Question 1

You are working in a Global Pharma firm, having its Head Office in Washington & Branch offices in Chicago & Paris. The Firm has a two-tier Intranet website deployed in US-East-1 Region & database servers deployed on-premise at the Head office. The Head Office has a Direct Connect link to VPC, and it is connected to Chicago & Paris offices via WAN links, while each of these offices has separate internet links from the local ISP. Recently they faced link outage issues with WAN links that resulted in the isolation of the branch offices from the head office. They are looking for a cost-effective backup solution that could be set-up quickly without any additional devices and links. What would be the most suitable connectivity option in this scenario?

- A. With existing Internet connections in Washington, Chicago, and Paris, set up a Direct Connection with us-east-1 VGW advertising prefixes via BGP. BGP ASN should be unique at these locations. VGW at us-east-1 will re-advertise these prefixes to the Washington office.

- B. With existing Internet connection in Chicago and Paris, set up a VPN connection with us-east-1 VGW advertising prefixes via BGP. BGP ASN should be unique at these locations. VGW at us-east-1 will re-advertise these prefixes to the Washington office.right
- C. With existing Internet connection in Chicago and Paris, set up a VPN connection between us-west-1 and eu-west-3 regions.

- D. With existing Internet connections in Chicago and Paris, set up VPC peering connections from the branch offices to the VPC in the head office.

Explanation:

Correct Answer – B

This question is about cloud networking and how to build resilient architectures along with some constraints mentioned in the description e.g. cost-effectiveness.

The key is understanding networking concepts and VPC connectivity options. The question says that the Head Office in Washington has a Direct Connect link to a VPC and also has on-premise database servers. There are two separate ISPs with their own internet links in each branch office in Chicago and Paris. These two offices use WAN links to connect back to the Head Office in Washington.

The question is about availability between the Head Office and the two branches i.e. what infrastructure is useful to prevent WAN link outages between the Head Office and branches. There is only one VPC in one Region mentioned in the question which is currently on the Head Office in Washington and the other branches seem not be using VPCs at all. Thus, this is related to AWS Direct Connect Resiliency recommendations or the use of AWS-managed VPN options in place.

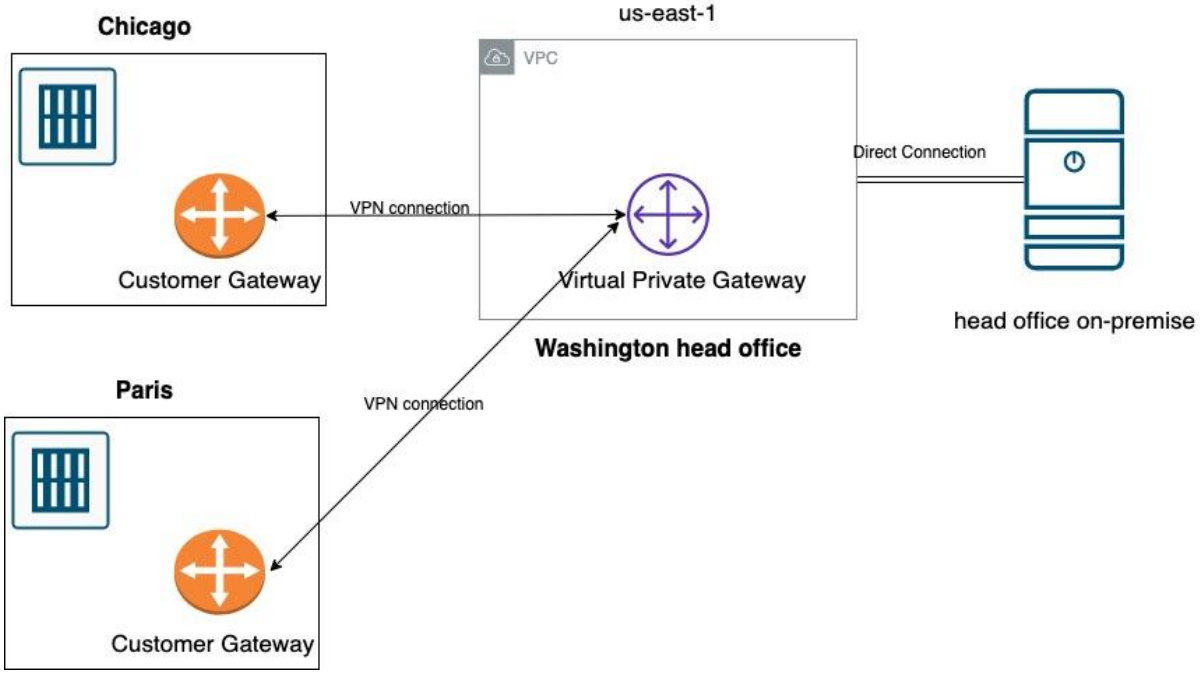
Option A is incorrect as there is no need to set up Direct Connection in us-east-1 because it already exists in this Region. This solution does not describe a high or maximum resiliency topology for availability in critical workloads. The problem is still about connectivity solutions between the Head Office in Washington and the two branches in Chicago and Paris.

Option B is CORRECT because a VPN connection is suitable to establish the communications between the branch offices and the Head Office VPC while keeping in mind cost-effectiveness constraints.

Option C is incorrect because even though it uses an AWS managed VPN option, someone might assume that Chicago is close to us-west-1 Region in N. California (which is obviously not) and Paris is the eu-west-3 Region, Head Office in Washington is the real connectivity problem described in the question. This answer doesn't even make sense in this context.

Option D is incorrect as VPC peering connection is used for private traffic between two VPCs via networking connection relying on the same VPC infrastructure. In this question, the branch offices in Chicago and Paris do not even use VPCs. Otherwise, the question itself would not make sense.

Please check the following **diagram**:



References:

- VPC_VPN

- directconnect_faqs
- directconnect_resiliency-recommendation
- whitepaper_network-to-amazon-vpc-connectivity-options
- directconnect_virtualgateways
- vpc-peering

Question 2

You have a lifecycle rule for an S3 bucket that archives objects to the S3 Glacier storage class 60 days after creation. The archived objects are no longer needed one year after being created. How would you configure the S3 bucket to save more cost?

- A. Configure a rule in S3 Glacier to place delete markers for objects that are one year old.

- B. Configure the S3 lifecycle rule to expire the objects after 365 days from object creation.right
- C. Modify the S3 lifecycle rule to clean up expired object delete markers for one year old objects.

- D. Modify the S3 lifecycle rule to use S3 Glacier Deep Archive which automatically deletes objects one year after creation.

Explanation:

Correct Answer – B

Users can configure the expiration actions in S3 lifecycle management. Details can be found in https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html.

- Option A is incorrect: Because users cannot configure a rule to place delete markers in S3 Glacier.
- Option B is CORRECT: Because users can configure the object expiration in the S3 life cycle, Amazon S3 will remove the expired objects.
- Option C is incorrect: Because cleaning up expired object delete markers does not expire the objects. This action does not save costs.
- Option D is incorrect: Because S3 Glacier Deep Archive does not automatically delete objects.

Question 3

An application currently allows users to upload files to an S3 bucket. You want to ensure that the file name for each uploaded file is stored in a DynamoDB table. How could this be achieved? (SELECT TWO)

- A. Create an AWS Lambda function to insert the required entry for each uploaded file.right
- B. Use AWS CloudWatch to probe for any S3 event.

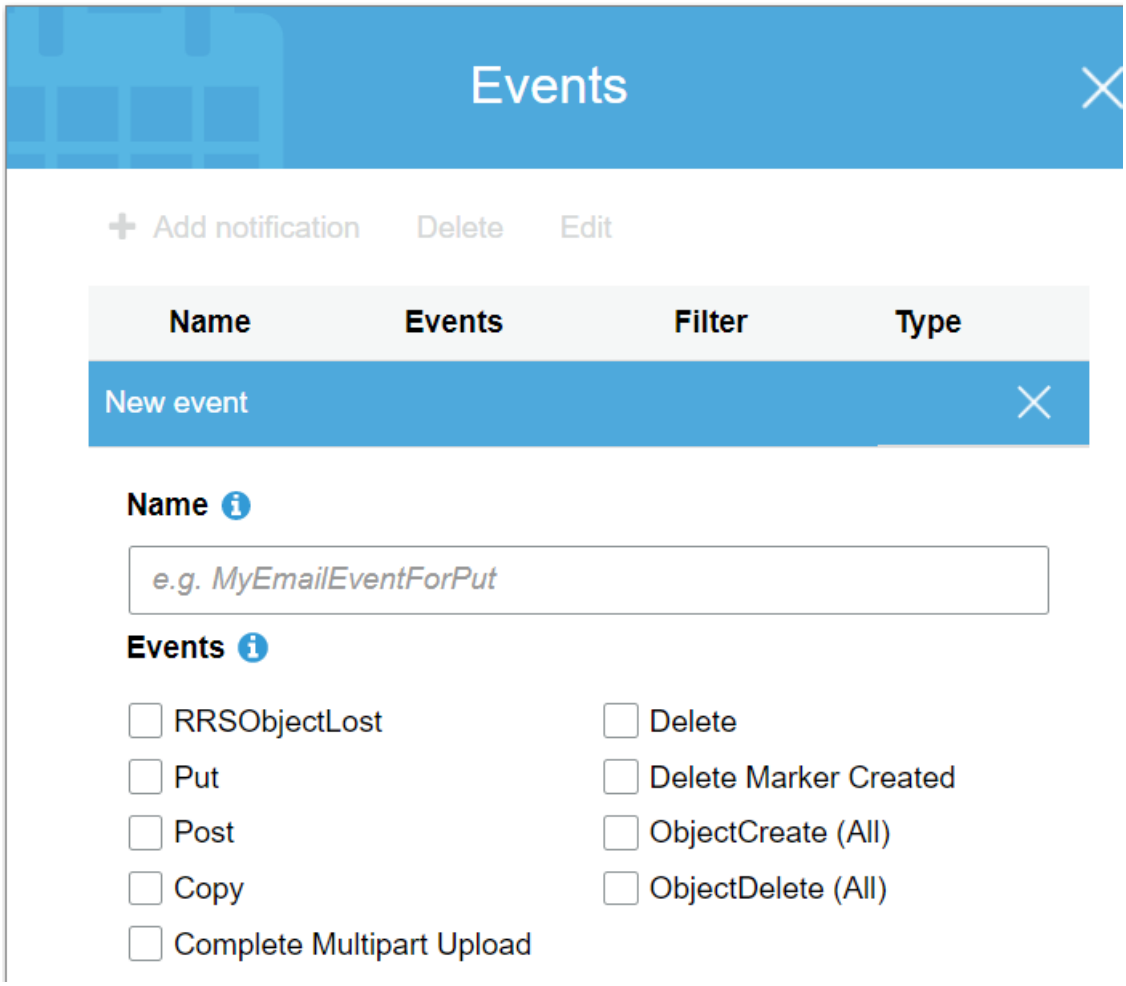
- C. Add an event in S3 with notification send to Lambda.right
- D. Add the CloudWatch event to the DynamoDB table streams section.

Explanation:

Correct Answers – A and C

You can create a Lambda function containing the code to process the file and add the file's name to the DynamoDB table.

You can then use an Event Notification from the S3 bucket to invoke the Lambda function whenever the file is uploaded.



For more information on Amazon S3 Event Notifications, please visit the following URL-

- https://docs.aws.amazon.com/AmazonS3/latest/dev/NotificationHowTo.html

Question 4

A famous mobile brand is launching its much-awaited mobile phone on Christmas weekend. The company's web applications are deployed in multiple regions and expecting a huge increase in traffic. They want to prioritize their Platinum customers in us-east-1 over new global customers to select various models of new mobile. The IT Team wants the infrastructure to handle huge amounts of traffic without any impact

on latency to global users. Which of the following cost-effective design solutions will meet this requirement?

- A. Create a Lambda@Edge function in all regions to segregate Platinum users along with Amazon CloudFront to cache content nearer to users in all regions.

- B. Create a Lambda@Edge function in the US-East-1 region to segregate Platinum users & execute at all regions along with Amazon CloudFront to cache content nearer to users in all regions.right
- C. Use Auto-scaling for origin servers to scale dynamically along with creating separate distribution for Platinum users with Amazon CloudFront to cache content nearer to users in all regions.

- D. Use Auto-scaling for origin servers to scale on a predefined schedule along with creating separate distribution for Platinum Users with Amazon CloudFront to cache content nearer to users in all regions.

Explanation:

Correct Answer – B
Lambda@Edge can be a scalable solution to segregate different types of users accessing web applications. Amazon CloudFront can be used to cache web content from the origin server to provide users with low latency access.

- Option A is incorrect as Lambda@Edge needs not be created in all regions. It needs to be created in the US-East-1 region & replicated to all regions.
- Option C is incorrect as using On-Demand Auto-scaling with separate distributions will incur additional cost & is not a scalable option.
- Option D is incorrect as using Schedule Auto-scaling with separate distributions will incur additional cost & is not a scalable option.

For more information using Lambda@Edge with Amazon CloudFront, refer to the following URL-

- https://aws.amazon.com/blogs/networking-and-content-delivery/visitor-prioritization-on-e-commerce-websites-with-cloudfront-and-lambdaedge/

Question 5

You are working for a global software firm having offices in various continents. The pre-sales team needs to provide a new application demo to a prospective customer. For this, they are looking urgently for a separate temporary connection between 3 on-premises regional offices at Sydney, London, and Tokyo & Demo VPC at the us-west-1 region.

You are planning to set up a VPN CloudHub in VGW (Virtual Private Gateway) at us-west-1 for the other three on-premise sites to connect. What are the factors required to meet this connectivity solution? (SELECT TWO)

- A. VGW at us-west-1 should be enabled to advertise IP prefixes of each regional office to other regional offices.

- B. Non-overlapping IP address pool should be configured at each of the regional offices.right
- C. Each router should have a BGP (Border Gateway Protocol) peering with other routers at each regional office over VPN connection.

- D. BGP (Border Gateway Protocol) ASN (Autonomous System Number) should be unique at these regional offices.right
- E. Each of these offices should set up VPN connection to VGW only in that specific region instead of to VGW at us-west-1.

Explanation:

Correct Answers – B, D

AWS VPN CloudHub provides connectivity between spoke location over VPN connection. In this case, VGW acts as a Hub & re-advertise prefixes received from one regional office to another regional office. For this connectivity to establish, each regional site should have non-overlapping IP prefixes & BGP ASN unique at each site. If BGP ASN is not unique, additional ALLOWS-IN will be required.

- Option A is incorrect as VGW by default acts as a Hub and spoke & no additional configuration needs to be done at the VGW end.

- Option C is incorrect as the router needs to have BGP peering only with VGW & not with routers in other locations.

- Option E is incorrect as a regional office can set up a VPN connection to VGW of the different regions.

For more information on using AWS VPN CloudHub, refer to the following URL-

- https://docs.aws.amazon.com/vpn/latest/s2svpn/VPN_CloudHub.html

Question 6

A hybrid architecture is used for a popular blogging website. Application servers are spread between On-premise Data Centre & EC2 Instance deployed in a custom VPC. An Application Load Balancer is used to offload traffic to the cloud due to capacity constraints at Data Centre. From Traffic trends, it is observed that the first week of every month, when new blogs are uploaded, a spike in traffic is observed. They are looking for an automated faster option to mitigate additional load on EC2 servers launched behind ALB for this period. Which of the following options can be implemented to meet this requirement?

- A. Use Auto-Scaling OnDemand Scaling to add additional EC2 instances on a VPC different from the VPC in which the ALB is located.

- B. Use Auto-Scaling Scheduled Scaling to add additional EC2 instances on a VPC different from the VPC in which the ALB is located.

- C. Use Auto-Scaling Scheduled Scaling to add additional EC2 instances within the same VPC as the ALB.right
- D. Use Auto-Scaling OnDemand Scaling to add additional EC2 instances within the same VPC as the ALB.

Explanation:

Correct Answer – C

Autoscaling provides an automated way to scale EC2 instances as per capacity requirements. For using ELB with Autoscaling group, both should be in the same region & launched in the same VPC. EC2 Auto-Scaling Scheduled Scaling allows you to set your own scaling schedule with a Cron expression that specifies when to act.

- Option A & B are incorrect as ELB & EC2 instances launched should be in the same VPC.
- Option D is incorrect as for the above case, Scheduled Scaling is a better option than OnDemand scaling.

For more information on using Auto-Scaling with ELB, refer to the following URLs-

- https://docs.aws.amazon.com/autoscaling/ec2/userguide/scaling_plan.html
- https://docs.aws.amazon.com/autoscaling/ec2/userguide/autoscaling-load-balancer.html

Question 7

You are working for an electrical appliance company that has a web-application hosted in AWS. This is a two-tier web application with web-servers hosted in VPC's & on-premise data-center. You are using a Network Load balancer in the front end to distribute traffic between these servers. You are using instance Id for configuring targets for Network Load Balancer. Some clients are complaining about the delay in accessing this website.

To troubleshoot this issue, you are looking for a list of Client IP address having longer TLS handshake time. You have enabled access logging on Network Load balancing with logs saved in Amazon S3 buckets. Which tool could be used to quickly analyze many log files without any visualization in a cost-effective way?

- A. Use Amazon Athena to query logs saved in Amazon S3 buckets.right
- B. Use Amazon S3 console to process logs.

- C. Export Network Load Balancer access logs to third-party application.

- D. Use Amazon Athena along with Amazon QuickSight to query logs saved in Amazon S3 buckets.

Explanation:

Correct Answer – A
Amazon Athena is a suitable tool for querying Network Load Balancers logs. In the above case, since a large amount of logs are saved in S3 buckets from the Network load balancer, Amazon Athena can be used to query logs and generate required details of client IP address and TLS handshake time.

- Option B is incorrect as processing many logs directly from the S3 console will be a time-consuming process.
- Option C is incorrect as using a third-party tool will not be a cost-effective solution.
- Option D is incorrect as in the above case, we require only details of Client IP details along with TLS handshake time for troubleshooting purposes. Amazon QuickSight will be useful in case you need data visualization.

For more information on using Amazon Athena to query Network Load Balancer logs, refer to the following URL-

- https://docs.aws.amazon.com/athena/latest/ug/networkloadbalancer-classic-logs.html

Question 8

You are requested to guide a large Pharma company. They are looking for a solution to save all their R&D test analysis data securely. Daily large numbers of reports are generated; this data would be accessed from multiple R&D centers spread across the globe. The company requires this data to be instantaneously available to all users. Which of the following is the most suitable way for AWS storage to provide low latency access to users across the globe with the least cost?

- A. Use Amazon EC2 instance with instance store to store data.
- B. Use Amazon EFS volumes to store data.
- C. Use Amazon EBS volumes connected to the EC2 instance to store data
- D. Use Amazon S3 Standard storage class from Amazon S3 to store data.right

Explanation:

Correct Answer – D
S3 Standard offers high durability, availability, and performance object storage for frequently accessed data. Because it delivers low latency and high throughput, S3 Standard is appropriate for a wide variety of use cases, including cloud applications,

dynamic websites, content distribution, mobile and gaming applications, and big data analytics.

- Option A is incorrect as the Instance store will provide low latency access from EC2 instances, but it's a temporary storage option.
- Option B is incorrect. Since this data would be accessed globally, Amazon EFS will not be ideal for this requirement.
- Option C is incorrect as Amazon EBS volumes would be useful storage for single Amazon EC2 instances.

For more information on AWS Storage options, refer to the following URLs-

- https://aws.amazon.com/s3/storage-classes/
- https://docs.aws.amazon.com/efs/latest/ug/storage-classes.html

Question 9

A financial firm, which has a web server in an EC2 Instance, is developing a new web application with static informational content and dynamic functional content with server-side scripting. They expect heavy traffic on the launch of the application. The dynamic content should be stored as files in a file system. The storage of static content should be highly available and cost-effective. Which of the following solutions is the most suitable?

- A. Use Amazon EFS for dynamic content & Amazon S3 for static content.right
- B. Use Amazon EBS for dynamic content & Amazon EFS for static content.
- C. Use Amazon S3 for dynamic content & Amazon EBS for static content.
- D. Use Amazon Instance Store for dynamic content & Amazon S3 for static content

Explanation:

Correct Answer – A

For websites with dynamic user interactions, using Amazon EFS is an ideal option to use along with using Amazon S3 for static non-changing data. EFS provides a scalable, distributed file system solution where dynamic content can be stored and scaled elastically allowing parallel access from EC2 instances while S3 is best suited for storing & serving static content using a CloudFront distribution

- Option B is incorrect as EBS is for block storage, not suitable for storing dynamic content.
- Option C is incorrect as Amazon S3 cannot be used for dynamic content. Amazon EC2 or EFS can be used.
- Option D is incorrect as Amazon Instance Store is temporary storage and is not suited for dynamic web content.

For more information on AWS Storage Options, refer to the following URLs-

- https://aws.amazon.com/products/storage/

Question 10

You are working for a global financial company. Company locations spread across various countries upload transaction details data to the S3 bucket in the US-West region. A large amount of data is uploaded daily from each of these locations simultaneously. You are using Amazon Athena to query this data & create reports using Amazon QuickSight to create a daily dashboard for the management team. In some cases, while running queries, you are observing Amazon S3 exception errors.

Also, in the monthly bills, a high percentage of cost is associated with Amazon Athena. Which of the following could help eliminate S3 errors while querying data and reducing the cost associated with queries? (SELECT TWO)

- A. Partition data based upon user credentials

- B. Partition data based upon date & location.right
- C. Create a separate Workgroups based upon user groups.right
- D. Create a single Workgroup for all users.

Explanation:

Correct Answers – B and C

AWS Athena pricing is based upon per query and the amount of data scanned in each query. In the above case, each regional office is uploading a large amount of data simultaneously. This data needs to be partitioned based upon location & date. A separate Workgroup can be created based upon users, teams, applications or workloads. This will minimize the amount of data scanned for each query, improve performance & reducing cost.

- Option A is incorrect as partitioning the data on user credentials is irrelevant here.

- Option D is incorrect as a single Workgroup will not decrease the amount of data scanned per query.

For more information on Partitioning data & using Workgroups, refer to the following URLs-

- https://docs.aws.amazon.com/athena/latest/ug/partitions.html
- https://docs.aws.amazon.com/athena/latest/ug/manage-queries-control-costs-with-workgroups.html

Question 11

You are planning to use Auto Scaling groups to maintain the performance of your web application. How would you ensure that the scaling activity has sufficient time to stabilize without executing another scaling action?

- A. Modify the Instance User Data property with a timeout interval.

- B. Increase the Auto Scaling Cooldown timer value.right
- C. Enable the Auto Scaling cross zone balancing feature.

- D. Disable CloudWatch alarms till the application stabilizes.

Explanation:

Correct Answer – B
AWS Documentation mentions the following.

The Cooldown period is a configurable setting for your Auto Scaling group, ensuring that it doesn't launch or terminate additional instances before the previous scaling activity takes effect. After the Auto Scaling group dynamically scales using a simple Scaling Policy, it waits for the Cooldown period to complete before resuming scaling activities.

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

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

Question 12

A company hosts a popular web application that connects to an Amazon RDS MySQL DB instance running in a private VPC subnet created with default ACL settings. The IT Security department has identified a DoS attack from a suspecting IP. How would you protect the subnets from this attack?

- A. Change the Inbound Security Groups to deny access from the suspecting IP.

- B. Change the Outbound Security Groups to deny access from the suspecting IP.

- C. Change the Inbound NACL to deny access from the suspecting IP.right
- D. Change the Outbound NACL to deny access from the suspecting IP.

Explanation:

Correct Answer – C
Options A and B are incorrect because the Security Groups block traffic by default. You can use NACLs as an additional security layer for the subnet to deny traffic.
Option D is incorrect since just changing the Inbound Rules is sufficient.
The following are the characteristics of security groups:
You can specify allow rules, but not deny rules.
You can specify separate rules for inbound and outbound traffic.
Security group rules enable you to filter traffic based on protocols and port numbers.
Security groups are stateful — if you send a request from your instance, the response traffic for that request is allowed to flow in regardless of inbound security group rules. Responses to allowed inbound traffic are allowed to flow out, regardless of outbound rules.

A Network Access Control List (ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You might set up network ACLs with rules similar to your security groups to add an additional layer of security to your VPC.

References:

- VPC_ACLs
- VPC_SecurityGroupRules
- vpc-network-acls_nacl-examples
- how-to-help-prepare-for-ddos-attacks-by-reducing-your-attack-surface
- whitepapers_aws-best-practices-ddos-resiliency (PDF)

Question 13

A popular educational website is facing a surge in demand for online video training. They have their large number of video content distributed between on-premise data centers & on Amazon S3 bucket in the us-west region. Students worldwide face glitches in videos & complaining about the time required to get these videos running even though each video size is less than 1 Gb. The Marketing Team expects a further increase in demand & you need to provide a scalable solution for this concern that can be deployed in the shortest time frame. Which of the following is a recommended cost-optimized scalable solution?

- A. Use Amazon S3 Cross-Region Replication to replicate content from the us-west region to other regions.
- B. Use Throughput optimized EBS volumes to save video content.
- C. Use Amazon CloudFront for videos saved in on-premise & Amazon S3 origin.right
- D. Move all content from on-premise data centers to Amazon S3 & enable Transfer Acceleration on this bucket.

Explanation:

Correct Answer – C

Amazon CloudFront Can be used to offload origin server loads. In the above case, for videos saved in on-premise servers & Amazon S3 bucket, Amazon CloudFront can be used to deliver this content to users with less latency & offload load on servers.

- Option A is incorrect as Using storing video content in the Amazon S3 bucket in different regions would incur additional charges.
- Option B is incorrect as EBS would be preferred for rapidly changing web content. In the above case, video content would not be rapidly changing. So storing content in Amazon S3 bucket with Amazon CloudFront distribution is a better option.
- Option D is incorrect as using Amazon S3 transfer Acceleration would be costly compared to Amazon CloudFront. Also, for files less than 1 Gb, using Amazon

CloudFront would provide better performance than Amazon S3 Transfer Acceleration.

For more information on using Amazon CloudFront for scalable web content, refer to the following URLs-

- https://aws.amazon.com/blogs/architecture/scale-your-web-application-one-step-at-a-time/
- https://aws.amazon.com/s3/faqs/

Question 14

A global conglomerate is looking for a Multi-site DR plan for an application deployed on a server fleet at the on-premises Data Centre. There is also a large database that needs to back up daily. Incomplete backups can impact RPO in case of failure. They are looking for high bandwidth links with fast data transfer speed from on-premises to AWS VPC. The connections should be reliable with redundancy. Which of the following is the most appropriate?

- A. Create a Direct Connection between on-premise and VPC.
- B. Create multiple Direct Connections with LAG enabled in active mode to provide redundancy.right
- C. Create multiple VPN connections with LAG enabled in active mode to provide secure connections.
- D. Create a VPN CloudHub.

Explanation:

Correct Answer – B

For higher throughput, LAG can aggregate multiple DX connections to give a maximum of 40 Gig bandwidth.

Option A is incorrect because there is no redundancy provided in this option.
Option C is incorrect because the VPN connections cannot provide high performance.
Option D is incorrect because this option does not provide high speed connections.

For more information on using LAG over AWS Direct Connect, refer to the following URLs-

- https://docs.aws.amazon.com/directconnect/latest/UserGuide/lags.html

Question 15

Videos are uploaded to an S3 bucket, and you need to provide access to users to view the same. What is the best way to do so while maintaining a good user experience for all users regardless of the region in which they are located?

- A. Enable Cross-Region Replication for the S3 bucket to all regions.

- B. Use CloudFront with the S3 bucket as the source.right
- C. Use API Gateway with S3 bucket as the source.

- D. Use AWS Lambda functions to deliver the content to users.

Explanation:

Correct Answer – B
AWS Documentation mentions the following to back up this requirement.

Amazon CloudFront is a web service that speeds up the distribution of 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 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. If the content is not in that edge location, CloudFront retrieves it from an Amazon S3 bucket or an HTTP server (for example, a web server) that you have identified as the source for the definitive version of your content.

Option A is incorrect. S3 Cross-region replication is a feature that enables an automatic and asynchronous copy of user data from one destination bucket to another destination bucket located in one of the other AWS regions. It is region-based rather than a global scale, which is what the question asks regarding all users having a good experience, regardless of region locale.

For more information on Amazon CloudFront, please visit the following URL-

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

Question 16

Your company has a set of 100 servers hosted on the AWS Cloud. There is a need to stream the Logs from the Instances for analysis purposes. From a security compliance perspective, additional logic will be executed to analyze the data for any sort of abnormal behaviour. Which of the following would be used to stream the log data?

- A. Amazon CloudFront

- B. Amazon SQS

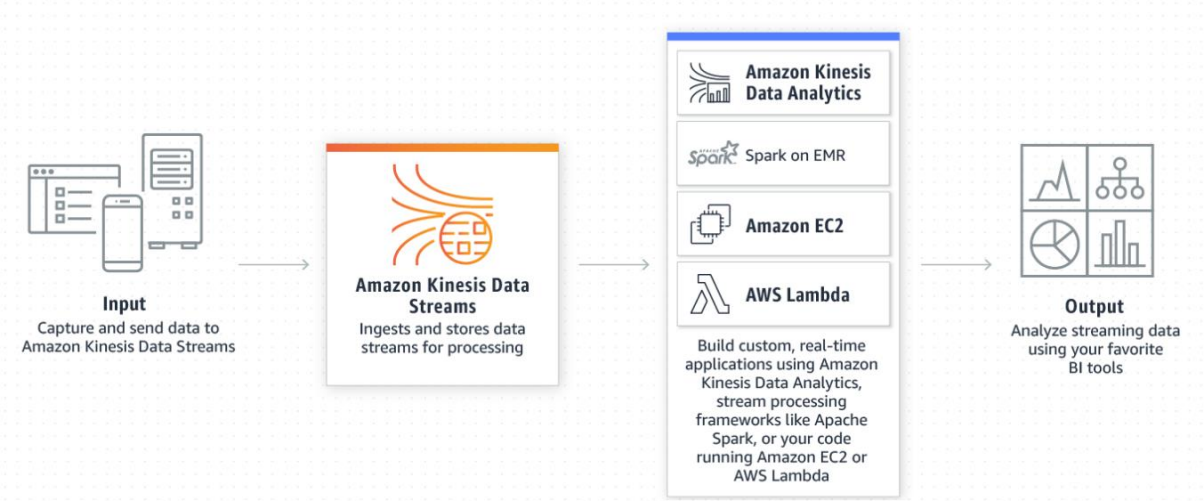
- C. Amazon Kinesis Data Streams (KDS)right
- D. Amazon SES (Simple Email Service)

Explanation:

Correct Answer: C
The AWS Documentation mentions the following

Amazon Kinesis Data Streams enables you to build custom applications that process or analyze streaming data for specialized needs. You can continuously add various types of data such as clickstreams, application logs, and social media to an Amazon Kinesis data stream from hundreds of thousands of sources. Within seconds, the data will be available for your Amazon Kinesis Applications to read and process from the stream.

Use cases of Kinesis Data Streams:
Log and event data collection
Real-time analytics
Mobile data capture
Gaming data feed



- Option A is incorrect since CloudFront is a content distribution service.
- Option B is incorrect since SQS is used as a messaging service.
- Option D is incorrect since SES is an email service.

For more information on AWS Kinesis, please visit the below URL

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

Question 17

A startup company wants to launch an online learning portal on AWS using CloudFront and S3. They have different subscription models. One model where all the members will have access to basic content but another model where the company provides premium content that includes access to multiple private contents without changing their current links.

How should a Solution Architect design this solution to meet the requirements?

- A. Design the learning portal using CloudFront web distribution to deliver the premium private content using Signed Cookies.right
- B. Design the learning portal using CloudFront web distribution to deliver the premium private content using Signed URLs.

- C. Design the learning portal using CloudFront web distribution to deliver the premium private content using S3 pre-signed URLs.

- D. Design the learning portal using CloudFront web distribution to deliver the premium private content using CloudFront geographic restrictions feature.

Explanation:

Answer: A
Option A is CORRECT. Use signed cookies in the following cases to provide access to multiple restricted files. For example, all the files for a video in HLS format or all of the files in the subscribers' area of the website. You don't want to change your current URLs.
Option B is incorrect. CloudFront signed URLs and signed cookies provide the same basic functionality, and they allow users to control who can access the content.
Use signed URLs in the following cases.

- You want to restrict access to individual files, for example, an installation download for your application-

- Your users are using a client (for example, a custom HTTP client) that doesn't support cookies.

Option C is incorrect because S3 pre-signed URLs won't provide access without changing current links.
Option D is incorrect because the CloudFront geographic restrictions feature is used to prevent users in specific countries from accessing your content, but there is no such requirement in the question.
References:

- https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-choosing-signed-urls-cookies.html
- https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/georestrictions.html
- https://docs.aws.amazon.com/AmazonS3/latest/dev/ShareObjectPreSignedURL.html
- https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-signed-urls.html

Question 18

An organization has an on-premises messaging application. They want to migrate this application to the AWS cloud without making much code changes while running an on-prem system parallel with the AWS cloud in the hybrid model.

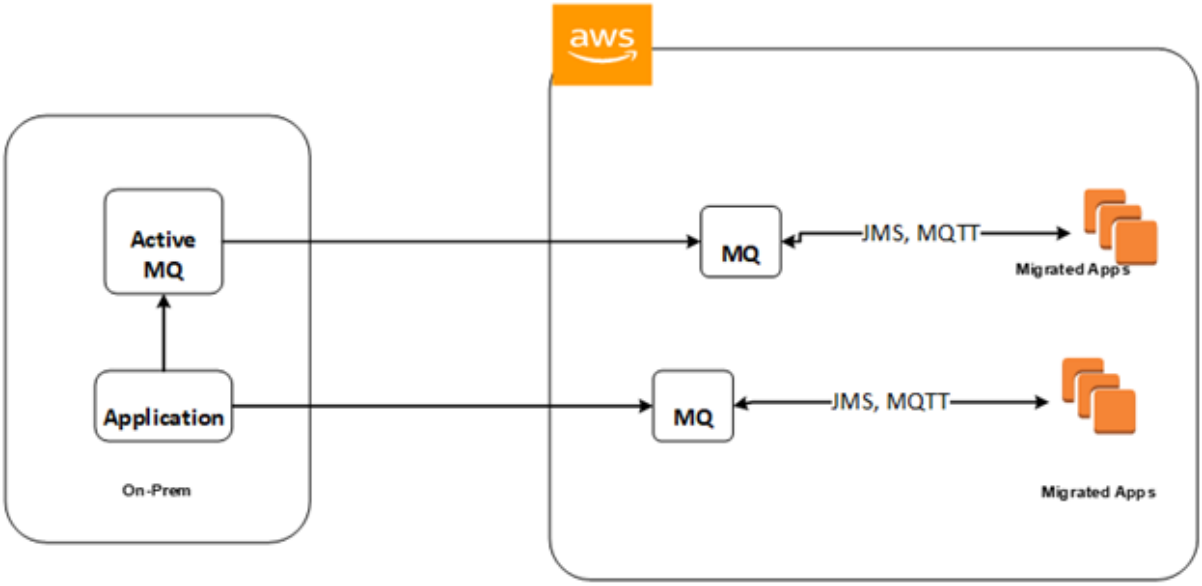
How would Solution Architect migrate the highly available solution and support JMS APIs, AMQP, and MQTT protocols?

- A. Design the solutions using SNS that also supports integration with other AWS services.
- B. Design the solutions using SQS that also supports integration with other AWS services.
- C. Design the solutions using SQS, SNS and Lambda.
- D. Design the solutions using Amazon MQ in 2 private subnets across multiple Availability Zones.right

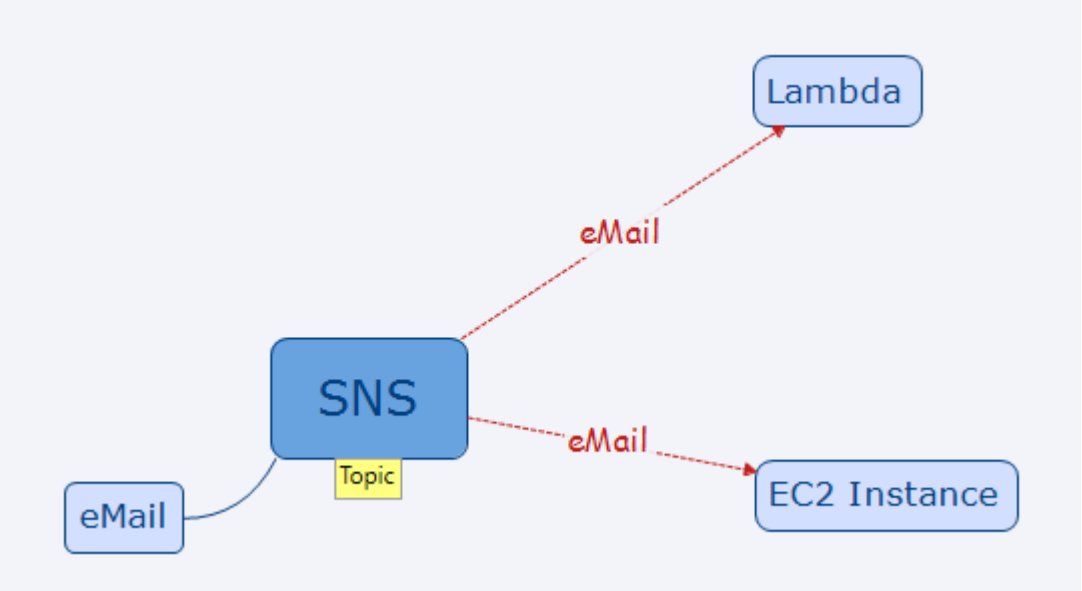
Explanation:

Correct Answer : D

Key points to note in this question are hybrid running two systems. Systems should be highly available, cloud migration, supports both queues and topics (pub and sub), supports JMS API and MQTT protocols, without making code change.



- Option A is incorrect: SNS is a highly available AWS service that provides topics but doesn't make code change requirements and hybrid running of two systems. SNS supports the push model of asynchronous communications in the following picture.



- Option B is incorrect: SQS is a highly available AWS service that provides queues but doesn't make code change requirements and hybrid running of two systems.
- Option C is incorrect: SQS and SNS are highly available AWS services that provide queues and topics but don't make code change requirements. This will be a good solution for the long run if I need to rewrite with SNS and SQS that supports other AWS services.
- Option D is CORRECT: Amazon MQ is a managed AWS service for Apache Active MQ that meets both SQS (queues) and SNS (Topics) functionality. It also supports JMS API and other key protocols like MQTT etc. This is a good fit to migrate on-prem applications using traditional message brokers.

Reference:

- https://aws.amazon.com/amazon-mq/?amazon-mq.sort-by=item.additionalFields.postDateTime&amazon-mq.sort-order=des

Question 19

A company needs to monitor the read and write IOPS metrics for its AWS MySQL RDS instance and send real-time alerts to its Operations team. Which AWS services could help to accomplish this? (SELECT TWO)

- A. Amazon Simple Email Service
- B. Amazon CloudWatchright
- C. Amazon Simple Queue Service
- D. Amazon Route 53
- E. Amazon Simple Notification Serviceright

Explanation:

Correct Answers – B and E

Amazon CloudWatch may be used to monitor IOPS metrics from the RDS instance and Amazon Simple Notification Service to send the notification if an alarm is triggered.

For more information on CloudWatch metrics, please refer to the link below.

- http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CW_Support_For_AWS.html

Question 20

You run an ad-supported photo-sharing website using S3 to serve photos to visitors of your site. At some point, you find out that other sites have been linking to photos on your site, causing loss to your business. What would be an effective method to mitigate this?

- A. Use CloudFront distributions for static content.
- B. Store photos on an EBS volume of the web server.
- C. Remove public read access and use presigned URL with expiration.right
- D. Block the IPs of the offending websites in Security Groups.

Explanation:

Correct Answer – C

When you create a presigned URL for your object, you must provide your security credentials, specify a bucket name, an object key, specify the HTTP method (GET to download the object) and expiration date and time. The presigned URLs are valid only for the specified duration.

The credentials that you can use to create a presigned URL include:

- IAM instance profile: Valid up to 6 hours.
- AWS Security Token Service: Valid up to 36 hours when signed with permanent credentials, such as the credentials of the AWS account root user or an IAM user
- IAM user: Valid up to 7 days when using AWS Signature Version 4

  To create a presigned URL that's valid for up to 7 days, first designate IAM user credentials (the access key and secret access key) to the SDK that you're using. Then, generate a presigned URL using AWS Signature Version 4.

For more information on presigned URLs, please visit the link below.

- https://docs.aws.amazon.com/AmazonS3/latest/dev/ShareObjectPreSignedURL.html

Question 21

An Organization has an application using Amazon S3 Glacier to store large CSV objects. While retrieving these large objects end users are observing some performance issue. In most cases, users only need a small part of the data instead of the entire objects.

A solutions Architect has been asked to re-design this solution to improve the performance. Which solution is the most cost-effective?

- A. Use AWS Athena to retrieve only the data that users need.
- B. Use S3 Select to retrieve only the data that users need.
- C. Use Glacier Select to retrieve only the data that users need.right
- D. Use custom SQL statements and S3 APIs to retrieve only the data that users need.

Explanation:

Correct Answer : C

- Option A is incorrect because Athena supports standard SQL to retrieve data, but it's more used for analytical data.
- Option B is incorrect because the objects are stored in Glacier. The correct method should be Glacier Select.
- Option C is CORRECT because the application needs to retrieve data from Glacier. With Glacier Select, you can perform filtering directly against a Glacier object using standard SQL statements.
- Option D is incorrect because writing custom SQL statements with S3 APIS wouldn't improve performance.

Reference:

- https://aws.amazon.com/blogs/aws/s3-glacier-select/

Question 22

A cash-starved start-up firm is using AWS Storage Gateway to back up all on-premise data to Amazon S3. For this, they have set up VPN connectivity to VGW from client end devices using existing internet links. They are recently observing data backups taking a long time to complete due to large data size. They are also looking for an immediate resolution for quick data backup. Which of the following is a cost-effective way to faster data backups on the VPN tunnel?

- A. Create a new VPN tunnel with ECMP enabled on a separate VGW.
- B. Create a new VPN tunnel with ECMP enabled on the same VGW.
- C. Create an additional VPN tunnel using a different VGW-Client end device

- D. Enable ECMP with multiple VPN tunnels associated with a transit gateway.right

Explanation:

Correct Answer – D
For each VPN Tunnel, AWS provides two different VPN endpoints. ECMP (Equal Cost Multi-Path) can be used to carry traffic on both VPN endpoints, increasing performance & faster data transfer.

- Options A & B are incorrect because ECMP needs to be enabled through a transit gateway.
- Option C is incorrect as creating a separate VPN tunnel will incur additional cost & will not enhance any performance without enabling ECMP.

For more information on AWS VPN performance, refer to the following URL-

- https://aws.amazon.com/vpn/features/
- https://aws.amazon.com/premiumsupport/knowledge-center/transit-gateway-ecmp-multiple-tunnels/

Question 23

Developer Team is working on a new mobile game that will use Amazon DynamoDB to store player details. The team is unsure of the success of this game, but needs to make sure it will meet demand for any number of concurrent players. During the table's initial creation, they are planning to create a local secondary index to create a top ten players scores dashboard. Also, a global secondary index is created to prepare a separate top ten players per country. IT Head is concerned about the game's performance, which will be used as a reference for all future games. Which of the following can be used to meet this requirement?

- A. Enable Auto-Scaling for DynamoDB Table with same setting applied to Global Secondary Index.right
- B. Enable Auto-Scaling for DynamoDB Table with same setting applied to Local Secondary Index.
- C. Enable Auto-Scaling only for Global Secondary Index.
- D. Enable Auto-Scaling only for Local Secondary Index.

Explanation:

Correct Answer – A
For applications where database utilization cannot be predicted, Amazon DynamoDB can be used with Auto Scaling, which can help to scale dynamically to any load. Auto-Scaling needs to be applied to the DynamoDB table and Global Secondary Index that use separate read /write capacity.

- Option B is incorrect as the Local Secondary Index uses the same read & write capacity as the primary DynamoDB table. Hence, it needs to enable a separate Auto-Scaling policy.
- Option C is incorrect as Auto-Scaling needs to enable for both DynamoDB tables and Global Secondary Index.
- Option D is incorrect as Auto-Scaling needs to enable on the DynamoDB table & Global Secondary Index & not on the Local Secondary index.

For more information on using Auto-Scaling with Amazon DynamoDB, refer to the following URL-

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

Question 24

A global pharma company has a tie-up with hospitals across the globe. The hospitals share patient reports with the pharma company, which are further analyzed & used to create new drug formulations. Daily large numbers of reports are shared by these hospitals, which are uploaded from various sources. Pharma firm is planning to tie up with more hospitals, which will increase the data load. These uploadings should be scalable to save a large amount of data for further analysis. Which of the following can be used for a scalable application solution in AWS?

- A. Use AWS Kinesis Streams to upload data to Amazon Redshift.
- B. Use AWS Kinesis Firehose to upload data to Amazon Redshift.right
- C. Use AWS Kinesis Streams to upload data to Amazon RDS.
- D. Use AWS Kinesis Firehose to upload data to Amazon RDS.

Explanation:

Correct Answer – B

Amazon Kinesis Firehose is a scalable option to load data to analytical tools like Amazon Redshift from multiple sources. Amazon Redshift can be used for complex analytical queries for large amounts of data.

- Option A is incorrect as AWS Kinesis Streams cannot directly upload data to Amazon Redshift. Additional applications need to be installed to get these data from Kinesis Streams & upload them to Amazon Redshift.
- Options C & D are incorrect as Amazon Redshift will be a better option for analyzing large streams of data instead of Amazon RDS.

For more information on using Amazon Redshift with Kinesis Firehose, refer to the following URLs-

- https://aws.amazon.com/kinesis/data-firehose/
- https://aws.amazon.com/redshift/faqs/

Question 25

An IT firm is using AWS cloud infrastructure for its three-tier web application. They are using memory-optimized EC2 instances for application hosting & SQL-based database servers deployed in Multi-AZ with auto-failover. Recently, they are observing heavy loads on database servers. This is impacting user data lookup from application servers resulting in slow access. As AWS Consultants, they are looking for guidance to resolve this issue. Which of the following will provide a faster scalable option to deliver data to users without impacting backend servers?

- A. Use Amazon ElastiCache to cache data.right
- B. Configure the Multi-AZ replicas to serve the read traffic.
- C. Use Amazon CloudFront to save recently accessed data in cache.
- D. Use on-host caching on memory optimised EC2 instance.

Explanation:

Correct Answer – A
Amazon ElastiCache provides a scalable faster approach to cache data which can be used with both SQL/NoSQL databases. These can be used to save application data, significantly improving latency & throughout the application, and offloading load on back-end database servers.

- Option B is incorrect as a Multi-AZ replica is used for data redundancy. It is not used to share the read traffic.
- Option C is incorrect as Amazon CloudFront is more suitable for website caching & not for application caching.
- Option D is incorrect as this would provide a faster lookup of data, but it's not scalable.

For more information on using Amazon ElastiCache, refer to the following URLs-

- https://d0.awsstatic.com/whitepapers/performance-at-scale-with-amazon-elasticache.pdf
- https://aws.amazon.com/about-aws/whats-new/2018/01/amazon-rds-read-replicas-now-support-multi-az-deployments/

Question 26

Your company has setup EC2 Instances in a VPC for their application. They now have a concern that not all of the EC2 instances are being utilized. Which of the below mentioned services can help you find underutilized resources in AWS? Choose 2 answers from the options given below

- A. AWS Cloudwatchright
- B. SNS
- C. AWS Trusted Advisorright

- D. Cloudtrail

Explanation:

Correct Answers: A and C

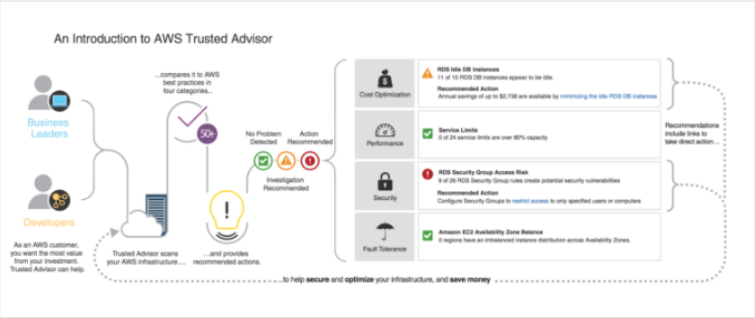
The AWS Documentation mentions the following

"An online resource to help you reduce cost, increase performance,and improve security by optimizing your AWS environment,Trust Advisor provides real time guidance to help you provison your resources following AWS best practices"

> An online resource to help you reduce cost, increase performance, and improve security by optimizing your AWS environment, Trusted Advisor provides real time guidance to help you provision your resources following AWS best practices.

An Introduction to AWS Trusted Advisor

(click to enlarge)



Amazon CloudWatch is a monitoring and management service built for developers, system operators, site reliability engineers (SRE), and IT managers. CloudWatch provides you with data and actionable insights to monitor your applications, understand and respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health.

- Option B is incorrect since this is a notification service
- Option D is incorrect since this is an API monitoring service

For more information on AWS Trusted Advisor and Cloudwatch, please visit the below URL

- https://aws.amazon.com/premiumsupport/trustedadvisor/
- https://aws.amazon.com/cloudwatch/

Question 27

Your architecture for an application currently consists of EC2 Instances sitting behind a classic ELB. The EC2 Instances are used to serve an application and are accessible through the internet. What could be done to improve this architecture if the number of users accessing the application increases regularly?

- A. Add another ELB to the architecture.
- B. Use Auto Scaling Groups.right
- C. Use an Application Load Balancer instead.

- D. Use the Elastic Container Service.

Explanation:

Correct Answer – B

AWS Documentation mentions the following.

AWS Auto Scaling monitors your applications and automatically adjusts the capacity to maintain steady, predictable performance at the lowest possible cost. Using AWS Auto Scaling, it is easy to setup application scaling for multiple resources across multiple services in minutes.

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

https://aws.amazon.com/autoscaling/

Question 28

A solutions Architect has been asked to design a serverless media upload web application that will have the functionality to upload thumbnail images, transcode videos, index files, validate contents, and aggregate data in real-time. He needs to visualize the distributed components of his architecture through a graphical console. How can this be designed wisely?

- A. Host a static web application using Amazon S3, upload images to Amazon S3, trigger a Lambda function when media files are uploaded, coordinate other media files processing Lambdas using several SQS queues, and store the aggregated data in DynamoDB.

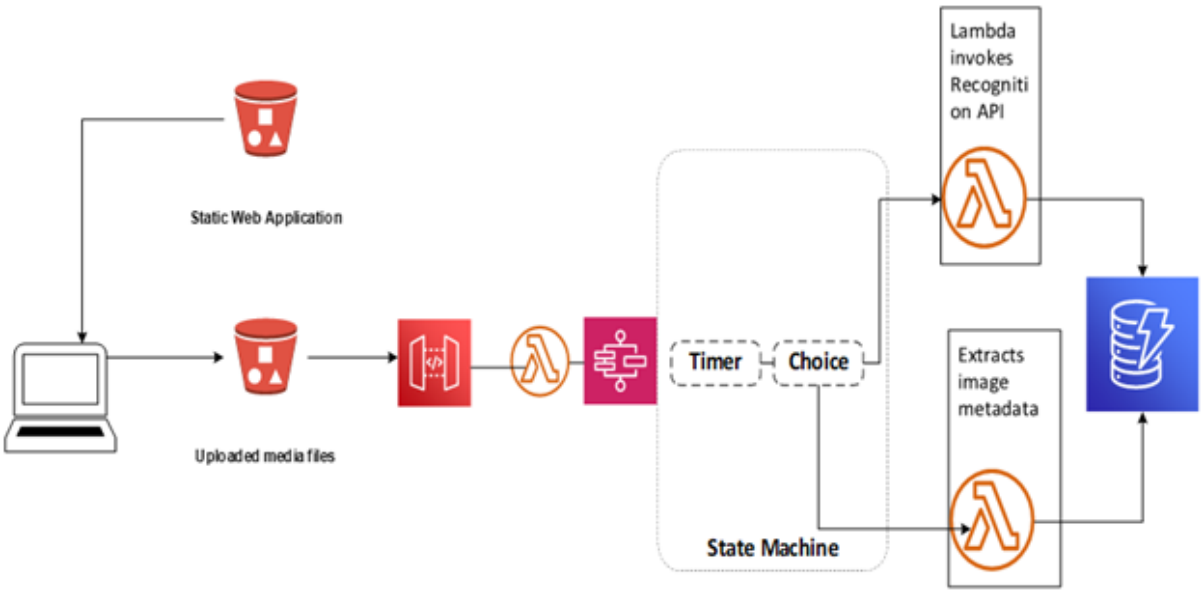
- B. Host a static web application using Amazon S3, upload images to Amazon S3, trigger a Lambda function when media files are uploaded, coordinate other media files processing Lambdas using Simple Workflow Service, and store the aggregated data in DynamoDB.

- C. Host a static web application using Amazon S3, upload images to Amazon S3, trigger a Lambda function when media files are uploaded, process media files using various Lambdas, and store the aggregated data in DynamoDB.

- D. Host a static web application using Amazon S3, upload images to Amazon S3, use S3 event notification to trigger a Lambda function when media files are uploaded, coordinate other media files processing Lambda using Step functions, and store the aggregated data in DynamoDB.right

Explanation:

Correct Answer : D



As an above diagram, Steps functions are used to coordinate processing Lambda functions and store the data on DynamoDB.

Differences between Steps function and SWF are as follows:

Step Functions	SWF
Good for any new serverless application where coordination is required between various components using a visual workflow	Need external signals to intervene in processes, OR Good if there are child processes and those require passing signals to parents.
Easy to use while developing application	More complex while developing application but complete control of orchestration logic
Uses declarative JSON to write state machine	Need to write decider program (programing of your choice) to separate activities between steps or use AWS flow framework
Serverless, lower admin overhead	Uses servers
Short running workflows	Long-running workflows,
Mostly used for synchronous tasks	Mostly used for asynchronous tasks
New AWS Service, less complex applications	Legacy application, Complex decisions (custom decide application)
	Integrate with AWS Mechanical Turk

- Option A is incorrect: Using SQS queues to coordinate several Lambda functions is not suitable.

- Option B is incorrect: SWF can manage workflows, but managing Lambda functions with step functions are better. SWF is used to manage the infrastructure that runs workflow logic and tasks. SWF is the least used service
- Option C is incorrect: Managing Lambda functions will be challenging without a managed workflow service such as Step functions.
- Option D is CORRECT: This is the best answer as Step functions are used to coordinate the processing of Lambda functions. It also provides a graphical way to visualize the processing steps.

Reference:

- https://aws.amazon.com/step-functions/faqs/
- https://aws.amazon.com/step-functions/use-cases/

Question 29

You are the architect for a business intelligence application that reads data from a MySQL database hosted on an EC2 Instance. The application experiences a high number of read and write requests.

Which Amazon EBS Volume type can 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

Since there is a Business intelligence requirement with a large number of read and write requests, one needs to opt for EBS Provisioned IOPS SSD.

	General Purpose SSD		Provisioned IOPS SSD		
Volume type	gp3	gp2	io2 Block Express ‡	io2	io1
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)	99.999% durability (0.001% annual failure rate)	99.999% durability (0.001% annual failure rate)	99.8% - 99.9% durability (0.1% - 0.2% annual failure rate)
Use cases	• Low-latency interactive apps • Development and test environments		Workloads that require: • Sub-millisecond latency • Sustained IOPS performance • More than 64,000 IOPS or 1,000 MiB/s of throughput	• Workloads that require sustained IOPS performance or more than 16,000 IOPS • I/O-intensive database workloads	

	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

Reference:

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

Question 30

An organization is planning to use AWS for its production roll-out. The organization wants to implement automation for deployment such that it will automatically create a LAMP stack, download the latest PHP installable from S3, set up the ELB and Auto Scaling. Which AWS service would meet these requirements for making an orderly deployment of the software?

- A. AWS Elastic Beanstalkright
- B. AWS CloudFront
- C. AWS CodePipeline
- D. AWS DevOps

Explanation:

Correct Answer – A
The Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services.

For a typical web application, configuring for HA requires running multiple web servers behind a load balancer, configuring Auto Scaling to replace lost instances and launch more instances in response to surges in traffic, and having a standby database instance configured for automatic failover.

For AWS Elastic Beanstalk, production HA configuration also includes running your database instances outside of your web server environment which allows you to perform blue/green deployments and advanced database management operations.

And Elastic Beanstalk uses EC2 Autoscaling Group to handle elasticity but Lightsail doesn't support autoscaling.

Hence, **option A is the correct answer**.
For more information on launching a LAMP stack with Elastic Beanstalk, please refer to the link below.

- https://aws.amazon.com/getting-started/projects/launch-lamp-web-app/faq/
- https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/php-ha-tutorial.html?icmpid=docs_tutorial_projects

Question 31

Your company is planning to use the API Gateway service to manage APIs for developers and users. There is a requirement to segregate access rights for both developers and users. How could this be accomplished?

- A. Use IAM permissions to control the access.right
- B. Use AWS Access keys to manage the access.
- C. Use AWS KMS service to manage the access.
- D. Use AWS Config Service to control the access.

Explanation:

Correct Answer - A

AWS Documentation mentions the following.

You can control access to Amazon API Gateway with IAM permissions by controlling access to the following two API Gateway component processes.

- To create, deploy, and manage an API in API Gateway, you must grant the API developer permissions to perform the required actions supported by the API management component of API Gateway.
- To call a deployed API or to refresh the API caching, you must grant the API caller permissions to perform required IAM actions supported by the API execution component of API Gateway.

For more information on permissions for the API gateway, please visit the following URL-

https://docs.aws.amazon.com/apigateway/latest/developerguide/permissions.html

Question 32

You have 2 development environments hosted in 2 different VPCs in an AWS account in the same region. There is now a requirement to access the resources of one VPC from another. How could this be accomplished?

- A. Establish a Direct Connect connection.
- B. Establish a VPN connection.
- C. Establish VPC Peering.right
- D. Establish Subnet Peering.

Explanation:

Correct Answer – C
A VPC peering connection is a networking connection between two VPCs that enable 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 URL below.

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

Question 33

Your company is planning to use Amazon EMR service for testing a new application and also wants to minimize the cost of running the EMR service. How would you achieve this?

- A. Choose dedicated instances.
- B. Choose Spot Instances for the underlying nodes.right
- C. Choose On-Demand Instances for the underlying nodes.
- D. Disable automated backups.

Explanation:

Correct Answer - B
AWS Documentation mentions the following.

When you are testing a new application in order to prepare it for launch in a production environment, you can run the entire cluster (master, core, and task instance groups) as Spot Instances to reduce your testing costs.

Spot Instances are often used to run task nodes, Amazon EMR has default functionality for scheduling YARN jobs so that running jobs do not fail when task nodes running on Spot Instances are terminated.

Option A is incorrect because choosing dedicated instances will not be cost-efficient.
Dedicated Instances can be purchased using Amazon EC2 and then create a VPC with the **Dedicated** tenancy attribute. Within Amazon EMR, you then specify that a cluster should launch in this VPC. Amazon EMR does not support setting the *dedicated* attribute on individual instances.

Options C and D are incorrect because choosing On-demand instances and disabling automated backups will not help in testing the application with minimal costs.
For more information on Instance types for EMR, please visit the following URLs-

- https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-plan-instances-guidelines.html
- https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-plan-instances-guidelines.html#emr-plan-spot-scenarios
- https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-instance-purchasing-options.html

Question 34

You have an S3 bucket hosted in AWS that is used to store the promotional videos you upload. You need to provide users access to the S3 bucket's object for a limited duration of time. How could this be achieved?

- A. Use versioning and enable a timestamp for each version.
- B. Use Pre-signed URLs with session duration.right
- C. Use IAM Roles with a timestamp to limit the access.
- D. Use IAM policies with a timestamp to limit the access.

Explanation:

Correct Answer - B
AWS Documentation mentions the following.

All objects by default are private. Only the object owner has permission to access these objects. However, the object owner can optionally share objects with others by creating a pre-signed URL, using their own security credentials, to grant time-limited permission to download the objects.

For more information on pre-signed URLs, please visit the URL below.

- https://docs.aws.amazon.com/AmazonS3/latest/dev/ShareObjectPreSignedURL.html

Question 35

An application currently writes a large number of records to a DynamoDB table in one region. There is a requirement for a secondary application to retrieve new records written to the DynamoDB table every 2 hours and process the updates accordingly. What would be an ideal method to ensure that the secondary application gets the relevant changes from the DynamoDB table?

- A. Insert a timestamp for each record and then, scan the entire table for the timestamp as per the last 2 hours.

- B. Create another DynamoDB table with the records modified in the last 2 hours.

- C. Use DynamoDB Streams to monitor the changes in the DynamoDB table.right
- D. Transfer records to S3 which were modified in the last 2 hours.

Explanation:

Correct Answer – C

AWS Documentation mentions the following.

A DynamoDB Stream is an ordered flow of information about changes to items in an Amazon DynamoDB table. When you enable a stream on a table, DynamoDB captures information about every modification to data items in the table.

Whenever an application creates, updates or deletes items in the table, DynamoDB Streams write a stream record with the primary key attribute(s) of the modified items. A stream record contains information about a data modification to a single item in a DynamoDB table. You can configure the stream to capture additional information, such as the "before" and "after" images of modified items.

For more information on DynamoDB Streams, please visit the URL below.

http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Streams.html

Question 36

An organization has a distributed application running. This application is implemented with microservices architecture using AWS services including Lambda, API Gateway, SNS and SQS.

What is the cost-effective best way to analyze, debug and notify if any issues arise in production?

- A. Use Cloud watch dashboard to monitor the application, create a cloud watch alarm to notify for any errors.

- B. Use Cloud watch events to trigger a lambda and notify.

- C. Use X-Ray to analyse and debug the application and use CloudWatch alarm to notify.right
- D. Use 3rd party tools to debug and notify.

Explanation:

Correct Answer : C

- Option A is incorrect. Amazon cloud watch dashboards can help to monitor all the resources. You can have a single view and multiple view across all the AWS regions to see how things are going across the services. But it cannot give detailed debugging and monitoring of each service.
- Option B is incorrect because a cloud watch event is created if any event happens in a service and can not be used for detailed analysis and debugging.
- Option C is CORRECT as AWS X-ray collects data, analysis and debug of microservice application. Amazon X-Ray helps to analyze and debug modern applications. It will also collect the traces about the request from each of the applications. It also records the traces. After recording, it can create a view service map that can be seen to trace data latency and analyze the issues. This can help to find any unusual behavior to identify any root cause.
- Option D is incorrect. Any custom monitoring tool will not help for detailed debugging of any microservices applications running on AWS.

Question 37

Your IT Security department has mandated that all the traffic flowing in and out of EC2 instances needs to be monitored. The EC2 instances in question are launched in a VPC. Which services would you use to achieve this?

- A. Trusted Advisor
- B. VPC Flow Logsright
- C. Use CloudWatch metrics
- D. Use CloudTrail

Explanation:

Correct Answer – B

AWS Documentation mentions the following.

VPC Flow Log 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

Note:
The question asks to monitor all traffic flowing in and out of EC2 instances. Now you have to launch the EC2 instance inside the VPC. As there is no other option available to monitor IP traffic navigation, we use **VPC Flow Logs**.
Now coming to the question - why not CloudTrail?

Before venturing into it, let's look into the types of log categories we have in AWS.
1. AWS Infrastructure Logs - AWS CloudTrail, Amazon VPC Flow Logs
2. AWS Service Logs - Amazon S3, AWS Elastic Load Balancing, Amazon CloudFront, AWS Lambda, AWS Elastic Beanstalk, etc.,
3. Host-Based Logs - Messages, Security, NGINX/Apache/IIS, Windows Event Logs, Windows Performance Counters, etc.,

AWS CloudTrail: it is used to record AWS API calls for your account like,
- who made the API call?
- when was the API call made?
- what was the API call?
- which resources were acted upon in the API call?
- where were the API calls made from and made to?

NOTE:

AWS has launched a new feature called VPC Traffic Mirroring, which is used to capture and inspect network traffic at scale. To know more about this feature, please check the link below.

- https://aws.amazon.com/blogs/aws/new-vpc-traffic-mirroring/

Question 38

A company is currently utilizing a Redshift cluster as its production warehouse. As a cloud architect, you are tasked to ensure that disaster recovery is in place. Which would be the best option in addressing this issue?

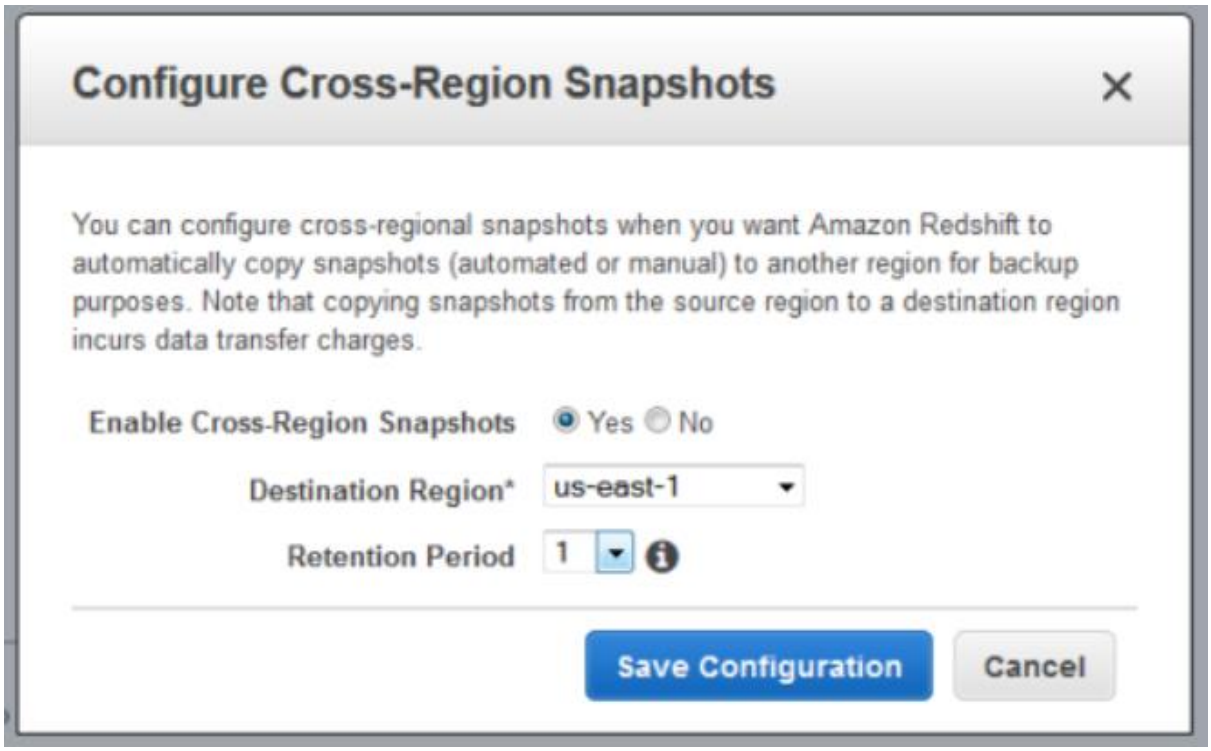
- A. Take a copy of the underlying EBS volumes to S3 and then do Cross-Region Replication.

- 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 URL-

https://docs.aws.amazon.com/redshift/latest/mgmt/managing-snapshots-console.html

Question 39

You have an AWS RDS PostgreSQL database hosted in the Singapore region. You need to ensure that the database is asynchronously copied to another one that can also share the read workload. What would be helpful to fulfill this requirement?

- A. Enable Multi-AZ for the database
- B. Enable Read Replicas for the databaseright
- C. Enable Asynchronous replication for the database
- D. Enable manual backups for the database

Explanation:

Correct Answer – B
AWS Documentation mentions the following.

Amazon RDS Read Replicas enable you to create one or more read-only copies of your database instance within the same AWS Region or in a different AWS Region. Updates made to the source database are then asynchronously copied to your Read Replicas. In addition to providing scalability for read-heavy workloads, Read Replicas can be promoted to become a standalone database instance when needed.

For more information on Read Replicas, please visit the following URL-

https://aws.amazon.com/rds/details/read-replicas/

Note:
When you enable Multi-AZ for the database, you enable synchronous replication rather than asynchronous replication mentioned in the question.

When you create a Read Replica, you first specify an existing DB instance as the source. Then Amazon RDS takes a snapshot of the source instance and creates a read-only instance from the snapshot. Amazon RDS then uses the **asynchronous replication** method for the DB engine to update the Read Replica whenever there is a change to the source DB instance.

You can use the Read Replica promotion as a data recovery scheme if the source DB instance fails.

For more information, please click the link given below.

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html

Question 40

Your current log analysis application takes more than four hours to generate a report of the top 10 users of your web application. You have been asked to implement a system that can report this information in real-time. You need to ensure that the report is always up to date, and handle increases in the number of requests to your web application. Which of the following is a cost-effective option to fulfill these requirements?

- A. Publish your data to CloudWatch Logs, and configure your application to Auto Scale to handle the load on demand.

- B. Publish your log data to an Amazon S3 bucket. Use AWS CloudFormation to create an Auto Scaling group to scale your post-processing application which is configured to pull down your log files stored in Amazon S3.

- C. Post your log data to an Amazon Kinesis data stream, and subscribe your log-processing application so that it is configured to process your logging data.right

- D. Configure an Auto Scaling group to increase the size of your Amazon EMR cluster.

Explanation:

Correct Answer – C
AWS Documentation mentions the below.

Amazon Kinesis makes it easy to collect, process, and analyze real-time, streaming data so you can get timely insights and react quickly to new information. Amazon Kinesis offers key capabilities to cost-effectively process streaming data at any scale, along with the flexibility to choose the tools that best suit the requirements of your application. With Amazon Kinesis, you can ingest real-time data such as application logs, website clickstreams, IoT telemetry data, and more into your databases, data lakes, and data warehouses, or build your own real-time applications using this data. Amazon Kinesis enables you to process and analyze data as it arrives and respond in real-time instead of having to wait until all your data is collected before the processing can begin.

For more information on AWS Kinesis, please see the below link-

https://aws.amazon.com/kinesis/

Question 41

You have been hired as an AWS Architect in a global financial firm. They provide daily consolidated reports to their clients for trades in stock markets. For a large amount of data processing, they store daily trading transaction data in S3 buckets, which triggers the AWS Lambda function. This function submits a new AWS Batch job in the Job queue. These queues use EC2 compute resources with this customized AMI and Amazon ECS to complete the job.

You have been working on an application created using the above requirements. While performing a trial for the application, even though it has enough memory/CPU resources, the job is stuck in a Runnable state. Which of the following checks would help to resolve the issue?

- A. Ensure that AWS logs driver is configured on compute resources.right
- B. AWS Batch does not support customized AMI, use ECS-optimized AMI.
- C. Check dependencies for the job which holds the job in Runnable state.
- D. Use only On-Demand EC2 instance in compute resources.

Explanation:

Correct Answer – A
If your compute environment contains compute resources, but your jobs don't progress beyond the `RUNNABLE` status, then there is something preventing the jobs

from actually being placed on a compute resource. Here are some common causes for this issue:

- The `awslogs` log driver isn't configured on your compute resources
- Insufficient resources
- No internet access for compute resources
- Amazon EC2 instance limit reached

Option A is correct as this is one of the reasons which is preventing the jobs from actually being placed on a compute resource.

Option B is incorrect as AWS Batch supports both customized AMI and Amazon ECS-optimized AMI. This is not a reason for Job being stuck in the Runnable state.

Option C is incorrect as a Job moves into a Runnable state only after all dependencies are processed. If there are any dependencies, Job stays in the Pending state, not the Runnable state.

Option D is incorrect as Compute resource can be an On-Demand Instance or a Spot Instance. In the question, it is given that the application has enough memory/CPU resources, so this is not a reason for Job being stuck in the Runnable state.

For more information on AWS Batch Job state & troubleshooting, if a job is stuck in Runnable state, refer to the following URLs-

- https://docs.aws.amazon.com/batch/latest/userguide/job_states.html
- https://docs.aws.amazon.com/batch/latest/userguide/troubleshooting.html#job_stuck_in_runnable

Question 42

There is a requirement to load a lot of data from your on-premises network to AWS S3, bypassing the internet service. What can be used for this data transfer? (SELECT TWO)

- A. Data Pipeline
- B. Direct Connectright
- C. Snowballright
- D. AWS VPC Peering

Explanation:

Correct Answers – B and C

AWS documentation mentions the following about the above services.

With a Snowball, you can transfer hundreds of terabytes or petabytes of data between your on-premises data centers and Amazon Simple Storage Service (Amazon S3). AWS Snowball uses Snowball appliances and provides powerful interfaces that you can use to create jobs, transfer data, and track your jobs' status to completion. By shipping your data in Snowballs, you can transfer large amounts of

data at a significantly faster rate than if you were transferring that data over the Internet, saving you time and money.

AWS Direct Connect links your internal network to an AWS Direct Connect location over a standard 1-gigabit or 10-gigabit Ethernet fiber-optic cable. One end of the cable is connected to your router, the other to an AWS Direct Connect router. With this connection in place, you can create *virtual interfaces* directly to public AWS services (for example, Amazon S3) or Amazon VPC, bypassing Internet service providers in your network path.

For more information on Direct Connect, please refer to the below URL-

- http://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html

- Option A is Incorrect because AWS Data Pipeline is a web service that you can use to automate data movement and transformation. Here, we are not transforming the data, and we are just moving the data from on-premises to S3.

- Option D is Incorrect because VPC Peering is used for the connection between two AWS VPCs. It cannot transfer the data from on-premises to AWS S3.

For more information on AWS Snowball, please refer to the below URL:

- http://docs.aws.amazon.com/snowball/latest/ug/whatissnowball.html

Question 43

With a Redshift cluster in AWS, you are trying to use SQL Client tools from an EC2 Instance. But you aren't able to connect to the Redshift Cluster. What must you do to ensure that you can connect to the Redshift Cluster from the EC2 Instance?

- A. Install Redshift client tools on the EC2 Instance first.

- B. Modify the Security Groups.right
- C. Use the AWS CLI instead of the Redshift client tools.

- D. Modify the Route Table of the subnet.

Explanation:

Correct Answer – B

AWS Documentation mentions the following.

By default, any cluster that you create is closed to everyone. IAM credentials only control access to the Amazon Redshift API-related resources: the Amazon Redshift console, Command Line Interface (CLI), API, and SDK. To enable access to the cluster from SQL client tools via JDBC or ODBC, you use security groups:

- If you are using the EC2-Classic platform for your Amazon Redshift cluster, you must use Amazon Redshift security groups.
- If you are using the EC2-VPC platform for your Amazon Redshift cluster, you must use VPC security groups.

For more information on Amazon Redshift, please refer to the URL below.

http://docs.aws.amazon.com/redshift/latest/mgmt/overview.html

Question 44

You currently work for a company that is specialized in baggage management. GPS devices installed on all the baggages deliver the coordinates of the unit every 10 seconds. You need to collect and analyze these coordinates in real-time from multiple sources. Which tool should you use to collect the data in real-time for processing?

- A. Amazon EMR
- B. Amazon SQS
- C. AWS Data Pipeline
- D. Amazon Kinesisright

Explanation:

Correct Answer – D

The AWS Documentation mentions the following.

Amazon Kinesis makes it easy to collect, process, and analyze real-time, streaming data so you can get timely insights and react quickly to new information. Amazon Kinesis offers key capabilities to cost-effectively process streaming data at any scale, along with the flexibility to choose the tools that best suit the requirements of your application.

With Amazon Kinesis, you can ingest real-time data such as video, audio, application logs, website clickstreams, and IoT telemetry data for machine learning, analytics, and other applications. Amazon Kinesis enables you to process and analyze data as it arrives and respond instantly instead of having to wait until all your data is collected before the processing can begin.

For more information on Amazon Kinesis, please visit the link below.

Question 45

You are planning to host a web and MySQL database application in an AWS VPC. The database should only be accessible by the web server. What would you change to fulfill this requirement?

- A. Environment variables
- B. AWS RDS Parameter Groups
- C. Route Tables
- D. Security groupsright

Explanation:

Correct Answer – D
The security group associated with the DB instance should allow port 3306 traffic from the EC2 instance. The AWS Documentation additionally mentions the following.

A *security group* acts as a virtual firewall for your instance to control inbound and outbound traffic. When you launch an instance in a VPC, you can assign a maximum of five security groups to the instance. Security groups act at the instance level, not the subnet level. Therefore, each instance in a subnet in your VPC could be assigned to a different set of security groups. If you don't specify a particular group at launch time, the instance is automatically assigned to the default security group for the VPC. For more information on VPC Security Groups, please visit the link below.

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

Question 46

A company has a requirement for block-level storage that should be able to store 800GB of data. Also, encryption of the data is required. What can be used in this case?

- A. AWS EBS Volumesright
- B. AWS S3
- C. AWS Glacier
- D. AWS EFS

Explanation:

Correct Answer - A
For block-level storage, consider EBS Volumes.

Options B and C are incorrect since they provide object-level storage.

Option D is incorrect since this provides file-level storage.

For more information on EBS Volumes, please visit the following URL-

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

Question 47

You are working as an AWS Architect for a media firm. The firm has large text files that need to be converted into audio files. They are using S3 buckets to store this text files.

AWS Batch is used to process these files along with Amazon Polly. For the compute environment, you have a mix of EC2 On-Demand & Spot instances. Critical Jobs are required to be completed quickly, while non-critical Jobs can be scheduled during non-peak hours. While using AWS Batch, management wants a cost-effective solution with no performance impact. Which of the following Job Queue can be selected to meet this requirement?

- A. Create single Job Queue with EC2 On Demand instance having higher priority & Spot Instance having lower priority.

- B. Create multiple Job Queues with one Queue having EC2 On Demand instance & having higher priority while another queue having Spot Instance & lower priority.right
- C. Create multiple Job Queues with one Queue having EC2 On Demand instance & having lower priority while another queue having Spot Instance & higher priority.

- D. Create single Job Queue with EC2 On Demand instance having lower priority & Spot Instance having higher priority.

Explanation:

Correct Answer – B
You can create multiple Job queues with different priority & mapped Compute environments to each Job queue. When Job queues are mapped to the same compute environment, queues with higher priority are evaluated first.

- Option A is incorrect as Multiple queues need to be created for each Job type. In the requirement, critical Jobs will be processed using EC2 instance while low priority jobs will be using Job queue with Spot Instance.

- Option C is incorrect as Priority for a Job queue is selected in descending order. Higher priority Job queue is preferred first.

- Option D is incorrect as Multiple queues need to be created for each Job type. In the requirement, critical Jobs will be processed using EC2 instance while low priority jobs will be using Job queue with Spot Instance. Also, a higher priority Job queue is preferred first.

For more information on Job queues in AWS Batch, refer to the following URL-

- https://docs.aws.amazon.com/batch/latest/userguide/job_queue_parameters.html

Question 48

As the company's cloud administrator, you notice that one of the EC2 instances is frequently restarting. There is a need to troubleshoot and analyze the system logs with an embedded metric format. What can be used in AWS to store and analyze the log files from the EC2 Instance?

- A. AWS SQS
- B. AWS S3
- C. AWS CloudTrail
- D. AWS CloudWatch Logsright

Explanation:

Correct Answer – D
You can use Amazon CloudWatch Logs to monitor, store, and access your log files from Amazon Elastic Compute Cloud (Amazon EC2) instances, AWS CloudTrail, and other sources.

For more information on CloudWatch Logs, please visit the following URL-

https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/WhatIsCloudWatchLogs.html
Refer to page 638 on the below link:

https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/acw-ug.pdf

Ingesting high-cardinality logs and generating metrics with CloudWatch embedded metric format

The CloudWatch embedded metric format enables you to ingest complex high-cardinality application data in the form of logs and to generate actionable metrics from them. You can embed custom metrics alongside detailed log event data, and CloudWatch automatically extracts the custom metrics so that you can visualize and alarm on them, for real-time incident detection. Additionally, the detailed log events associated with the extracted metrics can be queried using CloudWatch Logs Insights to provide deep insights into the root causes of operational events.

Embedded metric format helps you to generate actionable custom metrics from ephemeral resources such as Lambda functions and containers. By using the embedded metric format to send logs from these ephemeral resources, you can now easily create custom metrics without having to instrument or maintain separate code, while gaining powerful analytical capabilities on your log data.

When using the embedded metric format, you can generate your logs using a client library— for more information, see Using the client libraries to generate embedded metric format logs (p. 639). Alternatively, you can manually construct the logs and submit them using the PutLogEvents API or the CloudWatch agent.

Note: The question is not about compliance or auditing or tracking any kind of malicious activity or monitoring API calls in your account. If that had been the case, we would have used CloudTrail as it provides info such as who made the request, when the request was made, the request, the response, etc.

In this question, we need cloud watch logs to store and analyze logs from EC2 to find why the instance is frequently restarting.

Question 49

Your company migrated its production environment into AWS VPC 6 months ago. As a cloud architect, you must revise the infrastructure and ensure that it is cost-effective in the long term. More than 50 EC2 instances are up and running all the time to support the business operation. What can you do to lower the cost?

- A. Reserved instancesright
- B. On-demand instances
- C. Spot instances
- D. Regular instances

Explanation:

Correct Answer – A

When you have instances that will be used continuously and throughout the year, the best option is to buy reserved instances. By buying reserved instances, you actually allocate an instance for the entire year or the duration you specify with a reduced cost.

To understand more on reserved instances, please visit the below URL-

https://aws.amazon.com/ec2/pricing/reserved-instances/

Question 50

Your organization is building a collaboration platform for which they chose AWS EC2 for web and application servers and MySQL RDS instance as the database. Due to the nature of the traffic to the application, they would like to increase the number of connections to the RDS instance. How could this be achieved?

- A. Login to RDS instance and modify database config file under /etc/mysql/my.cnf
- B. Create a new parameter group, attach it to DB instance and change the setting.right

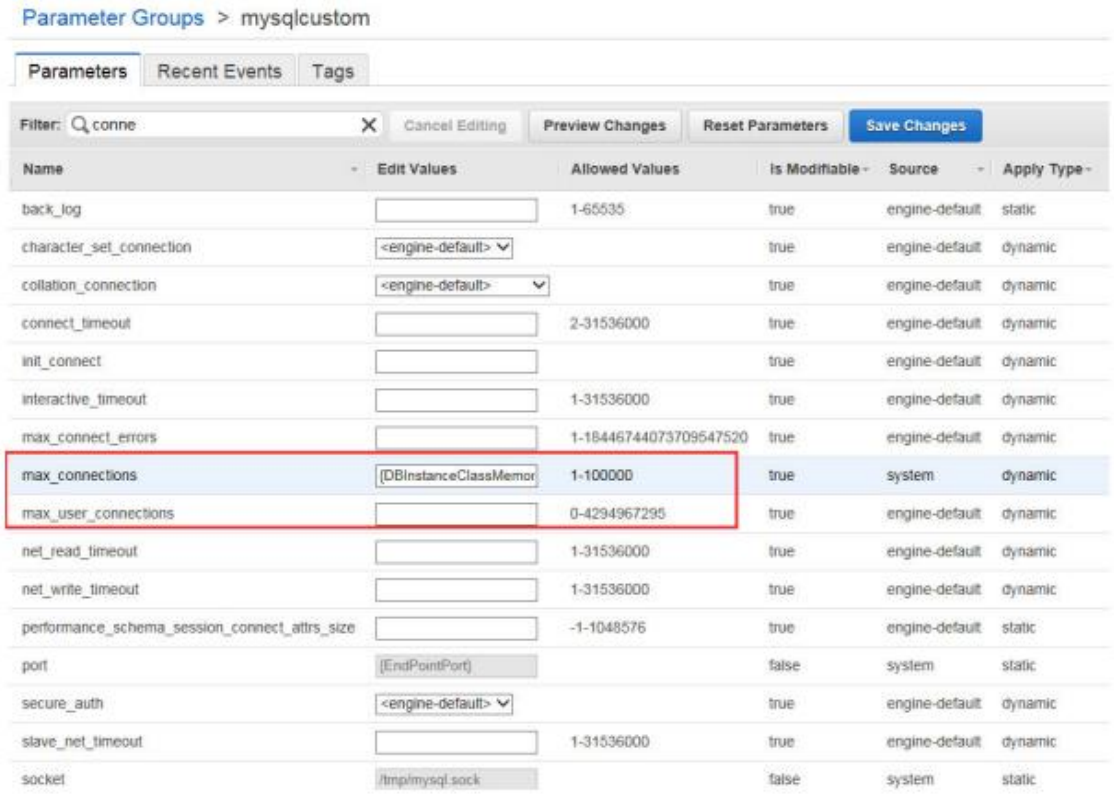
- C. Create a new option group, attach it to DB instance and change the setting.
- D. Modify setting in default options group attached to DB instance.

Explanation:

Correct Answer – B
You manage your DB engine configuration through the use of parameters in a DB parameter group. DB parameter groups act as a container for engine configuration values that are applied to one or more DB instances.

A default DB parameter group is created if you create a DB instance without specifying a customer-created DB parameter group. Each default DB parameter group contains database engine defaults and Amazon RDS system defaults based on the engine, compute class, and allocated storage of the instance. You cannot modify the parameter settings of a default DB parameter group. You must create your own DB parameter group to change parameter settings from their default value. Note that not all DB engine parameters can be changed in a customer-created DB parameter group.

If you want to use your own DB parameter group, you simply create a new DB parameter group, modify the desired parameters, and modify your DB instance to use the new DB parameter group. All DB instances that are associated with a particular DB parameter group get all parameter updates to that DB parameter group.



For more information, please visit the URL below-

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

Question 51

You are working for a Pharma firm. You are using S3 buckets to save a large amount of sensitive project documents for new medical research. You need to ensure that all data at rest in these buckets are encrypted. All the keys need to be managed by the in-house Security team. Which of the following can be used as a best practice to encrypt all data securely?

- A. Generate a data key using Customer managed CMK. Encrypt data with Plaintext data key & delete Plaintext data key. Store Encrypted data key & data in S3 buckets. For decryption, use CMK to decrypt the Encrypted data key into the Plaintext data key & then decrypt data using the Plaintext data key.right
- B. Generate a data key using AWS-managed CMK. Encrypt data with Plaintext data key & delete Plaintext data key. Store Encrypted data key & data in S3 buckets. For decryption, use CMK to decrypt the Encrypted data key into the Plaintext data key & then decrypt data using the Plaintext data key.

- C. Generate a data key using Customer managed CMK. Encrypt data with Plaintext data key & do not delete Plaintext data key. Store Encrypted data key & data in S3 buckets. For decryption, use the Plaintext data key to decrypt data.

- D. Generate a data key using AWS-managed CMK. Encrypt data with Plaintext data key & do not delete Plaintext data key. Store Encrypted data key & data in S3 buckets. For decryption, use the Plaintext data key to decrypt data.

Explanation:

Correct Answer - A

Since the In-house security team will do key Management, Customer Managed CMK needs to be used. Customer-managed CMK will generate plain text Data Key & encrypted Data Keys. All project-related sensitive documents will be encrypted using these plain text Data Keys. After encryption, plain text Data keys need to be deleted to avoid any inappropriate use, and encrypted Data Keys and encrypted data are stored in S3 buckets.

Data keys = Plaintext Data Key and Encrypted Data Key

While decryption, encrypted Data Key is decrypted using Customer CMK into plain text Key, which is further used to decrypt documents. This Envelope Encryption ensures that data is protected by a Data key, which is further protected by another key.

- Option B is incorrect. Since all keys need to manage by the in-house customer Security team, AWS-managed CMKs cannot be used.

- Option C is incorrect as it's not the best practice to save data key files in plain text format. All plain text data keys should be deleted and only encrypted data keys need to be saved.
- Option D is incorrect since all keys need to be managed by the in-house customer Security team. AWS-managed CMKs cannot be used. Also, all plain text data keys should be deleted and only encrypted data keys need to be saved.

For more information on AWS KMS, refer to the following URLs-

- https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#data-keys
- https://d0.awsstatic.com/whitepapers/aws-kms-best-practices.pdf

Question 52

A company is building a service using Amazon EC2 as a worker instance to process an uploaded audio file and generate a text file. You must store both of these files in the same durable storage until the text file is retrieved. You do not know what the storage capacity requirements are. Which storage option is both cost-efficient and scalable?

- A. Multiple Amazon EBS Volume with snapshots
- B. A single Amazon Glacier vault
- C. A single Amazon S3 bucketright
- D. Multiple instance stores

Explanation:

Correct Answer – C

Amazon S3 is the best storage option for this. It is durable and highly available.

For more information on Amazon S3, please refer to the below URL-

Question 53

You are working as an AWS developer for an online multiplayer game start-up company. Elasticache with Redis is used for gaming leaderboards to provide low latency for online games. Redis clusters are deployed within a dedicated VPC in the us-east-1 region.

Last week, due to configuration changes in Redis Clusters, the gaming application was impacted for two hours. You have been requested to plan for secure access to all the new clusters to avoid such incidents in the future. What would you prefer to secure Redis Clusters while accessing from EC2 instances, initialized in a different VPC located in the us-east-1 region? (SELECT TWO)

- A. Use Redis AUTH with in-transit encryption disabled for clusters.

- B. Create a Transit Gateway to have connectivity between 2 VPC's.right
- C. Use Redis AUTH with in-transit encryption, enabled for clusters.right
- D. Create an Amazon VPN connection between 2 VPCs.

- E. Use Redis AUTH with At-Rest encryption, enabled for clusters.

Explanation:

Correct Answer – B, C

To use Redis AUTH which will require users to provide a password before accessing Redis Cluster, in-transit encryption needs to be enabled on the cluster while creating the cluster. For accessing Redis Cluster from the EC2 instance in different VPCs from the same region, a Transit Gateway can be established between two VPCs.

- Option A is incorrect. For Redis AUTH, clusters must be enabled with in-transit encryption during initial deployment.
- Option B is also correct. Transit Gateway is suitable to access Redis Clusters from EC2 instance in VPC created in different regions. Transit Gateway is more secure because it reduces the security footprint available between the VPCs.

Refer: https://aws.amazon.com/transit-gateway/?whats-new-cards.sort-by=item.additionalFields.postDateTime&whats-new-cards.sort-order=desc

- Option D is incorrect as VPN Connections will be required to access the Redis Cluster from on-prem servers.
- Option E is incorrect. For Redis AUTH, clusters must be enabled with in-transit encryption during initial deployment.

For more information on Authentication with Redis & Accessing Redis Clusters from a different VPC, refer to the following URLs-

- https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/auth.html
- https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/elasticache-vpc-accessing.html

Question 54

Your company is utilizing CloudFront to distribute its media content to multiple regions. Users frequently access the content. As a cloud architect, which of the following options would help you improve the system's performance?

- A. Change the origin location from an S3 bucket to an ELB.

- B. Use a faster Internet connection.

- C. Increase the cache expiration time.right
- D. Create an "invalidation" for all your objects, and recache them.

Explanation:

Correct Answer – C

You can control how long your objects stay in a CloudFront cache before CloudFront forwards another request to your origin. Reducing the duration allows you to serve dynamic content. Increasing the duration means your users get better performance because your objects are more likely to be served directly from the edge cache. A longer duration also reduces the load on your origin.

For more information on CloudFront cache expiration, please refer to the following link-

http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Expiration.html

Question 55

Your supervisor has instructed you to devise a disaster recovery model for the resources in the AWS account. The key requirement while devising the solution is to ensure that the cost is at the minimum. Which disaster recovery mechanism would you employ in such a scenario?

- A. Backup and Restoreright
- B. Pilot Light
- C. Warm standby
- D. Multi-Site

Explanation:

Correct Answer – A
Since the cost needs to be at the minimum, the best option is to back up all the resources and then perform a restore in the event of a disaster.

For more information on disaster recovery, please refer to the below link-

- https://aws.amazon.com/blogs/aws/new-whitepaper-use-aws-for-disaster-recovery/
- https://aws.amazon.com/disaster-recovery/

Question 56

An application consists of the following architecture.

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

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

c. There is a NAT instance used so that instances can download updates from the internet.

Due to the high bandwidth being consumed by the NAT instance, it has been decided to use a NAT Gateway. How could this be implemented?

- A. Use NAT Instances along with the NAT Gateway.
- B. Host the NAT instance in the private subnet.
- C. Migrate from NAT Instance to a NAT Gateway and host the NAT Gateway in the public subnet.right
- D. Host the NAT gateway in the private subnet

Explanation:

Correct Answer – C
One can simply start using the NAT Gateway service and stop using the deployed NAT instances. But you need to ensure that the NAT Gateway is deployed in the public subnet.

- For more information on migrating to a NAT Gateway, please visit the following URL-
  - https://aws.amazon.com/premiumsupport/knowledge-center/migrate-nat-instance-gateway/

Question 57

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) Must be able to collect and analyze logs about ELB's performance.

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

What should be used to achieve this requirement? (SELECT TWO)

- A. Use CloudWatch for monitoring.right
- B. Enable VPC Flow logs and then investigate the logs whenever there is an issue.
- C. Enable the logs on the ELB with Latency Alarm that sends an email and then investigate the logs whenever there is an issue.right
- D. Use CloudTrail to monitor whatever metrics need to be monitored.

Explanation:

Correct Answer – A and C
When you use CloudWatch metrics for an ELB, you can get some read requests and latency out of the box.

For more information on using CloudWatch with the ELB, please visit the following URL-

https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-cloudwatch-metrics.html
Elastic Load Balancing provides access logs that capture detailed information about requests sent to your load balancer. Each log contains information on when the request was received, the client's IP address, latencies, request paths, and server responses. You can use these access logs to analyze traffic patterns and to troubleshoot issues.

For more information on using ELB logs, please visit the following URL-

https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/access-log-collection.html
Option B is INCORRECT because using VPC flow logs, we cannot pinpoint the issues related to ELB performance.

Option D is INCORRECT because CloudTrail is used only for monitoring API activities on AWS resources.

Question 58

Your company would like to leverage the AWS storage option and integrate it with the current on-premises infrastructure. There is a requirement of low latency access to the entire dataset and backup. Which of the following options would be best suited for this scenario?

- A. Configure the Simple Storage Service.
- B. Configure Storage Gateway Cached Volume.
- C. Configure Storage Gateway Stored Volume.right
- D. Configure Amazon Glacier.

Explanation:

Correct Answer – C
Option A is incorrect because S3 is not used to provide low latency data access by integrating with the on-premises data center.
Option B is incorrect because cached volumes do not provide low latency to all the data.
Option C is correct because it provides low latency to all the data and maintains backup in AWS.
Option D is incorrect because Amazon Glacier is used to achieve data for a longer period of time, not related to the required scenario.

Cached volumes – Cached volumes offer substantial cost savings on primary storage and minimize the need to scale your storage on-premises. You also retain low-latency access to your frequently accessed data.

Stored volumes – Stored volumes provide your on-premises applications with low-latency access to their entire datasets. At the same time, they provide durable, offsite backups. With stored volumes, you maintain your volume storage on-premises in your data center. This solution is ideal if you want to keep data locally on-premises, because you need to have low-latency access to all your data, and also to maintain backups in AWS.

Reference:

- https://docs.aws.amazon.com/storagegateway/latest/userguide/backing-up-volumes.html
- https://docs.aws.amazon.com/storagegateway/latest/userguide/StorageGatewayConcepts.html

Question 59

Domain: Design High-Performing Architectures

An IT company has a set of EC2 Instances hosted in a VPC. They are hosted in a private subnet. These instances now need to access resources stored in an S3 bucket. The traffic should not traverse the internet. The addition of which of the following would help to fulfill this requirement?

- A. VPC Endpointright
- B. NAT Instance
- C. NAT Gateway
- D. Internet Gateway

Explanation:

Correct Answer - A

A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network.

For more information on AWS VPC endpoints, please visit the following URL-

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

Question 60

Domain: Design Resilient Architectures

You need to host a set of web servers and database servers in an AWS VPC. What would be the best practice in designing a multi-tier infrastructure?

- A. Use a public subnet for the web tier and a public subnet for the database layer.

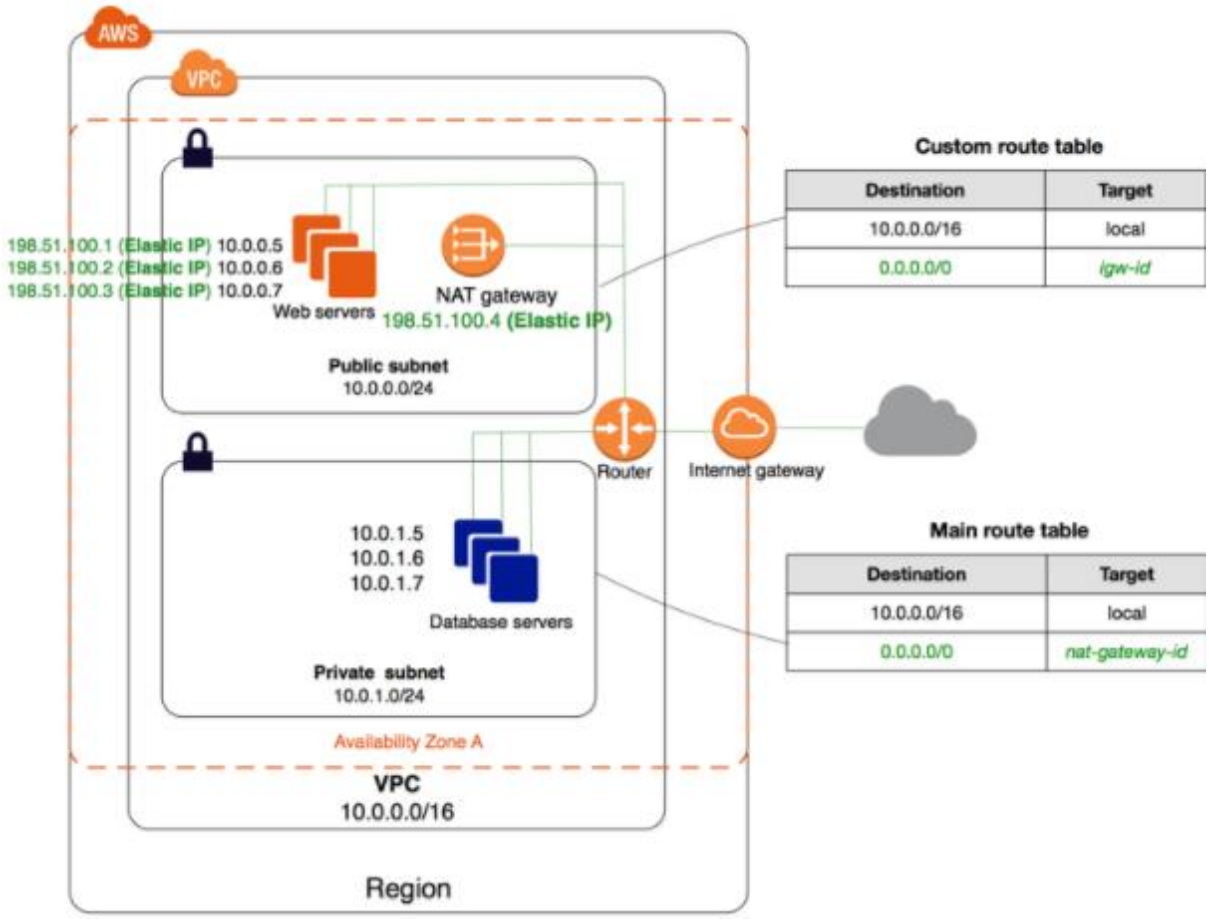
- B. Use a public subnet for the web tier and a private subnet for the database layer.right
- C. Use a private subnet for the web tier and a private subnet for the database layer.

- D. Use a private subnet for the web tier and a public subnet for the database layer.

Explanation:

Correct Answer – B
The ideal setup ensures that the web server 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 from AWS Documentation 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 61

Domain: Design Secure Applications and Architectures

An IT company wants to secure its resources in its AWS Account. Which of the following options would secure data at rest and in transit in AWS? (SELECT THREE)

- A. Encrypt all EBS volumes attached to EC2 Instances.right
- B. Use Server-Side Encryption for S3.right
- C. Use SSL/HTTPS when using the Elastic Load Balancer.right
- D. Use IOPS Volumes when working with EBS Volumes on EC2 Instances.

Explanation:

Correct Answers – A, B and C

AWS documentation mentions the following.

Amazon EBS encryption offers you a simple encryption solution for your EBS volumes without the need for you to build, maintain, and secure your own key management infrastructure. When you create an encrypted EBS volume and attach it to a supported instance type, the following types of data are encrypted.

- Data at rest inside the volume
- All data moving between the volume and the instance
- All snapshots created from the volume

Data protection refers to protecting data while in transit (as it travels to and from Amazon S3) and at rest (while it is stored on disks in Amazon S3 data centers). You can protect data in transit by using SSL or by using client-side encryption. You have the following options of protecting data at rest in Amazon S3.

- Use Server-Side Encryption – You request Amazon S3 to encrypt your object before saving it on disks in its data centers and decrypt it when you download the objects.
- Use Client-Side Encryption – You can encrypt data client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, the encryption keys, and related tools.

You can create a load balancer that uses the SSL/TLS protocol for encrypted connections (also known as *SSL offload*). This feature enables traffic encryption between your load balancer and the clients who initiate HTTPS sessions and connections between your load balancer and your EC2 instances.
For more information on securing data at rest, please refer to the below link-

https://d0.awsstatic.com/whitepapers/aws-securing-data-at-rest-with-encryption.pdf

Question 62

Domain: Design Cost-Optimized Architectures
Your company currently has a set of EC2 Instances running a web application that sits behind an Elastic Load Balancer. You also have an Amazon RDS instance which is accessible from the web application. You have been asked to ensure that this architecture is self-healing in nature. What would fulfill this requirement? (SELECT TWO)

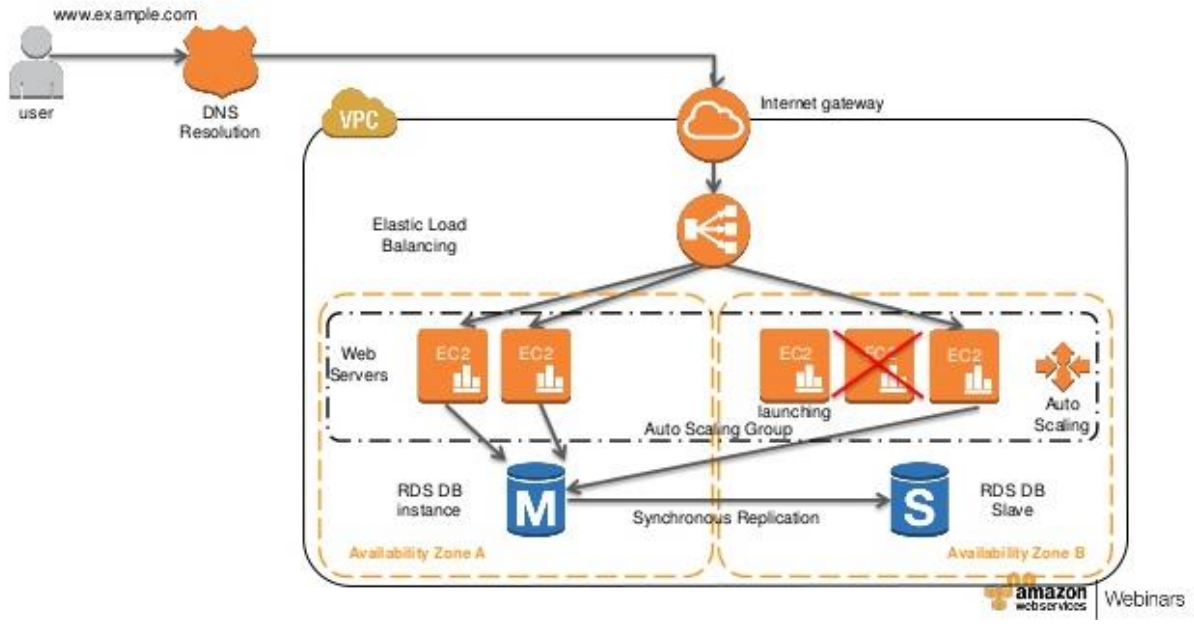
- A. Use CloudWatch metrics to check the utilization of the web layer. Use Auto Scaling Group to scale the web instances accordingly based on the CloudWatch metrics.right
- B. Use CloudWatch metrics to check the utilization of the database servers. Use Auto Scaling Group to scale the database instances accordingly based on the CloudWatch metrics.

- C. Utilize the Read Replica feature for the Amazon RDS layer.

- D. Utilize the Multi-AZ feature for the Amazon RDS layer.right

Explanation:

Correct Answers - A and D
The following diagram from AWS showcases a self-healing architecture where you have a set of EC2 servers as a Web server launched by an Auto Scaling Group.



AWS Documentation mentions the following.

Amazon RDS Multi-AZ deployments provide enhanced availability and durability for Database (DB) Instances, making them a natural fit for production database workloads. When you provision a Multi-AZ DB Instance, Amazon RDS automatically creates a primary DB Instance and synchronously replicates it to a standby instance in a different Availability Zone (AZ). Each AZ runs on its own physically distinct, independent infrastructure and is engineered to be highly reliable.

In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby (or to a read replica in the case of Amazon Aurora) so that you can resume database operations as soon as the failover is complete. Since the endpoint for your DB Instance remains the same after a failover, your application can resume database operation without the need for manual administrative intervention.

- For more information on Multi-AZ RDS, please refer to the below link-
  - https://aws.amazon.com/rds/details/multi-az/

Question 63

Domain: Design Secure Applications and Architectures

Your company has a set of EC2 Instances that access data objects stored in an S3 bucket. Your IT Security department is concerned about this architecture's security and wants you to implement the following.

1) Ensure that the EC2 Instance securely accesses the data objects stored in the S3 bucket.

2) Prevent accidental deletion of objects.

What would be helpful to fulfill the requirements of the IT Security department? (SELECT TWO)

- A. Create an IAM user and ensure the EC2 Instances use the IAM user credentials to access the bucket data.

- B. Create an IAM Role and ensure the EC2 Instances use the IAM Role to access the bucket data.right
- C. Use S3 Cross-Region Replication to replicate the objects so that the integrity of data is maintained.

- D. Use an S3 bucket policy that ensures that MFA Delete is set on the objects in the bucket.right

Explanation:

Correct Answers - B and D
AWS Documentation mentions the following.

IAM roles are designed to securely make API requests from your instances without requiring you to manage the security credentials that the applications use. Instead of creating and distributing your AWS credentials, you can delegate permission to make API requests using IAM roles.

For more information on IAM Roles, please refer to the link below.

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html
MFA Delete can be used to add another layer of security to S3 Objects to prevent accidental deletion of objects.

For more information on MFA Delete, please refer to the link below.

https://aws.amazon.com/blogs/security/securing-access-to-aws-using-mfa-part-3/

Question 64

Domain: Design High-Performing Architectures
You have a requirement to get a snapshot of the current configuration of resources in your AWS Account. Which service can be used for this purpose?

- A. AWS CodeDeploy

- B. AWS Trusted Advisor

- C. AWS Configright
- D. AWS IAM

Explanation:

Correct Answer - C
AWS Documentation mentions the following.

With AWS Config, you can do the following.

- Evaluate your AWS resource configurations for desired settings.
- Get a snapshot of the current configurations of the supported resources that are associated with your AWS account.
- Retrieve configurations of one or more resources that exist in your account.
- Retrieve historical configurations of one or more resources.
- Receive a notification whenever a resource is created, modified or deleted.
- View relationships between resources. For example, you might want to find all resources that use a particular security group.

For more information on AWS Config, please visit the below URL-

http://docs.aws.amazon.com/config/latest/developerguide/WhatIsConfig.html

Question 65

Domain: Design High-Performing Architectures
Your company is hosting an application in AWS. The application is read-intensive and consists of a set of web servers and AWS RDS. It has been noticed that the response time of the application increases due to the load on the AWS RDS instance. Which of the following measures can be taken to scale the data tier? (SELECT TWO.)

- A. Create Amazon DB Read Replicas. Configure the application layer to query the Read Replicas for query needs.right
- B. Use Auto Scaling to scale out the database tier.
- C. Use SQS to cache the database queries.
- D. Use ElastiCache in front of your Amazon RDS DB to cache common queries.right

Explanation:

Correct Answers - A and D
AWS documentation mentions the following.

Amazon RDS Read Replicas provide enhanced performance and durability for database (DB) instances. This replication feature makes it easy to elastically scale out beyond a single DB Instance's capacity constraints for read-heavy database workloads. You can create one or more replicas of a given source DB Instance and serve high-volume application read traffic from multiple copies of your data, thereby

increasing aggregate read throughput. Read replicas can also be promoted when needed to become standalone DB instances.

For more information on AWS RDS Read Replica's, please visit the URL below:

https://aws.amazon.com/rds/details/read-replicas/
Amazon ElastiCache is a web service that makes it easy to deploy, operate, and scale an in-memory data store or cache in the cloud. The service improves web applications' performance by allowing you to retrieve information from fast, managed, in-memory data stores instead of relying entirely on slower disk-based databases.