

Question 1: (a) Create VPC and add internet gateway to it

The screenshot shows the AWS VPC dashboard. A prominent blue banner at the top left reads "Introducing VPC encryption control" with a subtext about managing and enforcing encryption settings across VPC resources. Below the banner, the main heading "Your VPCs" is displayed, followed by a sub-heading "VPCs | VPC encryption controls - new". A search bar and a "Create VPC" button are visible. On the left, a sidebar lists various VPC-related services like Subnets, Route tables, Internet gateways, and Security groups. The main content area shows a table for "Your VPCs (1/2) info". The table has columns for Name, VPC ID, State, Encryption controls, Block Public Access, and IP version. One row is selected, showing "vpc-01979dd9374e07da9" with "Available" status and "Off" for Block Public Access. At the bottom of the table, there's a note: "Last updated less than a minute ago".

The screenshot shows the AWS Internet gateways dashboard. A blue banner at the top left reads "Introducing VPC encryption control". Below it, the main heading "Internet gateways (2) Info" is shown, followed by a sub-heading "Actions | Create internet gateway". A search bar and a "Create internet gateway" button are present. The main content area displays a table titled "Internet gateways (2) Info". The table has columns for Name, Internet gateway ID, State, VPC ID, and Owner. Two rows are listed: "igw-022db2d30470a01d3" (Attached, vpc-00c14ca1b7e33e580, 033691785749) and "igw-0c2824bc37adc642e" (Attached, vpc-01979dd9374e07da9 | Assign, 033691785749). At the bottom of the table, there's a note: "Last updated less than a minute ago".

(b) Create a user with administrator access

Screenshot of the AWS IAM 'Create user' wizard - Step 1: Specify user details.

User name: Assign

Provide user access to the AWS Management Console - optional

Autogenerated password

Custom password: Enter a custom password for the user: @Bagri2007

Show password

Users must create a new password at next sign-in - Recommended

If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)

Cancel Next

Screenshot of the AWS IAM 'Create user' wizard - Step 2: Set permissions.

Permissions options:

- Add user to group: Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
- Copy permissions: Copy all group memberships, attached managed policies, and inline policies from an existing user.
- Attach policies directly: Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Permissions policies (1/1423):

Policy name	Type	Attached entities
AdministratorAccess	AWS managed - job function	6
AccessAnalyzerServiceRolePolicy	AWS managed	0
AdministratorAccess-Amplify	AWS managed	0
AdministratorAccess-AWSElasticBeanstalk	AWS managed	0
AIOpsAssistantIncidentReportPolicy	AWS managed	0
AIOpsAssistantPolicy	AWS managed	0
AIOpsConsoleAdminPolicy	AWS managed	0

Assign / Now

(c) Create a S3 Bucket by enable versioning and have one file

Create bucket [info](#)
Buckets are containers for data stored in S3.

General configuration

AWS Region: US East (N. Virginia) us-east-1

Bucket type: [info](#)

General purpose
General purpose buckets are for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

Directory
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name: [info](#)
`assigns3bucket-toso`

Bucket names must be 3 to 63 characters and unique within the global namespace. Bucket names must also begin and end with a letter or number. Valid characters are a-z, 0-9, periods (.), and hyphens (-). [Learn more](#)

Copy settings from existing bucket - optional
Copy the bucket settings in the following configuration are copied.

[Choose bucket](#)
Format: `s3://bucket/prefix`

Object Ownership [info](#)
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

Object Ownership

ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

Bucket owner enforced

Block Public Access settings for this bucket
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply to all objects in this bucket.

[CloudShell](#) [Feedback](#) [Console Mobile App](#)

Bucket Versioning
Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Enable

Tags - optional
You can use bucket tags to analyze, manage and specify permissions for a bucket. [Learn more](#)

You can use s3>ListTagsForResource, s3:TagResource, and s3:UntagResource APIs to manage tags on S3 general purpose buckets for access control in addition to cost allocation and resource organization. To ensure a seamless transition, please provide permissions to s3>ListTagsForResource, s3:TagResource, and s3:UntagResource actions. [Learn more](#)

No tags associated with this bucket.

[Add new tag](#)
You can add up to 50 tags.

Default encryption [info](#)
Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type: [info](#)

Server-side encryption provides two separate layers of encryption. For details on pricing, see [DSS-E-KMS pricing](#) on the Storage tab of the [Amazon S3 pricing page](#).

Server-side encryption with Amazon S3 managed keys (SSE-S3)

Server-side encryption with AWS Key Management Service keys (SSE-KMS)

Dual-layer server-side encryption with AWS Key Management Service keys (DSS-E-KMS)

Bucket Key
Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSS-E-KMS. [Learn more](#)

Disable

Enable

[Advanced settings](#)

[CloudShell](#) [Feedback](#) [Console Mobile App](#)

assigns3bucket-toso [Info](#)

[Objects](#) [Metadata](#) [Properties](#) [Permissions](#) [Metrics](#) [Management](#) [Access Points](#)

Objects (1)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

[Find objects by prefix](#) Show versions

Name	Type	Last modified	Size	Storage class
index.html	html	November 30, 2025, 12:20:16 (UTC+05:30)	59.4 KB	Standard

(d) Create a Ec2 instance

Instances (1/1) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 IP	Elastic IP	IPv6 IPs
i-07a6e9536ffabc97	i-07a6e9536ffabc97	Stopped	t3.micro	-	-	us-east-1f	-	-	-	-

i-07a6e9536ffabc97 (exam)

Details Status and alarms Monitoring Security Networking Storage Tags

Instance summary

Instance ID	i-07a6e9536ffabc97	Public IPv4 address	Private IPv4 addresses
IPv6 address	-	Instance state	Public DNS
Hostname type	IP name: ip-172-31-76-54.ec2.internal	Private IP DNS name (IPv4 only)	-
Answer private resource DNS name	IPv4 (A)	ip-172-31-76-54.ec2.internal	Elastic IP addresses
		Instance type	-
		t3.micro	-

(e) Create a Dynamodb table and add some entries in it and then delete a entry from it

DynamoDB

The item has been saved successfully.

Tables (1) Info

Name	Status	Partition key	Sort key	Indexes	Replication Regions	Deletion protection	Favorite	Read capacity mode	Write capacity mode	Total size	Table class
test (0336-0178-0740)	Active	Name (\$)	Id (N)	0	0	Off	★	On-demand	On-demand	0 bytes	Standard

Screenshot of the AWS DynamoDB Assign page for the 'Assign' table.

The 'General information' section shows:

- Partition key: Name (String)
- Sort key: Id (Number)
- Point-in-time recovery (PITR): Off
- Average item size: 0 bytes
- Resource-based policy: Not active
- Amazon Resource Name (ARN): arn:aws:dynamodb:us-east-1:033691785749:table/Assign

The 'Read/write capacity' section shows:

- Capacity mode: On-demand

The 'Scan or query items' section shows:

- Scan selected
- Query unselected
- Select attribute projection: All attributes
- Completed - Items returned: 2

The table data is:

Name (String)	Id (Number)
Tao	2
Sahoo	1

Screenshot of the AWS DynamoDB Explore items page for the 'Assign' table.

The 'Scan or query items' section shows:

- Scan selected
- Query unselected
- Select attribute projection: All attributes
- Completed - Items returned: 2

The table data is:

Name (String)	Id (Number)
Tao	2
Sahoo	1

Screenshot of the AWS DynamoDB Assign page after items have been deleted.

A green banner at the top states: "Selected items have been deleted successfully."

The 'Scan or query items' section shows:

- Scan selected
- Query unselected
- Select attribute projection: All attributes
- Completed - Items returned: 1

The table data is:

Name (String)	Id (Number)
Sahoo	1

Question 2: Secure ML Pipeline Network Architecture

The screenshots show the AWS VPC configuration interface for creating a VPC and its associated components.

Screenshot 1: Create VPC - VPC Settings

This screenshot shows the "VPC settings" section of the VPC creation wizard. It includes fields for:

- VPC settings:** Options to create "VPC only" or "VPC and more".
- Name tag auto-generation:** Set to "Auto-generate" with the prefix "Assign2".
- IPv4 CIDR block:** Set to 10.0.0.0/16 (65,536 IPs).
- IPv6 CIDR block:** Set to "No IPv6 CIDR block".
- Tenancy:** Set to "Default".
- Encryption settings - optional:** Set to "None".
- Number of Availability Zones (AZs):** Set to 1.

Preview: Shows the VPC structure with one Subnet (us-east-1a) and two Route Tables (Assign2-rtb-public and Assign2-rtb-private1-us-east-1a) attached to it.

Screenshot 2: Create VPC - Additional Configuration

This screenshot shows the "Additional configuration" section of the VPC creation wizard. It includes fields for:

- Customize AZs:** Number of public subnets: 0, number of private subnets: 2.
- Customize subnets CIDR blocks:** Public subnet CIDR block in us-east-1a: 10.0.1.0/24 (256 IPs), Private subnet CIDR block in us-east-1a: 10.0.2.0/24 (256 IPs).
- NAT gateways (5) - updated:** NAT gateway allows private instances to access the internet from any availability zone. One NAT gateway is selected.
- VPC endpoints:** None selected.
- DNS options:** Enable DNS hostnames and Enable DNS resolution are checked.
- Additional tags:** No tags are present.

Preview: Shows the VPC structure with two Subnets (us-east-1a and us-east-1b) and two Route Tables (Assign2-rtb-public and Assign2-rtb-private1-us-east-1a) attached to it.

Screenshot 3: Internet Gateways - Internet gateways

This screenshot shows the list of Internet Gateways in the AWS VPC dashboard. There are three Internet Gateways listed:

Name	Internet gateway ID	State	VPC ID	Owner
-	igw-022db2d30470901d3	Attached	vpc-00c14ca1b7e33e580	033691785749
Assign	igw-0c2824bc37ad562e	Attached	vpc-01979d09374e07da9 Assign	033691785749
Assign2-igw	igw-0bbcd7b0fffd4287658	Attached	vpc-03e0373f34ecf2bd1 Assign2-vpc	033691785749

Actions: Create internet gateway.

Select an internet gateway above: A dropdown menu is open, showing the three Internet Gateways listed above.

Screenshot of the AWS VPC NAT gateways console page. The left sidebar shows navigation for VPC dashboard, Virtual private cloud, Security, PrivateLink and Lattice, and Resource gateways. The main content area displays a table of two NAT gateways:

Name	NAT gateway ID	Connectivity...	State	State message	Availability ...	Route table ID	Primary public IP...	Primary private I...	Primary network...
Assign2	nat-175b92a269f294503	Public	Available	-	Regional	rtb-0807df044...	52.55.216.100	-	-
Assign	nat-1302c043f60227d1	Public	Available	-	Regional	rtb-0842377d6...	3.23.125.196	-	-

Actions buttons include: Actions, Create NAT gateway, and a refresh icon.

Screenshot of the AWS VPC Route tables console page. The left sidebar shows navigation for VPC dashboard, Virtual private cloud, Security, PrivateLink and Lattice, and Resource gateways. The main content area shows a success message: "Updated routes for rtb-04c048af07204e84a / Assign2-rtb-public successfully". It displays route details for route table rtb-04c048af07204e84a / Assign2-rtb-public:

Main	No	Owner ID	vpc-03e0573f54ecf2b8c Assign2-vpc

Explicit subnet associations: subnet-0x78d6c726a1b91aae / Assign2-subnet-public1-us-east-1a

Edge associations: -

Routes tab shows three routes:

Destination	Target	Status	Propagated	Route Origin
0.0.0.0/16	nat-175b92a269f294503	Active	No	Create Route
0.0.0.0/0	igw-0bad7b8fb6428768	Active	No	Create Route
10.0.0.0/16	local	Active	No	Create Route Table

Question 3: ML Team Access Control & Data Governance

Screenshot of the AWS IAM User groups console page. The left sidebar shows navigation for Identity and Access Management (IAM), Access management, Access reports, and IAM Identity Center. The main content area displays user groups:

Group name	Users	Permissions	Creation time
admin	1	Defined	2 months ago
DataScientists	0	Not defined	31 minutes ago
DataStewards	0	Not defined	18 minutes ago
MLEngineers	0	Not defined	20 minutes ago

Actions buttons include: Delete, Create group, and a refresh icon.

User groups (4) Info

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Group name	Users	Permissions	Creation time
admin	1	Defined	2 months ago
DataScientists	0	Defined	7 hours ago
DataStewards	0	Defined	6 hours ago
MIEngineers	0	Defined	6 hours ago

CloudShell Feedback Console Mobile App

User groups (3) Info

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Group name	Users	Permissions	Creation time
DataScientists	1	Defined	8 days ago
DataStewards	1	Defined	8 days ago
MIEngineers	1	Defined	8 days ago

CloudShell Feedback Console Mobile App

Role MLTraining created.

Roles (8) 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.

Role name	Trusted entities	Last activity
AWSServiceRoleForNATGateway	AWS Service: ec2-nat-gateway (Service)	9 days ago
AWSServiceRoleForResourceExplorer	AWS Service: resource-explorer-2 (Service)	27 minutes ago
AWSServiceRoleForSupport	AWS Service: support (Service)	-
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service)	-
ec2ssm	AWS Service: ec2	10 days ago
EMRServiceRole	AWS Service: ec2	-
MLTraining	AWS Service: machinelearning	-
SageMakerServiceRole	AWS Service: sagemaker	-

Roles Anywhere Info

Authenticate your non AWS workloads and securely provide access to AWS services.

Access AWS from your non AWS workloads

Operate your non AWS workloads using the same authentication and

X.509 Standard

Use your own existing PKI infrastructure or use AWS Certificate Manager

Temporary credentials

Use temporary credentials with ease and benefit from the enhanced

