+=,. @-/\ [{}]!#$%^&*();:"'<>`


Instances (1/2) Info
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
Instance state = running
Clear filters
Name
Instance ID
Instance state
Instance type
private-instance
i-01d5d71e1ffd33598
Running
t2.micro
public-instance
i-09c256fa02ca93ef6
Running
Connect
View details
Manage instance state
Instance settings
Networking
Security
Image and templates
Monitor and troubleshoot
Change security groups
Get Windows password
Modify IAM role
i-09c256fa02ca93ef6 (public-instance)
Details
Status and alarms
Monitoring
Security
Networking
Storage
Tags
Instance summary Info
Instance ID
i-09c256fa02ca93ef6 (public-instance)
Public IPv4 address
3.17.177.230 | open address
Private IPv4 addresses
10.0.10.156
IPv6 address
Instance state
Public IPv4 DNS



Final output