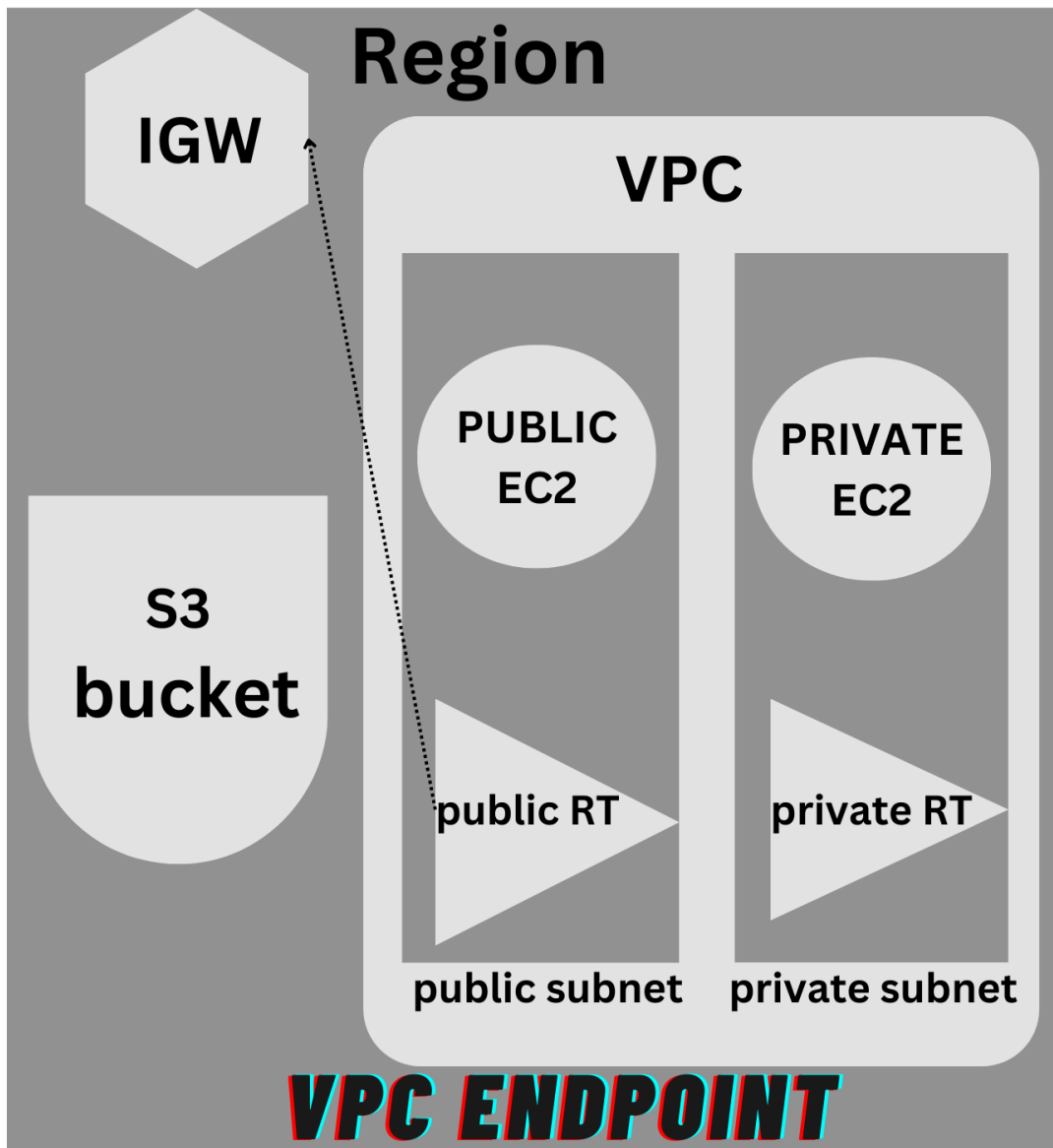


VPC Endpoint

- 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:

us-east-2.console.aws.amazon.com/vpcconsole/home?region=us-east-2#CreateVpc:createMode=vpcOnly

Services Search [Alt+S]

EC2 VPC

VPC > Your VPCs > Create VPC

Create VPC [Info](#)

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

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

Endpoint-demo

IPv4 CIDR block [Info](#)
☒ IPv4 CIDR manual input ☐ IPAM-allocated IPv4 CIDR block

IPv4 CIDR
10.0.0.0/16
CIDR block size must be between /16 and /28.

Activate Windows
Go to Settings to activate Windows

CloudShell Feedback © 2024 Amazon Web Services, Inc. or its affiliates. Privacy Terms

- Create one IGW for Public Subnet

You successfully created vpc-0dc7cc8d7b21ff684 / Endpoint-demo

VPC > Internet gateways > Create internet gateway

Create internet gateway [Info](#)

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Internet gateway settings

Name tag
Creates a tag with a key of 'Name' and a value that you specify.

IGW

Tags - optional
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key Value - optional

Name IGW Remove

Add new tag

Activate Windows
Go to Settings to activate Windows

- Attach Internet Gateway to VPC

us-east-2.console.aws.amazon.com/vpcconsole/home?region=us-east-2#igws:

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

Internet gateways (1/2) Info

Search

Name	Internet gateway ID	State
-	igw-001f4ed0dadcc13c7	Attached
<input checked="" type="checkbox"/> IGW	igw-07ed7e449e13e48d7	Detached

Actions

- Create internet gateway
- View details
- Attach to VPC
- Detach from VPC
- Manage tags
- Delete internet gateway

igw-07ed7e449e13e48d7 / IGW

Details Tags

Details

Internet gateway ID	State	VPC ID	Owner
igw-07ed7e449e13e48d7	Detached	vpc-0dc7cc8d7b21ff684	sonali-admin @ 6546-5455-502

aws Services Search [Alt+S]

EC2 VPC

VPC > Internet gateways > Attach to VPC (igw-07ed7e449e13e48d7)

Attach to VPC (igw-07ed7e449e13e48d7) [Info](#)

VPC

Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs

Attach the internet gateway to this VPC.

► AWS Command Line Interface command

Cancel **Attach internet gateway**

- Create Public Subnet

aws Services Search [Alt+S]

EC2 VPC

VPC > Subnets > Create subnet

Create subnet [Info](#)

VPC

VPC ID

Create subnets in this VPC.

Associated VPC CIDRs

IPv4 CIDRs

10.0.0.0/16

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Activate V
Go to Setting

us-east-2.console.aws.amazon.com/vpconsole/home?region=us-east-2#CreateSubnet:

aws Services Search [Alt+S]

EC2 VPC

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
public-sub
The name can be up to 256 characters long.

Availability Zone [Info](#)
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
US East (Ohio) / us-east-2a

IPv4 VPC CIDR block [Info](#)
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
10.0.0.0/16

IPv4 subnet CIDR block
10.0.10.0/24 256 IPs

▼ **Tags - optional**

Key	Value - optional	
Name	public-sub	Remove

- Create private subnet

aws Services Search [Alt+S]

EC2 VPC

Subnet 2 of 2

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
private-sub
The name can be up to 256 characters long.

Availability Zone [Info](#)
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
US East (Ohio) / us-east-2a

IPv4 VPC CIDR block [Info](#)
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
10.0.0.0/16

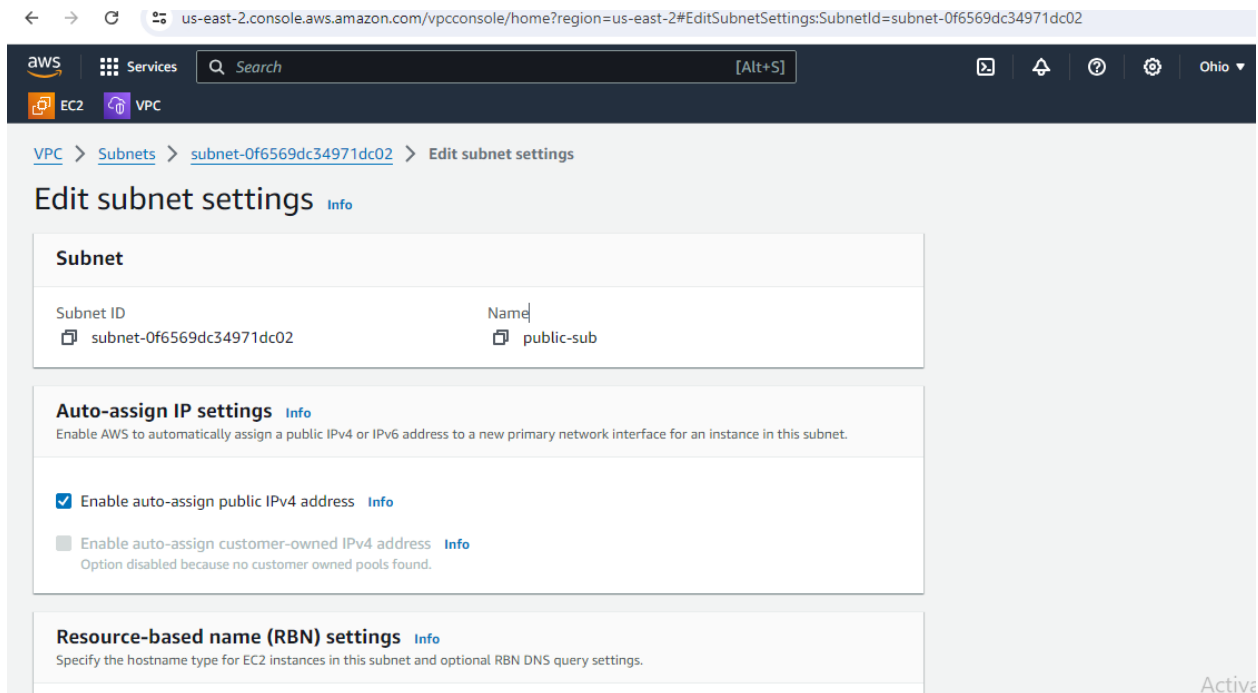
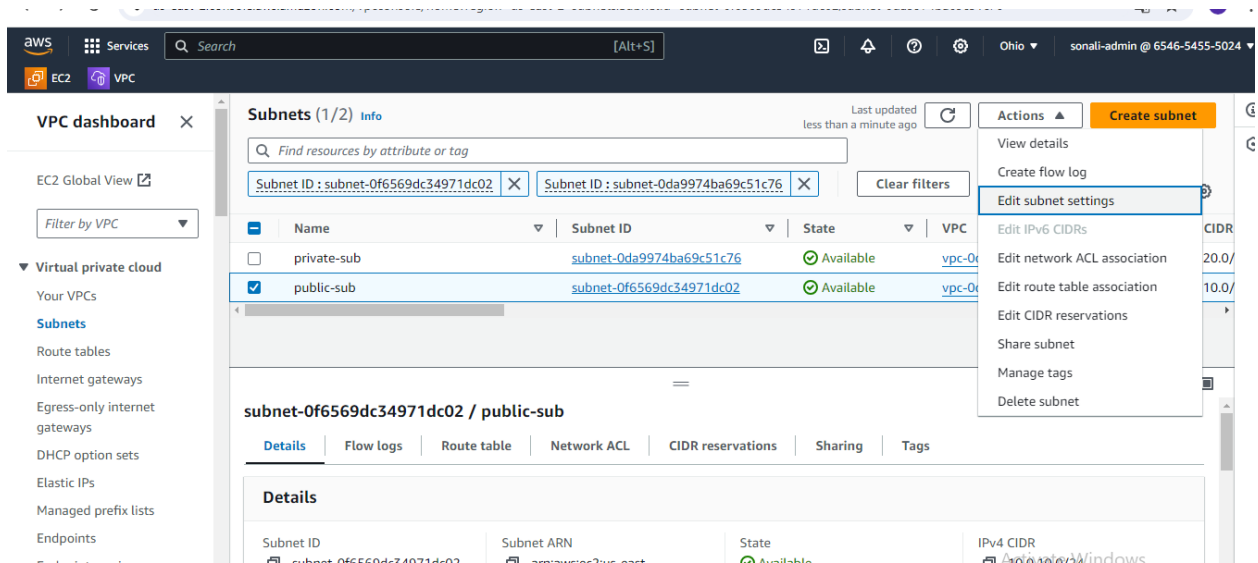
IPv4 subnet CIDR block
10.0.20.0/24 256 IPs

▼ **Tags - optional**

Key	Value - optional	
Name	private-sub	Remove

Activate Windows

- Make your subnet public by enabling the setting



- Create one Route for public subnet

aws Services Search [Alt+S] Ohio sonali-ad

EC2 VPC

VPC > Route tables > Create route table

Create route table [Info](#)

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Route table settings

Name - optional
Create a tag with a key of 'Name' and a value that you specify.

My-RT

VPC
The VPC to use for this route table.

vpc-0dc7cc8d7b21ff684 (Endpoint-demo)

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional	
Name	My-RT	Remove

- Do subnet Association with public subnet.

us-east-2.console.aws.amazon.com/vpcconsole/home?region=us-east-2#RouteTableDetails:RouteTableId=rtb-0b055efc2db4dd614

aws Services Search [Alt+S] Ohio sonali-admin @ 6546-5455-5

EC2 VPC

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

Endpoint services

You have successfully updated subnet associations for rtb-0b055efc2db4dd614 / My-RT.

VPC vpc-0dc7cc8d7b21ff684 | Endpoint-demo

Owner ID 654654555024

Routes Subnet associations Edge associations Route propagation Tags

Explicit subnet associations (1) [Edit subnet associations](#)

Find subnet association

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
public-sub	subnet-0f6569dc34971dc02	10.0.10.0/24	-

Subnets without explicit associations (1) [Edit subnet associations](#)

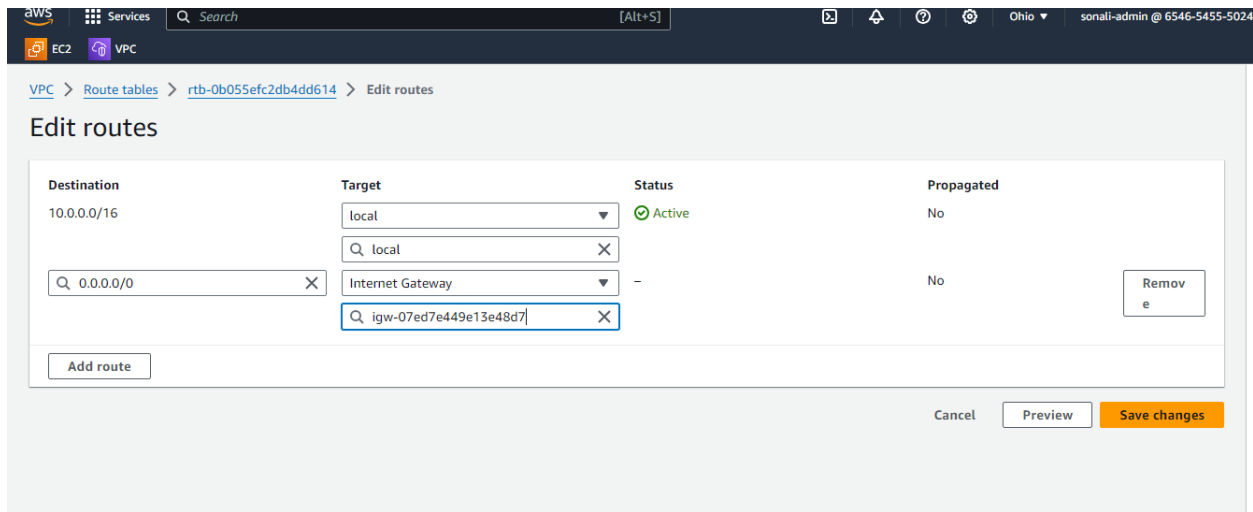
The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

Find subnet association

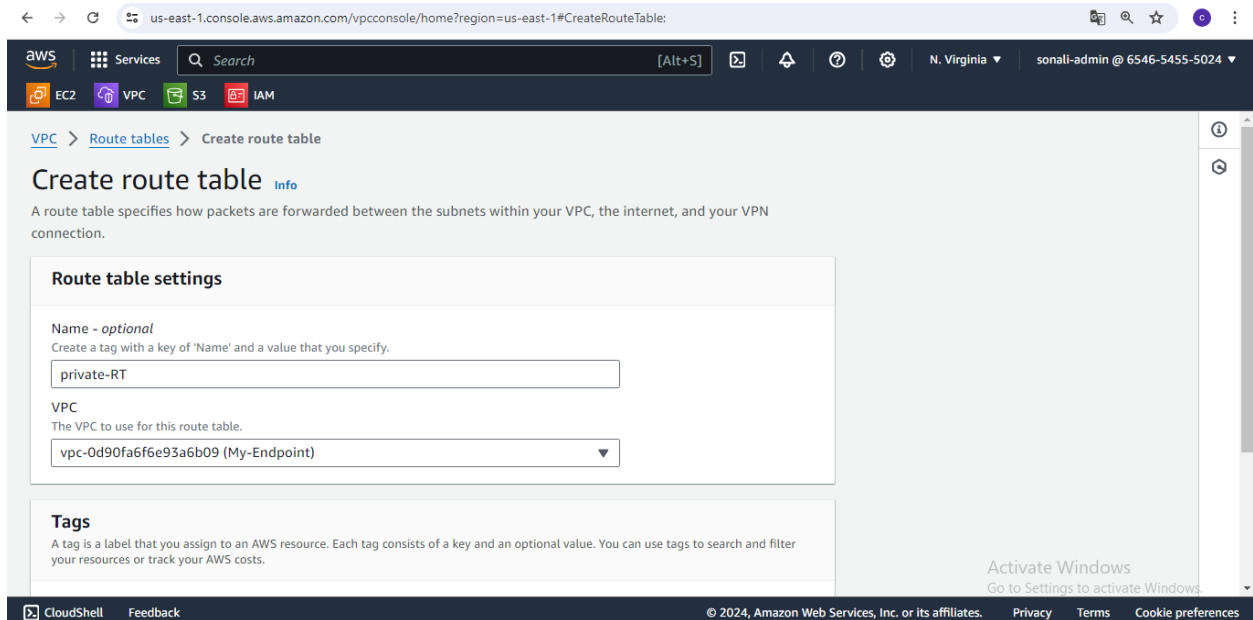
Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
private-sub	subnet-0da9974ba69c51c76	10.0.20.0/24	-

Activate Windows
Go to Settings to activate Windows.

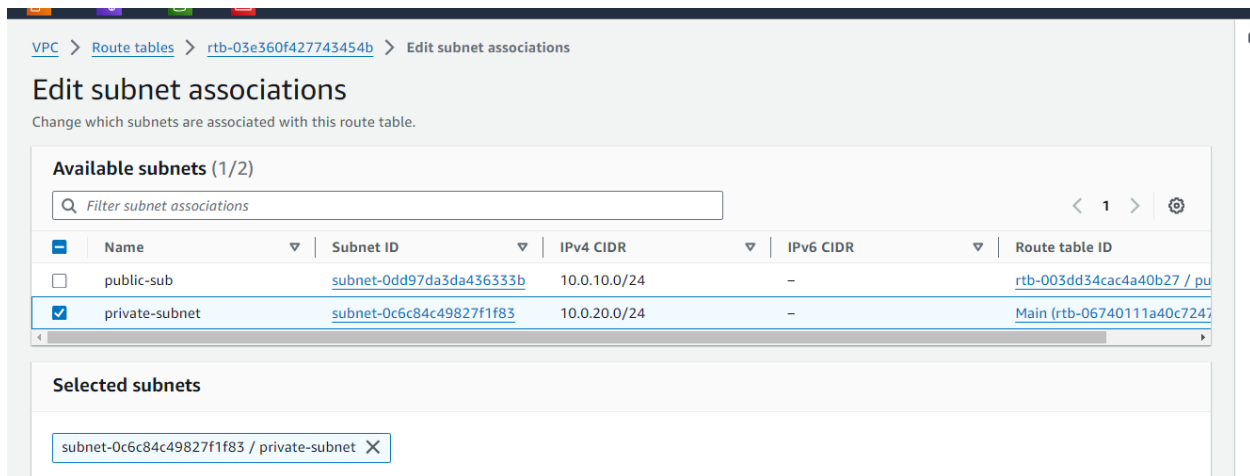
- Add Route of internet gateway to the Route Table



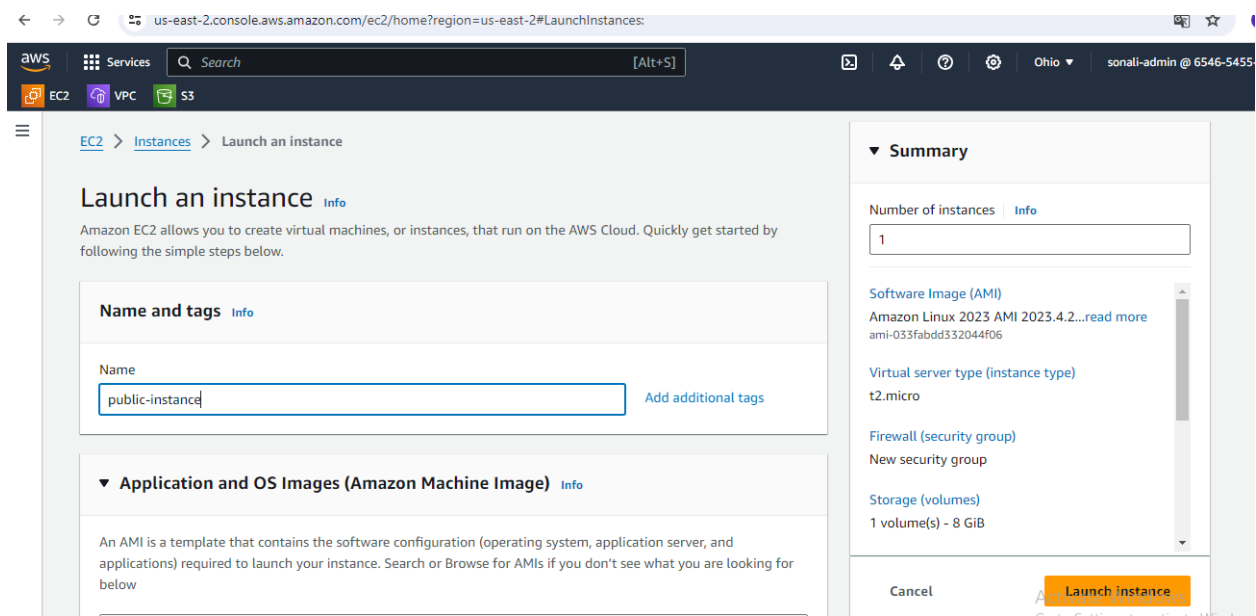
- Create private RT for private subnet.



- Do subnet Association with public subnet.



- Launch the public Instance



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

us-east-2.console.aws.amazon.com/ec2/home?region=us-east-2#LaunchInstances:

Services Search [Alt+S]

EC2 VPC S3 Ohio sonali-admin

Network settings Info

VPC - required Info

vpc-0dc7cc8d7b21ff684 (Endpoint-demo)
10.0.0.0/16

Subnet Info

subnet-0f6569dc34971dc02 public-sub
VPC: vpc-0dc7cc8d7b21ff684 Owner: 654654555024 Availability Zone: us-east-2a
IP addresses available: 251 CIDR: 10.0.10.0/24

Auto-assign public IP Info

Enable

Additional charges apply when outside of free tier allowance

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

Summary

Number of instances Info

1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.4.2...read more
ami-033fabdd332044f06

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Cancel Launch Instance

- Launch private instance and select private subnet

us-east-2.console.aws.amazon.com/ec2/home?region=us-east-2#LaunchInstances:

Services Search [Alt+S]

EC2 VPC S3 Ohio sonali-admin @ 6546-5455-50

EC2 > Instances > Launch an instance

Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags Info

Name

private-instance Add additional tags

Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Summary

Number of instances Info

1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.4.2...read more
ami-033fabdd332044f06

Virtual server type (instance type)

t2.micro

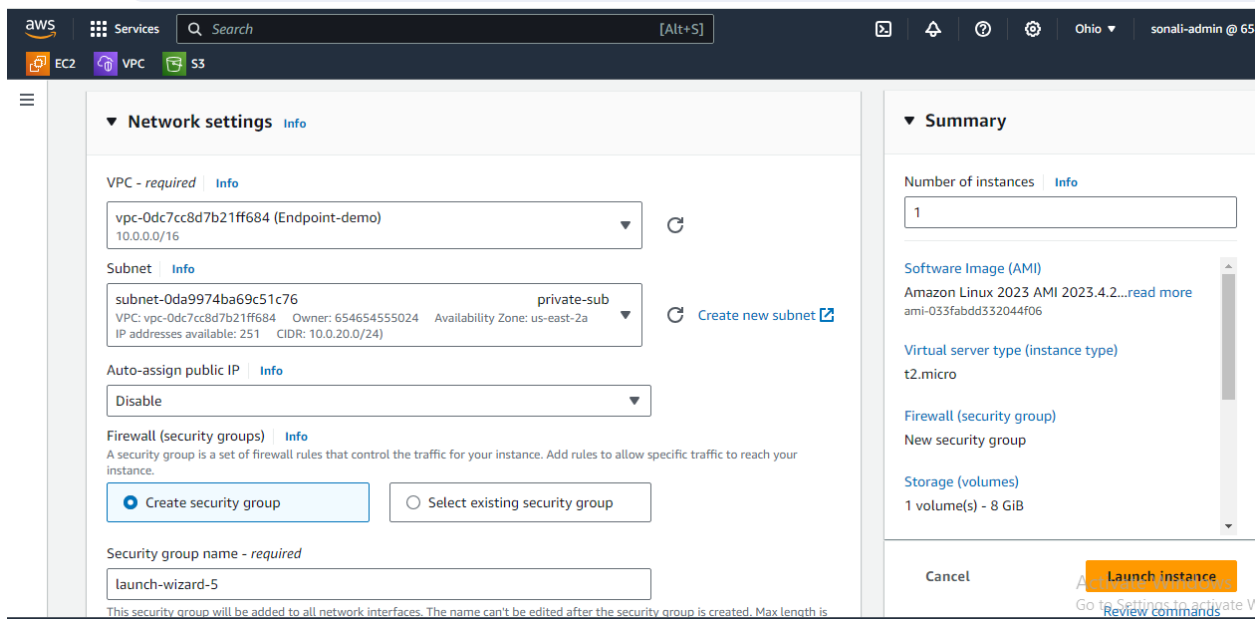
Firewall (security group)

New security group

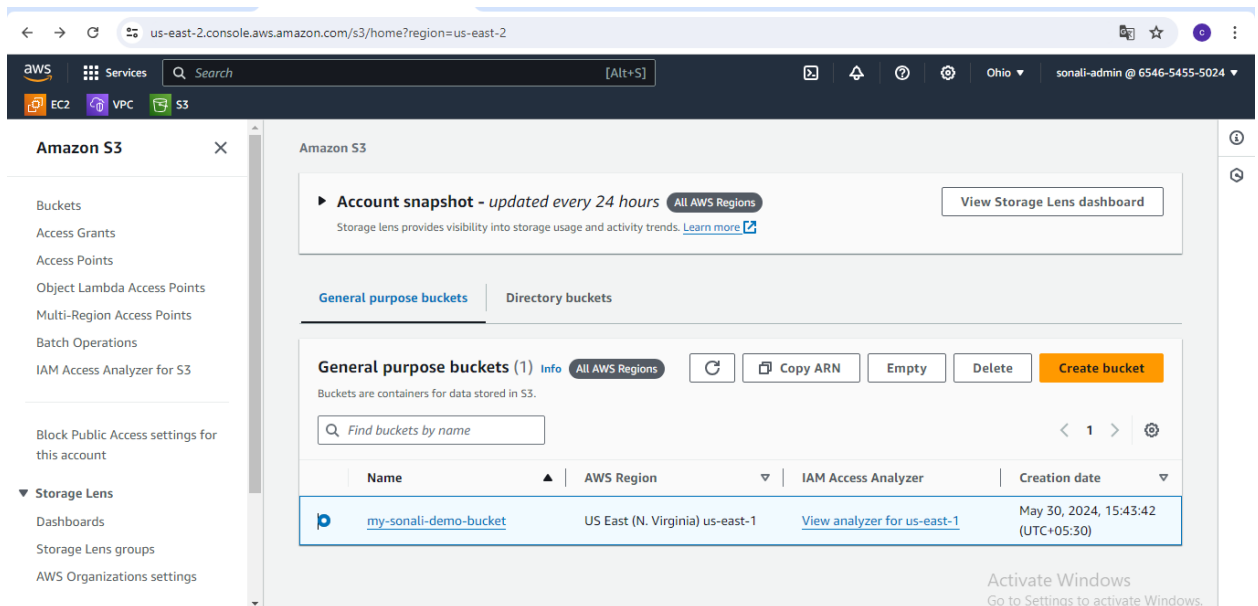
Storage (volumes)

1 volume(s) - 8 GiB

Cancel Launch Instance



- Create s3 Bucket



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

```
aws | Services | Search [Alt+S]
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]
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
```


aws

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 X Clear filters


< 1 > ⚙


	Service Name	Owner	Type
<input type="radio"/>	com.amazonaws.s3-global.accesspoint	amazon	Interface
<input checked="" type="radio"/>	com.amazonaws.us-east-2.s3	amazon	Gateway
<input type="radio"/>	com.amazonaws.us-east-2.s3	amazon	Interface
<input type="radio"/>	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](#) 


<input type="checkbox"/>	Name	Route Table ID	Main	Associated Id
<input checked="" type="checkbox"/>	private-RT	rtb-03e360f427743454b (private-RT)	No	subnet-0c6c84c49827f1f8
<input type="checkbox"/>	public RT	rtb-003dd34cac4a40b27 (public RT)	No	subnet-0dd97da3da43633
<input type="checkbox"/>	-	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 addresses, not public IP addresses. Existing connections from your affected subnets to the AWS service that use public IP addresses may be disrupted. Ensure that you...


us-east-2.console.aws.amazon.com/vpcconsole/home?region=us-east-2#Endpoints:vpcEndpointId=vpc-0c666443e12539427

Services [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**
vpc-0c666443e12539427 

Endpoints (1/1) [Info](#)  **Actions**  **Create endpoint**

<input checked="" type="checkbox"/>	Name	VPC endpoint ID	VPC ID	Service name
<input checked="" type="checkbox"/>	My-Endpoint	vpc-0c666443e12539427	vpc-0dc7cc8d7b21ff684 Endpoint-demo	com.amazonaws.us-east-2.s3

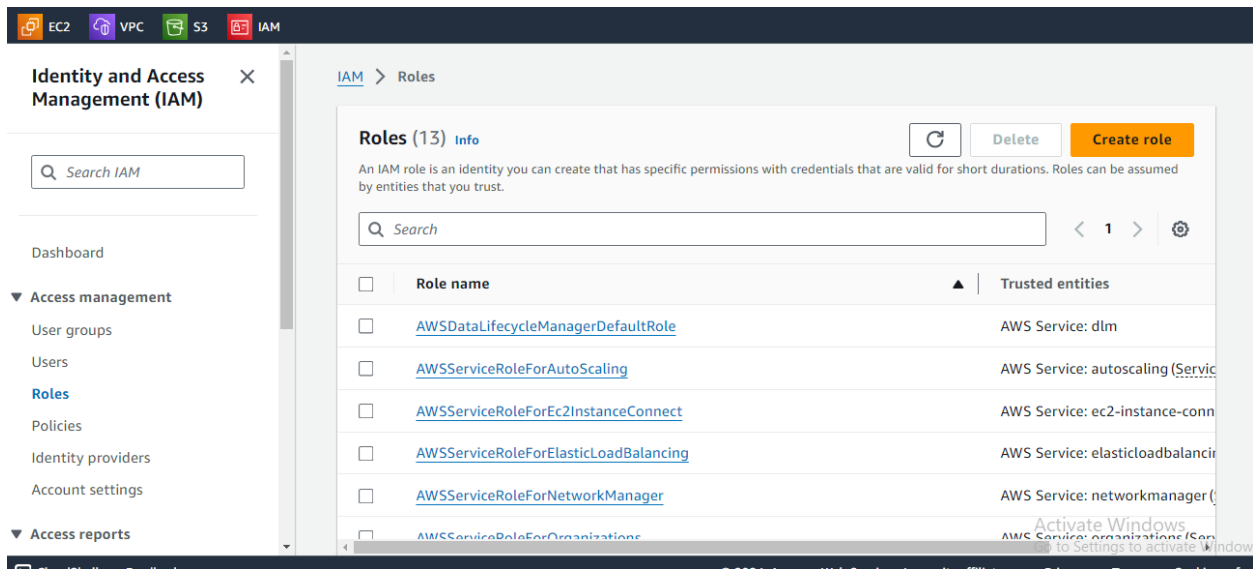
vpce-0c666443e12539427 / My-Endpoint

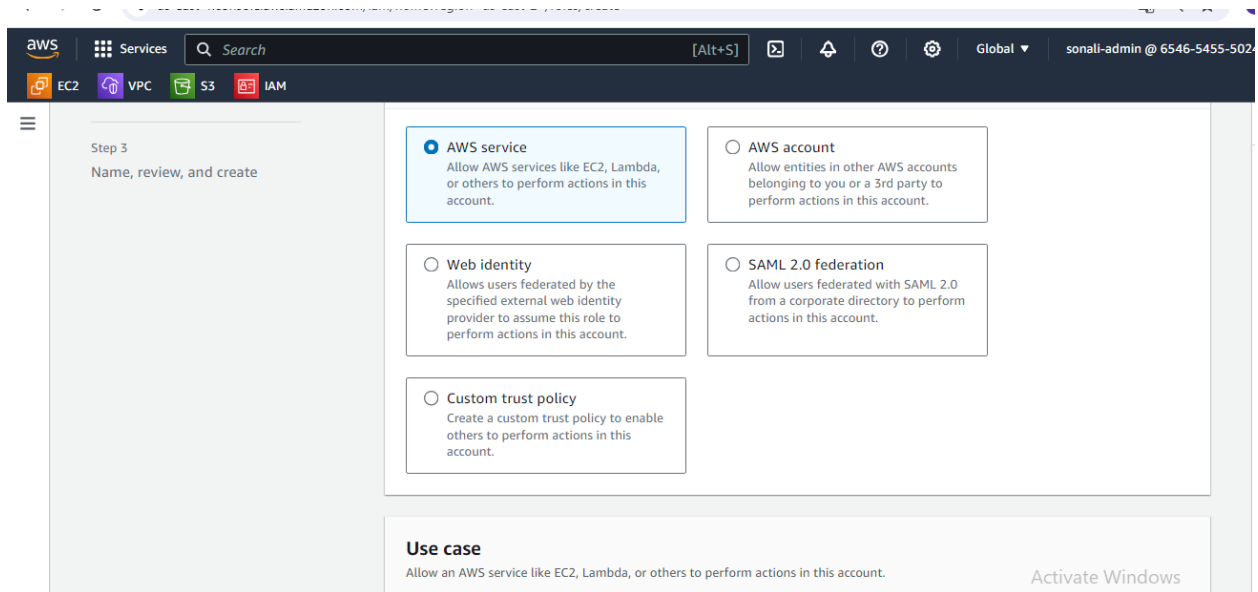
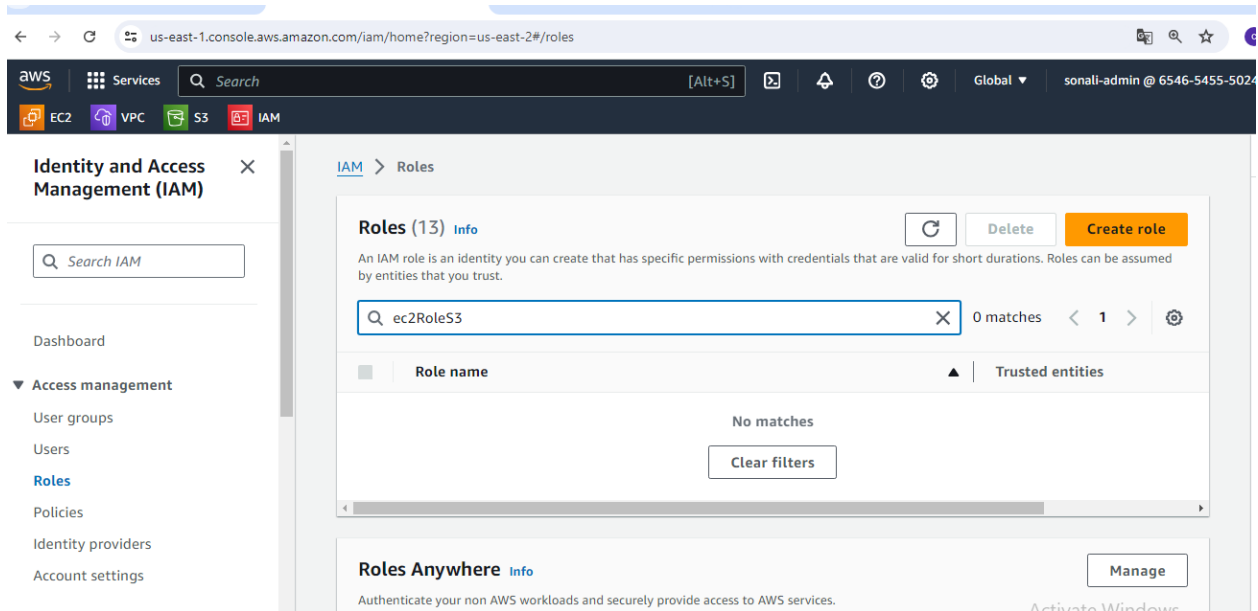
[Details](#) [Route tables](#) [Policy](#) [Tags](#)

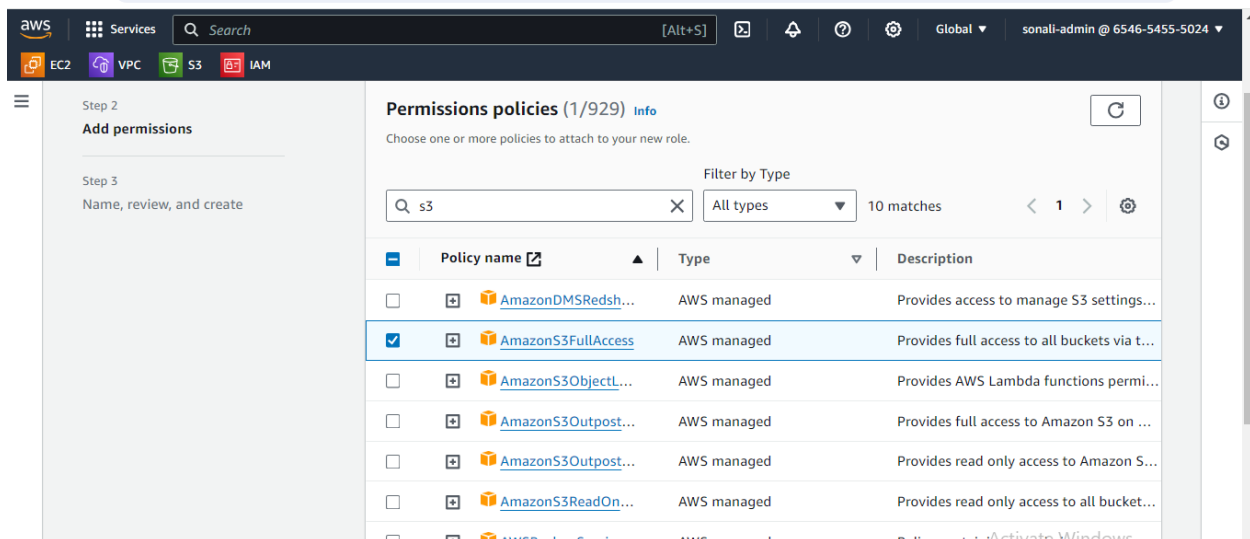
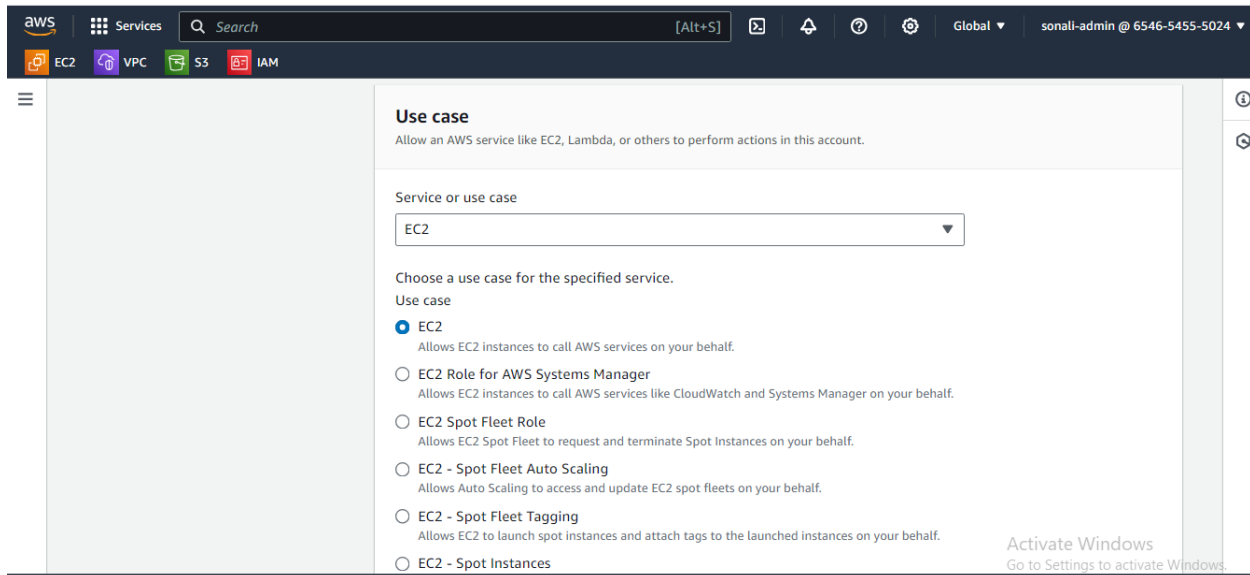
Details


```
aws
Services
Search [Alt+S]
EC2 VPC S3
Last login: Sat Jun 22 09:47:23 2024 from 3.16.146.4
[ec2-user@ip-10-0-10-156 ~]$ ls
linux_ohio.pem
[ec2-user@ip-10-0-10-156 ~]$ ssh -i "linux_ohio.pem" ec2-user@10.0.20.164
#
#####
      Amazon Linux 2023
#####
      https://aws.amazon.com/linux/amazon-linux-2023
#####
Last login: Sat Jun 22 09:47:58 2024 from 10.0.10.156
[ec2-user@ip-10-0-20-164 ~]$ aws s3 ls
Unable to locate credentials. You can configure credentials by running "aws configure".
[ec2-user@ip-10-0-20-164 ~]$
```

Create Role for password







us-east-1.console.aws.amazon.com/iam/home?region=us-east-2#/roles/create?trustedEntityType=AWS_SDKVULC&selectedService=EC2&selectedUseCase=EC2&pol...

aws Services Search [Alt+S] Global sonali-admin @ 6546-54

EC2 VPC S3 IAM

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: _+@, @-/ \ [] ! # \$ % ^ & * () ; ' " < > `

us-east-2.console.aws.amazon.com/ec2/home?region=us-east-2#Instances:instanceState=running

aws Services Search [Alt+S] Ohio sonali-admin @ 6546-5455-5024

EC2 VPC S3 IAM

EC2 Dashboard
EC2 Global View
Events

▼ Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations

▼ Images
AMIs
AMI Catalog

Instances (1/2) Info

Find Instance by attribute or tag (case-sensitive)

Instance state = running Clear filters

Name	Instance ID	Instance state	Instance type	Status checks
private-instance	i-01d5d71e1ffd33598	Running	t2.micro	2/2 checks passing
<input checked="" type="checkbox"/> public-instance	i-09c256fa02ca93ef6	Running	t2.micro	2/2 checks passing

Actions

- Connect
- View details
- Manage instance state
- Instance settings
- Networking
- Security
- Image and templates
- Monitor and troubleshoot

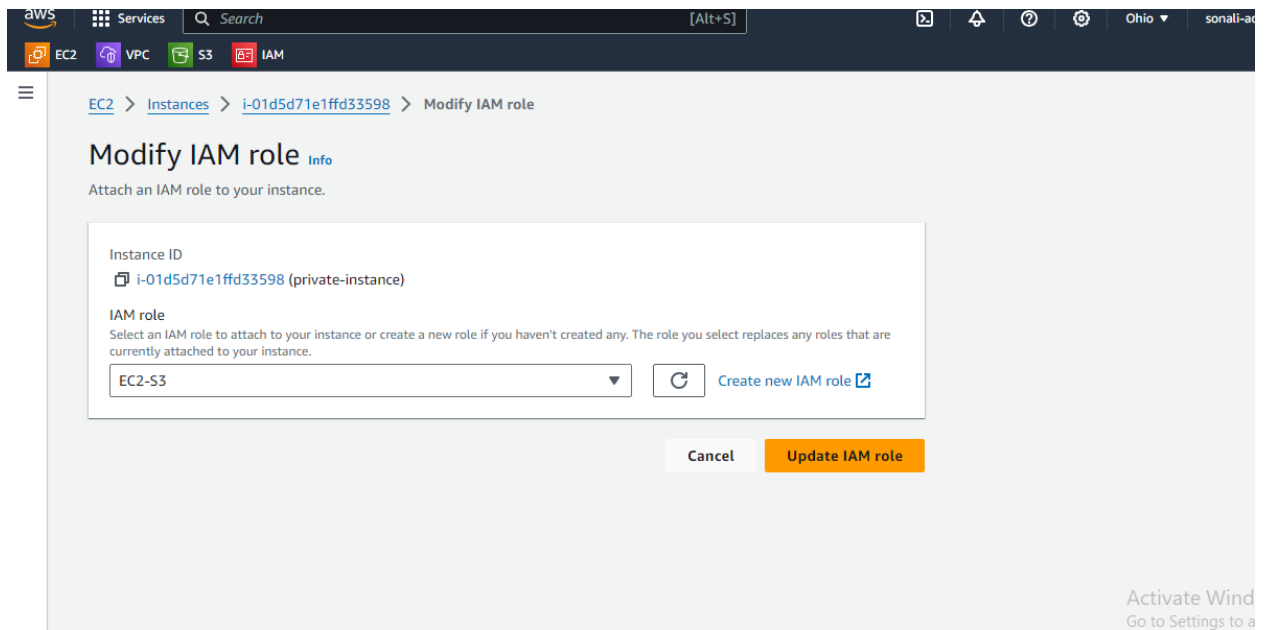
Change security groups
Get Windows password
Modify IAM role

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

```
aws s3 ls
2024-06-22 10:22:18 my-demo-sonali
2024-05-30 10:13:42 my-sonali-demo-bucket
```