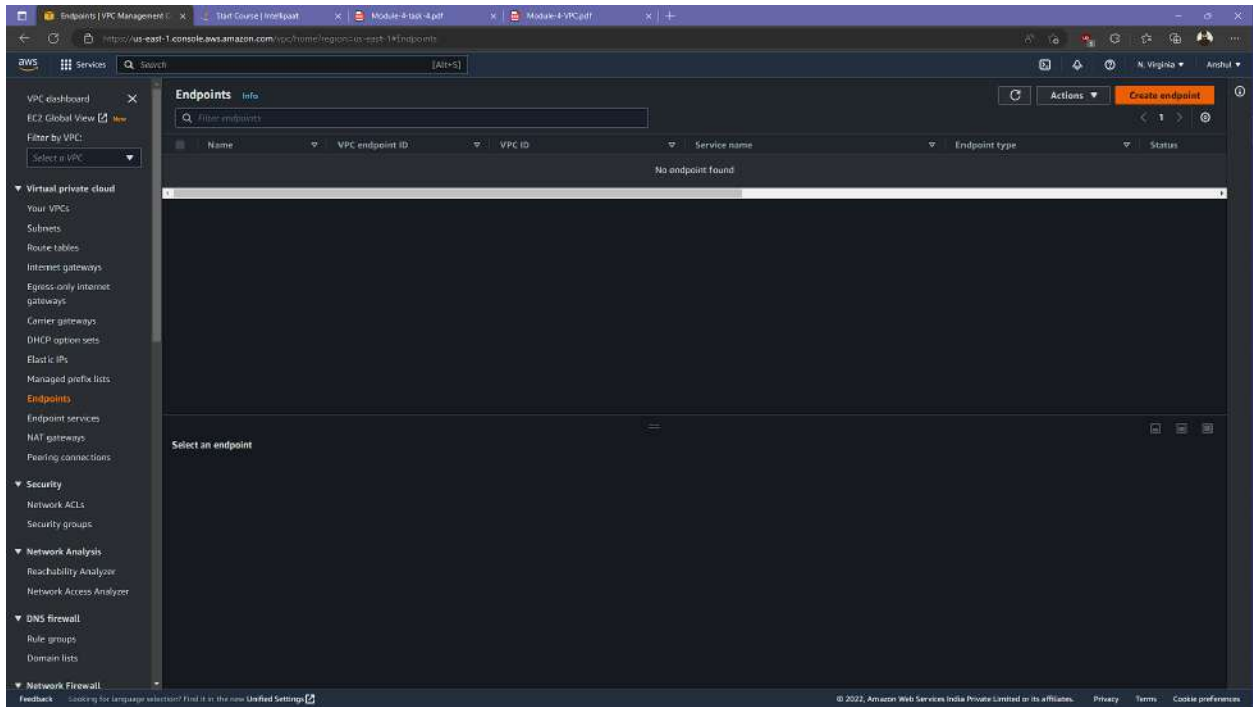


Module 4: VPC Assignment - 4

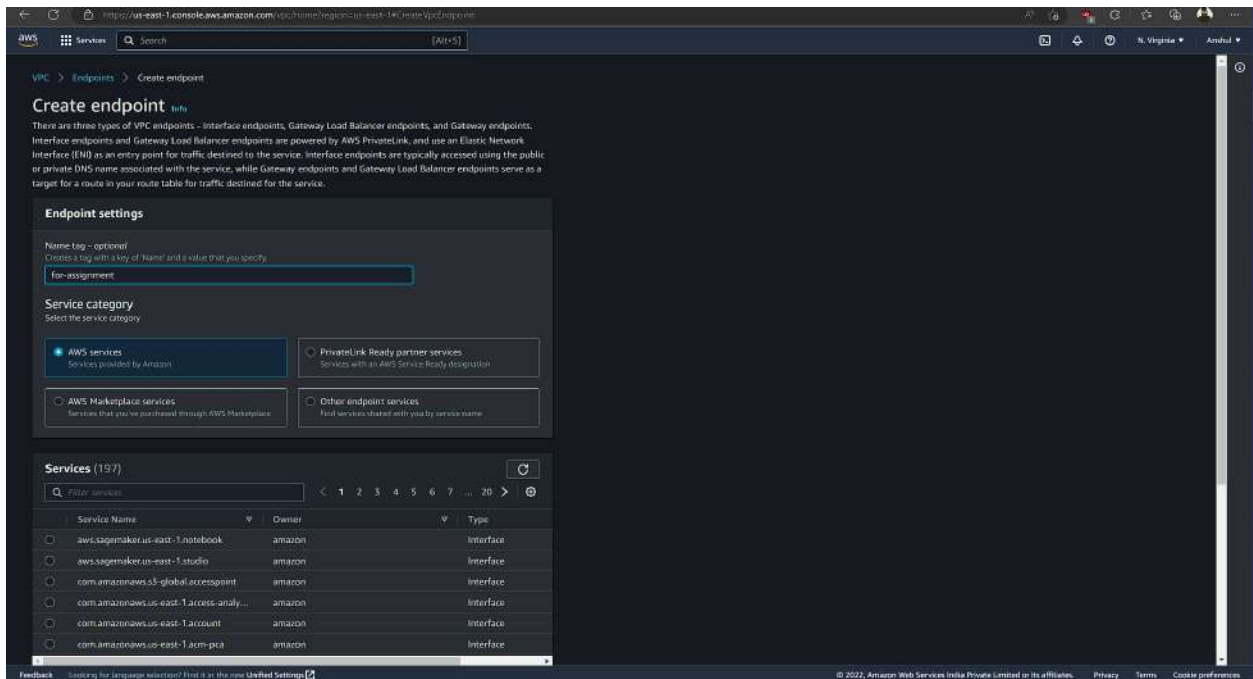
You have been asked to:

1. Create a VPC Endpoint for an S3 bucket of your choice.

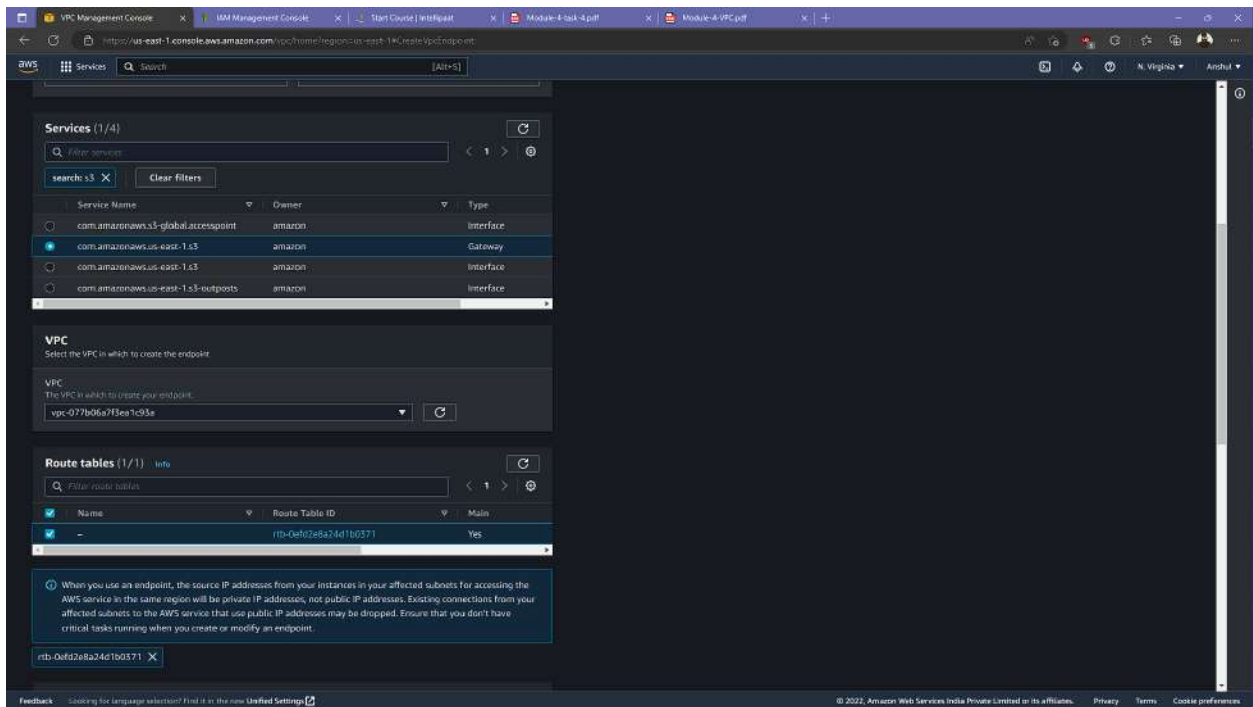
Create an endpoint by selecting 'Endpoints' feature in VPC services.



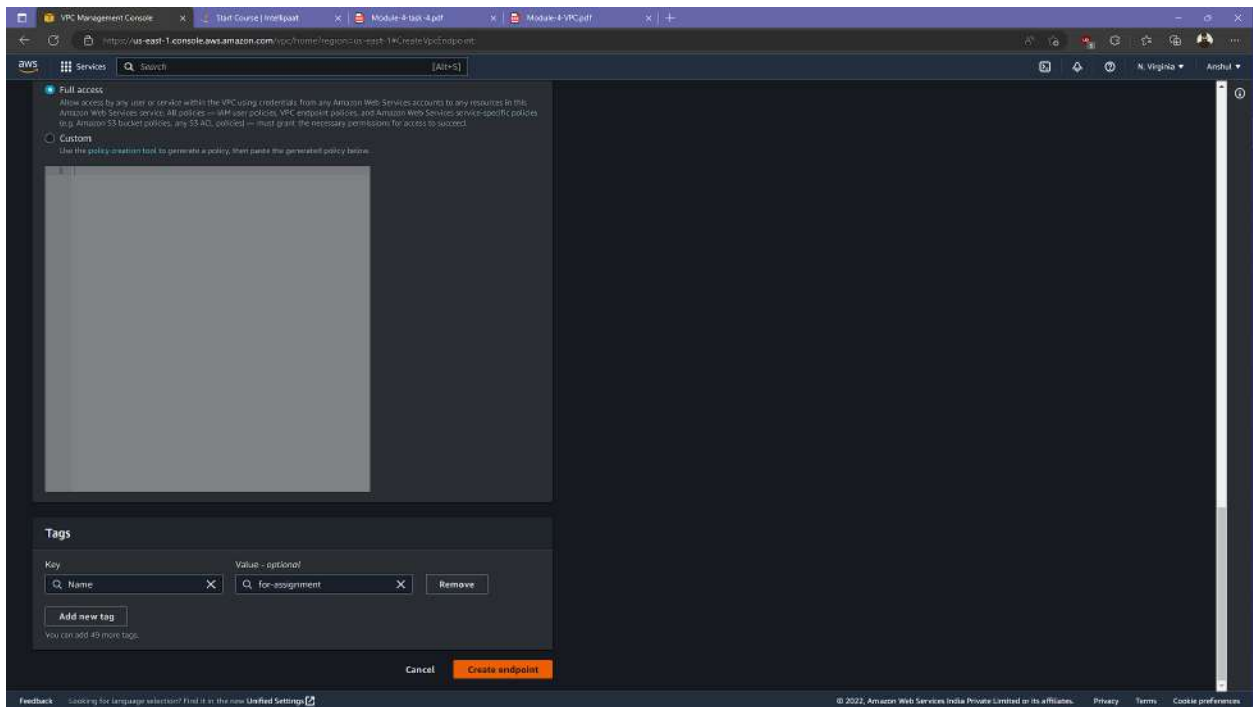
Give a name to your endpoint.



Select S3 services and default VPC and Route Table.



Create an endpoint.



Endpoint has been created.

The screenshot shows the AWS Management Console for the 'us-east-1' region. A green notification banner at the top states 'Successfully created VPC endpoint vpc-06f19b424dc40b04'. Below this, the 'Endpoints (1/1)' section displays a table with one endpoint:

Name	VPC endpoint ID	VPC ID	Service name	Endpoint type	Status
for-assignment	vpc-06f19b424dc40b04	vpc-077b66a7d3e1c53e	com.amazonaws.us-east-1.ec2	Interface	Pending

Below the table, the 'Details' section for the endpoint 'vpc-06f19b424dc40b04 / for-assignment' is shown. It includes fields for Endpoint ID, VPC ID, Status (Pending), Creation time (Thursday, December 22, 2022 at 20:40:16 GMT+5:30), Endpoint type (Interface), and Private DNS names enabled.

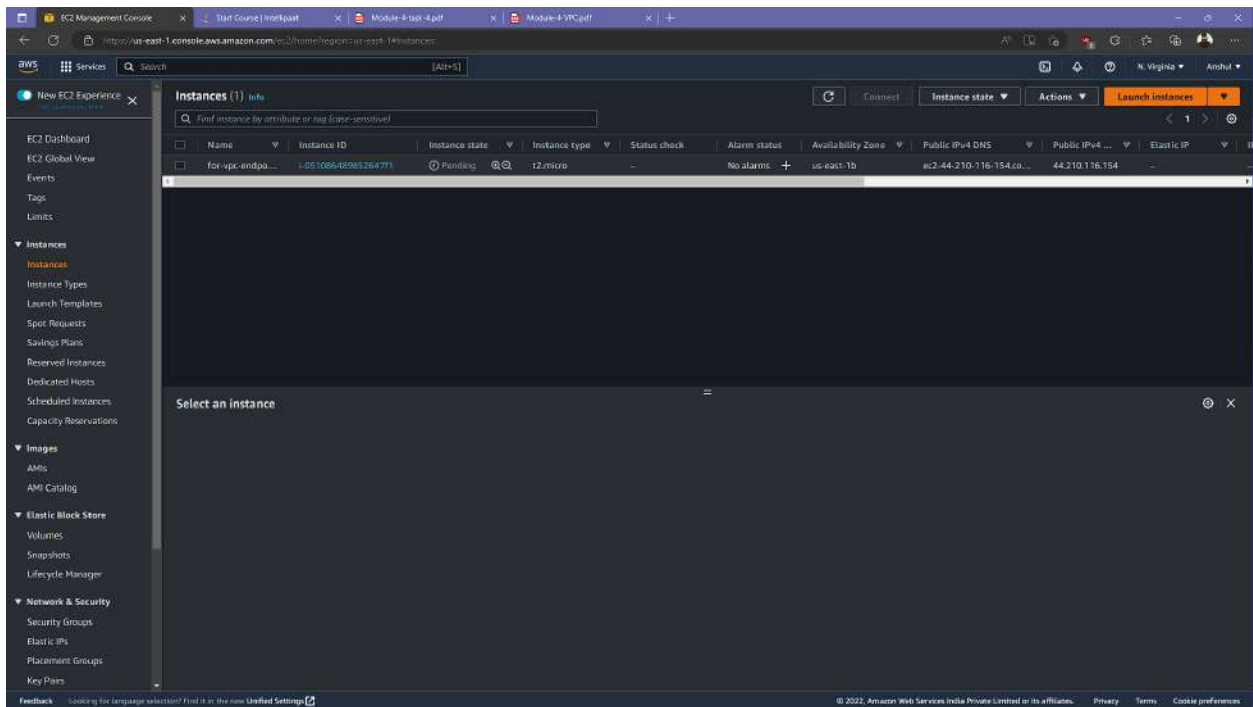
Let's create an instance for accessing the s3 bucket from endpoint.

The screenshot shows the 'Launch an instance' page in the AWS Management Console. The 'Name and tags' section has the name 'for-vpc-endpoint'. The 'Application and OS Images (Amazon Machine Image)' section shows a search bar and a list of AMIs. The 'Summary' section on the right provides details about the instance configuration:

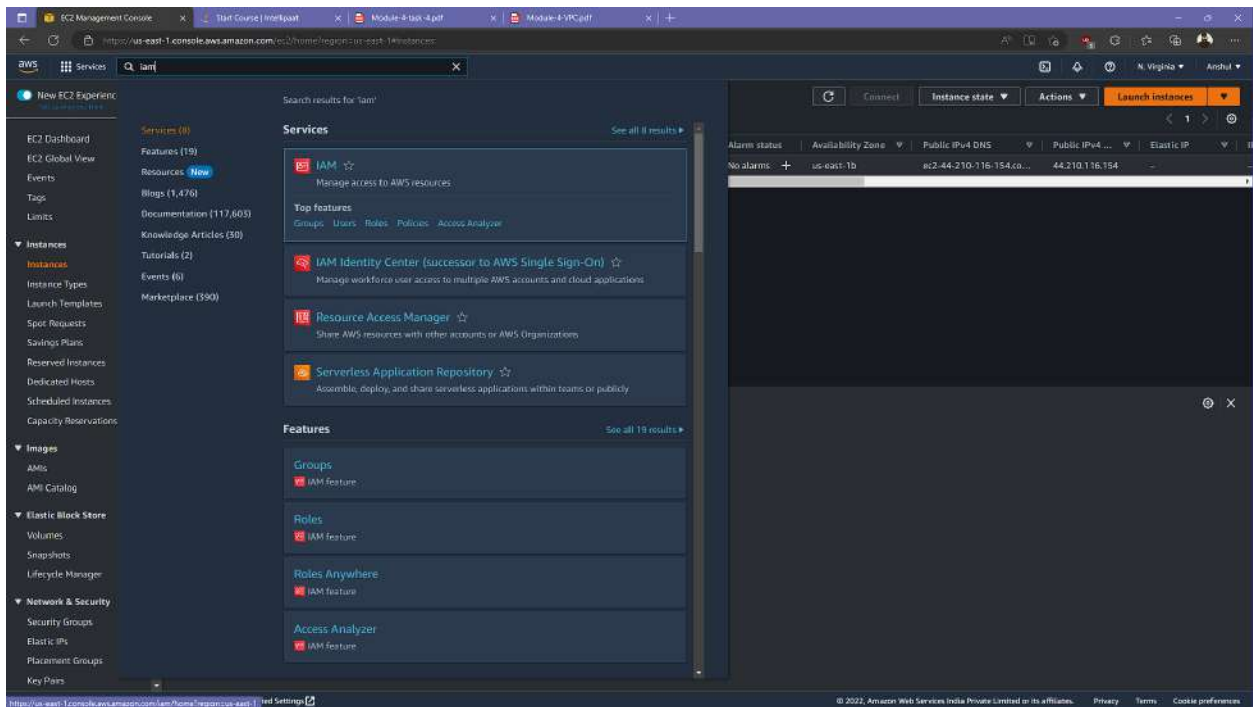
- Number of instances: 1
- Software (image (AMI)): Amazon Linux 2 Kernel 5.10 AMI (local more ami-056ea7688371c61)
- Virtual server type (instance type): t2.micro
- Firewall (security group): New security group
- Storage (volumes): 1 volume(s) - 8 GiB

A 'Free tier' notification is displayed, stating that the first year includes 750 hours of t2.micro usage. The 'Launch instance' button is visible at the bottom right.

Instance has been created.



To make a role, Go to IAM services.



Select create roles.

The screenshot shows the AWS IAM console 'Roles' page. The left sidebar contains navigation links for Identity and Access Management (IAM), Access management, Users, Policies, Identity providers, Account settings, Access reports, and Related console links. The main content area displays a list of roles with columns for Role name, Trusted entities, and Last activity. A 'Create role' button is visible in the top right. Below the list, there are sections for 'Roles Anywhere' and 'Access AWS from your non AWS workloads'.

Role name	Trusted entities	Last activity
AWSServiceRoleForAmazonElasticFileSystem	AWS Service: elasticfilesystem (Service-Linked Role)	6 days ago
AWSServiceRoleForAutoScaling	AWS Service: autoscaling (Service-Linked Role)	Yesterday
AWSServiceRoleForBackup	AWS Service: backup (Service-Linked Role)	10 hours ago
AWSServiceRoleForElasticLoadBalancing	AWS Service: elasticloadbalancing (Service-Linked Role)	Yesterday
AWSServiceRoleForRDS	AWS Service: rds (Service-Linked Role)	7 days ago
AWSServiceRoleForSupport	AWS Service: support (Service-Linked Role)	-
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linked Role)	-
rds-monitoring-role	AWS Service: monitoring.rds	-

Choose a use case as EC2.

The screenshot shows the 'Create role' wizard in the AWS IAM console, specifically Step 1: Select trusted entity. The wizard is titled 'Select trusted entity' and includes a 'Trusted entity type' section with radio buttons for AWS service, AWS account, Web identity, SAML 2.0 federation, and Custom trust policy. The 'Use case' section has a 'Common use cases' section with radio buttons for EC2 and Lambda, and a 'Use cases for other AWS services' section with a dropdown menu. The 'Next' button is visible at the bottom right.

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: Allow 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.

Common use cases

- ☒ EC2: Allow EC2 instances to call AWS services on your behalf.
- ☐ Lambda: Allow Lambda functions to call AWS services on your behalf.

Use cases for other AWS services

Choose a service to view use case

Give permission to Full S3 Access.

The screenshot shows the 'Add permissions' step in the AWS IAM console. The left sidebar indicates the current step is 'Add permissions'. The main area is titled 'Add permissions' and shows a list of permissions policies. The 'AmazonS3FullAccess' policy is selected, indicated by a blue checkmark. Below the list, there is a section for 'Set permissions boundary - optional'.

Permissions policies (Selected 1/801)

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

Filter policies by property or policy name and press enter: 9 matches

Policy name Type Description

- ☐ AmazonDMSRedshif... AWS ma... Provides access to manage S3 settings for Redshift endpoints for DMS.
- ☒ AmazonS3FullAccess AWS ma... Provides full access to all buckets via the AWS Management Console.
- ☐ QuickSightAccessPo... AWS ma... Policy used by QuickSight team to access customer data produced by S3 Storage Management Analytics.
- ☐ AmazonS3ReadOnly... AWS ma... Provides read only access to all buckets via the AWS Management Console.
- ☐ AmazonS3Outposts... AWS ma... Provides full access to Amazon S3 on Outposts via the AWS Management Console.
- ☐ AWSBackupServiceI... AWS ma... Policy containing permissions necessary for AWS Backup to backup data in any S3 bucket. This includes read access to all S3 objects and any decrypt access for all...
- ☐ AWSBackupServiceI... AWS ma... Policy containing permissions necessary for AWS Backup to restore a S3 backup to a bucket. This includes read/write permissions to all S3 buckets, and permission...
- ☐ AmazonS3ObjectLa... AWS ma... Provides AWS Lambda functions permissions to interact with Amazon S3 Object Lambda. Also grants Lambda permissions to write to CloudWatch Logs.
- ☐ AmazonS3Outposts... AWS ma... Provides read only access to Amazon S3 on Outposts via the AWS Management Console.

Set permissions boundary - optional

Get a permissions boundary to control the maximum permissions this role can have. This is not a common setting, but you can use it to delegate permission management to others.

Cancel Previous Next

Give name to the role.

The screenshot shows the 'Name, review, and create' step in the AWS IAM console. The left sidebar indicates the current step is 'Name, review, and create'. The main area is titled 'Name, review, and create' and shows the 'Role details' section. The 'Role name' field is filled with 'for endpoint i'. The 'Description' field is filled with 'Allows EC2 instances to call AWS services on your behalf'. Below the description, there is a section for 'Step 1: Select trusted entities'.

Role details

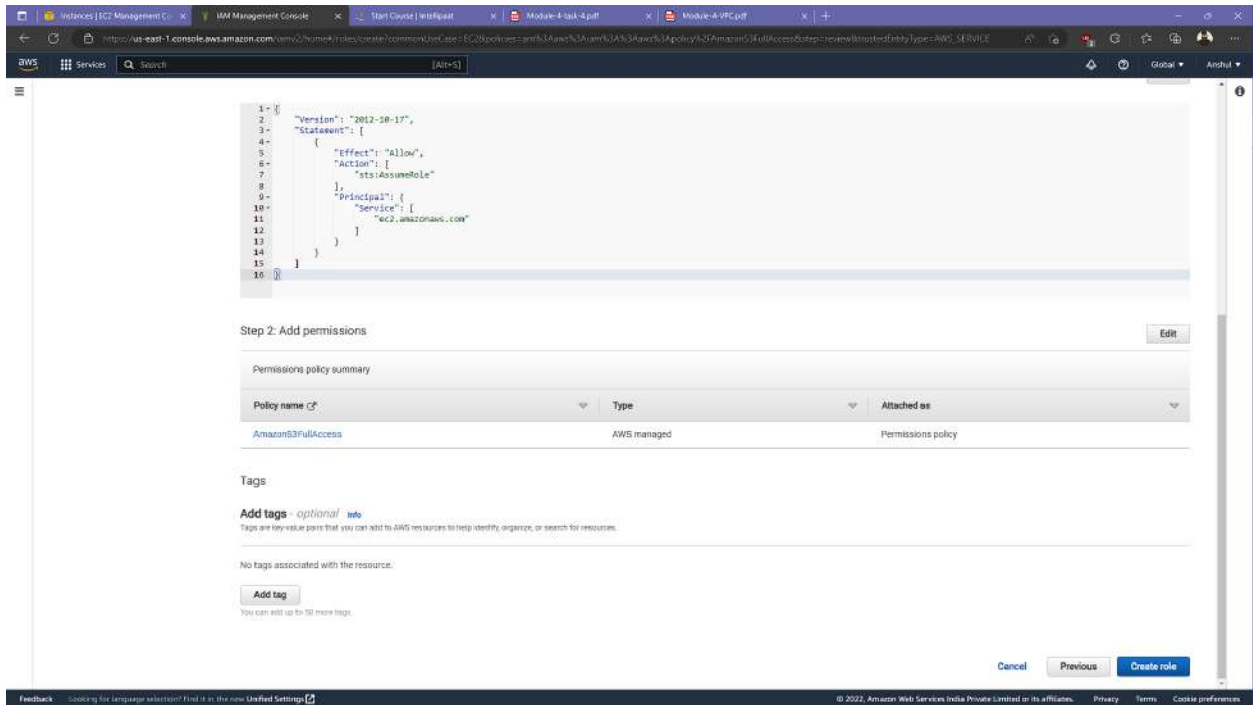
Role name: for endpoint i

Description: Allows EC2 instances to call AWS services on your behalf.

Step 1: Select trusted entities

```
1- {
2-   "Version": "2012-10-17",
3-   "Statement": [
4-     {
5-       "Effect": "Allow",
6-       "Action": [
7-         "sts:AssumeRole"
8-       ],
9-       "Principal": {
10-        "Service": [
11-          "ec2.amazonaws.com"
12-        ]
13-      }
14-    ]
15-  }
16- }
```


Select create role.



The screenshot shows the AWS IAM console interface for creating a new role. The role is named "ec2.amazonaws.com" and is attached to the "AmazonS3FullAccess" policy. The "Add permissions" step is shown, with a table listing the policy name, type, and attached permissions.

```
1- {
2-   "Version": "2012-10-17",
3-   "Statement": [
4-     {
5-       "Effect": "allow",
6-       "Action": [
7-         "sts:AssumeRole"
8-       ],
9-       "Principal": {
10-        "Service": [
11-          "ec2.amazonaws.com"
12-        ]
13-      }
14-    ]
15-  }
16- }
```

Step 2: Add permissions

Permissions policy summary

Policy name	Type	Attached as
AmazonS3FullAccess	AWS managed	Permissions policy

Tags

Add tags - optional

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

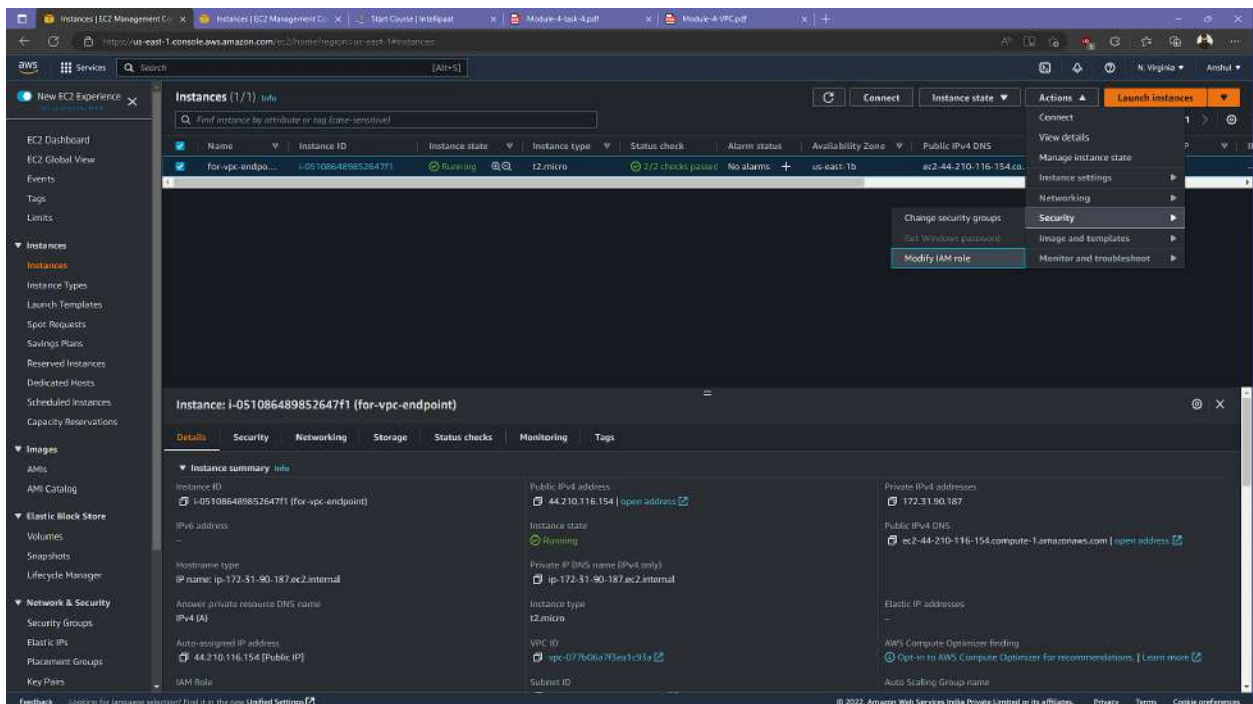
No tags associated with the resource.

Add tag

You can add up to 50 more tags.

Cancel Previous Create role

Now apply that role to ec2 instance. Select ec2 instance, in actions drop down menu go to security and modify roles.



The screenshot shows the AWS Management Console interface for the 'Instances' page. The 'Actions' dropdown menu is open, showing options like 'Connect', 'View details', 'Manage instance state', 'Instance settings', 'Networking', 'Security', 'Image and templates', and 'Monitor and troubleshoot'. The 'Security' option is highlighted, leading to the 'Modify IAM role' action.

Instances (1/1) info

Find instance by attribute or tag (case-sensitive)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
for-ec2-endo...	i-051086489852647f1	running	t2.micro	2/2 checks passed	No alarms	us-east-1b	ec2-44-210-116-154.co

Instance: i-051086489852647f1 (for-vpc-endpoint)

Details Security Networking Storage Status checks Monitoring Tags

Instance summary

Instance ID: i-051086489852647f1 (for-vpc-endpoint)

Public IPv4 address: 44.210.116.154 | open address

Private IPv4 address: 172.31.90.187

Instance state: running

Public IPv4 DNS: ec2-44-210-116-154.compute-1.amazonaws.com | open address

Private IP (DNS name (IPv4 only)): ip-172-31-90-187.ec2.internal

Instance type: t2.micro

VPC ID: vpc-07b06a703e1c93a

Subnet ID: subnet-07b06a703e1c93a

Hostname type: ec2-internal

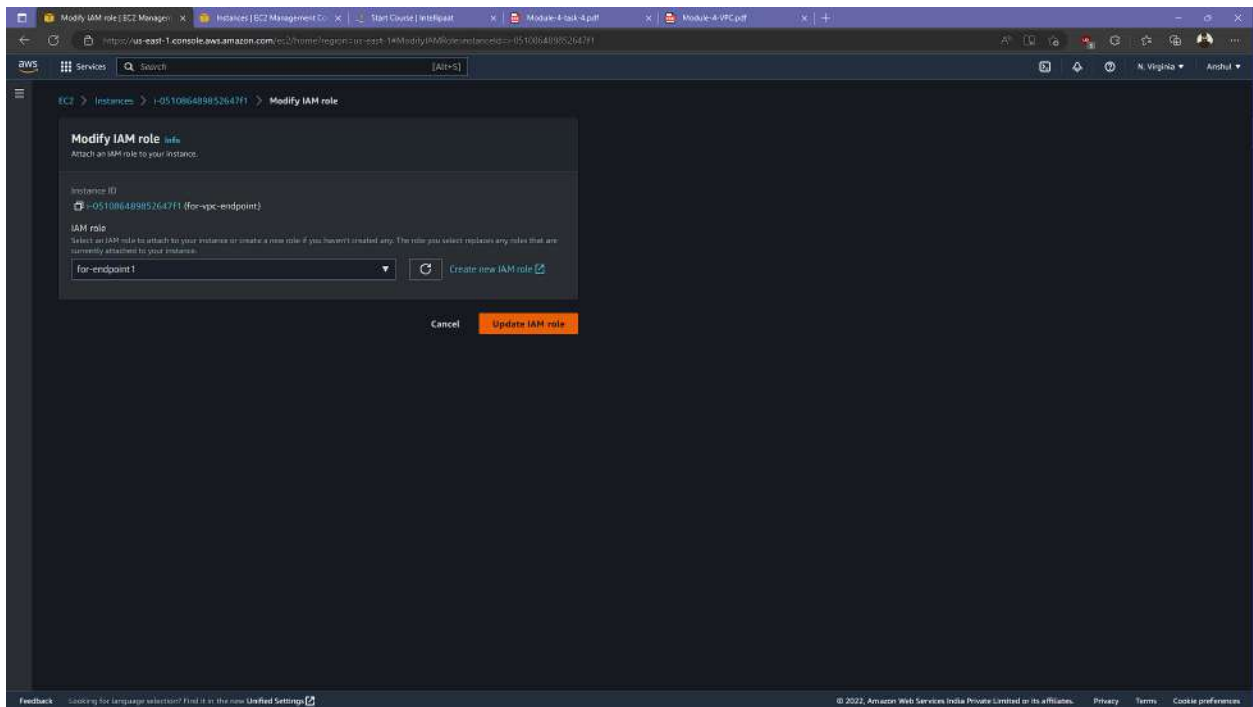
IP name: ip-172-31-90-187.ec2.internal

Answer private resource DNS name: ip-172-31-90-187.ec2.internal

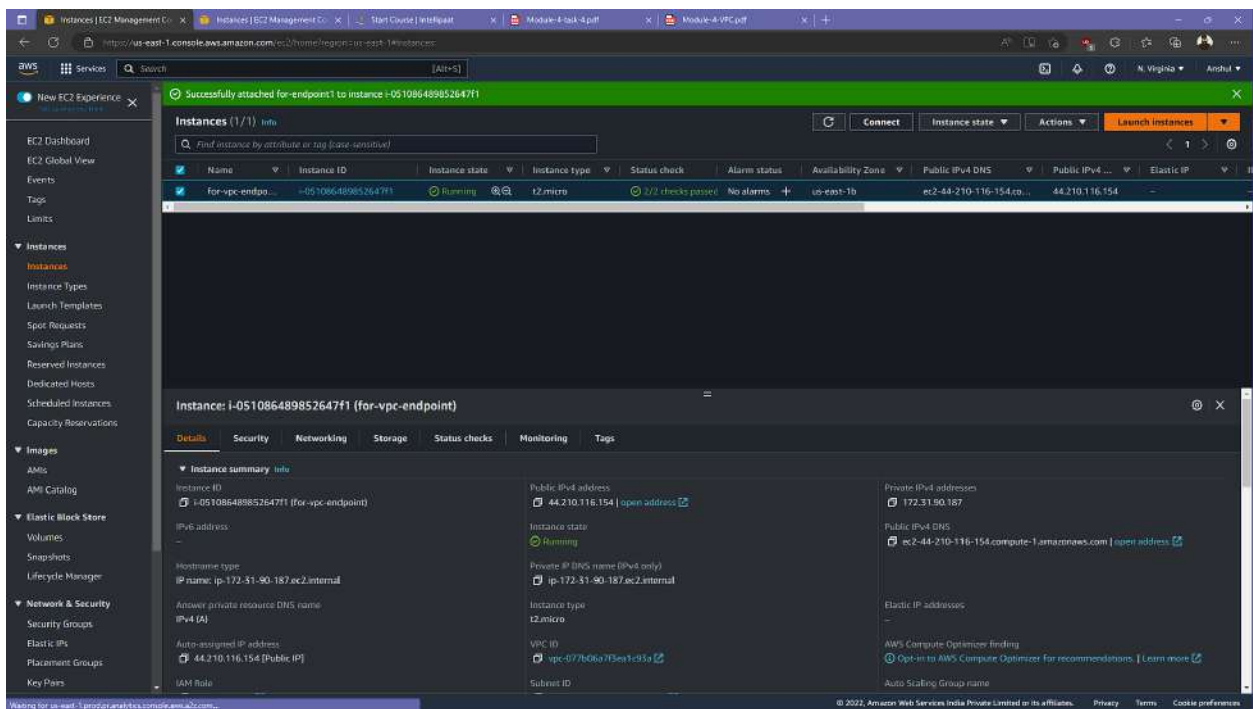
Auto-assigned IP address: 44.210.116.154 [Public IP]

IAM Role: AmazonS3FullAccess

Give the role that we just created for s3 full access.



Connect to the instance.



Use the command 'aws s3 ls'. We will get a list of objects in s3. Hence S3 can be accessed through instance and Endpoint has been successfully tested.

