practice questions

*A compilation of practice questions for the AWS Solution Architect Certification*

# iam roles & aws cli

## Question

What is a proper definition of an IAM Role?

1. IAM Users in multiple User Groups
2. An IAM entity that defines a password policy for IAM Users
3. An IAM entity that defines a set of permissions for making requests to AWS services, and will be used by an AWS service
4. Permissions assigned to IAM Users to perform actions.

A. IAM Users and User Groups are different entities; a Role is not a group of users.

B. Password policies are set for users but are not related to Roles.

**C**. An IAM Role defines a set of permissions and is assumed by trusted entities (users, AWS services, applications) to perform actions.

D. Permissions assigned directly to IAM Users are called policies, not Roles.

## Question

Which of the following is an IAM Security Tool?

1. IAM Credentials Report
2. IAM Root Account Manager
3. IAM Services Report
4. IAM Security Advisor

**A**. The IAM Credentials Report provides a detailed overview of all IAM users’ credentials (passwords, access keys, MFA status), helping identify security risks.

B. There’s no such thing as “IAM Root Account Manager” in AWS.

C. No official AWS tool named “IAM Services Report.”.

D. “IAM Security Advisor” is not an AWS service/tool.

## Question

Which answer is INCORRECT regarding IAM Users?

1. IAM Users can belong to multiple User Groups
2. IAM Users don’t have to belong to a User Group
3. IAM Policies can be attached directly to IAM Users
4. IAM Users access AWS Services using root account credentials

A. IAM Users can belong to multiple groups.

B. IAM Users don’t have to be in any group; they can have standalone permissions.

C. Policies can be attached directly to IAM Users.

**D**. IAM Users do not use root account credentials; the root account is separate and only one per AWS account.

## Question

Which of the following is an IAM best practice?

1. Create several IAM Users for one physical person
2. Don’t use the root user account
3. Share your AWS account credentials with your colleagues, so (s)he can perform a task for you
4. Do not enable MFA for easier access

A. Best practice is one IAM User per person to track actions clearly.

**B**. Avoid using the root account for daily tasks; use IAM Users with least privilege instead.

C. Sharing credentials is a major security risk and violates best practices.

D. MFA (Multi-Factor Authentication) should be enabled to enhance security, not disabled.

## Question

What are IAM Policies?

1. A set of policies that defines how AWS accounts interact with each other
2. JSON Documents that define a set of permissions for making requests to AWS services, and can be used by IAM Users, User Groups, and IAM Roles.
3. A set of policies that define a password for IAM Users.
4. A set of policies defined by AWS that show how customers interact with AWS.

A. Policies don’t define interactions between AWS accounts; that’s handled by things like resource policies or AWS Organizations.

**B**. IAM Policies are JSON documents that specify permissions and can be attached to Users, Groups, or Roles.

C. Password policies are separate from IAM Policies and define password rules, not permissions.

D. IAM Policies are not about customer interactions; they control permissions inside AWS.

## Question

Which principle should you apply regarding IAM Permissions?

1. Grant most privilege
2. Grant more permissions if your employee asks you to
3. Grant least privilege
4. Restrict root account permission

A. Granting most privilege increases security risks.

B. Permissions should be carefully reviewed, not blindly granted on request.

**C**. Least privilege means giving only the permissions necessary to perform the task, improving security.

D. Partially true but incomplete — Root account should be restricted, but this is not the core principle of IAM permissions.

## Question

What should you do to increase your root account security?

1. Remove permissions from the root account
2. Only access AWS Services through AWS Command Line Interface (CLI)
3. Don’t create IAM users, only access your AWS account using the root account.
4. Enable Multi-Factor Authentication (MFA)

A. You can’t remove permissions from the root account; it always has full access.

B. Using CLI doesn’t increase root security; security depends on how the account is protected.

C. Best practice is to create IAM users and avoid using the root account regularly.

**D**. Enabling MFA on the root account adds an essential layer of security.

## Question

IAM User Groups can contain IAM Users and other User Groups.

1. True
2. False

A. IAM User Groups can contain only IAM Users, not other User Groups.

**B**. Nested groups (groups within groups) are not supported in AWS IAM.

## Question

An IAM policy consists of one or more statements. A statement in an IAM Policy consists of the following, EXCEPT:

1. Effect
2. Principal
3. Version
4. Action
5. Resource

A. Specifies whether to allow or deny the action (required).

B. Specifies who the policy applies to; only used in resource-based policies, not in IAM user/group/role policies.

**C**. Declares the policy language version; it is at the top level of the policy, not part of individual statements.

D. Defines what actions are allowed or denied.

E. Specifies the AWS resources the actions apply to.

# ec2 instances

## Question

Which EC2 Purchasing Option can provide you the biggest discount, but it is not suitable for critical jobs or databases?

1. Convertible Reserved Instances
2. Dedicated Hosts
3. Spot Instances

A. Offer significant savings (~up to 66%) and flexibility, but not the highest discount.

B. Provide physical server access for compliance or licensing needs — very expensive, not discounted.

**C**. Offer up to 90% discount, but can be terminated at any time, making them unsuitable for critical workloads like databases or stateful services

## Question

What should you use to control traffic in and out of EC2 instances?

1. Network Access Control Lists (NACL)
2. Security Groups
3. IAM Policies

A. Control traffic at the subnet level, not directly at the instance level.

**B**. Act as virtual firewalls that control inbound and outbound traffic for EC2 instances.

C. Control permissions for AWS resources, not network traffic.

## Question

How long can you reserve an EC2 Reserved Instance?

1. 1 or 3 years
2. 2 or 4 years
3. 6 months or 1 year
4. Anytime between 1 and 3 years

**A**. EC2 Reserved Instances can be purchased for 1-year or 3-year terms.

B, C, D. AWS does not offer 2, 4, or flexible custom durations for Reserved Instances.

## Question

You would like to deploy a High-Performance Computing (HPC) application on EC2 instances. Which EC2 instance type should you choose?

1. Storage Optimized
2. Compute Optimized
3. Memory Optimized
4. General Purpose

A. Best for high IOPS or throughput-intensive workloads, not compute-heavy tasks.

**B**. Designed for CPU-intensive tasks like HPC, scientific modeling, and batch processing.

C. Suitable for memory-heavy applications (e.g., in-memory databases), not HPC.

D. Balanced performance, but not ideal for HPC which demands specialized compute capacity.

## Question

Which EC2 Purchasing Option should you use for an application you plan to run on a server continuously for 1 year?

1. Reserved Instances
2. Spot Instances
3. On-Demand Instances

**A**. Offer significant cost savings (up to 72%) for predictable, long-term workloads running continuously over 1 year or more.

B. Not suitable — Can be interrupted at any time, not reliable for continuous workloads.

C. More flexible, but much more expensive for long-term use.

## Question

You are preparing to launch an application that will be hosted on a set of EC2 instances. This application needs some software installation, and some OS packages need to be updated during the first launch. What is the best way to achieve this when you launch the EC2 instances?

1. Connect to each EC2 instance using SSH, then install the required software and update your OS packages manually
2. Write a bash script that installs the required software and updates to your OS, then contact AWS Support and provide them with the script. They will run it on your EC2 instances at launch
3. Write a bash script that installs the required software and updates to your OS, then use this script in EC2 User Data when you launch your EC2 instances

A. Manually installing software via SSH is error-prone, not scalable, and not automated.

B. AWS Support does not run custom scripts for you.

**C**. EC2 User Data lets you provide a script that runs automatically at first boot, perfect for installing software and configuring the instance.

## Question

Which EC2 Instance Type should you choose for a critical application that uses an in-memory database?

1. Compute Optimized
2. Storage Optimized
3. Memory Optimized
4. General Purpose

A. Best for CPU-intensive tasks, not memory-heavy workloads.

B. Optimized for disk throughput/IOPS, not RAM.

**C**. Designed for high-performance, memory-intensive applications like in-memory databases (e.g., Redis, Memcached).

D. Balanced resources, but not ideal for critical memory-intensive applications.

## Question

You have an e-commerce application with an OLTP database hosted on-premises. This application has popularity which results in its database has thousands of requests per second. You want to migrate the database to an EC2 instance. Which EC2 Instance Type should you choose to handle this high-frequency OLTP database?

1. Compute Optimized
2. Storage Optimized
3. Memory Optimized
4. General Purpose

A. Useful for CPU-bound workloads, but OLTP databases are typically I/O-intensive, not CPU-intensive.

**B**. Designed for high disk IOPS and throughput, ideal for high-frequency OLTP databases that perform constant read/write operations.

C. Useful for in-memory databases, but not the best fit if the main bottleneck is disk I/O.

D. Not suitable for high-performance database workloads; lacks optimized storage or compute.

## Question

Security Groups can be attached to only one EC2 instance.

1. False
2. True

**A**. Security Groups are reusable — you can attach the same Security Group to multiple EC2 instances. This makes it easier to manage network rules for groups of instances with similar requirements.

B. …

## Question

You're planning to migrate on-premises applications to AWS. Your company has strict compliance requirements that require your applications to run on dedicated servers. You also need to use your own server-bound software license to reduce costs. Which EC2 Purchasing Option is suitable for you?

1. Convertible Reserved Instance
2. Dedicated Hosts
3. Spot Instances

A. Offers cost savings and flexibility but runs on shared hardware — not compliant with dedicated server requirements.

**B**. Provide physical servers fully dedicated to your use. Also support bring-your-own-license (BYOL) scenarios for server-bound software (e.g., Windows, Oracle).

C. Run on shared infrastructure and can be terminated at any time — not suitable for compliance or licensing needs.

## Question

You would like to deploy a database technology on an EC2 instance, and the vendor license bills you based on the physical cores and underlying network socket visibility. Which EC2 Purchasing Option allows you to get visibility into them?

1. Spot Instances
2. On-Demand
3. Dedicated Hosts
4. Reserved Instances

A. Shared hardware, no visibility into physical cores or sockets.

B. Also runs on shared hardware, no physical server visibility.

**C**. Provides full visibility into physical cores and sockets, allowing compliance with license billing based on hardware.

D. Pricing discount model only, still on shared hardware without physical visibility.

## Question

You have launched an EC2 instance that will host a NodeJS application. After installing all the required software and configured your application, you noted down the EC2 instance public IPv4 so you can access it. Then, you stopped and then started your EC2 instance to complete the application configuration. After restart, you can't access the EC2 instance, and you found that the EC2 instance public IPv4 has been changed. What should you do to assign a fixed public IPv4 to your EC2 instance?

1. Allocate an Elastic IP and assign it to your EC2 instance.
2. From inside your EC2 instance OS, change network configuration from DHCP to static and assign it a public IPv4
3. Contact AWS Support and request a fixed public IPv4 to your EC2 instance
4. This can't be done, you can only assign a fixed private IPv4 to your EC2 instance

**A**. Elastic IPs are static public IPv4 addresses you allocate and attach to your EC2 instance. They remain the same across stops/starts.

B. Public IPs are assigned by AWS and cannot be statically configured inside the instance OS.

C. AWS Support doesn’t assign fixed public IPs; Elastic IPs are the user-managed solution.

D. Fixed private IPs are possible, but fixed public IPs require Elastic IPs.

## Question

You have an application performing big data analysis hosted on a fleet of EC2 instances. You want to ensure your EC2 instances have the highest networking performance while communicating with each other. Which EC2 Placement Group should you choose?

1. Spread Placement Group
2. Cluster Placement Group
3. Partition Placement Group

A. Distributes instances across distinct hardware to reduce correlated failures but not optimized for network performance.

B. Places instances physically close within a single Availability Zone to provide low-latency, high-bandwidth network performance, ideal for tightly coupled HPC or big data workloads.

C. Useful for large, distributed workloads needing fault isolation, but not focused on maximizing network throughput.

## Question

You have a critical application hosted on a fleet of EC2 instances in which you want to achieve maximum availability when there's an AZ failure. Which EC2 Placement Group should you choose?

1. Spread Placement Group
2. Cluster Placement Group
3. Partition Placement Group

A. Distributes instances across different underlying hardware and Availability Zones (AZs) to minimize correlated failures and maximize availability.

B. Packs instances closely in a single AZ, improving network but vulnerable to AZ failure.

C. Distributes instances into partitions within an AZ to isolate failures, but does not span multiple AZs.

## Question

Elastic Network Interface (ENI) can be attached to EC2 instances in another AZ.

1. True
2. False

A. …

B. An Elastic Network Interface (ENI) is bound to a specific subnet, and subnets are AZ-specific. Therefore, ENIs cannot be attached to instances in a different Availability Zone than the subnet they belong to.

## Question

The following are true regarding EC2 Hibernate, EXCEPT:

1. EC2 Instance Root Volume must be an Instance Store volume
2. Supports On-Demand and Reserved Instances
3. EC2 Instance RAM must be less than 150GB
4. EC2 Instance Root Volume type must be an EBS volume

A. Hibernate requires the root volume to be an EBSvolume, not an Instance Store.

B. Hibernate supports both On-Demand and Reserved Instances.

C. There is a limit on RAM (typically under 150GB) for instances that can hibernate.

D. The root volume must be EBS to support hibernation.

## Question

You have just terminated an EC2 instance in us-east-1a, and its attached EBS volume is now available. Your teammate tries to attach it to an EC2 instance in us-east-1b but he can't. What is a possible cause for this?

1. He's missing IAM permissions
2. EBS volumes are locked to an AWS Region
3. EBS volumes are locked to an Availability Zone

A. IAM permissions would prevent the attach action entirely, but the key issue here is cross-AZ attachment.

B. EBS volumes are regional resources but are specifically tied to an Availability Zone within that region.

C. EBS volumes cannot be attached across different Availability Zones; the volume must be in the same AZ as the EC2 instance.

## Question

You have launched an EC2 instance with two EBS volumes, Root volume type and the other EBS volume type to store the data. A month later you are planning to terminate the EC2 instance. What's the default behavior that will happen to each EBS volume?

1. Both the root volume type and the EBS volume type will be deleted
2. The Root volume type will be deleted and the EBS volume type will not be deleted
3. The root volume type will not be deleted and the EBS volume type will be deleted
4. Both the root volume type and the EBS volume type will not be deleted

B. By default, the root EBS volume is set to delete on termination. Additional attached EBS volumes (non-root/data volumes) are not deleted by default and persist after instance termination unless configured otherwise.

## Question

You can use an AMI in N.Virginia Region us-east-1 to launch an EC2 instance in any AWS Region.

1. True
2. False

A. …

B. AMIs are region-specific. To use an AMI in another region, you must **copy** the AMI to that region first.

## Question

Which of the following EBS volume types can be used as boot volumes when you create EC2 instances?

1. Gp2, gp3, st1, sc1
2. Gp2, gp3, io1, io2
3. Io1, io2, st1, sc1

A, C. St1 and sc1 (HDD types): Only for throughput-optimized or cold storage data volumes, not supported for boot volumes.

B. Gp2 and gp3 (General Purpose SSD): Commonly used for boot volumes. Io1 and io2 (Provisioned IOPS SSD): Also supported as boot volumes for high-performance needs.

## Question

What is EBS Multi-Attach?

1. Attach the same EBS volume to multiple EC2 instances in multiple AZs
2. Attach multiple EBS volumes in the same AZ to the same EC2 instance
3. Attach the same EBS volume to multiple EC2 instances in the same AZ
4. Attach multiple EBS volumes in multiple AZs to the same EC2 instance

A. Multi-Attach works only within the same Availability Zone, not across AZs.

B. This describes attaching multiple volumes, not Multi-Attach.

C. EBS Multi-Attach lets you attach a single io1/io2 volume to multiple EC2 instances within the same AZ.

D. EC2 instances cannot span multiple AZs, and Multi-Attach does not work across AZs.

## Question

You would like to encrypt an unencrypted EBS volume attached to your EC2 instance. What should you do?

1. Create an EBS snapshot of your EBS volume. Copy the snapshot and tick the option to encrypt the copied snapshot. Then, use the encrypted snapshot to create a new EBS volume
2. Select your EBS volume, choose Edit Attributes, then tick the Encrypt using KMS option
3. Create a new encrypted EBS volume, then copy data from your unencrypted EBS volume to the new EBS volume.
4. Submit a request to AWS Support to encrypt your EBS volume

A. You can’t encrypt an existing unencrypted volume directly. The supported method is to create a snapshot, copy it while enabling encryption, and then create a new encrypted volume from that snapshot.

B. You cannot just edit volume attributes to enable encryption after creation.

C. Possible but manual and error-prone; data copying is your responsibility and more complex.

D. AWS Support does not handle volume encryption requests.

## Question

You have a fleet of EC2 instances distributes across AZs that process a large data set. What do you recommend making the same data to be accessible as an NFS drive to all of your EC2 instances?

1. Use EBS
2. Use EFS
3. Use an Instance Store

A. Cannot be shared across multiple instances simultaneously; it's AZ-specific and designed for single-instance attachment.

B. A fully managed, scalable Network File System (NFS) that can be mounted concurrently by multiple EC2 instances across multiple AZs.

C. Local to a single EC2 instance; data is ephemeral and not shareable.

## Question

You would like to have a high-performance local cache for your application hosted on an EC2 instance. You don't mind losing the cache upon the termination of your EC2 instance. Which storage mechanism do you recommend as a Solutions Architect?

1. EBS
2. EFS
3. Instance Store

A. Persistent storage but slower compared to instance store for local cache.

B. Network file system, shared storage, not local or as fast as instance store.

C. Provides high-performance, ephemeral (non-persistent) local storage directly attached to the physical host. Data is lost when the instance stops or terminates, perfect for cache.

## Question

You are running a high-performance database that requires an IOPS of 310,000 for its underlying storage. What do you recommend?

1. Use an EBS gp2 drive
2. Use an EBS io2 drive
3. Use an EC2 Instance Store
4. Use an EBS io2 Block Express drive

A. General Purpose SSD, max IOPS up to 16,000 (far below 310,000).

B. High-performance SSD supports up to 64,000 IOPS (still below 310,000).

C. Very fast but ephemeral and limited in size; not designed for sustained IOPS at this scale.

D. The latest EBS volume type that supports up to 256,000 IOPS per volume, and can be combined with Multi-Attach and other features to meet ultra-high IOPS requirements.