Domain: Design High-Performing Architectures
You are working as an AWS Architect for a start-up company. They have a two-tier production website. Database servers are spread across multiple Availability Zones and are stateful.

You have configured Auto Scaling Group for these database servers with a minimum of 2 instances & a maximum of 6 instances. During post-peak hours, you observe some data loss. Which feature needs to be configured additionally to avoid future data loss (and copy data before instance termination)?

- A. Modify the cooldown period to complete custom actions before the Instance terminates.

- B. Add lifecycle hooks to Auto Scaling group. right
- C. Customize Termination policy to complete data copy before termination.
- D. Suspend Terminate process that will avoid data loss.

Explanation:

Correct Answer – B
Explanation: Adding Lifecycle Hooks to the Auto Scaling group puts the instance into a wait state before termination. During this wait state, you can perform custom activities to retrieve critical operational data from a stateful instance. The Default Wait period is 1 hour.

- Option A is incorrect as the cooldown period will not help copy data from the instance before termination.
- Option C is incorrect as the Termination policy is used to specify which instances to terminate first during scale in. Configuring termination policy for the Auto Scaling group will not copy data before instance termination.
- Option D is incorrect as the Suspending Terminate policy will not prevent data loss but disrupt other processes & prevent scale-in.

For more information on lifecycle-hooks, refer to the following URLs:

- https://docs.aws.amazon.com/autoscaling/ec2/userguide/lifecycle-hooks.html
- https://aws.amazon.com/ec2/autoscaling/faqs/

Question 2Correct

Domain: Design Resilient Architectures
You have an application running in us-west-2 that requires 6 EC2 Instances running at all times. With 3 Availability Zones in the region viz. us-west-2a, us-west-2b, and us-west-2c, which of the following deployments provides fault tolerance if ONE Availability Zone in us-west-2 becomes unavailable? (SELECT TWO.)

- A. 2 EC2 Instances in us-west-2a, 2 EC2 Instances in us-west-2b, and 2 EC2 Instances in us-west-2c

- B. 3 EC2 Instances in us-west-2a, 3 EC2 Instances in us-west-2b, and no EC2 Instances in us-west-2c

- C. 4 EC2 Instances in us-west-2a, 2 EC2 Instances in us-west-2b, and 2 EC2 Instances in us-west-2c

- D. 6 EC2 Instances in us-west-2a, 6 EC2 Instances in us-west-2b, and no EC2 Instances in us-west-2cright

- E. 3 EC2 Instances in us-west-2a, 3 EC2 Instances in us-west-2b, and 3 EC2 Instances in us-west-2cright

Explanation:

Answer – D and E
Option D- US West 2a-6 , US West 2b - 6, US West 2c-0

- If US West 2a goes down, we will still have 6 instances running in US West 2b.
- If US West 2b goes down, we will still have 6 instances running in US West 2a.
- If US West 2c goes down, we will still have 6 instances running in US West 2a, 6 instances running in US West 2b.

Option E- US West 2a-3 , US West 2b - 3, US West 2c-3

- If US West 2a goes down, we will still have 3 instances running in US West 2b and 3 instances running in US West 2c.
- If US West 2b goes down, we will still have 3 instances running in US West 2a and 3 instances running in US West 2c.
- If US West 2c goes down, we will still have 3 instances running in US West 2a and 3 instances running in US West 2b.

Option A is incorrect because, even if one AZ becomes unavailable, we will only have 4 instances available. This does not meet the specified requirements.

Option B is incorrect because, when either us-west-2a or us-west-2b is unavailable, you would only have 3 instances available. This does not meet the specified requirements.

Option C is incorrect because, if us-west-2a becomes unavailable, you would only have 4 instances available. This also does not meet the specified requirements.

For more information on AWS Regions and Availability Zones, please visit the following URL:

- https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.RegionsAndAvailabilityZones.html

Note:
In this scenario, we need to have 6 instances running all the time, even when 1 AZ is down.

Hence options D & E are correct.

Question 3Correct

Domain: Design Cost-Optimized Architectures0
An application allows a manufacturing site to upload files. Each uploaded 2500 MB file is processed to extract metadata, and this process takes a few seconds per file. The frequency at which the uploading happens is unpredictable. For instance, there may be no upload for hours, followed by several files being uploaded concurrently.

Which architecture will address this workload in the most cost-efficient manner?

- A. Use a Kinesis Data Delivery Stream to store the file. Use Lambda for processing.

- B. Use an SQS queue to store the file to be accessed by a fleet of EC2 Instances.
- C. Store the file in an EBS volume, which can then be accessed by another EC2 Instance for processing.
- D. Store the file in an S3 bucket. Use Amazon S3 event notification to invoke a Lambda function for file processing.right

Explanation:

Answer – D
You can first create a Lambda function with the code to process the file.

Then, you can use an Event Notification from the S3 bucket to invoke the Lambda function whenever a file is uploaded.

Option A is incorrect as Kinesis is used to collect, process, and analyze real-time data.
Option B is incorrect as SQS cannot store a message that is 3GB. The maximum payload supported by SQS is 2GB.
To manage large Amazon Simple Queue Service (Amazon SQS) messages, you can use Amazon Simple Storage Service (Amazon S3) and the Amazon SQS Extended Client Library for Java. This is especially useful for storing and consuming messages up to 2 GB.
Option C is incorrect as EBS is a service to provide block-level storage. S3 is more suitable in this scenario.
Note: The total volume of data and the number of objects you can store are unlimited. Individual Amazon S3 objects can range in size from a minimum of 0 bytes to a maximum of 5 terabytes. The largest object that can be uploaded in a single PUT is 5 gigabytes.
For more information on Amazon S3 event notification, please visit the following URL:

- https://docs.aws.amazon.com/AmazonS3/latest/dev/NotificationHowTo.html
- https://aws.amazon.com/s3/faqs/
- https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-s3-messages.html

Question 4Correct

Domain: Design High-Performing Architectures
You are part of the IT team of a streaming application. Your application is hosted in two separate regions, us-east-1(N Virginia) and ap-south-1 (Mumbai). Your application recently became very popular, and now you have users from all around the world. However, these new users have been experiencing high latency in the application. How can you solve this problem, keeping in mind that possible failovers in the app need to be solved very quickly?

- A. Enable a DNS-based traffic management solution with Geolocation route policies in Route53.
- B. Enable AWS WAF to securely serve your application content to the nearest Edge Locations to the users.

- C. Enable Global Accelerator endpoint for your two regions.right
- D. Enable Direct Connect.

Explanation:

Answer: C

- Option A is incorrect because if there is a failover, you will need to modify the source application's IP address or configure Route53 records. That will take time to solve the failover. More details please check https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html#routing-policy-geo.
- Option B is incorrect because AWS WAF is a service to protect applications from attacks. It does not help to improve the performance or reduce latency.
- Option C is CORRECT because AWS Global Accelerator is a service that redirects users requests to the nearest edge location and then routes the data to the Amazon global network, increasing the speed and security of data transfer, therefore, increasing the performance of our applications. It also reroutes requests to healthy IPs if it fails and changes propagations. It is automatic and lasts some seconds. More details please check https://aws.amazon.com/global-accelerator/faqs/.
- Option D is incorrect because Direct Connect is a service used to increase data transfer between On-Premise data centers and AWS services. More details: https://aws.amazon.com/directconnect/.

Here is the additional explanation on AWS website on Global accelerator FAQ. Why DNS/Route 53 is an inferior option as compared to Global accelerator.

Q: How is AWS Global Accelerator different from a DNS-based traffic management solution?
A: First, some client devices and internet resolvers cache DNS answers for long periods of time. So when you make a configuration update, or there's an application failure or change in your routing preference, you don't know how long it will take before all of your users receive updated IP addresses. With AWS Global Accelerator, you don't have to rely on the IP address caching settings of client devices. Change propagation takes a matter of seconds, which reduces your application downtime. Second, with Global Accelerator, you get static IP addresses that provide a fixed entry point to your applications. This lets you easily move your endpoints between Availability Zones or between AWS Regions, without having to update the DNS configuration or client-facing applications.

Question 5Correct

Domain: Design High-Performing Architectures
For which of the following scenarios should a Solutions Architect consider using ElasticBeanStalk? (Choose TWO.)

- A. A Java web application using Amazon Linux EC2 instancesright
- B. An Enterprise Data Warehouse
- C. Configuring AWS resources using Chef
- D. A worker environment with an SQS queue and an Auto Scaling groupright
- E. A management task run once on nightly basis

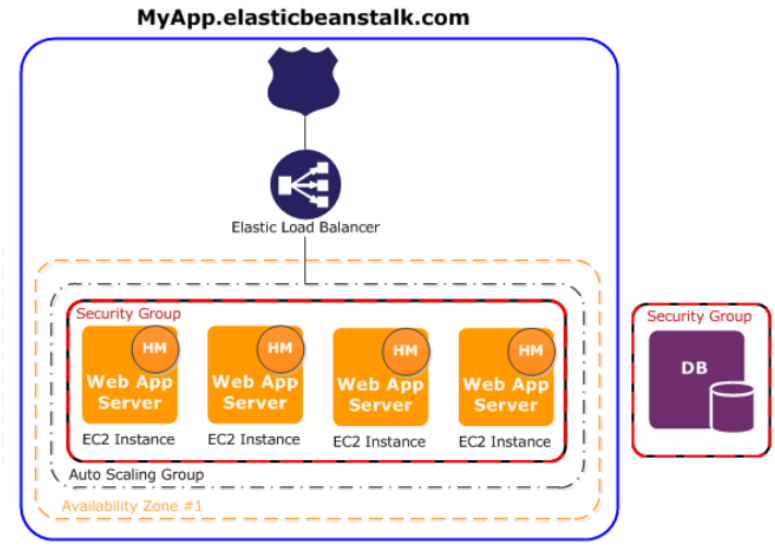
Explanation:

Answer – A and D
AWS Documentation clearly mentions that the Elastic Beanstalk component can create Web Server environments and Worker environments.

The following diagram illustrates an example of Elastic Beanstalk architecture for a web server environment tier and shows how the components in that type of environment tier work together.

https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features-managing-env-tiers.html

This following diagram illustrates an example Elastic Beanstalk architecture for a web server environment tier and shows h the components in that type of environment tier work together. The remainder of this section discusses all the component more detail.



- For more information on AWS Elastic beanstalk Web server environments, please visit the URL https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/concepts-webserver.html
- Option B is incorrect. Elastcibeanstalk is used to deploy and manage the applications on AWS. It's not used to store the data. https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/Welcome.html.
- For more information on AWS Elastic beanstalk Worker environments, please visit the following URL: https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/concepts-worker.html
- Option C is incorrect. OpsWorks is more suitable when Chef is used to configure AWS resources.

- Option D is correct. The worker environments in Elastic Beanstalk include an Auto Scaling group and an SQS queue. This option is suitable.

- Option E is incorrect. When you launch an Elastic Beanstalk environment, you first choose an environment tier. The environment tier that you choose determines whether Elastic Beanstalk provisions resources to support an application that handles HTTP requests or an application that pulls tasks from a queue. An application that serves HTTP requests runs in a web server environment. An environment that pulls tasks from an Amazon Simple Queue Service queue runs in a worker environment.

  Further, when you create an environment, Elastic Beanstalk provisions the resources required to run your application. AWS resources created for an environment include one elastic load balancer (ELB in the diagram), an Auto Scaling group, and one or more Amazon EC2 instances.

  So, these resources must run the application 24/7, not for only at night or day.

Question 6

Domain: Design Cost-Optimized Architectures0

You need to install a 150 GB volume on an EC2 Instance for a new application. While the data in the volume is used less frequently with small peaks in the morning and evening, Which storage type would be the most cost-effective option for the given requirement?

- A. Amazon EBS provisioned IOPS SSD.
- B. Amazon EBS Cold HDD.right
- C. Amazon EBS General Purpose SSD.
- D. Amazon EFS.

Explanation:

Answer – B
The volume data is used infrequently, not throughout the day, and the question requires the MOST cost-effective storage type. So the preferred choice would be Amazon Cold HDD. Cold HDD is suitable for the following scenarios:

- Throughput-oriented storage for data that is infrequently accessed.
- Scenarios where the lowest storage cost is important.

The volume size of EBS Cold HDD is 125 GiB - 16 TiB. The database size is 150G and is suitable in this scenario.

Option D is incorrect because EFS is file storage, not block or volume storage.
Note: IOPS measures the number of reads and writes operations per second, while throughput measures the number of bits read or written per second.

	Throughput Optimized HDD	Cold HDD
Volume type	st1	sc1
Durability	99.8% - 99.9% durability (0.1% - 0.2% annual failure rate)	99.8% - 99.9% durability (0.1% - 0.2% annual failure rate)
Use cases	• Big data • Data warehouses • Log processing	• Throughput-oriented storage for data that is infrequently accessed • Scenarios where the lowest storage cost is important

References:

- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volume-types.html
- https://aws.amazon.com/ebs/features/

Question 7

Domain: Design Cost-Optimized Architectures0
You are working as an AWS consultant for a start-up company. They have developed a web application, that requires a lot of memory, for their employees to share files with external vendors securely. They created an Auto Scaling group for the web servers that require two m4.large EC2 instances running at all times, scaling up to a maximum of twelve instances. Post-deployment of the application, a huge rise in cost was observed. Due to a limited budget, the CTO has requested your advice to optimize the usage of instances in the Auto Scaling groups. What do you suggest for reducing the costs and minimizing the risk of adverse impact on the performance?

- A. Create an Auto Scaling group with t2. micro On-Demand instances.

- B. Create an Auto Scaling group with a mix of On-Demand & Spot Instance. Select the On-Demand base as zero. Above On-Demand base, select 100% of On-Demand instance & 0% of Spot Instance.

- C. Create an Auto Scaling group with all Spot Instance.

- D. Create an Auto Scaling group with a mix of On-Demand & Spot Instance. Select the On-Demand base as 2. Above On-Demand base, select 20% of On-Demand instance & 80% of Spot Instance.right

Explanation:

Correct Answer – D

Auto Scaling group supports a mix of On-Demand & Spot instances, which helps design a cost-optimized solution without impacting the performance. You can choose the percentage of On-Demand & Spot instances based on the application requirements. With Option D, the Auto Scaling group will have 2 instances initially as the On-Demand instances. In contrast, the remaining instances will be launched in a 20 % On-Demand instance & 80% Spot Instance ratio.

No matter, if 80% of spot instances get terminated. The required 20% on-demand will be available with 2 on-demand instances always running.

- Option A is incorrect. With t2. Micro, there would be a cost reduction, but it will impact the performance of the application. The question requires that the performance is not impacted, so changing the instance type is not suitable.
- Option B is incorrect as there would not be any cost reduction with all On-Demand instances.
- Option C is incorrect. Although this will reduce cost, all spot instances in an auto-scaling group may cause inconsistencies in the application & lead to poor performance.

For more information on Auto Scaling with multiple Instance types & purchase options, refer to the following URLs:

- https://aws.amazon.com/blogs/aws/new-ec2-auto-scaling-groups-with-multiple-instance-types-purchase-options/
- https://docs.aws.amazon.com/autoscaling/ec2/userguide/AutoScalingGroup.html#asg-purchase-options

Question 8Correct

Domain: Specify Secure Applications and Architectures

You are working as an AWS Architect for a start-up company. The company has a two-tier production website on AWS with web servers in the front end & database servers in the back end. The third-party firm has been looking after the operations of these database servers. They need to access these database servers in private subnets on the SSH port. As per standard operating procedure provided by the Security team, all access to these servers should be over a jumpbox accessible from internet. What will be the best solution to meet this requirement?

- A. Deploy Bastion hosts in Private Subnet

- B. Deploy NAT Instance in Private Subnet

- C. Deploy NAT Instance in Public Subnet

- D. Deploy Bastion hosts in Public Subnetright

Explanation:

Correct Answer – D
External users will be unable to access the instance in private subnets directly. To provide such access, we need to deploy Bastion hosts in public subnets. In case of the above requirement, third-party users will initiate a connection to Bastion hosts in public subnets & from there, they will access SSH connection to database servers in private subnets.

- Option A is incorrect as Bastion hosts need to be in Public subnets & not in Private subnets, as third-party users will be accessing these servers from the internet.
- Option B is incorrect as NAT instance is used to provide internet traffic to hosts in private subnets. Users from the internet will not be able to do SSH connections to hosts in private subnets using NAT instance. NAT instance is always present in Public subnets.
- Option C is incorrect as NAT instance is used to provide internet traffic to hosts in private subnets. Users from the internet will not be able to do SSH connections to hosts in private subnets using NAT instance.

For more information on bastion instance, refer to the following URL:

- https://docs.aws.amazon.com/quickstart/latest/linux-bastion/architecture.html

Question 9Correct

Domain: Design Resilient Architectures
An AWS Solutions Architect designing a solution to store and archive corporate documents has determined Amazon Glacier as the right choice.

An important requirement is that the data must be delivered within 5 minutes of a retrieval request.

Which feature in Amazon Glacier could help to meet this requirement?

- A. Vault Lock
- B. Expedited retrievalright
- C. Bulk retrieval
- D. Standard retrieval

Explanation:

Correct Answer – B
AWS Documentation mentions the following:

Expedited retrievals allow you to access data in 1–5 minutes for a flat rate of $0.03 per GB retrieved. Expedited retrievals allow you to quickly access your data when occasional urgent requests for a subset of archives are required.

The Vault Lock and Standard Retrieval are standard with 3-5 hours retrieval time while Bulk retrievals which can be considered the cheapest option have 5-12 hours retrieval time.

For more information on AWS Glacier Retrieval, please visit the following URL:

- https://docs.aws.amazon.com/amazonglacier/latest/dev/downloading-an-archive-two-steps.html

Question 10Correct

Domain: Design High-Performing Architectures

You are working for a start-up company that develops mobile gaming applications using AWS resources. For creating AWS resources, the project team is using CloudFormation Templates. The Project Team is concerned about the changes made in EC2 instance properties by the Operations Team, apart from parameters specified in CloudFormation Templates. To observe changes in AWS EC2 instance, you advise using CloudFormation Drift Detection. After Drift detection, when you check drift status for all AWS EC2 instances, drift for certain property values with default values for resource properties is not displayed. What would you do to include these resource properties to be captured in CloudFormation Drift Detection?

- A. Run CloudFormation Drift Detection on individual stack resources instead of entire CloudFormation stack.
- B. Explicitly set the property value, which can be the same as the default value.right
- C. Manually check these resources as this is not supported in CloudFormation Drift Detection.
- D. Assign Read permission to CloudFormation Drift Detection to determine drift.

Explanation:

Correct Answer – B

AWS CloudFormation Drift Detection can be used to detect changes made to AWS resources outside the CloudFormation Templates. AWS CloudFormation Drift Detection only checks property values explicitly set by stack templates or by specifying template parameters. It does not determine drift for property values that are set by default. To determine drift for these resources, you can explicitly set property values that can be the same as that of the default value.

- Option A is incorrect. If property values are assigned explicitly to these properties, running AWS CloudFormation Drift Detection would be detected in both individuals and the entire CloudFormation Stack.
- Option C is incorrect as CloudFormation Drift Detection supports the AWS EC2 instance.
- Option D is incorrect. Since for all other resources, CloudFormation Drift Detection has already determined drift, there is no other read permission to be granted further.

For more information on CloudFormation Drift Detection, refer to the following URL:

https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-cfn-stack-drift.html

Question 11Correct

Domain: Design Resilient Architectures

You are responsible for performing a migration from your company's on-premise data to the AWS cloud. You have about 400 GB of data stored in an NFS. One requirement of this migration is to transfer some of this data to AWS EFS and the other part to S3. Which is the easiest to use and with the most cost-effective solution?

- A. Use AWS Storage gateway.
- B. Use S3 Transfer Acceleration.

- C. Use AWS DataSync.right
- D. Use AWS Database Migration Service.

Explanation:

Answer: C

- Option A is incorrect. Storage Gateway is a hybrid cloud storage service to share and access data between your on-premise resources and AWS resources. It is not mainly designed to migrate data from On-Premise to AWS. Additionally, all three storage gateway patterns are backed by S3, not EFS. More details: https://aws.amazon.com/storagegateway/faqs/.
- Option B is incorrect. S3 Transfer Acceleration is used to transfer data to S3 using Amazon CloudFront's globally distributed edge locations, increasing data transfer speed. However, this option doesn't work to transfer data to AWS EFS. More details: https://docs.aws.amazon.com/AmazonS3/latest/dev/transfer-acceleration.html.
- Option C is CORRECT. DataSync is a service used to transfer data between on-premise storage to AWS S3, EFS and FSx. It is cost-effective, easy to use, and can handle the transfer to EFS and S3. More details: https://aws.amazon.com/datasync/faqs/.
- Option D is incorrect because AWS Database Migration Service is used to migrate databases to AWS databases like Aurora, DynamoDB, etc. In this scenario, we don't mention a database migration, and with this service, you can not transfer data to EFS nor S3. More details: https://aws.amazon.com/dms/.

Question 12Incorrect

Domain: Design High-Performing Architectures

A company hosts a popular web application that connects to an Amazon RDS MySQL DB instance running in a default VPC private subnet with NACL settings that was created by AWS as default. The web servers must be accessible only to customers on HTTPS connections, and the database must only be accessible to web servers in a public subnet. Which solution would meet these requirements without impacting other applications? (SELECT TWO)

- A. Create a network ACL on the Web Server's subnets, allow HTTPS port 443 inbound and specify the source as 0.0.0.0/0.
- B. Create a Web Server security group that allows HTTPS port 443 inbound traffic from anywhere (0.0.0.0/0) and apply it to the Web Servers.right
- C. Create a DB Server security group that allows MySQL port 3306 inbound and specify the source as the Web Server security group.right
- D. Create a network ACL on the DB subnet, allow MySQL port 3306 inbound for Web Servers and deny all outbound traffic.
- E. Create a DB Server security group that allows HTTPS port 443 inbound and specify the source as a Web Server security group.wrong

Explanation:

Correct Answer – B and C

This sort of setup is explained in the AWS documentation.

1) To ensure that traffic can flow into your webserver from anywhere on secure traffic, you need to allow inbound security at 443.

2) And then, you need to ensure that traffic can flow from the webserver to the database server via the database security group.

The below snapshots from the AWS Documentation show rule tables for security groups related to the same requirements as in the question.

WEBSERVER SG			
Inbound			
Source	protocol	port range	comments
0.0.0.0/0	TCP	443	Allow inbound HTTPS access to the Web Servers from any IPv4 Address

DBServerSG: Recommended Rules

Inbound			
Source	**Protocol**	**Port Range**	**Comments**
The ID of your WebServerSG security group	TCP	1433	Allow inbound Microsoft SQL Server access from the web servers associated with the WebServerSG security group.
The ID of your WebServerSG security group	TCP	3306	Allow inbound MySQL Server access from the web servers associated with the WebServerSG security group.

- For more information on this use case scenario, please visit the following URL:
  - https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2.html

- Options A and D are invalid answers.

- Network ACLs are stateless. So we need to set rules for both inbound and outbound traffic for Network ACLs.

- Option E is also invalid because, in order to communicate with the MySQL servers, we need to allow traffic to flow through port 3306.

- Note: The above correct options are the combination of steps required to secure your web and database servers. Besides, the company may implement additional security measures from their end.

Question 13 Correct

Domain: Design High-Performing Architectures

You lead a team to develop a new web application in AWS EC2. The application will have a large number of users globally. For a great user experience, this application requires very low network latency and jitter. If the network speed is not fast enough, you will lose customers. Which tool would you choose to improve the application performance? (Select TWO.)

- A. AWS VPN
- B. AWS Global Accelerator right

- C. Direct Connect
- D. API Gateway
- E. CloudFrontright

Explanation:

Correct Answer – B, E
This web application has global users and needs low latency. Both CloudFront and Global Accelerator can speed up the distribution of contents over the AWS global network.

- Option A is incorrect: AWS VPN links on-premise network to AWS network. However, no on-premise services are mentioned in this question.
- Option B is CORRECT: AWS Global Accelerator works at the network layer and can direct traffic to optimal endpoints. For reference, check the link https://docs.aws.amazon.com/global-accelerator/latest/dg/what-is-global-accelerator.html
- Option C is incorrect: Direct Connect links on-premise network to AWS network. However, no on-premise services are mentioned in this question.
- Option D is incorrect: API Gateway is a regional service and cannot improve the application performance. API Gateway is suitable for serverless applications such as Lambda.
- Option E is CORRECT: Because CloudFront delivers content through edge locations, and users are routed to the edge location with the lowest time delay.

Question 14Correct

Domain: Design Secure Applications and Architectures
You are deploying an application on Amazon EC2 that must call AWS APIs. Which method would you use to allow the application access to the APIs securely?

- A. Pass API credentials to the instance using Instance userdata.
- B. Store API credentials as an object in Amazon S3.
- C. Embed the API credentials into your application.
- D. Assign IAM roles to the EC2 Instances.right

Explanation:

Correct Answer - D
AWS Documentation mentions the following:

You can use roles to delegate access to users, applications, or services that don't normally have access to your AWS resources. It is not a good practice to use IAM credentials for a production-based application. However, it is a good practice to use IAM Roles.

For more information on IAM Roles, please visit the following URL:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html

Question 15Correct

Domain: Design High-Performing Architectures

A website runs on EC2 Instances behind an Application Load Balancer. The instances run in an Auto Scaling Group across multiple Availability Zones and deliver several static files stored on a shared Amazon EFS file system. The company needs to avoid serving the files from EC2 Instances every time a user requests these digital assets.

What should the company do to improve the user experience of the website?

- A. Move the digital assets to Amazon Glacier.
- B. Cache static content using CloudFront.right
- C. Resize the images so that they are smaller.
- D. Use reserved EC2 Instances.

Explanation:

Answer - B

AWS Documentation mentions the following about the benefits of using CloudFront:

Amazon CloudFront is a web service that speeds up distribution of your static and dynamic web content, such as .html, .css, .js, and image files to your users. CloudFront delivers your content through a worldwide network of data centers called edge locations. When a user requests content that you're serving with CloudFront, the user is routed to the edge location that provides the lowest latency (time delay), so that the content is delivered with the best possible performance. If the content is already in the edge location with the lowest latency, CloudFront delivers it immediately.

For more information on AWS CloudFront, please visit the following URL on page 3 under the section "Accelerate Static Website Content Delivery":

- https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html

The glacier is not used for frequent retrievals. So Option A is not a good solution. Options C & D will also not help in this situation.

Question 16Correct

Domain: Design Resilient Architectures

A Solutions Architect is designing a highly scalable system to track records. These records must remain available for immediate download for up to three months and then must be deleted. What is the most appropriate decision for this use case?

- A. Store the files in Amazon EBS and create a Lifecycle Policy to remove files after 3 months.
- B. Store the files in Amazon S3 and create a Lifecycle Policy to remove files after 3 months.right
- C. Store the files in Amazon Glacier and create a Lifecycle Policy to remove files after 3 months.
- D. Store the files in Amazon EFS and create a Lifecycle Policy to remove files after 3 months.

Explanation:

Correct Answer – B

- Option A is incorrect since the records need to be stored in a highly scalable system.
- Option C is incorrect since the records must be available for immediate download.
- Option D is incorrect since EFS lifecycle management is used to migrate files that have not been accessed for a certain period of time to the Infrequent Access storage class. Files moved to this storage remain indefinitely and not get deleted. And due to this reason, this option is not correct.

AWS Documentation mentions the following about Lifecycle Policies:

Lifecycle configuration enables you to specify the Lifecycle Management of objects in a bucket. The configuration is a set of one or more rules, where each rule defines an action for Amazon S3 to apply to a group of objects. These actions can be classified as follows:

Transition actions – In which you define when the transition of the object occurs to another storage class. For example, you may choose to transition objects to the STANDARD_IA (IA, for infrequent access) storage class 30 days after creation or archive objects to the GLACIER storage class one year after creation.
Expiration actions – In which you specify when the objects will expire. Then Amazon S3 deletes the expired objects on your behalf.
For more information on AWS S3 Lifecycle Policies, please visit the following URL:

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

To know more about EFS Lifecycle Management, please check the following URL:

https://docs.aws.amazon.com/efs/latest/ug//lifecycle-management-efs.html

Question 17Correct

Domain: Design High-Performing Architectures
A consulting firm repeatedly builds large architectures for their customers using AWS resources from several AWS services, including IAM, Amazon EC2, Amazon RDS, DynamoDB and Amazon VPC. The consultants have architecture diagrams for each of their architectures and are frustrated that they cannot use them to create their resources automatically.

Which service should provide immediate benefits to the organization?

- A. AWS Beanstalk
- B. AWS CloudFormationright
- C. AWS CodeBuild
- D. AWS CodeDeploy

Explanation:

Answer - B
AWS CloudFormation: This supplements the requirement in the question and enables consultants to use their architecture diagrams to construct CloudFormation templates.

AWS Documentation mentions the following on AWS CloudFormation:

AWS CloudFormation is a service that helps you model and set up your Amazon Web Service resources so that you can spend less time managing those resources and more time focusing on your applications that

run in AWS. You create a template that describes all the AWS resources that you want (like Amazon EC2 instances or Amazon RDS DB instances), and AWS CloudFormation takes care of provisioning and configuring those resources for you.

For more information on AWS Cloudformation, please visit the following URL:

https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/Welcome.html

AWS Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services developed with Java, .NET, PHP, Node.js etc. You can upload your code, and Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring.

In question mentioned that "A consulting firm **repeatedly builds large architectures for their customers using AWS resources from several AWS services including IAM, Amazon EC2, Amazon RDS, DynamoDB and Amazon VPC.**"

When you are building large architectures repeatedly, you can use the CloudFormation template to create or modify an existing AWS CloudFormation template. A template describes all of your resources and their properties. When you use that template to create an AWS CloudFormation stack, AWS CloudFormation provisions the Auto Scaling group, load balancer, and database for you. After the stack has been successfully created, your AWS resources are up and running. You can delete the stack just as easily, which deletes all the resources in the stack. By using AWS CloudFormation, you easily manage a collection of resources as a single unit. Whenever working with more number of AWS resources together, CloudFormation is the best option.

Question 18Correct

Domain: Design Secure Applications and Architectures

The security policy of an organization requires an application to encrypt data before writing to the disk. Which solution should the organization use to meet this requirement?

- A. AWS KMS APIright
- B. AWS Certificate Manager
- C. API Gateway with STS
- D. IAM Access Key

Explanation:

Correct Answer – A

Option B is incorrect. The AWS Certificate Manager can be used to generate SSL certificates to encrypt traffic in transit, but not at rest.

Option C is incorrect. It is used for issuing tokens while using the API gateway for traffic in transit.

Option D is used for providing secure access to EC2 Instances.

AWS Documentation mentions the following on AWS KMS:

AWS Key Management Service (AWS KMS) is a managed service that makes it easy for you to create and control the encryption keys used to encrypt your data. AWS KMS is integrated with other AWS services including Amazon Elastic Block Store (Amazon EBS), Amazon Simple Storage Service (Amazon S3),

Amazon Redshift, Amazon Elastic Transcoder, Amazon WorkMail, Amazon Relational Database Service (Amazon RDS), and others to make it simple to encrypt your data with encryption keys that you manage.

For more information on AWS KMS, please visit the following URL:

https://docs.aws.amazon.com/kms/latest/developerguide/overview.html
The AWS KMS API can be used to encrypt, decrypt and reencrypt content. Please refer the following guide:

https://docs.aws.amazon.com/kms/latest/APIReference/kms-api-reference.pdf#Welcome

Question 19Correct

Domain: Design High-Performing Architectures
You are an AWS Solutions Architect. Your company has a successful web application deployed across multiple AWS Regions. The application attracts more and more global customers. However, the application's performance is impacted. Your manager asks you how to improve the performance and availability of the application. Which of the following AWS services would you recommend?

- A. AWS DataSync
- B. Amazon DynamoDB Accelerator
- C. AWS Lake Formation
- D. AWS Global Acceleratorright

Explanation:

Correct Answer – D
AWS Global accelerator provides static IP addresses that are anycast in the AWS edge network. Incoming traffic is distributed across endpoints in AWS regions. The performance and availability of the application are improved.

- Option A is incorrect: Because DataSync is a tool to automate the data transfer and does not improve the performance.
- Option B is incorrect: DynamoDB is not mentioned in this question.
- Option C is incorrect: Because AWS Lake Formation is used to manage a large amount of data in AWS, which would not help in this situation.
- Option D is CORRECT: Check the AWS Global Accelerator use cases in https://docs.aws.amazon.com/global-accelerator/latest/dg/introduction-benefits-of-migrating.html. The Global Accelerator service can improve both the application performance and availability.

Question 20Correct

Domain: Design Secure Applications and Architectures
A retailer exports data daily from its transactional databases into an S3 bucket in the Sydney region. The retailer's Data Warehousing team wants to import this data into an existing Amazon Redshift cluster in their VPC in Sydney. Corporate security policy mandates that data can **only be transported within the AWS's private network.**

Which steps would satisfy the security policy?
(SELECT TWO.)

- A. Enable Amazon Redshift Enhanced VPC Routing.right
- B. Create a Cluster Security Group to allow the Amazon Redshift cluster to access Amazon S3.
- C. Create a NAT gateway in a public subnet to allow the Amazon Redshift cluster to access Amazon S3.
- D. Create and configure an Amazon S3 VPC endpoint. right

Explanation:

Correct Answer – A and D
Amazon Redshift Enhanced VPC Routing provides VPC resources access to Redshift.

Redshift will not be able to access the S3 VPC endpoints without enabling Enhanced VPC routing. So one option will not support the scenario if another is not selected.

NAT instance (the proposed answer) cannot be reached by Redshift without enabling Enhanced VPC Routing.

- https://aws.amazon.com/about-aws/whats-new/2016/09/amazon-redshift-now-supports-enhanced-vpc-routing/

Option D:

- VPC Endpoints - It enables you to privately connect your VPC to the supported AWS Services and VPC Endpoint services powered by Private Link without requiring an IGW, NAT Device, VPN Connection or AWS Direct Connect connections. Instances in VPC do not require Public IP addresses to communicate with resources in the service and traffic between your VPC and other service does not leave the Amazon network.
- S3 VPC Endpoint - it is a feature that will allow you to make even better use of VPC and S3.

I recommend you to look into the following URLs to know the concept further.

- https://aws.amazon.com/blogs/aws/new-vpc-endpoint-for-amazon-s3/
- https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints-s3.html

Question 21Correct

Domain: Design Resilient Architectures
A team is building an application that must persist and index JSON data in a highly available data store. The latency of data access must remain consistent despite very high application traffic.

Which service would help the team to meet the above requirement?

- A. Amazon EFS
- B. Amazon Redshift
- C. DynamoDB right
- D. AWS CloudFormation

Explanation:

Correct Answer – C
AWS Documentation mentions the following about DynamoDB:

Amazon DynamoDB is a fully managed NoSQL database service that provides fast and predictable performance with seamless scalability.

The data in DynamoDB is stored in JSON format. Hence it is the perfect data storage to meet the requirement mentioned in the question.

For more information on AWS DynamoDB, please visit the following URL:

https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Introduction.html

Question 22Correct

Domain: Design High-Performing Architectures
An organization hosts a multi-language website on AWS, which is served using CloudFront. Language is specified in the HTTP request as shown below:

- http://d11111f8.cloudfront.net/main.html?language=de
- http://d11111f8.cloudfront.net/main.html?language=en
- http://d11111f8.cloudfront.net/main.html?language=es

How should AWS CloudFront be configured to deliver cached data in the correct language?

- A. Forward cookies to the origin
- B. Based on query string parametersright
- C. Cache objects at the origin
- D. Serve dynamic content

Explanation:

Correct Answer – B
Since language is specified in the query string parameters, CloudFront should be configured for the same.

For more information on configuring CloudFront via query string parameters, please visit the following URL:

- https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/QueryStringParameters.html

Question 23Correct

Domain: Design Resilient Architectures
You have developed a new web application on AWS for a real estate firm. It has a web interface where real estate employees upload photos of newly constructed houses in S3 buckets. Prospective buyers log in to the website and access photos. The marketing team has initiated an intensive marketing event to promote new housing schemes which will lead to customers who frequently access these images. As this is a new application, you have no projection of traffic on the S3 bucket. You need an S3 storage class that

can automatically optimize the storage costs with changing access patterns. Which of the following is a recommended storage solution to meet this requirement?

- A. Use One Zone-IA storage class to store all images.
- B. Use Standard-IA to store all images.
- C. Use S3 Intelligent-Tiering storage class.right
- D. Use Standard storage class and use Storage class analytics to identify & move objects using lifecycle policies.

Explanation:

Correct Answer – C
When the access pattern to web applications using S3 storage buckets is unpredictable, you can use S3 intelligent-Tiering storage class. S3 Intelligent-Tiering storage class includes two access tiers: frequent access and infrequent access. Based upon access patterns, it moves data between these tiers, which helps in cost saving. S3 Intelligent-Tiering storage class has the same performance as that of Standard storage class.

- Option A is incorrect. Although it will save costs, it will not provide any protection in case of AZ failure. Also, this class is suitable for infrequently accessed data & not for frequently access data.
- Option B is incorrect as Standard-IA storage class is for infrequently accessed data & there are retrieval charges associated. In the above requirement, you do not know the data access pattern, which may result in a higher cost.
- Option D is incorrect. It has operational overhead to set up Storage class analytics & moves objects between various classes. Also, since the access pattern is undetermined, this will run into a costlier option.

For more information on S3 Intelligent-Tiering, refer to the following URLs:

- https://aws.amazon.com/blogs/aws/new-automatic-cost-optimization-for-amazon-s3-via-intelligent-tiering/

Question 24Correct

Domain: Design Cost-Optimized Architectures
You are part of the IT team of an assurance company. You have been having a consistent amount of usage of your EC2 instances and Fargate. However, there is also a consistent amount of usage increase. Because of this, you can predict that you may need to increase the size of the instances in 2 or 3 years. The finance team has asked you if there is a way to save costs in the EC2 instances and Fargate. What do you suggest?

- A. Purchase a Compute Saving plan.right
- B. Purchase an EC2 instance saving plan.
- C. Purchase a Convertible Reserved Instance.
- D. Purchase a Standard Reserved Instance.

Explanation:

Answer: A

- Option A is CORRECT. With a Compute Saving Plan, you can save up to 66% and it applies to Fargate and EC2 instances. It also lets you change the instance's family and size. More details-
- https://aws.amazon.com/savingsplans/faq/
- Option B is incorrect. The EC2 instance saving plan does not apply automatically to Fargate instances. More details-
- https://aws.amazon.com/savingsplans/faq/
- Options C and D are incorrect. Reserved instances do not save the cost of Fargate. More details-
- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-reserved-instances.html

Question 25Correct

Domain: Design High-Performing Architectures

A company is generating large datasets with millions of rows to be summarized column-wise. To build daily reports from these data sets, Business Intelligence tools would be used.

Which storage service would meet these requirements?

- A. Amazon Redshiftright
- B. Amazon RDS
- C. ElastiCache
- D. DynamoDB

Explanation:

Correct Answer – A

AWS Documentation mentions the following:

Amazon Redshift is a fully managed, petabyte-scale data warehouse service in the cloud. You can start with just a few hundred gigabytes of data and scale to a petabyte or more. This enables you to use your data to acquire new insights for your business and customers.

For more information on AWS Redshift, please visit the following URL:

- https://docs.aws.amazon.com/redshift/latest/mgmt/welcome.html

Columnar storage for database tables is an important factor in optimizing analytic query performance because it drastically reduces the overall disk I/O requirements and the amount of data you need to load from disk.

Amazon Redshift uses a block size of 1 MB, which is more efficient and further reduces the number of I/O requests needed to perform any database loading or other operations that are part of query execution.

For more information on how redshift manages the columnar storage, please visit the following URL:

- https://docs.aws.amazon.com/redshift/latest/dg/c_columnar_storage_disk_mem_mgmnt.html

Question 26Correct

Domain: Design High-Performing Architectures

A company is developing a web application to be hosted in AWS. This application needs a data store for session data.

As an AWS Solution Architect, what would you recommend as an ideal option to store session data? (SELECT TWO)

- A. CloudWatch
- B. DynamoDBright
- C. Elastic Load Balancing
- D. ElastiCacheright
- E. Storage Gateway

Explanation:

Correct Answer - B and D
DynamoDB and ElastiCache are perfect options for storing session data.

AWS Documentation mentions the following on Amazon DynamoDB:

Amazon DynamoDB is a fast and flexible NoSQL database service for all applications that need consistent, single-digit millisecond latency at any scale. It is a fully managed cloud database and supports both document and key-value store models. Its flexible data model, reliable performance, and automatic scaling of throughput capacity make it a great fit for mobile, web, gaming, ad tech, IoT, and many other applications.

For more information on AWS DynamoDB, please visit the following URL:

- https://aws.amazon.com/dynamodb/

AWS Documentation mentions the following on AWS ElastiCache:

AWS ElastiCache is a web service that makes it easy to set up, manage, and scale a distributed in-memory data store or cache environment in the cloud. It provides a high-performance, scalable, and cost-effective caching solution while removing the complexity associated with the deployment and management of a distributed cache environment.

For more information on AWS Elasticache, please visit the following URL:

- https://docs.aws.amazon.com/AmazonElastiCache/latest/UserGuide/WhatIs.html

Option A is incorrect. AWS CloudWatch offers cloud monitoring services for the customers of AWS resources.

Option C is incorrect. AWS Elastic Load Balancing automatically distributes incoming application traffic across multiple targets.

Option E is incorrect. AWS Storage Gateway is a hybrid storage service that enables your on-premises applications to use AWS cloud storage seamlessly.

Question 27Correct

Domain: Design Resilient Architectures
A company needs to store images that are uploaded by users via a mobile application. There is also a need to ensure that security measures are in place to avoid data loss.

What step should be taken for protection against unintended user actions?

- A. Store data in an EBS volume and create snapshots once a week.

- B. Store data in an S3 bucket and enable versioning.right
- C. Store data on Amazon EFS storage.

- D. Store data on EC2 instance storage.

Explanation:

Correct Answer - B
Amazon S3 has an option for versioning, as shown below. Versioning is on the bucket level and can be used to recover prior versions of an object.

For more information on AWS S3 versioning, please visit the following URL:

https://docs.aws.amazon.com/AmazonS3/latest/dev/Versioning.html
Option A is incorrect as it does not offer protection against accidental deletion of files.

Option C is incorrect. It is not the ideal solution because multiple EC2 instances can access the file system.

Option D is ephemeral.

Question 28Correct

Domain: Design High-Performing Architectures
An application needs to have a relational Datastore hosted in AWS. The following requirements are in place for the Datastore:

a) The initial storage capacity of 8 TB

b) The ability to accommodate a database growth of 8GB per day

c) The ability to have 4 Read Replicas

Which of the following Datastore is the best for this requirement?

- A. DynamoDB

- B. Amazon S3

- C. Amazon Auroraright
- D. ElastiCache

Explanation:

Correct Answer – C
Aurora can have a storage limit of 64TB and can easily accommodate the initial 8TB plus a database growth of 8GB/day for nearly a period of 20+ years. It can have up to 15 Aurora Replicas that can be distributed across the Availability Zones that a DB cluster spans within an AWS Region.

Aurora Replicas work well for read scaling because they are fully dedicated to read operations on the cluster volume. Write operations are managed by the primary instance. Because the cluster volume is shared among all DB instances in your DB cluster, no additional work is required to replicate a copy of each Aurora Replica data.

For more information on AWS Aurora, please visit the following URL:

- https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Aurora.Replication.html

Note:
Our DB choice needs to fulfill the 3 criteria.

1. Initial Storage capacity 8 TB
2. Daily DB growth of 8GB/day
3. Need 4 Read replicas

DynamoDB is incorrect because it is not a relational database.

ElastiCache is incorrect because it is a distributed in-memory cache service. In this scenario, a datastore is required.

Question 29Correct

Domain: Design Resilient Architectures0
There is a requirement to host a database on an EC2 Instance. It is also required that the EBS volume should support 32,000 IOPS.
Which Amazon EBS volume type would meet the performance requirements of this database?

- A. EBS Provisioned IOPS SSDright
- B. EBS Throughput Optimized HDD
- C. EBS General Purpose SSD
- D. EBS Cold HDD

Explanation:

Correct Answer – A
For high performance and high IOPS requirements, as in this case, the ideal choice would be to choose EBS Provisioned IOPS SSD.

The below snapshot from the AWS Documentation shows the usage of Provisioned IOPS for better IOPS performance in database-based applications.

For more information on AWS EBS Volume types, please visit the following URL:

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

Question 30Correct

Domain: Design Resilient Architectures

In your organization, development teams use S3 buckets to store log files for various applications hosted in AWS development environments. The developers intend to keep the logs for a month for troubleshooting purposes and subsequently purge the logs.

Which feature should be used to enable this requirement?

- A. Adding a bucket policy on the S3 bucket.
- B. Configuring lifecycle configuration rules on the S3 bucket.right
- C. Creating an IAM policy for the S3 bucket.
- D. Enabling CORS on the S3 bucket.

Explanation:

Correct Answer – B

AWS Documentation mentions the following on Lifecycle policies:

Lifecycle configuration enables you to specify the Lifecycle management of objects in a bucket. The configuration is a set of one or more rules, where each rule defines an action for Amazon S3 to apply to a group of objects. These actions can be classified as follows:

- Transition actions – In which you define when objects transition to another storage class. For example, you may choose to transition objects to the STANDARD_IA (IA, for infrequent access) storage class 30 days after creation or archive objects to the GLACIER storage class one year after creation.
- Expiration actions – In which you specify when the objects expire. Then, Amazon S3 deletes the expired objects on your behalf.

For more information on AWS S3 Lifecycle policies, please visit the following URL:

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

Question 31Correct

Domain: Design Resilient Architectures0

You are creating a new architecture for a financial firm. The architecture consists of some EC2 instances of different types and sizes. The management team has asked you to create this architecture by ensuring the reduction of the risk of simultaneous failures. Which placement group option could you suggest for the instances?

- A. Clustered Placement Group
- B. Partition Placement Group
- C. Multi-AZ Placement Group
- D. Spread Placement Groupright

Explanation:

Answer: D

- Option A is incorrect. In Clustered Placement Groups, all the instances are placed in the same rack in the same availability zone. Therefore, they are very susceptible to hardware failures and simultaneous failures. Also, it is suggested to have the same size and types of instances in this Placement Group. More details-
- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html
- Option B is incorrect. In partition placement groups, the chances of hardware failures and simultaneous failure are reduced compared to the Clustered placement group. Still, the Spread Placement group has fewer chances of this kind of failure. It is also suggested to have the same size and types of instances in this Placement Group. More details-
- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html
- Option C is incorrect. The Multi-AZ Placement Group does not exist. More details-
- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html
- Option D is CORRECT. Spread Placement Groups place the instances in different racks. Every rack has its own hardware and power source. So, there is a minimum chance of simultaneous failure. More details-
- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html

Question 32Correct

Domain: Design High-Performing Architectures

You are creating a new architecture for a financial firm. The architecture consists of some EC2 instances with the same type and size (M5.large). In this architecture, all the EC2 mostly communicate with each other. Business people have asked you to create this architecture keeping in mind low latency as a priority. Which placement group option could you suggest for the instances?

- A. Partition Placement Group
- B. Clustered Placement Groupright
- C. Spread Placement Group
- D. Enhanced Networking Placement Group

Explanation:

Answer: B

- Option A is incorrect. Partition Placement Groups distribute the instances in different partitions. The partitions are placed in the same AZ, but do not share the same rack. This type of placement group does not provide low latency throughput to the instances. More details-
- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html
- Option B is CORRECT. Clustered Placement Group places all the instances on the same rack. This placement group option provides 10 Gbps connectivity between instances (Internet

connectivity in the instances has a maximum of 5 Gbps). This option of placement group is perfect for the workload that needs low latency. More details-

- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html
- Option C is incorrect. Placement Groups place all the instances in different racks in the same AZ. These types of placement groups do not provide low latency throughput to the instances. More details-
- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html
- Option D is incorrect. Enhanced Networking Placement Group does not exist. More details-
- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html

Question 33Correct

Domain: Design High-Performing Architectures

A company has a media processing application deployed in a local data center. Its file storage is built on a Microsoft Windows file server. The application and file server need to be migrated to AWS. You want to set up the file server in AWS quickly. The application code should continue working to access the file systems. Which method should you choose to create the file server?

- A. Create a Windows File Server from Amazon WorkSpaces.
- B. Configure a high performance Windows File System in Amazon EFS.
- C. Create a Windows File Server in Amazon FSx.right
- D. Configure a secure enterprise storage through Amazon WorkDocs.

Explanation:

Correct Answer – C

In this question, a Windows file server is required in AWS, and the application should continue to work unchanged. Amazon FSx for Windows File Server is the correct answer as it is backed by a fully native Windows file system.

- Option A is incorrect: Because Amazon WorkSpace configures a desktop server which is not required in this question. Only a Windows file server is needed.
- Option B is incorrect: Because EFS cannot be used to configure a Windows file server.
- Option C is CORRECT: Because Amazon FSx provides fully managed Microsoft Windows file servers. Check the reference in https://docs.aws.amazon.com/fsx/latest/WindowsGuide/what-is.html.
- Option D is incorrect: Because Amazon WorkDocs is a file sharing service in AWS. It cannot provide a native Windows file system.

Question 34Correct

Domain: Design Secure Applications and Architectures

There is a requirement to get the source IP addresses that access resources in a private subnet. Which of the following cost-optimized service could be used to fulfill this purpose?

- A. Trusted Advisor
- B. VPC Flow Logsright

- C. Use CloudWatch metrics

- D. Use CloudTrail

Explanation:

Correct Answer – B
The AWS Documentation mentions the following:

VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. Flow log data is stored using Amazon CloudWatch Logs. After you've created a flow log, you can view and retrieve its data in Amazon CloudWatch Logs.

For more information on VPC Flow Logs, please visit the following URL:

https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/flow-logs.html
Option A is INCORRECT because AWS Trusted Advisor is your customized cloud expert! It helps you to observe the best practices for using AWS by inspecting your AWS environment to save money, improve system performance and reliability, and close security gaps.
Option C is INCORRECT because CloudWatch Metric is mainly used for performance metrics and cannot provide the source IP addresses.
Option D is INCORRECT because AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. However, it is costly to use a CloudTrail.
https://aws.amazon.com/about-aws/whats-new/2018/08/aws-cloudtrail-adds-vpc-endpoint-support-to-aws-privatelink/#:~:text=This%20enables%20you%20to%20connect,VPC%20through%20the%20Amazon%20network.&text=By%20using%20AWS%20CloudTrail%20with,your%20compliance%20and%20regulatory%20requirements

Question 35Correct

Domain: Design Resilient Architectures
You are part of the IT team of a small car manufacturer company. The company is starting to move its On-Premise resources to the cloud. The Marketing department was the first department to migrate its applications to the cloud. Now the finance team wants to do the same. Each department should have its own AWS account but you need one management account to pay for the bills of all the AWS accounts. What do you suggest to solve this?

- A. Create a different VPC for the Finance Department and limit their access to resources with IAM Roles and Policies.

- B. Use AWS Control Tower.

- C. Use AWS Organizations to manage both AWS accounts.right
- D. Use AWS Cost Explorer to divide the bills and use IAM policies to limit the access to resources.

Explanation:

Correct Answer: C

- Option A is incorrect. This option does not cover the splitting bill requirements. Also, a different VPC is not the best option to separate projects or environments.

- Option B is incorrect. Control Tower is more suitable to automate a deployment in multi-account environments. More details: https://aws.amazon.com/controltower/faqs/
- Option C is CORRECT. With AWS Organizations, you can have separate bills for every account and pay it with the same account using consolidating billing. More details: https://aws.amazon.com/organizations/faqs/.
- Option D is incorrect. With AWS Cost Explorer, you can analyze and explore your bills and service usage in the account. But in the end, there will be one bill for the account. More details- https://aws.amazon.com/aws-cost-management/faqs/

Question 36Correct

Domain: Design High-Performing Architectures

Your team is developing a high-performance computing (HPC) application. The application resolves complex, compute-intensive problems and needs a high-performance and low-latency Lustre file system. You need to configure this file system in AWS at a low cost. Which method is the most suitable?

- A. Create a Lustre file system through Amazon FSx.right
- B. Launch a high performance Lustre file system in Amazon EBS.
- C. Create a high-speed volume cluster in EC2 placement group.
- D. Launch the Lustre file system from AWS Marketplace.

Explanation:

Correct Answer – A

The Lustre file system is an open-source, parallel file system that can be used for HPC applications. Refer to http://lustre.org/ for its introduction. In Amazon FSx, users can quickly launch a Lustre file system at a low cost.

- Option A is CORRECT: Amazon FSx supports Lustre file systems, and users pay for only the resources they use.
- Option B is incorrect: Although users may be able to configure a Lustre file system through EBS, it needs lots of extra configurations. Option A is more straightforward.
- Option C is incorrect: Because the EC2 placement group does not support a Lustre file system.
- Option D is incorrect: Because products in AWS Marketplace are not cost-effective. For Amazon FSx, there are no minimum fees or set-up charges. Check its pricing in
  - https://aws.amazon.com/fsx/lustre/pricing/.

Question 37Correct

Domain: Design Resilient Architectures

A Redshift cluster currently contains 60TB of data. There is a requirement that a disaster recovery site is put in place in another region. Which solution would help ensure that this requirement is fulfilled?

- A. Take a copy of the underlying EBS volumes to S3, and then do Cross-Region Replication.
- B. Enable Cross-Region snapshots for the Redshift Cluster.right
- C. Create a CloudFormation template to restore the Cluster in another region.
- D. Enable Cross Availability Zone snapshots for the Redshift Cluster.

Explanation:

Correct Answer – B
The below diagram shows that snapshots are available for Redshift clusters enabling them to be available in different regions.

For more information on managing Redshift snapshots, please visit the following URLs:

- https://docs.aws.amazon.com/redshift/latest/mgmt/managing-snapshots-console.html
- https://aws.amazon.com/blogs/aws/automated-cross-region-snapshot-copy-for-amazon-redshift/

Question 38

Domain: Design Secure Applications and Architectures0
A company is using a Redshift cluster to store its data warehouse. There is a requirement from the Internal IT Security team to encrypt data in the Redshift database. How could this be achieved? (SELECT TWO)

- A. Encrypt the EBS volumes of the underlying EC2 Instances.
- B. Use AWS KMS Customer Default master key.right
- C. Use SSL/TLS for encrypting the data.wrong
- D. Use hardware security module (HSM) to manage the top-level encryption keys .right

Explanation:

Correct Answer - B and D
AWS documentation mentions the following:

Amazon Redshift uses a hierarchy of encryption keys to encrypt the database. You can use either AWS Key Management Service (AWS KMS) or a hardware security module (HSM) to manage the top-level encryption keys in this hierarchy. The process that Amazon Redshift uses for encryption differs depending on how you manage keys.

- Option D is correct. We can use the hardware security module (HSM) to manage the top-level encryption keys for key management with Amazon Redshift.

Reference:
https://aws.amazon.com/blogs/big-data/encrypt-your-amazon-redshift-loads-with-amazon-s3-and-aws-kms/
https://docs.aws.amazon.com/redshift/latest/mgmt/working-with-db-encryption.html

Question 39Correct

Domain: Design Cost-Optimized Architectures
An EC2 instance in the private subnet needs access to the S3 bucket placed in the same region as that of the EC2 instance. The EC2 instance needs to upload and download bigger files to the S3 bucket frequently.

As an AWS Solutions Architect, what quick and cost-effective solution would you suggest to your customers? You need to consider that the EC2 instances are present in the private subnet, and the customers do not want their data to be exposed over the internet.

- A. Place the S3 bucket in another public subnet of the same region and create a VPC peering connection to this private subnet where the EC2 instance is placed. The traffic to upload and download files will go through secure Amazon's private network.

- B. Create an IAM role having access over the S3 service and assign it to the EC2 instance.

- C. Create a VPC endpoint for S3, use your route tables to control which instances can access resources in Amazon S3 via the endpoint. The traffic to upload and download files will go through the Amazon private network.right
- D. A private subnet can always access S3 bucket/ service through the NAT Gateways or NAT instances, so there is no need for additional setup.

Explanation:

Correct Answer: C

- Option A is incorrect because the S3 service is region-specific, not AZ's specific, and the statement talks about placing the S3 bucket in Public Subnet.
- Option B is incorrect because the VPC endpoint has a policy that controls the use of the endpoint to access Amazon S3 resources. The default policy allows access by any user or service within the VPC, using credentials from any AWS account to any Amazon S3 resource.
- Option C is correct. It can help to access the S3 services in the same region for the EC2 instance. You can create a VPC endpoint and update the route entry of the route table associated with the private subnet. This is a quick solution as well as cost-effective as it will use Amazon's own private network. Hence, it won't expose the data over the internet.
- Option D is incorrect as this is certainly not a default setup unless we create a NAT Gateway or Instance. Even if they are there, it's an expensive solution and exposes the data over the internet.

References:

- https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints-s3.html
- https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints-access.html

Question 40Correct

Domain: Design High-Performing Architectures

You are developing an application using AWS SDK to get objects from AWS S3. The objects have big sizes. Sometimes there are failures when getting objects, especially when the network connectivity is poor. You want to get a specific range of bytes in a single GET request and retrieve the whole object in parts. Which method can achieve this?

- A. Enable multipart upload in the AWS SDK.

- B. Use the "Range" HTTP header in a GET request to download the specified range bytes of an object.right
- C. Reduce the retry requests and enlarge the retry timeouts through AWS SDK when fetching S3 objects.

- D. Retrieve the whole S3 object through a single GET operation.

Explanation:

Correct Answer – B
Through the "Range" header in the HTTP GET request, a specified portion of the objects can be downloaded instead of the whole objects. Check the explanations in https://docs.aws.amazon.com/AmazonS3/latest/dev/GettingObjectsUsingAPIs.html.

- Option A is incorrect: Because the question asks for multipart download rather than multipart upload.
- Option B is CORRECT: Because with byte-range fetches, users can establish concurrent connections to Amazon S3 to fetch different parts from within the same object.
- Option C is incorrect: Because adjusting retry requests and timeouts cannot download specific parts of an object.
- Option D is incorrect: Because the method to retrieve the entire object does not meet the requirement.

Question 41Correct

Domain: Design Resilient Architectures
An application needs to access resources from another AWS account of another VPC in the same region. Which of the following ensure that the resources can be accessed as required?

- A. Establish a NAT instance between both accounts.
- B. Use a VPN between both accounts.
- C. Use a NAT Gateway between both accounts.
- D. Use VPC Peering between both accounts.right

Explanation:

Correct Answer – D

- Options A and C are incorrect because these are used when private resources are required to access the Internet.
- Option B is incorrect because it's used to create a connection between the On-premises and AWS resources.

AWS Documentation mentions the following about VPC Peering:

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them privately. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC Peering connection between your own VPCs, with a VPC in another AWS account, or with a VPC in a different AWS Region.

For more information on VPC Peering, please visit the following URL:

- https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-peering.html

Question 42Correct

Domain: Design High-Performing Architectures

You host a static website in an S3 bucket, and there are global clients from multiple regions. You want to use an AWS service to store cache for frequently accessed content so that the latency is reduced and the data transfer rate increases. Which of the following options would you choose?

- A. Use AWS SDKs to horizontally scale parallel requests to the Amazon S3 service endpoints.
- B. Create multiple Amazon S3 buckets and put Amazon EC2 and S3 in the same AWS Region.
- C. Enable Cross-Region Replication to several AWS Regions to serve customers from different locations.
- D. Configure CloudFront to deliver the content in the S3 bucket.right

Explanation:

Correct Answer – D
CloudFront can store the frequently accessed content as a cache, and the performance is optimized. Other options may help with the performance. However, they do not store cache for the S3 objects.

- Option A is incorrect: This option may increase the throughput. However, it does not store cache.
- Option B is incorrect: Because this option does not use cache.
- Option C is incorrect: This option creates multiple S3 buckets in different regions. It does not improve the performance using cache.
- Option D is CORRECT: Because CloudFront caches copies the S3 files in its edge locations. Users are routed to the edge location that has the lowest latency.

Question 43Correct

Domain: Design Resilient Architectures0
An application consists of the following architecture:

a. EC2 Instances in multiple AZ's behind an ELB

b. EC2 Instances are launched via an Auto Scaling Group.

c. There is one NAT instance to download the updates from the Internet.

What is a bottleneck in the architecture based on the availability?

- A. The EC2 Instances
- B. The ELB
- C. The NAT Instanceright
- D. The Auto Scaling Group

Explanation:

Correct Answer – C
Since there is only one NAT instance, this is a bottleneck in the architecture. For high availability, launch NAT instances in multiple Available Zones and make them part of an Auto Scaling Group.

For more information on NAT Instances, please visit the following URL:

- https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_NAT_Instance.html

Note:
NAT Gateway is a better choice than NAT instance as NAT Gateway is highly available. If you're already using a NAT instance, you can replace it with a NAT gateway.

Question 44Correct

Domain: Define Performant Architectures
A company owns an API deployed in EC2 written using Python. All the requests can be finished within 1 second. Most of traffic happens during the daytime. The company wants to save the API cost and simplify the maintenance of the server without impacting the performance. How can this be achieved?

- A. Use API Gateway with the backend services as it is.
- B. Use the API Gateway along with AWS Lambda.right
- C. Use CloudFront along with the API backend service as it is.
- D. Use ElastiCache along with the API backend service as it is.

Explanation:

Correct Answer – B
Since the company has full ownership of the API, the best solution would be to convert the code for the API and use it in a Lambda function. This can help save on cost since, in the case of Lambda, you only pay for the time the function runs and not for the infrastructure.

Then, you can use the API Gateway along with the AWS Lambda function to scale accordingly.

For more information on using API Gateway with AWS Lambda, please visit the following URL:

https://docs.aws.amazon.com/apigateway/latest/developerguide/getting-started-with-lambda-integration.html

Note: With Lambda, you do not have to provision your own instances. Lambda performs all the administrative activities on your behalf, including capacity provisioning, monitoring fleet health, applying security patches to the underlying compute resources, deploying your code, running a web service front end, and monitoring and logging your code. AWS Lambda provides easy scaling and high availability to your code without additional effort on your part.

Question 45Correct

Domain: Design High-Performing Architectures
You have an application hosted in an Auto Scaling group, and an application load balancer distributes traffic to the ASG. You want to add a scaling policy that keeps the average aggregate CPU utilization of the Auto Scaling group to be 60 percent. The capacity of the Auto Scaling group should increase or decrease based on this target value. Which scaling policy does it belong to?

- A. Target tracking scaling policy.right
- B. Step scaling policy.

- C. Simple scaling policy.

- D. Scheduled scaling policy.

Explanation:

Correct Answer – A
In ASG, you can add a target tracking scaling policy based on a target. For different scaling policies, please check https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scale-based-on-demand.html

- Option A is CORRECT: Because a target tracking scaling policy can be applied to check the ASGAverageCPUUtilization metric according to https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-scaling-target-tracking.html.
- Option B is incorrect: Because Step scaling adjusts the capacity based on step adjustments instead of a target.
- Option C is incorrect: Because Simple scaling changes the capacity based on a single adjustment.
- Option D is incorrect: With Scheduled scaling, the capacity is adjusted based on a schedule rather than a target.

Question 46

Domain: Design High-Performing Architectures
An application sends images to S3. The metadata for these images needs to be saved in persistent storage and is required to be indexed. Which one of the following is the best for the underlying metadata storage?

- A. Amazon Aurora

- B. Amazon S3

- C. Amazon DynamoDBright
- D. Amazon RDSwrong

Explanation:

Correct Answer – C
The most efficient storage mechanism for just storing metadata is Amazon DynamoDB. Amazon DynamoDB is normally used in conjunction with the Simple Storage service. So, after storing the images in S3, you can store their metadata in DynamoDB. You can also create secondary indexes for DynamoDB Tables.

For more information on managing indexes in DynamoDB, please visit the following URL:

https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/SQLtoNoSQL.Indexes.html

Question 47Correct

Domain: Design High-Performing Architectures
An application hosted on EC2 Instances has its promotional campaign due to start in 2 weeks. The performance team performs some analysis based on the historical data and informs you the number of instances that are required for the campaign. You need to make sure that the Auto Scaling group is properly configured with the provided number of instances. What should be done to fulfill this requirement?

- A. Migrate the application from the Auto Scaling group to a Lambda function so that the application scales automatically by AWS.

- B. Configure Scheduled scaling in the Auto Scaling Group.right
- C. Configure a Lambda function that scales up the ASG when the activity starts and scales down when the activity ends.

- D. Configure Static scaling for the Auto Scaling Group.

Explanation:

Correct Answer – B
In the question, the promotional campaign will start in 2 weeks. As you already know how many instances are required, you can configure a scaling schedule in the Auto Scaling group to plan the scaling actions.

Option A is incorrect because it is unsuitable to migrate the application to a Lambda function since the campaign will start in 2 weeks. You can configure an Auto Scaling policy for the campaign.

Option C is incorrect because it is easier to use an Auto Scaling policy to achieve this requirement.

Option D is incorrect because there is no static scaling policy in an Auto Scaling group.

For more information on Scheduled Scaling, please visit the following URLs:

- https://docs.aws.amazon.com/autoscaling/ec2/userguide/schedule_time.html

Question 48Correct

Domain: Design Resilient Architectures
Currently, a company uses EBS snapshots to back up their EBS Volumes. As a part of the business continuity requirement, these snapshots need to be made available in another region. How could this be achieved?

- A. Directly create the snapshot in the other region.

- B. Create Snapshot and copy the snapshot to a new region.right
- C. Copy the snapshot to an S3 bucket and then enable Cross-Region Replication for the bucket.

- D. Copy the EBS Snapshot to an EC2 instance in another region.

Explanation:

Correct Answer - B
AWS Documentation mentions the following:

A snapshot is constrained to the region where it was created. After you create a snapshot of an EBS volume, you can use it to create new volumes in the same region. For more information, follow the link on Restoring an Amazon EBS Volume from a Snapshot below. You can also copy snapshots across regions, making it possible to use multiple regions for geographical expansion, data center migration, and disaster recovery.

For more information on EBS Snapshots, please visit the following URL:

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

For more information on Restoring an Amazon EBS Volume from a Snapshot, please visit the following URL:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-restoring-volume.html
Option C is incorrect because the EBS snapshots are stored in S3, which is managed by AWS. We don't have the option to see the snapshots in S3.

Question 49Correct

Domain: Design High-Performing Architectures
A company has an application hosted in AWS. This application consists of EC2 Instances that sit behind an ELB. The following are the requirements from an administrative perspective:

a) Ensure that notifications are sent when the read requests go beyond 1000 requests per minute.

b) Ensure that notifications are sent when the latency goes beyond 10 seconds.

c) Monitor all AWS API request activities on the AWS resources.

Which of the following can be used to satisfy these requirements? (SELECT TWO)

- A. Use CloudTrail to monitor the API Activity.right
- B. Use CloudWatch Logs to monitor the API Activity.

- C. Use CloudWatch Metrics for the metrics that need to be monitored as per the requirement and set up an alarm activity to send out notifications when the metric reaches the set threshold limit.right
- D. Use custom log software to monitor the latency and read requests to the ELB.

Explanation:

Correct Answer – A and C

- Option A is correct. CloudTrail is a web service that records AWS API calls for all the resources in your AWS account. It also delivers log files to an Amazon S3 bucket. The recorded information includes the identity of the user, the start time of the AWS API call, the source IP address, the request parameters, and the response elements returned by the service.

https://docs.aws.amazon.com/awscloudtrail/latest/APIReference/Welcome.html

- Option B is incorrect because CloudWatch Logs can be used to monitor log files from other services. CloudWatch Logs and CloudWatch are different.

Amazon CloudWatch Logs are used to monitor, store, and access your **log files** from Amazon Elastic Compute Cloud (Amazon EC2) instances, AWS CloudTrail, Route 53, and other sources. CloudWatch Logs reports the data to a CloudWatch metric.
Rather you can monitor **Amazon EC2 API** requests using Amazon CloudWatch.
https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/WhatIsCloudWatchLogs.html

- Option C is correct. Use Cloudwatch Metrics for the metrics that need to be monitored as per the requirement. Set up an alarm activity to send out notifications when the metric reaches the set threshold limit.

https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-cloudwatch-metrics.html

- Option D is incorrect because there is no need to use custom log software as you can set up CloudWatch alarms based on CloudWatch Metrics.

Question 50Correct

Domain: Design Secure Applications and Architectures

A company has resources hosted in its AWS Account. There is a requirement to monitor API activity for all regions and the audit needs to be applied for future regions as well. What would fulfill this requirement?

- A. Ensure CloudTrail trail for each region, then enable trail for each future region.
- B. Ensure one CloudTrail trail is enabled for all regions.right
- C. Create a CloudTrail for each region. Use CloudFormation to enable the trail for all future regions.
- D. Create a CloudTrail for each region. Use AWS Config to enable the trail for all future regions.

Explanation:

Correct Answer – B

AWS Documentation mentions the following:

You can now turn on a trail across all regions for your AWS account. CloudTrail will deliver log files from all regions to the Amazon S3 bucket and an optional CloudWatch Logs log group you specified. Additionally, when AWS launches a new region, CloudTrail will create the same trail in the new region. As a result, you will receive log files containing API activity for the new region without taking any action.

For more information on this feature, please visit the following URL:

https://aws.amazon.com/about-aws/whats-new/2015/12/turn-on-cloudtrail-across-all-regions-and-support-for-multiple-trails/

Question 51

Domain: Design Resilient Architectures

You are part of the IT sector at the finance department of your country. Your organization has implemented AWS Organizations for each internal department, and you have access to the master account. You need to manage Amazon EC2 Dedicated Hosts centrally, and share the host's instance capacity with other AWS accounts in the AWS Organizations. How can you accomplish this in the easiest way?

- A. Use AWS Resource Access Manager to manage the EC2 Dedicated Hosts centrally and share them with other member accounts.right
- B. Use service control policies to share the EC2 Dedicated Hosts in the member accounts.
- C. Use AWS Control Tower.wrong
- D. Create IAM policies with conditions and assign them to users in every member account.

Explanation:

Correct Answer: A

- Option A is CORRECT. With AWS Resource manager, you can share resources with other AWS accounts joined to your AWS Organizations reducing the operational overhead. More details: https://docs.aws.amazon.com/ram/latest/userguide/shareable.html#shareable-ec2.
- Option B is incorrect. SCP is not a service to share resources such as EC2 Dedicated Hosts with other accounts within the AWS Organizations.
- Option C is incorrect. AWS Control Tower is used to do automated deployments in multi-account environments.
- Option D is incorrect. Creating IAM policies is not used to manage and share resources within the AWS Organizations.

Question 52

Domain: Design High-Performing Architectures

Your company has an online game application deployed in an Auto Scaling group. The traffic of the application is predictable. Every Friday, the traffic starts to increase, remains high on weekends and then drops on Monday. You need to plan the scaling actions for the Auto Scaling group. Which method is the most suitable for the scaling policy?

- A. Configure a scheduled CloudWatch event rule to launch/terminate instances at the specified time every week.
- B. Create a predefined target tracking scaling policy based on the average CPU metric and the ASG will scale automatically.
- C. Select the ASG and on the Automatic Scaling tab, add a step scaling policy to automatically scale out/in at fixed time every week.wrong
- D. Configure a scheduled action in the Auto Scaling group by specifying the recurrence, start/end time, capacities, etc.right

Explanation:

Correct Answer – D

The correct scaling policy should be scheduled scaling as it defines your own scaling schedule. Refer to https://docs.aws.amazon.com/autoscaling/ec2/userguide/schedule_time.html for details.

- Option A is incorrect: This option may work. However, you have to configure a target such as a Lambda function to perform the scaling actions.
- Option B is incorrect: The target tracking scaling policy defines a target for the ASG. The scaling actions do not happen based on a schedule.
- Option C is incorrect: The step scaling policy does not configure the ASG to scale at a specified time.
- Option D is CORRECT: With scheduled scaling, users define a schedule for the ASG to scale. This option can meet the requirements.

Question 53

Domain: Design High-Performing Architectures

There is an application that consists of frontend and backend EC2 Instances behind classic ELBs. The database is deployed in AWS RDS. The application might not be able to scale properly.

What should be used to scale the application appropriately? (SELECT TWO.)

- A. Use Auto Scaling for the frontend EC2 instances.right
- B. Use Auto Scaling for the backend EC2 instances.right
- C. Replace the Classic ELB with Application ELB.

- D. Use Network ELB for both the frontend and backend instances.wrong

Explanation:

Correct Answer – A and B

When you see a requirement for scaling, consider the Auto Scaling service provided by AWS. This can be used to scale both the frontend and backend instances.

For more information on Auto Scaling, please visit the following URL:

- https://docs.aws.amazon.com/autoscaling/plans/userguide/what-is-aws-auto-scaling.html

Question 54

Domain: Design Resilient Architectures

There is a multi-region website hosted in AWS EC2 under an ELB. Route 53 is used to manage its DNS record. The website might get a lot of traffic over the next couple of weeks. If the application experiences a natural disaster in the region during the time, what should be used to reduce potential disruption to users?

- A. Use an ELB to divert traffic to an Infrastructure hosted in another region.

- B. Use an ELB to divert traffic to an Infrastructure hosted in another AZ.

- C. Use CloudFormation to create backup resources in another AZ.

- D. Use Route53 to route requests to another instance in a different regionright

Explanation:

Correct Answer – D

In a disaster recovery scenario, the best choice out of all given options is to divert the traffic to a static website.

- Option A is wrong because ELB can only balance traffic in one region, not across multiple regions.

- Options B and C are incorrect because using backups across AZs is not enough for disaster recovery purposes.

For more information on disaster recovery in AWS, please visit the following URLs:

- https://aws.amazon.com/premiumsupport/knowledge-center/fail-over-s3-r53/
- https://aws.amazon.com/disaster-recovery/
- The wording "to reduce the potential disruption in case of issues" points to a disaster recovery situation. There is more than one way to manage this situation. However, we need to choose the best option from the list given here. Out of this, the most suitable one is Option D.

Most organizations try to implement High Availability (HA) instead of DR to guard them against any downtime of services. In the case of HA, we ensure that there exists a fallback mechanism for our

services. The service that runs in HA is handled by hosts running in different availability zones but the same geographical region. However, this approach does not guarantee that our business will be up and running in case the entire region goes down.

DR takes things to a completely new level, wherein you need to recover from a different region that is separated by over 250 miles. Our DR implementation is an Active/Passive model, meaning that we always have minimum critical services running in different regions. But a major part of the infrastructure is launched and restored when required.

For more information on large scale disaster recovery using AWS regions, please visit the following URL:

- https://aws.amazon.com/blogs/startups/large-scale-disaster-recovery-using-aws-regions/

Note:
Usually, when we discuss a disaster recovery scenario, we assume that the entire region is affected due to some disaster. So we need the service to be provided from yet another region. So, setting up a solution in another AZ will not work as it is in the same region. Option A is incorrect though it mentions yet another region because ELBs cannot span across regions.
So out of the options provided, Option D is the most suitable solution.

Question 55

Domain: Define Operationally-Excellent Architectures
You have a requirement to host a static website for a domain named mycompany.com in AWS.

Which of the listed steps will you follow in order to set this up? (SELECT TWO.)

- A. Host the static site on an EC2 Instance.
- B. Use Route53 with static web site in S3.right
- C. Use Route53 as the domain registrar to register the domain name.right
- D. Place the EC2 instance behind the ELB.wrong

Explanation:

Correct Answer – B and C
You can register the domain name in your domain registrar (Route53) and then configure a record set in Route53 to host the static website in S3.

For more information on website hosting in S3, please visit the following URLs:

- https://docs.aws.amazon.com/AmazonS3/latest/dev/WebsiteHosting.html
- https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/RoutingToS3Bucket.html

Question 56

Domain: Design High-Performing Architectures
A database, hosted using the Amazon RDS service, is getting many database queries. It has now become a bottleneck for the associating application. Which action would ensure that the database is not a performance bottleneck?

- A. Setup a CloudFront distribution in front of the database.
- B. Setup an ELB in front of the database.
- C. Setup ElastiCache in front of the database.right
- D. Setup SNS in front of the database.wrong

Explanation:

Correct Answer – C
ElastiCache is an in-memory solution that can be used in front of a database to cache the common queries issued against the database. This can reduce the overall load on the database.

- Option A is incorrect because this is normally used for content distribution.
- Option B is partially correct. But you need to have one more database as an internal load balancing solution.
- Option D is incorrect because SNS is a simple notification service.

For more information on ElastiCache, please visit the following URL:

https://aws.amazon.com/elasticache/

Question 57

Domain: Design Resilient Architectures
A database is being hosted using the Amazon RDS service. This database will be deployed in production and needs to be highly available. Which of the following could be used to achieve this requirement?

- A. Use Multi-AZ for the RDS instance to ensure that a secondary database is created in another region.
- B. Use the Read Replica feature to create another instance of the DB in another region.wrong
- C. Use Multi-AZ for the RDS instance to ensure that a secondary database is created in another Availability Zone.right
- D. Use the Read Replica feature to create another instance of the DB in another Availability Zone.

Explanation:

Correct Answer - C
Option A is incorrect because the Multi-AZ feature allows high availability across Availability Zones, not regions.

Options B and D are incorrect because Read Replicas can be used to offload database reads. But if you want high availability, the Multi-AZ feature is required.

AWS Documentation mentions the following:

Amazon RDS Multi-AZ deployments provide enhanced availability and durability for Database (DB) Instances. When you provision a Multi-AZ DB Instance, Amazon RDS automatically creates a primary DB Instance and synchronously replicates the data to a standby instance in a different Availability Zone (AZ).
For more information on AWS RDS Multi-AZ, please visit the following URL:

https://aws.amazon.com/rds/details/multi-az/

Question 58 Incorrect

Domain: Design Secure Applications and Architectures

A company wants to host a web application and a database layer in AWS. This will be done with the use of subnets in a VPC.

What would be a proper architectural design for supporting the required tiers of the application?

- A. Use a public subnet for the web tier and another public subnet for the database layer.
- B. Use a public subnet for the web tier and a private subnet for the database layer. right
- C. Use a private subnet for the web tier and another private subnet for the database layer. wrong
- D. Use a private subnet for the web tier and a public subnet for the database layer.

Explanation:

Correct Answer – B

The ideal setup is to ensure that the webserver is hosted in the public subnet so that users on the internet can access it. The database server can be hosted in the private subnet.

The below diagram shows how this can be set up:

For more information on public and private subnets in AWS, please visit the following URL:

https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2.html

Question 59

Domain: Design Resilient Architectures

You need to launch several EC2 instances to run Cassandra. There are large distributed and replicated workloads in Cassandra and you plan to launch instances using EC2 placement groups. The traffic should be distributed evenly across several partitions and each partition should contain multiple instances. Which strategy would you use when launching the placement groups?

- A. Cluster placement strategy.
- B. Spread placement strategy.
- C. Partition placement strategy. right
- D. Network placement strategy. wrong

Explanation:

Correct Answer – C

Placement groups have the placement strategies of Cluster, Partition and Spread. With the Partition placement strategy, instances in one partition do not share the underlying hardware with other partitions. This strategy is suitable for distributed and replicated workloads such as Cassandra. For

details, please refer to https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html#placement-groups-limitations-partition.

- Option A is incorrect. Cluster placement strategy puts instances together in an availability zone. This does not resolve the problem mentioned in the question.
- Option B is incorrect. Because Spread placement strategy puts instances across different racks. It does not group instances in a partition.
- Option C is CORRECT: With the Partition placement strategy, instances in a partition have their own set of racks.
- Option D is incorrect: Because there is no Network placement strategy.

Question 60

Domain: Design Resilient Architectures

A company has an infrastructure that consists of machines that send log information every 5 minutes. The number of these machines can run into thousands. It is required to ensure that the analysis of every log item is completed within 24 hours. What could help to fulfill this requirement?

- A. Use Kinesis Data Streams to collect the logs and persist the data to S3 using Kinesis Firehose and Lambda.right
- B. Launch an Elastic Beanstalk application to take the processing job of the logs.
- C. Launch an EC2 instance with enough EBS volumes to consume the logs which can be used for further processing.
- D. Use CloudTrail to store all the logs which can be analyzed at a later stage.wrong

Explanation:

Correct Answer – A

AWS Documentation mentions the following:

Amazon Kinesis Data Streams (KDS) is a massively scalable and durable real-time data streaming service. KDS can continuously capture gigabytes of data per second from thousands of sources such as website clickstreams, database event streams, financial transactions, social media feeds, IT logs, and location-tracking events.

Make your streaming data available to multiple real-time analytics applications, to Amazon S3 or AWS Lambda within 70 milliseconds of the data being collected.
For more information on Amazon Kinesis firehose, please visit the following URL:

- https://aws.amazon.com/kinesis/data-streams/

Question 61

Domain: Define Operationally-Excellent Architectures

An application hosted in AWS allows users to upload videos to an S3 bucket. A user is required to be given access to upload some videos for a week based on the profile. How could this be accomplished in the best way possible?

- A. Create an IAM bucket policy to provide access for one week.

- B. Create a pre-signed URL for each profile which will last for one week.right
- C. Create an S3 bucket policy to provide access for one week.wrong
- D. Create an IAM role to provide access for one week.

Explanation:

Correct Answer – B
Pre-signed URLs are the perfect solution when you want to give temporary access to users for S3 buckets. So, whenever a new profile is created, you can create a pre-signed URL to ensure that the URL lasts for a week and allows users to upload the required objects.

For more information on pre-signed URLs, please visit the following URL:

https://docs.aws.amazon.com/AmazonS3/latest/dev/PresignedUrlUploadObject.html
For Choice D, the maximum time you can set for IAM Role Session is 12 hours. So this doesn't satisfy the 1-week requirement.

Ref: https://docs.aws.amazon.com/singlesignon/latest/userguide/howtosessionduration.html

Question 62

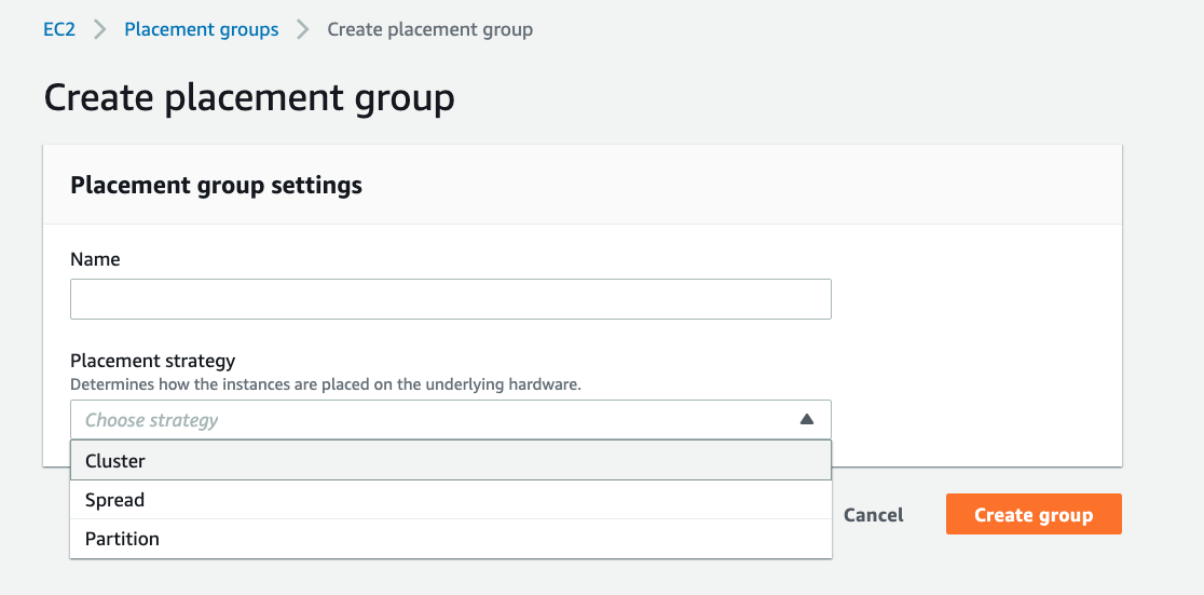
Domain: Design Resilient Architectures
You are creating several EC2 instances for a new application. The instances need to communicate with each other. For a better performance of the application, both low network latency and high network throughput are required for the EC2 instances. All instances should be launched in a single availability zone. How would you configure this?

- A. Launch all EC2 instances in a placement group using a Cluster placement strategy.right
- B. Auto assign a public IP when launching the EC2 instances.
- C. Launch EC2 instances in an EC2 placement group and select the Spread placement strategy.wrong
- D. When launching the EC2 instances, select an instance type that supports enhanced networking.

Explanation:

Correct Answer – A
The Cluster placement strategy helps to achieve a low-latency and high throughput network. The reference is in https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html#placement-groups-limitations-partition.

- Option A is CORRECT: The Cluster placement strategy can improve the network performance among EC2 instances. The strategy can be selected when creating a placement group.



- Option B is incorrect: Because the public IP cannot improve the network performance.
- Option C is incorrect: The Spread placement strategy is recommended when several critical instances should be kept separate from each other. This strategy should not be used in this scenario.
- Option D is incorrect: The description in the option is inaccurate. The correct method is creating a placement group with a suitable placement strategy.

Question 63

Domain: Design High-Performing Architectures0

To improve the network performance, you launch a C5 EC2 Amazon Linux instance and enable Enhanced Networking by modifying the instance attribute with “aws ec2 modify-instance-attribute --instance-id instance_id --ena-support”. Which mechanism does the EC2 instance use to enhance the networking capabilities?

- A. Intel 82599 Virtual Function (VF) interface.
- B. Transit Virtual Interface
- C. Elastic Network Adapter (ENA).right
- D. Elastic Network Interface (ENI).

Explanation:

Correct Answer – C

Enhanced networking has two mechanisms: Elastic Network Adapter (ENA) and Intel 82599 Virtual Function (VF) interface. For ENA, users can enable it with --ena-support.

An EFA is an Elastic Network Adapter (ENA) with added capabilities. It provides all of the functionality of an ENA, with additional OS-bypass functionality. OS-bypass is an access model that allows HPC and machine learning applications to communicate directly with the network interface hardware to provide low-latency, reliable transport functionality."

- Option A is incorrect: Because the option of "--ena-support" is not used by Intel 82599 Virtual Function (VF) interface.
- Option B is incorrect: Because a Transit Virtual Interface is used to connect resources hosted in an Amazon VPC (using their private IP addresses) through a transit gateway, not suitable for the above scenario.
  https://aws.amazon.com/premiumsupport/knowledge-center/public-private-interface-dx/
- Option C is CORRECT: In Amazon Linux, users can enable the enhanced networking attribute with the AWS CLI command mentioned in the question.
- Option D is incorrect: In this scenario, the mechanism used for enhanced networking should be Elastic Network Adapter (ENA) instead of Elastic Network Interface (ENI).

References:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enhanced-networking-ena.html.

Question 64

Domain: Design Secure Applications and Architectures0
A company hosts 5 web servers in AWS. They want to ensure that multiple values for a DNS query should be returned and traffic routed to multiple IP addresses. In addition, you want to associate your routing records with a Route 53 health check. Which routing policy should be used to fulfill this requirement?

- A. Simple
- B. Weighted
- C. Multivalue Answer right
- D. Latencywrong

Explanation:

Correct Answer - C
The AWS Documentation mentions the following to support this:

If you want to route traffic randomly to multiple resources such as web servers, you can create one multivalue answer record for each resource and, optionally, associate an Amazon Route 53 health check with each record.

For example, suppose you manage an HTTP web service with a dozen web servers where each has its own IP address. No web server could handle all the traffic. But if you create a dozen multivalue answer records, Amazon Route 53 responds to DNS queries with up to eight healthy records in response to each DNS query. Amazon Route53 gives different answers to different DNS resolvers. If a web server becomes unavailable after a resolver cache a response, client software can try another IP address in the response.

- Simple routing policy – Use a single resource that performs a given function for your domain, such as a web server that serves the example.com website.
- Latency routing policy – Use when you have resources in multiple locations, and you want to route traffic to the resource that provides the best latency.
- Weighted routing policy – Use to route traffic to multiple resources in proportions that you specify.
- Multivalue answer routing policy – Use when you want Route53 to respond to DNS queries with up to eight healthy records selected randomly.

For more information on different routing policies, please visit the following URL:

- https://aws.amazon.com/premiumsupport/knowledge-center/multivalue-versus-simple-policies

- https://aws.amazon.com/about-aws/whats-new/2017/06/amazon-route-53-announces-support-for-multivalue-answers-in-response-to-dns-queries/

Question 65

Domain: Design High-Performing Architectures

You are working as AWS Solutions Architect for a large banking organization. The requirement is that under normal business hours, there would always be at least 24 web servers up and running in a region (example: US - West (Oregon)). It will be a three-tier architecture connecting to the databases. The solution offered should be highly available, secure, and cost-effective. It should respond to the heavy requests during peak hours and fault-tolerate up to one AZ failure.

What would be the best solution to meet this requirement?

- A. In a given region, use ELB behind two different AZs, each AZ with minimum or desired 24 web servers hosted in a public subnet and Multi-AZ database architecture in a private subnet.

- B. In a given region, use ELB behind three different AZs, each AZ having ASG, with minimum or desired 12 web servers hosted in a public subnet and Multi-AZ database architecture in a private subnet.right
- C. In a given region, use ELB behind two different AZs, each AZ having ASG, with minimum or desired 12 web servers hosted in a public subnet and Multi-AZ database architecture in a private subnet.

- D. In a given region, use ELB behind three different AZs, each AZ having ASG, with minimum or desired 8 web servers hosted in public subnet and Multi-AZ database architecture in a different public subnet.wrong

Explanation:

Correct Answer: B

- Option A is incorrect. Everything looks good, but the designed architecture does not look cost-effective, as all the time 48 servers will be running. It does not have ASG to cater to additional load on servers. However, it is fault-tolerant to one AZ failure.

Besides, it is always a good practice to use multiple AZs to make the application highly available.

- Option B is correct. The solution needs to be tolerant up to one AZ failure. It means there are always 36 web servers to cater to the service requests. If one AZ fails, then there will be 24 servers running all the time. In case two AZs fails, there will be 12 servers running. Also, ASG can be utilized to scale out the required number of servers.
- Option C is incorrect. It will not be a suitable solution. If there is one AZ failure, the other AZ will have only 12 web servers running. The question requires at least 24 web servers are running at all times.
- Option D is incorrect. Remember the design principle of keeping the databases in the private subnet. As this solution mentions placing databases in another public subnet, the data can be exposed over the internet, and hence it's an insecure application.