



Navigation

Our CEO Anthony is doing a 500 gem give away! [Go here for more details!](https://twitter.com/anthonydjames/status/1177994905593024512)  
(<https://twitter.com/anthonydjames/status/1177994905593024512>)

## AWS Solutions Architect Associate (SAAC01) - Final Practice Exam

⌚ 2 hours 15  
minutes

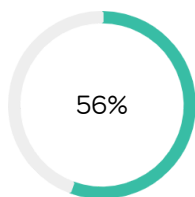
★ 60  
Questions

⌚ 2.25 Minutes per  
Question

[Intermediate \(/search?type=Practice Exam  
Challenge&difficulty=Intermediate&categories=AWS\)](/search?type=Practice Exam Challenge&difficulty=Intermediate&categories=AWS)

[Go Back](#)[Start Challenge](#)

### Question List [Show All Answers](#)

[← Go Back](#)**Great Start!**

You did not pass this challenge on this attempt.

### Expectations Report Card

Design Resilient Architectures	66.67%
Define Performant Architectures	33.33%
Specify Secure Applications and Architectures	58.33%
Design Cost-Optimized Architectures	58.33%
Define Operationally-Excellent Architectures	66.67%

### Exam Breakdown

[Design Resilient Architectures](#)

1. You are conducting an architecture review. A client has around 100 TB of important data stored as objects on S3, using the Standard storage class. They have asked you to either confirm the solution is resilient to an AZ failure or to suggest what should be done to ensure it can tolerate an AZ failure with no data loss.



What should you advise the client?

**A** Do nothing – the solution is resilient.

B Disable S3 One Zone to ensure the data is replicated between Availability Zones.

C Use CRR to ensure the data is replicated between AZs.

D Use an S3 snapshot to ensure a backup of the S3 objects are stored in multiple Availability Zones.

### Correct Answer: A

#### Why is this correct?

The question states S3 standard is used, which is resilient by design – objects are replicated across multiple Availability Zones.

2. You have been given a requirement for a new deployment in AWS. The deployment needs to operate from two AZs with one application tier and the option to launch public and private EC2 instances. From the options available, which meets the requirement with the least amount of infrastructure?



A One VPC and four subnets

B Two VPCs and two subnets

**C** One VPC and two subnets

D One VPC and one subnet

### Correct Answer: C

#### Why is this correct?

This solution can operate from two AZs (because of the two subnets). Each of the subnets can launch public or private instances if they are configured as public subnets.

3. Why does stopping and starting an instance usually fix a system status check error?



A Stopping and starting an instance reboots the operating system.

**B** Stopping and starting an instance causes the instance to be provisioned on different AWS hardware.

C None of these options are correct.

D Stopping and starting an instance causes the instance to use the latest version of the AMI it was provisioned with.

### Correct Answer: B

**Why is this correct?**

Unless you have dedicated tenancy enabled, stopping and starting an instance will generally cause it to be launched onto different AWS host hardware.

4. You have a Multi-AZ RDS instance. Its primary Availability Zone is `us-east-1a`, and the secondary is `us-east-1b`. Which of the following events will cause a failover from the primary to secondary instance?



A RDS OS patching in `us-east-1b`

B Storage failure in `us-east-1b`

**C Failure of `us-east-1a`**

D Storage failure in `us-east-1a`

E Performance alarms in `us-east-1a`

**Correct Answer: C****Why is this correct?**

Failure of the primary AZ will cause an automatic failover to the standby instance.

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html>

(<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html>)

**Correct Answer: D****Why is this correct?**

Storage failure of the primary instance will cause a failover.

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html>

(<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html>)

5. An application you are auditing runs from 10 EC2 instances. It needs to store logs on a file system that can be accessed from all the EC2 instances, and those logs need to be accessible from a central location where they can be searched from the AWS console. What two AWS products should you suggest?



**A CloudWatch Logs and EFS**

B EBS and CloudTrail

C Instance store volumes and CloudWatch Logs

D CloudWatch Logs and S3

**Correct Answer: A****Why is this correct?**

The Elastic File System (EFS) provides shared storage for EC2 instances and should be used when storage needs to be accessible from more than one EC2 instance. CloudWatch Logs can be used to ingest the application logs so they are accessible from the AWS console.

INCORRECT

6. You have been asked to design an upgrade to a legacy environment running in an AWS VPC. There will be an EC2 instance in each AZ's private subnet. The region the environment is in has four AZs. The VPC has eight subnets: four private (one in each AZ) and four public (one in each AZ). You have been asked to ensure the solution uses NAT gateways and that if any AZ fails, an instance in the other AZs can **always** access the internet.



What is the minimum number of NAT gateways required?

- A Two – each one is located in a single public subnet but not the same one. Private subnets are set to round-robin across them both.
- B One – spanning all four public subnets. All private subnets use the single NAT gateway.**
- C Four – each is located in a single but different public subnet. Each private subnet is set to use the NAT gateway in the same AZ.
- D Two – each spans two different public subnets, with private subnets set to round-robin across them both.

**Your Answer: B**

**Why is this incorrect?**

A NAT gateway occupies a single subnet. It cannot span multiple subnets. It is not HA by design.

**Correct Answer: C**

**Why is this correct?**

For true HA, a NAT gateway per AZ is required. Each private subnet would use the NAT gateway in its AZ.

7. You have been asked to provide a recommendation on the most resilient database solution available within AWS. The business requirements are that it is optimized for structured, relational data. They require multiple Availability Zones and **very** low latency between mirrors. Initially, two Availability Zones are required, but the selected solution needs to be able to cope with three or more. Which product would you recommend?



**A Aurora**

B DynamoDB

C RDS

D Athena

**Correct Answer: A**

**Why is this correct?**

Aurora supports more than two AZ replicas and uses a shared storage platform. It's the most suitable candidate.

8. You are architecting a web application that runs on EC2 instances. The application is stateless and stores its session state within DynamoDB. You want to ensure the application can scale as quickly as possible to increasing and decreasing demand in a cost-effective way. What options should you suggest?



A Vertical scaling

B Horizontal scaling

C Small instances

D Large instances

**Correct Answer: B**

**Why is this correct?**

This method of scaling involves adding or removing instances, SCALE-OUT and SCALE-IN, and is one part of elastic scaling.

**Correct Answer: C**

**Why is this correct?**

Smaller instances ensure capacity can be added and removed in smaller gradients. Additionally, smaller instances tend to have fewer capacity issues or restrictions.

INCORRECT

9. Your client is currently running a MySQL RDS instance running in `us-east-1a`. It uses a single instance, and the client wants to add the ability to automatically, quickly, and easily failover in the event of a disaster in `us-east-1a`. What should you suggest?



A Enable Multi-AZ mode.

B Enable EBS replication between AZs.

C Create an RDS read replica in `us-east-1b`.

D Enable automated backups and recovery mode.

**Your Answer: C**

**Why is this incorrect?**

RDS read replicas can be used for AZ resilience and can be used for failover, **but** it's a manual process and doesn't match the question requirements.

[https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER\\_ReadRepl.html](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html)

([https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER\\_ReadRepl.html](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html))

**Correct Answer: A**

**Why is this correct?**

Multi-AZ mode provides AZ resilience by adding a standby instance in another AZ and supports automatic failover.

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html>

(<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html>)

INCORRECT

10. You are running an application on an EC2 instance in `us-east-1a`. `us-east-1a` fails – what options do you have to recover the application running on the EC2 instance?



A The EC2 instance will recover using EC2-Recover automatically.

B If available, use a snapshot of the EBS volume to make a new volume AND then create a new EC2 instance.

C Create a new EC2 instance in `us-east-1b` and attach the EBS volume.

D Copy a snapshot of the EBS volume from `us-east-1a` to `us-east-1b`, recreate the EBS volume, and then create a new EC2 instance.

**Your Answer: D**

**Why is this incorrect?**

EBS snapshots are stored in S3 – they don't have a region, so it's not possible to copy a snapshot between AZs.

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html>

(<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html>)

**Correct Answer: B**

**Why is this correct?**

This is the only recovery option assuming AZ 1a doesn't return.

INCORRECT

11. Which of the following statements is **correct** about networking high availability in AWS?



A A virtual private gateway is HA by design.

B A NAT gateway is highly available by design.

C An IGW should be created in each AZ that a VPC uses to ensure full HA.

D A NAT gateway should be added to each AZ a VPC uses for full HA.

**Your Answer: B**

**Why is this incorrect?**

A NAT gateway is **not** HA by design. It occupies a single public subnet, which is in one AZ. If that AZ fails, the service provision fails.

**Correct Answer: A**

**Why is this correct?**

A VGW is HA by design in two AZs, so it can tolerate the failure of one.

[https://docs.aws.amazon.com/vpn/latest/s2svpn/VPC\\_VPN.html](https://docs.aws.amazon.com/vpn/latest/s2svpn/VPC_VPN.html)

([https://docs.aws.amazon.com/vpn/latest/s2svpn/VPC\\_VPN.html](https://docs.aws.amazon.com/vpn/latest/s2svpn/VPC_VPN.html))

**Correct Answer: D**

**Why is this correct?**

A NAT gateway should be created in one subnet in each AZ to be highly available.

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html>

(<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html>)

12. You have three VPCs in the same region. You need to ensure all three VPCs have network connectivity to the other VPCs and can tolerate failure within AWS. How many VPC peers are needed?



A One – connecting all the VPCs

B Two – connecting VPC1 -> VPC2 and VPC2 -> VPC3

C Three – connecting VPC1<->2, 2<->3, 1<->3

D Six – connecting VPC1<->2, 2<->3, 1<->3, but with a redundant VPC peer for each

**Correct Answer: C****Why is this correct?**

This is the correct approach – additionally, VPC peers are HA by design, so no more than three are required.

<https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html>

(<https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html>)

## Define Performant Architectures

**INCORRECT**

13. Your company has a distributed workforce: 60% are based in the United States, 30% in Europe, and 10% in Asia. All workers upload video- and image-based survey data to an S3 bucket based in `us-east-1`. Users in Europe and Asia have been experiencing performance issues. What would you suggest to improve the experience of all workers?



A Use S3 transfer acceleration and a bucket located in `eu-central-1`.

B Use S3 Global Buckets.

C Use S3 transfer acceleration and a bucket located in `us-east-1`.

D Use multiple S3 buckets – one in the United States, one in Europe, and one in Asia – and implement cross-region replication (CRR). Have remote workers upload objects to the bucket closest to them.

**Your Answer: D****Why is this incorrect?**

CRR is one way only between one source and one destination bucket, so this is not a workable solution.

**Correct Answer: C**

**Why is this correct?**

This solution positions the data close to the largest group and uses transfer acceleration to provide accelerated upload for the remaining users.

<https://docs.aws.amazon.com/AmazonS3/latest/dev/transfer-acceleration.html>

(<https://docs.aws.amazon.com/AmazonS3/latest/dev/transfer-acceleration.html>)

INCORRECT

14. You have been asked to implement a private connection between a client's premises and the AWS VPC they are using. The connection must be active within three weeks. The customer has a router that supports BGP, IPSec, and IPv4. Which option should you suggest?



A VPC peer

B AWS Direct Connect

C OpenVPN

D VPC hardware VPN

**Your Answer: B****Why is this incorrect?**

Direct Connect is a physical connection between AWS and another (non-AWS) location. The installation timeframe can be measured in months, especially if physical backhaul is required.

<https://aws.amazon.com/directconnect/getting-started/> (<https://aws.amazon.com/directconnect/getting-started/>)

**Correct Answer: D****Why is this correct?**

A VPC hardware VPN is based on IPSec and can be configured and operational within minutes. This is the preferred option given the customer's restrictions.

[https://docs.aws.amazon.com/vpn/latest/s2svpn/VPC\\_VPN.html](https://docs.aws.amazon.com/vpn/latest/s2svpn/VPC_VPN.html)

([https://docs.aws.amazon.com/vpn/latest/s2svpn/VPC\\_VPN.html](https://docs.aws.amazon.com/vpn/latest/s2svpn/VPC_VPN.html))

15. You have an application that demands extreme database performance. It needs to handle millions of read operations per second and offer low latency. What product or combination of products would you suggest?



A DynamoDB and DAX

B Aurora and SQS

C Aurora and SNS

D DynamoDB

**Correct Answer: A**



**Why is this correct?**

DynamoDB Accelerator (DAX) adds performance enhancements to DynamoDB and is the best solution available to meet this scenario's demands.

16. A large fleet of IoT devices is sending data to a Kinesis stream but experiencing an error of `ProvisionedThroughputExceededException`. How should you resolve the issue?



A Create an additional Kinesis stream and load balance the IoT devices.

B Adjust the partition key of the Kinesis data records.

**C Increase the number of shards in the stream.**

D Increase the size of the Kinesis shards.

**Correct Answer: C****Why is this correct?**

Increasing the number of shards is the recommended way to improve the performance of a Kinesis stream.

<https://docs.aws.amazon.com/streams/latest/dev/service-sizes-and-limits.html>

(<https://docs.aws.amazon.com/streams/latest/dev/service-sizes-and-limits.html>)

INCORRECT

17. You are reviewing a video transcoding platform for a client. The client is unable to use Elastic Transcoder due to feature requirements. The system currently uses a fleet of EC2 instances created by a launch template and Auto Scaling group. Instances are using the **C** family. Videos to be transcoded are entered into an SQS queue, and the size of the Auto Scaling group is controlled by messages in the queue. Any failed jobs are retried a number of times before being canceled. What options does the client have to reduce costs without negatively impacting performance over time?



**A Move from C type to X type instances.**

B Move from C type to T3 type instances.

**C Use spot instances.**

D Enable enhanced networking on all EC2 instances.

**Your Answer: A****Why is this incorrect?**

A move from C to X increases the instance cost significantly — so while the solution performance will improve, so will the cost.

**Correct Answer: C****Why is this correct?**

Spot instances will significantly reduce the ongoing cost of the solution. Even assuming some jobs will fail because of terminating spot instances, the Auto Scaling group will grow to compensate and the solution will still be lower cost.



18. Which Route 53 routing policy type should you use to ensure clients are connected to servers that offer the best potential performance?

- A Weighted routing policy
- B Simple
- C Geolocation routing policy
- D Latency routing policy**

**Correct Answer: D**

**Why is this correct?**

Latency routing attempts to resolve requests to a record that offers the lowest latency, so this will likely translate to the best performance.

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html>

(<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html>)

INCORRECT

19. A consultancy client is running a high-throughput application on-premises that stores data onto S3. The host running the software is experiencing high CPU usage and seems unable to keep up with demand while encrypting the data on-host before transit. The system requires that no data be stored in a plaintext form and has to be encrypted in transit. What potential fixes should you recommend that meet the requirements and have the least admin overhead?



- A Use S3 transfer acceleration.
- B Use client-side encryption.**
- C Use SSE-C.
- D Use SSE-S3.**

**Your Answer: B**

**Why is this incorrect?**

Client-side encryption is likely what the system is already using. If the encryption is being done on-host and CPU usage is high, that's a classic sign.

**Correct Answer: D**

**Why is this correct?**

This solution will show improvements – S3 will handle the encryption process and the encryption keys. Data will be stored in encrypted form and, assuming HTTPS is used, encrypted in transit.

20. A data scientist is trying to upload a 500 GB object to S3. The scientist is in N. Virginia and the S3 bucket is located in the `us-east-1` region. Previous smaller uploads have been running slowly, achieving ~2 Mbps on a 1 Gbps internet connection. What options can you suggest to speed up the data transfer of this larger



file?

A S3 transfer acceleration

B SSE-S3

C S3 CRR

D Multipart upload

**Correct Answer: D****Why is this correct?**

Multipart upload allows multiple transfers to occur at the same time, improving reliability for larger files but also improving speed.

<https://docs.aws.amazon.com/AmazonS3/latest/dev/mpuoverview.html>

(<https://docs.aws.amazon.com/AmazonS3/latest/dev/mpuoverview.html>)

INCORRECT

21. You are working for a large global biotech firm. Your global offices upload huge data sets regularly to a `us-east-1`-hosted S3 bucket. Which AWS service will provide all remote offices with improved transfer rates and reliability to S3?



A Direct Connect

B Enhanced networking

C DAX

D S3 transfer acceleration

**Your Answer: B****Why is this incorrect?**

Enhanced networking or SR-IOV offers EC2 instances lower and more consistent latency, but it won't improve performance for this scenario.

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enhanced-networking.html>

(<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enhanced-networking.html>)

**Correct Answer: D****Why is this correct?**

S3 transfer acceleration offers local S3 endpoints and routing back to the source bucket over the global AWS network backbone and can increase performance for all global offices.

<https://docs.aws.amazon.com/AmazonS3/latest/dev/transfer-acceleration.html>

(<https://docs.aws.amazon.com/AmazonS3/latest/dev/transfer-acceleration.html>)

INCORRECT

22. A large regional voting application is running on an EC2 instance and has been performing badly. The application vendor has tried to assist but mentioned that for usage at this level, the application needs



around 40,000 IOPS. The EC2 instance is currently running using GP volumes. When the voting has concluded, the volume needs to be detached and used on a bespoke analytics application. Which type of storage should you suggest?

**A** Change to io1.

B Leave on GP2 and increase the IOPS level.

**C** Change to sc1.

D Change to instance store.

### Your Answer: C

#### Why is this incorrect?

sc1 is designed for cold storage and cannot reach the required performance levels.

### Correct Answer: A

#### Why is this correct?

io1 can reach a max performance of 64,000 IOPS and is the best option for these extreme levels.

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html>

(<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html>)

INCORRECT

**23.** You are attempting to resolve the cause of DB performance issues on an application that uses Aurora. Which of the following are **not** options for reviewing or fixing performance concerns with Aurora? (Choose two.)



A If the performance is read related, add replicas.

**B** Log in to the aurora leader node via SSH and review OS performance metrics.

**C** Review CloudWatch metrics for CPU and MEM and adjust the instance sizes as required.

D Reboot all Aurora nodes.

**E** Storage performance is based on size – increase the size of the Aurora cluster volume.

### Your Answer: C

#### Why is this incorrect?

This is a potential solution.

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/MonitoringOverview.html>

(<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/MonitoringOverview.html>)

### Correct Answer: B

#### Why is this correct?

Aurora has no leader node – this is not a valid solution.

### Correct Answer: E

**Why is this correct?**

Aurora cluster storage is not allocated in the same way RDS is. Available space can scale to the maximum allowed 64 TiB.  
<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Overview.StorageReliability.html>  
(<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Overview.StorageReliability.html>)

INCORRECT

24. Your application needs to perform 100 **eventually consistent reads** per second from DynamoDB. Each read is 7 KB in size. What is the minimum number of RCUs required to meet this demand?



A 700

B 100

C 200

D 350

**Your Answer: C****Why is this incorrect?**

For each 7 KB read, two RCUs are used, since an RCU is 4 KB. If the demand was for **strongly consistent reads**, the application would need 200 RCU, but this question pertains to **eventually consistent reads**.

**Correct Answer: B****Why is this correct?**

Since eventually consistent reads are needed, then 100 RCUs is enough. Each read is 2 RCU (7 KB rounded to 8 KB), but **eventually consistent reads** are half the cost of strongly consistent ones.

## Specify Secure Applications and Architectures



25. If an EC2 instance uses an instance role, key rotation is automatic and handled by \_\_\_.



A A script containing a valid IAM username and password stored on the EC2 instance.

B ssh-keygen on the EC2 instance

C The EC2 service

D IAM/STS

**Correct Answer: D****Why is this correct?**

Instance role key rotation is handled by IAM/STS.

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html>  
(<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html>)

26. You have been asked to advise a junior colleague how to explicitly **deny** traffic from an EC2 instance to a specific remote internet FQDN. What advice would you give?



- A Use a security group attached to the instance, and explicitly **deny** traffic to the FQDN.
- B Use a security group attached to the VPC, and explicitly **deny** traffic to the FQDN.
- C Use a NACL on the subnet that the EC2 instance is on, and **deny** traffic from the EC2 instance to the FQDN.
- D Implement a proxy service in the VPC, adjust route tables, and use the proxy server to **deny** access to the remote hostname.**

### Correct Answer: D

#### Why is this correct?

This is the only valid option. AWS has no products capable of handling this type of denying traffic to an FQDN.

INCORRECT

27. You have been asked to suggest a solution that can monitor the flow of IP data between different EC2 instances. You need to be able to inspect the contents of the IP traffic. What solution should you suggest?



- A VPC Flow Logs**
- B CloudTrail
- C CloudWatch Logs and agent
- D IP sniffer**

### Your Answer: A

#### Why is this incorrect?

VPC flow logs can only show IP traffic metadata – they cannot show traffic contents, which is part of the requirement.

### Correct Answer: D

#### Why is this correct?

Using an IP data sniffer such as Wireshark is the only solution from the ones offered to actually see the contents of IP data.

INCORRECT

28. You have been asked to implement a personal S3 storage area for every staff member within a client. There are 1,000 staff members and each requires access to an area no other staff members can access. What option is both possible and is the least amount of admin overhead to implement and manage?



- A Create an S3 bucket for each staff member, create an IAM group, apply a policy using variables to the group, and add staff members to the group.
- B Create an S3 bucket for each staff member and add a resource policy onto each bucket, restricting access.
- C** Create a single S3 bucket. Give each staff member a prefix in the bucket. Create a single managed policy using variables, apply it to a group, and add staff members to the group.
- D Create a single S3 bucket. Give each staff member a prefix in the bucket. Create a single managed policy and apply it to every staff member's IAM user.

**Your Answer: D**

**Why is this incorrect?**

This is a potential solution but has admin overhead because of applying a managed policy to so many users.

**Correct Answer: C**

**Why is this correct?**

This is the best solution. An IAM policy using the username variable would limit each staff member to a prefix based on their username. Create the policy once, apply it once to a group, and add users to this group.

INCORRECT

29. Multiple directors in your company have opened AWS accounts. The Chief Security Officer has expressed a concern that accounts may be using unapproved AWS services and wants your advice. What action would you take?



- A Create a new account. Contact AWS Support and have them move all IAM users into the new account.
- B Create a Lambda function to delete the IAM users in each account.
- C** Create a CloudTrail trail to monitor the API calls in each account.
- D Create an organization with AWS Organizations, and have each account join your organization. Then apply service control policies to the child accounts.

**Your Answer: C**

**Why is this incorrect?**

A trail in your account won't have permissions to monitor the other accounts. To do this, you would have to set up a bucket in your account, enable access for each of the rogue accounts, and have the rogue accounts create trails that deliver logs to your bucket.

**Correct Answer: D**

**Why is this correct?**

Service control policies will override IAM policies that use unauthorized services.

INCORRECT

30. You are designing an AWS systems implementation for a medical imaging company that performs X-rays, ultrasounds, and other scans across multiple national premises. You have suggested AWS Simple Storage



Service (S3) to store the images. You have been asked to implement appropriate encryption where AWS handles the encryption and decryption process, but the customer manages the encryption keys (which are **never** stored within AWS).

What technology should you suggest?

A SSE-KMS

B SSE-Symmetrical

C SSE-C

D SSE-S3

### Your Answer: D

#### Why is this incorrect?

This is server-side encryption – the keys would reside with AWS.

<https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html>

(<https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html>)

### Correct Answer: C

#### Why is this correct?

Using SSE-C, you provide AWS with plaintext data and an encryption key. AWS performs the encryption but doesn't store or manage the keys. This is the only option that meets the customer's requirements.

<https://docs.aws.amazon.com/AmazonS3/latest/dev/ServerSideEncryptionCustomerKeys.html>

(<https://docs.aws.amazon.com/AmazonS3/latest/dev/ServerSideEncryptionCustomerKeys.html>)

31. You operate a commercial stock images website with millions of images. Watermarked preview images are available via an EC2 instance application. Full-resolution versions are stored on an EBS volume. The EBS volume is attached to the EC2 instance and delivered by the application. You have been asked to find a cheaper solution that can scale. Which option is the most suitable?



A Move the images to S3, and enable SFTP read support.

B Add a storage-optimized EBS volume to the EC2 instance.

C Move the images to S3, and use pre-signed URLs.

D Move the images to S3, and add **read** permissions for **everyone**.

### Correct Answer: C

#### Why is this correct?

S3 is more economical for large-scale object storage. Using pre-signed URLs allows the application to provide access rights to private objects to be downloaded.

<https://docs.aws.amazon.com/AmazonS3/latest/dev/PresignedUrlUploadObject.html>

(<https://docs.aws.amazon.com/AmazonS3/latest/dev/PresignedUrlUploadObject.html>)

32. You just created a VPC. For security purposes, you are using NACLs and security groups. You launched an





EC2 instance into a subnet, where you have set an inbound rule for SSH (22) in the security group and both inbound and outbound rules for port 22 on the subnet NACL. However, you are not able to access the instance via SSH. What is the most likely issue?

**A** The NACL needs an outbound rule for the high ephemeral port range (1024-65535).

B You need to add an outbound rule allowing SSH for the security group.

C You have not enabled IPv6 for the VPC.

D Your IAM user does not have SSH permissions.

### Correct Answer: A

#### Why is this correct?

SSH uses port 22 for the inbound request, but a dynamic port for the response. So there has to be an **allow** for the ephemeral port range outbound.

33. You are running a web application in your on-premises data center. The application currently has three web servers that receive traffic using round-robin DNS. As part of the move to AWS, you have been asked to design a solution that uses a load balancer to accept traffic, distributing it to web servers that are not accessible from the internet. Additionally, a database instance should only be accessible from the web servers and should not be in the same subnets. You have been asked to make the solution highly available using three AZs. How many subnets will you require?



A Three

**B** Nine

C Six

D One

### Correct Answer: B

#### Why is this correct?

Three tiers are required: load balancer, web/app servers, and database servers. Each AZ needs its own subnet for that tier –  $3 \times 3 = 9$ .

INCORRECT

34. You have been asked to perform a security review for a client. They have a fleet of EC2 instances created by an Auto Scaling group and SQS queue to process jobs stored in DynamoDB. Currently, they retrieve access keys from an S3 bucket to gain access to other AWS resources. Recently, the bucket was exploited and the keys were leaked. The business has asked for a best-practice alternative solution for this architecture. What should you suggest?



A Configure an S3 bucket policy only allowing access to the Auto Scaling group instances.

**B** Add access keys to the Auto Scaling group configuration for delivery via the instance metadata.

**C** Create a new launch template, IAM role, and instance profile.

**D** Remove the access keys from the S3 bucket.

**E** Leave the access keys stored in S3.

**Your Answer: B**

**Why is this incorrect?**

This isn't a valid technical solution.

**Correct Answer: C**

**Why is this correct?**

An IAM role and instance profile can be used to deliver temporary credentials to EC2 instances securely. By configuring this in the launch template, it can be applied to all EC2 instances created by the Auto Scaling group.

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html>

(<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html>)

**Correct Answer: D**

**Why is this correct?**

This resolves the immediate issue causing the credential leak.

35. You are about to create an AWS Lambda function and need to give it the permissions to access Amazon S3. Which of the following would be the best approach to perform this action?



**A** Create an IAM user, set the username and password in the Lambda function authentication options, and then set the method to *interactive*.

**B** Create an IAM role, assign a policy to the role, and set the Lambda function to use the role.

**C** Store the credentials inside an S3 bucket and have the Lambda function retrieve them upon execution.

**D** Create an IAM user, create access keys, and enter them into your function code.

**Correct Answer: B**

**Why is this correct?**

With this AWS-supported approach, the function will gain access to the role permissions when it's invoked.

<https://docs.aws.amazon.com/lambda/latest/dg/lambda-intro-execution-role.html>

(<https://docs.aws.amazon.com/lambda/latest/dg/lambda-intro-execution-role.html>)

36. One of your environments utilizes DynamoDB as a database. You need to ensure it can only be accessed by a select number of people using specific IP addresses. What design changes do you suggest?



**A** Create a security group, add *allow* rules for the IPs who need access, and attach the security group to DynamoDB

- B Using the AWS console or CLI, edit the table(s) requiring the restrictions, set the default security to **Deny**, and add the IPs they'll be accessing the table from.
- C** Configure an IAM group (for each level of access), and add the people who need access. Give those groups access to the DynamoDB operations they need, but add a **condition** to the policy so it has to match the specific IP address.
- D Create an isolated VPC that is not connected to the internet, provision a private DynamoDB instance in the VPC, and allow those "select people" to connect to the VPC using a VPN.

**Correct Answer: C****Why is this correct?**

This is the best solution. By default, nobody has access to the DynamoDB tables unless they're granted access. Grants can be allowed via IAM users, who have policies with conditions matching specific IP addresses.

## Design Cost-Optimized Architectures



37. You are consulting for a manufacturing company who use a set of EC2 instances to automate the production of products. The EC2 instances run software that runs through a workflow, executing various different AWS services, storing and retrieving data, and ensuring orders flow through a set of steps: A->B->C->D->E. The steps include some human interaction and can take weeks to complete. What might be a cost effective alternative?



- A** Migrate the flows to one or more state machines.
- B Continue using EC2; the long-running workflows require compute to run 24/7/365.
- C Use a Lambda function to coordinate the tasks.
- D Use a Lambda function, but ensure the timeout is set to 1 year.

**Correct Answer: A****Why is this correct?**

State machines are used by Step Functions. This product is serverless and can orchestrate long-running workflows involving other AWS services and human interaction.

<https://docs.aws.amazon.com/step-functions/latest/dg/welcome.html> (<https://docs.aws.amazon.com/step-functions/latest/dg/welcome.html>)

INCORRECT

38. You have an EC2 instance that currently runs about 100 Python-based admin scripts for a business' IT team. The scripts interact with other AWS services using an instance role. The scripts run hourly and take around two to three minutes to run. The business has asked for your suggestions on cost-optimization for this scenario. The instance has been running for one year and has two years of a reserved instance term left. What options should you suggest?



**A** Run the scripts from Elastic Beanstalk environments within the same application.

**B** Sell the remaining term of the instance reservation and stop the instance.

**C** Migrate the scripts to a Chef recipe and use AWS OpsWorks.

**D** Migrate the scripts to use individual Lambda functions.

**E** Terminate the EC2 instance to avoid costs.

### Your Answer: A

#### Why is this incorrect?

This would involve additional work and offer very little, if any, cost reductions.

### Correct Answer: B

#### Why is this correct?

This will remove most of the cost of the EC2 instance, and storage will still have costs, but it's the best solution available.

### Correct Answer: D

#### Why is this correct?

Lambda charges only for the execution time, and since the scripts have low runtimes, this is the most economical option. Since IAM roles are used for the instance, the permissions can be migrated easily to Lambda execution roles.

INCORRECT

**39.** An application utilizes a relational MySQL-based database. The application runs 24/7/365 but only gets use during brief periods at the end of each month. Your client has asked for suggestions on how database costs can be reduced. The application is currently running within RDS MySQL. The client would like solutions involving as little effort as possible. They are open to suggestions that include manual effort to save costs but have a preference for automatic solutions. What should you suggest?



**A** Migrate the database to Aurora Serverless.

**B** Purchase reservations to reduce costs.

**C** Configure a schedule to shut down and start up the RDS instance.

**D** Migrate to DynamoDB on demand.

### Your Answer: C

#### Why is this incorrect?

This could work, but it's a manual activity and, as such, not the most preferred option.

[https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER\\_StopInstance.html](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_StopInstance.html)

([https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER\\_StopInstance.html](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_StopInstance.html))

### Correct Answer: A

#### Why is this correct?

Aurora Serverless can scale down to zero instances during periods of no load. There is a brief startup time, but because of the shared storage, it happens in less than a minute.

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-serverless.how-it-works.html>  
(<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-serverless.how-it-works.html>)

40. One of your systems is suffering from performance problems. It's a critical system, and you have been asked to design an upgrade to resolve the issues. Checking CloudWatch, you can see the instance is historically running at 20% CPU and 99% memory utilization. It currently runs on the second smallest C type instance. What should your suggestion be for the most economical way to resolve the performance issues?



- A Increase the size of the instance moving from the current C class instance to the next step.
- B Edit the EC2 instance properties and select the custom memory option. Add additional memory until the performance issues are resolved.
- C Power down the instance and change the instance to a memory-optimized instance type.**
- D Rebuild the application, reinstalling all components and the data into a new memory-optimized instance type.

### Correct Answer: C

#### Why is this correct?

Memory-optimized instances sacrifice vCPU and provide more memory allocation for a similar cost. You will generally achieve better value from a memory-intensive application by moving to a memory-optimized instance type.

41. You are designing the storage needs for a movie processing application. Large videos are uploaded to your website and stored on S3. AWS Elastic Transcoder processes these master copies into multiple formats and stores them on S3. The master copies can be used directly up to a year, sometimes less. There are over 20 size and bit rate variations for each master movie file. Ninety percent of your website users only use two of these size variants. Storage costs are increasing rapidly, and you have been asked to optimize the running costs. Which option should you suggest?



- A Store the master video files on Glacier immediately and all resized versions on S3 Standard.
- B Store the master video files on Glacier immediately and all resized versions on S3 One Zone-IA.
- C Store the master video files on S3 Standard-IA, and migrate them to Glacier after 12 months. Store the popular resized versions on S3 Standard and the less popular resized versions on S3 One Zone-IA.**
- D Store the master video files on S3 One Zone-IA and migrate them to Glacier after 12 months. Store the resized versions on S3 Standard-IA.

### Correct Answer: C

#### Why is this correct?

Storing source data on Standard IA is a good choice. It means they still have the level of resilience needed but cost less to store. Then once they're older, migrating them to Glacier will provide a significant cost reduction. Resized versions can, in theory, be stored on One Zone to save costs, but the popular versions that will be regularly accessed should remain on Standard.



- 42.** A client has asked for your suggestions on a cost-optimization exercise. They have a set of financial processes that occur daily at 6 a.m. local time in every country of operation. The processes last four hours and occur daily, 24/7/365. The processes cannot be interrupted — this would require 100% of the work to be completed again.  
What billing model would offer the best price, given the information you have?

A Use Reserved instances on a two-year term.

B Use On-Demand instances.

C Use Spot instances.

**D Use Scheduled reservations.**

### Correct Answer: D

#### Why is this correct?

Scheduled reservations make the most sense in this situation. The processing occurs regularly, at the same time for the same duration. Scheduled reservations are not subject to interruption and offer a good level of cost savings.

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-scheduled-instances.html>

(<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-scheduled-instances.html>)

INCORRECT

- 43.** A customer is deploying large amounts of infrastructure using CloudFormation. The platform uses three AWS regions and 100 EC2 instances. The business' AWS costs have increased, and there is concern that using the CloudFormation service itself is the cause.  
How would using CloudFormation service be billed in this scenario? (Not including the resources it creates).



**A There is no cost for CloudFormation.**

B CloudFormation has an on-demand cost while infrastructure is being deployed — billed by the second with a 60-second minimum.

C The cost for CloudFormation is based on the number of resources the template creates.

**D There is a per-stack cost for CloudFormation.**

### Your Answer: D

#### Why is this incorrect?

Untrue. There is no cost for CloudFormation — the cost increases are based only on the infrastructure deployed.

<https://aws.amazon.com/cloudformation/faqs/> (<https://aws.amazon.com/cloudformation/faqs/>)

### Correct Answer: A

#### Why is this correct?

There is no cost for CloudFormation — the cost increases are based only on the infrastructure deployed.

<https://aws.amazon.com/cloudformation/faqs/> (<https://aws.amazon.com/cloudformation/faqs/>)

44. You manage an application that is in-use within your employer. The environment currently uses the same infrastructure for dev and production environments: three large On-Demand EC2 instances, running behind an Application Load Balancer with an RDS MySQL Multi-AZ deployment. You have been asked for suggestions to cost-optimize the solution while not negatively impacting production availability or performance.  
What should you suggest?



**A** Purchase instance reservations for PROD.

B Remove Multi-AZ from PROD.

C Use Spot instances for PROD.

**D** Remove Multi-AZ from DEV.

E Purchase instance reservations for DEV.

### Correct Answer: A

#### Why is this correct?

For any instances that need to be available consistently, instance reservation makes sense.

<https://aws.amazon.com/ec2/pricing/reserved-instances/> (<https://aws.amazon.com/ec2/pricing/reserved-instances/>)

### Correct Answer: D

#### Why is this correct?

This is a potential way to reduce costs. Multi-AZ is generally not worth the additional costs for dev environments.

INCORRECT

45. You manage a fleet of 30 EC2 instances for a client, split across 10 AWS regions. To aid in managing these machines, you have been asked to allocate the instances' static public IP IPv4 addressing. Before this work is completed, you have been asked to provide a cost estimation for the change in addressing.  
What should you tell your client?



**A** Use EC2 IPv4 public IPs – they are allocated at no cost.

B Static public IPv4 addressing is not available in AWS – use IPv6 instead.

C Use Elastic IP addresses – there is a per-IP charge.

**D** Use Elastic IP addresses – there is no charge, assuming the IP is attached to a network interface.

### Your Answer: A

#### Why is this incorrect?

EC2 IPv4 public addresses are dynamic and change if the instance is stopped and started.

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-instance-addressing.html>

(<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-instance-addressing.html>)

### Correct Answer: D

#### Why is this correct?

Elastic IPs are static, and, as long as you use them, there is no charge.

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-instance-addressing.html>

(<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-instance-addressing.html>)

46. A medical imaging company generates around 300 GB of important data on a weekly basis and stores this on S3. They need to ensure they are using resources in the most cost-effective way possible. Data is stored in S3 Standard and tends to be accessed frequently in real-time in the first 30 days after the scan takes place and then rarely if ever after that. The company needs to keep data for seven years for regulatory reasons. What option could you suggest?



A Upload the data to S3-Standard and use lifecycle rules.

B Use Standard-IA.

C Use S3 Onezone-IA.

D Upload the data directly to Glacier.

### Correct Answer: A

#### Why is this correct?

Lifecycle rules can be used to transition objects between storage classes after a certain period. This would allow initial real-time access and then transition to Glacier for low-cost ongoing storage.

<https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html>

(<https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html>)

INCORRECT

47. You are consulting for a web hosting company that runs hundreds of WordPress deployments. Each WordPress deployment generally runs on one EC2 instance and is part of an Auto Scaling group with min 1, max 1, and desired 1. Each environment is using a Classic Load Balancer to provide self-healing capability. SSL certificates are also used. The business has asked you to suggest improvements that could reduce costs. What should you suggest?



A Use Network Load Balancers instead of Classic Load Balancers.

B Migrate all SSL certificates onto a single Classic Load Balancer using SNI.

C Snapshot the EC2 instances and migrate each to an Elastic Beanstalk application.

D Migrate the Classic Load Balancers to Application Load Balancers.

### Your Answer: C

#### Why is this incorrect?

This isn't a valid technical solution. Elastic Beanstalk is a PaaS product with significant technical differences to EC2.

### Correct Answer: D



**Why is this correct?**

Application Load Balancers can use host-based rules to support multiple hostnames and SSL certs on one Application Load Balancer. The Classic Load Balancers could be merged into less Application Load Balancers, which would offer substantial cost savings.

48. You are reviewing a high volume transactional application. The application consumes a large portion of the business' AWS bill, and most of the costs seem to be associated with SQS costs. The operations team has advised you that they have noticed 65% of the application's calls to SQS are during periods when the work queue is empty. How can you reduce the application costs with the information provided?



A Modify the queue from standard to FIFO.

**B Use long polling.**

C Reduce the queue shards.

D Use short polling.

**Correct Answer: B****Why is this correct?**

This could potentially reduce costs by reducing the number of SQS API calls and ensuring as many as possible return results.

<https://aws.amazon.com/sqs/faqs/> (<https://aws.amazon.com/sqs/faqs/>)

## Define Operationally-Excellent Architectures

**INCORRECT**

49. You have an order processing system where you are printing high-quality pictures onto glass panels. The ordering system currently uses a custom application running on an EC2 instance to design the order, an SQS queue to hold the orders, and a fleet of EC2 instances inside an Auto Scaling group to control the printing machines. There is a growing issue with duplicate orders. How could you resolve this using AWS services?



A Ensure you are using a standard SQS queue, ensuring once-only delivery.

**B Change the architecture to use a state machine.**

**C Change the standard SQS queue to a FIFO queue, ensuring once-only delivery.**

D Adjust the visibility timeout value on the SQS queue.

**Your Answer: C****Why is this incorrect?**

FIFO does add exactly-once processing, but this doesn't fix the situation where a message is read from the queue, the processing crashes or times out, and another EC2 instance starts the job again.

<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/FIFO-queues.html#FIFO-queues-exactly-once-processing> (<https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/FIFO-queues.html#FIFO-queues-exactly-once-processing>)

### Correct Answer: B

#### Why is this correct?

State machines are part of Step Functions, which would allow you to create an order flow with fixed steps and controls. It functions in much the same way as the legacy SWF (Simple Workflow Service), but Step Functions is serverless.

<https://docs.aws.amazon.com/step-functions/latest/dg/welcome.html> (<https://docs.aws.amazon.com/step-functions/latest/dg/welcome.html>)

50. You have created a CloudFront distribution to improve the performance of your global stock images website. Private images are distributed using CloudFront signed URLs, and the distribution is configured to be private. You recently found a group of users accessing images directly from the S3 origin without paying. How can you resolve this?



A Remove the DNS name on the S3 bucket.

B Add an OAI to CloudFront and the bucket policy.

C Apply a bucket policy to the bucket, blocking all access.

D Apply an object-level restriction to each object in the origin using the ARN of the CloudFront distribution.

### Correct Answer: B

#### Why is this correct?

This is the recommended approach. An OAI is a virtual identity that can be associated with a CloudFront distribution and then used in a bucket policy.

<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html> (<https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html>)

51. You are designing a system that takes data from hundreds of thousands of solar panel installations, ingests the data into AWS, and is used to display data on four different visualization systems. Each system needs to read the data ingested and present the data in a different way. What product should you use to handle the data volume above?



A SQS

B API Gateway

C Kinesis Data Streams



D S3

### Correct Answer: C

**Why is this correct?**

This is a perfect use case for Kinesis, as it's designed for high-volume data streaming and can support multiple consumers accessing data from its rolling window.

<https://aws.amazon.com/kinesis/data-streams/> (<https://aws.amazon.com/kinesis/data-streams/>)

52. You have been asked to create a scalable deployment for a new business application. The application uses Java and requires lots of supporting libraries and frameworks. The total time for the installation is 25 minutes. If the business needs the application to scale in an elastic way, rapidly reacting to changes in system load, what method should you suggest for installing, deploying, and scaling the application?  

A Use a launch template to add the application installation commands.

**B** Install the application on an EC2 instance and create an AMI.



C Install the application directly using instance metadata.

D Add the application installation commands to an Auto Scaling group.

**Correct Answer: B****Why is this correct?**

This is an example of an **AMI Pre-bake** architecture, which would work. The 25-minute installation would be done once, with the results stored in an AMI — and this could be used with a launch configuration/launch template and an Auto Scaling group to scale the application.

<https://aws.amazon.com/answers/configuration-management/aws-ami-design/>  
(<https://aws.amazon.com/answers/configuration-management/aws-ami-design/>)

53. You run a single instance application on an EC2 instance in AWS. Your architecture teams are looking to make changes and convert the application to operate on multiple servers. The app runs on Linux and currently accesses millions of flat file data files in the `/data/...` folder structure. This database is stored on an EBS volume attached to the EC2 instance. How can this be moved to work on multiple servers, with as little application changes as possible? What product would you suggest?  

A Use EBS to mount the existing volume on all the new instances.

B S3

**C** EFS

D EMR and HDFS

**Correct Answer: C****Why is this correct?**

EFS is a network file system and could be utilized to provide access to the database files for all instances. It can also be mounted locally on Linux systems.

<https://docs.aws.amazon.com/efs/latest/ug/mounting-fs.html> (<https://docs.aws.amazon.com/efs/latest/ug/mounting-fs.html>)

INCORRECT

54. You are working on a migration project from a large enterprise's on-premises location into AWS. One of the client's systems stores files on a local file system that is shared to the business's local Microsoft Windows 10 workstations. You need to migrate the data into AWS without outage and ensure the files can be accessed both using SMB and over HTTPS. What option should you suggest?



A Storage Gateway volume gateway

B Store the files directly on S3 using the S3 connector.

C Storage Gateway file gateway

D Migrate the application and server onto an EC2 instance and share the files using SMB.

**Your Answer: A**

**Why is this incorrect?**

Volume gateway cannot present the files over SMB, nor would the files be available directly on S3.

**Correct Answer: C**

**Why is this correct?**

Using a file gateway would mean files could be migrated onto the gateway, presented via SMB, and accessible directly from S3 as objects.

<https://docs.aws.amazon.com/storagegateway/latest/userguide/WhatIsStorageGateway.html>

(<https://docs.aws.amazon.com/storagegateway/latest/userguide/WhatIsStorageGateway.html>)

55. You are reviewing and improving an application that uses a relational database and is currently hosted on a single-AZ RDS MySQL database. The application database pattern is 20% writes and 80% reads and is showing signs of read slowdown. You need to make changes to allow the application to scale more effectively. What change could you implement to improve read performance with as little change as possible?



A Modify the RDS instance and enable Multi-AZ.

B Modify the application to use DynamoDB in relational mode and enable Auto Scaling.

C Migrate the database to Aurora and add replicas.

D Add read replicas to the RDS cluster.

**Correct Answer: C**

**Why is this correct?**

Aurora is MySQL compatible, and the migration path from RDS MySQL is well documented and low risk. Aurora replicas can be used to scale reads across the cluster.

<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Replication.html>

(<https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Aurora.Replication.html>)

56. Your business operates in a very security-sensitive industry. You are looking at how to secure a small VPC. Your environment consists of a single S3 bucket and an EC2 instance running in an internet-connected VPC. Only the EC2 instance needs access to S3. What is the best way to lock down the environment, allowing the EC2 instance access to S3 but keeping the environment as secure as possible?



- A Create an S3 VPC endpoint. Apply a policy restricting access to the S3 bucket from the VPC endpoint.
- B Create a new security group, denying all IPs except the EC2 instance, and associate it with the S3 bucket.
- C Create an S3 VPC endpoint. Apply a policy restricting access to the S3 bucket from the VPC endpoint, and remove the internet gateway. Set up a VPN connection to securely log in to the EC2 instance via SSH when needed.**
- D Provision a privately addressable S3 bucket in your VPC. Migrate the contents of the public bucket and update the application. Remove the internet gateway to isolate the VPC.

### Correct Answer: C

#### Why is this correct?

A VPC endpoint doesn't require an internet gateway. It allows access to S3, which is a public service from a VPC. This is the most secure option that meets the criteria.

57. You've been asked to host a Docker container within your AWS environment using the least amount of effort or overhead. What is the most appropriate product to use for this task?



- A Lambda
- B EC2
- C ECS**
- D OpsWorks

### Correct Answer: C

#### Why is this correct?

ECS (Elastic Container Service) should be the preference when it comes to hosting Docker inside AWS. The Fargate deployment method further minimizes the overhead of running Docker in AWS.

<https://docs.aws.amazon.com/AmazonECS/latest/developerguide/docker-basics.html>

(<https://docs.aws.amazon.com/AmazonECS/latest/developerguide/docker-basics.html>)

[https://docs.aws.amazon.com/AmazonECS/latest/developerguide/AWS\\_Fargate.html](https://docs.aws.amazon.com/AmazonECS/latest/developerguide/AWS_Fargate.html)

([https://docs.aws.amazon.com/AmazonECS/latest/developerguide/AWS\\_Fargate.html](https://docs.aws.amazon.com/AmazonECS/latest/developerguide/AWS_Fargate.html))

INCORRECT

58. You have been asked to design modifications to an existing application deployed into EC2 using an Auto Scaling group. Your client needs to make sure data can be obtained from EC2 instances for compliance reasons. They need CPU usage, network data transfer levels, and application process memory usage. What should you tell them?



A The data is accessible by default using CloudWatch.

B The data is accessible using CloudWatch if the agent is installed.

C The data is accessible using CloudWatch, but detailed monitoring needs to be enabled.

D Data can be accessed using CloudWatch, but for the process memory usage, CloudWatch Logs should be used.

### Your Answer: C

#### Why is this incorrect?

Detailed monitoring doesn't add metrics – it just increases the level of detail for existing metrics. To capture the process memory usage, the agent is required.

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/metrics-collected-by-CloudWatch-agent.html>  
(<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/metrics-collected-by-CloudWatch-agent.html>)

### Correct Answer: B

#### Why is this correct?

The CloudWatch agent allows for many more internal metrics to be gathered and is required in this case for the process memory usage.

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/metrics-collected-by-CloudWatch-agent.html>  
(<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/metrics-collected-by-CloudWatch-agent.html>)

59. A client has asked your advice. They have a huge amount of CSV data currently stored on an on-premises file store. They need to keep the data stored for five years and have an occasional need to perform queries on the data using SQL. The need isn't commercial – it's for freedom of information reasons, so the client would like to do it with as little investment as possible. The query volume is unknown and ad hoc. What should you suggest?



A Create an EMR cluster, load the CSV files onto HDFS, and query when required.

B Load the CSV files onto S3, define tables, and use Athena to query when required.

C Create an Aurora cluster, load the CSV files into the cluster, and have staff query the cluster when required.

D Create a large EBS volume, create an EC2 instance and attach the volume, load the CSV files into the volume, and allow staff to query the files when required.

### Correct Answer: B

#### Why is this correct?

This is the best option. Athena is ideally suited to ad-hoc queries, and only data processed carries a cost, so it would be perfect for occasional use.

INCORRECT

60. You have created a S3 bucket in the `us-east-1` region called `youramazingcatpictures123` and a bucket in the `ap-southeast-2` region called `backupmycats123`. You are attempting to configure cross-region replication (CRR) between the buckets, but the configuration is generating an error. Which of the options below could be a potential reason?



A The source bucket has no objects inside it to replicate.

**B** Cross-region replication isn't supported between two S3 buckets – only S3 -> Glacier.

C The source bucket uses SSE-S3.

**D** Versioning is not enabled.

### Your Answer: B

#### Why is this incorrect?

Cross-region replication is **only** supported between two S3 buckets.

<https://docs.aws.amazon.com/AmazonS3/latest/dev/crr.html>

(<https://docs.aws.amazon.com/AmazonS3/latest/dev/crr.html>)

### Correct Answer: D

#### Why is this correct?

To support replication, both the source and destination buckets must have versioning enabled.

<https://docs.aws.amazon.com/AmazonS3/latest/dev/crr.html>

(<https://docs.aws.amazon.com/AmazonS3/latest/dev/crr.html>)