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)

Go Back Start Challenge

Question List Show All Answers

< 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 >

90%

← Go Back

Congratulations!

You passed this challenge on this attempt.

Expectations Report Card

Design Resilient Architectures	100%
Define Performant Architectures	75%
Specify Secure Applications and Architectures	91.67%
Design Cost-Optimized Architectures	91.67%
Define Operationally-Excellent Architectures	83.33%

Exam Breakdown

Design Resilient Architectures

1. 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.

---

2. You need to design a VPC that is resilient to AZ failure from an internet access perspective. The VPC is in a four-AZ region. How many internet gateways are required to ensure multiple AZ failures won't disrupt internet connectivity?

A Zero — internet access is provided by a NAT gateway

B Four

C One

D Two

Correct Answer: C

Why is this correct?

An IGW is resilient by design, and only one needs to be attached to a VPC in order to provide ***all*** subnets in ***all*** AZs with resilient internet connectivity. You cannot assign more than one IGW to a VPC.

---

3. 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.
https://aws.amazon.com/efs/when-to-choose-efs/ (https://aws.amazon.com/efs/when-to-choose-efs/)

---

4. 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.

Correct Answer: B

Why is this correct?

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

---

5. You are reviewing an existing VPN between a data center and an AWS VPC. Your client has asked you to suggest any HA improvements; the system must be able to tolerate the failure of an AWS AZ and a customer internet connection or router. Currently, the system includes:

- One VPC
- One business location with two internet connections — each with a router
- One VPN connection using one virtual private gateway and two IPSec tunnels to one of the customer routers

Which option below is the most appropriate and correct?

A Add an additional virtual private gateway to the VPC.

B Move one of the IPSec tunnels to the other customer router.

C Add another VPN connection to the second CGW.

D Take no action — the system meets the HA requirements with no changes.

Correct Answer: C

Why is this correct?

This will add an additional two IPSec tunnels between the VGW and the second CGW. This will tolerate the failure of one customer connection and one AWS AZ because the VGW is already HA across multiple AZs.

---

6. You have been asked to ensure the Lambda component of an AWS deployment is resilient across 3+ AZs. What modifications are required (if any) to meet this requirement?

A None.

B Ensure the Lambda scaling settings are updated with subnets in three or more AZs.

C Create a Lambda subnet group, ensure it has the subnets in 3+ AZs, and associate it with the Lambda function.

D Ensure the Lambda environment has an associated internet gateway.

Correct Answer: A

Why is this correct?

Lambda is HA and scalable by design, so no changes are required.

---

7. 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.

---

8. A medical system that is used within 40 major hospitals requires 100% resilience. The service requires six EC2 instances to be running at all times to function correctly and should be able to tolerate the failure of one AZ without ***any*** performance impact.
Which of the following options are valid, given this scenario?

A **AZ-A: Six instances**

- **AZ-B: Zero instances**

- **AZ-C: Two instances**
- **AZ-D: Four instances**

B AZ-A: Two instances

- AZ-B: Two instances
- AZ-C: Two instances

C AZ-A: Three instances

- **AZ-B: Three instances**
- **AZ-C: Three instances**
- **AZ-D: Three instances**

D AZ-A: Four instances

- AZ-B: Two instances
- AZ-C: Two instances

Correct Answer: A

Why is this correct?

This solution meets the criteria — any single AZ failure would leave six operational instances.

Correct Answer: C

Why is this correct?

This solution meets the criteria, but it can go further and support two AZ failures while still having the minimum of six instances.

---

9. 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.

---

10. 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.

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.

---

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.

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)

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. 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.

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)

Define Performant Architectures

13. 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

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)

14. 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.

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)

---

15. 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.

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)

---

16. You have created a GP2 EBS volume in AWS. It is 1 TiB in size. What level of sustained IOPS should it deliver?

A 300

B 10,000

C 3,000

D 1,000

Correct Answer: C

Why is this correct?

GP2 delivers 3 IOPS per GiB — a volume of 1 TiB (1,000 GiB) would deliver 3,000 IOPS.
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html
(https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html)

---

17. 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

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.

---

18. You are running an application on an EC2 instance that is extremely sensitive to variations in network performance, specifically the variation in ping times and latency. The application also devours CPU cycles when this network jitter happens, so you need to implement a solution that removes any risk of network performance degradation. What option works in this scenario?

A Ensure the VPC is running in dedicated tenancy mode.

B Ensure the instance has enhanced networking.

C Ensure you are using an X1 instance.

D Ensure the instance is EBS optimized.

Correct Answer: B

Why is this correct?

Enhanced networking (https://aws.amazon.com/premiumsupport/knowledge-center/enable-configure-enhanced-networking/ (https://aws.amazon.com/premiumsupport/knowledge-center/enable-configure-enhanced-networking/)) allows high-performance networking by bypassing the need for CPU involvement in virtualizing a network interface. This increases packets per second and decreases the variability in network performance.

---

19. 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

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)

---

20. You have been asked to provide a recommendation for a database platform that meets the following requirements:

- Able to work with relational data
- Resilience across 3+ Availability Zones in supported regions
- Read scaling using group addressable replicas

What product should you suggest?

A RDS - PostgreSQL

B RDS - MySQL

C Aurora

D DynamoDB

Correct Answer: C

Why is this correct?

Aurora is the best solution. Replicas can be added in 3+ AZs and can be addressed as a group via a reader endpoint DNS address.

INCORRECT

21. You have been asked to architect the networking for a high-performance financial modeling application. It runs on four EC2 instances, and you need the lowest network latency and highest throughput possible.
What AWS products, services, or features should you suggest?

A Burstable instances

B VPC Flow

C Spread placement group

D Cluster placement group

Your Answer: A

Why is this incorrect?

Burstable instances (T2 or T3) are designed for economic applications that don't need consistent CPU.

Correct Answer: D

Why is this correct?

Cluster placement groups influence the physical placement of instances on hardware, and this allows the highest performance possible.
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html)

INCORRECT

22. 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: B

Why is this incorrect?

T3 instances are burst instances, which are suitable for situations where workloads don't use 100% CPU. This will reduce costs but also negatively impact performance.

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.

---

23. 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

24. 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: C

Why is this incorrect?

SSE-C uses S3 for CPU-intensive encryption operations. No data is stored in plaintext and, assuming HTTPS is used, data is encrypted in transit. The problem is SSE-C requires the customer to manage keys, which is risky and involves high admin overhead.

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.

Specify Secure Applications and Architectures

25. You have an EC2 instance located in a private subnet. The instance is using a private IPv4 address in the 10.0.0.0/24 range and has no public IP or Elastic IP attached. NACLs and security groups are configured to allow the needed traffic.
How can you provide this instance with access to the internet for updates?

A Attach an internet gateway to the VPC, provision a NAT gateway, and then update routes.

B Attach an internet gateway to the VPC and update routes.

C Use PrivateLink to access AWS-provided update servers.

D Provision a NAT gateway into the VPC.

Correct Answer: A

Why is this correct?

By adding an internet gateway, the NAT gateway can itself access the internet. Then it can provide this to private instances after routes have been added or updated.

---

26. 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.

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.

---

27. 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 x 3 = 9.

---

28. 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

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.

---

29. 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)

---

30. 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)

---

31. 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.

---

32. 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

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)

INCORRECT

33. A team of developers within your business has developed a mobile application, and it needs to access a DynamoDB table. The mobile application will be used by ~1,000,000 users.
Which security access method would you suggest the developers use in order to minimize costs and admin overhead while maximizing security?

A Configure the DynamoDB and Twitter firehose integrations to allow connectivity between the mobile app (using Twitter IDs) and DynamoDB.

B Create a single IAM user, a service user for the mobile app. Hard-code the username and password into the application, and allow all instances of it to connect to DynamoDB using those credentials.

C Configure web identity federation in the mobile app. Use AWS Cognito, and set up an IAM role with permissions to connect to DynamoDB.

D Create an IAM user for the application. Allow the application to connect to AWS and create an IAM user for every new user of the application. Generate access keys for that user, and use those keys to connect to DynamoDB.

Your Answer: B

Why is this incorrect?

Using a single account goes against good security practices. An IAM username and password cannot be used to log in to AWS public services via the APIs.

Correct Answer: C

Why is this correct?

This is the most secure method, and it avoids the need to manage any additional IAM users. It also avoids any account limits.

---

34. You are running a WordPress instance in a non-default VPC's public subnet. As part of A/B testing, you

have deployed another instance in the same subnet, using the same security group, same AMI, and an instance of the same family. After provisioning the instance, you cannot access it. Which of the following issues ***could*** be the problem?

A Create an Elastic IP, and assign it to the new instance.

B Make sure the public IP is configured on the instance's OS.

C Add a route for the new instance.

D Configure the NAT gateway to route traffic to the new instance.

Correct Answer: A

Why is this correct?

The instance could have been launched without a public IP. The quickest way to test and fix this is to allocate an Elastic IP.

---

35. 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.

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.

---

36. 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.

Design Cost-Optimized Architectures

37. 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.

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/)

38. 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

39. You operate two EC2 instances that are currently running inside an Auto Scaling group. The instances serve high-resolution mapping images for a group of resource companies. The Auto Scaling group can scale OUT or IN to meet the demand on these instances. For 70% of the day, the number of instances is two, and for two to three hours per day, the load is zero, but the business cannot tolerate ***any*** delay or outages to the data.
What option could you suggest to improve the cost-effectiveness of this solution?

A Change the Auto Scaling group options to 1:1:1 and don't allow any changes.

B Use io1 storage.

C Move the mapping data to instance store volumes.

D Use S3.

Your Answer: A

Why is this incorrect?

This will lock the Auto Scaling group on one EC2 instance, which isn't enough for a nominal load.

Correct Answer: D

Why is this correct?

S3 can be used as an effective host for static content. By enabling the static web hosting function or using pre-signed URLs, the data can be made available for access with no consistent compute costs.
https://docs.aws.amazon.com/AmazonS3/latest/dev/ShareObjectPreSignedURL.html
(https://docs.aws.amazon.com/AmazonS3/latest/dev/ShareObjectPreSignedURL.html)

---

40. 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/)

---

41. 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)

---

42. You are reviewing a set of API endpoints for your development team that currently runs on a fleet of 50 EC2 instances. You have been asked to reduce costs. Are there any pairs of AWS products and/or features you could suggest to reduce the cost of the current solution?

A S3 and static web hosting

B API Gateway and Kinesis

C Lambda and API Gateway

D ALB and Elastic Beanstalk

Correct Answer: C

Why is this correct?

Lambda and API Gateway can be used together to host APIs. Rather than being billed 24/7/365 for all of the EC2 instances, Lambda only has a cost when functions are invoked.

---

43. 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.

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)

---

44. Your business needs a small database for storing simple names, addresses, and ID picture information for 1,000 employees. The usage will be low, queries will occur every day, and the business wants the most suitable low-cost solution available within AWS.
Which database would you suggest?

A Aurora

B DynamoDB

C Redshift

D ElastiCache

Correct Answer: B

Why is this correct?

DynamoDB is a perfect solution for this. The data requirements are simple, and DynamoDB has little to no base costs when not being used.

---

45. 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.

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.

---

46. Which of the following suggestions could help reduce DynamoDB running costs?

A Utilize indexes.

B Filter the attributes read from a table.

C Use `Scan` rather than `Query` operations.

D Increase RCU.

Correct Answer: A

Why is this correct?

Indexes allow you to define alternative partition and/or sort keys, which can allow you to use `Query` rather than `Scan` operations. Additionally, you can choose which attributes are projected into the indexes, meaning you will read less data for each ITEM retrieved.
https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/LSI.html (https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/LSI.html)
https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/GSI.html (https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/GSI.html)

---

47. 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.

---

48. 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)

Define Operationally-Excellent Architectures

49. 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)

---

50. Your CIO is reviewing the expected technical effort required to manage an AWS environment. Which of the following AWS services can be accessed directly or require system-level access to configure some/all of their settings?

A DynamoDB

B Amazon EMR

C Amazon RDS

D Amazon EC2

Correct Answer: B

Why is this correct?

EMR allows you to log in to the master node via SSH.

Correct Answer: D

Why is this correct?

You can SSH/RDP to the operating system of your EC2 instances — for certain installation/configuration and admin tasks, it's required.

INCORRECT

51. You are consulting for a client who is migrating their entire infrastructure into AWS. The client's engineers are used to managing infrastructure as code and have been using both Puppet and Chef to manage infrastructure on-premises. Which AWS product should you suggest they explore to manage infrastructure within AWS?

A Ansible

B Elastic Beanstalk

C OpsWorks

D CloudFormation

Your Answer: A

Why is this incorrect?

Ansible isn't an AWS product, and the question makes no mention of preexisting experience, so it's less than ideal.

Correct Answer: C

Why is this correct?

OpsWorks is an AWS infrastructure management platform that supports Chef and Puppet.
https://aws.amazon.com/opsworks/ (https://aws.amazon.com/opsworks/)

---

52. 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)

---

53. 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.

---

54. You have a collection of several million JSON documents. You want to store their data within AWS. The data needs to be searchable based on a unique ID in the JSON, and the searches need to be available from a public endpoint. The data is important, so it needs to be able to survive an AZ failure in AWS, and the data latency needs to be in the low milliseconds. What service should you suggest?

A S3

B EC2 and EBS

C DynamoDB

D EFS

Correct Answer: C

Why is this correct?

DynamoDB is the ideal solution. It offers low latency, can store data for querying, and replicates data across AZs in the region the table is created in.

---

55. 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.

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)

INCORRECT

56. Which of the following statements are true about instance store volumes?

A Data stored on instance store volumes will ***always*** be lost when an instance stops and starts.

B Data stored on instance store volumes will ***always*** be lost when an instance restarts.

C Data stored on instance store volumes ***can sometimes*** be lost when an instance stops and starts.

D Data stored on instance store volumes ***can*** be lost when an instance restarts.

Your Answer: B

Why is this incorrect?

An instant restart by default doesn't move the instance between EC2 hosts and so normally the data on instance store volumes will persist. It is ***not*** always lost.

Correct Answer: A

Why is this correct?

If an instance is stopped and started, it will move hosts, so it's correct to say the data on volumes will ***always*** be lost when stopping and starting.

Correct Answer: D

Why is this correct?

Data can be lost if the cause of the restart was an underlying hardware failure.

---

57. 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)

---

58. 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.

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)

---

59. 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/)

---

60. 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.
